

Setting up Security in User Access Mode

Summary: This article is a step by step guide for Shortcuts users who wish to setup security on their system in User Access Mode. User Access Mode is when Users are required to log on using a PIN (Personal Identification Number) each time they want to use the program. Shortcuts will recognise the User's Security Level and will allow them to only enter screens and perform actions according to the Accesses defined in their Security Level.

Article Applies to: Shortcuts V7

Related Articles: Security Overview & Definitions
Setting up Security in Instance Access Mode

Step 1: Check the Default Security Level Setup

- 1) From the Navigation bar select the **Setup Menu** and then select the **Configuration** icon. From the Configuration bar select the **General Setup Menu** and then select the **Security** Icon. The Security Setup Window will appear.
- 2) Shortcuts' default security settings will display 3 Security Levels; Owner, Manager and Employee with common Access privileges already defined. These Security Levels have been set up as a **guide only** and should be reviewed and changed according to the needs of your business. See over the page for instructions on how to add, delete or modify a Security Level.

The screenshot shows the 'Security Setup' window. On the left is a navigation bar with icons for Sales Setup, General Setup, Security, Business, General, Stock, Clients, Walkin, Confirmation, Internet, and Region Setup. The main area is titled 'Security Setup' and contains a table of Security Levels. The table has columns for 'Levels' and 'Override'. The levels listed are Owner, Manager, Employee, Receptionist, and Stock Controller, with checkboxes in the 'Override' column. There is also an '<Unassigned>' level. To the right of the table are 'New' and 'Delete' buttons. At the bottom of the window, there are checkboxes for 'Double PIN Verification to delete Transactions', 'Require Return or Done when entering PIN's', 'Security Enabled', and 'Support Verification Devices'. A 'Done' button is located in the bottom right corner.

Levels	Override
Security Levels	
Owner	<input checked="" type="checkbox"/>
Manager	<input checked="" type="checkbox"/>
Employee	<input type="checkbox"/>
Receptionist	<input type="checkbox"/>
Stock Controller	<input type="checkbox"/>
<Unassigned>	

Editing Security Level Names

1. Click to select the **Security Level** you want to change (e.g. Employee), and then click again to edit the selected Security Level name. The field will change colour and the text will be highlighted.
2. Using the keyboard, **type in a name** for the new Security Level (e.g. Supervisor).
3. Place a tick in the **Override** tick box if you want the Users within this Security Level to be able to access their defined areas regardless of the Security Settings for Terminals. (The Owner and Manager have the Override tick box ticked by default).*

****Note: Security for Terminals is explained in more detail in Step 3.***

Adding a New Security Level

1. Click to select the heading **Security Levels**.
2. Click the **New** button. A new field will appear in the list under Security Levels.
3. Using the keyboard, **type in a name** for the new Security Level (e.g. Receptionist).
4. Place a tick in the **Override** field if you want Users within this Security Level to be able to access their defined areas regardless of the Security Settings for Terminals.*

Note: When a new security level is added all accesses will be ticked by default. This security level will have access to all features and until otherwise specified.

Deleting a Security Level

1. Click to select the **Security Level** (e.g. Owner) you want to Delete from the list.
2. Click the **Delete** button. A message will appear asking you to confirm the request.
3. Click the **Yes** button to continue or the No button to cancel this request.

Note: You can only delete a security level if there are no users assigned to that level.

Step 2: Assign Users to Security Levels

By default Shortcuts will display all Users in the Unassigned Security Level. You must assign each User to their appropriate Security Level.

- 1) Select the **Levels Tab** so the Security Levels are displayed.

The screenshot shows the 'Security Setup' window with the 'Levels' tab selected. The table below shows the current state of security levels and user assignments.

Levels	Override
Security Levels	
Owner	<input checked="" type="checkbox"/>
Business	
Manager	<input type="checkbox"/>
Employee	<input type="checkbox"/>
Receptionist	<input type="checkbox"/>
Stock Controller	<input type="checkbox"/>
<Unassigned>	
Kathy	
Jason	
Sandra	

Drag Bar
Click on the Drag Bar to select an employee, drag the employee to the relevant Security Level and release to drop.

Note: If the Export menu appears when clicking on the drag bar to select an employee, this indicates that you are holding down on the drag bar for far too long. Click away and attempt to click and drag again.

- 2) Using the Drag Bar, **select all Users** that you want assigned to a particular Security Level.
- 3) **Drag and drop** the selected Users into the appropriate Security Level.

Note: VERY IMPORTANT! You must ensure that a user is assigned to the 'owner/manager' level (specifically be able to; access security setup; change other employee PIN; and turn security on/off) at all times otherwise you will be locked out of shortcuts.

Step 3: Define Security Access for Security Levels

- 1) Select the **Access Tab**, each Security Level is displayed along with which Screens and/or Actions that Users within that Security Level have access to.

Levels/Terminals	Item/Action	Access	Type
Security Levels	Configuration	<input checked="" type="checkbox"/>	Action
Owner	Stock	<input checked="" type="checkbox"/>	Action
Manager	Clients	<input checked="" type="checkbox"/>	Action
Employee	Appointment Book	<input checked="" type="checkbox"/>	Action
Receptionist	Point Of Sale	<input checked="" type="checkbox"/>	Action
Stock Controller	Security	<input type="checkbox"/>	Action
Terminals	Walkin Manager	<input checked="" type="checkbox"/>	Action
lail	Walkin Manager	<input checked="" type="checkbox"/>	Screen
	Promote Vists	<input checked="" type="checkbox"/>	Action
	Delete a Visit From WIM	<input type="checkbox"/>	Action
	Employee Performance	<input checked="" type="checkbox"/>	Screen
	Reports	<input type="checkbox"/>	Screen
	Marketing	<input type="checkbox"/>	Screen
	Roster	<input checked="" type="checkbox"/>	Screen

Double PIN Verification to delete Transactions
 Require Return or Done when entering PIN's
 Security Enabled
 Support Verification Devices

Done

- 2) It is important that you review and define Accesses for each Security Level carefully.

Defining Access for each Security Level

1. Click to select the appropriate **Security Level** (eg Manager)
2. Place a **tick** in the Access column for each screen and/or action that you want this Security Level to have Access to (a tick means Users in this Security Level will have Access). Alternatively remove the tick from the Access column for each screen and/or action that you would like to be restricted for this Security Level (no tick means Users in this Security Level will not have Access).*

*If you would like a further explanation to what each Screen/Action is, then please refer to article "Security Overview & Definitions".

Note: If all accesses are enabled for all security levels, there will be no security in place for the relevant screen/action.

Step 4: Define Security Access for Terminals (if required)

In the Access tab each Terminal is displayed along with which Screens and/or Actions that Users will have access to. By default Shortcuts security will check the terminal accesses first.

When to define Security Access for Terminals:

For example, you are running a network of 3 computers (more than one computer using Shortcuts). The two computers on the front desk are mainly used for making appointments and putting transaction thru the Point of Sale. Terminal security is defined so only the relevant screens and actions can be carried out on the front computers. For example the reports screen is not to be accessed on the front computers, so under Item/Action the Reports tick box is not ticked. Whether the Employee logging on has access or not to the Reports screen, the Reports icon will not be displayed unless their Security Level has the Override option ticked, under the Levels tab (which will override the Terminal Security).



It is important that you review and define Accesses for each Terminal carefully.

Defining Access for each Terminal

1. Click to select the appropriate **Terminal**.
2. Place a **tick** in the Access column for each screen and/or action that you want this Terminal to provide Access to (a tick means this Terminal will have Access). Alternatively remove the tick from the Access column for each screen and/or action that you would like to be restricted for this Terminal (no tick means this Terminal will not have Access).

Note: By default Shortcuts security will check the terminal accesses first. If you want security level accesses to override terminal accesses, you will need to tick the override option for the appropriate security level(s).

Step 5: Set Other Security Options

Please read below and see which other Security Options you wish to enable.

The screenshot displays the 'Security Setup' window. On the left is a navigation pane with icons for Sales Setup, General Setup, Security, Business, General, Stock, Clients, Walkin, Confirmation, Internet, and Region Setup. The main area is titled 'Security Setup' and has two tabs: 'Levels' and 'Access'. The 'Levels' tab is active, showing a table of security levels and their overrides.

Levels	Override
Security Levels	
Owner	<input checked="" type="checkbox"/>
Chris	
Manager	<input checked="" type="checkbox"/>
Kathy	
Employee	<input type="checkbox"/>
Sandra	
Jason	
Receptionist	<input type="checkbox"/>
Judy	
Stock Controller	<input type="checkbox"/>
Paul	
<Unassigned>	
Business	

Below the table are four security options, each with a checkbox:

- Double PIN Verification to delete Transactions
- Require Return or Done when entering PIN's
- Security Enabled
- Support Verification Devices

Other UI elements include a 'Password' button with a lock icon, a 'Done' button with a green checkmark, and a 'Delete' button with a trash can icon. A 'New' button with a star icon is also present. Callouts identify the 'Password Button' and 'Other Security Options'.

Double PIN to Delete Transactions

If you want it to be mandatory that two different Users enter their PINs in order to delete a transaction, place a tick in the Double PIN to Delete Transactions tick box. Remember that a transaction cannot be deleted unless two users have the appropriate access to do so.

Require Enter or Done when Entering PIN's

If this option is turned On (Ticked), users will be required to either hit the Enter key on the keyboard or Click the Done button after entering their PIN. If this option is turned Off (Not Ticked), users will be given access to the relevant screen or allowed to perform the relevant action as soon as a recognised 4 digit PIN has been typed into the PIN field.

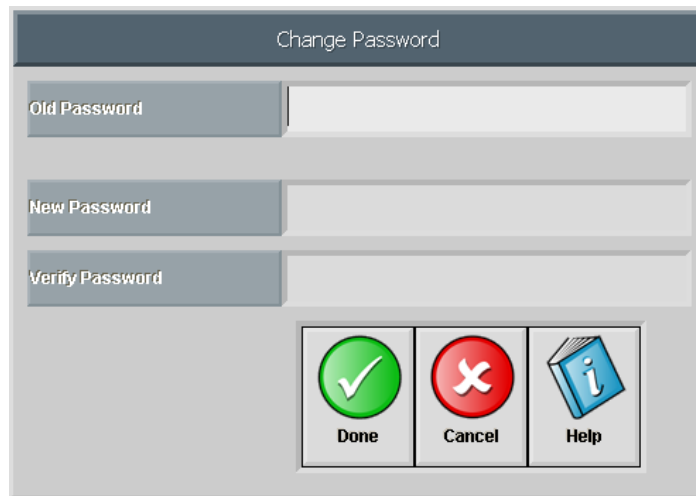
Support Verification Devices

Once Security has been enabled (turned On) the support Verification Devices option will be available. If this option is ticked Shortcuts will recognise magnetic swipe cards for users.

Step 6: Set Startup Password

The Password button allows you to set up a Password or change an existing Password. If a Password is setup, you will need to enter the correct Password to start up Shortcuts.

- 1) Click the **Password** button. The Change Password window will appear:



- 2) Using the keyboard, type in the Old Password for verification (This is if you already have a Startup Password, if this is the first time you are going into this screen, do not enter anything in the Old Password field).
- 3) Hit Tab on the keyboard to get to the next field.
- 4) Using the keyboard, type in the **New Password**.
- 5) Hit Tab on the keyboard to get to the next field.
- 6) Using the keyboard, type the **password again** to verify that you have spelt it correctly.
- 7) Click the **Done** button.

If the Old Password is correct, and the New Password matches the second attempt the New Password will be set. If there is a problem you will have to re-enter the Passwords.

- 8) The next time you launch Shortcuts the Password window will appear. You will be required to enter the correct password to start up Shortcuts. Note, the password is case sensitive.



Note: *Startup passwords will continue to operate regardless of whether security is turned on or off.*

Step 7: Enable the Feature "Must Log On"

- 1) Select the **Setup Menu** from the Navigation Bar, select the **Configuration Icon**. Select the **Sales Setup Menu** from the Configuration Bar and then select the **Terminals Icon**. The Terminal Setup window will appear.
- 2) Tick the option **Must Logon**

Register
If the Terminal is being used to process sales place a tick in the Register option.

Time Out
This option allows you to set the number of seconds that will lapse after a period of inactivity before the current user is automatically logged off from Shortcuts.

Setting the Time Out Lapse
Click to select the Time Out field, and then click again to edit the selected Time Out period. The field will change colour and the text will be highlighted. Using the keyboard, type in the relevant number of seconds appropriate for the selected Terminal.

Active	Terminal Name	Computer Name	Register	Must Logon	Timeout
<input checked="" type="checkbox"/>	lail	lail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	60

Show

Done

Step 8: Assign User PINs or Swipe Card

Assign User PINs

- 1) Select the **Setup Menu** from the Navigation Bar and select the **Employee** icon. The Employee setup window will appear.



Default PIN

The User's/Employee's default PIN is a 4-digit number. It is made up of zeros before his/her ID number (e.g. If an Employee's ID number is 4 his/her initial PIN will be 0004; if a Employee's ID number is 23 the default PIN will be 0023). The default PIN may be required when the 'owner/manager' needs to initially change his/her PIN and/or change other Employee PINs.

- 2) Select an **Employee** from the Alias drop down menu.
- 3) Select the **PIN** icon, the Enter New PIN window will appear.
- 4) Enter the Employee's **New PIN** into the Change PIN window by either clicking the numbers on the screen or using the keyboard. PIN needs to be 4 digits.
- 5) Click the **Done**.
- 6) A message will appear asking you to confirm the New PIN. Click the **Done** button and confirm the New PIN by entering it a second time.
- 7) Click the **Done** button to complete the change, the User's/Employee's PIN will now be set.

Note: If security has not been turned on you will not require an owner/manager's pin to change employee PINs. Note:

VERY IMPORTANT! You must ensure that a user is assigned to the 'owner/manager' level (specifically be able to; access security setup; change other employee PIN; and turn security on/off) at all times otherwise you will be locked out of Shortcuts

Assign Swipe Card (If you plan to use the Swipe Card feature you must Enable Security First, see Step 9)

The card swipe verification feature allows employees to log on and off with a magnetic swipe card using the security feature in Shortcuts. The swipe card reader is either on or attached to the keyboard. Each employee can have only one card and the number must be unique. There are three instances in which it can be used:

- If an employee is logged on to the system and their card is swiped they will be logged off and the Log-On screen will appear. This will allow another employee to log on when required.
- If an employee is logged on and a different employee card is swiped the current employee will be logged off and the new employee will be logged on.
- If an employee card is swiped in the Log-On screen the employee will be logged on.

1) Select the **Setup Menu** from the Navigation Bar and select the **Employee** icon. The Employee setup window will appear.



2) Select the **Employee** who's PIN you want to set from the Employee Alias's drop down menu.

3) Click the **Cfg Verify** button. The Verification Keys window will appear. Simply swipe the employee's card. The swipe card numbers will appear in the field.

Technical Details

The plastic cards with a magnetic stripe can be created from various companies. The following technical information is required to produce these cards:

- The data (swipe number) should be printed on track 2.
- Do not add any other characters. A preceding ";" and ending "?" will automatically be created.
- When the Swipe card is swiped the @ symbol will appear in front of the number. This is not written to the card, it is purely used to identify the number as a swipe card number rather than a barcode.

Note: For employee swipe card verification to be recognised you have User Access Mode turned on (Must Log On Option) in the terminal setup screen. You must also ensure that security is turned on along with the Support Verification Devices option.

Step 9: Enable Security (turn on)

1. Select the **Setup Menu** from the Navigation Bar, select the **Configuration Icon**, select the **General Setup Menu** from the Configuration Bar and then select the **Security Icon**. The Security Setup window will appear.
2. Place a tick in the Security Enabled tick box to turn Security On. A tick means Security is ON. No tick means Security is OFF.
3. The PIN protected window will appear, the User/Owner needs to enter their PIN.



Note: You will only be able to turn security on or off if you have access for this action.