

## Appendix A: Security Access and PublicView

### Security Access Mode

The MX<sup>4</sup> provides administrators with four modes of security access in addition to the login security. Depending on your business and security needs, choose the option best suited to manage your system.

- ☞ Users with admin privileges are always able to access any computers regardless of the mode.
1. **Free Access:** All users have free access to all channels. The only security is the login user name and password—if used. Setting security classes has no effect when this mode is invoked. Free Access is the default setting.
  2. **Exact Match:** The user's security class must be exactly the same as the channel security class in order for the user to access that channel.
    - Example: If both the user class and a channel class are B1, then the user can access that channel; if the user class is any other security class, access will not be allowed in Exact Match security mode.
  3. **2 Digit Level:** The user security class must be higher or equal to the channel security class in order to gain access. **A0 is highest; P9 is lowest.**
    - Example: A user of security class C2 can access all channels with a security class of C2 or lower, but cannot access any channels of security class C1 or higher.
  4. **Level/Group:** Access to a channel is determined by the following rules:  
**A0 is highest; P9 is lowest.**
    - If the letter level (1<sup>st</sup> position) of the user is higher than the letter level of the channel (1<sup>st</sup> position), access is allowed; if the level of the user is lower than the level of the channel, access is denied.
    - If the letter levels are equal, then the group (2<sup>nd</sup> position)—a number—determines access
    - Group 0 (zero) is the universal group: if either the user group or the channel group is 0, access is allowed.
    - Otherwise, the channel group number (2<sup>nd</sup> position) must match the user group number (2<sup>nd</sup> position) in order to gain access.

### PublicView Video Sharing Options

Users of the MX<sup>4</sup> have exclusive control of the computer selected. However, depending on your business needs, the administrator can configure the MX<sup>4</sup> PublicView feature to allow users to view video of a computer controlled by another user. There are 5 PublicView options:

1. **No PublicView:** No video sharing—system default.

2. **Always On:** All users are permitted to view the video of computers being used by other users.
3. **Admin Only:** Only users with administrator privileges are permitted to view the video of computers being used by other users.
4. **User Permit:** User is permitted to view the video of another computer if the user currently in control of that computer has granted permission to do so.
5. **Admin or UP (User Permit):** This is a combination of options 3 and 4.

## PublicView (P-View) Action

When a user is viewing the video of a connected user, there are four optional actions that can be executed when the connected user switches. The viewing user selects the action from the User Profile Menu. The actions are:

- **Do Nothing:** Continue viewing the video of the same computer.
- **Follow User:** Follow the connected user and continue viewing the video of the newly selected computer.
- **Camp-On:** Take control—become the connected user—of the computer that the original connected user has switched away from—unless access is denied due to specific user security.
- **Notify:** Do nothing but display a message when the connected user has switched away.