Security Administrator 2.0

Overview

Security Administrator manages accounts, privilege sets, and passwords for your FileMaker Pro solutions by leveraging the built-in FileMaker features for scripted account management (create/delete accounts, enable/disable accounts, change or reset passwords).

Security Administrator comes into play when you are not using External Authentication (where the accounts and passwords are managed outside of FileMaker) and is extremely powerful in the following scenarios:

- You have a multi-file solution: With Security Administrator you no longer have to create or manage the same accounts in each individual file of the solution
- You develop a commercial solution but still want to give your end users the power to manage their own accounts and passwords
- You are an in-house or professional developer who usually works on offline copies of the solution and when features are finished you replace the live files with your copy. Security Administrator will let you very quickly implement the correct accounts and passwords in the new live files

You can work with files individually, in subsets (logical groups of files), and by entire solution sets. As is described in this manual, by logically grouping files into subsets of modules you can significantly cut down on the configuration labor and increase the accuracy of implementing and administering accounts.

Working with Security Administrator is very simple, yet powerful.

The Security Administrator workflow divides into two phases: the Setup Phase in which you organize files, accounts, and privilege sets; then, in the Administer Phase, you simply select the files and accounts and tell Security Administrator what you want to do.

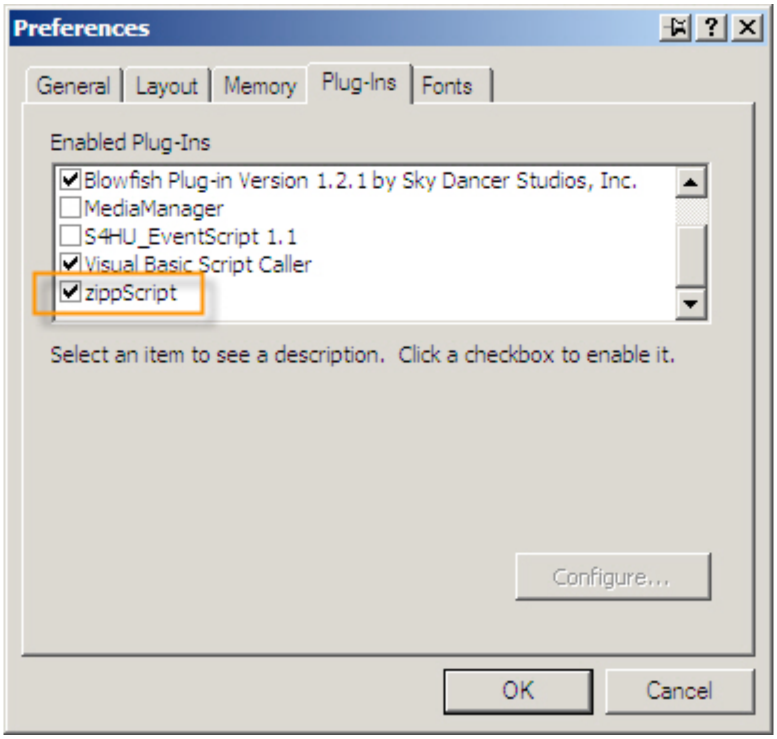
Before we describe the Security Administrator workflow, let's look at the general setup that is required to run Security Administrator.

You will need:

- FileMaker Pro 12.
- The free event script plugin ZippScript[1] that is included in the Security Administrator download. The plugin needs to be installed in the "Extensions" folder of your copy of FileMaker Pro and the plugin needs to be enabled in the FileMaker Preferences.

---

[1] - http://www.zipptools.com/
Security Administrator is tested with version 2.2 of this free plugin.



Enabled Plug-Ins

☑ Blowfish Plug-in Version 1.2.1 by Sky Dancer Studios, Inc.
☐ MediaManager
☐ S4HU_EventScript 1.1
☑ Visual Basic Script Caller
☑ zippScript

Select an item to see a description. Click a checkbox to enable it.

How to Use Security Administrator

Startup and Registration

Installing the ZippScript Plug-In

As already mentioned, the Security Administrator files come with the free ZippScript plug-in. Before launching Security Administrator for the first time, place the ZippScript plug-in into FileMaker Pro's "Extensions" folder. Restart FileMaker after installing the plug-in and make sure that ZippScript is active by going into the Application Preferences. Once you have confirmed that the ZippScript plug-in has been loaded and is active, then you can open Security Administrator.

Logging In

Security Administrator requires you to log in on launch in order to protect the sensitive data the file will hold.

You can log in under one of two account names:

user
user2

The default password for both user accounts is blank "".

Important: Change Passwords for File Security
We strongly recommend that you immediately change the password for both accounts. Doing so protects the Security Administrator file and all account data you've entered into it.

Registering Security Administrator

You can go to the Registration layout at any time by clicking the blue "Register" button at the upper left of the main matrix layout. Copy the entire User Name and Registration Key from your registration confirmation email, and paste it into the "Registration String" field, and click the gray "Register" button at the bottom.

Important: Registration String Changed for Security Administrator 2.0.0
Security Administrator 2.0.0 will not register with a registration string for previous versions of Security Administrator. You can purchase an upgrade from previous versions through the New Millennium website http://www.newmillennium.com.

Registration Troubleshooting

If you have pasted your registration string, clicked the gray “Register” button, and the response says “invalid” check these possibilities:

- Make sure you are no longer using the registration string for an older version. See the previous note about registration string change.
- The registration string is case sensitive. Make sure the registration string is exactly as it appears in your registration confirmation email.
- The registration string must have two “pipe character” dividers, regardless of platform. Make sure the pipe characters are both present and in the correct location.
- No hard returns should be present in your registration string. If you have copied the registration string from your confirmation email, you may need to remove any hard returns that have been formatted into your email by your email program.

Upgrade Import

If you are upgrading from an earlier version of Security Administrator, you can import all data from your previous copy of Security Administrator.

In the Admin Menu, click the “SA Upgrade Import” button. You will be asked to select the old copy of Security Administrator. Security Administrator will handle the rest.

Upgrade into an Empty Copy of Security Administrator

Security Administrator must have not account or privilege set data already entered before performing the upgrade import process. If you have entered any data before clicking the upgrade import button, Security Administrator will ask if you want to delete the current data or cancel the import.

Setup Phase

Files, Modules, and Solutions

Security Administrator allows you to either work on a file-by-file basis or, for more complex solutions, to organize your files into a hierarchy of files, modules, and solutions.

Modules are groups of files within a solution that share the same user accounts and privilege sets.

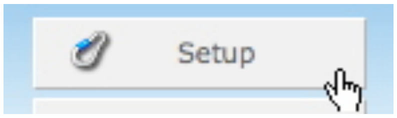
To further explain the distinction, let's suppose you have a solution divided into several different files for data and UI reasons:
Control
Contacts
ContactsUI
Products
ProductsUI
Invoices
InvoicesUI

All of those files together make up a single solution.

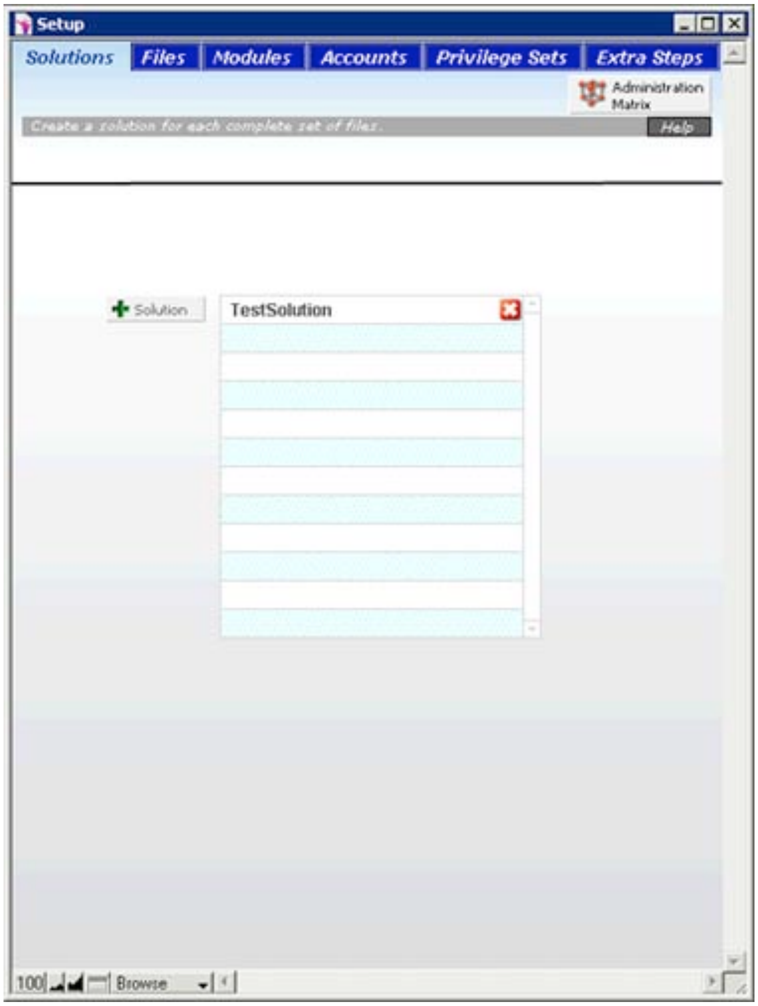
But, because different people have different access levels to specific files, your files may be further organized into subgroups or modules, each with different accounts and privilege sets.

In our example, the Control file might be a stand-alone file with limited accounts and privilege sets. But we might group Contacts and ContactsUI into a "Contacts Module" with user accounts and privileges that are different from the "Products Module" and "Invoices Module". Another possibility is that we've grouped the three UI files into a "UI Module" and the remaining files into a "Data Module."

The Setup Window



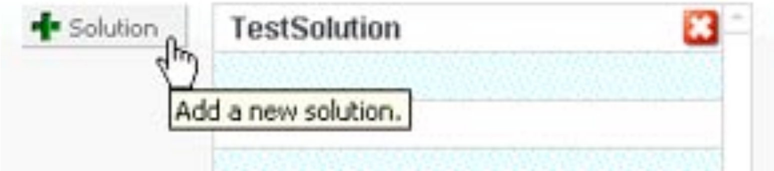
The initial setup phase is defined in the Setup Window.



Create a solution for each complete set of files.

1. Define the Solution

Click the “Solutions” tab in the Setup window.



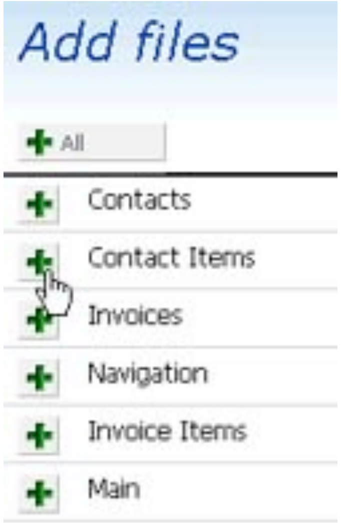
- Click the **‘+Solution’** button to create a solution record for each complete set of files you will manage with Security Administrator.

2. Add Files

Click the “Files” tab in the Setup window.

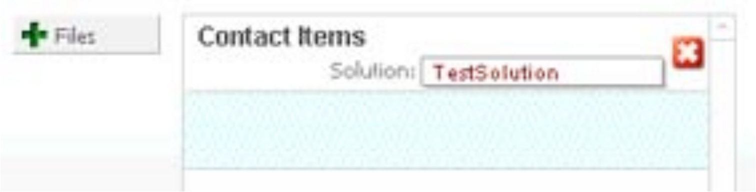
- Launch all FileMaker Pro files you want to manage, then bring Security Administrator to the front. In addition to the files being open, you should also make sure they are not “Open Hidden”.

- Click the **‘+Files’** button



- In the open file list, select each file you want to manage individually. If you want to manage all open files individually, click **'+All'**

Note: Only add the files you want to manage individually. Files that will be grouped into modules will be added in the following step.



Contact Items

Solution: TestSolution

- Assign each added file to a solution.

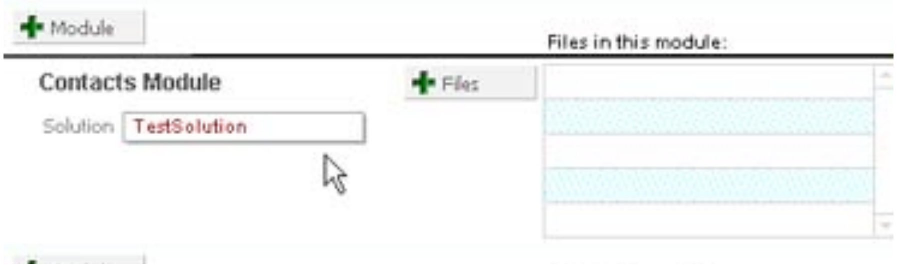
3. Organize Files into Modules (optional)

Click the “Modules” tab in the Setup window.

If you have sets of files that share the same user accounts and privilege sets, you may want to group them into modules. Doing so will allow you to easily select a privilege set for an account that is then applied to all files in the module. This is a huge time-saver and avoids configuration mistakes that could lead to an account being assigned a wrong privilege set in a file.

Creating a Module

- Click the "**+Module**" button, and name the new module group. This creates a listing that looks essentially like another file.

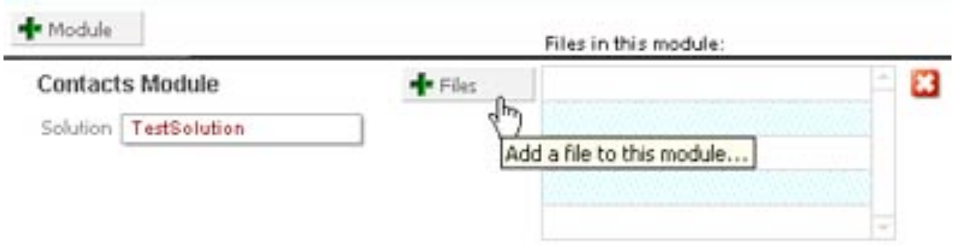


Contacts Module

Solution TestSolution

- In the new module, select the solution your module belongs to.

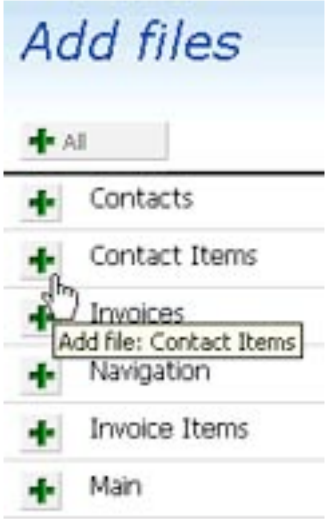
Grouping Files



Contacts Module

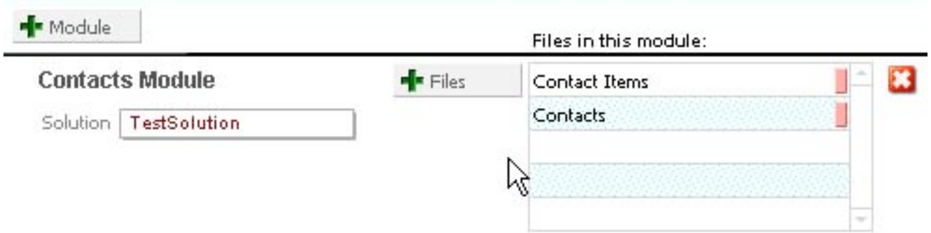
Solution TestSolution

- Click '**+Files**' in the new module record.



- Select each file you want add to the module group. To add all open files, click the '**+All**' button at the top of the file list.

Note: If a file does not appear in the selection list, it may not be currently open, is already listed as a single file, or it has been added to another module. To add it to your new module, you must first exit the open files list and remove the file from the module or file list it currently appears in.



Contacts Module

Solution TestSolution

Contact Items

Contacts

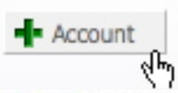
4. Define Accounts

Click the “Accounts” tab in the Setup window.

Creating Accounts

Security Administrator allows you to define accounts in one of three ways:

- **Manually**: Click the '**+Account**' button. In the blank account row and enter the account name.

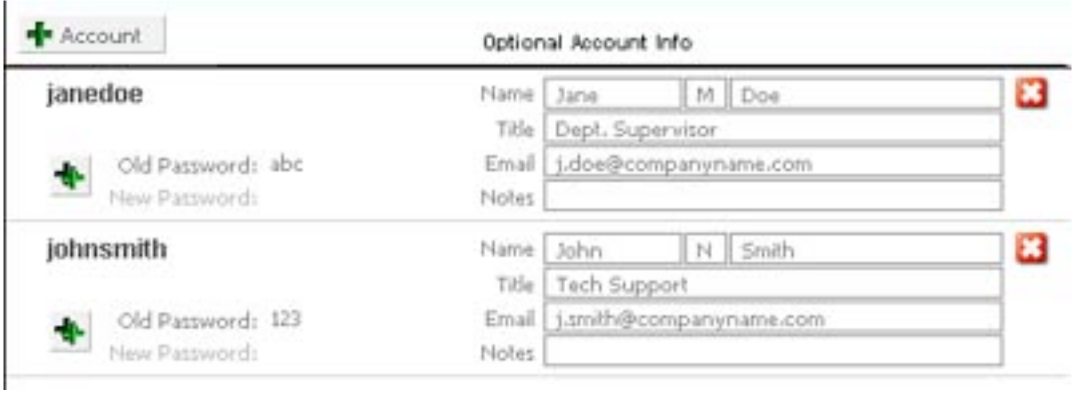


- **Import Accounts**: Click '**Import Accounts**' to import a list of accounts from a text file or spreadsheet.

- **Import From DDR**: Click '**Import From DDR’** to import accounts and privilege sets from a FileMaker Database Design Report saved in XML format.

Passwords

You should also enter the current password for each account.



janedoe

Old Password: abc
New Password:

Name: Jane | M | Doe
Title: Dept. Supervisor
Email: j.doe@companyname.com
Notes:

johnsmith

Old Password: 123
New Password:

Name: John | N | Smith
Title: Tech Support
Email: j.smith@companyname.com
Notes:

Title

An optional field to enter the account holder’s job title. This may be a useful reference when assigning privilege sets to each account.

Email

Although not required, it is a good idea to also enter an email address for each account. Security Administrator can also send an email notifying account holders of changes to their password. (See the documentation for emailing passwords under the Administer Phase section.)

Notes

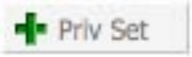
A notes field is provided for each account. In the Email Password function (see the Administer Phase section) you can optionally include account notes in the outgoing email.

5. Define Privilege Sets

Creating Privilege Sets

As with accounts, you can define privilege sets in one of two ways:

- **Manually**: Click the '**+Priv Set**' button to create a new privilege set.



- **Import Priv Sets**: Click '**Import Priv Sets**' to import a list of privilege sets from a text file or spreadsheet.

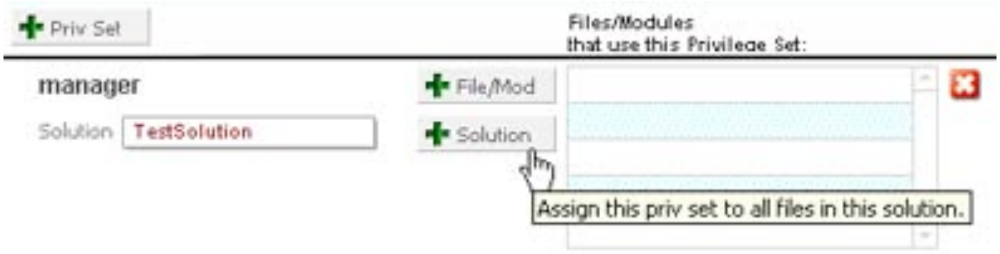
- **Import From DDR**: Click '**Import From DDR'** to import accounts and privilege sets from a FileMaker Database Design Report saved in XML format.

Note: No "[Full Access]" Privilege Sets
Security Administrator is not designed to create full access accounts in Genesis files. Accounts can only be set to full access privileges manually. Security Administrator can, however, work with user defined privilege sets that have high access privileges, just not the pre-defined "[Full Access]" privilege set. To avoid confusion on this issue, Security Administrator prevents you from creating a privilege set record named "[Full Access]." (There is, however, a Full Access checkbox to help you identify which accounts must be manually set to "[Full Access]." For more information, see the Administer Phase notes.)

Assigning Privilege Sets

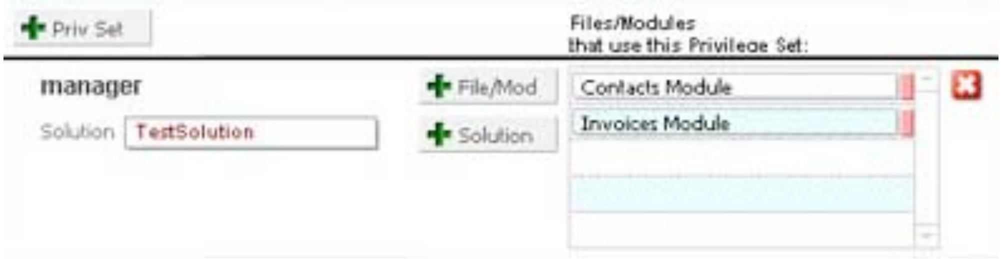
- Click '**+File/Mod**' to assign the privilege set to a specific file or module.

- Or, to assign the privilege set to an entire solution set, select the solution in the popup menu, then click '**+Solution**'.


Priv Set
Files/Modules that use this Privilege Set:
File/Mod
Solution
Assign this priv set to all files in this solution.

manager

Solution: TestSolution



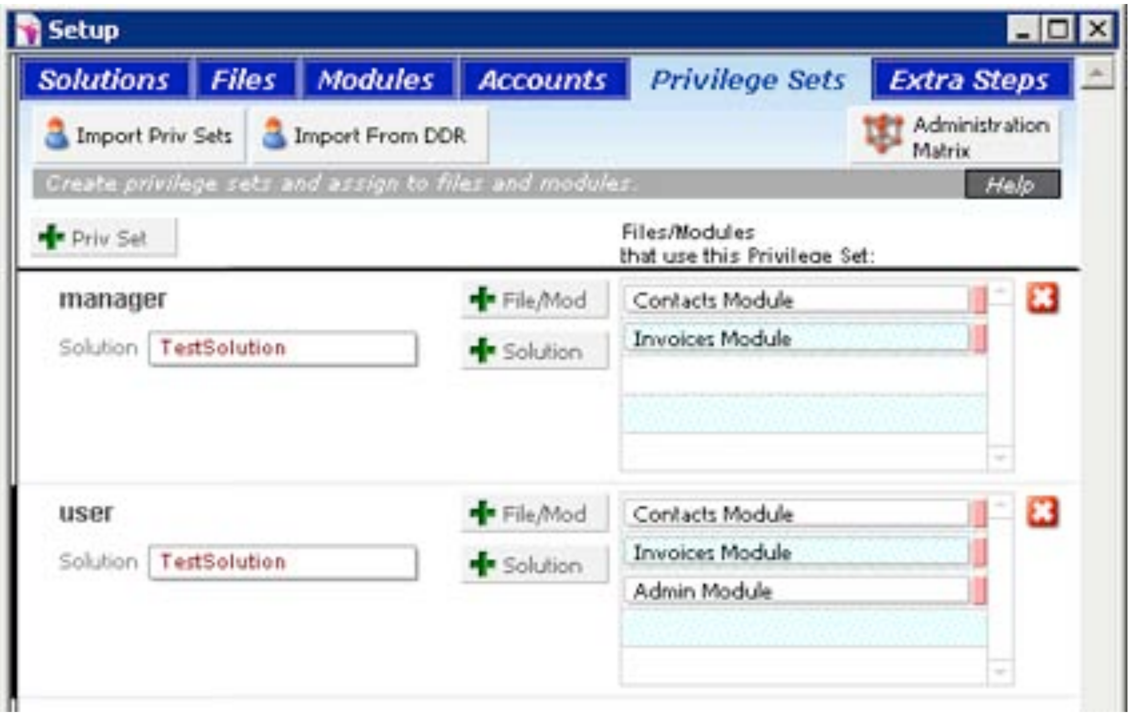
manager

Solution: TestSolution

Contacts Module

Invoices Module

The choices you make in this "Privilege Set" setup window dictate what privilege sets will be displayed in the value list on the main interface for an given account/file (or module). For instance this configuration:



manager

Solution: TestSolution

Contacts Module

Invoices Module

user

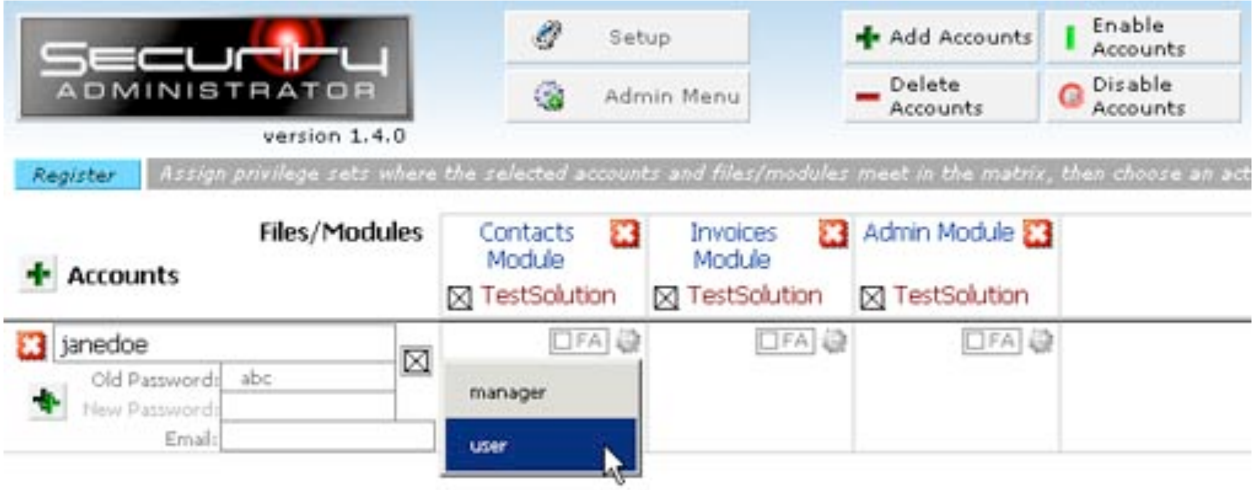
Solution: TestSolution

Contacts Module

Invoices Module

Admin Module

Results in Privilege Sets “user” and “manager” to be available choices for the files in “Contacts Module”:



Assign privilege sets where the selected accounts and files/modules meet in the matrix, then choose an act

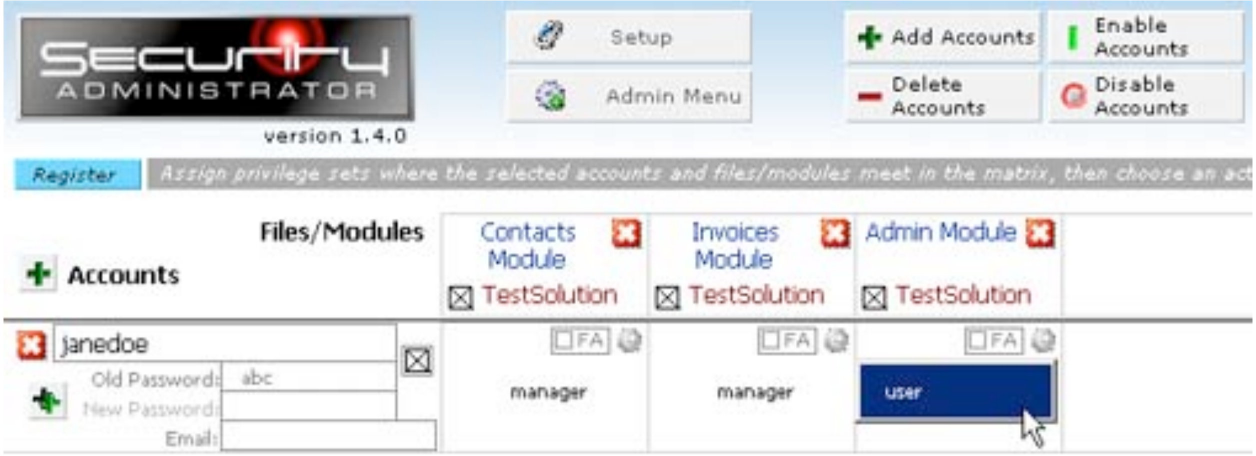
janedoe

Old Password: abc

New Password:

Email:

But only Privilege Set “user” is available for the “Admin Module” files:



Assign privilege sets where the selected accounts and files/modules meet in the matrix, then choose an act

janedoe

Old Password: abc

New Password:

Email:

6. Extra Steps

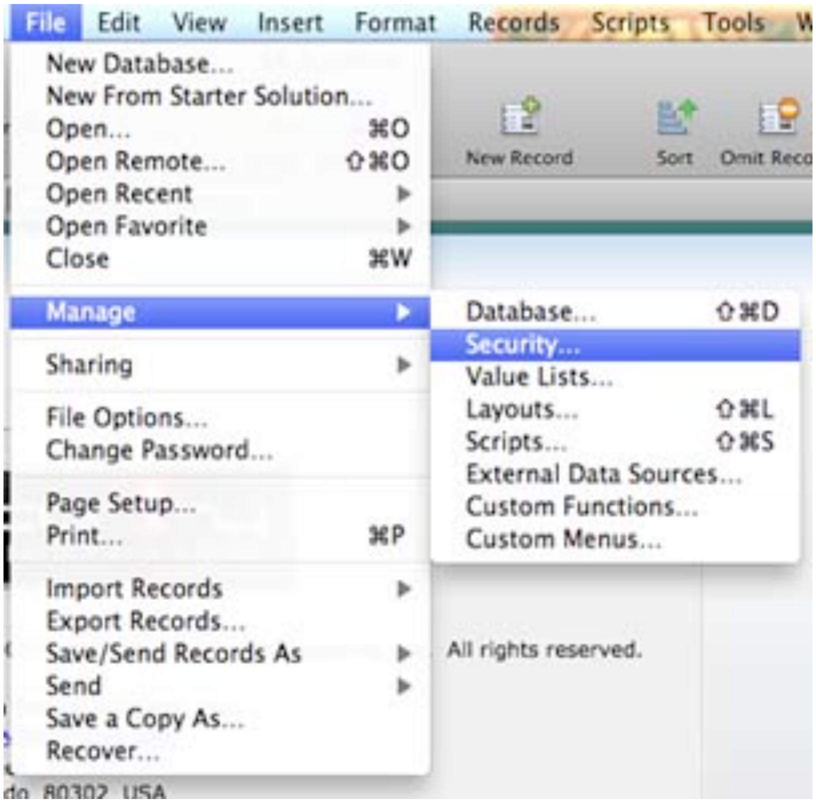
Because FileMaker’s privilege sets store the fundamental security data, FileMaker carefully controls them. As a result, privilege sets require a few extra steps for Security Administrator to work with them properly.   This setup work for privilege sets only needs to be done once, however.

6.1 Create Privilege Sets in SA_ScriptFile

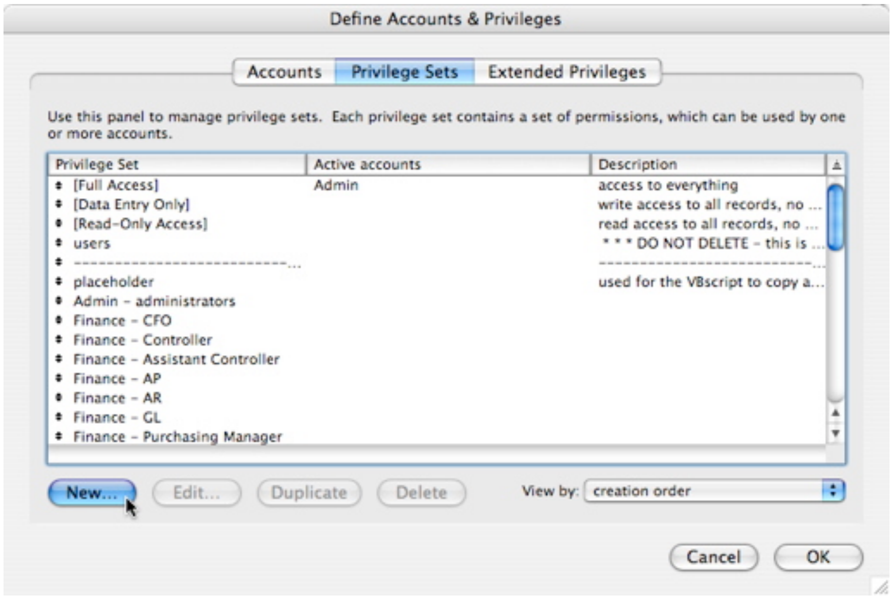
SA_ScriptFile.fmp12

In order to correctly modify the "Security Administrator" script in the next step, **you must first create all necessary privilege sets within SA_ScriptFile.fmp12**

- In SA_ScriptFile.fmp12, select File > Define > Accounts & Privileges…



- Under the Privilege Sets tab, click the “New” button and create a new privilege set for each of the privilege sets to be managed by Security Administrator. Make sure to name them correctly!

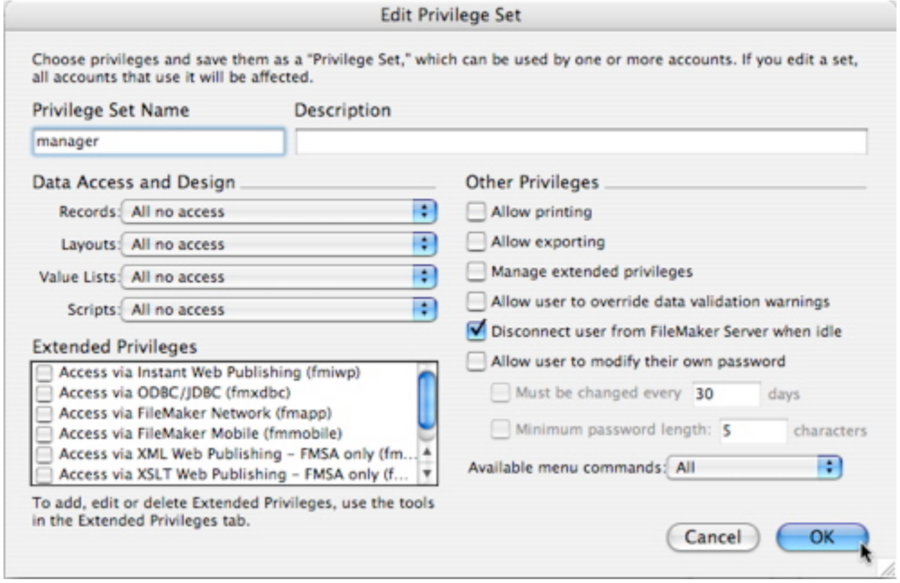


Use this panel to manage privilege sets. Each privilege set contains a set of permissions, which can be used by one or more accounts.

Privilege Set	Active accounts	Description
[Full Access]	Admin	access to everything
[Data Entry Only]		write access to all records, no ...
[Read-Only Access]		read access to all records, no ...
users		* * * DO NOT DELETE - this is ...
-------------------------...		-------------------------...
placeholder		used for the VBscript to copy a...
Admin - administrators		
Finance - CFO		
Finance - Controller		
Finance - Assistant Controller		
Finance - AP		
Finance - AR		
Finance - GL		
Finance - Purchasing Manager		

View by: creation order

+ You do not need to change the default settings for data access or other privileges. The privileges options can be left unselected, with “all no access.”



Choose privileges and save them as a "Privilege Set," which can be used by one or more accounts. If you edit a set, all accounts that use it will be affected.

Privilege Set Name: manager

Description:

Data Access and Design

Records: All no access

Layouts: All no access

Value Lists: All no access

Scripts: All no access

Extended Privileges

☐ Access via Instant Web Publishing (fmiwp)
☐ Access via ODBC/JDBC (fmxdbc)
☐ Access via FileMaker Network (fmapp)
☐ Access via FileMaker Mobile (fmmobile)
☐ Access via XML Web Publishing – FMSA only (fm…
☐ Access via XSLT Web Publishing – FMSA only (f…

To add, edit or delete Extended Privileges, use the tools in the Extended Privileges tab.

Other Privileges

☐ Allow printing
☐ Allow exporting
☐ Manage extended privileges
☐ Allow user to override data validation warnings
☑ Disconnect user from FileMaker Server when idle
☐ Allow user to modify their own password
  ☐ Must be changed every 30 days
  ☐ Minimum password length: 5 characters

Available menu commands: All

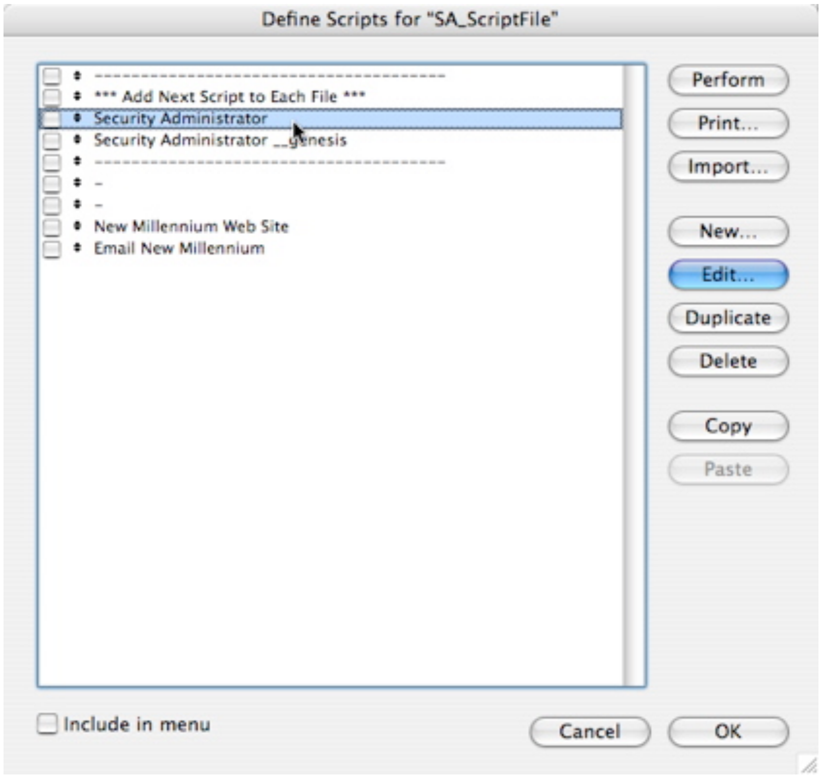
Create all of your managed privilege sets in SA_ScriptFile.fmp12.

6.2 Add Privilege Sets to the "Security Administrator" Script

After you have defined the privilege sets, incorporate them into the "Security Administrator" script.

- In SA_ScriptFile.fmp12, select Scripts > ScriptMaker

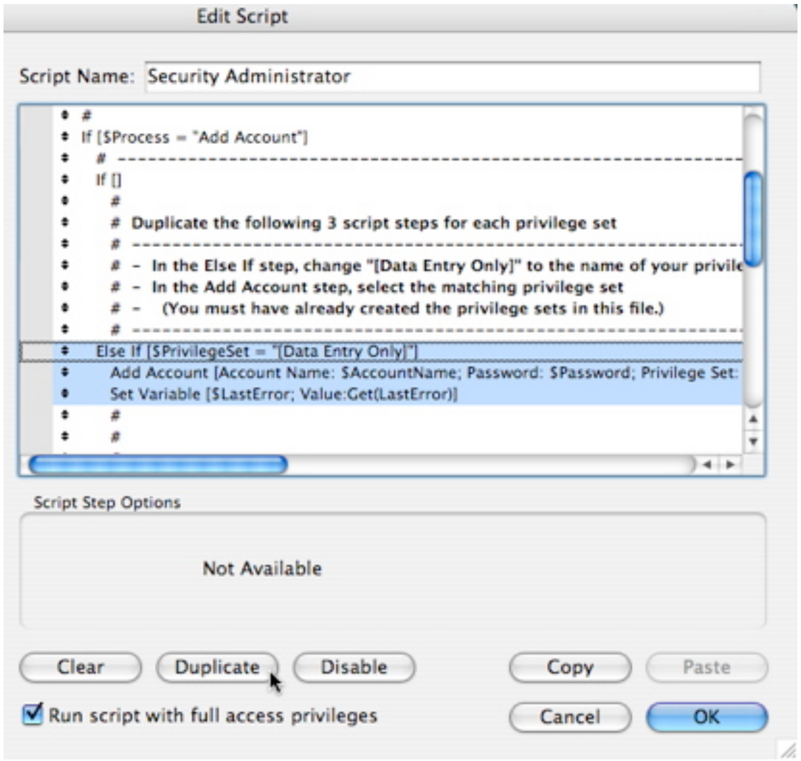
- Edit the “Security Administrator" script.



☐ ------------------------------------
☐ *** Add Next Script to Each File ***
☐ Security Administrator
☐ Security Administrator __genesis
☐ ------------------------------------
☐ -
☐ -
☐ New Millennium Web Site
☐ Email New Millennium

☐ Include in menu

- Near the beginning of the script, duplicate and modify the Else If steps to incorporate the new privilege sets:

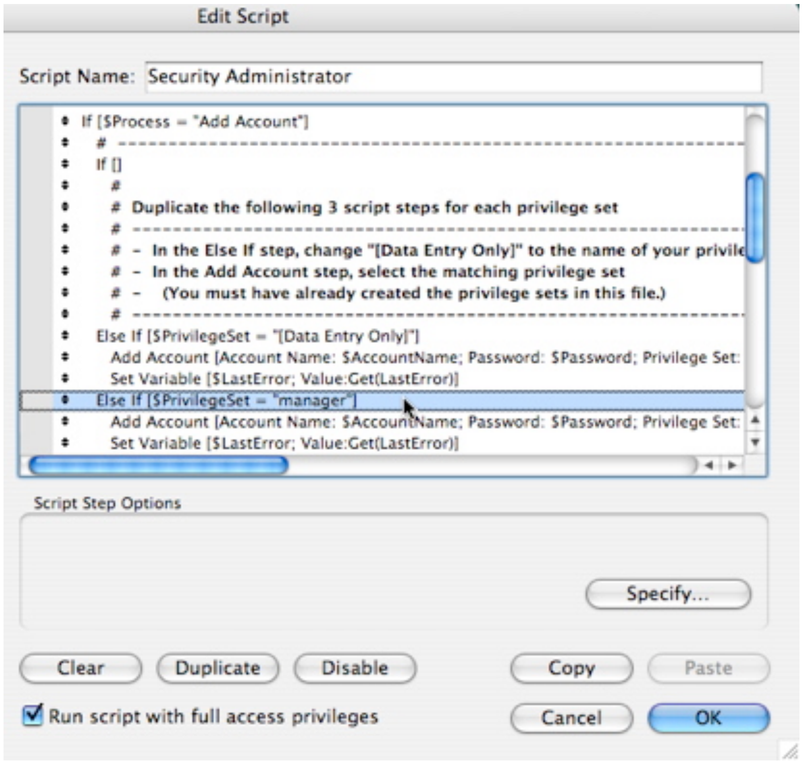


Script Name: Security Administrator

```
#
If [$Process = "Add Account"]
  # ------------------------------------------------------------------
  If []
    #
    #  Duplicate the following 3 script steps for each privilege set
    # ----------------------------------------------------------------
    # –  In the Else If step, change "[Data Entry Only]" to the name of your privile
    # –  In the Add Account step, select the matching privilege set
    # –    (You must have already created the privilege sets in this file.)
    # ----------------------------------------------------------------
  Else If [$PrivilegeSet = "[Data Entry Only]"]
    Add Account [Account Name: $AccountName; Password: $Password; Privilege Set:
    Set Variable [$LastError; Value:Get(LastError)]
    #
    #
```

☑ Run script with full access privileges

- Change the Else If step itself to incorporate the correct privilege set name.



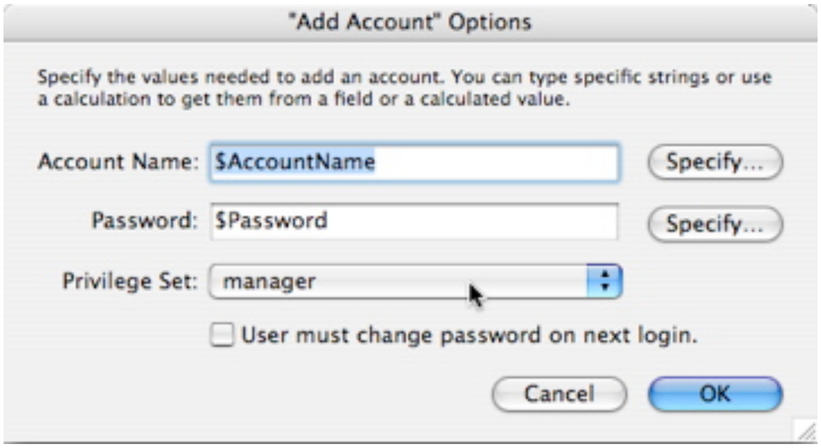
Script Name: Security Administrator

```
If [$Process = "Add Account"]
  # ------------------------------------------------------------------
  If []
    #
    #  Duplicate the following 3 script steps for each privilege set
    # ----------------------------------------------------------------
    # –  In the Else If step, change "[Data Entry Only]" to the name of your privile
    # –  In the Add Account step, select the matching privilege set
    # –    (You must have already created the privilege sets in this file.)
    # ----------------------------------------------------------------
  Else If [$PrivilegeSet = "[Data Entry Only]"]
    Add Account [Account Name: $AccountName; Password: $Password; Privilege Set:
    Set Variable [$LastError; Value:Get(LastError)]
  Else If [$PrivilegeSet = "manager"]
    Add Account [Account Name: $AccountName; Password: $Password; Privilege Set:
    Set Variable [$LastError; Value:Get(LastError)]
```

☑ Run script with full access privileges

+ And in the Add Account step, select the correct privilege set in the popup menu.

Note: The privilege set will only appear in the popup menu after you have created it in SA_ScriptFile.fmp12. (See step 6.1)



"Add Account" Options

Specify the values needed to add an account. You can type specific strings or use a calculation to get them from a field or a calculated value.

Account Name: $AccountName

Password: $Password

Privilege Set: manager

☐ User must change password on next login.

Repeat this process of duplicating the set of three script steps for each manage privilege set.

6.3 Copy the "Security Administrator" Script to Target Files

Now that the “Security Administrator” script has been updated for all of your privilege sets:

- Copy (or import) the modified "Security Administrator" script into every managed file.

***Important**: You **must** copy the updated “Security Administrator” script into all of your target files. Security Administrator will need to call this script in your files in order to correctly modify accounts and privilege sets.*

Setup Phase Conclusion

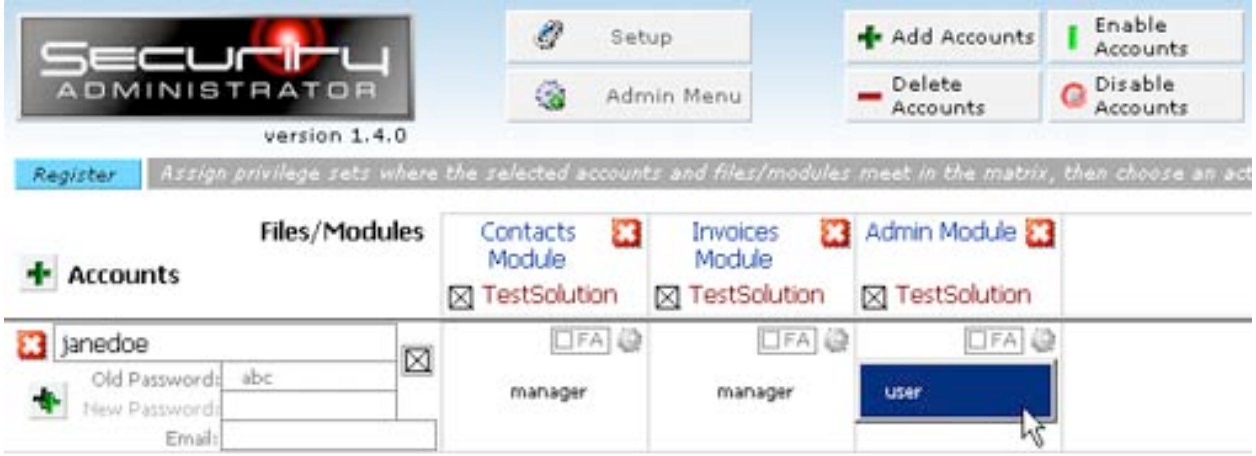
Once you’ve completed these steps, Security Administrator and your solution files are now fully configured and ready to be managed. You will not need to run through the Setup Phase again for these files, accounts, and privilege sets.

You can always add more elements for Security Administrator to manage, however.

Administer Phase

Now that the setup is complete, Security Administrator is ready to organize and update your accounts and privilege sets within your files.

Everything at this stage is managed in the security matrix layout.



Assign privilege sets where the selected accounts and files/modules meet in the matrix, then choose an act

janedoe ☒

Old Password: abc

New Password:

Email:

	Contacts Module ☒ TestSolution	Invoices Module ☒ TestSolution	Admin Module ☒ TestSolution
janedoe	manager	manager	user

1. Select Files and Accounts

- Select the files and accounts you want to work with:

  - Across the top, mark the checkboxes of the files and modules to work with. (Remember, modules are groups of files you've defined in the setup phase.)

  - Down the left, mark the checkboxes of the accounts to use.

  You can select all files / all accounts by holding down the shift key when selecting one.

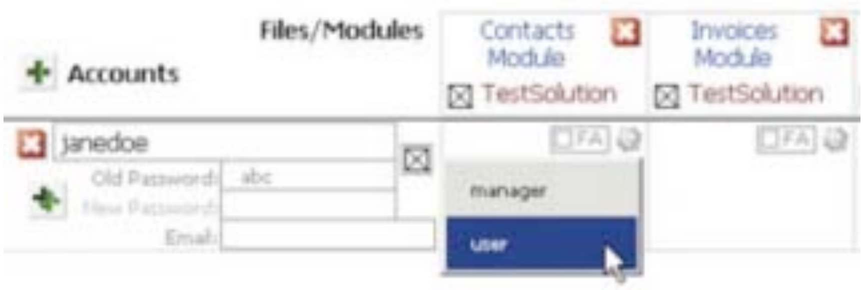
  Remember that the files you want to work with are open, and not hidden.
  A future version of the Security Administrator will include a VBscript (for Windows) and AppleScript (for OSX) to unhide hidden files.

  If you select only a subsection of files/modules from a solution, and the user's privilege set allows them to change their password, remember that this may lead to the user having different passwords in different parts of the solution. Security Administrator can not retrieve the user's current password.

2. Assign Privilege Sets

In the setup phase we listed all possible privilege sets and associated them with files and module sets. Now we need to assign a specific privilege set to each account for each file or module.

- Select the correct privilege set for each user account in each file where the account row intersects with the file/module column.



janedoe

Old Password: abc

New Password:

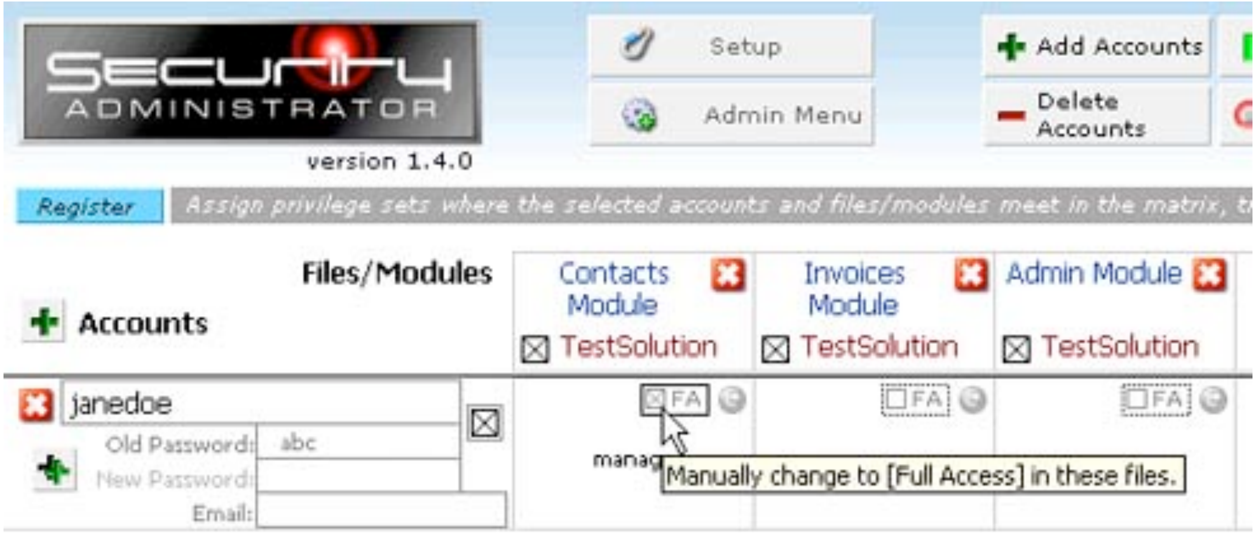
Email:

Note: You are only allowed to select from the possible privilege sets assigned to that file. If you don't see the desired privilege set, make sure it has been created in the Privilege Sets tab of the Setup window and assigned to the correct file.

Full Access ("FA") Checkboxes

As stated in the Setup Phase notes previously, Security Administrator does not create full access accounts in target files. Accounts can only be set to full access privileges manually. Many administrators will still want to use Security Administrator to manage full access accounts. To accommodate this need, each cell within the Security Administrator matrix has a full access ("FA") checkbox.

How to use the Full Access checkboxes:



Assign privilege sets where the selected accounts and files/modules meet in the matrix, t

janedoe

Old Password: abc

New Password:

Email:

Manually change to [Full Access] in these files.

- First, for all full access accounts, select another high-level privilege set from among those you've defined in Security Administrator. Which privilege set you select is not important since you will later change this manually.

- Mark the FA checkbox in all appropriate matrix cells.

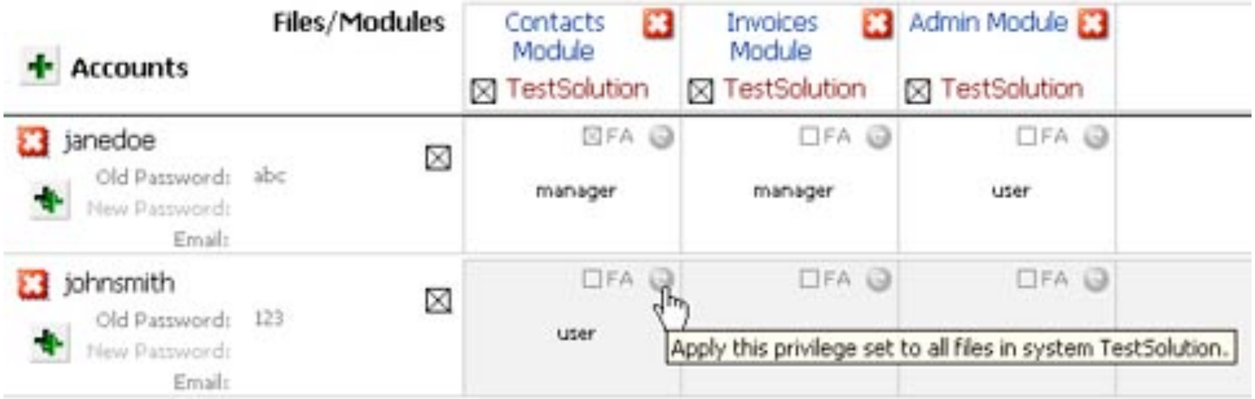
- Once your setup is ready, click Security Administrator's "Add Accounts" button.

- When the Add Accounts process is complete, Security Administrator will give you a reminder to manually update the full access accounts in your target files.

- In each affected target file, go to File > Manage > Security… and reset the full access accounts to the "[Full Access]" privilege set. Use the checkboxes in the Security Administrator matrix as a guideline.

Button: Apply Privilege Set Across to All Files

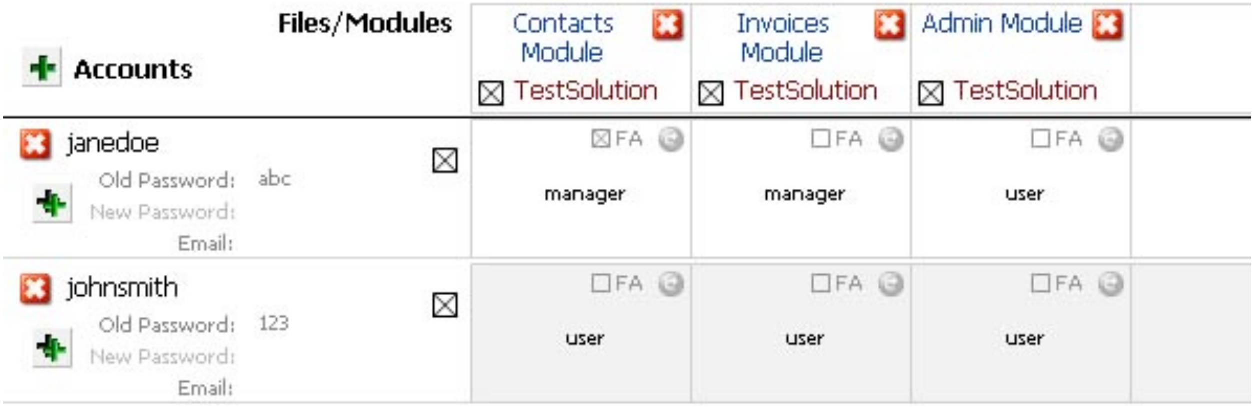
Often, the same account will use the same privilege set in all files. To make this easier to set up, all you need to do is select the correct privilege set in one cell, and then click the round gray button in the upper right of the cell:



Accounts	Files/Modules	Contacts Module ☒ TestSolution	Invoices Module ☒ TestSolution	Admin Module ☒ TestSolution
janedoe Old Password: abc New Password: Email:	☒	☒FA manager	☐FA manager	☐FA user
johnsmith Old Password: 123 New Password: Email:	☒	☐FA user	☐FA	☐FA

Apply this privilege set to all files in system TestSolution.

The same privilege set will be copied across to all files and modules for the same account:

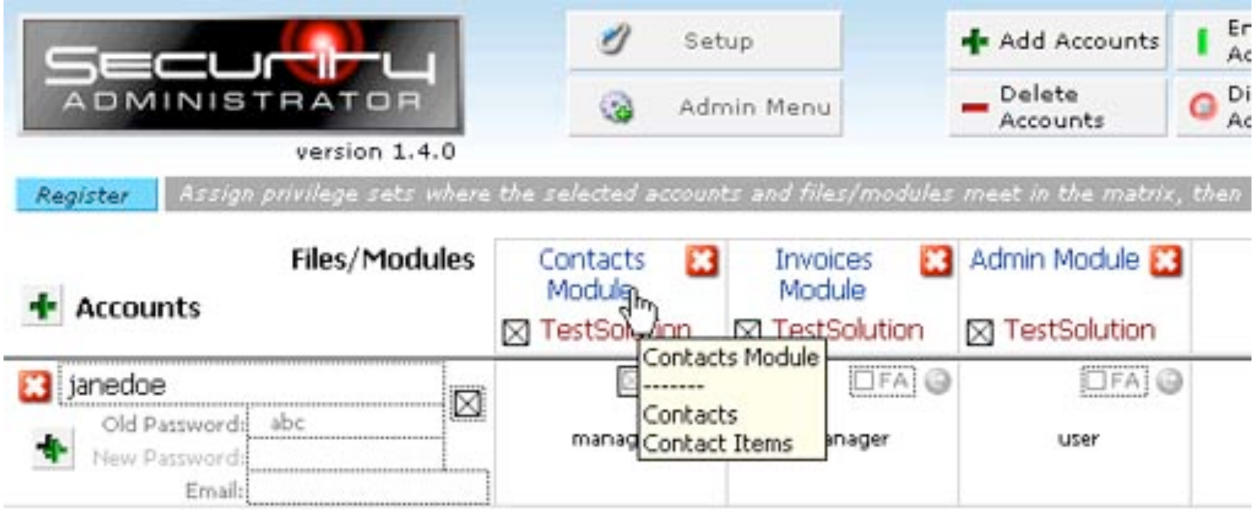


Accounts	Files/Modules	Contacts Module ☒ TestSolution	Invoices Module ☒ TestSolution	Admin Module ☒ TestSolution
janedoe Old Password: abc New Password: Email:	☒	☒FA manager	☐FA manager	☐FA user
johnsmith Old Password: 123 New Password: Email:	☒	☐FA user	☐FA user	☐FA user

Note: If the originally selected privilege set is not available for some of the files or modules, those columns will remain unaffected.

Module File List in Header Tooltip

Whenever you need a reminder of all files grouped within a module, just let your mouse pointer hover over the module's column header label. A tooltip will appear with a list of all files in that module.



Assign privilege sets where the selected accounts and files/modules meet in the matrix, then

janedoe

Old Password: abc

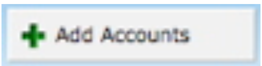
New Password:

Email:

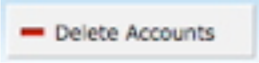
3. Let Security Administrator Do the Work

Once you have selected the files/modules and accounts to work with and assigned the Privilege Sets, then all you have to do is click the button for the Security Administrator function.

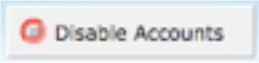
Account Functions



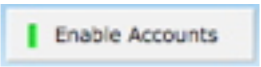
Add Accounts
Adds the selected accounts to the checked files/modules, using the assigned privilege sets.



Delete Accounts
Completely removes the marked accounts from the selected files/modules. (Once deleted the only way to add accounts back is to manually recreate them or add them back with the Add Accounts function.)

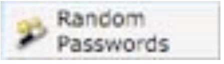


Disable Accounts
Disables the specified accounts from the selected files/modules, but does not actually remove the accounts. (Disabled accounts can be re-enabled either manually or by calling Security Administrator's Enable Accounts function.)



Enable Accounts
Re-enables the selected accounts, assuming they have been disabled.

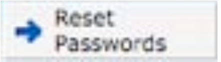
Password Functions



Random Passwords
Generates random passwords for all selected accounts.

After clicking the Random Password button, a dialog will ask you to enter the length of the password. For example, entering the numeral "7" will produce a random password seven characters in length.

A random password is entered into the "New Password" field for each marked account in the matrix layout. At this stage, the old "Password" field is not changed.



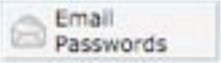
Reset Passwords
Resets the account passwords for the selected accounts in the specified files/modules.

Once you click the Reset Password button, Security Administrator will go through all selected files/modules and attempt to reset the password for the selected accounts. Once completed, the value in the account's "New Password" field is moved to the "Password" field.

Change Password and Reset Password
When the target file is open with full access privileges, Security Administrator will reset the specified account's password. If the target file is not open under full access, Security Administer can only change the password for the target file's active account after first verifying that the old "Password" value is correct. If Security Administrator cannot reset or change the password, the problem will be noted in the Log.

Setting Passwords to Expire
When running in FileMaker Pro 9, Security Administrator asks if you would like to set the new password to expire on the user's next login. This forces users to immediately change their new password. This is helpful when issuing random passwords that are not intended as permanent passwords. Passwords set to expire are noted in the matrix account record with a gray "Exp." (This functionality is only available in FileMaker Pro 9.)

Important: Only set to expire for accounts with privilege sets that allow users to change their passwords. Otherwise, users will get caught on next login.



Email Passwords
Sends an email to the account holder for each selected account, with a note about changes to the account password. This is especially useful when updating or randomizing passwords.

Once you click the Email Passwords button, you are taken to a layout that allows you to customize the email that will be sent out. The email generated will automatically include a note with the account name and new password. You can further modify the email Subject, Message, and Closing. You can also mark a checkbox if you want to include the contents of the Notes field for each account, as well.

Caution: Because the emails generated will contain account name and password, be certain that the email addresses are correct and up-to-date.

Note: *What about changing the privilege set for an existing account?*

FileMaker Pro does not allow the scripted change of a privilege set so the way to do this is to delete the accounts using Security Administrator, choosing a new privilege set for the account in Security Administrator and then letting the tool add the accounts again.

This approach has one down-side though: the user will get the password that is configured in Security Administrator which may or may not be the password they had before the change. For obvious security reasons there is no method for retrieving the current password for an account in FileMaker. So after removing and adding the accounts again the user will have the password as set in Security Administrator. If the privilege set in FileMaker allows for it, the user can then change their password.

Note: *Renaming the Security Administrator tool*

You can safely rename the Security Administrator tool. Doing so will not break its functionality. This allows you to keep different version throughout time or different version for different systems and/or different clients.

Appendix: Importing

Security Administrator offers several ways to import account and privilege set data. All import options are available in the Administration Menu, as well as in the appropriate Setup window tabs.

Upgrade Import

If you are upgrading from an earlier version of Security Administrator, you can import all data from your previous copy of Security Administrator.

In the Admin Menu, click the “SA Upgrade Import” button. You will be asked to select the old copy of Security Administrator. Security Administrator will handle the rest.

Upgrade into an Empty Copy of Security Administrator

Security Administrator must have not account or privilege set data already entered before performing the upgrade import process. If you have entered any data before clicking the upgrade import button, Security Administrator will ask if you want to delete the current data or cancel the import.

Import from Database Design Report

A quick way to gather account and privilege set data from your solution files and enter it into Security Administrator is by generating a Database Design Report.

Open your file in FileMaker Pro Advanced and, under the Tools menu, select Database Design Report. Make sure all account and privilege set checkboxes are marked. To conserve on the resulting DDR file’s size, you may want to uncheck unnecessary elements like field, layout, and script data. The DDR must be generated in XML format (not the default HTML format).

In the Admin menu, click the “Import From DDR” button. You will be asked to select the DDR file. (The file you select will have a name similar to the original FMP file, but with “.xml” as the extension. Do not select the “Summary” file.) Security Administrator will import the accounts and privilege sets, and correctly match them up in the matrix layout.

Import Accounts

In the Admin menu or Setup Accounts tab, click the “Import Accounts” button if you have a list of account names (with no other data) stored in a text file or spreadsheet that you want to import.

Import Privilege Sets

In the Admin menu or Setup Privilege Sets tab, click the “Import Privilege Sets” button if you have a list of privilege set names (with no other data) stored in a text file or spreadsheet that you want to import.

New Millennium
COMMUNICATIONS

New Millennium Communications is a software development company located in Boulder, Colorado. We specialize in making tools and advanced templates for FileMaker Pro developers.

New Millennium Communications
1332 Pearl Street
Boulder, CO 80302 USA
303-444-1476

www.newmillennium.com plug-ins@nmci.com