eKeypad
Mobile Solutions

Reliability Best Practices
eKeypad - Elk M1 XEP

version 1.1a

Overview
This document best describes the requirements and practices that should be used when integrating eKeypad Pro with an Elk M1 Gold or EZ8 alarm and automation panel. By following these guidelines, you will increase the reliability of eKeypad Pro, the M1-XEP module and the network they both require to operate.

If you are using a C1M1 module instead of the XEP, please see the dedicated C1M1 setup guide in the documents section of our web site: http://www.ekeypad.net/

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 these requirements and recommendations.

All of the topics listed in this document should be implemented. The only optional component is whether the external address of the router is managed by a Dynamic DNS or Static IP purchased from the internet provider. See the "Static External Address" section for more information.

At the end of this document is a single page checklist. It provides a convenient place to document key information about the install. Once you are familiar with the content of this document, this checklist also provides a simplified, single page reference to the requirements and practices.

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

Network Setup

Communications between eKeypad Pro and the Elk M1-XEP module occurs over a network. To ensure a reliable solution the local network must meet certain minimum requirements.

Multiple Routers

eKeypad contains a test to help identify this scenario. Start by connecting the mobile device to the local Wifi network. Next, open eKeypad Pro and navigate to the Config -> Support -> “Network Diagnostic Tools” screen. Touch the “Count Routers to Internet” action and view the output in the “Testing results” window.

If more than one router is identified by this test, all extra routers should be disabled or configured to be transparent. The process for setting up a network with multiple routers is outside the scope of this document and not supported.

IPv6 Networks

eKeypad contains a test to help identify this scenario. Start by connecting the mobile device to the local Wifi network. Next, open eKeypad Pro and navigate to the Config -> Support -> “Network Diagnostic Tools” screen. Touch the “List Local IP Address” action and view the output in the “Testing results” window.

Although eKeypad Pro supports IPv6 addressing, the M1-XEP module currently only supports IPv4 addressing. As a result eKeypad Pro requires an IPv4 network to work; IPv6 networks can not be supported.

Most routers provide the ability to disable IPv6 for internal Wifi networks. This option should be used. If disabling IPv6 is not possible, then using a dedicated Wifi access point connected to the same IPv4 network as the M1-XEP module will be required.

Multiple Wifi Networks

It is possible for some Wifi routers and access points to broadcast multiple SSIDs. In some cases not all of these SSIDs will connect to networks capable of accessing the wired network where the Elk M1-XEP is attached.

It is important to make sure you are always connecting to the correct Wifi SSID. It is easy to verify this from within eKeypad. Open the Config -> Status screen. At the top of the screen it will tell you the name of the Wifi SSID the iOS device is currently connected to.

If using permanently mounted iOS devices, such as iPads, it is recommended to use Ethernet instead of Wifi. This option requires requires additional equipment. See the “Ethernet Connectivity” section at the end of this document for more information.

Hardware Setup

The main Elk M1 alarm panel is designed and built for long term operation and can reliably run for years unattended. The M1-XEP module, switches and routers are responsible for providing the network access eKeypad requires to operate. These components providing the network access are not built to the same high levels of reliability as the Elk M1.

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

XEP Power Adapter

The M1-XEP module ships with a power adapter. Unfortunately, this exposes the XEP to any variations that may occur in the AC line power. Power brownouts and surges can affect the operation of the M1-XEP and even damage it.

It is recommended to wire the M1-XEP power adapter to the M1 VAUX power terminals on the lower left corner of the panel. This will isolate the M1-XEP from almost all issues related to line power variations.

The M1-XEP consumes 300ma of 12v DC power. This is well within the limits of the M1 VAUX power terminals but the size of the M1 battery should be re-validated. In some scenarios a larger capacity battery may be required to maintain sufficient runtime during power outages.

XEP Auto-Reboot

The M1-XEP module is a very stable device, but since it is the gateway for all eKeypad communications it does represent a single point of failure. It is recommended to setup the system described below to automatically restart the M1-XEP module periodically.

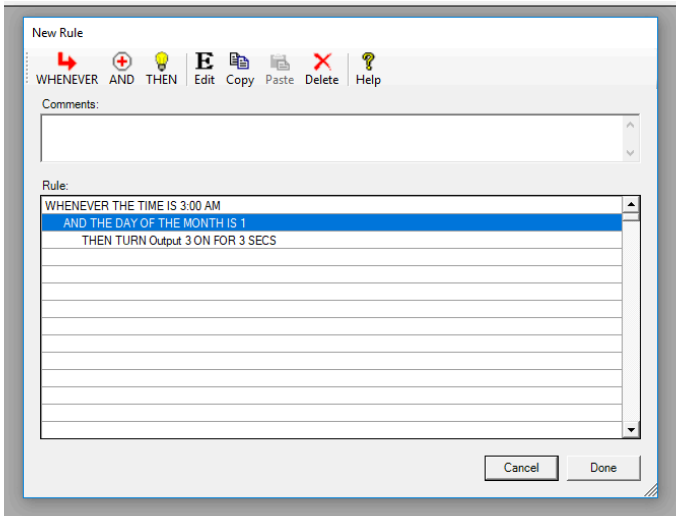
This document describes a solution for a monthly restart. If your scenario requires the restart to occur at a different frequently, please contact eKeypad support for more help.

The M1-XEP module uses 12 volt DC power. As such, the power cable for the XEP contains only two low voltage conductors. Take either one of these conductors and wire it through the Relay Output 3 located on the right side of the Elk M1 panel. Use the Normally Closed (NC) option on the relay.

Next, Use the Elk-RP application software to create an automation rule to manage opening this relay output which will cause the XEP to restart. Be sure to send the changes to the panel when you are done.

- Select “Rules” from the “Automation” section of the side menu in Elk-RP.

1. Add a ‘Whenever’ clause for “Time of Day” with a value of 3am.
2. Add an ‘And’ clause for ‘Date is’ and ‘A Specific Day of the Month’. Set it to when it is equal to a fixed value of 1.
3. Add a ‘Then’ clause to “Turn Output On/Off”. Turn on OUT3 for 3 seconds.



Router/Firewall Setup
Routers connect two or more computer networks together. The job of the router is to direct network traffic to its destination. In contrast, the job of the firewall function of the router is to secure networks by blocking unwanted traffic.

It is important that both the router and firewall are configured correctly. This is described in more detail in other parts of this document but includes:

1. Forwarding port 2601 on the M1-XEP module to the external side of the router.
2. Setting up a DHCP reservation for the static IP Address assigned to the M1-XEP.

The router and firewall are key components in the communications between eKeypad and the Elk M1. The best practices below are focused on increasing the reliability of communications by preventing unplanned or unintentional configuration changes.

- Install a secondary, customer owned router/firewall. It is impossible to prevent changes to the router and firewall if the equipment is owned and managed by the ISP. These changes should be moved to a second router/firewall where access to the configuration can be restricted.
- Disable the firewall function of the ISP provided router. With the addition of a second router, this device no longer needs to act as a firewall. This can be described using different terms but the goal is to transparently forward all traffic to the second router. Common terms for this include, but are not limited to Bridge Mode or DMZ.
- Enter all of the router/firewall configurations necessary to support eKeypad and the Elk M1-XEP into the secondary router/firewall. The only change to the ISP router is to disable it so the secondary router performs all functions.

Router/Switch Power
The key components necessary for eKeypad to connect to the M1 includes but is not limited to: ISP modem/router, customer owned router, network switches and Wifi access points. These network devices are susceptible to the same power line fluctuations that can affect the M1-XEP module.

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.

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.

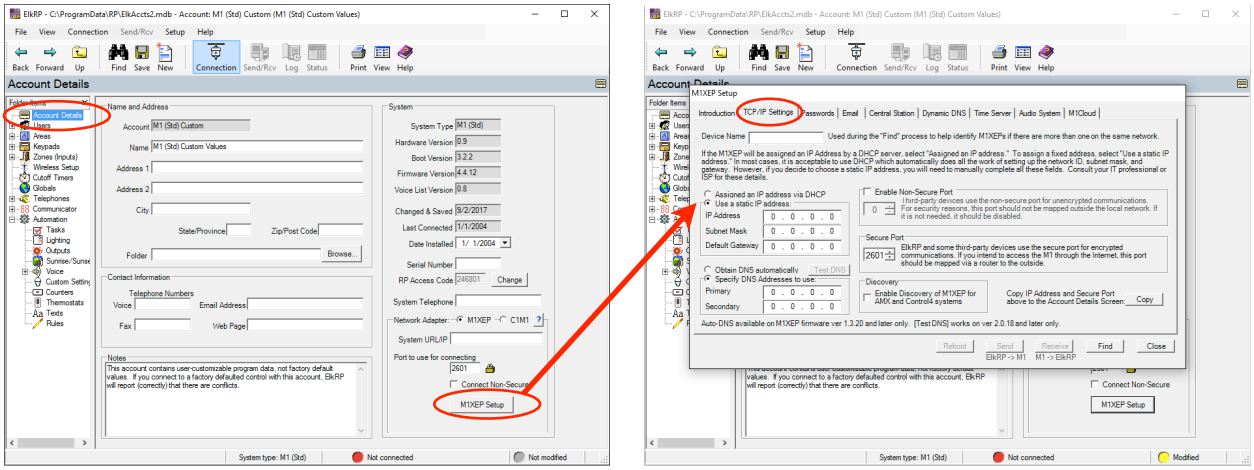
Please note that the following the changes will result in a restart of the M1-XEP module. It is important to remember that the restart process can take from 5 to 10 minutes to complete; be patient. During the early stages of this reboot, attempts to restart eKeypad will result in a “Connection Timeout” error as the M1-XEP module will not be operational.

It is also important to note that any time the Elk-RP application software is connected to the M1-XEP, all other connections will be paused. 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 that Elk-RP is connected. This message will automatically be removed when Elk-RP is disconnected from the M1-XEP.

Assign Static IP Address

By default the M1-XEP module is shipped with the DHCP option enabled. This setup guarantees the IP Address will change in the future causing connection issues in eKeypad. The Elk M1-XEP module must be changed to use a static IP Address. Be sure to send any changes made to the M1-XEP module.

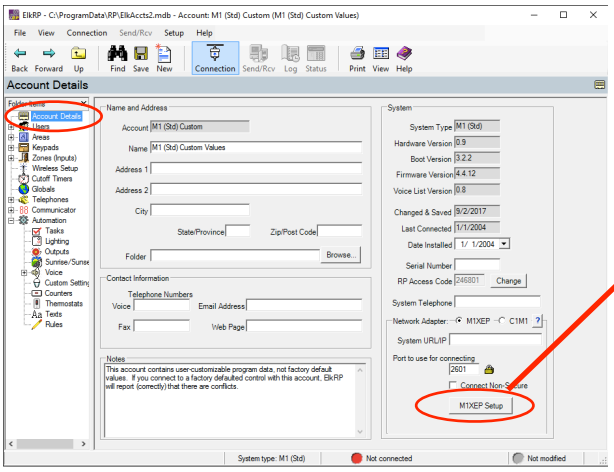
The M1-XEP IP Address settings are located on the “TCP/IP Settings” tab of the “M1XEP Setup” popup window in the Elk-RP application software. This window is opened from the “Account Details” screen using the button in the bottom right corner of the screen.

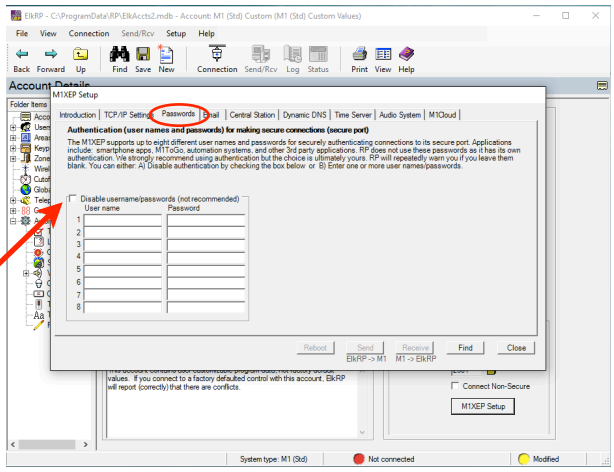


Create XEP Login

This setting is located on the “M1XEP Setup” window which is accessed from the “Account Details” entry in the side menu of the Elk-RP application software. The “M1XEP Setup” window is displayed by using the button in the lower right corner of the screen.

Select the “Passwords” tab and enter a Username/Password pair for use by eKeypad. Both the Username and Password fields are case sensitive and must not contain any spaces. It is also highly recommended to create a unique login that is only used by eKeypad. Be sure to send any changes made to the M1-XEP module.

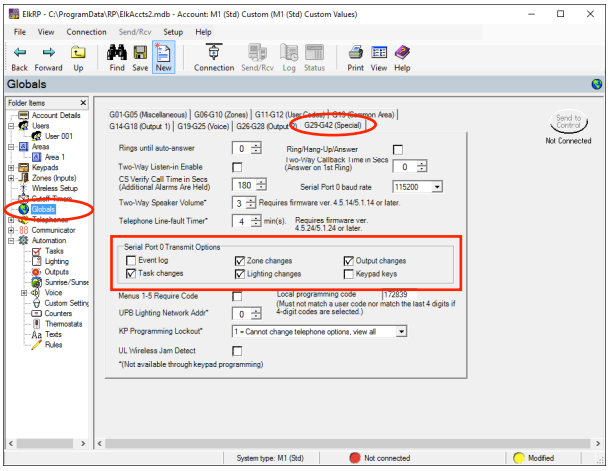




Serial Port Transmit Options

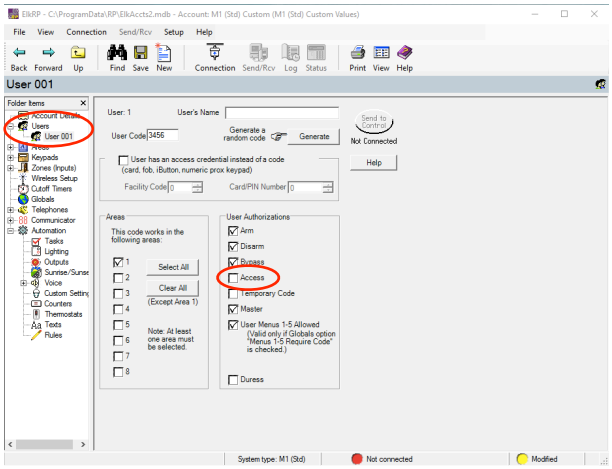
This option is located by selecting “Globals” from the side menu in Elk-RP then selecting the “G29-G42 (Special)” tab. On this tab you will find a group of six options labeled, “Serial Port 0 Transmit Options”. Only some of these check boxes are checked by default. All six check boxes must be checked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

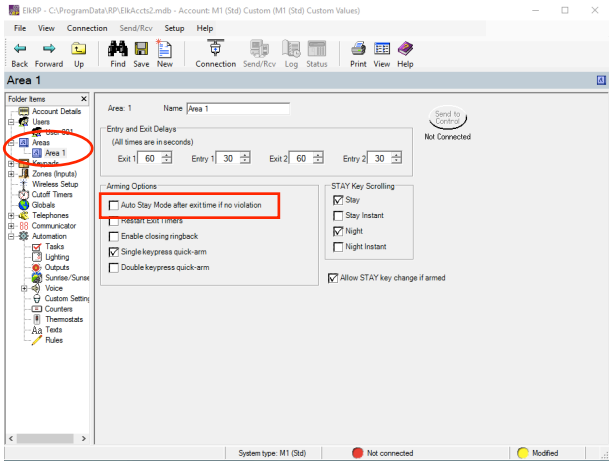


This change needs to be made to **ALL** User Codes that will be used in eKeypad to disarm the alarm. If this feature is enabled it will prevent the panel from being armed from eKeypad.

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.

Router Settings

Create DHCP Reservation
Using the static IP Address assigned to the M1-XEP module earlier, the same IP Address should also be setup as a DHCP reservation in the DHCP server. The DHCP server is often, but not always, located in the router.

This is an important step that should not be skipped. Both setting a static address in the XEP and reserving the same IP Address in the DHCP server are necessary to ensure reliable communications.

Setup Port Forwarding
The firewall functionality in the router is designed to block unwanted traffic. However, for eKeypad to remotely access the M1-XEP some traffic must not be blocked.

This requirement is **ONLY** needed when eKeypad will be connecting from outside the local network. If remote access is not required, port forwarding should not be setup.

This process uses the port forwarding functionality found in the router. Only TCP traffic and traffic on port 2601 need to be forwarded. The setup of the port forwarding entry will also request the static IP Address of the M1-XEP you assigned earlier.

Static External Address
The external IP Address (also called the WAN address) of the router is assigned by the internet service provider. By default it will be dynamically assigned using DHCP.

This requirement is **ONLY** needed when eKeypad will be connecting from outside the local network. If remote access is not required, this section is not need.

If remote access will be needed, the dynamically assigned WAN address must be addressed to maintain reliability. There are two options, but you only need to use one of them. Whichever option is used, the remote address will be needed during the eKeypad setup described later in this document. This value will be required for the “Failover Address” field.

1. Purchase a static IP Address. This is the most reliable option, but it can also be more complex to setup. Not all internet service providers offer this service. Research is recommended as some internet providers may also charge overpriced fees and/or require hardware changes.

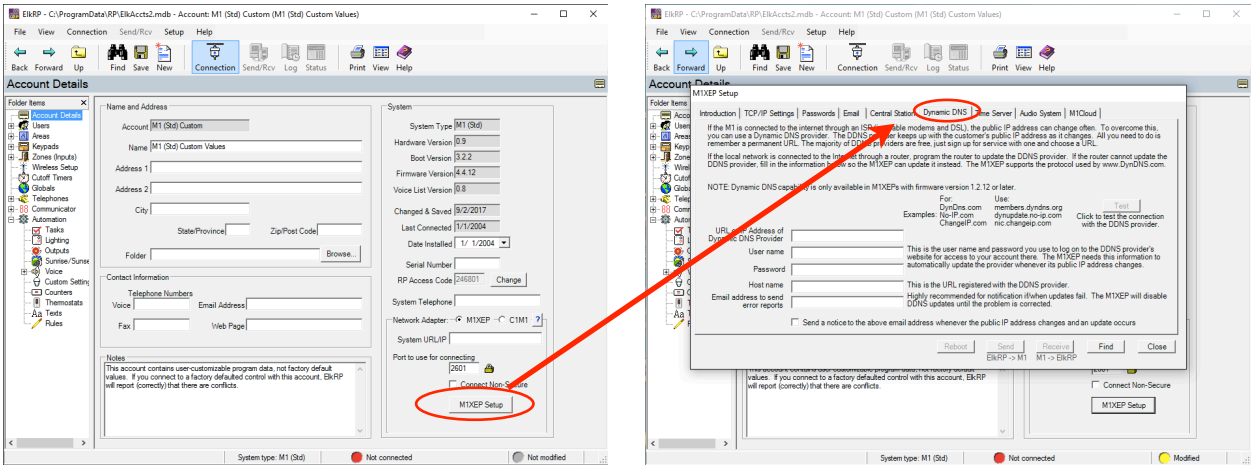
2. Setup a Dynamic DNS (DDNS) hostname service with www.dyndns.org. This option is the easy to setup but introduces additional dependencies on the internet connection. The use of DNS hostnames will require the use of DNS servers located

on the internet. Using a DDNS service is the most commonly used option for dealing with the External IP.

The setup of the DDNS account should always be done as early in the setup process as possible. It is recommended to perform the account setup at least one day before the rest of this document to make sure it has time to be fully setup.

After setting up the DDNS account, the Elk M1-XEP module must also be configured with the account details. The XEP module will monitor the external IP of the router for changes and updates the DDNS account as needed.

These details are located on “Dynamic DNS” tab of the the “M1XEP Setup” window which is accessed from the “Account Details” entry in the side menu of the Elk-RP application software. The “M1XEP Setup” window is displayed by using the button in the lower right corner of the screen. Be sure to send any changes made to the M1-XEP module.



Always test the DDNS settings entered into the XEP. Proper operation is very important.

eKeypad Setup

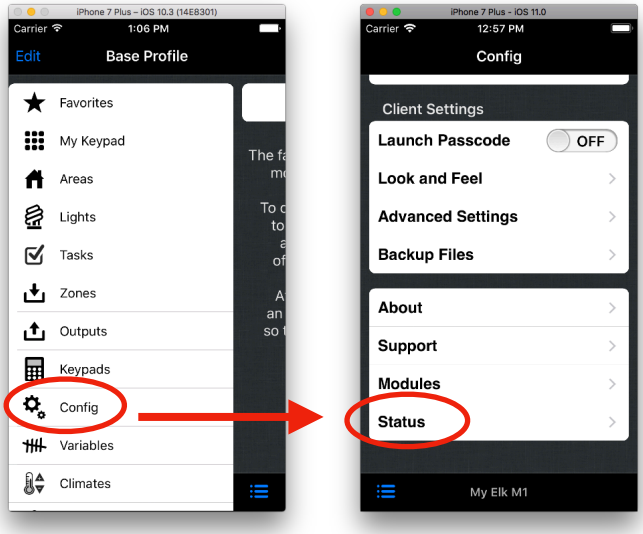
Check Network Connection

The most common method of connecting iOS devices to the local network is by using Wifi. However, some routers and access points broadcast multiple SSIDs where not all of them are able to connect to the Elk M1. You must make sure the iOS device running eKeypad is connected to the correct SSID before starting the setup process.

You can quickly check basic Wifi vs Cellular connectivity by looking at the icons in the top left corner of the iOS device screen. If you see the following icon, then the device is connected to a Wifi network.

For a more comprehensive check use the Config -> Status screen in eKeypad. At the top of the status screen the network connectivity will be displayed.

It will tell you how the iOS device is connected to the network: “No Network”, “Ethernet”, “Cellular Data”, or “Wifi”. If using Wifi, the name of the SSID will also be provided.



The local IP Address assigned to the IOS device will also be displayed. Be sure to verify that eKeypad is displaying an IPv4 address. For proper operation it must not be IPv6.

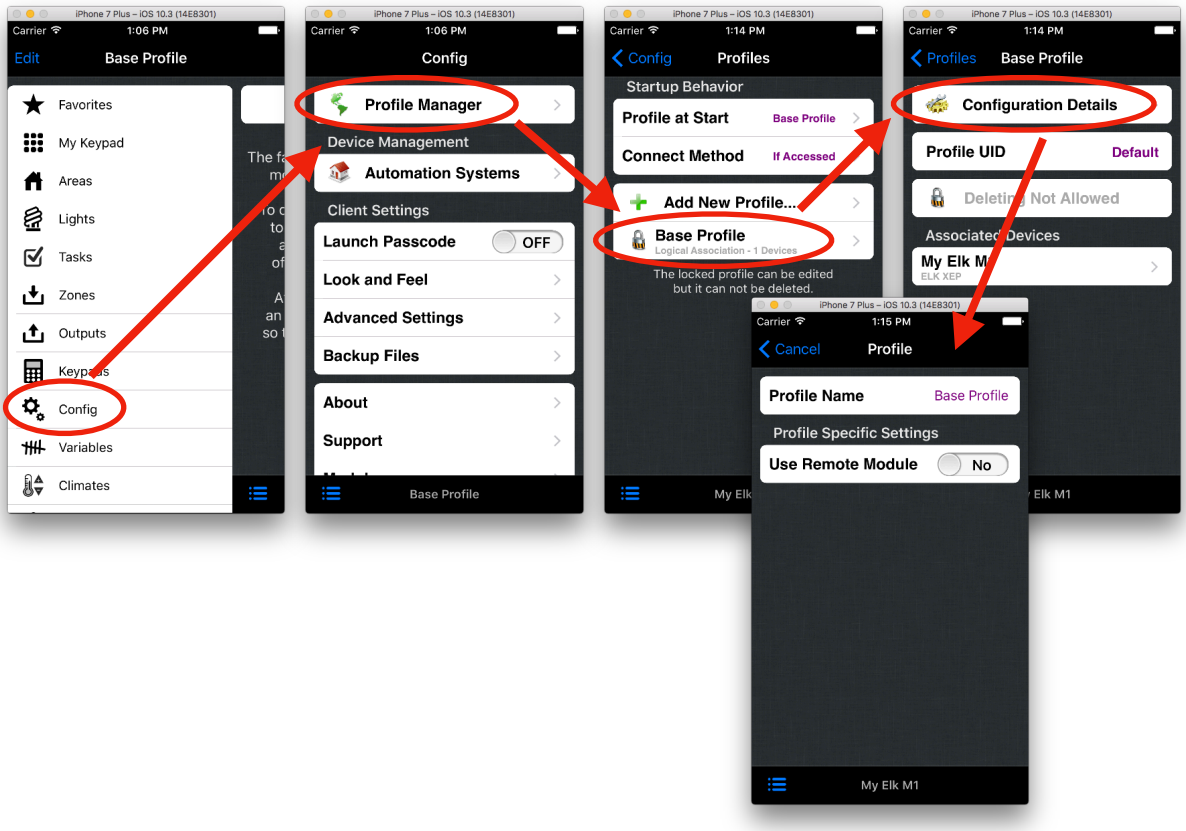
- An IPv4 Address can be identified by pattern: 4 numbers between 0 and 254, separated by periods. It can not contain any letters. For example, “192.168.10.55”.
- An IPv6 Address can be identified by the pattern multiple number and/or letter values separated by colons. For example, “1080::8:800:200C:417A”.

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.

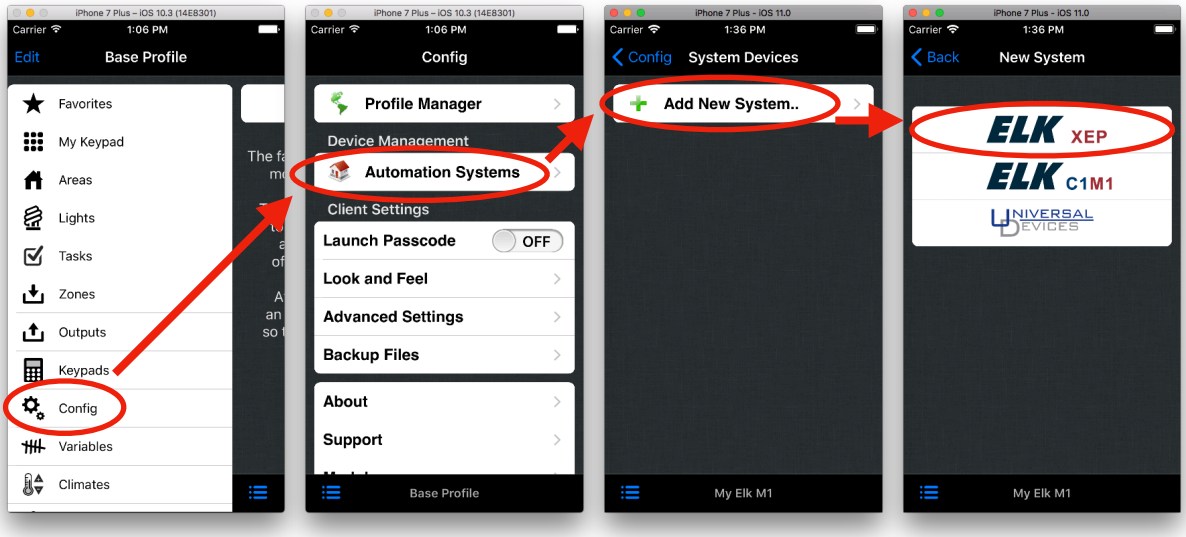
In eKeypad, open the Config -> “Profile Manager” screen. In the second section you will see the “Base Profile” entry. It can also be identified by the lock symbol on the left side of the row. Touch on this row and select the “Configuration Details” entry. Change the “Profile Name” field as necessary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



Add Elk M1 System

Make sure the iOS device is connected to the correct local Wifi or Ethernet network before continuing. This is **necessary** to properly test the setup of eKeypad. Please see the "Multiple Wifi Networks" and "Check Network Connection" sections earlier in this document for more information.

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 XEP" 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 section, please go back and do so first. The tasks described in this document are designed to be performed in the order 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. Network Address: This field should be set to the internal, static IP Address assigned to the M1-XEP module in the "Assign M1-XEP a Static IP Address" section earlier in this document.
3. Port Number: This field should normally be set to the secure port of the M1-XEP module. By default this port has a value of 2601, but it can be changed. Be sure to use the value listed on the "TCP/IP Settings" tab of the "M1XEP Setup" popup window in the Elk-RP application software. See the "Permanent Installs" section below for more information.

4. Use Failover: This switch must be set based on how eKeypad will be used. If configuring for remote access, it must be turned ON. If configuring for local network access only, it should be turned OFF.

5. Failover Address: This field is only visible if the “Use Failover” switch above is ON and is only needed for remote access. This field should be the IP Address or Hostname you setup in the “Static External IP” section earlier in this document.

6. Failover Port: This field is only visible if the “Use Failover” switch above is ON and is only needed for remote access. This field must be the same value used in the “Port Number” field above.

7. Port is Secure: This switch must be set based on which port eKeypad will connect to on the M1-XEP module. If connecting to the secure port, this field must be turned ON. If connecting to the non-secure port, this field must be turned OFF.

8. Login is Required: This switch is only visible if the “Port is Secure” switch is turned ON. This setting must match the setup of the “Passwords” tab of the “M1XEP Setup” window in the Elk-RP application software. See the “Create XEP Login” section earlier in this document for more detail.

9. Port Username: This field is only visible if the “Login is Required” switch is turned ON. This field should be set to one of the Usernames defined on the “Passwords” tab of the “M1XEP Setup” window. See the “Create XEP Login” section for more information.

10. Port Password: This field is only visible if the “Login is Required” switch is turned ON. This field should be set to one of the Passwords defined on the “Passwords” tab of the “M1XEP Setup” window in the Elk-RP application software. See the “Create XEP Login” section for more information.

11. 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 over the local network.

Testing Remote Access

If setting eKeypad up for remote access, additional test are necessary. The testing steps up to this point have all occurred on the local network. These additional tests must occur on Cellular data or a remote Wifi network.

Start by exiting out of the eKeypad application to the iOS home screen and unplugging any cables connected to the iOS device.

Next you need to temporarily disable Wifi on the iOS device.

1. Swipe up from the bottom of the screen to expose the iOS control panel. The look of this control panel will vary, but the icon will be the same.

2. Disable Wifi. The icon is blue when enabled and gray when disabled.
3. Swipe the control panel screen down and off of the screen.

Once the connection to the local network has been disabled, the iOS device will either be using cellular data or it will have no network connection at all. To determine which, start by looking at the top left corner of the screen.

If you have a cellular connection you will see a carrier name such as AT&T, Verizon, etc.

Make sure you have at least 2 bars in the meter to the left of the carriers name. If you have less than 2 bars will need to move the mobile device to a location with a stronger cellular signal.

If you have a cellular capable device, but no cellular service is available you will see the text “No Service”. You will need to move to another location or possibly outside of the building to obtain a cellular signal/service.

If you are unable to obtain a working cellular signal, you may need to perform the remaining tests on a remote Wifi network or use a cellular hotspot. A working connection is required to complete the remote access testing.

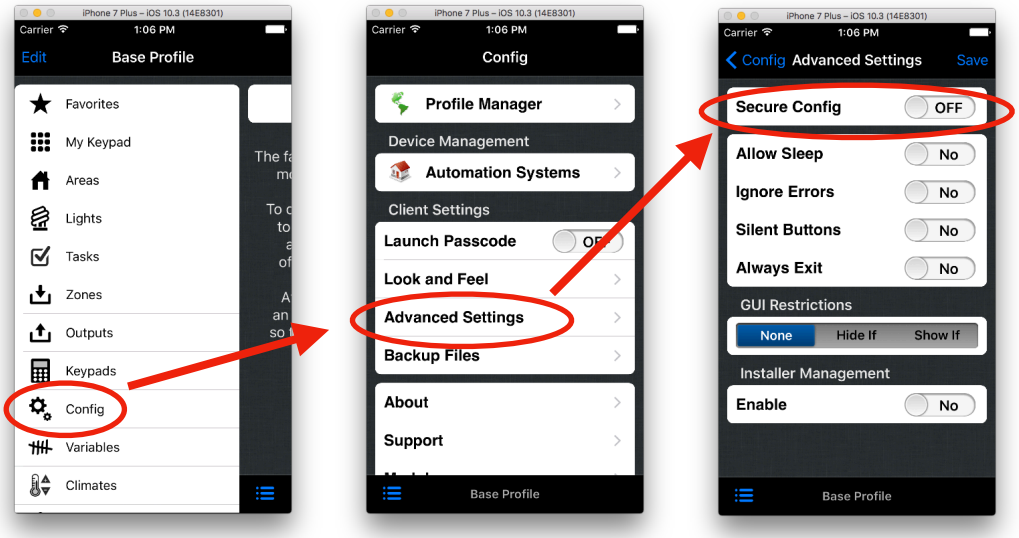
Once you have a working connection that is not on the local network, relaunch eKeypad and navigate back to the same “My Keypad” screen using in the first test. Perform the same arming and disarming tests again to verify that everything is operating.

Once you are finished with the remote access testing, be sure and re-enable the Wifi on the iOS device by following the same directions above that disabled Wifi.

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.

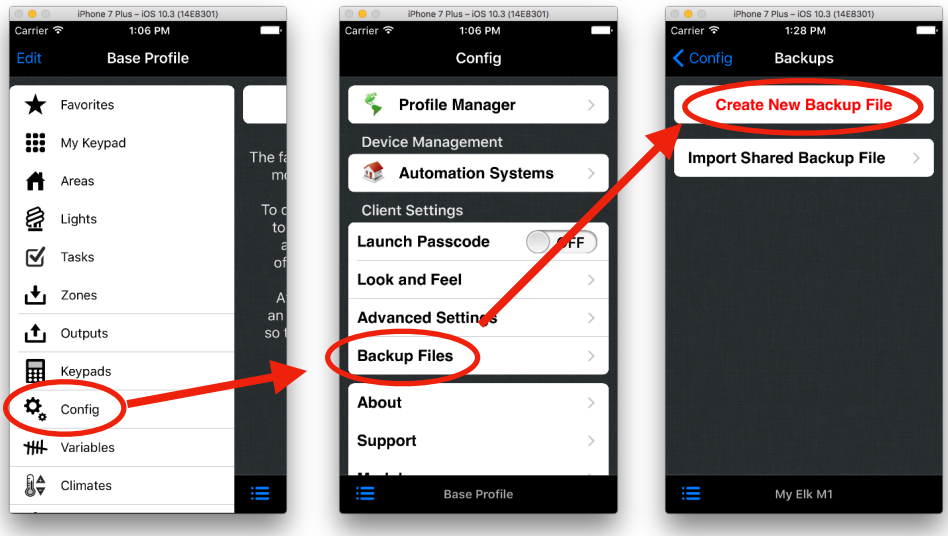
  To restore an emailed backup file, open the email message in the Apple Mail application on the iOS device and touch on the file attachment icon. A list of options will appear, select to open the attachment with eKeypad.

  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.

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:

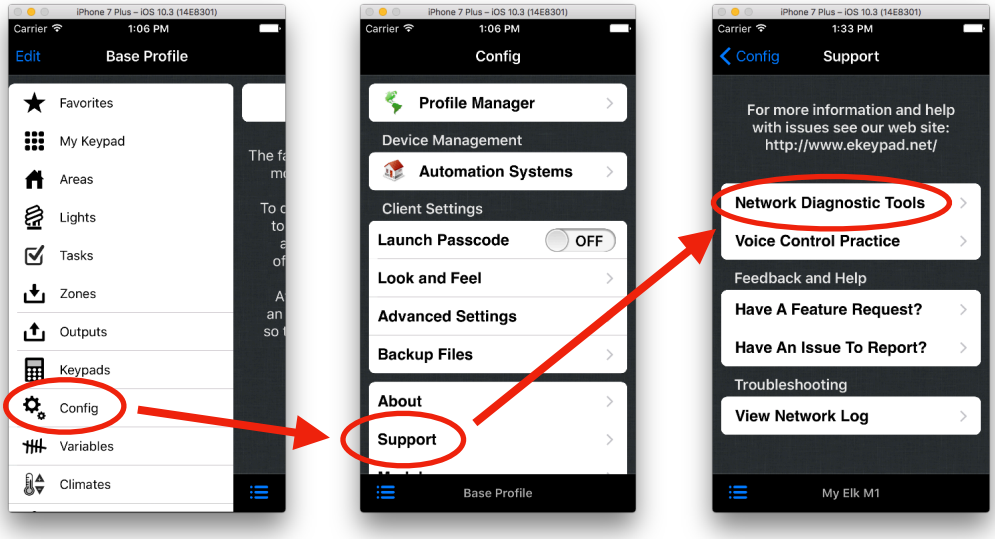
- Require a passcode to launch eKeypad
- Require a passcode to access the configuration screens in eKeypad
- Restrict viewing of IP Video streams
- Restrict the ability to control individual items
- Limit the types of control available for individual items

eKeypad Builtin Network Tools

eKeypad contains a number of useful tools and self diagnostic abilities to help you identify issues that may arise.

NetworkTools

These tools are located on the Config -> Support -> “Network Diagnostic Tools” screen. Not all tools require the use the Address and Port fields at the top of the screen. The descriptions below will list the testing actions that require use of the fields at the top of the screen. All tests support both IPv4 and IPv6 address unless specified otherwise.



- **Resolve Hostname**. By entering a hostname in the “Address” field at the top of the screen, this action will resolved the hostname into its IP Address.
- **Ping Network Address**. By entering a hostname or IP Address in the “Address” field at the top of the screen, this action will attempt to send 3 ICMP pings to the address. This action supports both IPv4 and IPv6 address. This will verify that the device is responding.

  A number of routers block ICMP traffic by default. Realistically, means this usually makes the ping action only useful for devices on the local network.
- **Query Public IP Address**. This action does not require the use of the fields at the top of the screen. This action will list the current IP Address assigned to the external side of the router.
- **List Local IP Address**. This action does not require the use of the fields at the top of the screen. This action will list the IP Address assigned to the mobile device.

- **List Interface Config**. This action does not require the fields at the top of the screen. This action will list the network interfaces setup on the mobile device.
- **Display Network Status**. This action does not require the fields at the top of the screen. This action will detect how the mobile device is making network connections. Options are Cellular, Wifi, Ethernet or None. If Wifi is detected the SSID will also be displayed.
- **Check Port Status**. This action requires the use of both the “Address” and “Port” fields at the top of the screen. This action will test remote connections. The results will be accurate even if connected to the local Wifi network.
- **Count Routers to Internet**. This action does not require the fields at the top of the screen. This action will detect the routers on the network between the mobile device and the internet. Note that some routers can not be detected. This action uses ICMP packets which are blocked by some routers.
- **List Default Gateway**. This action does not require the fields at the top of the screen. This action will list the default gateway being used by the mobile device. Note that this action only applies to IPv4 networks. Networks using IPv6 do not use the concept of a default gateway.

Dynamic DNS

At the bottom of the “Network Diagnostic Tools” screen is a section that allows you to perform a manual, one-time update of a dynamic DNS account. This form only support accounts provided by www.dyndns.org.

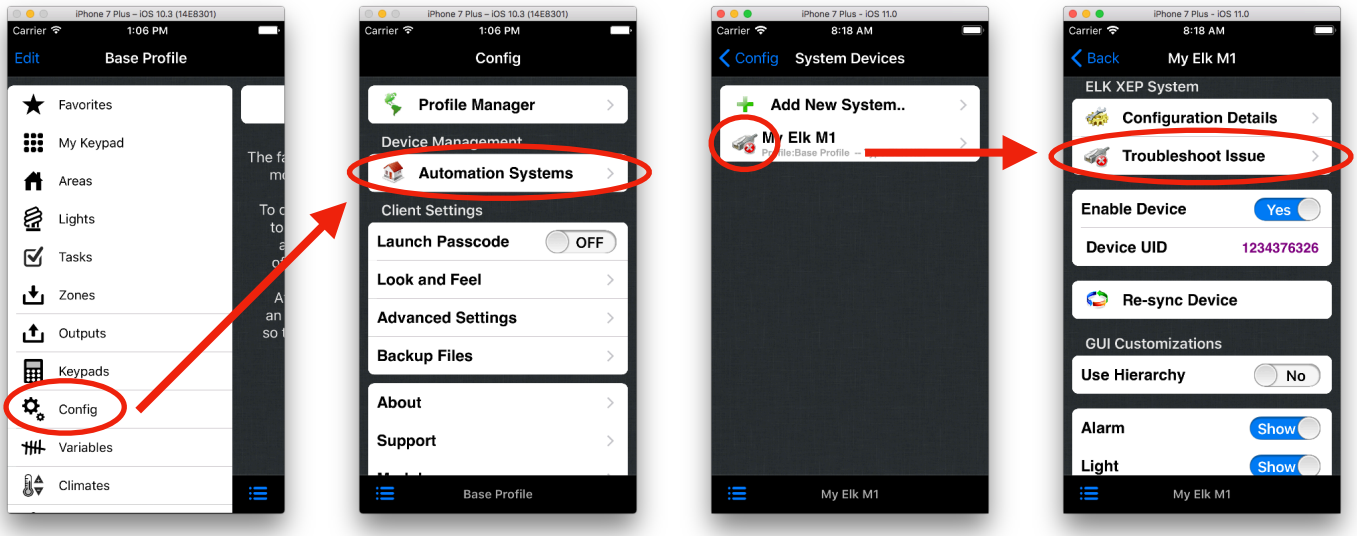
This functionality requires the mobile device to be located on the local wifi network with the equipment to operate correctly. It does **NOT** provide a replacement for the full time client needed to mange the Dynamic DNS account.

The setup of the DDNS client in the M1-XEP module described above should still be performed.

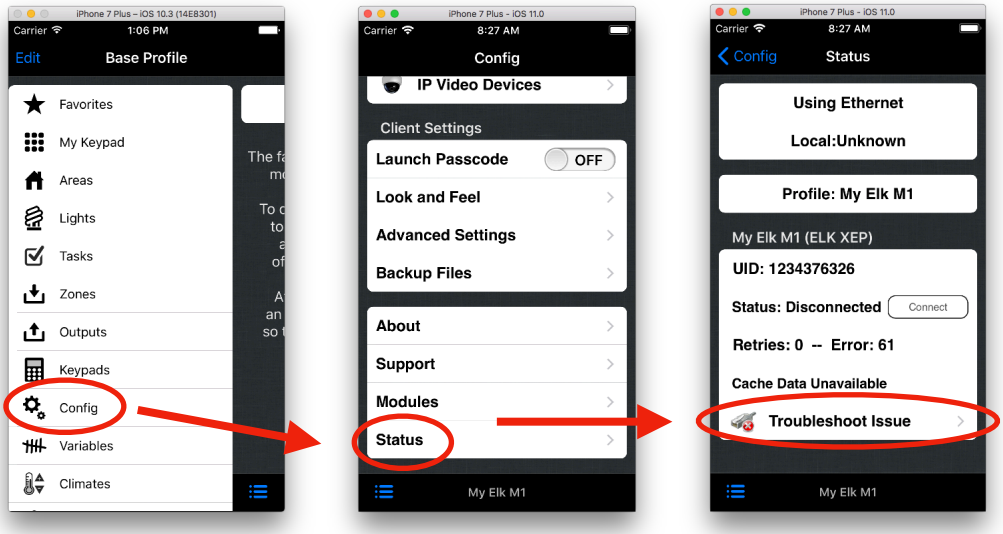
Automated Troubleshooting

For configured drivers in eKeypad Pro that are experiencing connection issues, an automated troubleshooting function is available to help diagnose the cause. This functionality is designed to identify issues when a driver was working initially but is no longer working. It can be accessed in several different ways.

- By opening any section in the “Device Management” section of the Config screen. Any driver experiencing a connection issue will be marked by a special icon. Touching on this driver will expose a “Troubleshoot Issue” link. This link will **ONLY** appear if the device is encountered a connection error.



- You can also access the “Troubleshoot Issue” link from the Config -> Status screen. Again, the link will **ONLY** appear if the device is experiencing a connection error.



Permanent Installs

One of the more advanced uses of eKeypad is to use it as a custom touch screen permanently mounted on a wall and dedicated to running eKeypad at all times. Due to the unique nature of this setup, some additional recommendations and altered practices are necessary.

Non-secure Port

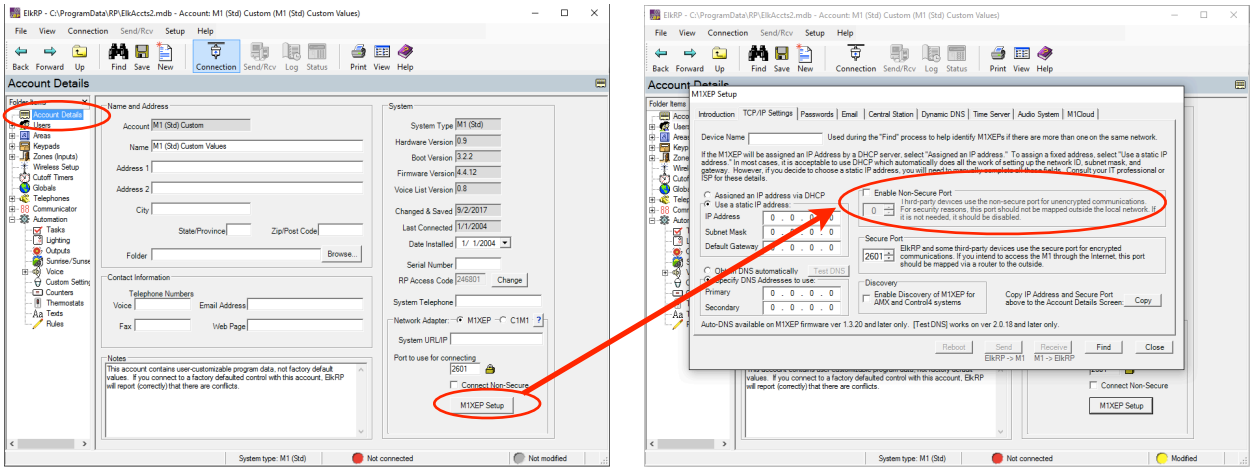
For devices that remain on site and never used remotely, it is recommended to use the Non-secure port for communications with the M1-XEP module.

Using the Non-secure port has several advantages:

- Faster communications. The use of the secure port is very fast, but the use of the Non-secure port is even faster.
- Lower M1-XEP overhead. The secure port encrypts all communications and adds noticeable overhead. The Non-secure port greatly reduces this overhead, especially when using multiple eKeypad instances.
- Lower eKeypad overhead. Apple iOS devices have very powerful processors, but certain configurations, especially multiple video streams, can benefit from reducing iOS overhead.

The Non-secure port must be used appropriately to maintain a secure system. It should **NOT** be port forwarded in the router. The Non-secure port contains no encryption or any protections for unauthorized access.

The Non-secure port is not enabled by default. The M1-XEP setting is located on the “TCP/IP Settings” tab of the “M1XEP Setup” popup window in the Elk-RP application software. This window is opened from the “Account Details” screen using the button in the bottom right corner of the screen.



Ethernet Connectivity
For permanent installs where the iOS device does not move, it is recommended to connect the iPad or iPhone to the wired ethernet network instead of using Wifi.

While this option requires a wire to be connected to the iOS device at all times, it does result in a more stable and dependable network connection.

For more information about how to setup this option and the extra hardware required, contact eKeypad support.

iPad Pro Power
The iPad Pro 12.9in has special consideration needs to be addressed related to power.

When in active use, the iPad Pro consumes more power that the 12W USB power adapter it ships with can provide. This will result in the iPad Pro slowly discharging and eventually powering off.

A more powerful power adapter is required if the iPad Pro will be used continuously in a permanent install. The Apple USB-C 29W power adapter and Apple USB-C to Lightning cable should be used. This adapter is capable of providing enough power to both operate the iPad Pro 12.9in and keep it fully charged charged.

This power solution will also make Ethernet Connectivity more complex. Contact eKeypad support for more information.

eKeypad Pro and Elk M1 Check List

Job Name: _____

- ☐ Create DDNS account.: www.dyndns.org

DDNS Details
Hostname: _____
Username: _____
Password: _____

Network Setup
- ☐ Check for Multiple Routers
- ☐ Disable/Bypass IPv6 Networks
- ☐ Connect to correct Wifi network

Hardware Setup
- ☐ Change XEP Power Adapter to M1 Battery
- ☐ Connect XEP Auto-Reboot Wiring
- ☐ Install/Setup Customer Owned Router
- ☐ Install Router/Switch Battery Backup

XEP Auto-reboot
Relay Output: _____

Elk M1 Settings
- ☐ Assign Static IP Address to XEP
- ☐ Create an Login for the XEP
- ☐ Setup Dynamic DNS client in the M1-XEP
- ☐ Setup XEP Auto-Reboot Automation Rules
- ☐ Set Serial Port Transmit Options
- ☐ Disable User Code Access Feature
- ☐ Disable Auto Stay Arming Feature

XEP Static IP
Address: _____

XEP Login
Username: _____
Password: _____

Router Setup
- ☐ Create DHCP reservation for M1-XEP Static IP
- ☐ Setup Inbound Port Forwarding of XEP Port 2601

eKeypad Setup
- ☐ Download eKeypad: http://www.ekeypad.net/pro/
- ☐ Verify DDNS hostname resolves to external router address
- ☐ Update “Base Profile” Name
- ☐ Create Elk M1 System Driver
- ☐ Test Local Network Connection
- ☐ Test Remote Access Connection
- ☐ Setup Configuration Access Passcode
- ☐ Create /Email Configuration Backup

Config Backup
File Name: _____

Advanced Setup
- ☐ Customize Application Interface
- ☐ Create Custom Blueprint Screens
- ☐ Setup Restricted Access

Notes:_____
_____
_____

* - Optional step. Only needed if not setting up a DDNS account.