eKeypad
Mobile Solutions

Setup Guide
eKeypad - Elk C1M1

version 1.0a

Overview
This document describes the process of integrating eKeypad Pro with an Elk M1 Gold or EZ8 panel which is utilizing an Elk-C1M1 dual-path alarm communicator module.

The C1M1 supports connections over both IP and Cellular. Please note that it is possible to configure the C1M1 to only use Cellular pathways. eKeypad is NOT compatible with Cellular only setups; the use of a broadband internet connection for the IP pathway is required.

The sections listed in this document are designed to be performed in the order in which they are listed. It is highly advisable to completely read through this document before you attempt to implement this guide.

This document can not cover every possible scenario you may encounter. Please contact eKeypad and Elk support if necessary. We are here to help.

eKeypad Support

www.ekeypad.net

support@ekeypad.net
214-497-4232

M-F 8am - 6pm (Local Time)
Sa By Appointment
Su Closed

Elk M1 Support

www.elkproducts.com

techsupport@elkproducts.com
800-797-9355 / 828-397-4200

M-F 8am - 6:45pm (EST)
Sa Closed
Su Closed

Hardware Setup

The Elk M1 alarm panel and the C1M1 module are designed and built for long term operation and can reliably run for years unattended. However, the C1M1 module relies on external components to integrate with eKeypad. A number of switches and routers will be responsible for providing the network access for the IP pathway of the C1M1 module. These IP pathway components are not typically built to the same high levels of reliability as the Elk M1and C1M1.

The reliability of these components can be greatly improved with a few enhancements. These changes are highly recommended to ensure a dependable integration with eKeypad.

Router/Switch Power

The key components of the IP pathway includes but is not limited to: ISP modem/router, customer owned router and network switches. These network devices are susceptible to power line fluctuations that can disrupt the IP pathway of the C1M1.

It is recommended to place all of these devices on a UPS (uninterruptible power supply) to protect them from power surges and power outages. It is also recommended to purchase a UPS with a replaceable battery and schedule the battery to be replaced at the same frequency as the Elk M1 batteries.

Cellular Signal Strength

The C1M1 modules contain a cellular modem which serves several purposes, but most importantly, it is integral to the process of establishing connections between eKeypad and the C1M1. It is very important that a usable and stable cellular signal is available.

The Elk C1M1 install guides states, “the C1M1 must be mounted in the enclose with the M1 to meet UL requirements and to provide a secure installation”. It also goes on to state that a cellular strength of 2 on the C1M1 unit is necessary for reliable communications.

For installations where the cellular signal is poor at the M1 enclosure location, a remote antenna should be used in place of the stubby antenna that ships with the unit. The Elk part umber for this remote antenna is ELK-WA003 and allows the antenna to be mounted up to 6 meters (20 feet) from the enclosure.

It is important that the C1M1 has a solid cellular strength of 2. In some scenarios the cellular signal strength can fluctuate over time. This should always be the first item checked if troubleshooting communication issues.

Elk M1 Settings

A key requirement for all installations is to properly configure the Elk M1 Gold using the Elk-RP application software on your computer. Without these options being set properly it can cause a variety of issues ranging from the inability to arm the panel to delayed status updates in eKeypad.

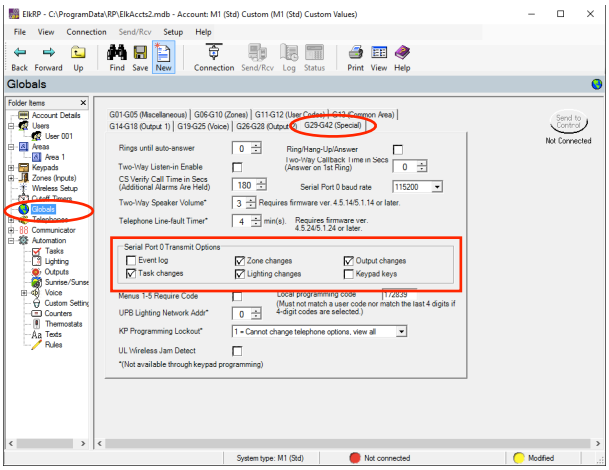
Please note that the following changes will result in a restart of the M1 panel. It is important to remember that the restart process can take from 5 to 10 minutes to complete; be patient. During the early stages of this reboot, attempts to launch eKeypad will result in a “Connection Timeout” error.

It is also important to note that any time the Elk-RP application software is connected to the M1 panel, all other connections will be paused or unavailable. No control commands will be accepted from eKeypad and no status updates will be sent to eKeypad. eKeypad detects these scenarios and will display a special message identifying when Elk-RP is connected and connections are not available.

Serial Port Transmit Options

This option is located by selecting “Globals” from the side menu in Elk-RP then selecting the “G29-G42 (Special)” tab. On this tab you will find a group of six options labeled, “Serial Port 0 Transmit Options”. Only some of these check boxes are checked by default. All six check boxes must be checked and the settings sent to the panel.

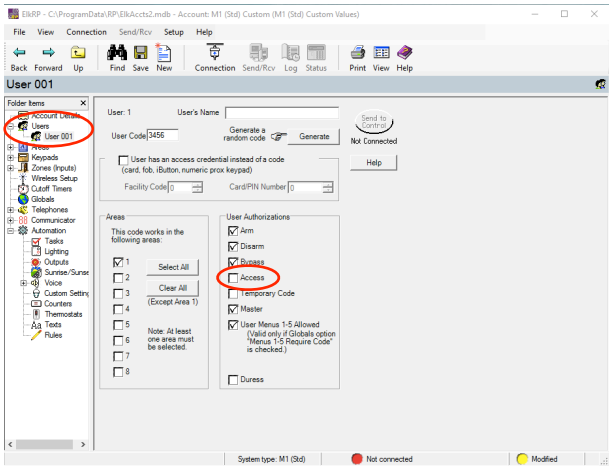
These settings are important. They are necessary for eKeypad to accurately display status. They tell the Elk M1 to proactively inform eKeypad of any changes that occur. Without enabling these items eKeypad will not be informed when changes happen resulting in inaccurate status information.



UserCode Access Feature

This option is located by selecting “Users” from the side menu in the Elk-RP application software then selecting the User Code that is being used in eKeypad.

In the “User Authorizations” group deselect the “Access” feature and send the changes to the panel.



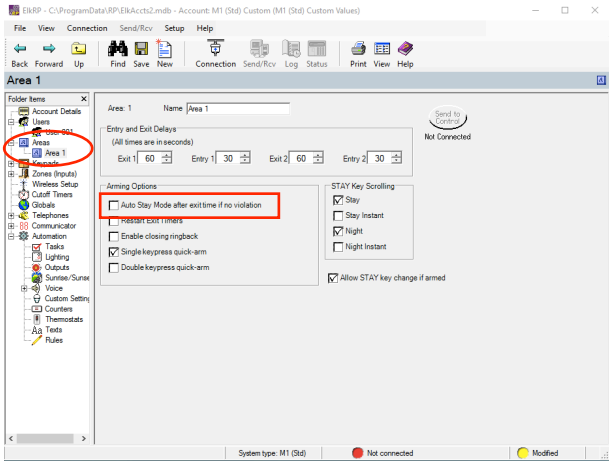
This change needs to be made to **ALL** User Codes that will be used in eKeypad to disarm the alarm. If this feature is enabled it will prevent the panel from being armed from eKeypad.

If you are using the Elk M1 to provide access control and believe this option is required for a given user code, please contact eKeypad support for help.

Auto Stay Arming

This option is located by selection “Areas” from the side menu in the Elk-RP application software then selecting an individual Area.

In the “Arming Options” group deselect the “ Auto Stay Mode after exit time if no violation” feature and send the changes to the panel.



If this feature is enabled, it will automatically change the Away arming mode to Stay mode if none of the perimeter delayed doors are opened during the exit delay countdown time.

This will have the side effect of making it impossible to arm the system into Away mode from eKeypad when not onsite. This feature should be disabled for all areas that will be controlled via eKeypad.

C1M1 Setup

ElkLink Login

As part of the normal setup of the C1M1 module, it must be registered with both Telguard and ElkLink. This process, performed by the installer, is outside of the scope of this document but is well documented by Elk. Please reference these sources to complete the setup of the C1M1 module before attempting to setup eKeypad.

High-level information about the C1M1 module can be found on the Elk web site here: http://www.elkproducts.com/c1m1

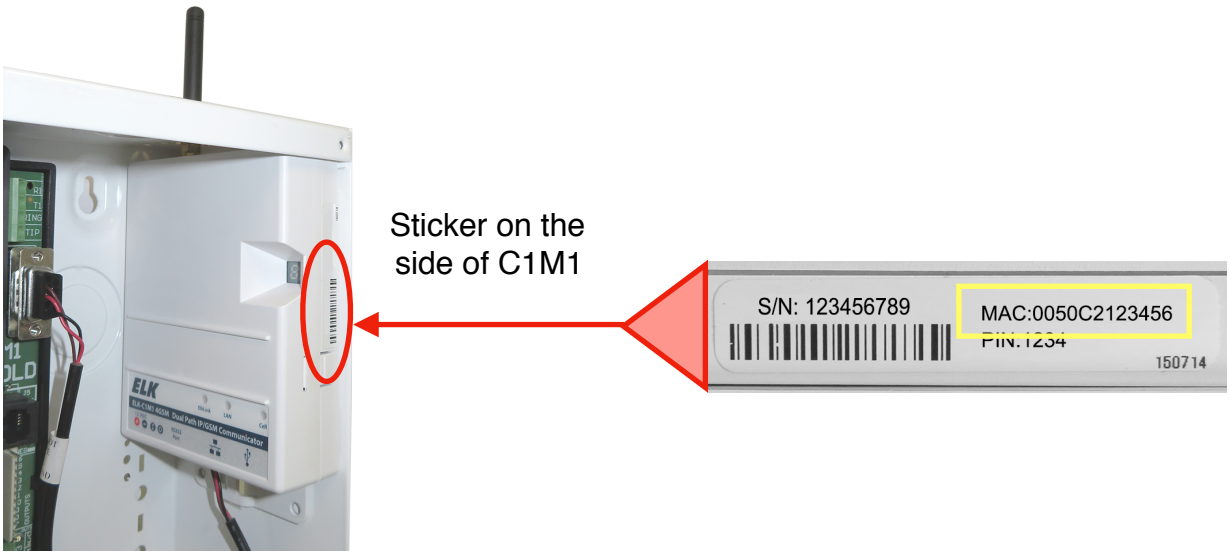
Detailed information on how to setup and troubleshoot the C1M1 Module can be found on Elk's web site here: https://www.elkproducts.com/elklink-help

One of the last steps in the registration and setup process involves the creation of an account for the "End Customer". The Username and Password created by the customer during this step should be documented for use during the setup eKeypad.

The correct login to use in the eKeypad setup is the "End Customer" login. The Telguard Dealer login and the ElkLink Alarm Company login should **NOT** be used in eKeypad.

C1M1 MAC Address

An identifier for the physical C1M1 module will be required as part of the eKeypad setup. This identifier is called the "MAC Address" and it is printed on the side of the physical C1M1 module.



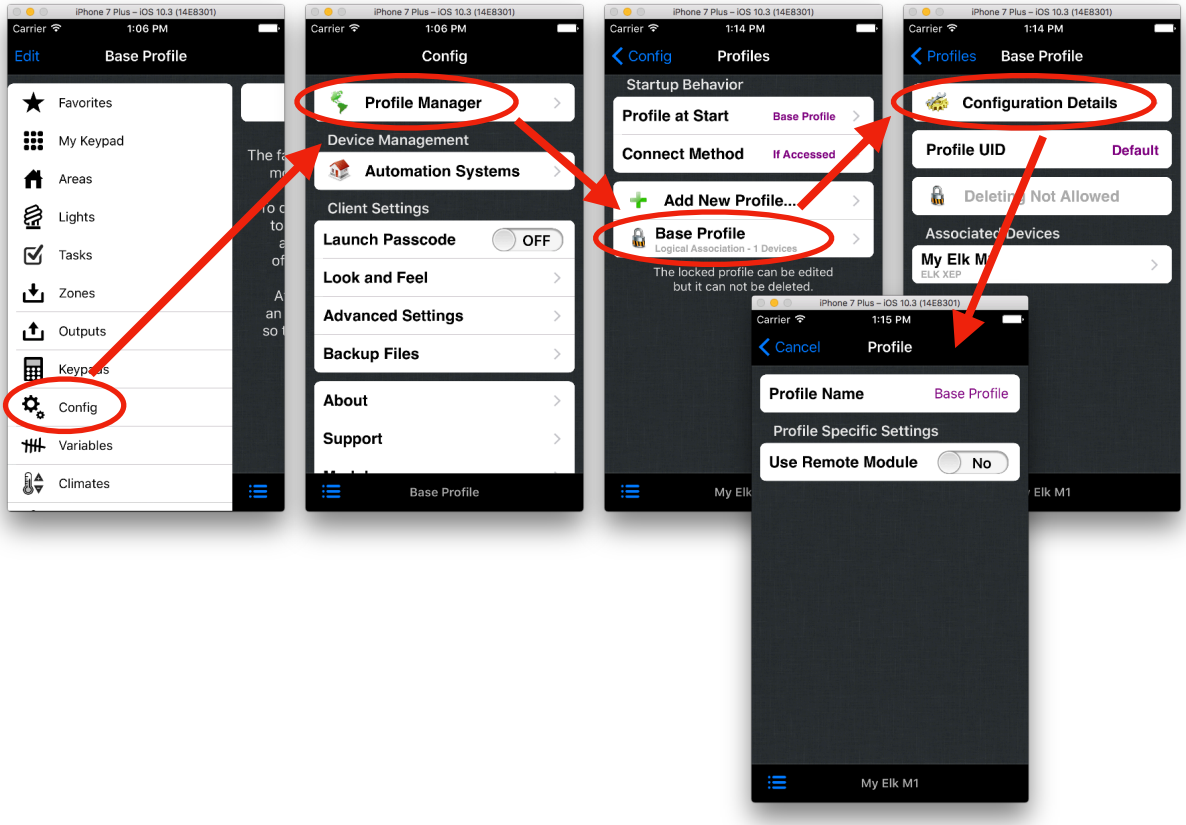
eKeypad Setup

Customize Profile Name

eKeypad contains an advanced function called Profiles that allow complex systems to be organized into smaller groups so the application is easier to use.

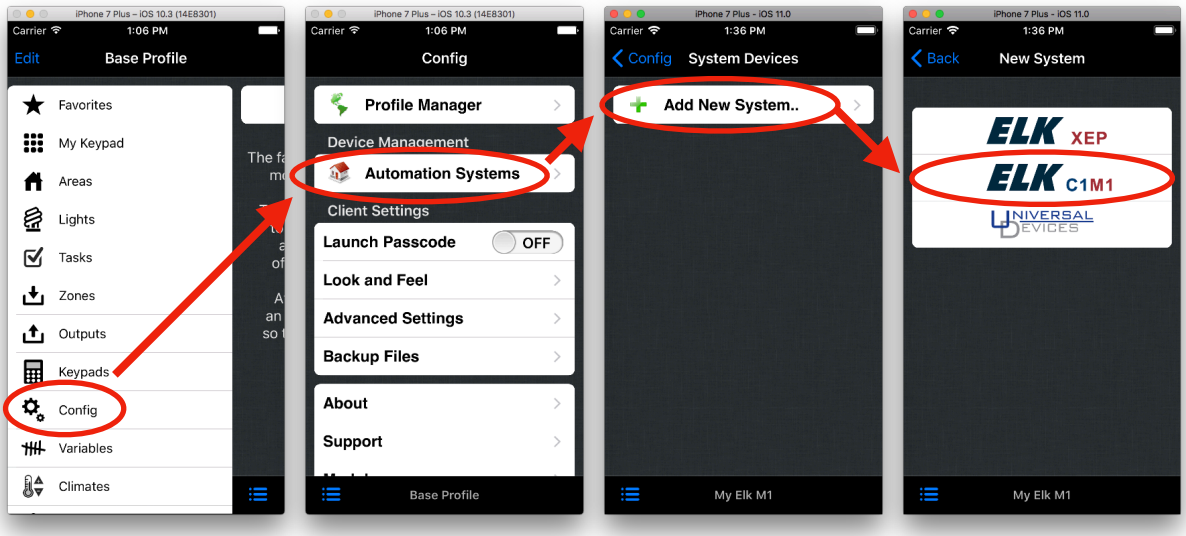
There is one special profile that is always present in eKeypad. By default it has the name “Base Profile”. This name should be updated to something more meaningful as it will be displayed on the application interface.

In eKeypad, open the Config -> “Profile Manager” screen. In the second section you will see the “Base Profile” entry. It can also be identified by the lock symbol on the left side of the row. Touch on this row and select the “Configuration Details” entry. Change the “Profile Name” field as necessary and save the changes using the save button at the top of the screen.



Add Elk C1M1 System

To start the setup of the Elk M1 system by launching eKeypad and dismiss any message that may appear. Next, navigate to the Config screen if it is not already visible. Select the “Automation Systems” link, then the “Add New System...” link and finally choose the “Elk C1M1” entry.



There are a number of settings that need to be entered using the values and information collected in the sections described above in this document. If you have not performed these sections, please go back and do so first. The tasks described in this document are designed to be performed in the order they are listed.

1. Device Name: Each device configured in eKeypad must have a unique name. This field is cosmetic and used it identify the system. Update this field appropriately.
2. C1M1 Proxy: This field is already set to the correct value required for the C1M1. Do not change this unless directed by eKeypad or Elk support.
3. Port Number: This field is already set to the correct value required for the C1M1. Do not change this unless directed by eKeypad or Elk support.
4. MAC Address: This value is found on the side of the physical C1M1 module. It should be exactly 12 digits in length and only contain the number 0-9 and letters A-F. All letters should be entered in upper case.
5. Username: This field should be set to the username which was created during the “End Customer” portion of the C1M1 registration.
6. Password: This field should be set to the password which was created during the “End Customer” portion of the C1M1 registration.

7. Valid UserCode: This is the 4 or 6 digit code used to arm/disarm the Elk M1 panel.

All remaining settings are advanced configuration settings that allow eKeypad behavior to mirror certain Elk M1 configuration settings. Changing these settings is uncommon.

To complete the addition of the new system, scroll back to the top of the screen and press the Save button. The save function will start with a full validation of the values entered. All values will be tested for validity and a test connection over the local network will be made to the system.

Any issues found will display an error message. Read the **full text** of the error message as it will describe in detail the nature of the issue that was found. In most cases the error message will also direct you to where it can be resolved.

Once the initial, local network validation process has completed eKeypad will perform a synchronization of the M1 panel settings. Once completed, eKeypad will require a restart to continue.

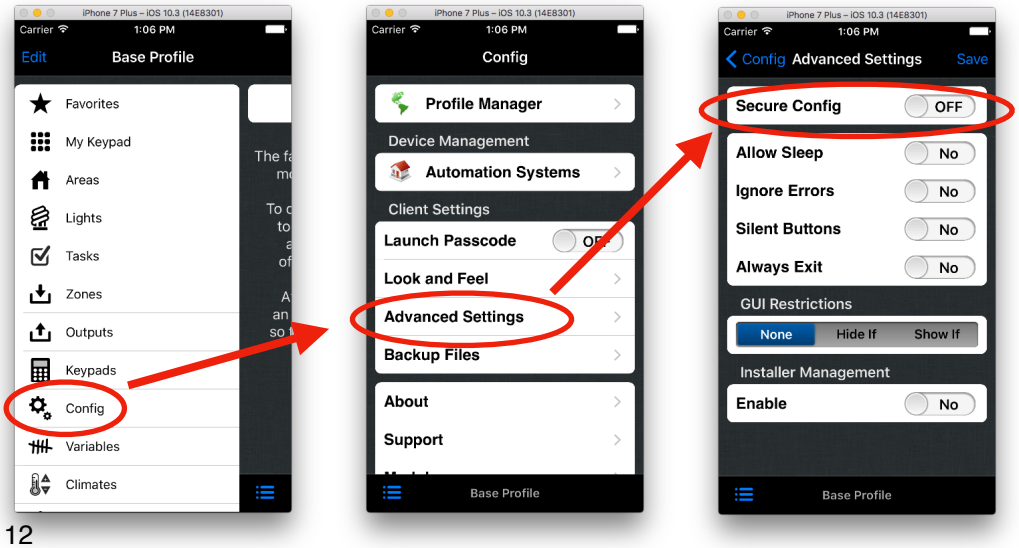
At this point eKeypad is setup, but additional testing must be performed to ensure that everything is working as intended.

Start testing by opening eKeypad and navigating to the “My Keypad” screen. Use this screen to perform two tests: Arm the M1 panel and then subsequently disarm the panel. This test will confirm basic connectivity and communication between eKeypad, C1M1 module and the Elk M1 panel.

Configuration Password

Once the testing of the eKeypad configuration has completed, the configuration settings should be locked down to prevent unintended changes.

Open the Config -> Advanced Settings screen. Turn the “Secure Config” switch to ON.



This will cause a passcode setup screen to appear where you will be asked to enter the passcode, verify the passcode a second time and provide a hint phrase that can be used to recover the passcode. Be sure to store this passcode in a safe place. It is not possible to recover it. If the hint phrase does not help, eKeypad will have to be reset and all settings re-entered manually.

Once setup, any attempt to access the configuration screens within eKeypad will require entering this passcode to proceed.

Configuration Backup

To safeguard the configuration and help manage the setup of secondary or replacement devices a configuration backup should be created.

This can be done on the Config -> “Backup Files” screen in eKeypad. After creating a backup file there are several options for transferring it between copies of eKeypad. The options displayed will vary based on the setup of the iOS device.

- Email. This option will attach the backup file to a normal email message as an attachment. This attachment is encrypted and unreadable without eKeypad.

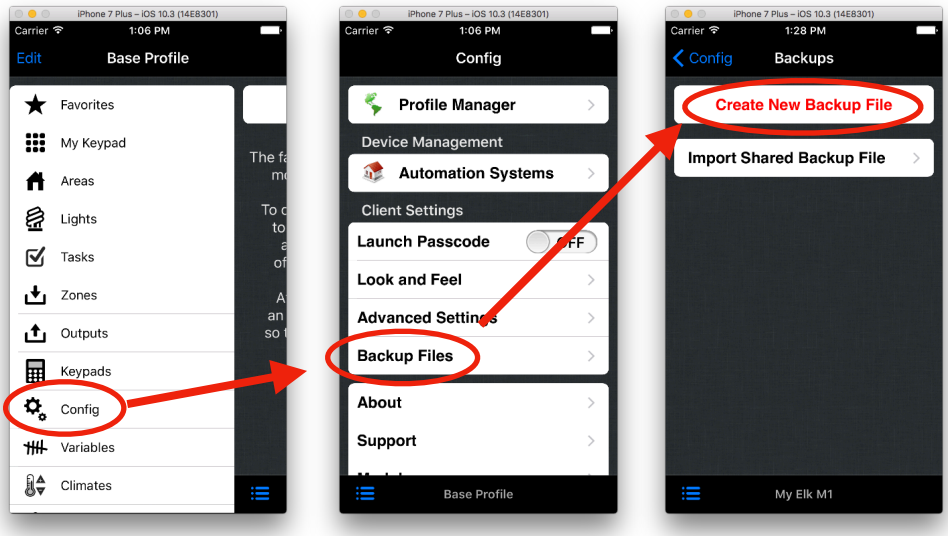
  To restore an emailed backup file, open the email message in the Apple Mail application on the iOS device and touch on the file attachment icon. A list of options will appear, select to open the attachment with eKeypad.

  This will automatically exit Mail, launch eKeypad and import the backup file. Make a point of reading the message window eKeypad displays. To prevent conflicts, the name of the imported backup file may be changed.

- Share. This option will share the backup file on the local Wifi and Ethernet network. Any other copies of eKeypad on this same network will be able to directly download a copy of the backup file. Files can not be transferred across routers.

Open the Config -> “Backup Files” screen in eKeypad and select the backup file to restore it. Restoring a backup file will replace **ALL** existing settings and can not be undone.

Backup files are application specific. Only backup files created eKeypad Pro can restore with a copy of eKeypad Pro. eKeypad Pro can not restore backup files created with any other eKeypad application.



Customization

Every install is unique. It is highly recommended to leverage the customization options available in eKeypad Pro. A detailed walkthrough is outside the scope of this document but an overview is listed below. For more information on customization and restricted access options, please see the “eKeypad Pro Customization” document.

iPhone Interface

Within eKeypad a completed configuration consists of four levels. The Application is eKeypad Pro itself and contains 1 or more Profiles. Each Profile contains 1 or more Devices such as an Elk M1. Each Device contains 1 or more Items such as a light, task or alarm area.

- Application level: These customizations affects everything in eKeypad Pro.
  - Disallow editing of customizations
  - High contrast GUI interface
  - Status indicator colors
  - On/Off switch colorization
  - Highlight colors applied to buttons
  - Silence interface sound effects
  - Global hide/show item filter
- Profile level: These customizations only affects the Profile and associated Devices.
  - Capability names
  - Blueprint interface
  - Favorites screen
  - Initial launch screen
- Device level: These customizations only affects the Device and the items within it.
  - Show/hide capabilities
  - Display items in hierarchy
- Item level: These customization only affects a single Item.
  - Audio alerts
  - Display name
  - Status indicator colors
  - Visible controls
  - Action button labels.

Blueprint Screens
On iPad devices, eKeypad allows for highly customized and fully custom interfaces. This capability is extremely robust and flexible. It allows you to design and build almost any interface you can imagine.

If integrating Blueprint screens on dedicated devices with a C1M1 it is recommended that you contact eKeypad support for guidance. Alternate setups are available that are better suited for permanently installed devices when using a C1M1 module.

You can find more information about creating blueprints here:

- Our YouTube walkthrough videos at www.youtube.com/eKeypad
- The Blueprint overview document at www.ekeypad.net/downloads
- Contact us to schedule a training session.

Restricted Access
To further enhance the security of remote access and wall mounted custom interfaces, a number of options in eKeypad restrictions to be placed on various aspects to control access to, control of and even viewing of items configured in eKeypad Pro.

This includes but is not limited to:

- Require a passcode to launch eKeypad
- Require a passcode to access the configuration screens in eKeypad
- Restrict viewing of IP Video streams
- Restrict the ability to control individual items
- Limit the types of control available for individual items