User Security Management
User Guide

Overview

The intent of this document, is to provide the user with the required skills relative to managing user system access within Maestro. There are many different ways where a Maestro Administrator is able to control access within specific areas of Maestro. This includes both restricting and granting access or permissions to each Maestro User, based on their day to day operational requirements and/or needs within the system.

There should always be at least one Maestro Administrator onsite, who is trained in managing User Security and Access within Maestro. It's a good idea to have at least 2-3 management team members with this access. Each administrator would require access to the Global Maintenance module. The reason for having multiple administrators is to control two of the most common user security issues; **Clerk Password Reset and/or Clerk Account Locked**. As a general rule, if a clerk gets locked out or forgets their login credentials and they attempt to contact Maestro Support or Maestro Live Chat, they will be advised to contact their Maestro Administrator and have them complete a password reset or unlock their account. The reason for this is, Maestro is not familiar enough with the current users onsite and who should have access to what areas, or even Maestro in general. If the user locked out or requires a password reset is actually the administrator, the user is required to submit a written request by email to either; support@maestropms.com and new credentials will be returned back to the user.

The general security restrictions within Maestro are primarily managed through either **Authorized Functions** or **Program Security**. When restricting access to specific modules within Maestro or specific menu options or screens, the administrator would control these through **Program Security**. However, for specific actions within Maestro such as; Rate Changes, Override a Do Not Move, Reset a Clerk Password, these are examples where the administrator would grant or restrict permissions based on the controlling of **Authorized Functions**. These two options are managed at two different user levels; **Clerk Codes** & **Clerk Group Codes**. The option to either apply or restrict Program Security is only applicable at the **Clerk Group level**. While the option to use Authorized Functions, is managed at **both** Clerk Code and Clerk Group Code.

Contents

Maestro

1 Managing Clerks and Clerk Groups

## 1.1 Creating Clerk Group Codes

This section will guide the user through the steps to create new **Clerk Group** Codes. This feature simplifies security setup and management. All users who perform the same functions within Maestro, are grouped together into the same **Clerk Group**. The system administrator defines security for the **Clerk Group** and applies to all users in the group.

Once the Clerk Group Codes have been configured and all relevant security restrictions and permissions have been applied, the individual user Clerk Codes can be created and assigned accordingly to each Clerk Group based on their department/position within the property.

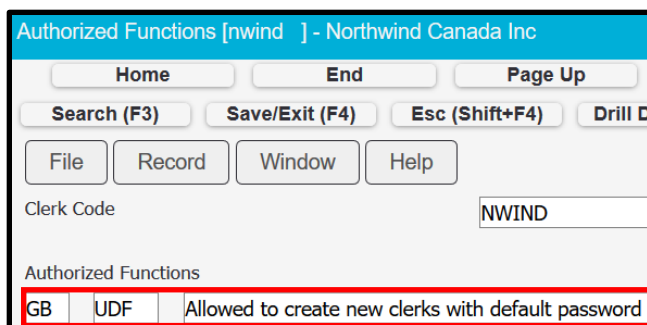1) Login to **Global Maintenance** | Select **Security** | Select **Clerk Group Code Maintenance**
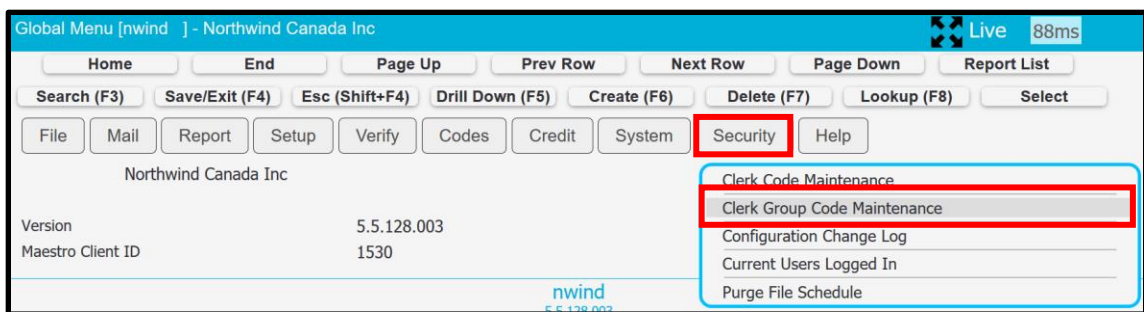
2) **Create (F6)** | Maestro will automatically generate a new record entry line
3) **GrpCode** | Type a code to identify the new **Clerk Group** (Character Limit = 4) | ENTER

4) **Description** | Type a description to identify the Clerk Group (Character Limit = 30) | ENTER

I.2   Creating Clerk Codes

1) Login to **Global Maintenance** | Select **Security** | Select **Clerk Code Maintenance**

2) **Create (F6)** | Maestro will automatically generate a new record entry line at the bottom of the list
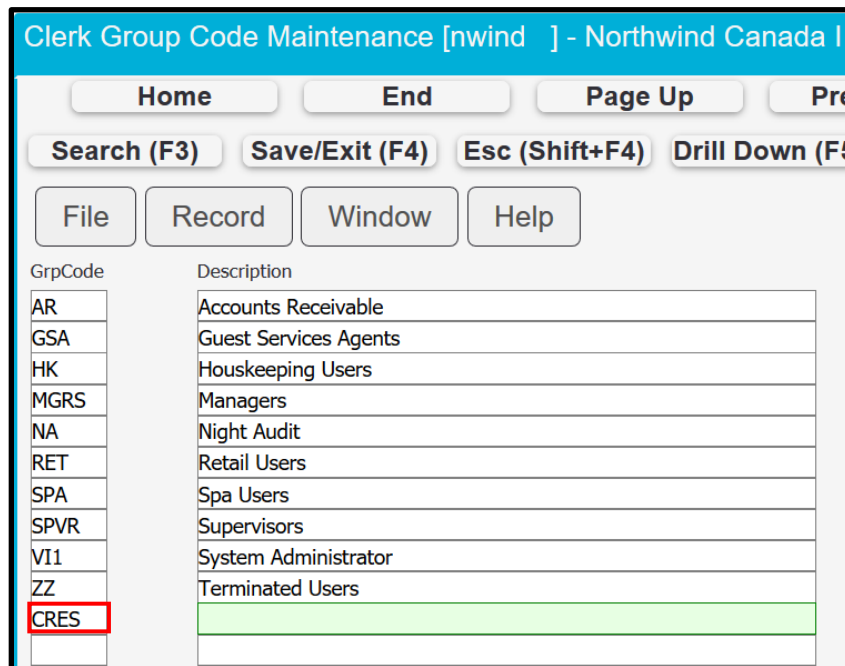
3) Complete each field based on the details for each field below. Press **ENTER** after entering a value in each field, to move onto the next field. Once all fields have been completed, press **ENTER** to the next line to ensure the previous record entry has been saved

Field	Action/Purpose of Field
Clerk	A unique code for each user. The property defines its own naming standards for users. General recommendation is 'First Initial+Last Name'. A character limit applies of 8
First Name	First Name of User
Surname	Last Name of User
Group	**Lookup (F8)** | Select the **Clerk Group** Code according to department/position | Press **ENTER**
DeptCode	If applicable | **Lookup (F8)** | Select the **Dept Code** according to department/position | Press **ENTER** ***Not a mandatory field**
Lang	This can be left BLANK, as it is reserved for future development
PwdRenew	The value entered should always be **90**. Identifies number of days until password must be rest. If set above 90, PCI compliance is not being followed and user will receive a notification
Active	Indicate the Status of the Clerk Code | **Lookup (F8)** | Select an Option Y = Clerk Code is Active for Login | Clerk can login at any time N = Clerk Code is Inactive for Login | When clerk attempts login, will display as **Invalid Login** L = Clerk Code is Locked | When clerk attempts login, will display as **Account Locked** In most cases, when a user reaches the max failed login attempts, the clerk status automatically defaults to 'L'. There is also the option to lock out a user, set the flag to 'L' manually, & user would need to contact the administrator to unlock their account. In either situation above, status must be changed back to 'Y' and the password <u>must</u> be reset before Clerk attempts login again. See 'Clerk Password Management' for steps to reset a password.

4) If the user creating the new clerk codes, has been associated to the authorized function below, the default password for all users created will be **'Maestro99'** and is case sensitive. When the user logs into Maestro for the first time, will be prompted to change their password


5) If the authorized function mentioned above has not been associated to the clerk creating the new clerk codes, Maestro will automatically generate a new password. Upon completion of the new clerk code, Maestro will display the password as shown on the next page. When users login, the 'clerk code' must be entered in the format of lowercase characters

Password for clerk SSMITH
has been temporarily set to:
notebook43

OK
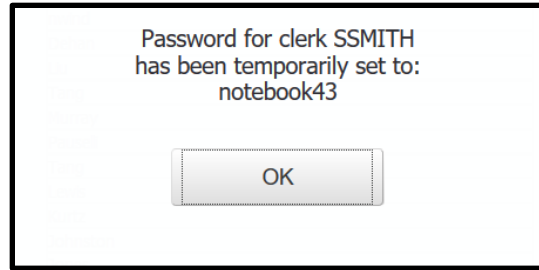
1.2.1   Managing Clerk Extra Information

Maestro has an optional screen that can be completed for each Clerk Code. Depending on how Maestro is being used at the property, some of these fields will be useful for many functions.

1) To access the Extra Information screen | Select **Clerk Code** | Select **Window** | Select **Extra Information**
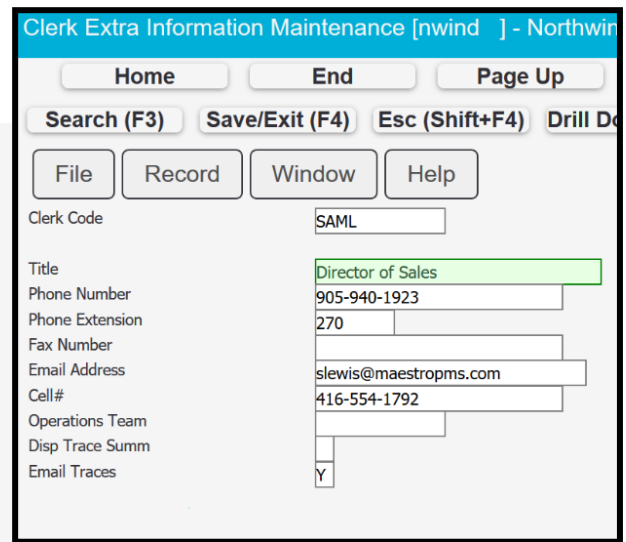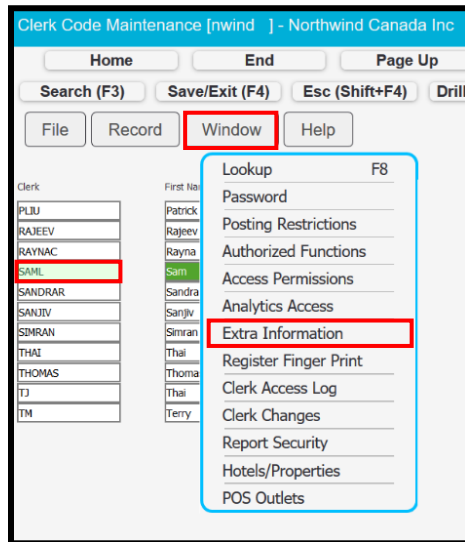
2) Complete each field based on the details for each field below. Press **ENTER** after entering a value in each field. When desired fields are completed | Select **Save/Exit (F4)**

Field	Action/Purpose of Field
Title	Enter the clerk's title at the property
Phone Number	Enter the contact phone number for the clerk. When user selects option '**Email Maestro Support**' from the **Help** menu, the phone number will populate in the support email form automatically. With no phone number, our support team will not be able to contact user by phone if needed.
Phone Extension	If the clerk has a specific extension, enter in this field
Fax Number	If the property has a fax number, enter the number in this field

Continued on Next Page

Field	Action/Purpose of Field
Email Address	Enter the contact email address. If the option below for 'Email Traces' is set to 'Y', this field should be completed so traces will be emailed to the clerk. Additionally, if the user selects the option 'Email Maestro Support' from the Help menu, the email will populate in the support email form automatically. With no email, our support team will not be able to contact user by email if needed. If the property is using the SMS/Alerts feature, if a user creates an Alert to send internally to team members and selected method is By Email, with no email configured in this field, the user will not receive the alert. Lastly, when a user initiates a Live Chat with Maestro, if their email is filled in on this screen, it will auto-populate into the chat, which they will then receive a copy of the chat transcript
Cell #	Enter the client's cell phone # if applicable. If using Maestro's SMS/Alerts feature, it's important to have this field entered, if they wish to receive any SMS Messages or Alerts
Operations Team	Select Lookup (F8)	Make a selection to identify which team at the property, the clerk works with
Disp Trace Summ	Select Lookup (F8)	Make a selection based on the options provided Y = Display Trace Summary	When selected, the Trace Summary Listing screen will appear automatically after logging in N = No Trace Display	When selected, the Trace Summary Listing screen will not appear automatically upon login. Flag can also be left BLANK for the same result D = Display Trace Details	When selected, the Received Messages screen will appear. This screen will include traces assigned as well as any internal messages sent from clerk to clerk internally with in Maestro S = Display Dashboard	When selected, all Maestro modules that have a dashboard (ie. Front Desk, Spa, Sales & Catering), it will display automatically upon logging into the module
Email Traces	Select Lookup (F8)	Make a selection based on the options provided Y = An email notification will be sent when traces are assigned **Email address must be added in the field mentioned above N = An email notification will NOT be sent when traces are assigned

I.2.2   Clerk Password Reset

When a clerk password requires reset, follow the steps below to reset a password for any clerk. Note that access to Global Maintenance is required to complete this action.

1)   Log into Global Maintenance | Select Security | Select Clerk Code Maintenance
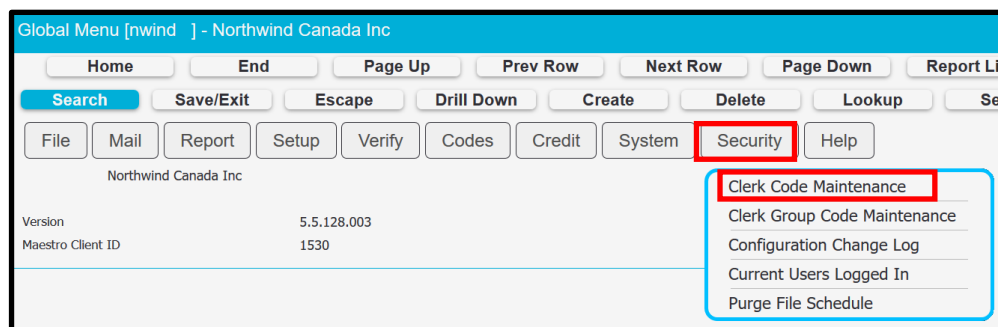
2) Select **Clerk** Code to Change Password | Select **Window** | Select **Password**
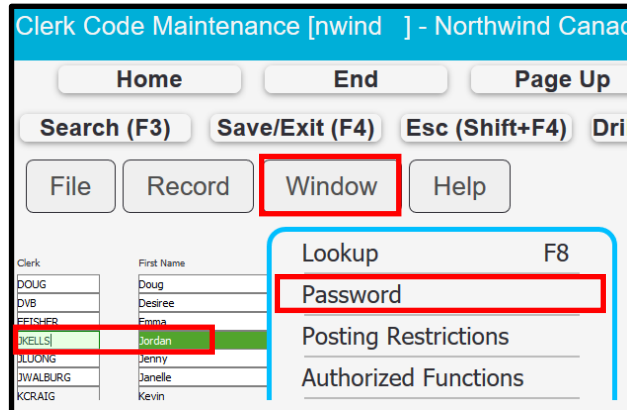
3) In most cases, the '**Current Password**' is unknown, which is why the reset is required | Select **Window** | Select **Reset Password**
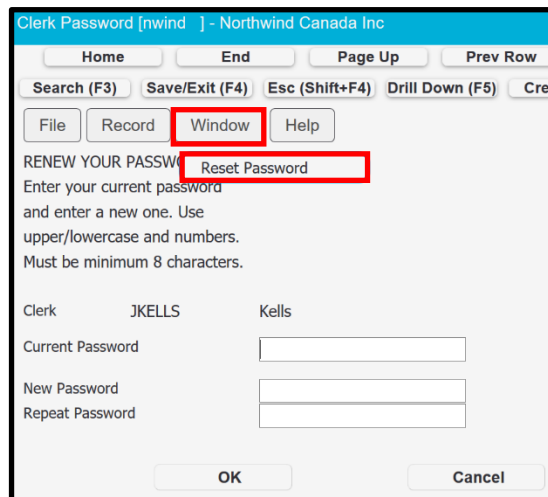

4) Confirm to Reset the Clerk's Password | Select **OK**
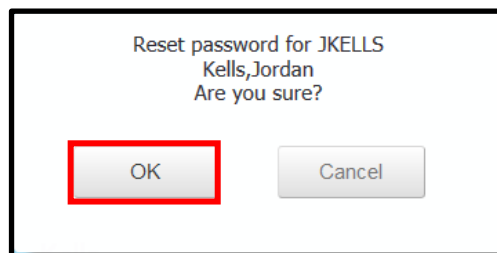
5) Maestro will generate a random password (two words and a number) for the clerk | Provide new temporary password to clerk | Select **OK**
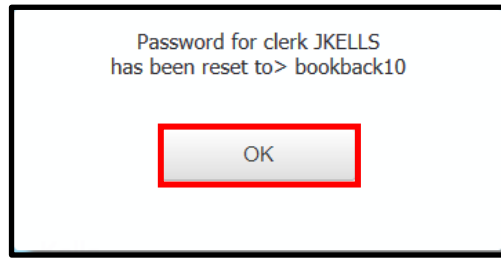
6) Clerk will use the same Clerk Code and new temporary password to login. Upon login the user will be prompted to Renew Password | Select **OK** | Follow the screen instructions
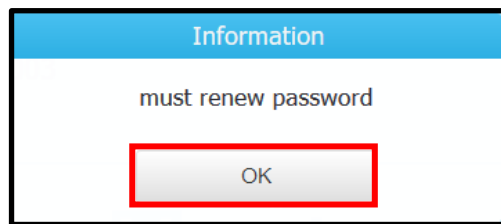
7) Complete all fields as indicated to complete password renewal | Select **OK**
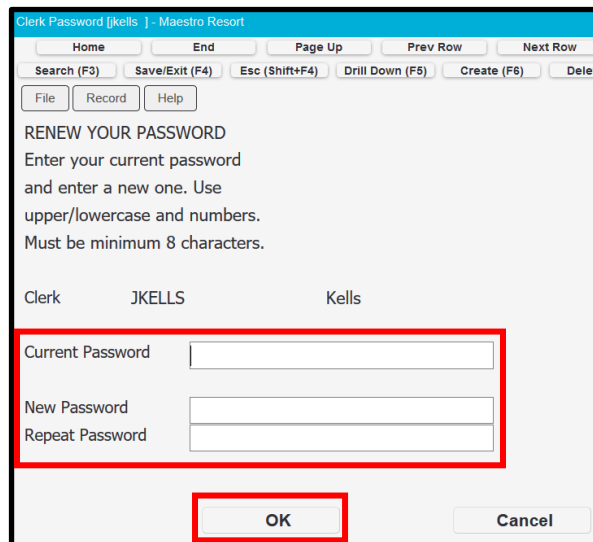
2 Managing Hotel/Property & POS Outlet Access

In order for a clerk to use Maestro, they must be granted access to a property and depending on the property, if applicable, must also be granted access to the POS Outlet(s). Access can be granted either at the individual Clerk or Clerk Group level.

2.1 Hotel/Property Access

In a single property environment, each Clerk or Clerk Group must be granted access to the property, or they will not be able to use Maestro. In a multi-property environment, where a user works at multiple properties, they must be granted access to each of those properties.

2.1.1 Assign Hotel/Property Access By Clerk Group

Follow the steps below, to assign Hotel/Property access at the Clerk Group level

1) Login to **Global Maintenance**
2) Select **Security** | Select **Clerk Group Code Maintenance**
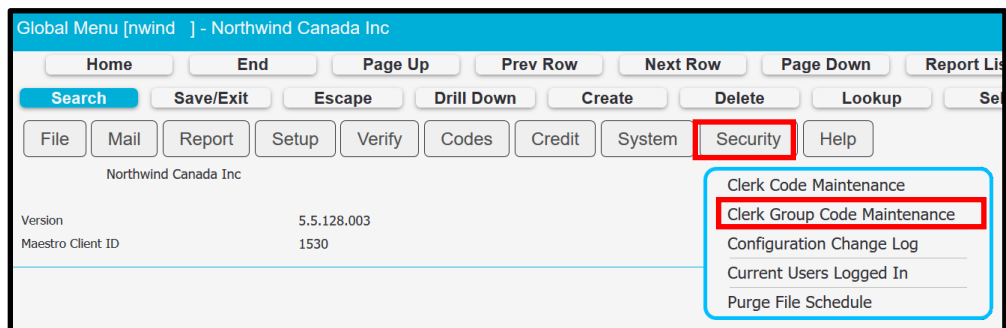
3) Select **Window** | Select **Hotels/Properties**
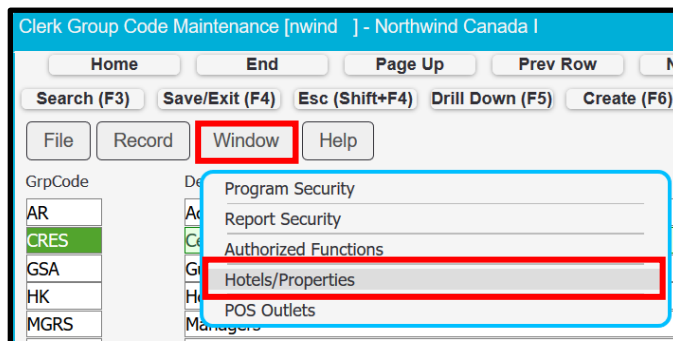
4) **Lookup (F8)** | Properties within the multi-property database will be listed. Any properties with no access granted as of yet, will show the Access column as **NONE**
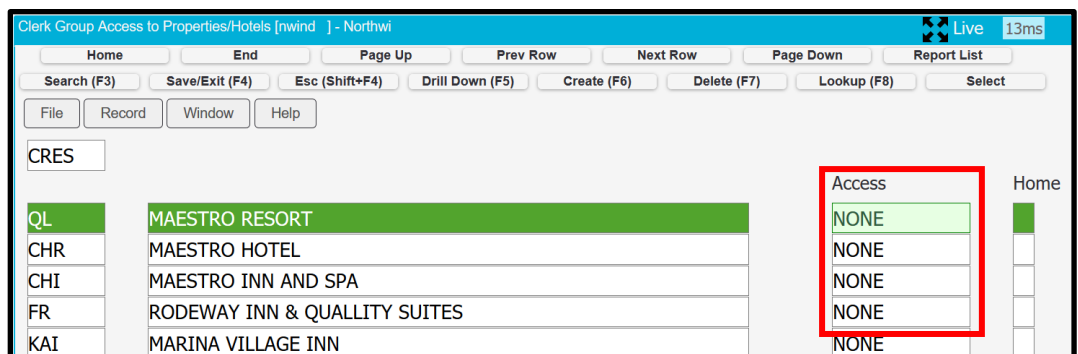
5) To grant access to a property | Select the property using the ↑/↓ keys on the keyboard or select the **Access** column for the property with the mouse

6) Lookup (F8) | F – Full Access | ENTER

7) If clerks assigned to the selected Clerk Group, require access to more than one property in a multi-property environment, repeat for all properties the clerk group should have access to. If multi-property access is only at the Clerk level, then perform the same process through Clerk Code Maintenance for the specific clerk. In a multi-property where either the Clerk or Clerk Group should have access to multiple properties, the screen should look like below

8) To assign a **Home** property to a Clerk or Clerk Group | Select the flag **Home** for the property to be assigned as the Home property

9) Lookup (F8) | Y - Yes | ENTER

When logging into a multi-property environment, where a **Home** property has _not_ been assigned, the **Accessible Properties** screen will appear once a module is selected from the homepage. The user must select a property to access | ENTER

2.2 Changing Between Properties

When a **Home** property _has_ been assigned, once the user selects a module to log into, they will be taken directly to that property database automatically, with no option to pick a property upon login. Once logged in, the user can change properties at any time.

Depending which screen the user is currently in, will determine which menu option to select if they wish to change properties.

In most cases, if there is no option on the menu bar for **WINDOW**, the user will then follow the below to change properties

1) Select **File** | Select **Change Property**
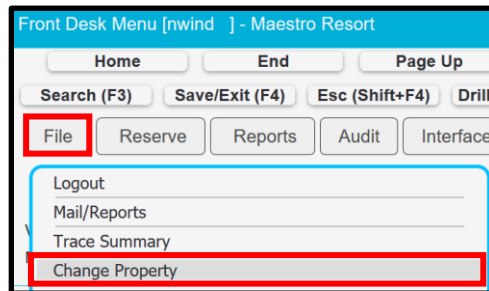
When there _is_ an option on the menu bar for **WINDOW**, the user will then follow the below to change properties

2) Select **Window** | Select **Property**
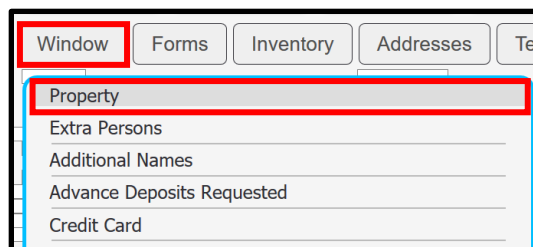
The **Accessible Properties** screen will appear, at which point the user will select which property they wish to change to | The desired property should be highlighted in green | ENTER
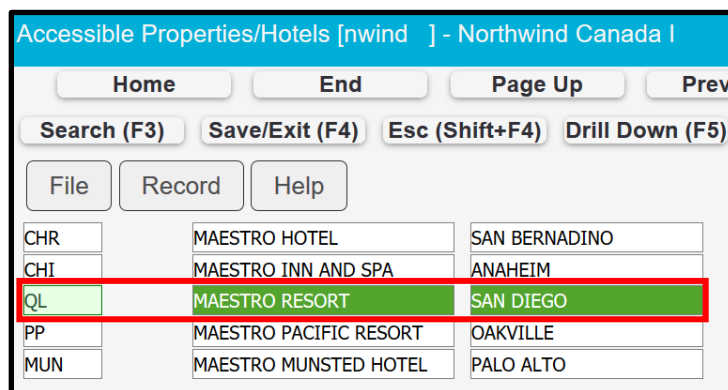
2.2.l   Assign Hotel/Property Access By Clerk

Follow the steps below, to assign Hotel/Property access at the Clerk level

1) Login to **Global Maintenance**
2) Select **Security** | Select **Clerk Code Maintenance**
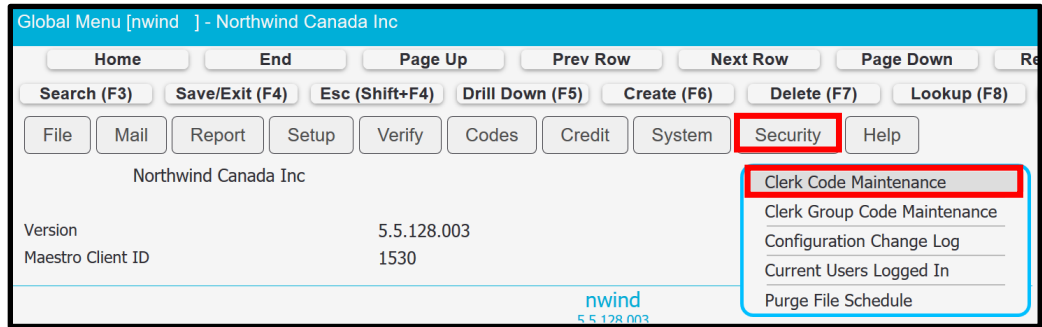
3) Follow the same steps above in the '**By Clerk Group**' section, beginning at <u>Step #3</u>

2.3   POS Outlet Access

For properties that are using the integrated Maestro Point of Sale, users that require access to this module must also be granted access to the POS Outlet as well. Without access, they will be unable to complete POS transactions. If they work at multiple properties where the properties are using the Maestro Point of Sale module, they must also have access to the POS Outlets. Similar to property access, outlet access can be granted at both the Clerk and Clerk Group levels. The steps to grant access are the same as Hotel/Property access, just choosing POS Outlets instead

2.3.l   POS Outlet Access By Clerk Group

Follow the steps below, to assign POS Outlet access at the Clerk Group level

1) Login to **Global Maintenance**
2) Select **Security** | Select **Clerk Group Code Maintenance**

Maestro
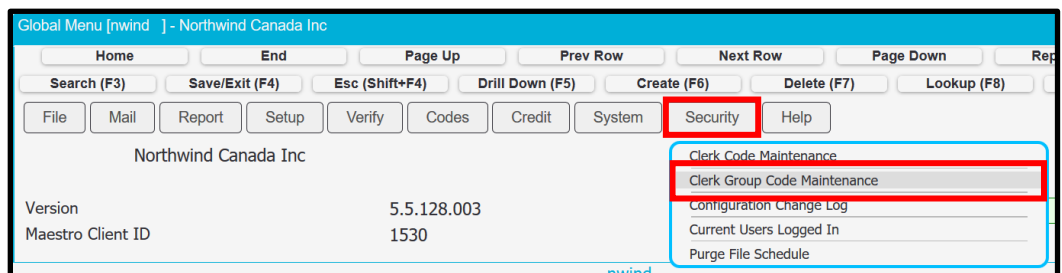
3) Select the **Clerk Group** | Select **Window** | Select **POS Outlets**
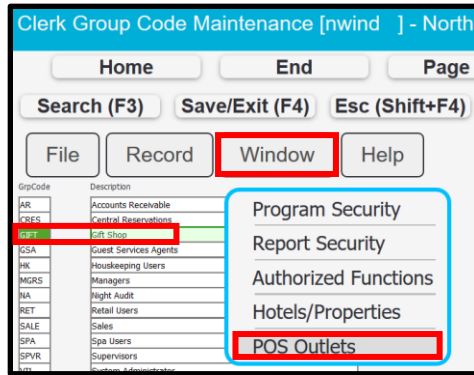
4) **Lookup (F8)** | All POS Outlets within the database will be listed. If no access has been granted yet, all outlets will show the Access column as **NONE**
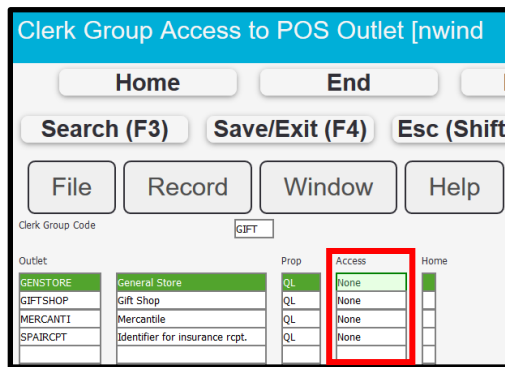
5) To grant access to an outlet | Select the outlet using the ↑/↓ keys on the keyboard or select the **Access** column for the outlet with the mouse

6) Lookup (F8) | F - Full Access | ENTER

7) When a Clerk Group, requires access to all or multiple outlets at one property, repeat the above for all outlets requiring access. If required at the Clerk level, complete the same process using Clerk Code Maintenance for a specific clerk. In a multi-outlet environment where either the Clerk or Clerk Group should have access to multiple outlets, the screen should look like below

8) To assign a **Home** outlet to a Clerk or Clerk Group | Select the flag **Home** for the Outlet to be assigned as the Home outlet

9) Lookup (F8) | Y - Yes | ENTER

When accessing the **POS Outlets** screen in a multi-outlet environment, where a **Home** outlet _has_ been assigned, the **Outlet Code** field will default to the Home Outlet Code

When accessing the **POS Outlets** screen in a multi-outlet environment, where a **Home** outlet has _not_ been assigned, the **Outlet Code** field will be BLANK as shown below

1) To select a POS Outlet | **Lookup (F8)** | Select an Outlet | ENTER

2) The selected outlet now appears in the POS Outlets screen and user can proceed with the transaction

3 Managing Clerk Group Program Security

This option is used to restrict access to specific modules or screens in Maestro. Changes made to Program Security will take effect the next time the users log out and log back into Maestro. This can only be applied to **Clerk Groups** and not individual Clerks.

3.1.1 Program Security by Maestro Module

One way to utilize this option is to restrict user access to an entire module itself. To achieve this, each module is identified by a Program ID and once that is determined, it is added to the Program Security restrictions screen.

1) Log into **Global Maintenance**
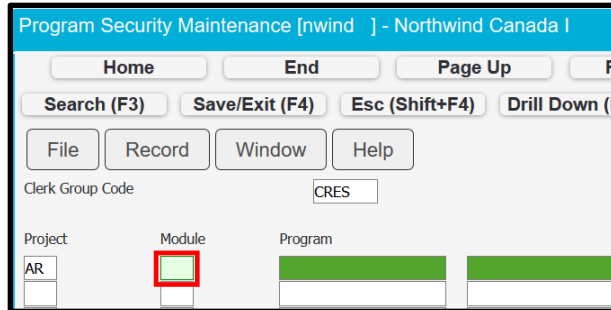2) Select **Security** | Select **Clerk Group Code Maintenance**
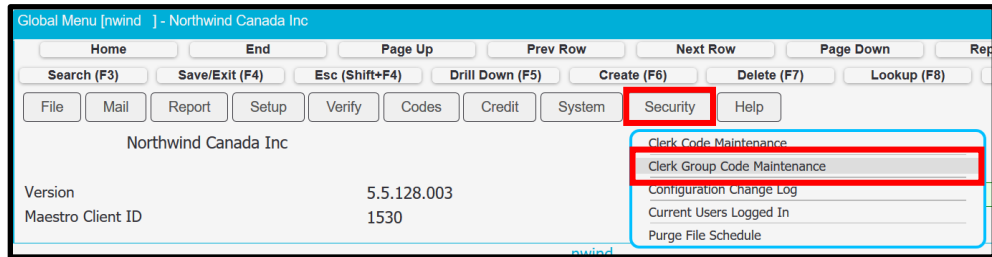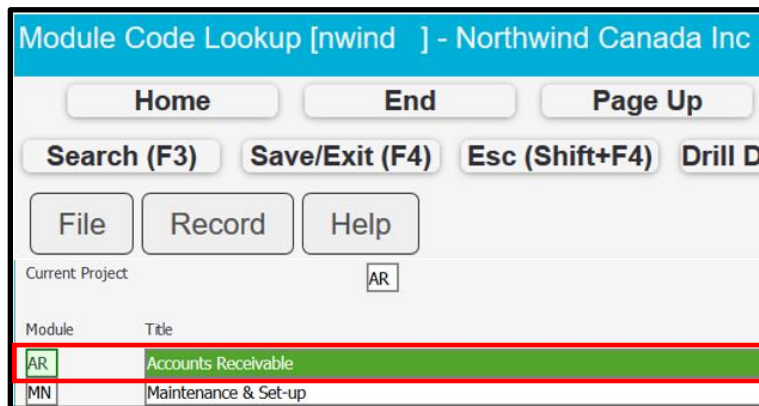

3) Select **Window** | Select **Program Security**
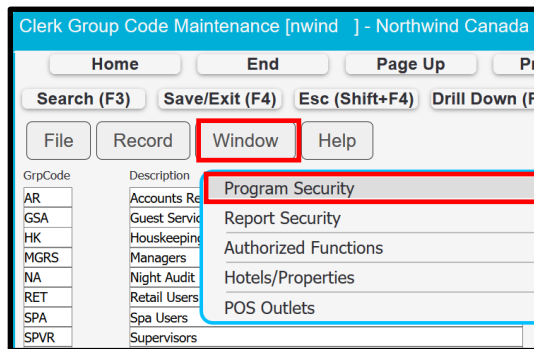
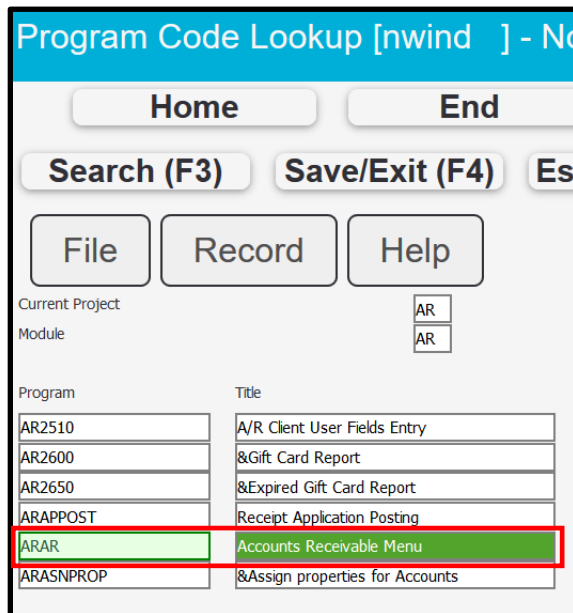4) **Create (F6)** | **Lookup (F8)** | **Project Code** to be restricted | **ENTER** twice
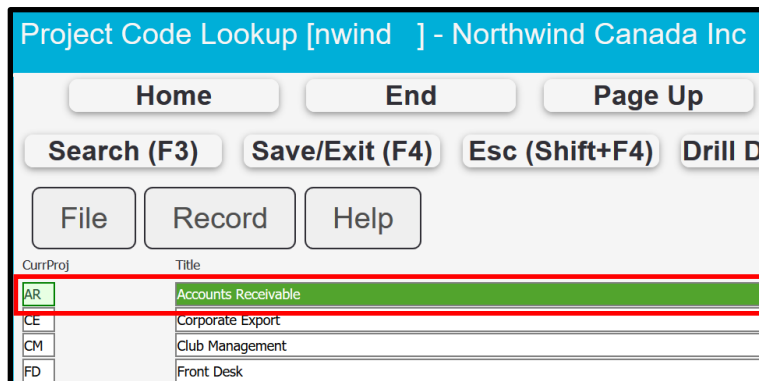
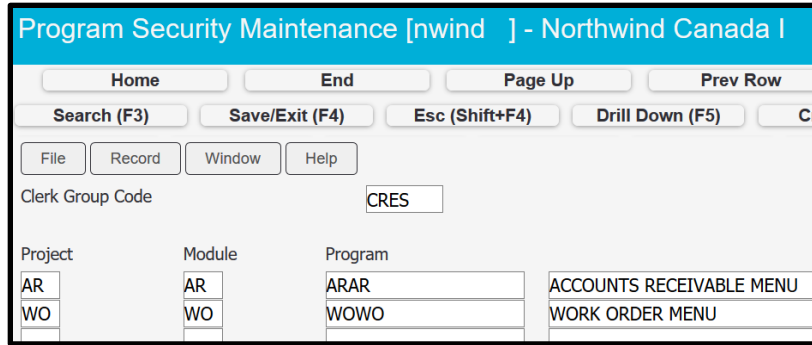

5) **Module** | **Lookup (F8)**

6) **Lookup (F8)** | **Module Code** to be restricted | **ENTER** twice

7) **Lookup (F8)** | **Program Code** to restrict access to | **ENTER** twice

8) In the below example, the selected Clerk Group of **'CRES'** has been restricted from accessing the **Accounts Receivable** and **Work Order** modules.

Program Security Maintenance [nwind] - Northwind Canada I

A quick reference to restrict access by a specific module. Use the codes below;

Maestro Module	Project Code	Module Code	Program
Accounts Receivable	AR	AR	ARAR
Accounts Receivable Maintenance	AR	MN	ARMN
Front Desk	FD	FD	FDFD
Front Desk Maintenance	FD	MN	FDMN
Global Maintenance	GB	GB	GBGB
Owner Management	TC	TC	TCTC
Owner Management Maintenance	TC	MN	TCMN
Point of Sale	PS	PS	PSPS
Point of Sale Maintenance	PS	MN	PSMN
Sales & Catering	SC	SC	SCSC
Sales & Catering Maintenance	SC	MN	SCMN
Spa & Activity	CM	CM	CMCM
Spa & Activity Maintenance	CM	MN	CMMN
Work Order	WO	WO	WOWO
Word Order Maintenance	WO	MN	WOMN

When a clerk logs into the **Maestro Web** environment module restrictions are applied, only the modules with access will appear on the **Maestro Homepage.** Based on the example above, the **CRES** Clerk Group, does not have access to **Accounts Receivable** or **Work Order** modules, which is reflected on the Maestro Homepage are they are not displayed as a selection.

When a clerk logs into the **Maestro Windows** environment and the module they selected to log into has been restricted to their Clerk Group, the clerk will be presented with the below notification. Clerk will select **OK**.
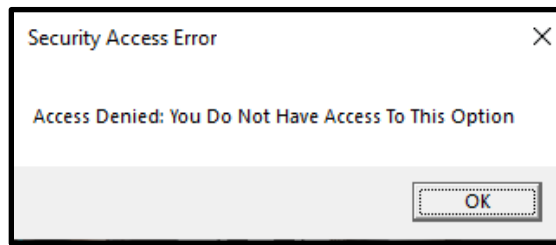
When the **Program ID** column (field) is left blank and the user presses ENTER to the next line, the description will appear as below for each module "FULL RESTRICTION - ALL PROGRAMS IN THIS MODULE." This will remove the module(s) from the Maestro homepage, similar to when using module specific Program ID's.
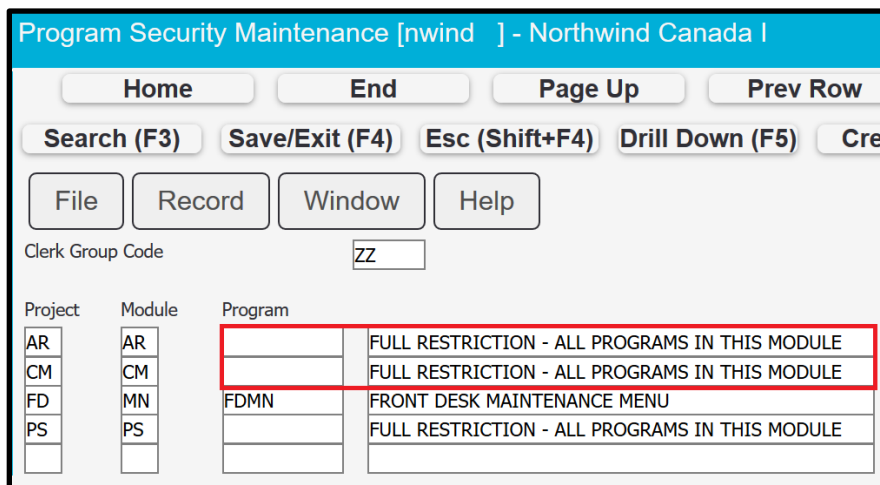
Unless the program security is being applied to a Clerk Group such as **Terminated Users,** it's generally not recommended to leave the Program ID blank with FULL RESTRICTION. Doing this can result in many issues from the front-end side, such as the Front Desk module.

For example, when full restriction is applied to **Accounts Receivable** (as shown above with AR | AR | No Program ID), the intent may be to only restrict users from accessing the AR module itself and creating AR accounts or AR folio management etc. But in fact, the user will not be able to perform the following actions from the front desk module;

    a)   **No Folio Access** | Accounts Receivable, Guest or Group Folios
    b)   **Guest Checkout** | When a balance is due
    c)   **AR Accounts** | Assign to Reservations or Settle Folio to AR Account
    d)   **Gift Cards** | Sell, Redeem, Check Balance

3.1.2   How to Remove Program Security

    1)   To remove restriction for a specific Program ID and reinstate access to the selected Clerk Group | Select the **Program ID**
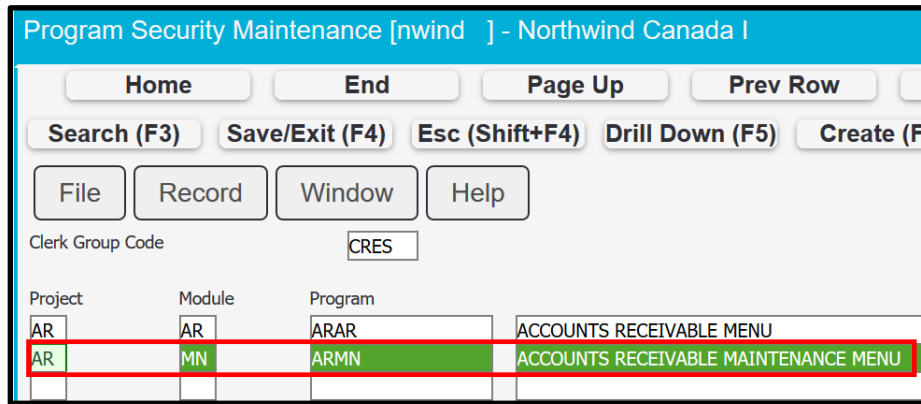
2) Delete (F7) | OK
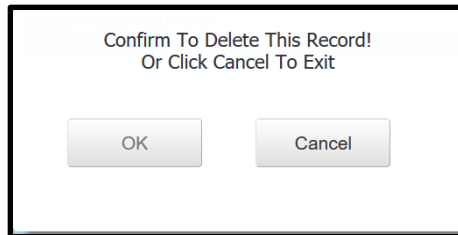
3) The selected program ID was removed and the selected Clerk Group has been granted access.
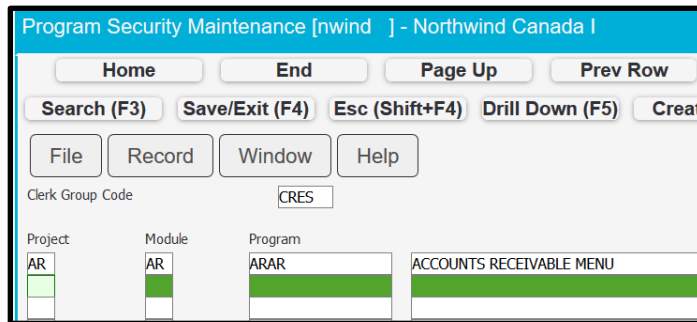

3.1.3 Program Security by Specific Maestro Menu Options and/or Screens

The additional option for restricting user access outside of entire modules, is to choose a specific Menu Option or Screen within Maestro. This is done in the same manor, by first identifying the Program ID for the area to be restricted. Then adding the Program ID into the Program Security restrictions screen.

1) To identify the Program ID if it is unknown | Go to the screen to be restricted
2) In this example, users will be restricted from the option 'Charge Folio Restrictions'
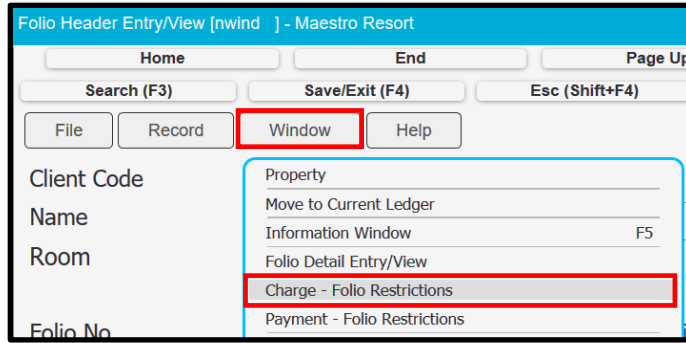
3) Navigate to the screen | Help | About
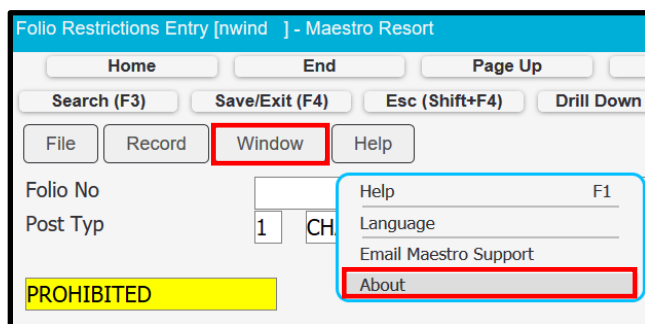
4) There are two things you want to make note of from this screen | Program & Module |
Be sure to write this information down, as it will be needed when applying the restriction
through Program Security

Maestro
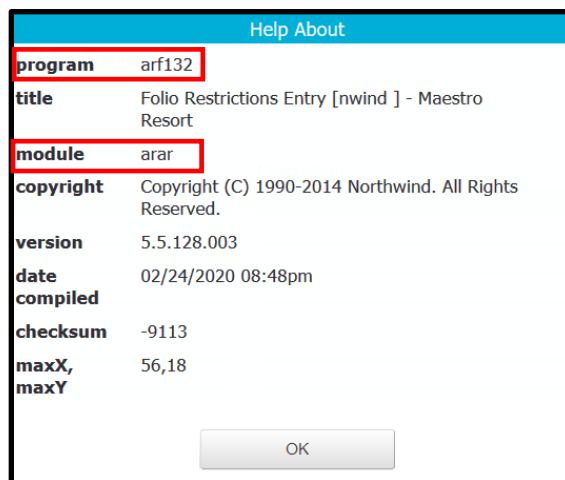
5) Navigate back to Global Maintenance | Security | Clerk Group Code Maintenance
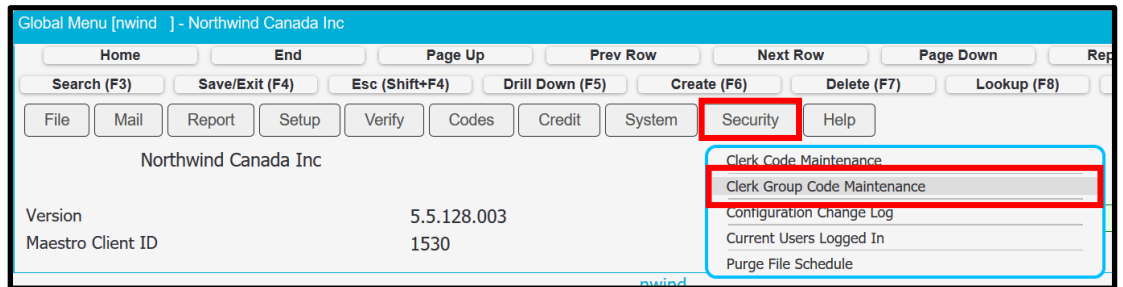
6) Select the **Clerk Group** Code to Apply the restriction | Select **Window** | Select **Program Security**
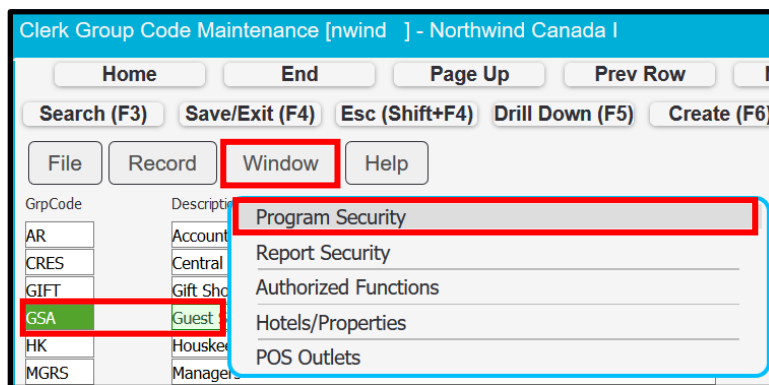
7) Based on the information from the screenshot in step #4 (shown below)
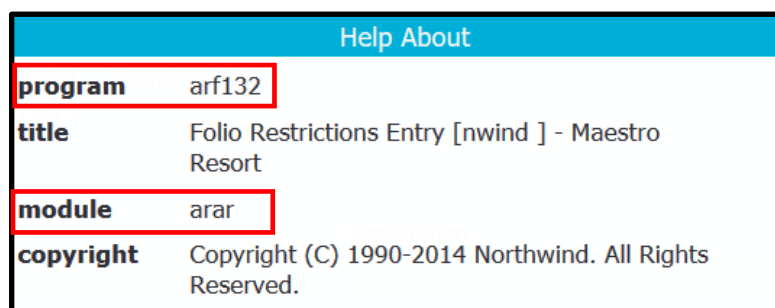
8) Enter into the below screen as shown
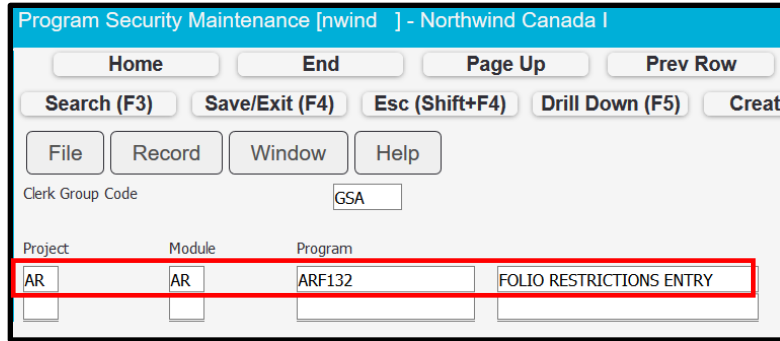
Any users affected by these changes, if they attempt to access a recently restricted area but had not logged out, the option will still be listed in the drop-down menu. However, the screen will not open and the screen will 'blink' and user will be in the same screen. Once the user logs out and logs back in, the menu option will have been removed from the drop-down list, depending on where it's accessed from in Maestro.

For example, in the below screenshot, the two programs have been added to the restrictions; Housekeeping & Night Audit
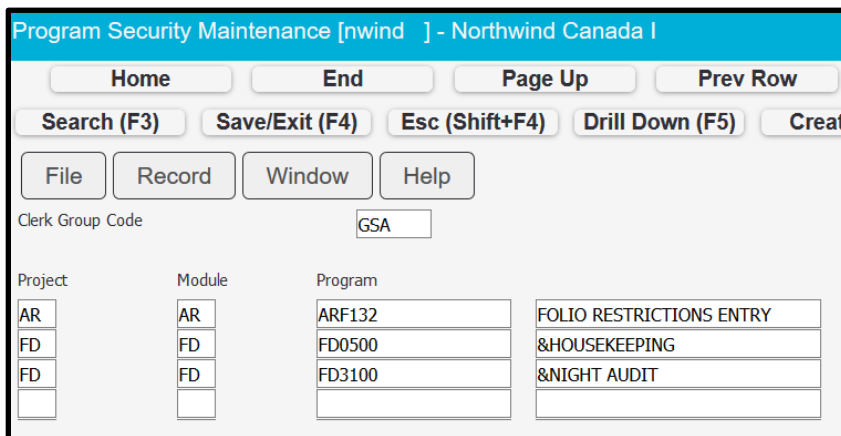
If attempting to access the screens noted above from the Front Desk Menu, this is what the drop down menu options would look like with no restrictions to the Housekeeping or Night Audit options
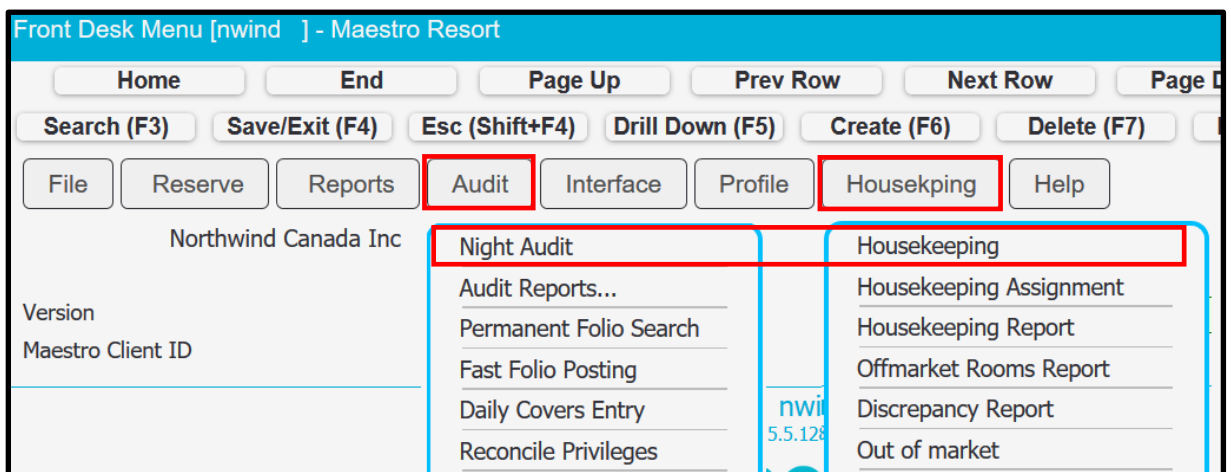
However, once restrictions have been applied to the Housekeeping & Night Audit menu bar options, when comparing the below screenshot with the above screenshot you will notice a difference. In the below screenshot, when attempting to access the same menu options from the Front Desk Menu, the first items on the drop down list shown in the above screenshot have been removed; Audit | Night Audit & Housekping | Housekeeping.
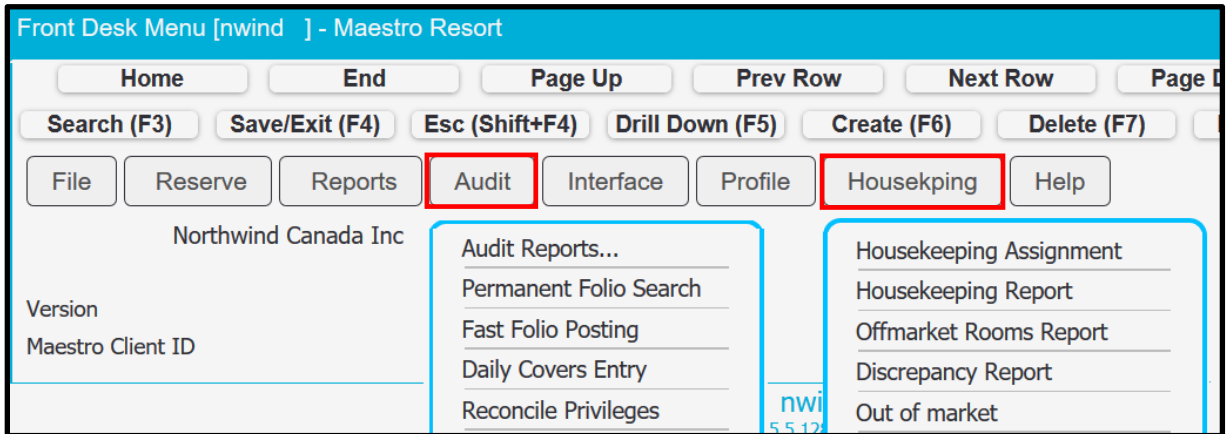
However, when user attempts to access the Housekeeping drop down menu option from the **Front Desk Dashboard**, the drop down menu is not affected visually. Although, if the user attempts to select the Housekeeping option, the screen will not appear.
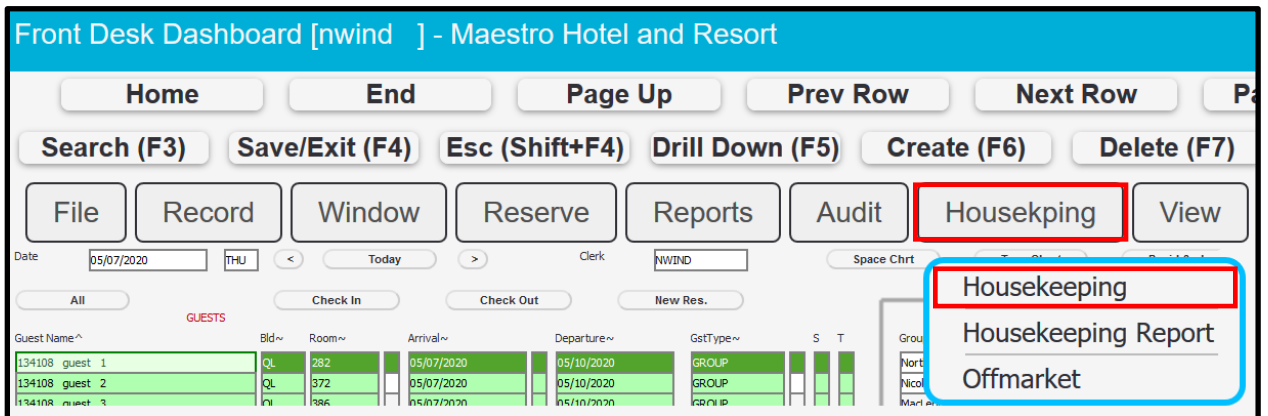
4 Managing Authorized Functions

This feature is used to grant or restrict access or permission to perform a specific action in Maestro. These functions can be assigned at the Clerk Group and Individual Clerk level. Each of the functions are module specific and when setting up, require a module code and the authorized function code.

4.1.1   Authorized Functions By Clerk Group

1) Log into **Global Maintenance**
2) Select **Security** | Select **Clerk Group Code Maintenance**
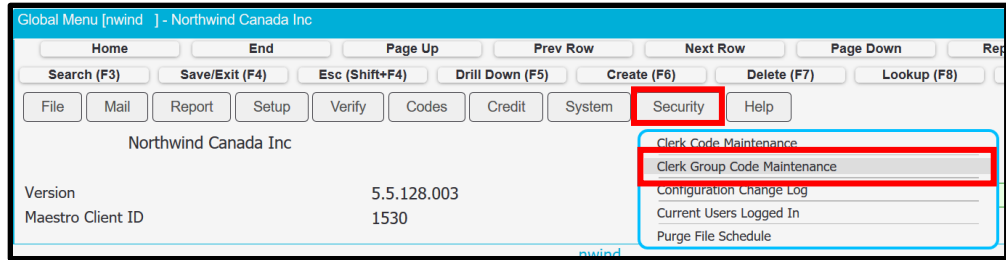
3) Select the **Clerk Group** to Modify | Select **Window** | Select **Authorized Functions**
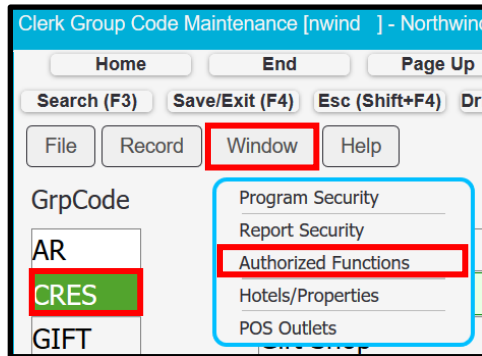
4) In the Authorized Functions screen, there may or may not be any listed record entries | **Create (F6)** | Maestro will create a new entry line
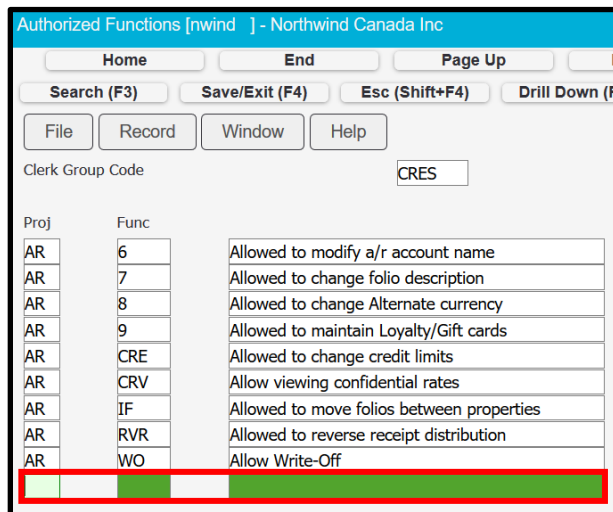
5) If the Clerk or Clerk Group should have access to ALL authorized functions within one module (Example - AR - Accounts Receivable), there is a convenient import feature
6) In the field **Proj** | **Lookup (F8)**

7) Press **ENTER** on the first listed function (**AR** - **1**)

8) Press **ENTER** twice | Screen should look like below

9) Ensure the function just added is selected (highlighted in green) | Select **Window** | Select **Import Functions**
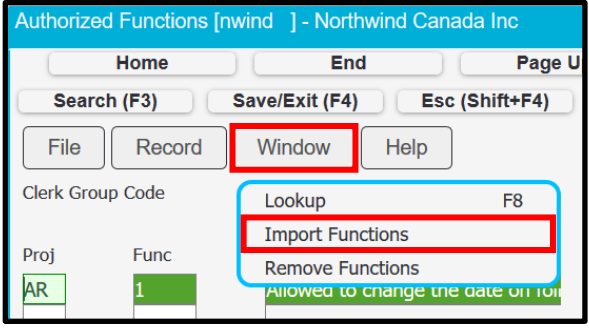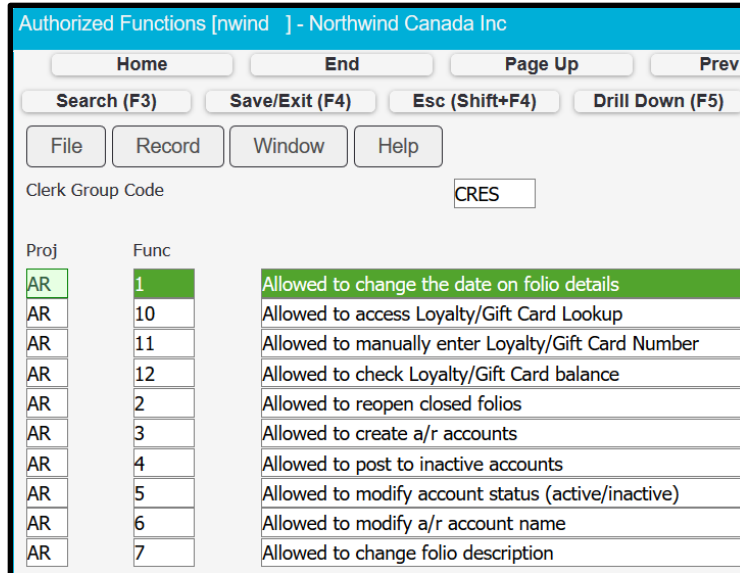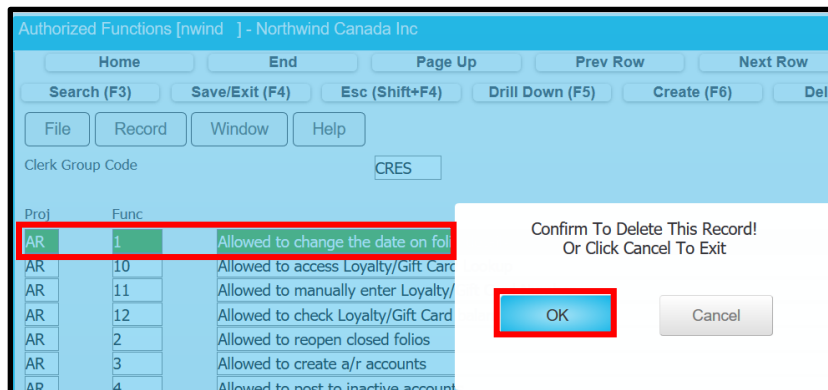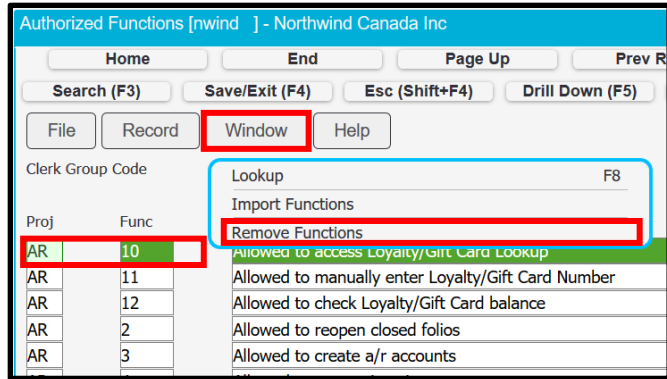

10) Select **OK**
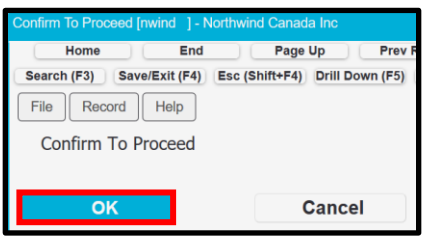
11) Select OK
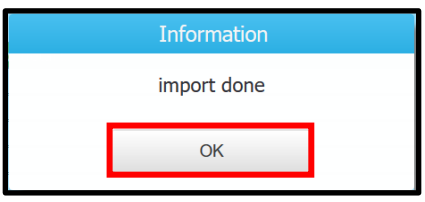
12) Notice all authorized functions for AR have been imported automatically

13) Be sure to always remove the first function (AR-1) as this should never be granted to any users. The same goes for the function (FD-1), if importing all FD authorized functions | Select the function so it's green | **Delete (F7)** | OK
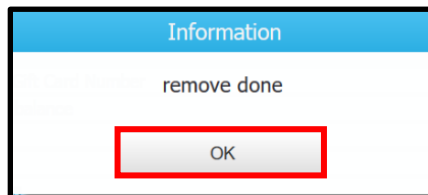

14) To remove all authorized functions for a specific module | Select the first function displayed in the list for the module | Select **Window** | Select **Remove Functions**
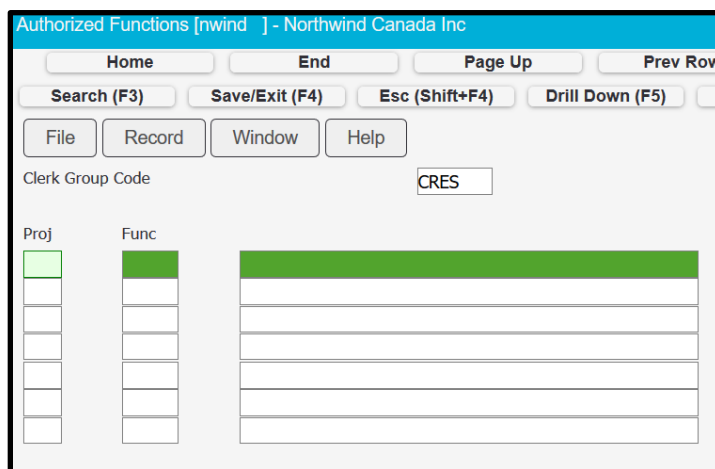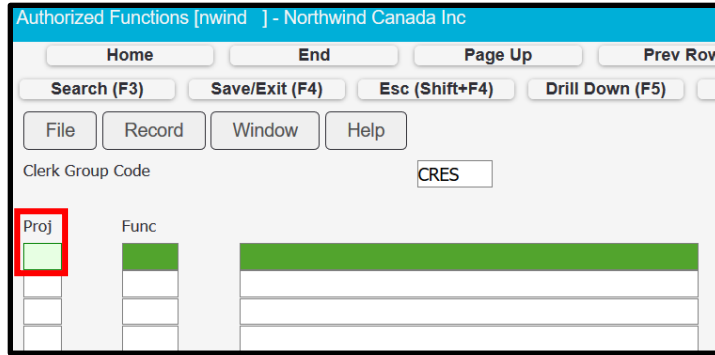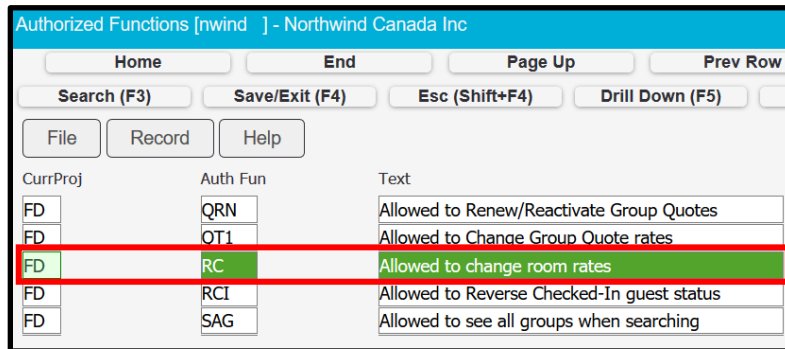
15) Select **OK**
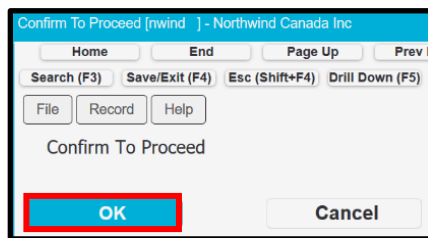
16) Select **OK**

17) All functions for the selected module, have now been removed
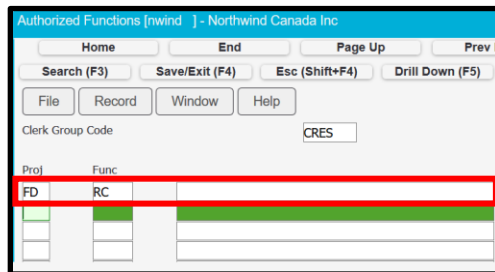

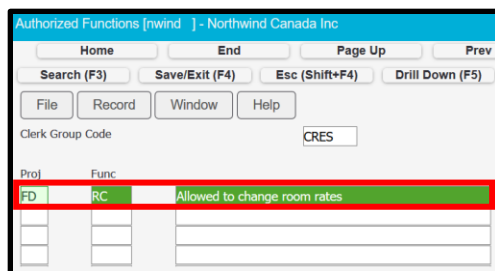18) When assigning a specific authorized function | **Proj** field | **Lookup (F8)**

19) Select **PgUp** or **PgDn** to find the authorized function to add | Press **ENTER** 3x

20) If when returned to the Authorized Functions screen and only the first two columns have populated a value and the 3rd column is missing the function description as shown below


21) Press the **UP**-arrow key on the keyboard and the function description will be displayed | **Save/Exit (F4)** when completed or repeat the above to add more authorized functions
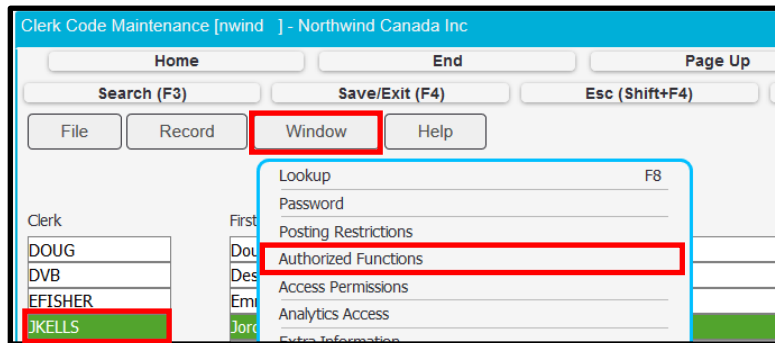
Maestro

4.1.2   Authorized Functions By Individual Clerks

There isn't much difference when assigning authorized functions as the individual clerk level.

1) Log into **Global Maintenance**
2) Select **Security** | Select **Clerk Code Maintenance**
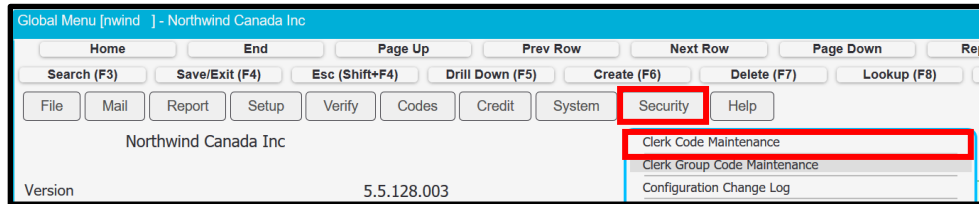
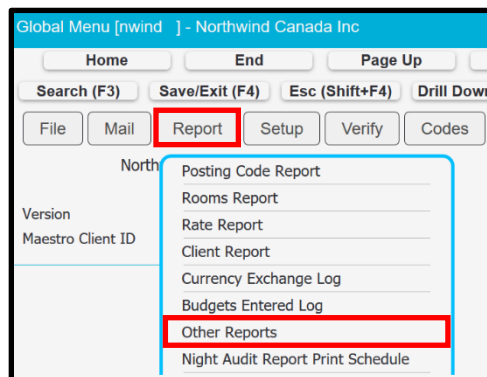3) Select the **Clerk Code** to Modify | Select **Window** | Select **Authorized Functions**

4) Continue the same steps as noted above for assigning Authorized Functions by Clerk Group, whether importing all functions from one module, or only adding specific functions
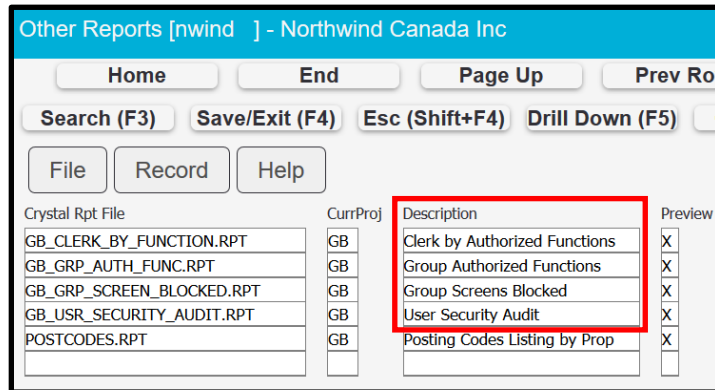
5   User Security Reporting Options

To run a report in Maestro to determine user access by Clerk Group or Individual Clerk, there are multiple reports that can be run.

1) Log into Global Maintenance
2) Select **Report** | Select **Other Reports**

Maestro

3) **Other Reports** | Review the **Description** column which indicates the Report Name

4) Select a report to run | Press **ENTER** | Follow each prompt accordingly

6 Reference Material

6.1.1   Maestro Program Security Codes

Please CLICK HERE for a complete list of all Program Security Codes in Maestro, located on our eLearning website.

6.1.2   Maestro Authorized Function Codes

Please CLICK HERE for a complete list of all Authorize Function Codes in Maestro, located on our eLearning website.