



**FPSGOLD**

# **Security System**

# Table of Contents

Security System .....	5
Company Options Screen .....	7
Rules for Valid Passwords .....	11
Institution Name .....	12
Employee Number Length .....	12
Days to Force Employee Password Change .....	12
Minutes Without Activity to Close Terminal .....	13
Minimum Length of Password (5-40) .....	13
Customer Service Security .....	14
Force Alpha-Numeric Passwords .....	14
Force Special Characters in Passwords .....	14
User Defined Fields field group .....	15
User Defined Field Type 1 - 5 .....	15
User Defined Field Length 1 - 5 .....	16
User Defined Field Description 1 - 5 .....	16
Security Reports Screen .....	17
History tab .....	17
Changes to Display field group .....	19
CIM GOLD Employee Security .....	19
CIM GOLD Profile Security .....	19
Customer Service Cross Reference .....	19
EFT GOLD Options .....	19
Employee Details .....	19
Employee Password Reset .....	19
Employee Field Level Security .....	19
System Security .....	20
Options .....	20
Profile Field Level Security .....	20
Teller Details .....	20
Terminal Violation Reset .....	20
Selection Criteria field group .....	20
Start Date .....	20



End Date .....	20
Start Time .....	20
End Time .....	21
Changed by Employee# .....	21
History List View .....	21
Access tab .....	21
Employees .....	22
Tellers .....	22
CIM GOLD Profiles .....	22
System Profiles .....	22
Search .....	22
Include field group .....	22
Details .....	22
Teller Information .....	23
CIM GOLD .....	23
System .....	23
Field Level .....	23
Profile Assignments .....	23
All Assigned Profiles .....	23
Report on Effective Security .....	24
Exclude Inactive/Terminated Employees .....	24
Access List View .....	24
Securables tab .....	24
CIM GOLD .....	25
System .....	25
Field Level .....	25
Include field group .....	25
Employees .....	25
Profiles .....	25
Effective Security .....	25
Profile Assignments .....	26
Exclude Inactive/Terminated Employees .....	26
Securables List View .....	26
Employee/Profile Listing tab .....	26
Include field group .....	26
Employees .....	26

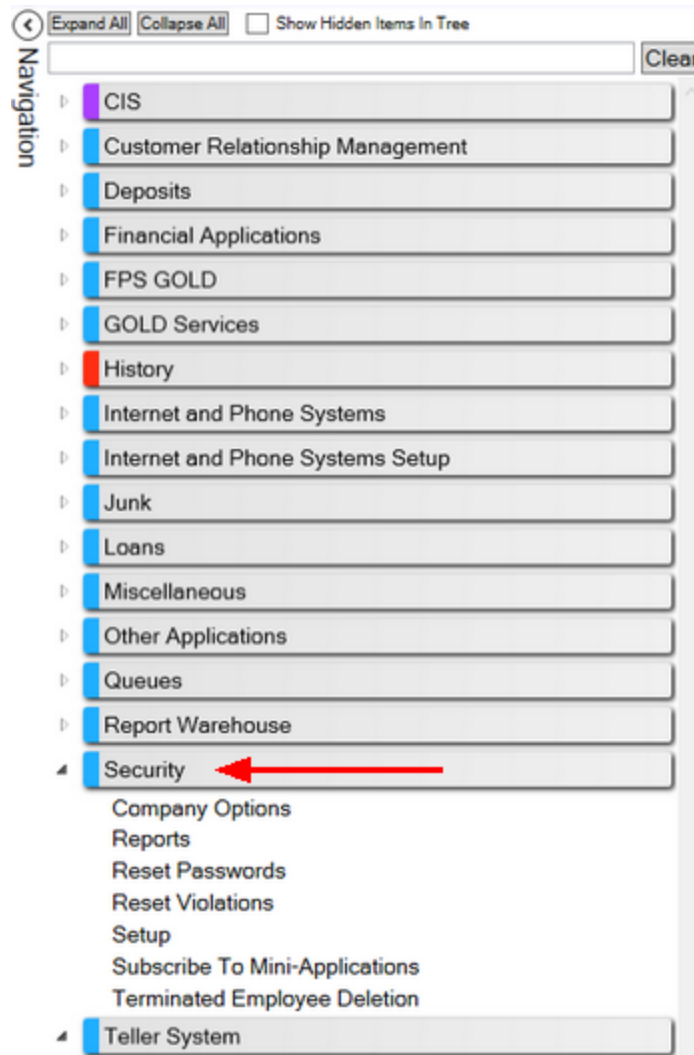


Profiles .....	26
Exclude Inactive/Terminated Employees .....	26
Sort By .....	27
Reset Passwords Screen .....	28
Rules for Valid Passwords .....	30
Search .....	31
Selection List .....	31
Reset Violations Screen .....	32
Number .....	33
Name .....	33
User Name .....	33
Enhanced User Name .....	34
Location .....	34
Security Setup Screen .....	35
Employee tab .....	36
CIM GOLD Profile tab .....	40
System Profile tab .....	42
CIM GOLD tab .....	46
System tab .....	48
System Security Details .....	49
Field Level tab .....	69
Subscribe to Mini-Applications Screen .....	71
Screens List View .....	72
Description .....	72
Cost per Month per User .....	72
Terminated Employee Deletion Screen .....	73
Display .....	73
Search .....	73
Selection List .....	73



## Security System

Before you can use CIM GOLD, security must be set up for each employee who will use CIM GOLD. Security for CIM GOLD is set up in the CIM GOLD application under Security in the left tree view, as shown below.



See any of the following topics for more information concerning the screens under Security:

- [Company security options](#)
- [Reports](#)
- [Reset Passwords](#)
- [Reset Violations](#)
- [Setup](#)
- [Subscribe to Mini-Applications](#)
- [Terminated Employee Deletion](#)



The following list shows the order in which security must be set up within CIM GOLD so that security will work properly for your institution and employees.

**NOTE**

FPS GOLD must add security for your institution's Security Administrator before employee security setups can begin.

1. [Subscribe to Mini-Applications](#) - Before security setup, your institution must subscribe to all applications and screens your institution will use.
2. [Company Options](#) - The fields on this screen define your institution name, length of employee numbers and passwords, days to force security code (password) changes, and minutes of inactivity to timeout CIM GOLD and other FPS GOLD products. Company Options are found on the CIM GOLD Security > Company Options screen.
3. [Setup](#) - Contains setup fields for employee, profile, teller security, CIM GOLD screens, and field-level security. If your institution chooses to use profiles, they must be set up before setting up individual employees.

Also see the [FPS GOLD Employee Profiles section in the Security Management](#) user guide for security information specifically for FPS GOLD employees.



## Company Options Screen

Security > Company Options

### Overview of Security

Before using CIM GOLD and other FPS GOLD product applications, security must be set up for your institution and its employees. The CIM GOLD Security screens are used to set up the following:

- Company security options
- Security for employees and tellers
- Security for CIM GOLD screens
- Security for system screens such as GOLDTeller and GOLDView
- CIM GOLD Field Level Security

The following list specifies the order in which security must be set up within CIM GOLD so that security will work properly for your institution and employees.

1. **Subscribe to Mini-Applications** - Your institution must subscribe to all applications and screens your institution will have access to before you can set up security.
2. **Company Options** - The options on this screen let you define your institution name, length of employee numbers and passwords, days to force security code (password) changes, and minutes of inactivity to time out CIM GOLD and other FPS GOLD products. Company Options are found on the CIM GOLD Security > Company Options screen.
3. **Setup** - Contains setup fields for employee, profile, teller security, CIM GOLD screens, system screens, and Field Level Security. If your institution chooses to use profiles, they must be set up before setting up individual employees.

Some of the features available in the CIM GOLD Security system are listed below.

- You can create profile groups to set up employees with similar security clearance. For example, all tellers could be set up with the same security access.
- You can set up multiple profiles per employee.
- You can specify a length of time after which password changes are forced.
- Users can select their own security codes (passwords).
- You can grant users one of three levels of security: File Maintenance, Inquiry, and None (no access).
- You can set the length of time an FPS GOLD program can remain inactive before automatically locking the program and requiring a password to be entered.
- You can grant specified FPS GOLD customer service employees defined levels of security access.
- You can delete security for terminated employees.
- You can delete unused profiles.
- Reports for changes made to the Security System are FPSDR218, Security Change Report, and Online Report.

### Setting Up Company Options

**To set up your company's security options:**

1. Enter your institution name in the **Institution Name** field.



2. In the **Employee Number Length** field, enter a number between 4 to 10. (For example, if you enter 8 here, all employee numbers must be eight digits long.)
3. In the **Days to Force Employee Password Change** field, enter a number between 15 and 99 (or 9999, never expires) to define the default number of days between forced password changes for your institution. The recommendation is to force a password change at least every 90 days. This company default can be overridden during individual employee setup.

Password changes are forced after the specified length of time. This feature protects your institution from fraudulent use of a security code for any extended period. Should a security code be violated, the user could immediately create a new security code. If the violation goes undetected, the violated code is only usable until the Days to Force Employee Password Change days are reached.

4. In the **Minutes Without Activity to Close Terminal** field, enter the number of minutes for your institution's default that will trigger a timeout for users. A minimum of 5 and maximum of 60 minutes must be entered; the system will not accept a number outside that range. This company default can be overridden during individual employee setup.

The first time a user attempts to enter anything on an FPS GOLD screen after the timeout value has expired, a timeout window will be displayed, and the user must enter their user name and password in order to continue.

This feature, also called an "inactivity logoff," increases security by locking FPS GOLD programs that are not in "active" use.

5. In the **Minimum Length of Password** (security code) field, enter the minimum password (security code) length for your institution's default, a minimum of 5 and maximum of 40. If a number outside this range is entered, the following error message will appear: "PASSWORD value must be from 5 to 8." If employees attempt to set passwords (security codes) with fewer characters than the minimum you specify in this field, they will receive the following error: "PASSWORD IS NOT LONG ENOUGH OR INVALID SPACES IN PASSWORD."
6. If left blank, the **Customer Service Security** field will allow all FPS GOLD support employees access to your institution files. A check mark will turn on the customer service security option, and you are given the option to select the security access granted for FPS customer service employees. You must select the FPS GOLD support employees from the Customer Service list; only those selected will be able to access and support your institution.
7. If you check the **Force Alpha-Numeric Passwords** field, all employees must use both letters and numbers in their passwords (security codes). If the field is left blank, employees can enter any variation of letters and/or numbers they want without restrictions.
8. When the **Force Special Characters in Passwords** field is checked, all employees will be required to have at least one special character in their passwords (security code). If the field is left blank, special characters will not be required in passwords.

For user names and passwords, all printable characters and embedded spaces are now allowed. (See the table below.)user names are not case sensitive. Passwords are case sensitive. Leading and trailing spaces will be ignored.





Characters Allowed in Passwords and User Names	
<b>Alphanumeric characters</b>	abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ 1234567890
<b>Special characters</b>	- = , . / \ ! @ # \$ % ^ & * ( ) _ + < > ? : " ' { }   [ ] ; ' ,

9. **User Defined Fields** are designated fields tied to each employee's security setup that can be used for any purpose within an institution. For example, an institution could set up a field to show the title of the employee, date of hire, birth date, etc.
10. For each **User Defined Field** implemented, enter the **Data Type** (Numeric or Alpha-Numeric), field Length, and **Field Description**. Each user-defined field set up at an institution will show on the Employee setup tab.

**WARNING**

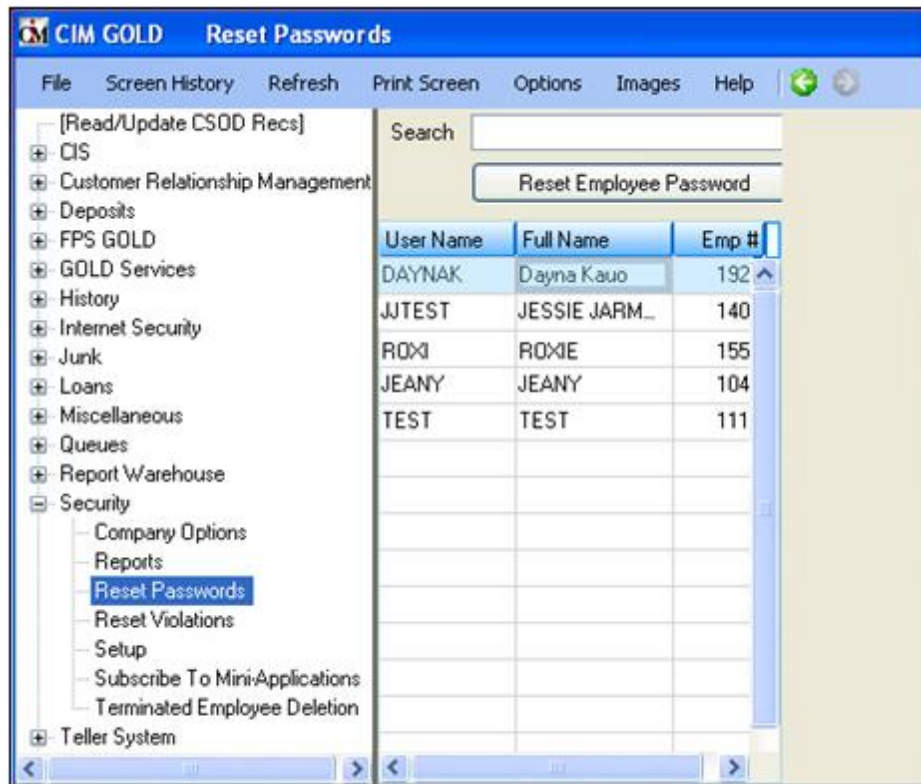
Once the User Defined Fields are set up, they cannot be removed or changed.

The reset password function is located in CIM GOLD Security > Reset Password. When an employee cannot remember their password, the security administrator can reset the password to the employee's user name. The employee would then log in using their user name as a password. The employee will then be prompted to provide a new password. If a user has violated a terminal by entering the password incorrectly three times and can't remember the password, first reset the violated terminal, and then reset the employee password. FPS GOLD recommends that only a limited number of employees be given the ability to reset passwords.

To reset a password, click on the employee's name in the list and click <Reset Password>, then click <Yes> on the Verify Action dialog box.

Only one employee can be reset at a time. Once the password has been reset, an employee has 12 hours to sign on using their user name as the password. At then next logon, the employee will be required to set a new password.





Reset Passwords Screen

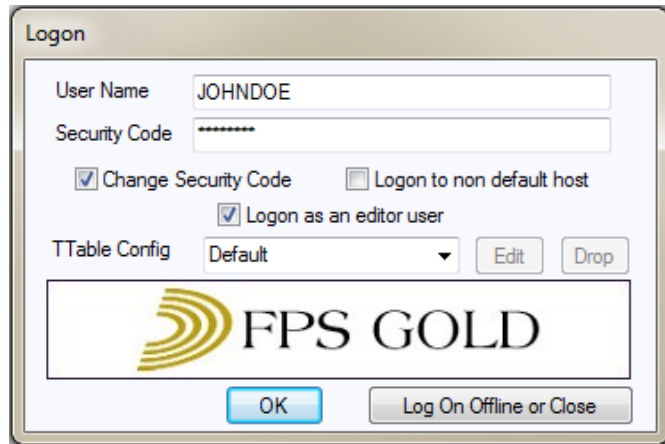
## Setting Passwords

For new employees, the password (security code) for their first sign-on will be the same as their assigned user name, and they will be forced to change them. The password they choose will be ruled based on the setup password fields in the Company Options menu. The password will automatically expire after the designated time selected to force an employee password change at your institution.

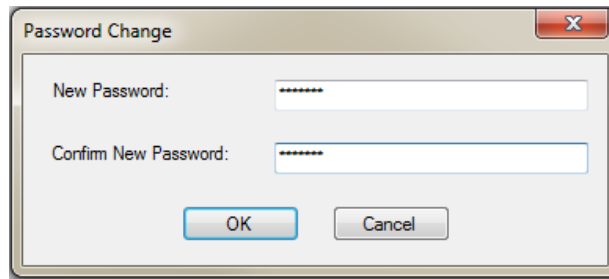
On the day the password is forced to change, the employee will log on to the system as usual and enter their current password. The program will then generate a Password Change dialog box that will prompt the employee to enter a new password (twice). A passwords can only be changed after the correct current code has been entered.

The system keeps track of the last five passwords for each user name. You cannot reuse a previously used password until at least five new passwords have been used. On the sixth password change, you are able to reuse the first password that was used.

If, at any time, you want to change your password, log on as you normally would. Enter your **User Name**, current **Security Code** (password), mark the **Change Security Code** (password) box, and click <OK>. The recommendation is for an employee to change their security code if they suspect that their password has been compromised.



The system will display a Password Change dialog box asking you for the new password (security code).



When changing a password, the system requires the user to enter the new code twice. This is to verify that the user entered the new password correctly.

See Also:

[Rules for Valid Passwords](#)

## Rules for Valid Passwords

For user names and passwords, all printable characters and embedded spaces are allowed. (See the table below.)user names are not case sensitive. Passwords are case sensitive. Leading and trailing spaces will be ignored.

Characters Allowed in Passwords and User Names	
<b>Alphanumeric characters</b>	abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ 1234567890
<b>Special characters</b>	- = , . / \ ! @ # \$ % ^ & * ( ) _ + < > ? : " { }   [ ] ; ' `

## Types of Passwords Not Allowed

The following table lists the kinds of passwords that are *not* valid. Based on the settings on the Company Options screen, users will have to follow these rules when creating passwords.



Password Length	A Password Is <i>Not</i> Valid If . . .
Any length	<ul style="list-style-type: none"> <li>The new password is the same as the current password or any of the last 4 previous passwords (regardless of case).</li> <li>The <b>Force Special Characters in Passwords</b> field is checked and the new password doesn't contain a special character.</li> <li>The <b>Force Alpha-Numeric Passwords</b> field is checked and the new password doesn't contain at least one number and one letter.</li> <li>The new password is shorter than the value in the <b>Minimum Length of Password</b> field.</li> <li>The new password is empty.</li> <li>The new password has ascending or descending sequences (sequences are found by splitting the password with a blank space). For example, "12 cba" is not valid, but "12 abc" is.</li> </ul>
More than 8 characters	<ul style="list-style-type: none"> <li>The new password contains the user name (regardless of case).</li> <li>The new password has a sequence of 5 or more consecutive ascending or descending characters. For example, "LONGabcdePASSWORD" and "LONG54321PASSWORD" are not valid, but "LONGabcdPASSWORD" is valid.</li> <li>The new password has 4 or more consecutive identical characters. For example, "long 1111 password" is not valid.</li> </ul>
8 characters or less	<ul style="list-style-type: none"> <li>The password is fewer than 5 characters.</li> <li>There are 3 or more characters that are the same as the last non-blank character. For example, "11121" is not valid.</li> <li>There are 4 or more characters that are the same as the first non-blank character. For example "1211118" is not valid.</li> <li>Characters 1–4 are the same as 5–8, or 2–4 are the same as 5–7, or 3–5 are the same as 6–8, or 1–3 are the same as 4–6. For example "abcdabcd" is not valid.</li> <li>There are more than 3 blank characters in the password.</li> <li>See "Characters Allowed in Passwords" above.</li> </ul>

## Institution Name

Enter your Institution name in this field.

## Employee Number Length

Enter the number of digits allowed in an employee number. The length can range from four to 10 digits and cannot be changed once it is set.

## Days to Force Employee Password Change

Enter a number between 15 and 9999 that defines the number of days between forced password changes for employees at your institution. 9999 means the password will never expire.

Password changes are forced after the specified length of time. This feature protects your institution from fraudulent use of a security code for any extended period. Should a security code be violated, the user could



immediately assign themselves a new security code. If the violation goes undetected, the violated code is only usable until the Days to Force Employee Password Change days are reached.

If you change the value in this field, the change is applied to all new employees added after the change. To change the password expiration deadline for your current employees, use the **Password Expiration** field on the Security > Setup screen, Employee tab for each employee.

## Minutes Without Activity to Close Terminal

Enter the default number of minutes for your institution that will trigger a timeout for users. A minimum of 5 and maximum of 60 minutes must be entered; the system will not accept a number outside that range. The default is 20 minutes.

The first time a user attempts to enter anything on an FPS GOLD screen after the timeout value has expired, a timeout window will be displayed, and the user must enter their user name and password in order to continue.

This feature, also called an "inactivity logoff," increases security by locking FPS GOLD programs that are not in "active" use. Should a user need more or less time before timeout occurs, the security officer can override the default and enter any length of time up to 546 minutes on the Employee Definition screen.

## Minimum Length of Password (5-40)

Enter the minimum password (security code) length for your institution's default, a minimum of 5 and maximum of 40. If employees attempt to set passwords (security codes) with fewer characters than the minimum you specify in this field, they will receive the following error: "PASSWORD IS NOT LONG ENOUGH OR INVALID SPACES IN PASSWORD."

### User-Selected Security Code

On the day security codes are forced to change, employees will log on to the system as normal and enter their old security codes. The computer will then ask them to enter a new security code (twice). Security codes can be changed only after the correct current security code has been entered.

The system keeps track of the last six security codes for each user name. You cannot reuse a previously used security code until at least six new security codes have been used. On the seventh time, you are allowed to reuse the old security code.

If at any time you want to change your security number, log on as you normally would. Enter all of the information you normally would as you sign on, except click the **Change Security Code** box. The system will display a dialog box asking you for the new security code.

When changing a security code, the system requires the user to enter the code twice. The reason for this is to verify that the user did in fact enter the number he or she wanted. One typo could cause a lot of confusion.

### See Also:

[Rules for Valid Passwords](#)



## Customer Service Security

If this field is left blank, all FPS GOLD support employees can access your institution files. A check mark will turn on the Customer Service Security option, and you will need to select the security access you want to grant for specific FPS customer service employees on the Customer Service tab. Only those selected will be able to access your files.

**FPS GOLD Only:** NCC Security employees can add an FPS GOLD employee to the list with proper authorization.

## Force Alpha-Numeric Passwords

If you check this box, all employees must use both letters and numbers in their passwords (security codes). If the field is left blank, employees can enter any combination of letters and numbers without restrictions.

### User-Selected Security Code

On the day security codes are forced to change, employees will log on to the system as normal and enter their old security codes. The computer will then ask them to enter a new security code (twice). Security codes can be changed only after the correct current security code has been entered.

The system keeps track of the last six security codes for each user name. You cannot reuse a previously used security code until at least six new security codes have been used. On the seventh time, you are allowed to reuse the old security code.

If at any time you want to change your security number, log on as you normally would. Enter all of the information you normally would as you sign on, except click the **Change Security Code** box. The system will display a dialog box asking you for the new security code.

When changing a security code, the system requires the user to enter the code twice. The reason for this is to verify that the user did in fact enter the number wanted. One typo could cause a lot of confusion.

**See Also:**

[Rules for Valid Passwords](#)

## Force Special Characters in Passwords

When this field is checked, all employees will be required to have at least one special character in their passwords (security code). If the field is left blank, special characters will not be required in passwords.

### User-Selected Security Code

On the day security codes are forced to change, employees will log on to the system as normal and enter their old security codes. The computer will then ask them to enter a new security code (twice). Security codes can be changed only after the correct current security code has been entered.



The system keeps track of the last six security codes for each user name. You cannot reuse a previously used security code until at least six new security codes have been used. On the seventh time, you are able to reuse the old security code.

If at any time you want to change your security number, log on as you normally would. Enter all of the information you normally would as you sign on, except click the **Change Security Code** box. The system will display a dialog box asking you for the new security code.

When changing a security code, the system requires the user to enter the code twice. The reason for this is to verify that the user did in fact enter the number he or she wanted. One typo could cause a lot of confusion.

**See Also:**

[Rules for Valid Passwords](#)

## User Defined Fields field group

User Defined Fields are designated fields tied to each employee's security setup that can be used for any purpose within an institution. For example, an institution could set up a field to show the title of the employee, date of hire, birth dates, etc.

For each User Defined Field implemented, enter the **Data Type** (Numeric or Alpha-Numeric), field **Length**, and **Field Description**. Each User Defined field set up at an institution will show on the Employee setup tab.

### WARNING

Once the User Defined Fields are set up, they cannot be removed or changed.

See the following topics:

[User Defined Field Type 1 - 5](#)

[User Defined Field Length 1 - 5](#)

[User Defined Field Description 1 - 5](#)

## User Defined Field Type 1 - 5

User-defined fields are designated fields tied to each employee's security setup that can be used for any purpose within an institution. For example, an institution could set up a field to show the title of the employee, date of hire, birth dates, etc.

For each User-defined field implemented, enter the **Data Type** (Numeric or Alpha-Numeric), field **Length**, and **Field Description**. Each User Defined field set up at an institution will show on the Employee setup tab.



**WARNING**

Once the User Defined Fields are set up, they cannot be removed or changed.

**User Defined Field Length 1 - 5**

User-defined fields are designated fields tied to each employee's security setup that can be used for any purpose within an institution. For example, an institution could set up a field to show the title of the employee, date of hire, birth dates, etc.

For each User-defined field implemented, enter the **Data Type** (Numeric or Alpha-Numeric), field **Length**, and **Field Description**. Each User Defined field set up at an institution will show on the Employee setup tab.

**WARNING**

Once the User Defined Fields are set up, they cannot be removed or changed.

**User Defined Field Description 1 - 5**

User-defined fields are designated fields tied to each employee's security setup that can be used for any purpose within an institution. For example, an institution could set up a field to show the title of the employee, date of hire, birth dates, etc.

For each User-defined field implemented, enter the **Data Type** (Numeric or Alpha-Numeric), field **Length**, and **Field Description**. Each User Defined field set up at an institution will show on the Employee setup tab.

**WARNING**

Once the User Defined Fields are set up, they cannot be removed or changed.





## Security Reports Screen

Use security reports to view and print reports for security setup and changes made for CIM GOLD screen access (including GOLDView, GOLDTeller, etc.), employee and teller information, and field-level security.

### NOTES

- Both afterhours reports [FPSDR218](#) and the [System Security Change Report](#) must be used to audit changes to security. FPSDR218 shows all changes to CIM GOLD Profiles and Employee Security changes to CIM GOLD screens. System Security shows all changes to Company Options, System Profiles, and Employee Security changes to System screens.
- If any security changes show file maintenance to inactive screens when you have made other security changes, the inactive screens are no longer used, and the security is automatically turned off by default by FPS GOLD during your changes.

## Tabs

Selection criteria are specific for each tab, based on the function of the screen. The tabs are briefly explained below.

- The [History tab](#) is used to report and print changes made to CIM GOLD Security using CIM GOLD. You can limit searches to profiles, to employee and teller details, or to other criteria.
- The [Access tab](#) allows you to select any employees, profiles, or tellers and display or print the access that has been granted in CIM GOLD Security. You can also refine your search to include only some or all of the access for employee details, CIM GOLD, System, teller details, and field-level security. If multiple profiles are assigned, the "effective" security will be determined.
- The [Securables tab](#) allows you to select any applications, Systems, or screens and display or print the employees and profiles that have been granted security for them in CIM GOLD Security. The report can also display employees and CIM GOLD profiles that are restricted by field-level security. If multiple profiles are assigned, the "effective" security will be determined.
- The [Employee/Profile Listing tab](#) allows you to include employees and profiles and to generate and print a detail report of employee/profile setup information (Employee Numbers, Employee or Profile Type, Status, User Name, Timeout, and Password Expiration). The report will also show which employees are sharing CIM GOLD or System profiles. You can sort the information by Full Name, System Profile, Employee/Profile Number, Password Expiration, Status, Timeout, Employee/Profile Type, and User/Profile Name.

## History tab

The History tab is used to report and print changes made to CIM GOLD Security using CIM GOLD. You can limit searches to profiles, to employee and teller details, or to other criteria. The search results will be shown on the screen. You can view the report by clicking the <Print Preview > button; click <Print> to print the report.



### To search for changes made to CIM GOLD security:

1. Click on one or more checkboxes in the Changes to Display field group.

**NOTE**

Searching with multiple criteria will take a little more time.

2. To view changes for a specific date range, enter or select the [Start Date](#) and [End Date](#).
3. Enter the [Start Time](#) and [End Time](#) to view changes for a specific time frame.
4. Enter an employee number in the [Changed by Employee#](#) field to view specific changes made by a user.
5. Click <Search> to perform the selected search.

### Buttons

**<Clear>** Click this button to clear the screen and start over with a new search. The search results and all sections will be removed from the screen, and the date and time will be changed back to the pre-selected date and times for today.

**<Search>** Click this button after you have made all the selections necessary for your search.

**<Print Preview>** Click this button after the search has been performed to see a preview of the report that can be printed. The details for both the Key and Data fields will be shown on the report. Right click in the print preview to open a pop-up menu with Find, Increase Zoom, and Decrease Zoom. You can also use <Ctrl>+<F> to find data within the print preview.

**<Print>** Click this button after the search has been performed to print the results of your search on a report. The details for both the Key and Data fields will be shown on the report. To view before printing, click <Print Preview>.

**NOTES**

- Both afterhours reports [FPSDR218](#) and the [System Security Change Report](#) must be used to audit changes to security. FPSDR218 shows all changes to CIM GOLD Profiles and Employee Security changes to CIM GOLD screens. System Security shows all changes to Company Options, System Profiles, and Employee Security changes to System screens.
- If any security changes show file maintenance to inactive screens when you have made other security changes, the inactive screens are no longer used, and the security is automatically turned off by default by FPS GOLD during your changes.



## Changes to Display field group

Use these fields to define a search for changes made to security access.

## CIM GOLD Employee Security

Check this box if you want to find history items that show changes made to CIM GOLD Employee security.

## CIM GOLD Profile Security

Check this box if you want to find history items that show changes made to CIM GOLD Profile security.

## Customer Service Cross Reference

Check this box to require FPS GOLD employees to be added to your institution's security. Once this is set, you must indicate which profile you want your FPS GOLD support staff to be tied to. All FPS GOLD employees who are required to help you with your files must be set up in the list on the Customer Service tab.

Check the box and save changes. The Customer Service tab will be added to your screen.

## EFT GOLD Options

Check this field to view changes made to EFT GOLD settings. This will show the EFT GOLD security operator limits and EFT GOLD options. All past history is available according to your history limits.

## Employee Details

Check this box if you want to display employee details.

## Employee Password Reset

Check this box if you want to find Employee Password Reset history items.

## Employee Field Level Security

Check this box if you want to find history items that show changes made to Employee Field Level security.



## System Security

Check this box if you want to find history items that show changes made to System security. System security consists of all other FPS PC products, including GOLDTeller, GOLDView, etc.

## Options

Changes made to employee and Profile options will be shown when you check this box.

## Profile Field Level Security

Check this box if you want to find history items that show changes made to Profile Field Level security.

## Teller Details

Check this box if you want to display teller details.

## Terminal Violation Reset

Check this box if you want to find Terminal Violation Reset history items.

## Selection Criteria field group

Use these fields to limit your search to certain dates and times, or to the employee who made changes.

## Start Date

Enter the start date to search for a file maintenance change, addition, or drop in the selected record.

## End Date

Enter the end date to search for a file maintenance change, addition, or drop in the selected record.

## Start Time

Enter the start time to search for a file maintenance change, addition, or drop in the selected record.



## End Time

Enter the end time to search for a file maintenance change, addition, or drop in the selected record.

## Changed by Employee#

If you know it, enter the employee number of the employee who made the change, addition, or drop you want to find in the selected record.

## History List View

This list view displays the results of the search criteria you entered above. The following explains the information under each column.

- **Change Category:** This column displays the type of record that was changed, added, or dropped. The results for the search are based on the selections made in the Changes to Display field group.
- **Date and Time:** This column displays the date and time a change, addition, or drop occurred on the selected record.
- **Action:** This column shows that the record was updated, added, or dropped. For records where data is changed, you will see "Add" for new records, "Update" for changes, and "Drop" for deleted records.
- **Changed By:** This column displays the name and number of the employee that made the add, change, or drop to the record.
- **Key Fields:** This column shows how many items are in the change. If you click on the arrow, you can view which record the changes were made to. When you print the report, these items will automatically print.
- **Data Fields:** This column shows how many items are in the change. If you click on the arrow, you can view the changes that were made. The old and new data are reported on the list. When you print the report, these items will automatically print.

## Access tab

Use the Access tab to select employees, profiles, or tellers and view or print the access that has been granted to them in CIM GOLD Security. You can also limit your search to only include some or all of the access for employee details, CIM GOLD, System, teller details, and field-level security. If multiple profiles are assigned, the "effective" security will be determined.

### Finding a Name

#### To quickly find a name in the list view:

1. Click on the appropriate radio button (Employees, Tellers, CIM GOLD Profiles, or System Profiles) to find a specific user name, teller name, or profile name.
2. Enter part of the name in the **Search** field.

When you click on a different radio button at the top left, the search criteria are removed.

#### To view security for employees, tellers, or profiles:

1. Select the appropriate radio button.
2. Select any combination of the Include fields to include that information in the report.



3. Select one name from the list view.

*or*

Select multiple names by holding holding the <Ctrl> key down and clicking on the names.

4. Click **<Run Report>**.

The results will display on the right side of the screen. Right click in the print preview to open a pop-up menu with Find, Increase Zoom, and Decrease Zoom. You can also use <Ctrl>+<F> keys to find data within the print preview. You can print the results by clicking the **<Print>** button.

## Employees

Select this option to display employees in the list view below.

## Tellers

Select this option to show tellers in the list view below.

## CIM GOLD Profiles

Select this option to show CIM GOLD Profiles in the list view below.

## System Profiles

Select this option to show System Profiles in the list view below. System security consists of all other FPS GOLD PC products, including GOLDTeller, GOLDView, etc.

## Search

Enter a portion of the employee's user name or the profile name for a quick search. Use this feature to find a specific user name, teller name or profile name based on the radio button selection.

## Include field group

Use these fields to specify the information you want in your report. You can select any combination of the choices to create one report with all data.

## Details

Check or uncheck this box to show or hide the employee information details such as name, profiles status, and user-defined fields. The setup for this type of security is handled on the Setup screen, Employee tab. To select more than one employee from the list, click on the names while holding the <Ctrl> key down.



## Teller Information

Check or uncheck this box to show or hide the details for your tellers. The setup for this type of security is handled on the Setup screen on the Teller tab. Only employees who will be processing monetary transactions to accounts need to be set up as tellers. Information such as name, employee number, transaction limits, and override authority will display. To select more than one name from the list, click on the names while holding the <Ctrl> key down.

## CIM GOLD

Check or uncheck this box to show or hide the CIM GOLD screens that employees have security to. The System also shows whether employees are tied to profiles. The setup for this type of security is handled on the Setup screen on the CIM GOLD tab and can be done by specific employee or profile. To select more than one name from the list, click on the names while holding the <Ctrl> key down.

## System

Check or uncheck this box to show or hide the System screens that employees have security rights to. The System also shows whether employees are tied to profiles. The setup for this type of security is handled on the Setup screen on the System tab and can be done by specific employee or profile. To select several employees from the list, click on the names while holding the <Ctrl> key down. System security consists of all other FPS PC products, including GOLDTeller, GOLDView, etc.

## Field Level

Check or uncheck this box to show or hide the fields that employees have security to. The setup for this type of security is handled on the Setup screen on the CIM GOLD tab and can be done by specific employee or profile. To select more than one name from the list, click on the names while holding the <Ctrl> key down.

## Profile Assignments

Check this box to run a report for profile security and add the employees' names and numbers to the report to show who is tied to specific profiles.

When running a report on an employee, you will be able to report the profiles that are tied to employees.

## All Assigned Profiles

When this field is checked, the employee's individual security will print as well as the security for each profile assigned to the employee. This field works only when printing Effective Security for an employee and is used in conjunction with the [CIM GOLD](#) and [System](#) fields in the [Include field group](#).

If the **CIM GOLD** and/or the **System** field is selected, the **All Assigned Profiles** field will print the profile's security settings for either CIM GOLD and/or System, depending on what is selected. This new field saves the



user from having to run another report with the [CIM GOLD Profiles](#) or the [System Profiles](#) radio button field selected and then having to match the profiles with the employees.

The report will show the Effective security of the employee followed by the Individual Security and Profiles security, in that order.

## Report on Effective Security

Check this box if you want the report to determine what the effective security is for your selection. If this box is not checked, only individual security will be reported.

## Exclude Inactive/Terminated Employees

When this box is checked, no Inactive or Terminated employees will show on the report.

## Access List View

To select more than one employee from the list, click on the names while holding the <Ctrl> key down. When you have made your search selection, click <Run Report>. The results will show on the right side of the screen.

## Securables tab

The Securables tab allows you to select an application, System, or screen and view or print which employees or profiles have been granted security to them in CIM GOLD Security. You can also show which employees are restricted by field-level security.

If multiple profiles are assigned to an employee, the employee's "effective" security will be determined.

### To view the people or profiles assigned security to specific screens:

1. Select either **CIM GOLD**, **System**, or **Field Level Security**.
2. Select **Employees** and/or **Profiles**.

Based on the application you select, the screens in the list will change.

3. Checkmark the screens you want to include on the report.
4. To expand the list view, click on the + sign.
5. To select all screens in the expanded list, click on the box next to the main tree item.
6. When you have made your search selection, click <Run Report>.

The results will display on the right side of the screen. The report shows the employees and/or profiles that have security to the selected screens. The report also shows whether they have INQ (inquiry) or F/M (file maintenance) rights to the screen.

Right-click in the print preview to use the Find, Increase Zoom, and Decrease Zoom features. You can also use <Ctrl>+<F> keys to find data within the print preview. You can print the results by clicking <Print>.





## CIM GOLD

Check this box to show the CIM GOLD screens that employees have security to. It also shows whether employees are tied to profiles. The setup for this type of security is handled on the setup screen on the CIM GOLD tab and can be done by specific employee or profile. To select more than one employee from the list, click on the names while holding the <Ctrl> key down.

## System

Select this option to show the System screens that employees have security to. It also shows whether employees are tied to profiles. The setup for this type of security is handled on the setup screen on the System tab and can be done by specific employee or profile. To select certain employees from the list, click on the names while holding the <Ctrl> key down.

## Field Level

Select this option to show the fields that employees have security to. The setup for this type of security is handled on the Setup screen on the Field Level tab and can be done by specific employee or profile. To select more than one employee from the list, click on the names while holding the <Ctrl> key down.

## Include field group

Use these fields to display employees, profiles, or both on the report.

## Employees

Check this box to display employees who have access to certain screens and also to display those who are restricted by field-level security. You can select both **Employees** and [Profiles](#).

## Profiles

Check this box to display profiles that have access to certain screens and also to display profiles restricted by field-level security. You can select both [Employees](#) and **Profiles**. If you check this box, both the profile and profile assignments will display.

## Effective Security

Check this box to report the Effective Security for the selected criteria. When checked, effective security will be reported. When not checked, only individual security will be reported.



## Profile Assignments

This box is automatically checked when you click on [Profiles](#). Your report will show profiles and which employees are assigned to each profile.

## Exclude Inactive/Terminated Employees

When this box is checked, no Inactive or Terminated employees will be shown on the report.

## Securables List View

To select more than one employee from the list, click on the names while holding the <Ctrl> key down. When you have made your search selection, click <Run Report>. The results will display on the right side of the screen.

## Employee/Profile Listing tab

Use the fields on this tab to include employees and/or profiles and view or print a detail report of employee and profile setup information (Employee Numbers, Employee or Profile Type, Status, User Name, Timeout, and Password Expiration). The report will also show which employees are sharing CIM GOLD profiles. You can sort the information by Full Name, System Profile, Employee/Profile Number, Password Expiration, Name, Status, Timeout, Employee/Profile Type, and User/Profile Name.

## Include field group

Select one or more of the fields in this group to include them on the report.

## Employees

Check this box to display employees who have access to certain screens and also to display those who are restricted by field-level security. You can select both **Employees** and [Profiles](#).

## Profiles

Check this box to display employees who have access to certain screens and also to display those who are restricted by field-level security. You can select both [Employees](#) and **Profiles**.

## Exclude Inactive/Terminated Employees

When this box is checked, no Inactive or Terminated employees will show on the report.



## Sort By

Select from the drop-down list to sort the report by that field. The options are defined below.

All sorts will be ordered first by the selection and then by full name. Regardless of sort order, the report will show the number, type, name, full name, status, CIM GOLD profile, System profile, timeout, and password expiration for each employee listed.

### Sort Options

- **CIM GOLD Profile:** All the employees in the list will be ordered by CIM GOLD Profile and then by full name.
- **Full Name:** All the employees in the list will be ordered by the employee full name and/or System Profile Description.
- **System Profile:** All the employees in the list will be ordered by the shared System Profile Name. Blanks (which mean not sharing a System Profile Name) sort to the top, followed by those employees sharing a System Profile Name.
- **Number:** All the employees in the list will be ordered by Employee/System Profile Name.
- **Password Expiration:** All the employees in the list will be ordered by Password Expiration days, from least to greatest.
- **Status:** All the employees in the list will be ordered alphabetically by Status first and then by Full Name and/or Profile Description.
- **Timeout:** All the employees in the list will be ordered by Timeout values, from least to greatest.
- **Type:** All the items in the list will be ordered by employee or profile type, with employees first.
- **User/Profile Name:** All the employees in the list will be ordered by the employees' user names and then by full name.



## Reset Passwords Screen

### Security > Reset Passwords

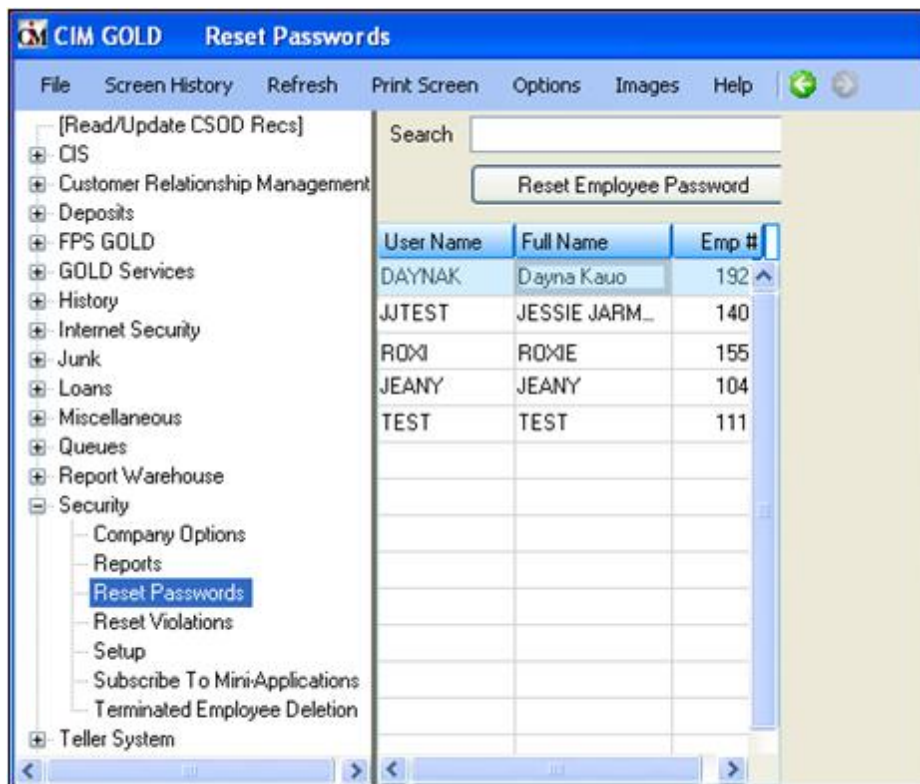
The Reset Passwords screen is located in CIM GOLD Security > Reset Passwords.

FPS GOLD *cannot* reset passwords for your employees. A security administrator at your institution must handle this function. Only one employee can be reset at a time.

If a user has violated their security by entering the password incorrectly three times and can't remember the password, first reset the restricted employee, and then reset the employee password. FPS GOLD recommends that only a limited number of employees be given the ability to reset passwords.

### To change an employee's password:

1. Click on the employee's name in the list.
2. Click <Reset Password>, then click <Yes> on the Verify Action dialog.
3. Enter the employee's Enhanced User name as the new password.
4. The employee can then log in within 12 hours using their user name, in all lower case, as a password.
5. The employee will then be prompted to provide a new password.



Reset Passwords Screen

**FPS GOLD Only:** Editor users do not have security to this function.

## Setting Passwords



For a new employee, the password (security code) for the first sign-on will be the same as the assigned Enhanced User name in lower case, and the employee will be forced to change it. The Security > Company Options screen controls rules for setting up new passwords (see the [Rules for Valid Passwords](#)). The password will automatically expire after the designated time selected to force an employee password change.

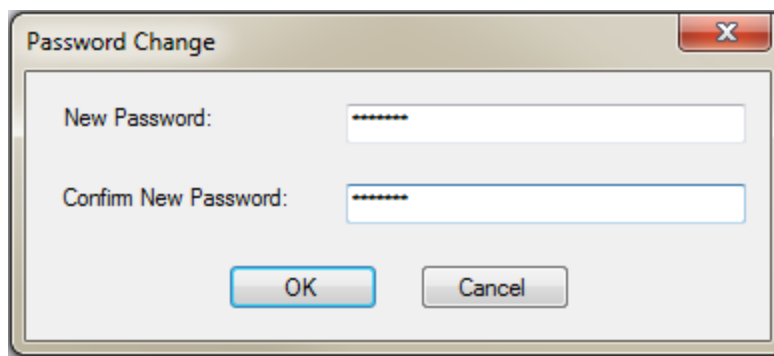
On the day the password is forced to change, the employee will log on to the system as usual and enter their current password. The program will then generate a Password Change dialog that will prompt the employee to enter a new password (twice). A password can be changed only after the correct current password has been entered.

### To change your own password:

1. Log on as you normally would.
2. Enter your **User Name**.
3. Enter your current **Security Code** (password).
4. Mark the **Change Security Code** (password) box.
5. Click <OK>.



The system will display a Password Change dialog box asking you for the new password (security code).



6. Enter the new code twice to verify that the password was entered correctly.

See the [rules for valid passwords](#).



See also:

[Security System](#)

## Rules for Valid Passwords

For user names and passwords, all printable characters and embedded spaces are allowed. (See the table below.) User names are not case sensitive. Passwords are case sensitive. Leading and trailing spaces will be ignored.

Characters Allowed in Passwords and User names	
<b>Alphanumeric characters</b>	abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ 1234567890
<b>Special characters</b>	- = , . / \ ! @ # \$ % ^ & * ( ) _ + < > ? : " { }   [ ] ; ' ,

### Types of Passwords Not Allowed

The following table lists the kinds of passwords that are *not* valid. Based on the settings on the Company Options screen, users will have to follow these rules when creating passwords.

Password Length	A Password Is Not Valid If . . .
<b>Any length</b>	<ul style="list-style-type: none"> <li>The new password is the same as the current password or any of the last 4 previous passwords (regardless of case).</li> <li>The institution setting <b>Force Special Characters in Passwords</b> is checked and the new password doesn't contain a special character.</li> <li>The institution setting <b>Force Alpha-Numeric Passwords</b> is checked and the new password doesn't contain at least one number and one letter.</li> <li>The new password is shorter than the value in the institution setting <b>Minimum Length of Password</b>.</li> <li>The new password is empty.</li> <li>The new password has ascending or descending sequences (sequences are found by splitting the password with a blank space). For example, "123 cba" is not valid, but "123abc" is.</li> </ul>
<b>More than 8 characters</b>	<ul style="list-style-type: none"> <li>The new password contains the user name (regardless of case).</li> <li>The new password has a sequence of 5 or more consecutive ascending or descending characters. For example, "LONGabcdePASSWORD" and "LONG54321PASSWORD" are not valid, but "LONGabcdPASSWORD" is valid.</li> <li>The new password has 4 or more consecutive identical characters. For example, "long 1111 password" is not valid.</li> </ul>
<b>8 characters or less</b>	<ul style="list-style-type: none"> <li>The password is fewer than 5 characters.</li> <li>There are 3 or more characters that are the same as the last non-blank character. For example, "11121" is not valid.</li> <li>There are 4 or more characters that are the same as the first non-blank character. For example "1211118" is not valid</li> <li>Characters 1–4 are the same as 5–8, or 2–4 are the same as 5–7, or 3–5 are the same as 6–8, or 1–3 are the same as 4–6. For example "abcdabcd" is not valid.</li> <li>There are more than 3 blank characters in the password.</li> <li>See "Characters Allowed in Passwords" above.</li> </ul>



## Search

To find a user name quickly in the list below, begin typing the name in this field.

## Selection List

This field displays a list of employees whose passwords you can change.

To change a password:

1. Select a name in this list.
2. Click <Reset Employee Password>.
3. Click <Yes> on the Verify Action dialog box.



## Reset Violations Screen

### Security > Reset Violations

The Reset Violations screen is located in CIM GOLD Security > Reset Violations. Use this screen to reset a password if one of the following occurs:

- the user has entered an incorrect password three consecutive times while attempting to log in;
- the user has been inactive for 90 days or more.

A user cannot sign on to any FPS GOLD product until the violation has been cleared. FPS GOLD recommends that only a limited number of employees be given security to reset violated terminals.

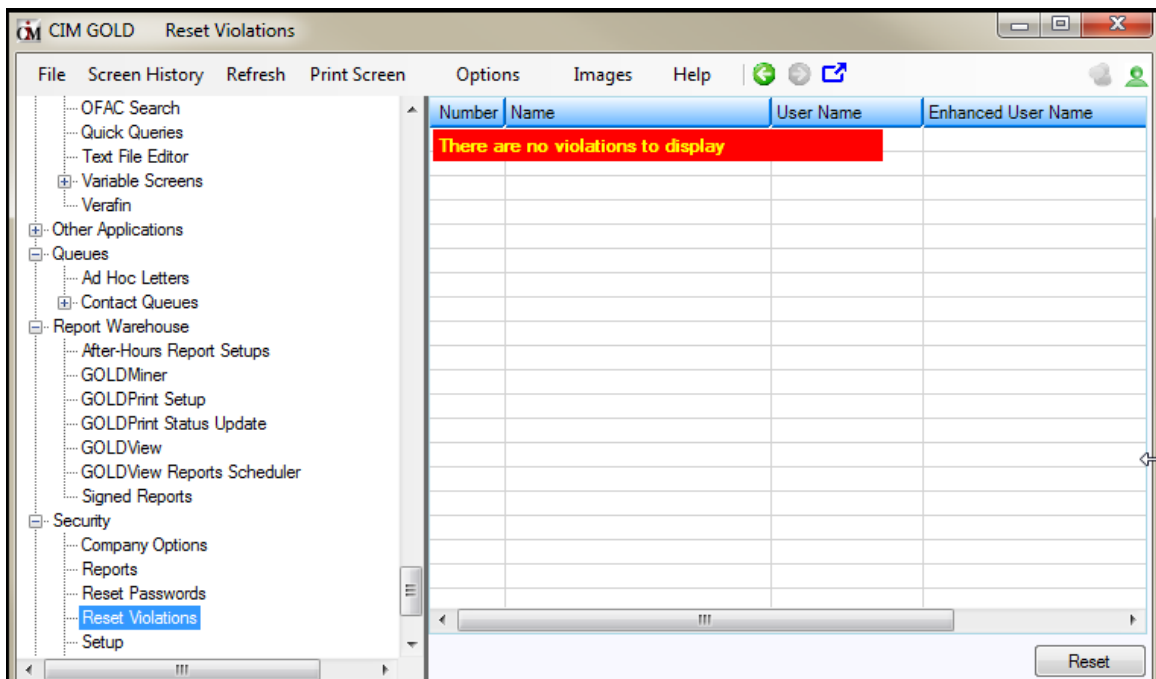
#### NOTE

FPS GOLD *cannot* reset security violations for your employees. An employee at your institution must reset them.

If there are no security violations when you open the Reset Violations screen, you will see the message “There are no violations to display” in a red box at the top of the screen. See the following example.

#### FPS GOLD ONLY

Editor users do not have security to this function.



Reset Violations Screen without a Violation

If there are security violations, they will be listed on the screen. See the following example.



Number	Name	User Name	Enhanced User Name	Location	
1810	JOHN DOE	JOHND	JOHN H. DOE	I0061234	

Reset Violations Screen with a Violation

### To clear a violation:

1. Highlight the name in the list.
2. Click the <Reset> button on the bottom of the screen.

The reset will clear the violation, and the user can attempt to log in again with their current password.

## Changing a Password

Resetting violations does not change the password to the user name. A password is only reset to the user name by resetting the password on the [Employee](#) screen in Security Setup or on the [Reset Passwords](#) screen. Use this method if a user forgets his or her password.

## Setting Timed Logoff

The Security > Company Options screen contains a field called **Minutes Without Activity to Close Terminal**. Each institution can set this field for any given employee to a number of minutes. When that amount of time has passed without any activity, the system automatically logs the employee off the terminal. That employee must then sign on to the system again following the normal procedure.

## Number

This field displays the teller number for the user who caused the violation.

For instructions on how to use this screen, see the [overview topic](#).

## Name

This field displays the name of the employee with the security violation.

## User Name

This field displays the user name of the user who caused the violation. This field is used on CIM GOLD screens and afterhours reports.

For instructions on how to use this screen, see the [overview topic](#).



## Enhanced User Name

This field displays the long user name (if your institution has entered this data) for the employee with the violation.

This name is only used in security. The [User Name](#) field is used on CIM GOLD screens and afterhours reports.

## Location

This field displays the PC VTAM location for the user with the violation.

For instructions on how to use this screen, see the [overview topic](#).



## Security Setup Screen

Before you can use CIM GOLD, each employee who will use CIM GOLD must have security to the screens or specific fields they will use.

### NOTE

FPS GOLD must add security for your institution's Security Administrator before employee security setups can begin. Some security settings can only be changed by a Security Administrator.

## Overview of CIM GOLD Security

Security for CIM GOLD is set up on several CIM GOLD screens. The following list shows the order in which security must be set up within CIM GOLD so that security will work properly for your institution and employees.

1. [Subscribe to Mini-Applications](#) - Before security setup, your institution must subscribe to all applications and screens your institution will use.
2. [Company Options](#) - The fields on this screen define your institution name, length of employee numbers and passwords, days to force security code (password) changes, and minutes of inactivity to timeout CIM GOLD and other FPS GOLD products. Company Options are found on the CIM GOLD Security > Company Options screen.
3. Institution defaults for CIM GOLD Customer Index Bubble, CIM GOLD Teller (for Menu and Speed Keys), and Document Imaging (for Firebird Signatures).
4. **Security > Setup** - Contains setup fields for [employee](#), [profile](#), [teller security](#), [CIM GOLD screens](#), and [field-level security](#). If your institution chooses to use profiles, they must be set up before setting up individual employees.

## What Is a Security Profile?

On the [CIM GOLD Profile tab](#) and [System Profile tab](#), you can set up security profiles. Profiles save time and ensure that security settings are the same for all employees with the same duties (such as all tellers or all loan officers). A profile is set up one time and then linked to all employees that require the same security access. For example, the security access for all tellers could be set up under the profile name "Teller." The "Teller" profile would then be linked to each employee who requires access to the security given under the "Teller" profile.

Profiles save time because you set up security only once for a group of employees that would require the same security clearance. Also, if a security change is needed for a group of employees that share the same profile, you can change the security one time on the profile, rather than changing each individual employee's security.

### NOTE

FPS GOLD client services representatives have inquiry-access only to institution security. We *cannot* release password violations or reset passwords for your institution at any time.



An employee at your institution must handle these types of security issues.

## Using the Security Setup Screen

Use the Security Setup screen to assign screen-level or field-level security to individual employees and tellers. You can also create security profiles for groups (such as the loan department) and then assign individual employees to those groups. All individuals assigned to the same group profile will then have the same security settings.

**Note:** This section gives overviews and how-to information on using Security Setup. For help on an individual field on the Security Setup screen, click in the field and press the <F1> key on your keyboard.

This section describes how to set up:

- [Company Security options.](#)

## Employee tab

Use the fields on the Employee tab of the Security > Setup screen to set up employee security.

### NOTE

FPS GOLD *cannot* reset passwords or security violations for your employees.

## Setting Up an Employee

To set up security for an employee, create a new employee. You can also copy security to a new employee or from one existing employee to another.

### To create a new employee:

1. On the [Security Setup screen](#), select **Employees** and click <New>.



Security Setup Screen, Employee Tab

- In the "Create a new Employee" dialog box, type a new **Employee Number**, **User Name**, **Enhanced User Name**, and **Full Name**. The fields on the dialog box are explained in the table below.

**NOTE**

After you click <OK>, you cannot change the **Employee Number** for this employee. You can only delete this employee and start over. To do this, change the employee **Status** to "Terminated" and delete the employee using the [Terminated Employee Deletion screen](#).

Field Name	Number of Characters	Purpose	Editable?
<b>Employee Number</b>	variable—established on the <a href="#">Company Options screen</a>	identify the employee within the organization	No. See the Note above.



<b>User Name</b>	maximum of eight alphanumeric characters	shown on reports and screens	Yes, if <b>Display Effective Security</b> is not checked
<b>Enhanced User Name</b>	up to 40 characters	used to log on to FPS GOLD products	Yes

3. Click <OK>.
4. On the Employee tab, enter the remaining data. The **Status** drop-down list will show the default "Active" status. Select another status if necessary.
5. An **Interface Profile** is used to determine the settings an employee should use for the following three functions: CIM GOLD Customer Index Bubble, Menus and Speed Keys in CIM GOLD Teller, and Document Imaging (for Firebird Signatures).
6. **Timeout Minutes** are defaulted from the Company Options screen. If the length of time is not appropriate for the new employee, you can enter 5 to 60 minutes.
7. **Password Expiration** is defaulted from the Company Options screen. If an employee needs more or fewer days between password (security code) changes, enter a number between 15 and 99 here. You can also enter 9999 for a password that never expires.
8. **SoftToken Key** is a two-step authentication that can be used in EFT GOLD for wires for added security. If your institution has selected **Require SoftToken Authentication** on the EFT GOLD Wire Options screen, enter the appropriate information in this field. For more information on using this feature, see the [EFT GOLD User's Guide](#) in DocsOnWeb.
9. If this employee will use a **System Profile**, select the appropriate profile(s) from the list below by checking the box in the **Member?** column.
10. If this employee will use a **CIM GOLD Profile**, select the appropriate profile(s) from the list below by checking the box in the **Member?** column.  
  
CIM GOLD and System Profiles must be set up before you can use the profile name on an employee security setup.
11. Enter the appropriate information in the **User Defined** fields that your organization may have set up on the Company Options screen.
12. Click <**Save Changes**>.

If the employee being set up is also a teller, continue to the Teller tab. If the employee is not a teller and is not using CIM GOLD or System Profiles, go to the [CIM GOLD](#) and System tabs to set the appropriate security.

**<Reset Password>** This button should only be used when employees forget their passwords. Clicking this button gives employees 12 hours to enter their user name as their password before the system will force them to create a new password. Giving employees security to the Reset Password mini-application allows them to reset passwords but does not allow them to change any security. The temporary password will be the same as the Enhanced User Name in lower case.

For example, John Doe's user name is JOHND. He would enter "JOHND" in the **User Name** field and "johnd" as the password. When he clicks <OK>, a Security Code Update window will display. To save the new code, John Doe would then enter a new password in the **Enter New Password** and **Re-enter New Password** fields and click <OK>.



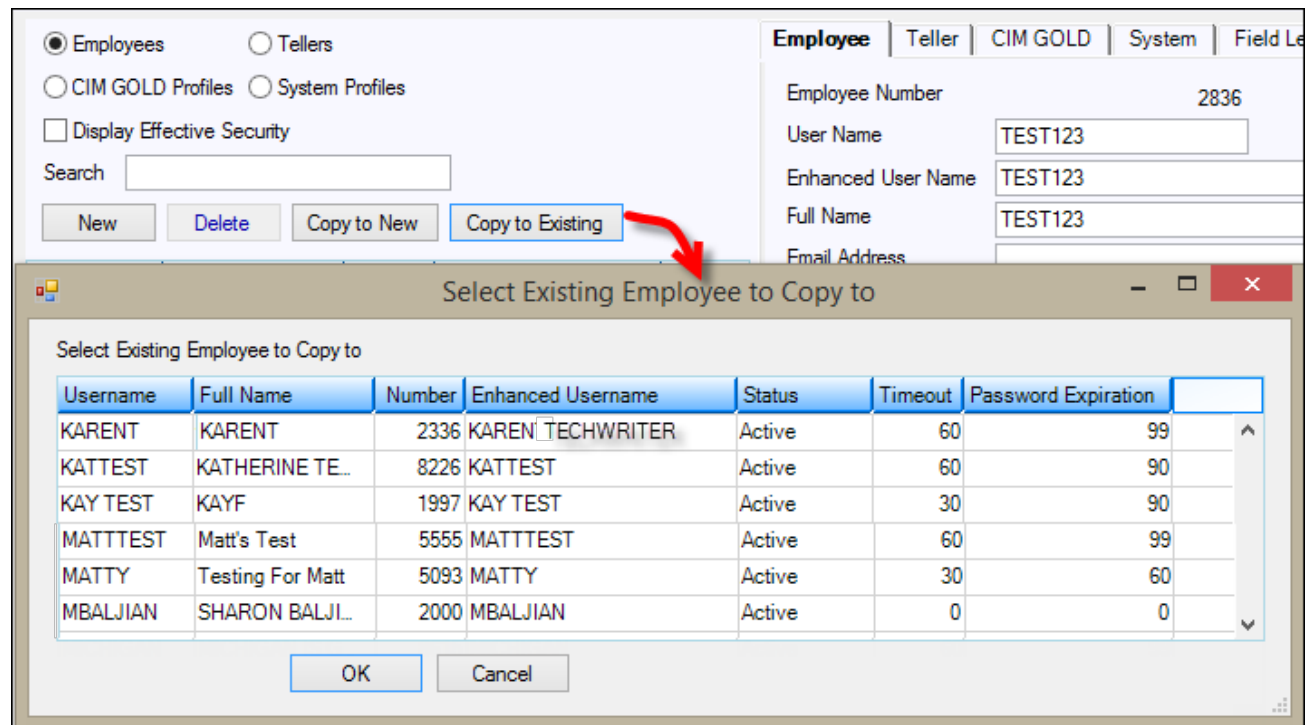
If a password is changed using this method, the password will remain valid until the next Password Expiration interval is reached or the employee forces a password change when logging in to CIM GOLD.

### To copy employee security to a new employee:

1. If the **Display Effective Security** box has a checkmark, click on it to remove it.
2. Select the employee in the list, then click <Copy to New> to copy the security settings from the selected employee to a new employee. All the security, including profiles, will be copied to the new employee. (This does *not* copy Teller information.)
3. Make any adjustments to the new employee's individual security as needed.
4. Click <Save Changes>.

### To copy security from one existing employee to another:

1. If the **Display Effective Security** box has a checkmark, click on it to remove it.
2. Select the employee you will copy from in the list, then click <Copy to Existing>. The "Select Existing Employee to Copy to" dialog box opens.



3. In the dialog box, select the employee you want to copy to. All the security, including profiles, will be replaced for the employee you are copying to. (This does *not* copy Teller information.)
4. Make any adjustments to the new employee's individual security as needed.
5. Click <Save Changes>.

### Deleting an Employee

You can't use the <Delete> button on this screen to remove an employee from the system. This prevents you from accidentally deleting an employee.



### To delete an employee:

1. Select "Terminated" from the **Status** drop-down list.
2. Open the Security > [Terminated Employee Deletion](#) screen and delete them from the system.

### See Also:

[CIM GOLD Profile tab](#)

[System Profile tab](#)

[CIM GOLD tab](#)

## CIM GOLD Profile tab

Use the fields on this tab to set up CIM GOLD profiles. Any CIM GOLD profiles that already exist on the system will be shown in the list view.

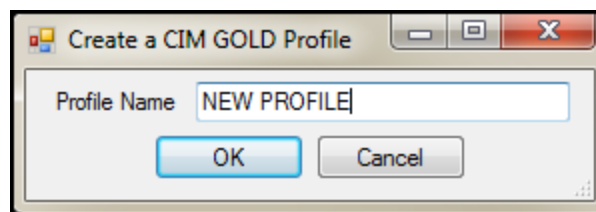
For information on how profiles work and why they are useful, see "[What Is a Security Profile?](#)" in the Security Setup Screen overview section.

### Creating a CIM GOLD Profile

You can copy from an existing profile or create a new one.

#### To create a CIM GOLD profile:

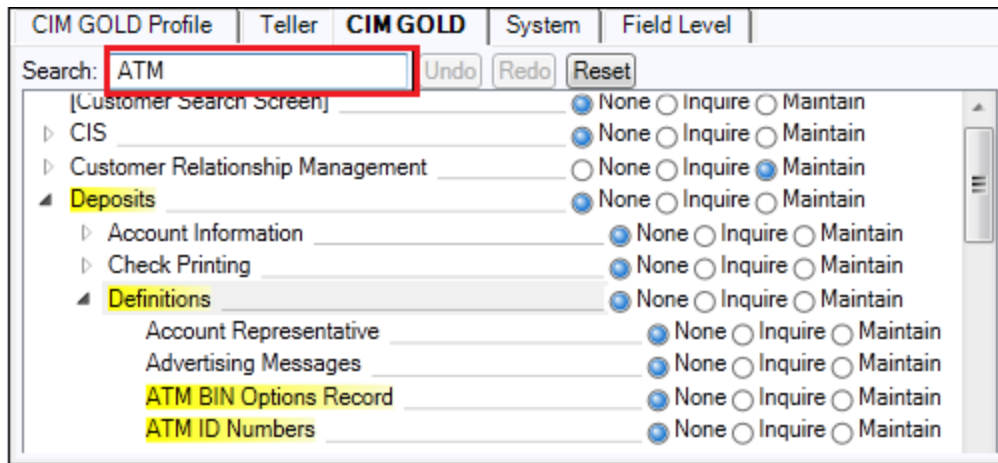
1. On the Security Setup screen, select and click <New>.
2. In the "Create a CIM GOLD Profile" dialog box, type a new **Profile Name** and click <OK>. CIM GOLD Profile names can have up to 12 characters.



3. The new Profile Name will be added to the bottom of the profile list with the default "Active" Status. The new profile name will also be added to the **CIM GOLD Profile Membership** list on the [Employee](#) setup tab and can be selected for employees that will be tied to a profile.
4. On the CIM GOLD tab, select all applications and screens the profile will need to use, then click <Save Changes>. The **Search** field allows you to enter data to find the security setting. If found in the main heading list, the main heading is highlighted. See the example below.







5. If you use field-level security restrictions, open the Field Level tab, select restrictions for the profile, then click <Save Changes>.



## Copying a CIM GOLD Profile

### To copy a profile:

1. Select a CIM GOLD profile from the list.
2. Click <Copy> to copy the security settings from an existing CIM GOLD profile to a new one.
3. Make any necessary adjustments to the new profile.
4. Click <Save Changes>.

## Deleting a CIM GOLD Profile

### To delete a profile:

1. Make sure the profile is not attached to any employees. Otherwise, you will get an error message that tells you employees are assigned to it.
2. Select the CIM GOLD profile and click <Delete>.

### See Also:

[Employee tab](#)

[System Profile tab](#)

[CIM GOLD tab](#)

## System Profile tab

Use the fields on this tab to set up security for all FPS GOLD products not listed on the CIM GOLD tab. Only employees with proper security (such as a Security Administrator) can set up system profiles.

For information on how profiles work and why they are useful, see "[What Is a Security Profile?](#)" in the Security Setup Screen overview section.

## Creating a System Profile

You can copy from an existing profile or create a new one.

### To create a System profile:

1. On the Security Setup screen, select **System Profiles**, then click <New>.



Employees     Tellers  
 CIM GOLD Profiles     System Profiles  
 Display Effective Security  
 Search   
           

Legacy Name	Description	Prof #	Profile Name		Timeout	Password Expiration
DEPLOYAD	Gold Deploy administrator	8765	DeployAdministrator	Active	0	0
DEPLOYER	Gold Deploy deployer	8766	Deployer	Active	0	0
DEPLOYUS	Gold Deploy user	8767	DeployUser	Active	0	0
TEST	System Profile Test	100	System Profile Test	Active	0	0

- In the Create a new Profile dialog box, enter the appropriate information in the fields (see the example below). FPS GOLD recommends that you designate an employee number range to use for System , such as 9900–9989. The name assigned to the profile will be listed in the System Profile drop-down list on the Employee setup tab and can be selected for employees that will be tied to a profile. A System **Legacy Name** can have up to eight characters. It cannot be the same as any other profile or user name. The **Profile Name** and **Profile Description** can be up to 40 characters long and can be used to further define the profile. When you have finished entering information, click <OK>.

Create a new Profile

Profile Number:   
 Legacy Name:   
 Profile Name:   
 Profile Description:   
   

The new profile will be shown in the profile list with the default “Active” Status.

- On the System tab, select all functions the profile will need to use, then click <Save Changes>.

After profiles have been set up, create individual employee security on the [Employee tab](#), and tie each employee setup to the appropriate profiles.

## Copying a System Profile

### To copy a profile:

- Select a System profile from the list.
- Click <Copy to New> to copy the security settings from an existing System profile to a new one.  
or



Click <Copy to Existing> to copy the security settings from one existing System profile to another.

3. Make any necessary adjustments to the new profile.
4. Click <Save Changes>.

## **Deleting a System Profile**

### **To delete a profile:**

1. Make sure the profile is not attached to an employees. Otherwise, you will get an error message that tells you employees are assigned to it.
2. Open the Security > [Terminated Employee Deletion](#) screen and delete the profile.



## EFT GOLD Security Groups

Add employees to EFT GOLD security profiles based on the actions they need to perform in EFT GOLD. The actions and functions the profiles control in EFT GOLD are explained below.

### IMPORTANT

The predefined System Profiles used for EFT GOLD *should not* be changed in any way. If they are changed, your user security functions will not work.

Within EFT GOLD, the security groups are found under Administrative Options > Users/Groups. The example below is sorted alphabetically. Your profile numbers and descriptions may not match these.

WireAdminSecurityGroup
WireCanOverrideTransactionErrors
WireMessageReaderGroup
WireMessageUpdaterGroup
WireOfacApproverGroup
WireOfacWhitelistUpdaterGroup
WireUserAdminSecurityGroup
WireUserSecurityGroup
WireViewFrbBalanceSecurityGroup

Predefined EFT GOLD User Profiles

### WireAdminSecurityGroup


The users in this group have access to all Admin functions except Users. The menu items secured by this option are found on the menu under Management, Options, Custom Rules, Alerts, OFAC Whitelist, and System Logs.

### WireCanOverrideTransactions

Users in this group can approve wires but not OFAC suspects. Dual control is used, so approvers cannot approve their own submitted wires. The user's limits are used when this action is processed.

### WireMessageReaderGroup


Users in this group can view FRB wire messages. "FRB Messages/View FRB Messages" is found on the menu.

Click  to open the menu.

### WireMessageUpdaterGroup



Users in this group can create and send FRB messages. If you can create and send messages, you can also view them if you do not remove WireMessageUpdaterGroup from the WireMessageReaderGroup.

"FRB Messages/View FRB Messages" is found on the menu. Click  to open the menu.

**WireOfacApproverGroup**

Users in this group can approve OFAC suspects, but not wires.

**WireOfacWhitelistUpdaterGroup**

Users in this group can approve OFAC suspects and add names to your Whitelist.

**WireUserAdminSecurityGroup**

The users in this group have access to Users functions on the menu under Admin > Users.

**WireUserSecurityGroup**

Every user that is going to access anything in EFT GOLD needs to be in this group. The billing for EFT GOLD is based on the users with this security.

**WireViewFrbBalanceSecurityGroup**

Users in this group can view your institution's FRB balance on the Dashboard. Without this security, the user cannot see the balance information.

## GOLDDeploy Security Groups/Profiles

The predefined System Profiles used for GOLDDeploy should not be changed in any way. If they are, your user security functions will not work. Add employees to these profiles based on the actions they need to perform in GOLDDeploy. The actions and functions the profiles control in GOLDDeploy are explained below.

**DeployAdministrator**

The users in this group have access to design parameters and options for deployment of FPS GOLD® software to your users. Users in this group are administrators, deployers, and viewers. They don't need any other security settings.

**Deployer**

The users in this group have access to schedule and deploy FPS GOLD software releases to your users. Users in this group can also view all screens.

**DeployUser**

The users in this group can only view the schedules and options that are set up but cannot make changes.

**See Also:**

[Employee tab](#)

[CIM GOLD Profile tab](#)

[CIM GOLD tab](#)

## CIM GOLD tab

Use the fields on the CIM GOLD tab of the Security > Setup screen to set up CIM GOLD security for your employees. Some CIM GOLD applications also require some security settings on the System tab. CIM GOLD security is used for the screens; System security is used for functions within the screens and for financial applications.



## Setting Up CIM GOLD Security

Before any employee can access CIM GOLD, security clearance must be set up for that employee. CIM GOLD security can be set up on individual employees and/or on . The profiles can be tied to employees who require the same security clearance to perform their job duties. If multiple profiles are tied to an employee, Effective Security can be viewed.

### To set up CIM GOLD access for an employee or profile:

1. On the Security Setup screen, select **Employees** or **CIM GOLD Profiles**.
2. Select the CIM GOLD tab.
3. In the **Security Setup list view**, select the employee or CIM GOLD Profile for which security is being set up or changed.

The screenshot shows the Security Setup interface with the following components:

- Navigation:** Radio buttons for Employees, Tellers, CIM GOLD Profiles (selected), and System Profiles. A checkbox for "Display Effective Security" is present.
- Search:** A search field and buttons for New, Delete, and Copy.
- Profile List:** A table with columns Name, Status, and Desc. The "ALL F/M" profile is selected.
- Application List:** A list of applications with radio buttons for access levels: None, Inquire, and Maintain. The "None" option is selected for all items.
- Buttons:** Undo, Redo, Reset, and Save Changes.

Name	Status	Desc
	Active	
ALL F/M	Active	
CIMSECADM	Active	jur
CIMSECAD2	Active	
CINDY TEST	Active	
CINDY TEST	Active	
CONNECTL..	Active	
COPY TEST	Active	

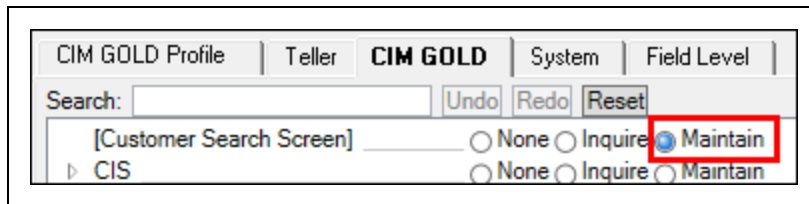
[Customer Search Screen]	<input checked="" type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ CIS	<input type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Customer Relationship Management	<input checked="" type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Deposits	<input checked="" type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ GOLD Services	<input checked="" type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ History	<input checked="" type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Internet and Phone Systems	<input type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Internet and Phone Systems Setup	<input checked="" type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Loans	<input type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Miscellaneous	<input type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Other Applications	<input checked="" type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Queues	<input type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Report Warehouse	<input type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Security	<input checked="" type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain
▶ Teller System	<input checked="" type="radio"/> None	<input type="radio"/> Inquire	<input type="radio"/> Maintain

4. Select **Inquire** or **Maintain** on each item listed below the applications to which the employee or CIM GOLD Profile should have access. If no access is allowed, select **None**.

### NOTE

If you want employees to have security to change User Preferences under the Options menu at the top of the CIM GOLD screen, you must select "Maintain" for the first item, [Customer Search Screen], on the CIM GOLD tab. See the example below.





5. When you have finished making selections, click **<Save Changes>**.

### See Also:

[Employee tab](#)

[CIM GOLD Profile tab](#)

[System Profile tab](#)

## System tab

Use the fields on the System tab on the [Security > Setup screen](#) to set up security for all other FPS GOLD products not listed on the CIM GOLD tab for your employees. Some CIM GOLD applications also require some security settings on the System tab. CIM GOLD security is used for the screens; System security is used for functions within the screens and for financial applications.

### Setting Up System Security

The System tab is used to set up security for employees and profiles that need to have access to all other FPS GOLD programs that are not listed on the CIM GOLD tab. The System tab will be disabled if you have not selected **Employees** or **System Profiles**.

Many of the applications listed on the System security tab are obsolete and have been programmed to be used in CIM GOLD, such as GOLD ExceptionManager and IRS GOLD. However, you must select the **Maintain** radio button for the **FPS PC Applications** function on the System tab to grant access to CIM GOLD. There are also other functions in PC Applications which can control access to CIS, employee and officer names, as well as other PC applications. Obsolete menus have been removed from this documentation.

Applications and functions are listed in alphabetic order. Set each option for access for each employee or profile.

### To set up System security:

1. On the Security > Setup screen, select either the **Employees** or **System Profiles** radio button.
2. In the list view on the left side of the screen, select the employee or profile you want to set up.
3. Select the System tab, as shown below.





Employees     Tellers  
 CIM GOLD Profiles     System Profiles  
 Display Effective Security  
 Search   
            

 Employee | Teller | CIM GOLD | **System** | Field Level |  
 Search:

User Name	Full Name	Emp #	Enhanced Username	Status
APRILY	April Non Editor	2131	apriyl	Active
BRETTG1	brett non editor	2206	brettg1	Inactive
BUDDY	Username2129	2129	buddy	Inactive
CORBINE	corbine	2351	corbine	Inactive
DAYNAK	daynak	1920	daynak	Active
DOUGB	Doug Brown	1275	dougb	Active
EASTON	Cindy Easton	8920	EASTON	Inactive
ELISHAB	Elisha Baker	2392	elishab	Inactive
ETHAN	Ethan Test User	2115	2115	Active
HERBIE	Username3129	3129	herbie	Inactive
JULIEW	juliew	1795	juliew	Active
JULIEW2	juliew2	1796	juliew2	Inactive
PENNYW	pennyw	2358	pennyw	Active
RMOYES	Rodger Non Editor	7777	rmoyes	Inactive
RODGER	Rodger M	1559	rodger	Inactive
STACEY	stacey	1790	stacey	Inactive
TAMMY2	Tammy Ford Non	1238	Tammy2	Inactive
TAMMYF	Tammy Ford	1237	TAMMYF	Active
TERESA	Teresa Ortiz Non...	1233	TERESA	Active
TERESAF	Teresa Ortiz Editor	1533	TERESAF	Active

Account Merchant List <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Accounting Report Writer <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Accounts Payable <input type="radio"/> None <input type="radio"/> Inquire <input type="radio"/> Maintain **drop <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain **drop Function <input type="radio"/> None <input type="radio"/> Inquire <input type="radio"/> Maintain Ach Invoice Verification <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Ach Pmt Threshold Verification <input checked="" type="radio"/> None <input type="radio"/> Inquire <input type="radio"/> Maintain Capital Approval <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Cash Planning <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Category Codes <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Change Client Number <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Check Reconciliation <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Check Register <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Contract File <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Control Statement Register <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Dist. Screen Formats <input type="radio"/> None <input type="radio"/> Inquire <input type="radio"/> Maintain Distribution Profile <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Emp. Code in Responsibility <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Flag Invoices for Payment <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Inventory Product <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Inventory Product Spcl Changes <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Invoice Payee <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Item Profiles <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Location Profiles <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Multiple File Changes <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Only Post To Term Table Office <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Post Recurring Payments <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Print Checks <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Print Control Statements <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Print Reports <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Print Requests <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Recurring Payments <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Report Formats <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain Set Up Report Writer Reports <input type="radio"/> None <input type="radio"/> Inquire <input checked="" type="radio"/> Maintain
--

3. Select **Inquire** or **Maintain** on each item listed below applications to which the employee or profile should have access. If no access is allowed, select **None**. "Inquire" means the employee can view information on the screen but cannot change it. "Maintain" means an employee can view and change information on the screen.
4. When you have finished making selections, click **<Save Changes>**.

For a list of all security options on this tab and a short description, see [System Security Details](#).

**See Also:**

- [Employee tab](#)
- [CIM GOLD Profile tab](#)
- [System Profile tab](#)

## System Security Details

The following tables list all possible security options on the [System tab](#) of the Security > Setup screen. Only specific security personnel at your institution can set up these screens for employees. These options affect which applications employees have access to, as well as other features and functions within applications.



Account Merchant List - OBSOLETE

[Accounting Report Writer](#)

[Accounts Payable](#)

Accounts Receivable - OBSOLETE

Additional Loan Security - OBSOLETE

[Allow Customer Support Access](#)

[Alter Terminal for Payroll](#)

Commercial Loan Menu - OBSOLETE

[Core File Synchronization](#)

[Core Tools](#)

Customer Information File - OBSOLETE

Deposit Document Prep System - OBSOLETE

Deposit System - OBSOLETE

Electronic Teller Journal - OBSOLETE

Event Letter Parameters - OBSOLETE

[Financial Options](#)

[Fixed Assets](#)

[FPS PC Applications](#)

[Fps-Change Terminal Options](#) - OBSOLETE

Funds Distribution - OBSOLETE

[General Institution Options](#)

[General Ledger System](#)

[GL GOLD](#)

[GOLD ExceptionManager](#)

[GOLD Miner Downloads](#)

GOLDPhone Processing - OBSOLETE

[GOLD Services](#)

[GOLDTeller Security](#)

[GOLDTrak Loan Tracking System](#)

[GOLDView](#)

[GOLDView 32](#)

Item Posting Rejects - OBSOLETE

Loan System - OBSOLETE

Materials Management - OBSOLETE



Office Management - OBSOLETE

Old Office Management System - OBSOLETE

Organization Options - OBSOLETE

[Payroll Management](#)

[PC Check Image Utilities](#)

Prrpts0 - OBSOLETE

[Report Warehouse Menu](#)

Report Writer - OBSOLETE

[Reports and Dacosys Options](#)

[Security Management](#)

[System Print Program](#)

Utility Programs - OBSOLETE

[Web Security](#)

Accounting Report Writer - Application 50		
Bit #	Function Name	Function
03	Dictionary	
01	Run Reports	
02	Set Up Reports	

Accounts Payable - Application 7		
Bit #	Function Name	Function
15	**DROP	6,10
17	**DROP Function OBSOLETE	
36	Ach Invoice Verification	16
39	Ach Pmt Threshold Verification	16
30	Capital Approval	
06	Cash Planning	4
18	Category Codes	
61	Change Client Number	66
12	Check Reconciliation	32
05	Check Register	27
27	Contract File	
38	Control Statement Register	43



Accounts Payable - Application 7		
14	Dist. Screen Formats	9/10
10	Distribution Profile	5/6
31	Emp. Code in Responsibility	
04	Flag Invoices for Payment	8, 12, 15
22	Inventory Product	
23	Inventory Product Spcl Changes	
08	Invoice Payee	30
24	Item Profiles	
28	Location Profiles	
29	Multiple File Changes	1-6 / 2-6
62	Only Post To Term Table Office	30, 34
09	Post Recurring Payments	34
03	Print Checks	20
3	Print Control Statements	36
02	Print Reports	
26	Print Requests	1-5 / 2-5, 15
13	Recurring Payments	13/14
01	Report Formats	59-2
16	Report Writer	63
20	Responsibility File	1-3 / 2-3
33	Restrict Detail Fields	18, 30
64	Run Report Writer Reports	63-1, 63-7
25	Screen Formats	
63	Set Up Report Writer Reports	63-2, 63-3, 63-4, 63-6
19	Ship To Locations	1-1 / 2-1
07	Transaction Processing	29/30
32	Vendor Alternate Payee	2-4, 18
21	Vendor File	1-4 / 2-4, 17/18
35	Vendor Master Ach Screen	17/18, <F2>
11	Void Checks	24
37	Void Control Statements	40



Accounts Receivable - **OBSOLETE**

Additional Loan Security - **OBSOLETE**

Allow Customer Support Access - Application 30

Bit #	Function Name	Function
01	Allow Customer Support Access	

Alter Terminal for Payroll - Application 30

Bit #	Function Name	Function
01	Access	Alter terminal institution and office number

Commercial Loan Menu - **OBSOLETE**

Core File Synchronization

Bit #	Function Name	Function
01	Download Security	

Core Tools

Bit #	Function Name	Function
01	Access	

Customer Information File - **OBSOLETE**

Deposit Document Prep System - Application 4 - **OBSOLETE**

Deposit System - Application 4 - **OBSOLETE**

Electronic Teller Journal - **OBSOLETE**

Event Letter Parameters - **OBSOLETE**



Financial Options - Application 18		
Bit #	Function Name	Function
16	Account Number Structure	
05	Accounts Payable	
06	Accounts Receivable	13/14
01	Company Name/Accounting Prds	3/4
	Financial Options	
	Financial Routing Info Rec	
04	Inventory	
07	Payroll Options	15/16
03	Requisition/Purchase Order	

Fixed Assets - Application 33		
Bit #	Function Name	Functions
01	Access to Program	Gives access to the <a href="#">Fixed Assets system (Application 33)</a> in GOLDVision.
04	Change Client Number	To access clients other than 0 (zero) in the Fixed Assets system, the <b>Maintain</b> radio button must be selected for this option. This is mainly for FPS GOLD use.
05	Distribution Profiles (F8)	
63	Report Writer Report Setup	63-2, 63-3, 63-4, 63-6
64	Report Writer Run Report	63-1, 63-7

FPS PC Applications - Application 57		
Bit #	Function Name	Function
01	Access to PC Applications	WinTerm, GOLDTeller, GOLDPrint, GOLDView, G/L GOLD, GOLDVision, GOLDWriter, GOLD ExceptionManager, GOLDAcquire, CIM GOLD, IRS GOLD
40	Allow Gateway to Alter Terminal	GOLDGateway
41	Chat/remote = F.Remote = I	Access to use chat and remote override
19	CheckWriter Change/add Checks	CheckWriter
22	CheckWriter Change/add Docs	CheckWriter



FPS PC Applications - Application 57		
18	CheckWriter List Checks	CheckWriter
21	CheckWriter List Docs	CheckWriter
20	CheckWriter Print Checks	CheckWriter
27	CIM Can See Employee Dep Accounts	CIM GOLD
38	CIM Can See Employee Dep History	CIM GOLD
33	CIM Can See Employee Ln Accounts	CIM GOLD
39	CIM Can See Employee Ln History	CIM GOLD
42	CIM GOLD Document Imaging	CIM GOLD
24	CIM Security Setup	CIM GOLD
26	CIM Subscription Setup	CIM GOLD
25	CIM User Defined Help Setup	CIM GOLD
02	CIS Access to Emp/offcr Name	CIS (in CIM GOLD)
29	EFTGOLD Access	EFT GOLD
31	EFTGOLD Approve Wires	EFT GOLD
32	EFTGOLD Change Options	EFT GOLD
30	EFTGOLD Submit Wires	EFT GOLD
36	EFTGOLD View Inbound Wires	EFT GOLD
37	EFTGOLD View Outbound Wires	EFT GOLD
28	EFTGOLD Wire Limits	EFT GOLD
23	Eis/dsr Email Setup	Executive Reports
50	File Services Access Settings	File Services Plus
46	File Services Attach Files	File Services Plus
47	File Services Delete Files	File Services Plus
52	File Services Edit Metadata	File Services Plus
51	File Services Export Files	File Services Plus
53	File Services F/M Cache Folder	File Services Plus
49	File Services Stats / History	File Services Plus
48	File Services Transfer Files	File Services Plus



FPS PC Applications - Application 57		
45	File Services Utility Access	File Services Plus
34	GOLDAcquire Access	GOLDAcquire
35	GOLDAcquire Upload	GOLDAcquire
44	GOLDEventLetters Access	GOLD EventLetters
43	GOLDLink Skip / Delete Loan	GOLDLink
11	GOLDWriter Access	GOLDWriter
05	Imaging Acquire From Scanner	GOLDDocument Imaging
14	Imaging Change Group	GOLDDocument Imaging
15	Imaging Change Subgroup	GOLDDocument Imaging
03	Imaging Create Database	GOLDDocument Imaging
12	Imaging Create Group	GOLDDocument Imaging
13	Imaging Create Subgroup	GOLDDocument Imaging
09	Imaging Delete Images	GOLDDocument Imaging
16	Imaging Export Images	GOLDDocument Imaging
07	Imaging Import Images	GOLDDocument Imaging
08	Imaging Modify Image Info	GOLDDocument Imaging
04	Imaging Open Database	GOLDDocument Imaging
10	Imaging Print	GOLDDocument Imaging
17	Imaging Properties	GOLDDocument Imaging
6	Imaging Select Scanning Source	GOLDDocument Imaging
55	Pci Card Vault	
54	View Entire Card Number	

#### Fps-Change Terminal Options - Application 24 - **OBSOLETE**

General Institution Options		
Bit #	Function Name	Functions
01	Access	
02	Batch Reports Fiche/print	
09	External G/L Posting Setup	
06	General Ledger Autopost Setup	





General Institution Options		
08	General Ledger Cross Reference	
11	Ledgers Control	
12	Ledgers Defaults	
10	Make an Available Account	
03	Print Batch Reports Options	
07	Print G/L Autopost Parameters	
13	Rate Tiers Processing	
05	Rates Tables Processing	
04	Teller Information Processing	

General Ledger System - Application 1		
Bit #	Function Name	Functions
13	Account Budget F/M	53/54, 57/58
26	Account Defaults	79/80
03	Account File Maintenance	53/54, 57/58
16	Account Number Structure	5/6
29	Allow Acct Drop with Bal/Trans	54, 58
30	Allow G/L Sweeps	95/96, 99
15	Budget Rec Disp/Del/Prep/Spred	72, 76, 83/84
25	Calculate Avg Daily Balance	78
11	Close Balances to Next Year	64
01	Company Options Definitions	1/2
27	Copy a Control Group	86
02	Custom Report Definitions	41/42
20	Custom Report Line Detail	40
24	Custom Report Messages	69/70
21	Define Group of Reports	55/56
28	Distribution Profile, Branch Allocation Table	87/88, 91/92



General Ledger System - Application 1		
14	Employee Report Security	81/82
23	Enter Client Number	66
19	Organizational Chart	36
12	Post From Other Applications	68
09	Print Custom Reports	24, 28, 32, 32-1, 32-2, 32-4
10	Print Custom Reports Outofbal	24, 28, 32
08	Print Standard Reports	19/20, 32-5
64	Reserved	
22	Statement Pre-requisites	59/60
18	Sub-Account Titles	17/18, 21/22, 25/26, 29/30, 33/34
04	Trans Dsply/Corr/Drop/Xfer	11/12
05	Trans F-M/Delete/Xfer/Clsd Grp	12
17	Transaction Deletion	16
06	Transaction Entry	8
07	Transaction Entry Past/Future	8

GL GOLD		
Bit #	Function Name	Function
01	Access	

GOLD Services - Application 8		
Bit #	Function Name	Function
21	ATM Comparative Totals <b>OBSOLETE</b>	
12	Bank table Inquiry <b>OBSOLETE</b>	
13	Bond Redemption <b>OBSOLETE</b>	
20	Calculate Date or Days <b>OBSOLETE</b>	
07	Check Recon Detail/Summary <b>OBSOLETE</b>	
09	Check Recon Mass Deletes <b>OBSOLETE</b>	



GOLD Services - Application 8		
08	Check Recon Print Reports <b>OBSOLETE</b>	
11	Check Recon Transmission Hist <b>OBSOLETE</b>	
10	Check Recon Void Checks <b>OBSOLETE</b>	
31	Comp Track Branch Setup	100, then 107/108
34	Comp Track Calculation (INQ)	100, then 113
33	Comp Track Default Setup	100, then 111/112
28	Comp Track Hist Summary (INQ)	100, then 101
29	Comp Track History Detail	100, then 103/104
30	Comp Track Pay Setup	100, then 105/106
32	Comp Track Teller Setup	100, then 109/110
22	Deposit Audit Confirmation <b>OBSOLETE</b>	
19	Deposit Event Setup <b>OBSOLETE</b>	
17	Field Level Security (Loans - APR screen) <b>OBSOLETE</b>	
01	G/L Autopost Setup <b>OBSOLETE</b>	
16	Holiday Scheduling (Loan Past Due Notices) <b>OBSOLETE</b>	
04	IRS Create Returns (F/M) <b>OBSOLETE</b>	
05	IRS Delete All Returns (INQ) <b>OBSOLETE</b>	
02	IRS Information Returns <b>OBSOLETE</b>	
03	IRS Print All Returns (INQ) <b>OBSOLETE</b>	
18	Loan Additional Fields Services <b>OBSOLETE</b>	
23	Loan Audit Confirmation <b>OBSOLETE</b>	
06	Online ACH Posting <b>OBSOLETE</b>	
14	Online ATM Journal <b>OBSOLETE</b>	
27	Privacy Options <b>OBSOLETE</b>	
15	Store/Forward Display/Print <b>OBSOLETE</b>	
24	System Printing <b>OBSOLETE</b>	
25	WWW ACH Batch Queue <b>OBSOLETE</b>	
26	WWW ACH Security <b>OBSOLETE</b>	



**GOLDPhone Processing - Application 35 - OBSOLETE**
**GOLD ExceptionManager**

Bit #	Function Name	Function
15	Allow Change To Transaction	
16	Allow Other User Pref Setup	
10	Can Post Loan Items	
4	Create Notification of Change	
17	May Make Posting Decisions	
11	Officer/employee Acct Access	
2	Process Exception Items	
13	Z Allow Save/remove Selections <b>OBSOLETE</b>	
8	Z Calibrate Printer <b>OBSOLETE</b>	
6	Z Create a Chargeback Item <b>OBSOLETE</b>	
5	Z Create a Return Item (noinq) <b>OBSOLETE</b>	
7	Z Print Reports and Notices <b>OBSOLETE</b>	
9	Z Save Notice Headers <b>OBSOLETE</b>	
12	Z User List Maintenance <b>OBSOLETE</b>	

**GOLDTeller Security**

Bit #	Function Name	Function
14	Allow Changing Institutions	Change Institutions
04	Check Imaging	
09	Clear/Synchronize Totals	Clear PC Totals/Synchronize PC Totals With Host Totals
16	Database Backup/Restore	Backup Data Files/Restore Data Files/Delete Data Files
05	Forms Design	View/Modify Forms and Droplists
15	GOLDTeller Platform	Platform Session
12	Jrnl Search on Other Ops	Journal/Forward on Other Operators
03	Not Used	
01	Operator File	Operator Information



<b>GOLDTeller Security</b>		
36	Platform Delete/Merge Sessions	
35	Platform File Directories	
34	Platform Options	
37	Platform Sales Tracking	
33	Platform Setup	
08	Print Configuration	Form/Font Configuration
11	Signature Capture	Signature Capture and Display
02	System Configuration	System Configuration
10	System Fields Dictionary	System Field Dictionary
06	Transaction Design	Transaction Design/PC Institution Options
07	Transaction Selection Design	Transaction Selection Design
13	Upload/Download Data File	Upload File to Host/Download File to Host

<b>GOLDTrak Loan Tracking System</b>		
<b>Bit #</b>	<b>Function Name</b>	<b>Function</b>
58	148 Access Apr Screens	
36	Access F1833, Plaza Savings	
29	Access To Appl. On Dead File	
7	Access To Docprep (pf2) Screen	
34	Access To F4385 - Allow Docs	
1	Access To GOLDTrak System	
37	Administrative Security	
44	Agent Screen Access	
18	Allow Unlk Of Lock, Table Flds	
17	Allow Update of 'lock' Group	
30	Allow Update to Default Number	
2	Appl. Inquiry, F/m, or New	
35	Appraisers I=select, F=change	
22	Appraisers Table #3	
46	Branch Manager Override	
38	Branch No. Control On New Apps	
39	Branch Supervisor Security	



GOLDTrak Loan Tracking System		
45	Broker, input, no Status	
23	Brokers Table #4	
5	Build Document Formats (pf2)	
6	Formula Setup (pf2)	
43	Formula Test Mode Access	
54	Freddie Mac Order Screen	
56	Internet Queue Security	
53	Inventory Queue Drop Security	
19	Literal Cnst & Table Acc (pf2)	
28	Literal Constants Access #0	
21	Loan Officers Table #2	
20	Loan Programs and Office Tab#1	
41	Loan Que Printing	
50	Lock Group 10 Access	
51	Lock Group 11 Access	
52	Lock Group 12 Access	
47	Lock Group 7 Access	
48	Lock Group 8 Access	
49	Lock Group 9 Access	
3	Modify Group Input Formats	
10	Move Info To Servicing Files	
33	New X-add Fm,limit Inq- Tables	
24	Override All Lock Security	
31	Override Off # Limits - Tables	
32	Override Status Code - Tables	
16	PC Forms Upload	
11	Print Document Params. (pf2)	
9	Print Documents	
12	Print Field Names (pf2)	
8	Print Formulas (pf2)	
13	Print Input Groups (pf2)	
15	Process Formula Calculations	
55	Release Formulas New Fmlas	



<b>GOLDTrak Loan Tracking System</b>		
4	Rename Field Names (pf2)	
14	Report Writer Access From Here	
42	Secondary Marketing	
57	Unlock Application Security	
27	Verification Of Deposits #8	
25	Verification Of Employments #6	
26	Verification Of Mortgages #7	
40	Wire Screen Access	

<b>GOLD Miner Downloads</b>		
<b>Bit #</b>	<b>Function Name</b>	<b>Function</b>
64	Administrator User	
01	CIF Download	
06	Deposit Download	
09	GOLDMiner Billing Download	
04	GOLDPhone Download	
07	GOLDTrak Deposit Download	
03	GOLDTrak Download	
05	Loan Download	
08	Loan Payee Download	

<b>GOLDView</b>		
<b>Bit #</b>	<b>Function Name</b>	<b>Function</b>
02	Access to Deposit Reports	
03	Access to General Ledger Rpts	
06	Access to GOLDView Reports	
01	Access to Loan Reports	
05	Access to Payroll Reports	
04	Access to Teller Reports	

<b>GOLDView 32</b>		
<b>Bit #</b>	<b>Function Name</b>	<b>Function</b>
02	Access to Deposit Reports	



GOLDView 32		
03	Access to General Ledger Rpts	
01	Access to Loan Reports	
05	Access to Payroll Reports	Payroll File Maintenance Report, FPSDR145
08	Access to Restricted Reports	Employee Deposit Statements, FPSDR199 based on Warehouse index category
07	Access to Special Reports	Reports FPS GOLD processes, such as loan drops
04	Access to Teller Reports	
06	Access to Warehouse Reports	Reports processed by FPS GOLD requiring a separate ISO file

**Loan System - OBSOLETE**

**Materials Management - OBSOLETE**

**Office Management - OBSOLETE**

**Old Office Management System - OBSOLETE**

**Organization Options - OBSOLETE**

**Payroll Management - Application 11**

Bit #	Function Name	Function
43	Alternate Posting	1-15/2-15
41	Batch Reports	
61	Change Client Number	66
13	Check Reconciliation	40
11	Co Emp Pay Change/F1 - Emp Mstr	13<F1>/14<F1>, 38
21	Company Benefits	1-5/2-5
19	Company Deductions	1-3/2-3
18	Company Earnings	1-2/2-2
28	Company User Fields	1-12/2-12
33	Daily F/M	59.1.1
16	Dept Employee Changes	58
37	Distribution	59.1.6





Payroll Management - Application 11		
08	Emp. Benefits	33/34
04	Emp. Earnings/Deductions	21/22, 25/26
06	Emp. Evaluation	
36	Emp. Not Posted and Balancing	59.1.4, 59.1.13
03	Emp. Payroll History	17
05	Emp. Profile	
15	Employee Master	13/14, 13<F1>/14<F1>, 13<F2>/14<F2>, 13<F7>/14<F7>, 13<F10>/14<F10>
34	Employee Master and Labels	59.1.2, 59.1.1
29	Employee Number Change	1-13/2-13
49	Employee Pay Amounts	13<F1>/14<F1>
35	Employee Pay Information	59.1.3, 59.1.5, 59.1.7, 59.1.9, 59.1.11, 59.1.14, 59.1.15, 59.1.18, 59.1.20, 59.1.21, 59.1.22
50	Employee User Field 1	41/42
51	Employee User Field 2	41/42
52	Employee User Field 3	41/42
53	Employee User Field 4	41/42
54	Employee User Field 5	41/42
42	FTE Report	59.1.19
23	Job Cost Codes	1-7/2-7
25	Job Description File	1-9/2-9
27	Job Status File	1-11/2-11
44	Monthly Tax Liability	
26	Pay Grade File	1-10/2-10
10	Payroll Adjustments	12
17	Payroll Cycles	1-1/2-1
09	Payroll Posting - F/M	8, 15/16
38	Position Control and Budget	59.1.8, 59.1.38
30	Position Control Budget Info	1-14/2-14, 2-8<F1>
24	Position Control File	1-8/2-8
55	Post Rate Changes	20, 24
40	Posting Errors	59.1.12
12	Print Payroll Checks	36



Payroll Management - Application 11		
02	Print Reports	59-1.34-42 / 59.2.34-42
22	Project Codes	1-6/2-6
01	Report Formats	59.2.34-42
07	Report Writer	63.1-63.7
63	Report Writer Report Setup	63.2-63.4
64	Report Writer Run Report	63.1, 63.7
20	Tax Tables	1-4/2-4
39	Time Cards	59.1.16
14	Void Checks	44, 48

PC Check Image Utilities		
Bit #	Function Name	Function
06	Modify Auto Print Options	
03	Process Check Exceptions	
02	View Check Exceptions	
01	View Check History	
05	View Check Image Options	
04	View Check Images	

Prrpts0 - **OBSOLETE**

Report Warehouse Menu - Application 53		
Bit #	Function Name	Functions
03	Print Position Selection	37/38
02	Report/Line/Index Selection	31/32, 33/34, 35/36
01	Warehouse Directory	1/2
04	Warehouse Options	39/40

Report Writer - **OBSOLETE**

Reports and Dacosys Options		
Bit #	Function Name	Function



Reports and Dacosys Options		
02	Report Functions	
01	Update Functions	

Security Management - Application 19		
Bit #	Function Name	Function
01	Administrative Functions	
04	Appl. Programmer Functions	
03	Print Requests (2, 3, 4)	<F9>, then 2, 3, or 4
05	Reset Security Code	<F11> Reset Emp. Password
02	Reset Security Violation (F9)	<F9>

System Print Program		
Bit #	Function Name	Function
01	Access	

#### Utility Programs - Application 10 - **OBSOLETE**

Web Security		
Bit #	Function Name	Function
16	Allow Customer Blog	Web banking
02	Allow Software Downloads	Web banking
13	Allow Ticket Submission	Web banking
01	Allow Web Logon/training	Web banking
14	Allow Wo Prioritization	Web banking
06	EIS All	Web banking
12	EIS Branch	Web banking
07	EIS Division a	Web banking
08	EIS Division B	Web banking
09	EIS Division C	Web banking
10	EIS Region	Web banking
11	EIS State	Web banking
05	E-work Orders	Web banking



<b>Web Security</b>		
15	Executive Files	Web banking
04	Executive Information System	Web banking
03	Knowledge Base Access	Web banking



## Field Level tab

The Field Level tab on the [Security > Setup screen](#) is used to set up *restricted* file maintenance to specific data fields for employees. In order to use this feature, employees must first be set up with CIM GOLD application and screen security using the [CIM GOLD tab](#) before any field-level security can be tied to them. If an employee is tied to a CIM GOLD profile, the profile name is used to set up restricted access in Field Level Security. If multiple profiles with different field-level security are tied to an employee, all the secured fields from all profiles will be restricted for the employee.

If the Field Level Security feature is not going to be used by your institution, no work is required with this screen. When “Maintain” access is given to applications and screens, all the fields are file maintainable until they have been restricted individually or on a profile setup using this screen.

### NOTE

Field Level Security is for CIM GOLD applications and does not correspond with any other PC product.

The Field Level Security screen is organized into two sections. The **Restricted Fields** list view shows all the fields that are restricted for the employee or profile selected. The **All Fields** list view is used to restrict the specific fields for an employee or profile based on **Record Type**.

The **Record Type** dictates what fields are available for the specified type. For example, CSPI is for CIS Customer Profile. The records are the same as the records used in GOLDWriter and system history. For a list of record types and descriptions, see the Master Records section in the help file.

If your institution uses field-level security for employees and CIM GOLD profiles, use the following instructions for setup and changes.

For details on how to use any of the fields on this tab, click in the field and press <F1>.

### Setting Up Field-level Security

**To set up or change field-level security for employees and profiles, complete the following steps.**

1. Select **Employees** or **CIM GOLD Profiles** on the left side of the screen.
2. Select the appropriate employee or profile from the list.
3. Click on the Field Level tab.
4. Select the **Record Type** from the drop-down list; all fields in the selected record will be shown.
5. Click on the **Restrict** box next to the field to restrict access and add it to the list of **Restricted Fields**.
6. Click <**Save Changes**> after restrictions are made for each Record Type.

If any fields need to be unrestricted, select them on the **Restricted Fields** list (use the <Ctrl> button on your keyboard to select multiple fields). Then click <**Clear Selected Restrictions**> and <**Save Changes**>.



Employees     Tellers  
 CIM GOLD Profiles     System Profiles  
 Display Effective Security  
 Search   
       

Number	Full Name
9201	FPS GOLD ONLY (PLATF...
9210	LINDA KEENEY
9220	MARILYN CRAWFORD
9301	LOGAN SMITH
9320	STEVE MCCREADY
9330	STEVE MCCREADY
9358	Dayna Kauo
9620	CHRISTOPHER VANBELL...
9730	JENNIFER VALENTINES
9920	Dayna K. Kauo
9930	AMY RASMUSSEN - EDIT...
9990	FPSGOLD(6)
9999	test teller

Employee | Teller | CIM GOLD | System | **Field Level**

**Restricted Fields**

Record	Field	Field Description
CSPI	PIENAM	EMPLOYEE NAME
CSPI	PIAWRD	AMOUNT KEYWORD
CSPI	PIPCMD	PREF CONTACT MET

**All Fields**

Record Type: CSPI - Customer Profile

Restrict	Field	Field Description
<input type="checkbox"/>	PIPYES	PROFILEYN ...
<input type="checkbox"/>	PIPAMT	PROFILE AMOUNT ...
<input type="checkbox"/>	PIPDAT	PROFILE DATE ...
<input checked="" type="checkbox"/>	PIPCMD	PREF CONTACT MET...
<input checked="" type="checkbox"/>	PIENAM	EMPLOYEE NAME ...
<input type="checkbox"/>	PILSDT	LAST SAVED DATE ...
<input type="checkbox"/>	PIDBDT	DEPENDANT BIRTHD...
<input type="checkbox"/>	PILIDN	LINK TO ID NUMBER ...
<input type="checkbox"/>	PILIDT	LINK ID NUMBER TY...
<input type="checkbox"/>	PILIDA	LINK ID NUMBR ACTI...
<input type="checkbox"/>	PIYWRD	YNKEYWORD ...
<input checked="" type="checkbox"/>	PIAWRD	AMOUNT KEYWORD ...
<input type="checkbox"/>	PIDWRD	DATE KEYWORD ...
<input type="checkbox"/>	PIEPCD	EXCLUDED PROD CO...



## Subscribe to Mini-Applications Screen

### Security > Subscribe to Mini-Applications

The Subscribe to Mini-Applications screen allows you to designate which applications and screens your institution will have access to in CIM GOLD. If a screen is not subscribed to, it will not be listed on the CIM GOLD Subscribe to Mini-Applications screen to give security access to. You must have proper security to access this screen.

The screens are listed in alphabetical order, which is the same way they appear in the CIM GOLD navigation tree. Please be aware that some applications and screens may have a billable fee for their use. You can see which screens are billable by clicking on a screen listed on the Subscribe to Mini-Applications screen; the price for using that screen will appear in the Cost per Month per User field at the bottom of the screen. The Description field will provide a short description of the application or screen selected.

Most screens can be unsubscribed to if you uncheck the box next to the screen. When unsubscribing to a screen, all security given to employees and CIM GOLD Profiles for that screen will be deleted. Use caution when unsubscribing to a screen; if a screen is unsubscribed to in error, all employees and CIM GOLD Profiles will need to be set up for security to the screen again. If a screen is required and cannot be unsubscribed to, you will get an error if you uncheck the box.

#### NOTE

Employees already signed on to the system can view a newly subscribed screen by deleting their cache. If they wait until the following day, they will be able to view the screen on their first sign on.

The list view displays all screens available to your institution. To subscribe to any screen, check the box next to it. The **Description** field gives a short description of the highlighted screen. The **Cost per Month per User** field shows the cost, if any, of the highlighted screen each month for each person using it.

After selecting all the screens you want to subscribe to, click <Save Changes>.

#### NOTE

Your institution must subscribe to a screen before that screen will appear in Security Setup or in the CIM GOLD navigation tree for any user. As new screens are added to the list, they are advertised in a release notification.

## Unsubscribing

To unsubscribe from a screen, remove the check in its box by clicking on it. If you unsubscribe to any screen, you will see a warning when you click <Save Changes>: "Warning! You are unsubscribing to at least one mini-application. This action will remove all security to these mini-applications for every person and every profile! Do you REALLY want to continue?" Click <Yes> to continue or <No> to cancel and return to the screen.

### See also:

[Security Setup System](#)



## Screens List View

This list view displays all screens available to your institution. To subscribe to any screen, check the box next to it. After selecting all the screens you want to subscribe to, click <Save Changes>.

## Description

This field gives a short description of the highlighted screen.

## Cost per Month per User

This field shows the cost, if any, of the highlighted screen each month for each person using it.





## Terminated Employee Deletion Screen

### Security > Terminated Employee Deletion

This screen is used to delete terminated employees and obsolete System Profiles and must be given very limited security. CIM GOLD profiles can be deleted on the Setup screen once they are inactive.

#### WARNING

All employee CIM GOLD screen access and employee details will be removed when an employee is deleted using this function. This is a final action and cannot be undone.

Only employees with "Terminated" status will be shown on this screen.

To delete terminated employees, complete the following steps.

1. Select one or more employees to delete. You can select several employees by holding down the <Ctrl> key.
2. After selecting all the employees you want to delete, click <Delete Terminated Employee>.
3. Verify deletion by clicking <Yes> on the Confirm Delete dialog.

If the employee is tied to profiles, the employee will be removed from the profile; the profile is not affected. If the employee is also a teller, the teller record and opers.dat information are also deleted.

Deleted employees will be shown on the Security > Reports > History screen.

#### See also:

[Security System](#)

## Display

Select **Employees** to delete terminated employees from the system. Select **System Profiles** to delete profiles that are not tied to any users. Only profiles that are orphaned will be shown in the list.

## Search

To find a username quickly in the list below, begin typing the name in this field.

## Selection List

This field displays a list of employees whose passwords you can change. To delete an employee, select a name in this list and click <Delete Terminated Employee>.

