

# Table of Contents

---

ACS and Network Rights and Permissions	3
Managing ACS Users	4
Adding ACS User Records	4
Editing ACS User Records	5
Deleting and Deactivating ACS User Records	5
Mass Assigning User Security Settings	6
Resetting ACS User Logins	8
Logging In as Another ACS User	8
Log In Users Automatically in Add/Edit Users	8
Working with Users and Security Templates	10
Working with the User Log	12
Viewing User Security Settings	13
Filtering and Sorting Information	13
Printing the User Profile Report	13
Setting People Suite Security Rights	15
Attendance Security Rights	15
Checkpoint Security Rights	16
Church Growth Tools Security Rights	18
Connections Security Rights	19
Contributions Security Rights	20
DataShare Security Rights	22
Organizations Security Rights	23
People Security Rights	25
Reservations Security Rights	28
Special Mailings Security Rights	29
Setting Financial Suite Security Rights	31
Accounts Payable Security Rights	31
Accounts Receivable Security Rights	33
Fixed Assets Security Rights	35
General Ledger Security Rights	36
Parochial Report Security Rights	38
Payroll Security Rights	39
Purchase Orders Security Rights	41
Report Designer Security Rights	42
Utilities Security Rights	43

# Users and Security

---

Ensuring that the ACS users in your organization have adequate security rights is a very important task. In Users and Security, you can assign usernames and passwords for ACS, along with each ACS user's security rights for the different modules. In some cases, users can only perform functions on data they have entered. For example, in Contributions, a user can only post transactions that they have entered into ACS.

Security in ACS is assigned per user. Users are granted rights for each module in ACS. Rights determine whether a user has access to different areas of the software. For example, a user who does not have rights to Add/Edit Chart of Accounts in General Ledger cannot add a new account or edit an existing account.

For information about file level rights and permissions, see the topic [ACS and Network Rights and Permissions](#).

# ACS and Network Rights and Permissions

---

## **OnDemand Customers**

If you are using OnDemand, click [here](#) for information on setting permissions.

Most operating systems allow an administrator to set security settings at the file and/or directory level. Often, a network administrator restricts certain users to read-only access to certain files and no access to others for security purposes.

ACS routinely writes temporary files into the various ACS directories on both the server and workstation. Because of this, users need full control permissions to certain folders and their sub-directories. Please note that this is full access and not administrative rights.

After installing ACS, users need full control permissions to the following folders:

- X:\ACSNET - the X represents your network drive
- C:\WINACS
- C:\ProgramData\ACSTechnologies

This does not allow uncontrolled access to sensitive data; ACS data files cannot be read in a text editor. These files must be read with special database software. Any files with sensitive information that can be easily discerned are password protected.

For information on how to set network rights and permissions, check your network operating system documentation or contact your network administrator.

## **Anti-Virus Software**

If you are using anti-virus software, view the help topic [Anti-Virus Software and ACS](#) to set up exclusions for the applicable files.

# Managing ACS Users

---

On the **Users** tab of the Add/Edit Users window, you can manage your organization's ACS users and their security rights.

Your first step is [adding a user record](#) for anyone in your church or organization who will use ACS. Then, you can set up security options for both ACS People Suite and ACS Financial Suite. If someone in your organization needs additional rights, you can [edit the user record](#) to assign those rights, or you can [delete or deactivate records](#) if an employee or volunteer leaves your organization.


You can also [mass assign security settings](#), which lets you update security settings for all or several user names at once. This is helpful after installing an ACS upgrade or revision that may have new security features.

## Adding ACS User Records

---

Before someone in your church or organization can use ACS, he or she must have a user record. You can set up a user record, including the individual's username, password, and security permissions, in Add/Edit Users.

To add a user record


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. In the Add/Edit Users window, click **Add**.
4. Enter a **User Name**, **First Name**, **Last Name**, and **Description** (such as a job description). All user names and passwords must be at least 3 characters in length.
5. If you want the user to be automatically logged into ACS when he/she logs into the network, enter a **Network Login Name**. This allows the user to skip the login window.
6. In the **Password** and **Confirm Password** fields, enter and confirm the user's password, then click Next.
7. Enter the user's **Address** and **Phone/E-mail** information, then click **Next**.
8. To limit the user's access in the People Suite, select the area you want to limit and click **Select** to choose the individual restrictions for the area.
9. To limit the user's access in the Financial Suite, select the area you want to limit and click **Select** to choose the individual restrictions for the area.
10. Under **Set Security**, select one of the following options:
  - **Add/Edit Users** — If the user is the primary user or system administrator, select this option. ACS Technologies suggests that you select this feature for at least one user to always make sure you can access the ACS system, since selecting this feature prevents deletion of the user's profile.
  - **Copy From Template** — To copy security settings for the user from an existing template, select this option. Select the template to use from the drop-down list.
  - **Copy From Another User** — To copy security settings for the user from another user, select this option. Select the user to copy security settings from in the drop-down list.
  - **Set to None** — To set all security settings for the user to **None**, select this option.
11. Click **Finish**.

## Editing ACS User Records

---

You can change or update existing user accounts in Add/Edit Users.

To edit a user's record

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. From the drop-down list, select **Add/Edit Users** and click **Go** .
3. Select the user whose information you want to edit, then click **Edit**.
4. On the **User Name** and **Password** pane, make any needed edits to the User Name, Password, and Network Login Name.
5. On the **Information** pane, make any needed edits to the user's First Name, Last Name, and Description.
6. On the **Information**, **Security**, and **Contact Information** tabs, change the user's profile, security rights, address, or contact information, as needed.
7. When finished, click **Apply**, then **OK**.

## Deleting and Deactivating ACS User Records


---

You can delete or deactivate ACS user records. Deleting a record removes the record from ACS completely, but if there's a chance you may need to update or use the record again in the future, you can deactivate it.


### Info

If you delete an ACS user, then add the user back, you can access that user's saved searches and reports. This is helpful if a staff member leaves the church or organization and you need to access these. However, all user settings in grids and windows are lost when you delete a user.

To delete a user record

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. Select the user you want to delete, then click **Delete**.
4. When the confirmation message displays, click **Yes**, then **OK**.

To deactivate a user record

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. From the drop-down list, select **Add/Edit Users** and click **Go** .
3. Select the user you want to deactivate, then click **Edit**.
4. Under **User Name and Password**, select **Inactive**.
5. Click **Apply**, then **OK**.


# Mass Assigning User Security Settings

---

If you want to update security settings for all or several user names at once, using the Mass Assign option can save you time and help avoid making errors. Since you select the security bit only once, you eliminate the risk of selecting a wrong security bit for a user.

An ideal time to use the Mass Assign expert is after installing an ACS upgrade with new features that require additional security settings. Once you determine your users who need the new security setting and the access you want to give them, use the following procedure to assign the security rights.

To update security settings with the Mass Assign expert

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. Click **Mass Assign**.
4. Make your selections in the first window of the expert, then click **Next**.
5. To update the security limits for the People or Financial Suites, make your selections in the second window of the expert, then click **Next**.
6. In the third window of the expert, select the users to which you want to assign the new security settings.
7. To update your security templates, select the templates that you want to update.
8. Click **Finish**, then **OK**.

## Additional Field Information

### First Window

- **Add/Edit Users** — Select the security setting in the drop-down list you want to assign to users.
- **Security** — A list of each module in the Financial and People Suites. Expand the module name to display the options that require security rights.
- **Access** — Displays the security rights assigned to the option. Double-click the security access to change it to your choice.

### Second Window

- **Retain Current** — No change is made to the current setting. To make a change to the setting, clear the check box.
- **Limit Comments** — To restrict the comment types a user can view, clear the **Retain Current** check box. Select **Limit Comments**, then click **Select** and choose the comment types you do not want the user to view.
- **Limit Groups** — To restrict the master groups a user can access, clear the **Retain Current** check box. Select **Limit Groups**, then click **Select** and choose the master groups you want the user to access.
- **Limit Contact Types** — To restrict the contact types a user can access, clear the **Retain Current** check box. Select **Limit Contact Types**, then click **Select** and choose the contact types you do not want the user to access.
- **Limit Reservation Activities** — To restrict the reservation activities a user can access, clear the **Retain Current** check box. Select **Limit Reservation Activities**, then click **Select** and choose the reservation activities you want the user to access.
- **Limit Departmental Fields** — To restrict the departmental fields a user can access, select the appropriate checkbox under **View Access** to grant the user viewing rights to a departmental field. To restrict a user from editing a departmental field, clear the appropriate checkbox under **Edit Access**.
- **Limit Datasets** — To restrict the datasets a user can access, clear the **Retain Current** check box. Select **Limit Datasets**, then click **Select** and choose the datasets you want the user to access.
- **Limit G/L Inquiry** — To restrict the general ledger account codes a user can access in Inquiry, clear the **Retain Current** check box. Select **Limit G/L Inquiry**, then click **Select**. Select the correct dataset, then select the areas to which you want to give the user access.

### Third Window


- **Assign?** — Select the check box for each user to whom you want to assign the new security settings.
- **User** — Displays the ACS user name or template name.
- **Name** — Displays the first and last name of the user, if available.
- **Description** — Displays the label or name of the user name or template, if available.

## Resetting ACS User Logins

---

If a user is unable to properly log out of ACS, the program may not let him or her log in, or an error displays saying that the user is already logged in. If this occurs, you can reset that user's login.

To reset a user's login


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. Select the user whose username you need to reset.
4. Click **Clear Login**.

## Logging In as Another ACS User

---

In Admin Utilities, you can log into ACS with another username and password. This is helpful if someone else needs to log into ACS on your computer, as you do not have to exit and restart the program. It's also helpful if you want to verify security rights when setting them up.

To log into ACS as another user


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Login as...** and click **Go** .
3. Enter the username and password, then click **OK** to log in.

## Log In Users Automatically in Add/Edit Users

---

You can set up an option to log into ACS automatically. This works along with your network username (the username you use to log in to your computer) to bypass the ACS log in window.

To login users automatically

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. Select **Login Users Automatically**.
4. Select a user, then click **Edit**.
5. In the **Network Login Name** field, enter the user's network username (the username used to log in to the computer).



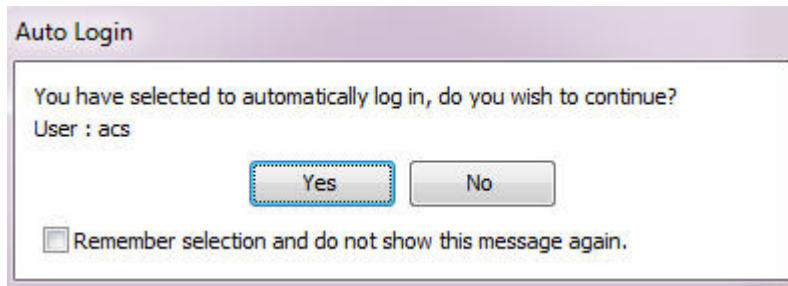
### **OnDemand Customers**

For OnDemand customers, the **Network Login Name** will be your OnDemand username.



6. Click **Apply**, then click **OK**.

Once this is set up, a message displays the next time you log in.



If you select to remember the selection and not display the message again, the program automatically opens. You can reset this so the message displays again upon opening the program, and you have the option to log in as another user.

To reset the automatic login feature for a user

1. Under Advanced Tools, click **My Preferences**.
2. Click **Reset Auto Login**.
3. When the confirmation message displays, click **Yes**.

# Working with Users and Security Templates


---

Templates identify the type of ACS user and assign default security rights.


For example, if your organization has several staff personnel who are responsible for tracking youth oriented activities, you can create a template called Youth. Then, you can enter these people as ACS users and apply the Youth template to assign the appropriate security access levels.

If you use a template, you are not limited to the default rights assigned by that template. You can edit the individual user's rights at any time. Editing or deleting a template does not affect the user rights of any user whose security was set up using the template.

To add a template


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. Click the **Templates** tab, then click **Add**.
4. In the **Template** field, enter a name for the template.
5. In the **Description** field, enter a description for the template.
6. **Optional:** Assign the user **All**, **View**, or **None** rights to all areas within the selected module using one of the following methods:
  - Type **A**, **V**, or **N** to set the security to **All**, **View**, or **None** respectively.
  - Right-click on the module field and select the security setting you want.
7. **Optional:** Double-click on a module. The available security fields for the module display.
8. **Optional:** Assign the user **All**, **View**, or **None** rights to a specific area within the selected module using one of the following methods:
  - Type **A**, **V**, or **N** to set the security to **All**, **View**, or **None** respectively.
  - Right-click on the field and select the security setting you want.
  - Double-click the field until the security setting you want displays.
9. Click **OK**.

To edit a template

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. On the **Templates** tab, select the template you want to edit, then click **Edit**.
4. **Optional:** Assign the user **All**, **View**, or **None** rights to all areas within the selected module using the following methods:
  - Typing **A**, **V**, or **N** to set the security to **All**, **View**, or **None** respectively.
  - Right-click on the module field and select the security setting you want.
5. **Optional:** Double-click on a module. The available security fields for the module display.

6. **Optional:** Assign the user **All**, **View**, or **None** rights to a specific area within the selected module using the following methods:
  - Typing **A**, **V**, or **N** to set the security to **All**, **View**, or **None** respectively.
  - Right-click on the field and select the security setting you want.
  - Double-click the field until the security setting you want displays.
7. Click **Apply**, then **OK**.

To delete a template


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go**  .
3. Select the template you want to delete and click **Delete**.
4. Click **Yes**, then **OK**.

# Working with the User Log



---

When **Enable Log Tracking** is active, the **User Log** tab displays the login and logout times for all users who have accessed the People Suite, Financial Suite, or Utility Manager.

To enable the user log

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go**  .
3. On the **User Log** tab, click **Enable Log Tracking**. To disable this option, click **Disable Log Tracking**.

To print the User Log Activity report

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go**  .
3. On the **User Log** tab, click **Print**.
4. When the report displays, click **Print Report**  .

# Viewing User Security Settings

---

The View User Security tab displays ACS users and their security settings in a grid view. You can sort and filter the grid, plus print several reports.

## Filtering and Sorting Information



---

You can sort the information in the grid in a variety of ways. For example, you may want to see all modules and all areas that one of your users has access to, or you may want to know who has rights to the Promotion option in Attendance. You can:

- **Group by item within a column** — Highlight an item in a column (such as a user name, module, or security option) and click the item heading.
- **Group by Heading** — Drag a column heading into the gray area above to group information by the heading. Expand the groupings to view additional information.
- **Sort column in ascending or descending order** — Click a heading then click the small gray up or down arrows in the heading bar.
- **Select multiple columns to sort** — Press Shift and select the columns you want to sort.

To filter the grid, you must select **Enable Filtering**.

To filter the grid


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. On the **View User Security** tab, highlight a column heading.
4. Click  in the heading.
5. Choose the filter you want to use.


## Printing the User Profile Report

---

You can also print the User Profile report, which includes each user and their permissions for each module. Select Print Limits on User Profile (in the right-click list) before printing if you want each user's limits included in the report. These limits include comment and contact types, and Master Groups, Reservation activity, financial dataset, and GL Inquiry limits.

To print the User Profile Report

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. Click on the **View User Security** tab.

4. Under **User Name**, select the user whose profile you want to print.
5. Inside the grid, right-click and select **Print**.
6. When the report displays, click **Print Report**  .


# Setting People Suite Security Rights

---

On the **Security** tab, you can set an ACS user's security rights in the People Suite.

When setting up security rights, remember it's easier to give more clearance as you go than take away access. It's also a good idea to make sure all employees and volunteers in your organization have access to what they need. To verify security rights, you can [log in as another ACS user](#).

To set an ACS user's People Suite security rights


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. On the **Users** tab, select the ACS user whose security rights you want to edit, then click **Edit**. If the user does not have an ACS username, see [Adding ACS User Records](#) to learn how to set one up.
4. In the Edit User window, click on the **Security** tab.
5. Expand the name of the module you want to edit security rights for.
6. Use one of the following methods to assign the user All, View, or None rights to a specific area:
  - Type **A**, **V**, or **N** to set the security to **All**, **View**, or **None** respectively.
  - Right-click on the field and select the security setting you want.
  - Double-click the field until the security setting you want displays.
7. When finished, click **Apply**, then **OK**.

## Attendance Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Attendance module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Attendance**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Add/Edit Individual Classes**

Determines whether the user can add an individual to an Attendance class.

### **Change Group's Parent**

Determines whether or not the user can edit a groups' parent.

### **Enter/Post Attendance**

Determines whether the user can record attendance.

### **Graphs**

Determines whether the user can view or print graphs.

### **Inquiry**

Determines whether the user can view individual or group Attendance markings.

### **Mark Non-Enrolled**

Determines whether the user can mark attendance as non-enrolled.

### **Promotion**

Determines whether the user can promote whole classes at one time.

### **Reports**

Determines whether the user can print or preview Attendance reports.

### **Searches**

Determines whether the user can perform searches on attendance data.

### **Setup**

Determines whether the user can add, edit, delete, or configure Attendance classes.

### **View/Edit Group Classes**

Determines whether the user can set up class rosters.


## **Checkpoint Security Rights**

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Checkpoint module.

To edit a user's security rights



1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go**  .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Checkpoint**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Add/Edit Badge Design**

Determines whether the user can add, edit, or delete a badge design.

### **Add/Edit Checkpoint Defaults**

Determines whether a user can add or edit Checkpoint defaults.

### **Add/Edit Individuals**

Determines whether a user can add, edit, or delete individual information in Checkpoint.

### **Add/Edit Sessions**

Determines whether the user can add, edit, or delete Checkpoint sessions.

### **Add/Edit Templates**

Determines whether the user can add, edit, or delete Checkpoint templates.

### **Check In/Out**

Determines whether the user can access the Check In/Out and Express Check In/Out menus.

### **Edit Add People Defaults**

Determines whether the user can modify the defaults for new individual records added in Checkpoint.

### **Edit Name Options**

Determines whether the user can modify name option defaults in Checkpoint.

### **Off-Site Synchronization**

Determines whether the user can import/export data to/from an off-site network.

### **Reports**

Determines whether the user can print or preview reports.

### **Session Statistics**


Determines whether the user can access or modify the Session Statistics window.

## **Church Growth Tools Security Rights**

---

You can grant rights to Reports in the Church Growth Tools module.

To edit a user's security rights


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go**  .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Church Growth Tools**.
6. Select **Reports**, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## Connections Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Connections module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go**  .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Connections**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Add/Edit Contacts**

Determines whether the user can add new contacts, schedule contacts, assign contacts, add special instructions for the connections team, record connections by prospects to your church, print the Connections Profile, and schedule future actions.

### **Allow Contact Completion**

Determines whether the user can complete a contact.

### **Define Lists**

Determines whether the user can rename the Assignment Team and Age Group lists, add elements to the Age Group list, add classifications and responses, assign responses, add and edit templates, add teams, and assign members to teams.

### **Edit Cards**

Determines whether the user can create new connections cards, edit existing cards, and delete old cards.

### **Graphs**

Determines whether the user can view or print graphs.

### **Inquiry**

Determines whether the user can view Connections information.

### **Mass Add**

Determines whether a user can add a contact to several Connections records at one time using the Mass Add function.

### **Mass Change**

Determines whether the user can use Mass Change to update multiple records at the same time.

### **Reports**

Determines whether the user can print or preview reports and cards from Connections.

### **Searches**


Determines whether the user can perform searches on contacts and responses.

## **Contributions Security Rights**

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Contributions module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Contributions**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

### **Additional Field Information**

#### **Add/Edit Fund Codes**

Determines whether the user can [add new funds](#), [change the accounts associated with a contributions fund](#), or [set up a giving plan for a fund](#).

#### **Add/Edit Pledges**

Determines whether the user can add a new [pledge](#) for an individual, change an existing pledge, delete a pledge record, or copy a group of pledges from one year to another.

#### **Edit All Users Transactions**

Select to allow the user to [edit](#) and [delete](#) contributions gifts entered by all users.

#### **Enter All Funds**

This option applies only to multi-campus users and the user has limited campus rights. Select to allow the user to enter a gift to another campus's fund. Once the gift is posted, the user no longer sees the gift. This situation happens when a contributor visits a campus other than their home campus and makes a contribution, but wants their gift applied to their home campus.

#### **Enter Transactions Contributions**

Determines whether the user can [enter contributions transactions](#).

#### **Graphs**

Determines whether the user can [view or print graphs](#).

#### **Inquiry By Fund Codes**

Determines whether the user can [view transactions for each fund](#).

#### **Inquiry By Individual**

Determines whether the user can [view an individual's giving record](#).

### **Post All Users Batches**

Determines whether the user can [post batches of gifts](#) entered by other users, or only batches the user has entered.

### **Post Transactions**

Determines whether the user can [post gifts](#) he/she entered.

### **Reports**

Determines whether the user can [print or preview Contributions reports](#), including statements listed on the Reports menu.

### **Searches**

Determines whether the user can perform searches on contributions gifts and pledges.

### **Setup**

Determines whether the user can [configure Contributions](#), update a contributor's checking account information, set up bank account information for use with direct withdrawal, and reassign envelope numbers for a group of contributors.

### **Setup Vanco Accounts**

Determines whether the user can setup Vanco Services Accounts for the Vanco Gift Import.

### **Statements**

Determines whether the user can print or preview [Contributions statements](#) listed on the Statements menu. This does not affect statements on the Reports menu.

### **Summarize Data**

Determines whether the user can [summarize Contributions data](#).

## **DataShare Security Rights**

---


Before using DataShare, you need to set up security rights in Add/Edit Users. The security options you select depend on the data you will send and receive.

For example, if your church or organization needs to send records to a denominational office, organization, or diocese, you need access to **Send Changes to DataShare**. If the denominational office or diocese changes records that also need to be updated in your database, you need access to **Get Changes from DataShare**.

Or, suppose you are a denominational office, organization, or diocese that needs to get updated records from various churches. You need access to **Get Changes from DataShare**. If you will send updated information to those churches, you also need access to **Send Changes to DataShare**.

In addition, you may not want volunteers in your church or organization to send and receive updated information in DataShare. For these users, select **None** to restrict access to DataShare. Users who do not have access to DataShare still see updated records after changes are received.

To grant or restrict DataShare access


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. Select **Add/Edit Users** and click **Go** .
3. On the **Users** tab, select the user whose DataShare security options you want to grant or restrict, then click **Edit**.
4. In the Edit User window, on the **Security** tab, expand **DataShare**.
5. If granting access to DataShare, under **Access**, select **All** for **Get Changes from DataShare** or **Send Changes to DataShare**.
6. If restricting access, select **None** for **Get Changes from DataShare** or **Send Changes to DataShare**.
7. Click **OK**.

## Organizations Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of ACS Organizations.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Organizations**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

### **Additional Field Information**

#### **Add Organizations**

Determines whether the user can add a new organization.

#### **Add/Edit Organization Activities**

Determines whether the user can add or edit organization activities.

#### **Add/Edit Staff**

Determines whether the user can add or edit an individual.

#### **Add/Edit Statistics**

Determines whether the user can add or edit statistics.

#### **Comments**

Determines whether the user can add, edit, view, or delete Organization's comments.

#### **Configure Statistics**

Determines whether the user can configure statistics.

#### **Define Lists**

Determines whether the user can set up organization levels, check whether pin numbers and envelope numbers are the same, set up user-defined fields, and define staff positions.

#### **Define Statistics Views**

Determines whether the user can define the view of statistics reports.

#### **Delete Organizations**

Determines whether the user can delete organizations.

#### **Edit Organizations**

Determines whether the user can view an organization's record, edit an organization's record, access the Organizations Library, and enter statistics.

#### **Mass Change**

Determines whether the user can perform mass change functions.

#### **Reports**

Determines whether the user can print or preview Organizations reports.

#### **Searches**

Determines whether the user can perform searches.

#### **Setup**

Determines whether the user can access Organizations setup options.

#### **Staff Maintenance**

Determines whether the user can copy staff and statistical records from one year to another.




# People Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the [People](#) module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **People**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Activities Setup**

Determines whether the user can create new activity groups and add, edit, or delete activity group elements.

### **Add Family/Individual**

Determines whether the user can add new families and individuals.

### **Add/Edit Individual Activities**

Determines whether the user can add an individual to an activity group.

### **Background Checks**

Determines whether the user can [request a background check](#) on an individual.

### **Change Family Unit**

Determines whether the user can move an individual from one family to another, start a new family with an individual who is already a member of a family, and change an individual's family position.

### **Comments**

Determines whether the user can add, edit, view, or delete family and individual comments.

### **Constant Contact**

Determines whether the user can access Constant Contact when sending e-mail.

**Date of Birth**

Determines whether the user can access Date of Birth records.

**Define Lists**

Determines whether the user can add, edit, or delete address types, phone types, or comment types and whether the user can define user-defined fields, lists, and dates.

**Delete Family/Individual**

Determines whether the user can delete organizations, families, and individuals.

**Document Library**

Determines whether the user can view, edit, copy, or delete files in the library.

**Edit Family/Individual**

Determines whether the user can edit or view existing user records.

**Exports**

Determines whether the user can create extracts, including the Phone Tree, which is found on the Reports menu. By selecting View, a user can run an extract, but cannot create a new extract or edit an existing extract.

**Graphs**

Determines whether the user can view or print graphs.

**Labels**

Determines whether the user can create and print labels. By selecting View, a user can print labels, but cannot create or edit the layout.

**Mass Change**

Determines whether the user can use Mass Change to update multiple records at the same time.

**Mass Delete**

Determines whether the user can use Mass Delete to delete multiple records at the same time.

**Member Status**

Determines whether the user can add and edit or only view an individual's Member Status.

**Merge Records**

Determines whether the user can [merge records](#).

**Multi-Campus Setup**

Determines whether the user can add, edit, and delete campuses. Besides adding, editing, and deleting campuses, the user can also select service times and the Contributions fund codes used by each campus.

**Pictures**

Determines whether the user can add, view, or remove pictures.

### **Quick View Setup**

Determines whether the user can access Setup to configure Quick View.

### **Reports**

Determines whether the user can print or preview People reports.

### **Safeguard Comments**

Determines whether the user can view, add, edit, or delete comments on the [Safeguard](#) tab.

### **Safeguard Tasks**

Determines whether the user can view, add, edit, or delete tasks on the [Safeguard](#) tab.

### **Safeguard Tasks Mass Create and Update**

Determines whether the user can mass change and create Safeguard tasks through search results.

### **Searches**

Determines whether the user can perform searches on individual information, families, addresses, phone numbers, e-mail addresses, activities, and comments.

### **Send Mass Email**

Determines whether the user can send a mass e-mail.

### **Setup**

Determines whether the user can access People setup options.

### **Setup Departmental Fields**

Determines whether the user can set up departments and fields.

### **Small Groups**

Determines whether the user can use the Small Groups option.

### **Social Security Number**

Determines whether the user can access Social Security Number records.

### **Sync with DioOffice**

Determines whether the user can use the sync option to upload People data to [PDS DioOffice](#).

### **Upload Records to Access ACS**

Determines whether the user can upload ACS records into Access ACS.

### **View/Edit Group Activities**

Determines whether the user can view or edit an activity group.

### **View/Edit Department Fields**


Determines whether the user can view or edit department fields.

## Reservations Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Reservations module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Reservations**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

### **Additional Field Information**

#### **Add/Edit Reservations**

Determines whether the user can add reservations to an activity or event, edit or delete a reservation, and enter payments.

#### **Refresh**

Determines whether the user can refresh Reservations information.

#### **Reports**

Determines whether the user can print or preview Reservations reports.

#### **Setup**


Determines whether the user can add new activities, edit an existing activity's properties, or delete an activity.

## **Special Mailings Security Rights**

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Special Mailings module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Special Mailing**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Add/Edit Groups**

Determines whether the user can add individuals to a mailing group, copy a mailing group's membership to another mailing group, move a mailing group's membership to another mailing group, and remove a group of individuals from a mailing group.

### **Add/Edit Individuals**

Determines whether the user can add new individuals, edit an existing individual's record, delete an individual, and add an individual to a mailing group.

### **Define Group Lists**

Determines whether the user can add new mailing groups, rename an existing mailing group, and delete a mailing group.

### **Reports**

Determines whether the user can print or preview reports and labels from Special Mailings.


# Setting Financial Suite Security Rights

---

On the **Security** tab, you can set an ACS user's security rights in the Financial Suite.

When setting up security rights, remember it's easier to give more clearance as you go than take away access. It's also a good idea to make sure all employees and volunteers in your organization have access to what they need. To verify security rights, you can [log in as another user](#).

To set an ACS user's Financial Suite security rights


1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users** and click **Go** .
3. On the **Users** tab, select the ACS user whose security rights you want to edit, then click **Edit**. If the user does not have an ACS username, see [Adding ACS User Records](#) to learn how to set one up.
4. In the Edit User window, click on the **Security** tab.
5. Expand the name of the module you want to edit security rights for.
6. Use one of the following methods to assign the user All, View, or None rights to a specific area:
  - Type **A**, **V**, or **N** to set the security to **All**, **View**, or **None** respectively.
  - Right-click on the field and select the security setting you want.
  - Double-click the field until the security setting you want displays.
7. When finished, click **Apply**, then **OK**.

# Accounts Payable Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Accounts Payable module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Accounts Payable**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **1099 Adjustments**

Determines whether the user can [enter dollar amounts that are reflected in year-to-date totals and 1099 statements](#), but are not posted to the General Ledger.

### **Add/Edit Vendors**

Determines whether the user can [add, edit, or delete vendors](#) in Accounts Payable.

### **Define Lists**

Determines whether the user can add, edit, or delete [vendor types](#) and invoice frequencies in Accounts Payable.

### **Edit All Users Invoices**

Determines whether or not the user can [modify all other users' invoices](#).

### **Enter Invoices**

Determines whether the user can [add and edit invoices](#).

### **Inquiry**

Determines whether the user can [view checks and invoices for vendors](#).

### **Period End Reports**

Determines whether the user can [print or preview Period End Reports](#).

### **Post All Users Invoices**

Determines whether the user can [post invoices](#) for all users.

### **Post Invoices**

Determines whether the user can [post invoices](#).

### **Print/Post Checks**

Determines whether the user can [issue checks, print checks, and post checks](#) to the general ledger.

### **Reports**

Determines whether the user can [print or preview reports](#) in Accounts Payable.

### **Setup**

Determines whether the user can [configure Accounts Payable](#) and [design custom checks](#).




# Accounts Receivable Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Accounts Receivable module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Accounts Receivable**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Add/Edit Customers**

Determines whether the user can [add new customers](#), edit a customer's record, or [delete customers](#).

### **Define Lists**

Determines whether the user can add, edit, or delete billing codes, payment codes, revenue centers, discount types, grades, and [user-defined lists](#).

### **Edit All Users Transactions**

Determines whether the user can edit all users' transactions.

### **Enter Invoices**

Determines whether the user can [add](#) and [edit](#) invoices.

### **Enter Payments**

Determines whether the user can [add](#) and [edit](#) payments.

### **Inquiry**

Determines whether a user can [view invoices and payments for customers](#).

### **Mass Assign Assistant**

Determines whether the user has access to the [mass assign assistant](#).

### **Post All Users Invoices**

Determines whether a user can [post all users' invoices](#).

### **Post All Users Payments**

Determines whether a user can [post all users' payments](#).

### **Post Invoices**

Determines whether the user can [post invoices](#).

### **Post Payments**

Determines whether the user can [post payments](#).

### **Reports**

Determines whether the user can [print or preview reports](#).

### **Setup**


Determines whether the user can [configure Accounts Receivable](#).

# Fixed Assets Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Fixed Assets module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Fixed Assets**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Add/Edit Fixed Assets**

Determines whether the user can [add new assets](#), [change the properties of an existing asset](#), set an asset's depreciation properties, delete an asset, or update an asset's maintenance records.

### **Define Lists**

Determines whether the user can [add, edit, or delete](#) asset categories, asset conditions, tax districts, and depreciation methods.

### **Enter/Post Depreciation**

Determines whether the user can [calculate depreciation](#) for the month or year, [print the Depreciation Journal](#), [post depreciation](#) to the General Ledger, and [close the month](#).

### **Import**

Determines whether the user can [import information into Fixed Assets](#).

### **Reports**

Determines whether the user can [print or preview Fixed Assets reports](#).

### **Setup**

Determines whether the user can [set the beginning posting month and year](#), and [set the default General Ledger source for depreciation](#).

# General Ledger Security Rights


---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the General Ledger module.

## Note

If you own the Accounts Payable module, the Add/Edit Vendors option in General Ledger controls the ability to add vendors through the Enter Checks option only. If you do not own the Accounts Payable module, the Add/Edit Vendors option in General Ledger controls all vendor information.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **General Ledger**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Account Inquiry**

Determines whether the user can [view transactions and balance information](#) for specific accounts, groups of accounts, bank accounts, and payees.

### **Add/Edit Budgets**

Determines whether the user can [enter or change budget information](#).

### **Add/Edit Chart of Accounts**

Determines whether the user can [add new accounts, add new account headings, move accounts, change account information, and delete accounts](#).

### **Add/Edit Vendors**

Determines whether the user can add, edit, or delete payees.

### **Bank Reconciliation**

Determines whether the user can [reconcile bank accounts](#) or [close the current month](#).

**Define Lists**

Determines whether the user can [add, edit, or delete](#) funds, departments, committees, areas, projects, sources, and bank account lists.

**Define Lists - Other**

Determines whether the user can [add, edit, or view](#) other options in Define Lists.

**Display/Merge Names**

Determines whether or not the user can merge names in the Global name list.

**Edit All Users Transactions**

Determines whether or not the user can [modify all other users' transactions](#).

**Enter Transactions**

Determines whether the user can [add and edit transactions](#).

**Post All Users Transactions**

Determines whether the user can [post all users' transactions](#).

**Post Transactions**

Determines whether the user can [post transactions](#).

**Reports**

Determines whether the user can [print or preview reports](#).

**Reprint Checks**

Determines whether the user can [reprint checks](#).

**Setup**

Determines whether the user can [set the default fund principal account](#), [set the account number format](#), [customize transaction options](#), and [design custom checks](#).

**Social Security Number**

Determines whether the user can view or change the social security number of a customer or employee.

**Year End Procedures**


Determines whether the user can [perform year-end procedures](#).

# Parochial Report Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Parochial Report.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Parochial Report**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Archive Reports**

Determines if users can [archive the parochial report](#).

### **Certification**

Determines if users can [complete the certification page](#) of the report.

### **Define Lists**

Determines if users can [add or edit user-defined fields](#).

### **Membership, Attendance and Services (Page 2)**

Determines if users can [generate the Membership, Attendance and Services page](#) of the report.

### **Services Register**

Determines if users can [add or edit information in the services register](#).

### **Setup for Membership, Attendance and Services (Page 2)**

Determines if users can [enter information in the Setup window for Membership, Attendance and Services \(Page 2\)](#).

### **Setup for Stewardship and Financial (Page 3)**

Determines if users can [enter information in the Setup window for Stewardship and Financial \(Page 3\)](#).

### **Stewardship and Financial (Page 3)**


Determines if users can [generate the Stewardship and Financial page](#) of the report.

## **Payroll Security Rights**

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Payroll module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Payroll**.

6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Add/Edit Employees**

Determines whether the user can [add a new employee](#), [edit an existing employee's payroll record](#), [deactivate an employee](#), and [delete an employee](#).

### **Add/Edit Lists**

Determines whether the user can [add](#), [edit](#), or [delete](#) pay types, adjustments, cost centers, and worker's compensation lists.

### **Add/Edit W2 Totals**

Determines whether a user can [enter or edit W-2 information](#).

### **Employee Self Service**

Determines whether a user can [register](#) for the [ACS Employee Self Service](#) site and upload records to the site.

### **Enter/Post Payroll**

Determines whether the user can [enter time sheets](#), process payroll, issue payroll checks, print payroll checks, void payroll checks, post payroll to the general ledger, print the payroll journal, and close the month.

### **Inquiry**

Determines whether a user can [view an employee's payroll history](#).

### **Period End Reports**

Determines whether a user can [print or preview period end Reports](#).

### **Reports**

Determines whether the user can [print or preview reports](#).

### **Setup**

Determines whether the user can [configure Payroll options](#).




# Purchase Orders Security Rights

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Purchase Orders module.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.
5. Expand **Purchase Orders**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

## **Additional Field Information**

### **Approve Purchase Orders**

Determines whether a user is authorized to [approve purchase orders](#).

### **Create A/P Invoices**

Determines whether the user can [create invoices in Accounts Payable from previously entered purchase orders](#) that have been received.

### **Define Lists**

Determines whether the user can [add, edit, or delete buyers and terms](#).

### **Edit All Users Purchase Orders**

Determines whether or not the user can [modify all other users' purchase orders](#).

### **Enter Purchase Orders**

Determines whether the user can [enter new purchase orders](#).

### **Post All Users Purchase Orders**

Determines whether a user is authorized to [post all users' purchase orders](#).

### **Post Purchase Orders**

Determines whether the user can enter [post purchase orders](#).

### **Reports**

Determines whether the user can [print Purchase Orders reports](#).

### **Setup**


Determines whether the user can [set Purchase Orders options](#).

## **Report Designer Security Rights**

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of the Report Designer.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go**  .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click the **Security** tab.

5. Expand **Report Designer**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

#### **Additional Field Information**

##### **Financial Direct Datasource**

Determines whether a user can access Financial Suite data for building reports.

##### **People Direct Datasource**

Determines whether a user can access People Suite data for building reports.

##### **Report Designer**


Determines whether a user can access the Report Designer program.

## **Utilities Security Rights**

---

You can grant rights to your users that allow them to have complete, limited, or no access to view or edit the different portions of Utilities.

To edit a user's security rights

1. Under Advanced Tools, click the **Admin Utilities** tab.
2. In the drop-down list, select **Add/Edit Users**, then click **Go** .
3. Select a user in the grid and click **Edit**.
4. If it is not already selected, click on the **Security** tab.
5. Expand **Utilities**.
6. Choose the security option you wish to change, then right-click to select the appropriate access level.
  - **All** allows the user to add and edit information.
  - **None** denies the user all access to the information.
  - **View** allows the user to view information without editing it.
7. Click **Apply**, then **OK**. Your changes take effect the next time the user logs into ACS.

#### **Additional Field Information**

**ACS Table Maintenance**

Determines whether the user can view or access ACS table information.

**Add/Edit SMTP Settings**

Determines whether a user can add or edit an SMTP address.

**Add/Edit ZIP Codes**

Determines whether the user can [add, edit, or delete ZIP codes](#).

**Backup Data**

Determines whether the user can [create an ACS backup file](#).

**Clear User Logins**

Determines whether the user can clear individual or all user logins.

**Edit Tax Tables**

Determines whether the user can make changes to the payroll tax tables.

**Maintenance Utilities**

Determines whether the user can access the [People](#) or [Financial](#) Maintenance Utilities.

**My Preferences**

Determines whether current users can [change their settings, grids, and menu style](#). Administrators can select settings for all users.

**Report Maintenance**

Determines whether the user can delete saved reports.

**Restore Data**

Determines whether the user can [restore an ACS backup file](#).

**Site Information/Financial Dataset Setup**

Determines whether the user can [create a new financial dataset](#), edit an existing financial dataset's address and tax numbers, delete an existing financial dataset, and switch between datasets. By selecting View, a user can switch between datasets, but cannot add, edit, or delete datasets.

**Support Utilities**

Determines whether the user can access the [Support Utility program](#).

**Year End Utilities**

Determines whether a user can access Year End Utilities.