Security Administration Guide

Security Administration

Security administration within Northwind Maestro provides the ability to restrict users to work within certain modules, programs and functions. The following section describes the capabilities of Northwind security and how to set up security to serve your needs. We suggest to start with a simple set-up and add new groups as required. All clerks must be part of one of the groups to have access to the application software.

Security Highlights

- Security may be integrated with Windows 9x/NT/2000/XP/UNIX operating system security to reduce the need for Maestro logins.
- Security may be integrated with Microsoft SQL Server to reduce the need for Maestro logins.
- Security is set up by clerk groups, not by individual clerks, providing an easy method of modifying clerk permissions.
- Clerk access can be limited to certain projects (e.g. Accounts Receivable), modules (e.g. Account
- Receivable Main Menu but not Maintenance Menu) or certain programs within a module (e.g. Client
- Entry in Accounts Receivable Main Menu).

Security Terminology

Clerk (code)

A clerk is defined as an individual person who requires access to the software. Within Maestro, each Clerk Code (eight (8) character field) must be unique.

Clerk Group Code

A four (4) character field used to identify a grouping or category for clerks to be associated with and whose members attain a certain level of access to programs.

Login

Login refers to the action of keying in a Maestro clerk code or operating system user id and password to have the software validate against, and the resulting values of that action.

Password

Within Northwind software, a ten (10) character field used to represent a clerks secret word to protect the clerks login from being used by others. Currently, clerk passwords never expire and can only be changed by the administrator.

Project

Each icon in the Northwind Maestro Program Folder belongs to a project (e.g. Accounts Receivable), and each project typically has two icons (modules), one for the main functions and one for maintenance functions (see Module).

Module

Within each project will typically exist two modules, one for the main function and one for maintenance of that function (e.g. Accounts Receivable Main and Accounts Receivable

Program

Within each module are many programs, each one providing certain capabilities in adding, changing and deleting information from the database. Each program has a system name and a title (e.g. gb1810 = Program Security Maintenance).

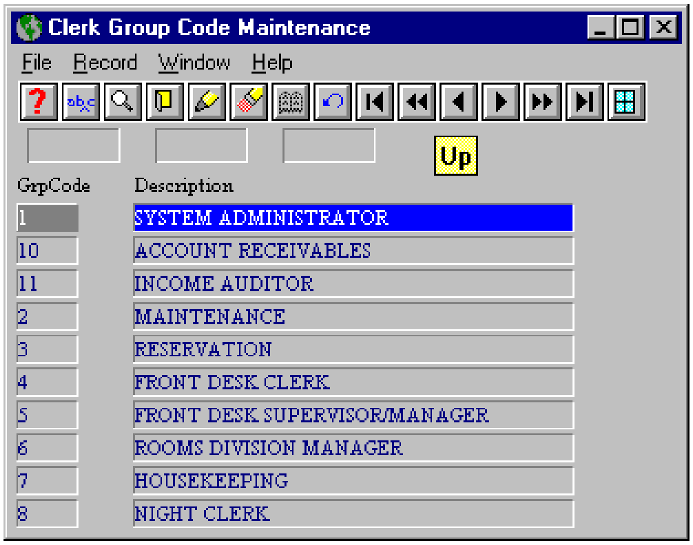
Security Setup

Step 1 - Setting up Clerk Group Codes

Prior to entering the clerk names and passwords, clerk groups must be set up. Clerk groups allow assigning different clerks to a grouping of similar job functions and abilities.

Clerk Group Code Maintenance

- From the *Global menu*, select *Clerk* | *Clerk Group Code Maintenance*
- Press *F6* to create clerk group code



GrpCode	Description
1	SYSTEM ADMINISTRATOR
10	ACCOUNT RECEIVABLES
11	INCOME AUDITOR
2	MAINTENANCE
3	RESERVATION
4	FRONT DESK CLERK
5	FRONT DESK SUPERVISOR/MANAGER
6	ROOMS DIVISION MANAGER
7	HOUSEKEEPING
8	NIGHT CLERK

- Enter a group code (up to 4 characters) to describe a specific group that will have a defined authority level under the *GrpCode* column, press *Ente*r.
- Enter a description for the group code.
- Repeat process until you have entered all the necessary clerk group codes.
- Proceed with Program Security Maintenance.

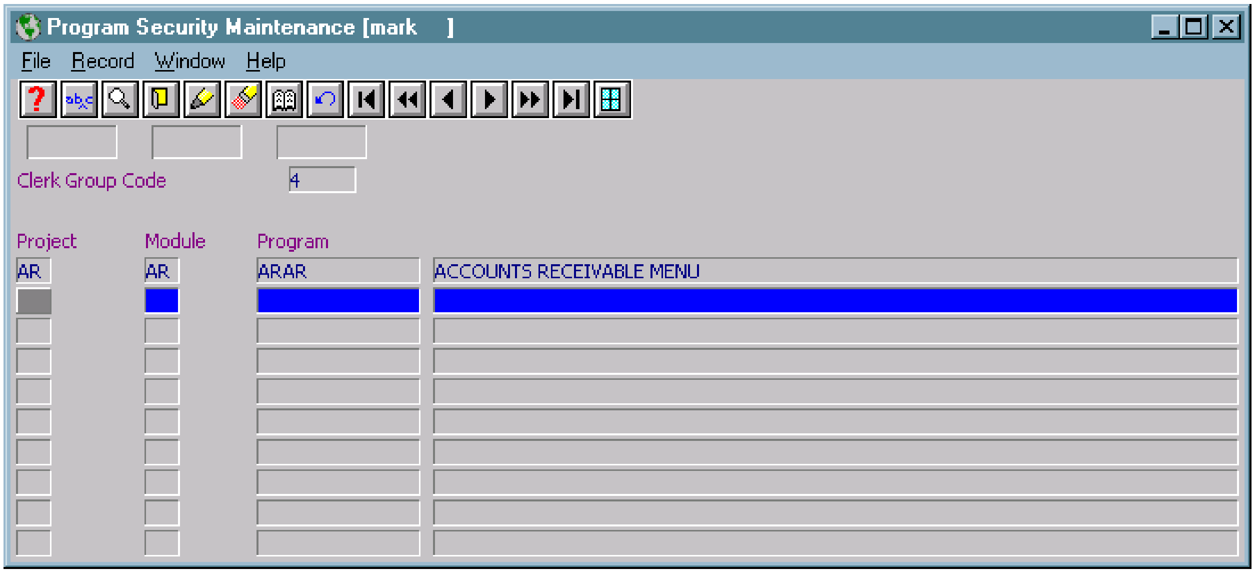
Program Security Maintenance

Program security maintenance specifies the access level a clerk group has to programs within the software.

Considerations

Maestro security works on an exclusionary basis. A clerk group is assumed to have access to projects, modules and programs unless explicitly stated otherwise. Additionally, many programs are called from within other programs, so an overly aggressive approach to program restriction will lead to end-user frustration. The **best** approach is to only exclude "front door" programs – typically menu selections. This prevents unauthorized access without creating the need to list every program related to the primary one.

For example, to prevent access to the Accounts Receivable module, restrict access to the main AR menu - ARAR.



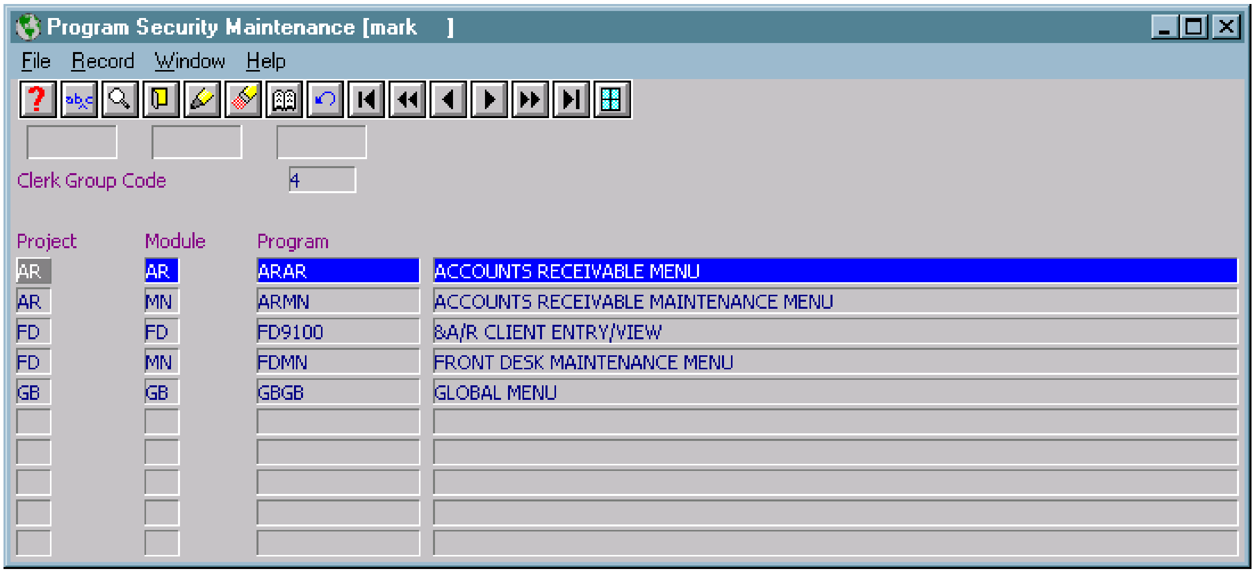
Clerk Group Code: 4

Project	Module	Program	
AR	AR	ARAR	ACCOUNTS RECEIVABLE MENU

Example 1

- Highlight a Group Code line
- Select *Window* | *Program Security*
- Press *F6* to create a program security entry for this clerk group
- Enter the project to which you wish to restrict this clerk group access. Pressing *F8* will display a list of projects from which to choose.
- Enter the module to which you wish to restrict this group from. Pressing *F8* will display a list of modules from which to choose.
- Enter the program to which you wish to deny access. Pressing *F8* will display a list of programs for the project and module previously selected which are valid, with a brief description.

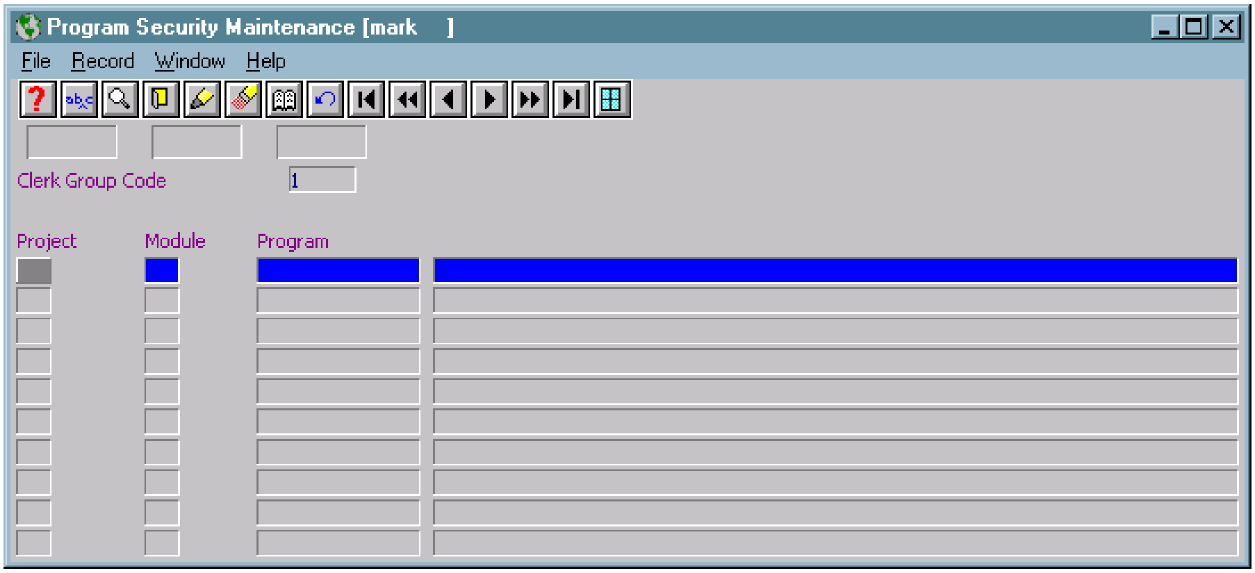
A typical set up for front desk clerks denies them access to Accounts Receivable and its maintenance program, as well as the “AR Client Entry View” Menu option in Front Desk. It can also exclude entry to Front Desk Maintenance and Global Maintenance. The setup for this would be as follows:
.



Clerk Group Code 4

Project	Module	Program	
AR	AR	ARAR	ACCOUNTS RECEIVABLE MENU
AR	MN	ARMN	ACCOUNTS RECEIVABLE MAINTENANCE MENU
FD	FD	FD9100	&A/R CLIENT ENTRY/VIEW
FD	MN	FDMN	FRONT DESK MAINTENANCE MENU
GB	GB	GBGB	GLOBAL MENU

Example 2



Clerk Group Code 1

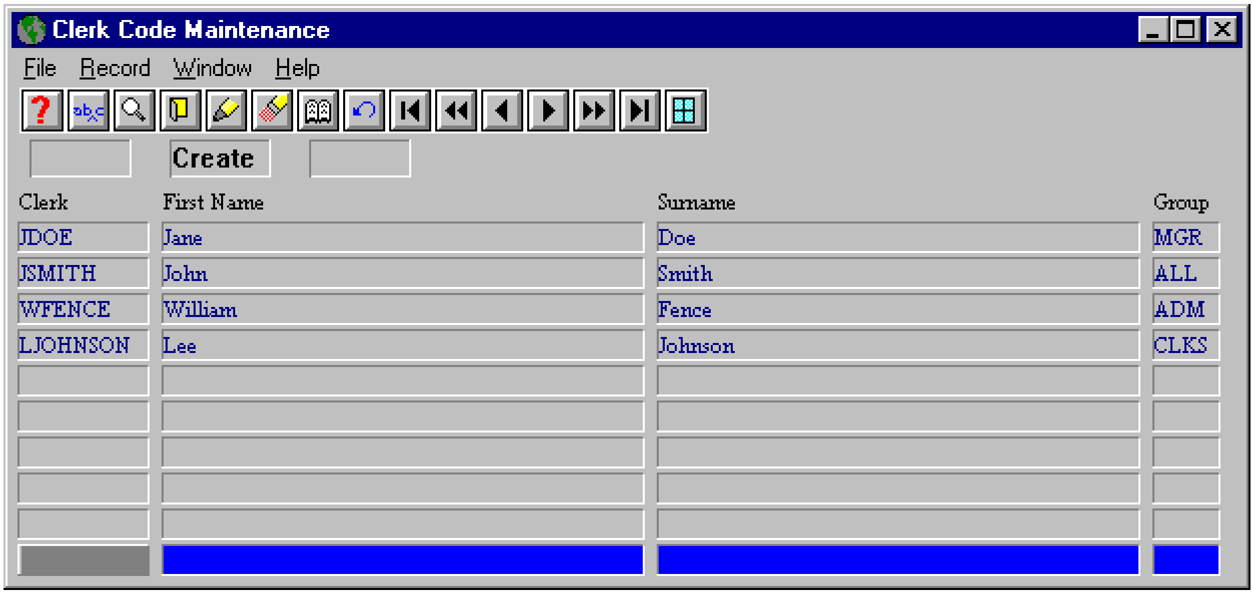
Sample Screen for Full Access 1

Step 2 - Clerk Code Maintenance

Once clerk groups have been established, the individual clerks should be setup.

Clerk Code Maintenance

- From the *Global Menu*, select *Clerk* | *Clerk Code Maintenance*
- Press *F6* to create clerks



Clerk	First Name	Surname	Group
JDOE	Jane	Doe	MGR
JSMITH	John	Smith	ALL
WFENCE	William	Fence	ADM
LJOHNSON	Lee	Johnson	CLKS

Screen Fields	Description
Clerk	Enter a maximum of 8 characters for clerk code
First Name	Enter clerk's first name
Surname	Enter clerk's last name
Group	Enter clerk group, press *F8/Lookup* to display group codes

Entering Clerk Passwords

Clerk passwords are not encrypted any can be read by anyone with access to this program. Clerk passwords never expire and can only be changed by an administrator with access to this program.

- From the *Clerk Code Maintenance*, highlight the clerk you wish to issue a password to.
- Then select *Window* | *Password*; enter up to a 10-character password.
- Press *F4* to exit
- Repeat process for all clerks in the system

Posting Restrictions by Clerk

The system has the ability to assign restricted posting codes that are only available to specified clerks. This may be used for such things as restricting who may provide rebates or discounts.

- From the *Clerk Code Maintenance*, highlight the clerk for whom to create a posting restriction.
- Then select *Window* | *Posting Restrictions*
- Press *F6* to create posting restrictions, pressing *F8* will display a list to choose from.
- Repeat process as necessary, use *F4* to exit.

Note: Posting restrictions will prohibit any user from using the posting codes specified.

Integrating Security with Windows 9X/NT/2000/XP

Security may be integrated with Windows per client workstation. To accomplish this Maestro uses the getusername feature to use the logged in Windows user information. For this to operate correctly, the Maestro clerk code must match the Windows user id exactly. The Maestro clerk password will be ignored as the user will have already logged in through Windows security. To implement this feature, edit the live.ini command file located in the c:\program files\northwind\ directory and search for the “rem_login” entry as shown below:

```
rem_login:
        user getusername
        computer getcomputername
```

Modify “rem_login” to “login” to activate this feature. To deactivate this feature simply change “login” to “rem_login”.

Repeat this step for each client workstation. Please note that if multiple clerks are sharing the same client workstation, using Windows security requires each clerk to log completely out of Windows, prior to the next clerk using the workstation.

Integrating Security With Microsoft SQL Server

Security may be integrated with Microsoft SQL Server per client workstation. To accomplish this Maestro specifies the login information in the live.ini command file under the command heading “odbc_username”. For this to operate correctly, the Maestro “odbc_username” entry must match the MS SQL Server login exactly. To implement this feature, edit the live.ini command file located in the c:\program files\northwind\ directory and search for the “odbc_username” entry as shown below:

```
odbc_username:
        username sa
        password ""
```

Modify the value to the right of “username” to the name of the user. Modify the value to the right of “password” to the users password. For a blank password place two double quotes as shown above with no space between them, otherwise enter the users password without quotes. To deactivate this feature simply change “odbc_username” to “rem_odbc_username”.

Repeat this step for each client workstation or copy the live.ini file to each workstation.

Note: MS SQL Server denies the username and password combination, if it is not accurate. In this condition, a Clerk Login window will be displayed and a login requested manually. The expected username and password in this case will be the users SQL Server login.

NOTE: It is not recommended to use a blank password. Assign the sa user a password and modify the live.ini file as specified above. Alternatively, to avoid using the sa user login, you may establish a Maestro user under MS SQL Server and place that username and password in the live.ini file. Currently, the password is not encrypted in this file, but plans for encryption in an upcoming version are underway.