

9.0 SYSTEM SECURITY

To protect the system against unauthorized online changes being made from the personal computer, AutoMax incorporates three types of security: a keyswitch on the rack Power Supply module, a password, and access levels. Note that access levels need to be considered only if multiple users will need simultaneous access to the same rack.

9.1 Keyswitch

The keyswitch on the rack Power Supply module provides security for online operations such as starting and stopping application tasks by defining a privilege level for the rack. Only online operations accessed through the Online Task Manager option on the Online menu in the Task Manager are affected by the position of the keyswitch. Saving tasks from the rack, however, is permitted regardless of the keyswitch position. The keyswitch has three possible settings: "PROTECT", "SETUP", and "PROGRAM". The AutoMax Executive software displays the current position of the keyswitch on the top of the screen while you are online. See below for a description of the privilege level defined by each keyswitch position.

9.1.1 PROTECT Position

If the keyswitch is in the "PROTECT" position, the user can only monitor variables and save tasks from the rack. Even if the user knows the password (see 9.2), he cannot perform any other operations.

9.1.2 SETUP Position

If the keyswitch is in the "SETUP" position, the user can monitor all variables, and save tasks from the rack only. If the USER knows the password (see 9.2), he can also modify tunable variables. He cannot perform any other operations.

9.1.3 PROGRAM Position

If the keyswitch is in the "PROGRAM" position, the user can perform all online operations from the personal computer, i.e., load, save, run, delete, and stop application tasks, and monitor and tune variables. If, however, the password (see 9.2) has not been entered previously, or is not entered when the user is prompted, the privilege level defaults to that of the "PROTECT" position.

9.2 Password and Access Levels

The password provides an additional level of security for the rack if the keyswitch on the power supply is kept in the “PROGRAM” position. Any online operations beyond what is allowed in the “SETUP” mode of the keyswitch will require the user to enter the password first. The password will time-out after 2 minutes.

Up to four users can access password-protected features in an AutoMax rack via the AutoMax network. See section 12.5 for how to connect to a rack over the network. In order to prevent conflicts, users will be granted one of the following access levels when they go online.

None - This level provides the user with monitoring capability only. The correct password has not been entered by the user.

Data Access - This level provides the user with the ability to Set/Tune/Force only common or I/O variables. Data Access will not be granted when another user has Rack Access. All users connected to a rack may have Data Access. It is the responsibility of all users to coordinate the effect of setting, tuning, or forcing on common variables and other areas of conflict.

Task Access - This level provides the user with the capabilities of Data Access plus the ability to Run/Stop/Delete/Load a task and to modify the local variables in the task using the Set/Tune/Force functions. If the user has Task access to all the tasks in a rack, he can Run/Stop/Delete/Load ALL tasks. Other network users trying to access the task will be denied access and will be shown the username of the user with privileged access. A user may have access to one or more tasks as long as no other user has access to those tasks and no other user has Rack Access.

Rack Access - This level gives the user complete control of all tasks in the rack. A user with this access level can Run/Stop/Delete/Load ALL tasks. Rack Access will not be granted if any other user has Data, Task, or Rack Access.

Users may set their level of access by using the Set Access function from the Connect menu (see 12.2). A specific level of access will be granted (if possible) when the user executes a function which requires that level of access. For example, if a user had previously entered the password and then attempts to force a local variable, Task Access will be granted to the user for the task containing the local data if no other user has access that task. Table 9.1 lists the access levels required to access password-protected features.

Data Access will be granted when the user first enters the password. The user will then be given the opportunity to acquire Rack Access. This will prevent other users from accessing the protected features in the rack. If another user has already reserved the rack, a message will be displayed on the user’s workstation that identifies the other users connected to the rack and their access levels. The user can also display a list of all other users currently logged onto the rack with their associated access levels (see 12.6).

Table 9.1 - Accessing Password-Protected Features

Rack Power Supply Key-switch Position	Any Position	PRO-TECT	SETUP			PROGRAM				
			User's Access Level	None	Any level	Data	Task	Rack	Data	Task
Action										
Force Common	No	No	No	No	No	Yes	Yes	Yes		
Force Local	No	No	No	No	No	No	Yes	Yes		
Force I/O	No	No	No	No	No	Yes	Yes	Yes		
Set Common	No	No	No	No	No	Yes	Yes	Yes		
Set Local	No	No	No	No	No	No	Yes	Yes		
Set I/O	No	No	No	No	No	Yes	Yes	Yes		
Set/Tune Tunable	No	No	No	Yes	Yes	No	Yes	Yes		
Load Normal Config	No	No	No	No	No	No	No	Yes		
Load Debug Config	No	No	No	No	No	No	No	Yes		
Load Single POB File	No	No	No	No	No	No	Yes ¹	Yes		
Load Single Task	No	No	No	No	No	No ²	Yes	Yes		
Delete Task	No	No	No	No	No	No	Yes	Yes		
Start Task	No	No	No	No	No	No	Yes	Yes		
Stop Non-Critical Task	No	No	No	No	No	No	Yes	Yes		
Save Task from Rack	No	Yes ³	No	Yes	Yes	No	Yes	Yes		
Load All POB Files	No	No	No	No	No	No	Yes	Yes		
Load All	No	No	No	No	No	No	No	Yes		
Delete All Tasks	No	No	No	No	No	No	Yes ⁴	Yes		
Start All Tasks	No	No	No	No	No	No	Yes ⁴	Yes		
Stop All Tasks	No	No	No	No	No	No	Yes ⁴	Yes		
Load AutoMax OS	No	No	No	No	No	No	No	Yes		
Load Single UDC OS	No	No	No	No	No	No	Yes ¹	Yes		
Load All UDC OS	No	No	No	No	No	No	Yes ¹	Yes		
Modify PC Task	No	No	No	No	No	No	Yes	Yes		
Auto Run	No	No	No	No	No	Yes	Yes	Yes		
Monitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		

Notes: A user with privileged access may relinquish this privilege by timing out after two minutes offline, or by selecting to relinquish access online. Functions not listed in the table do not require privileged access.

(notes continued on next page)

(Continued)

1. Must have TASK Access to both tasks in UDC.
2. A single task may be loaded with only DATA Access if the task does not already exist on the Processor or UDC module.
3. Requires TASK or RACK Access.
4. Must have TASK Access to all tasks.

As supplied by Reliance, the AutoMax Executive software requires the password "AUTOMAX". To change the password, you must use one of the two methods described below in 9.2.1 and 9.2.2.

The two utilities which can be used to change the password are not installed on the hard disk along with the AutoMax Executive. They reside on disk 1 of the AutoMax software. In order to use either method of changing the password, the user must have access to the original AutoMax installation disks, or the backup copy of those disks.

9.2.1 Changing the Password in the AutoMax Operating System File

This method of changing the password alters the AutoMax operating system file *.OS that is stored with the AutoMax Executive software in subdirectory <DRV>:\RPE\AMX4 on the hard disk, and that is also loaded onto the rack (see 5.4.3 for information about loading the operating system). After changing the password using this method, you need to load, or re-load, the operating system containing the new password into each rack. Note that if you load the Ethernet version of the operating system, you can still use this method of changing the password, i.e., follow the exact same directions below.

Note that you will need to enter the current (old) password in order to load the operating system onto the rack. Follow the steps below to change the password:

1. Access the DOS prompt.
2. Insert disk 1 of the original or backup disks of the AutoMax Executive software into drive A:
3. Type A:PWOS<CR>
4. When the system prompts you for the new password, enter the password you have chosen. You may enter a <CR> as the password. The operator will then be required to enter a <CR> in order to perform the online operations that require the password.

The operating system file with the old password is automatically re-named *.~ OS and the operating system with the new password is named *.OS.

5. When you are finished and back at the DOS prompt, type EXIT<CR>. The start the AutoMax Executive.
6. Load (or re-load, if applicable) the operating system into each rack using the procedure outlined in 5.4.3. When you re-load the operating system, you will be prompted for the password. This password is the current password for the rack, NOT the new password in the operating system that will be loaded onto the rack.

9.2.2 Changing the Password in a Rack

The method outlined below changes the password directly in the AutoMax Processor module without making any changes in the AutoMax Executive software. In order to use this method, the operating system must already be loaded onto the Processor (see 5.4.3). The Processor does not have to be stopped and the operating system does not have to be re-loaded when you use this method to change the password. In addition, to use this method, you do not need to know the current password to change it. Follow the steps below to change the password:

1. Access the DOS prompt.
2. Insert disk 1 of the original or backup disks of the AutoMax Executive software into drive A:
3. Type `A:PWRACK /C=(full pathname to WIN95)\AUTOMAX.INI <CR>`
For example, `A:PWRACK /C=C:\WIN95\AUTOMAX.INI <CR>`
4. When the system prompts you for the new password, enter the password you have chosen. You may enter a `<CR>` for the password. The user will then be required to enter a `<CR>` when performing online menu operations that require the password.
5. When you are finished and back at the DOS prompt, type `EXIT <CR>`. Note that you must exit the DOS session after running PWRACK. Failure to do so may cause problems with serial communication to the rack.

Note that with the above method for changing the password, the edited password file resides only in the AutoMax Processor module(s). The password can not be edited or read from the Processor module(s).