eKeypad
Mobile Solutions

Push/Email Notification Setup Guide

version 1.3

Table of Contents

Overview

The Push and Email Notification support in eKeypad are designed to address the needs of both small and large installations. It supports the most common requirements we have encountered throughout the years, and we continue to add functionality as needs evolve.

1. **Equipment Capabilities.** Most equipment eKeypad supports limited or no Push Notification support. Likewise, we have found Email Notifications have various limitations for real-world use. eKeypad add robust notification and email support to all equipment it supports.

2. **Multiple Devices and Locations.** eKeypad has support for multiple devices in multiple physical locations. The eKeypad Notification system has full supports for these complex installations.

3. **Installer Focused.** One of the key strengths of eKeypad is support for professional installers. The eKeypad Notification system includes a dedicated health monitoring function with the ability to notify installers of potential end-user affecting issues as they occur.

eKeypad Notification uses a dedicated, hardware device to monitor equipment installed in a single physical location. If equipment is located at multiple locations, each location will need a dedicated monitoring device. These devices run eKeypad in a special, full-time mode to monitor the equipment and send the configured push and email notifications alerts.

- **Distribution of Notifications.** With support for both many-to-one and one-to-many routing, eKeypad allows you to send messages selectively to some devices while other messages can be sent to a larger group of devices.

- **Advanced Functions.** Each notification has a number parameters for customization of the message and when it is sent. This includes: custom message text, failed message retries, time of day restrictions and message repeats.

- **Health Monitoring.** Beyond notifications, eKeypad will actively track the connection paths in the system. This allows for rapid identification of issues. This includes but is not limited: the equipment, local network, forwarded ports, internet access and the notification system. Optionally, the monitor can send special health notifications for potential issues.

The costs for Push Notifications in eKeypad includes a one time component and a recurring component. The one-time component is required for the cost of the hardware device while the recurring component covers the cost to accesses the notification delivery system.

Push Notification Installation Costs

Recurring		One Time		
Monthly	Yearly	Apple Wifi iPad	$329-$450	Link
$4.99 / month	$39.99 / year	Belkin Lightning to POE Adapter	$99	Link

See Appendix for more wired ethernet options.

The remainder of this document describes the steps to properly setup the hardware and various software components of an Email/Push Notification system.

This will also include our recommendations for achieving a secure and reliable Email/Push Notification setup and several examples of the more common complex configurations.

Please contact eKeypad Support if you have additional questions or need assistance.

Web Site:
https://www.ekeypad.net/

Help Articles:
https://www.ekeypad.net/help/

Document Downloads:
https://www.ekeypad.net/downloads/

Email Support:
support@ekeypad.net

PhoneSupport:
+1 (214) 497-4232

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

1. Hardware and Licensing Requirements

The first step to setup notifications in eKeypad is to ensure you have all of the necessary physical hardware and licensing requirements in place.

Hardware

This document refers to two devices: a Monitor and a Receiver. These terms describe the roles of the devices in the setup. The most important role is the monitoring device which will watch the equipment and send push and email notifications as needed. The receiver is a device carried by the end user and receives push notifications. There will not be a receiver email notification, only a destination email address.

In most installs, there will only be a single monitoring device, but in more advanced configurations, it is possible to have more than one. See the Advanced section at the end of this document for more information and examples. There will always be at least one and often more than one Receiving device for push notifications.

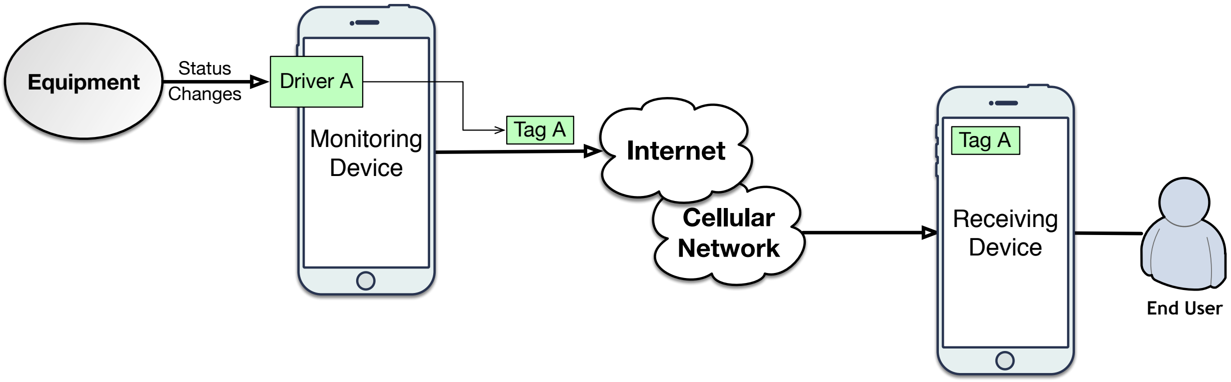


Diagram 1 : Simple Push Notification Setup

Monitoring Device

A Monitoring Device is a dedicated iOS device responsible for monitoring the equipment and sending both Push and Email Notifications based on the configured alerts in eKeypad. Interaction with this device will be minimal, only device setup and maintenance. It will be critical that the monitoring device remains connected to the local network and runs the eKeypad software continuously.

We recommend using an Apple iPod Touch for this device. This device should be mounted in the enclosure or near the equipment. In addition, this device must be capable of running iOS version 12 or higher.

- **Device Power.** The monitoring device should remain powered at all times. The power adapter will not meet this requirement alone. We recommend using a UPS to provide protection from power surges and to extend power outage runtime.

- **Network Connection.** The default network connection for iOS devices is Wifi, which will cause reliability issues over time. All installations should use a wired ethernet connection. The Wired Ethernet Connection section below provides more details on accomplishing this.

- **Application Locking.** Other iOS applications should be restricted using Guided Access to increase reliability. The process of enabling Guided Access can be found in the Appendix of this document.

Receiving Device

The Receiving Device is typically the device end-users carry with them and use daily. The only configuration change will be to define the push notification tags the device should receive.

Devices receiving Email Notifications do not require additional setup in eKeypad.

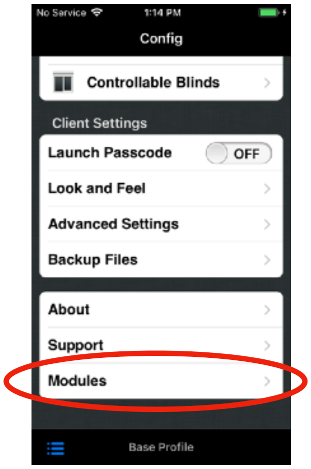
Licensing

Support for receiving Push Notifications is only available in the eKeypad and eKeypad Pro applications. It is impossible to enable notification support in any other eKeypad branded applications.

An upgrade bundle in the Apple App Store allows older eKeypad branded applications to upgrade to eKeypad Pro for a discount. Search for the term "eKeypad Pro Upgrade Bundle" in the Apple App Store.

Support for receiving Push Notifications is in the base license for the eKeypad and eKeypad Pro applications.

Support for monitoring and sending Push Notifications is available in the eKeypad Pro application by purchasing a recurring "Push Subscription module. This module is found on the Modules screen at the bottom of the main Config screen.



No Service 1:14 PM

Config

Controllable Blinds

Client Settings

Launch Passcode OFF

Look and Feel

Advanced Settings

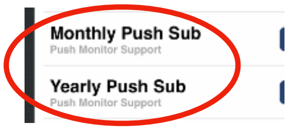
Backup Files

About

Support

Modules

Base Profile



Monthly Push Sub
Push Monitor Support

Yearly Push Sub
Push Monitor Support

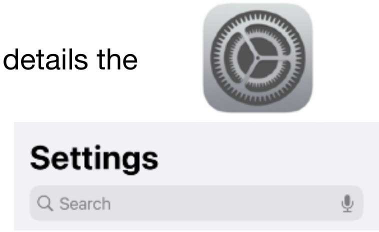
	- Ability to receive notifications included in the base license - Subscription Module required to function as a Push Monitor
	- Ability to receive notifications included in the base license

2. Monitoring Device Configuration

The second step is to set up Notifications is completing the software configuration on the Monitoring devices. There are three main areas of work: the iOS settings, the eKeypad Pro configuration, and the notification alert setup.

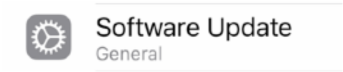
iOS Configuration

All iOS settings are in the iOS Settings application. This document details the location of these settings on iOS 16, but they can be different locations in other iOS versions. You can find the settings screen by searching for the title used in this document. Pull down the main iOS settings screen to expose the search function.



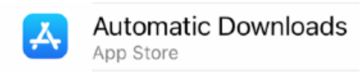
Software Updates

Reliable operation of the Monitoring device is essential. Turn OFF automatic iOS software updates. Open the “Software Update” screen under the “General” link on the main settings screen. Tap on the “Automatic Updates” link and turn OFF all switches on this screen.



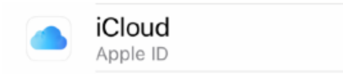
Automatic Downloads

Reliable operation of the Monitoring device also includes limiting automatic eKeypad updates. Turn OFF automatic download and installation of application updates. Open the “App Store” link on the main settings screen. Turn off all switches in the "Automatic Downloads “sections.



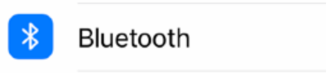
iCloud Services

The customer’s Apple ID is used to set up the Monitoring device. Unneeded services should be disabled. Open the “iCloud” screen under the Apple ID account link at the top of the main settings screen. Turn OFF all entries in the “Apps Using iCloud” section. Also, turn OFF all items under the “Show All” link.



Bluetooth

The Monitoring device does not use the Bluetooth function. Disable Bluetooth on the "Bluetooth" link on the main settings screen.



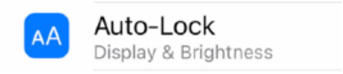
Wi-Fi

The Monitoring device should use a wired ethernet connection. It is reasonable to perform setup and configuration using Wi-Fi for convenience, but an ethernet connection is required to maintain reliable operation. Turn OFF Wi-Fi on the “Wi-Fi” link on the main settings screen.

Wi-Fi

Auto-Lock

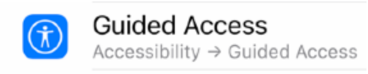
Automatically locking the screen will stop the operation of the Monitoring device. Turn OFF this functionality on the “Display & Brightness” link on the main settings screen.



Auto-Lock
Display & Brightness

Configure Guided Access

eKeypad must remain running at all times. If eKeypad is not visible on the screen, it is not running, and push notifications will not be sent. The Monitoring device should use the “Guided Access” functionality.



Guided Access
Accessibility → Guided Access

Before using Guided Access, it must be enabled and configured on the “Guided Access” link under the “Accessibility” link.

The accessibility screen is located at different places depending on the version of iOS you are using.

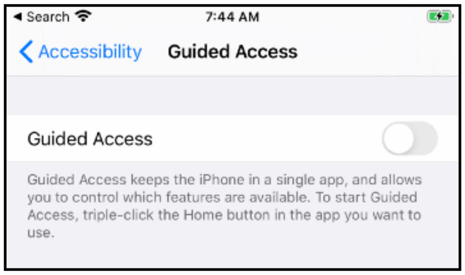
> If you have trouble locating the accessibility screen, scroll to the top of the main iOS Settings screen and search for “Accessibility”.

- On iOS 13 and higher, the accessibility screen is locate on the main settings screen.
- Prior to iOS 13 the accessibility screen was located under the General link.

Once you have located the the Accessibility screen, touch on the “Guided Access” row.

1. Turn the “Guided Access” switch to ON
2. Setup a Guided Access Passcode
3. Leave all of the Time Limits settings OFF
4. Leave the the Accessibility Shortcut setting OFF
5. Disable the “Display Auto-Lock” setting.

    - On iOS 13 and later, change the setting to Never.
    - Prior to iOS 13, turn“Mirror Display Auto-Lock” ON



◂ Search 7:44 AM

< Accessibility Guided Access

Guided Access ○

Guided Access keeps the iPhone in a single app, and allows you to control which features are available. To start Guided Access, triple-click the Home button in the app you want to use.

eKeypad Configuration

Follow the "Best Practices" document for your equipment. This document will describe all of the required steps for a working and reliable install.

All of the eKeypad documentation is available on the Downloads page of eKeypad web site: https://www.ekeypad.net/downloads/

The unique way in which the Monitoring Device is used will change a few of the best practice recommendations. The following topics should be bypassed to simplify the setup and reduce the possible sources of issues.:

- **Failover configurations.**
  Monitoring devices should only be run from the local network and have no need for failover functionality.

- **Dynamic DNS hostname.**
  DDNS hostnames are only needed for remote access.

- **Encrypted Equipment Ports.**
  If an unencrypted port is available on the equipment it should be used to improve responsiveness and allow for faster communications.

- **Ignore Errors.**
  Reconnect drivers in eKeypad forever. Should be set to ON so eKeypad can better handle network and equipment outages.

- **Allow Sleep.**
  Prevent iOS from putting device to sleep. Should be left OFF which is the default value.

Turning on Monitor Mode

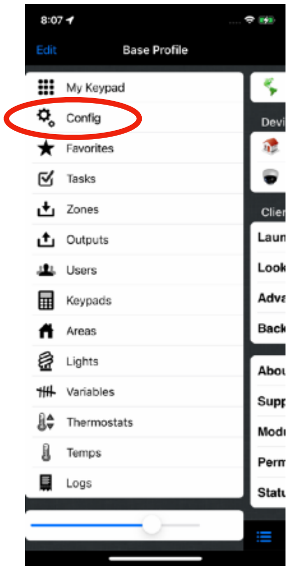
Before setting up the alerts, Notifications must be enabled and the device placed into Monitor mode. Notifications should not and can not be configured on Receiver devices.

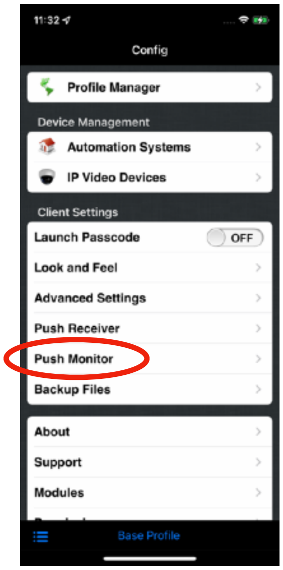
For eKeypad Pro, if a Notification subscription is not active the configuration screens described below will not be available. These screens are always available on the eKeypad application.

- Open the Config screen in eKeypad
- Touch on the Push Monitor link
- Turn the “Enable Push Server” switch to ON

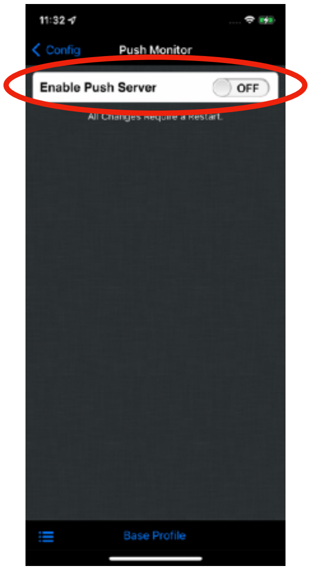
Troubleshooting:
If you do not see a “Push Monitor” row, a Push Notification subscription is not active.

Optionally, on this screen you may also enter a “Security Tag” for an additional level of security and privacy. The “Security Tag” field is a case sensitive string.



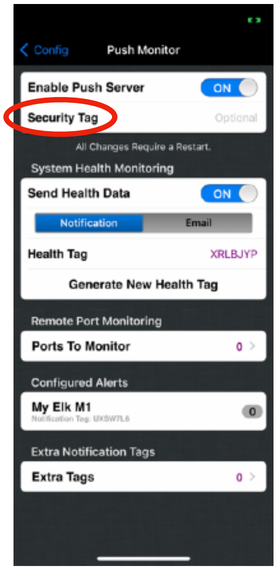


Launch Passcode OFF



Enable Push Server OFF

All Changes Require a Restart.



Enable Push Server ON

Security Tag Optional

All Changes Require a Restart.

Send Health Data ON

Notification | Email

Health Tag XRLBJYP

Ports To Monitor 0

My Elk M1 0
Notification Tag: UXSW7L6

Extra Tags 0

Additional Monitor functionality can also be enabled on this screen.

- **Send Health Data**. This feature will cause the monitor device to send push or email notifications with information about potential issues the monitor has detected that may be affecting end-user access to the equipment.

- **Ports to Monitor**. This feature will monitor ports forwarded through the local firewall to ensure that they are accessible remotely. This function can not monitor ports at remote locations.

- **Extra Tags**. This feature allows additional push notification tags to be defined.Each configured equipment driver in eKeypad is automatically assigned a unique push notification tag. Additional tags enables the ability to route notifications to multiple recipients.

Important:
A restart is required after making changes to the Notification Configuration

Setup Notification Alerts

After notifications have been enabled, the Push Notification Alerts need to be defined. This will tell eKeypad what status changes to monitor and the message that should be sent in each case. Currently push notification alerts can be setup on the the following capabilities:

- Alarm Zones
- Alarm Areas
- Relay Inputs
- Relay Outputs
- Lights
- Variables

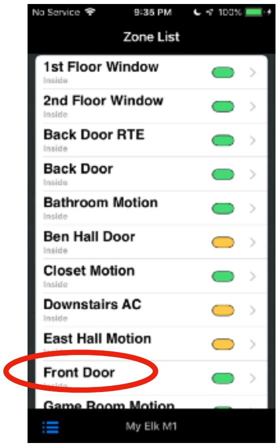
> For simplicity, this document will only outline the process of setting up a Push Notification for an Alarm Zone. The process for setting up Email Notifications and notifications for other capabilities is very similar.

To access the Alert Management on a Monitoring Device.

- Open the Zone list in eKeypad.
- Touch a Zone to display its detail screen.
- Find the "Customizations" section. Tap the triangle or title to toggle visibility.
- Touch on "Manage Alerts" link.

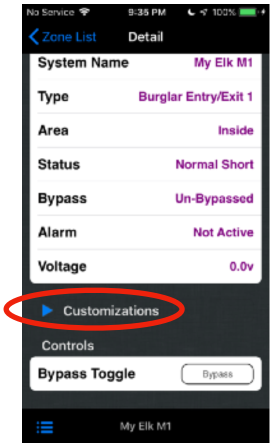
The screen displayed will be a list of the Alerts currently defined for this Alarm Zone.

> **Important Note**
>
> The "Customizations" section is **only** visible if editing is enabled. To enable editing, tap the "Look and Feel" link on the main eKeypad Configuration screen. The setting is labeled, "Edit Interface" and must be set ON.
>
> See the Security Considerations section later in this document for more detail.



Zone List

1st Floor Window
Inside
2nd Floor Window
Inside
Back Door RTE
Inside
Back Door
Inside
Bathroom Motion
Inside
Ben Hall Door
Inside
Closet Motion
Inside
Downstairs AC
Inside
East Hall Motion
Front Door
Game Room Motion



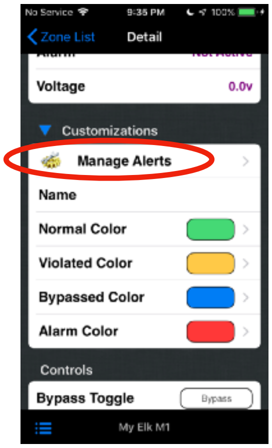
Zone List Detail

System Name	My Elk M1
Type	Burglar Entry/Exit 1
Area	Inside
Status	Normal Short
Bypass	Un-Bypassed
Alarm	Not Active
Voltage	0.0v

▶ Customizations

Controls

Bypass Toggle



Zone List Detail

Voltage	0.0v

▼ Customizations

Manage Alerts

Name

Normal Color 🟩

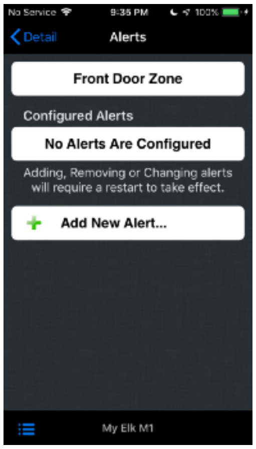
Violated Color 🟨

Bypassed Color 🟦

Alarm Color 🟥

Controls

Bypass Toggle



Detail Alerts

Front Door Zone

Configured Alerts

No Alerts Are Configured

Adding, Removing or Changing alerts will require a restart to take effect.

Add New Alert...

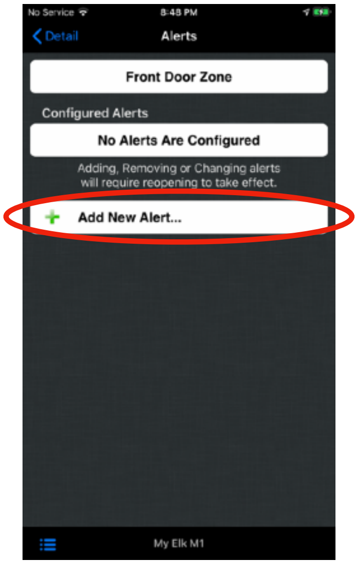
To add a new Push Notification Alert to a Monitoring Device tap the “Add New Alert…” button.

Note

Alerts are only triggered when the monitoring device observes the state of item changing to the specified state.

Alerts are **not** triggered when the item leaves the state or if the item is already in the state when eKeypad is launched.

- **“Alert Trigger”** is the state that will trigger the Alert and send the Notification.
- **“Alert Action”** should be set to the “Push Notification” or “Email Message” value. The remaining options are for local only alerts.
- **“Repeat Frequency”** is an optional feature allowing a Notification to be sent repeatedly for as long as the item remains in the triggering state.
- **“Time of Day”** is an optional feature allowing a period of time during which notifications will be sent. Outside this window of time, notification messages that are triggered will be discarded. They **will not** be sent later.
- **“Extra Tags”** this option will only appear if extra push notification tags were defined on the Push Notification screen in the eKeypad Configuration. It will allow you to select the additional tags this message should be sent to.
- Use the Save button in the top right corner of the screen to save the Alert.

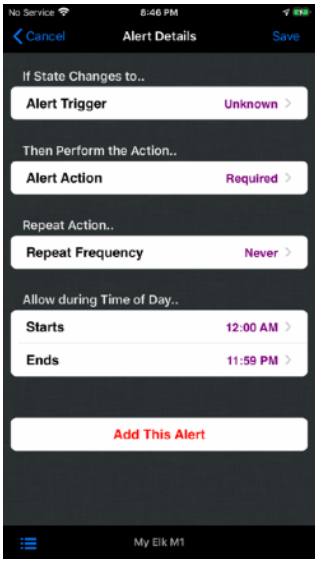


Front Door Zone

Configured Alerts

No Alerts Are Configured

Adding, Removing or Changing alerts will require reopening to take effect.



If State Changes to..

Alert Trigger Unknown

Then Perform the Action..

Alert Action Required

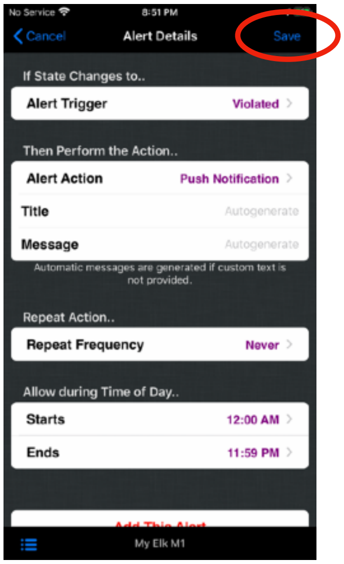
Repeat Action..

Repeat Frequency Never

Allow during Time of Day..

Starts 12:00 AM

Ends 11:59 PM



If State Changes to..

Alert Trigger Violated

Then Perform the Action..

Alert Action Push Notification

Title Autogenerate

Message Autogenerate

Automatic messages are generated if custom text is not provided.

Repeat Action..

Repeat Frequency Never

Allow during Time of Day..

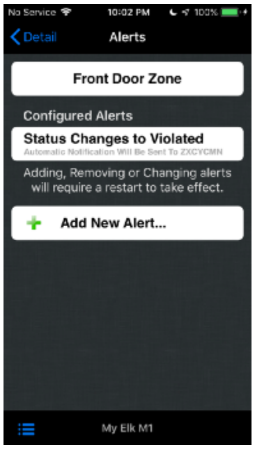
Starts 12:00 AM

Ends 11:59 PM

After saving the alert, the alert list will reappear and display a summary of the configured alerts for this capability item.

From this view, swiping left on the row will expose the option to delete the alert. Tapping on the row will allow you to update the alert details.

Pay special attention to the description of the alert. It contains a reference to the Push Notification Tag this alert message will be sent to. Write down this Tag code. This Tag will be required later during the setup of any device that needs to receive this push notification.



Front Door Zone

Configured Alerts

Status Changes to Violated

Automatic Notification Will Be Sent To ZXCYCMN

Adding, Removing or Changing alerts will require a restart to take effect.

Important:

A restart is required after Adding, Removing or Changing Alerts

Monitoring Device Security

The last activity to be performed on a Monitoring Device is to secure the configuration to prevent unauthorized access to the notification messages it sends.

Please see the Security Considerations section below for more detail and a walkthrough of the recommended security settings for Monitoring Devices.

3. Receiving Device Configuration

The setup of the Receiving Devices is a much simpler than the Monitoring Device.

Important:
A restart is required after making changes to the Notification Configuration

eKeypad Configuration

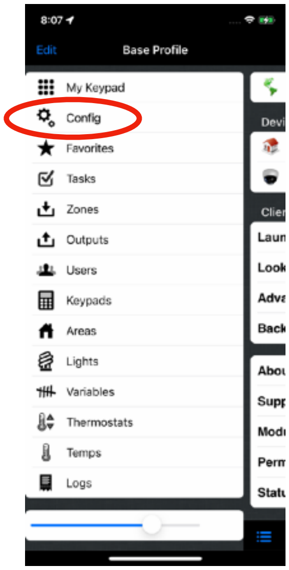
Start by completing the normal setup process for eKeypad and validate that it can connect to the equipment both locally and remotely. It is recommended to follow the “Best Practices” document for your equipment. This document will describe all of the required steps for a working and reliable install.

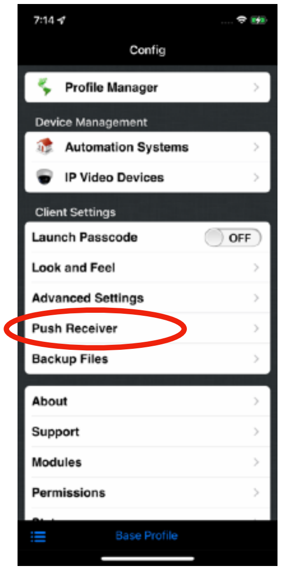
All of the eKeypad documentation is available on the Downloads page of eKeypad web site: https://www.ekeypad.net/downloads/

Enabling Receiver Mode

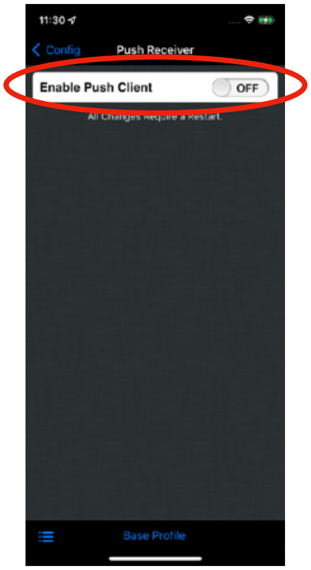
For eKeypad Pro, if a Notification subscription is not active the configuration screens described below will not be available. These screens are always available on the eKeypad application.

- Open the Config screen in eKeypad
- Touch on the Push Notifications link
- Turn the “Enable Push Client” switch to ON

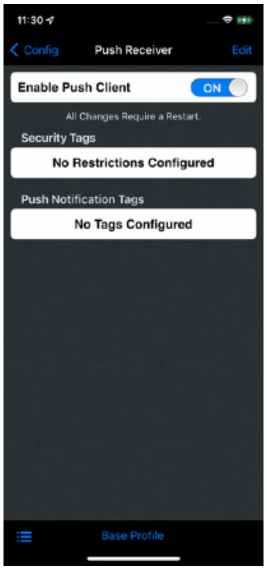




Launch Passcode OFF



Enable Push Client OFF
All Changes Require a Restart.

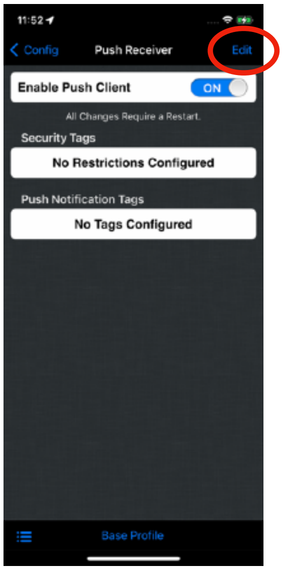


Enable Push Client ON
All Changes Require a Restart.
Security Tags
No Restrictions Configured
Push Notification Tags
No Tags Configured

Add Security Tags

Optional Security Tags can be setup on Monitoring Devices to increase the privacy and security. If used, these tags must also be configured on Receiving Devices. A missing Security Tag will prevent notifications from being received. Multiple Security Tags can be added. Tags including tags for different Monitoring Devices.

- Enter editing mode by pressing the Edit button.
- Touch the “Add New Security Tag” button to add a new Tag row.
- Touch on the newly added row to enter the tag. Tags are case sensitive.
- When done adding tags, exit editing mode by pressing the Done button.



Enable Push Client ON

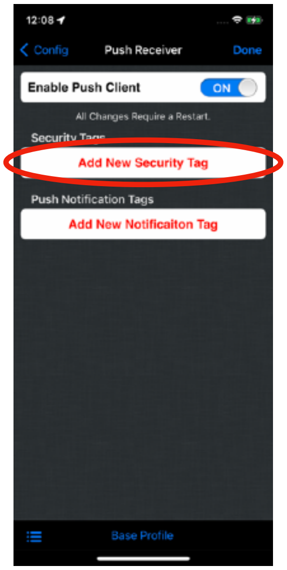
All Changes Require a Restart.

Security Tags

No Restrictions Configured

Push Notification Tags

No Tags Configured



Enable Push Client ON

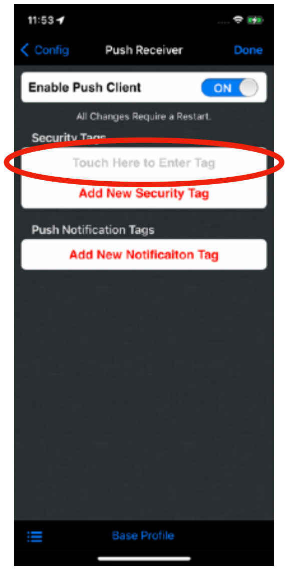
All Changes Require a Restart.

Security Tags

Add New Security Tag

Push Notification Tags

Add New Notificaiton Tag



Enable Push Client ON

All Changes Require a Restart.

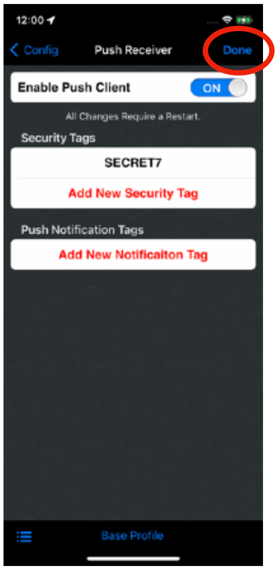
Security Tags

Touch Here to Enter Tag

Add New Security Tag

Push Notification Tags

Add New Notificaiton Tag



Enable Push Client ON

All Changes Require a Restart.

Security Tags

SECRET7

Add New Security Tag

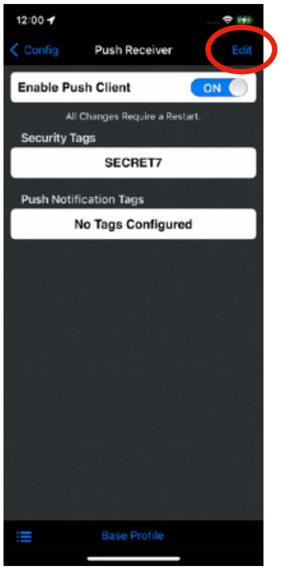
Push Notification Tags

Add New Notificaiton Tag

Add Notification Tags

Notification Tags control the push notifications that will be received and displayed by this Device. Multiple Notification Tags can be added including tags from different Monitoring Devices, Extra Tags setup on Monitoring Devices and Health Notification Tags.

- Enter editing mode by pressing the Edit button.
- Touch the "Add New Notification Tag" button to add a new Tag row.
- Touch on the new row to enter the tag . Tags are case sensitive.
- When done adding tags, exit editing mode by pressing the Done button.



12:00

Config Push Receiver Edit

Enable Push Client ON

All Changes Require a Restart.

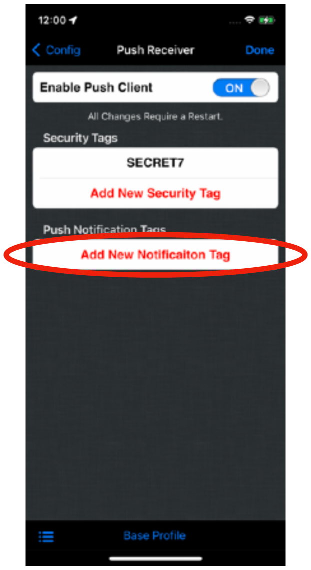
Security Tags

SECRET7

Push Notification Tags

No Tags Configured

Base Profile



12:00

Config Push Receiver Done

Enable Push Client ON

All Changes Require a Restart.

Security Tags

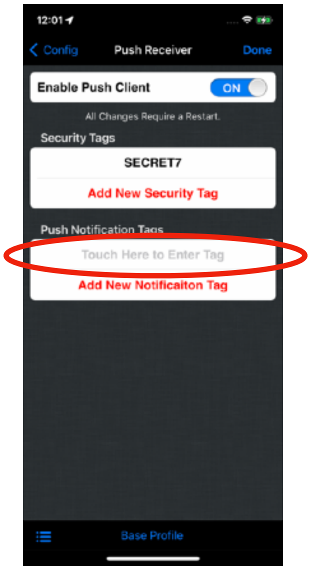
SECRET7

Add New Security Tag

Push Notification Tags

Add New Notificaiton Tag

Base Profile



12:01

Config Push Receiver Done

Enable Push Client ON

All Changes Require a Restart.

Security Tags

SECRET7

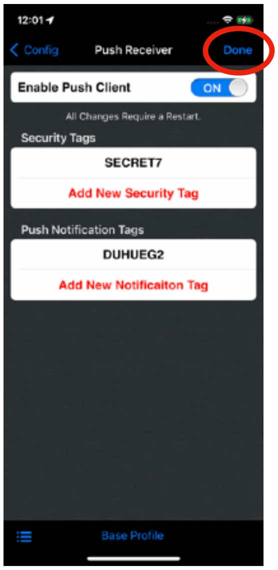
Add New Security Tag

Push Notification Tags

Touch Here to Enter Tag

Add New Notificaiton Tag

Base Profile



12:01

Config Push Receiver Done

Enable Push Client ON

All Changes Require a Restart.

Security Tags

SECRET7

Add New Security Tag

Push Notification Tags

DUHUEG2

Add New Notificaiton Tag

Base Profile

4. Security Considerations

It is important to apply basic safeguards to the Push Notification Tags being used. While these Tags are randomly generated they do uniquely identify the systems being monitored.

Additionally, for Monitoring Devices configured with a Security Tag this setting should be treated the same as any password.

Important Note

If a Receiving Device is **not** configured with a Push Notification Tag, the messages sent with this Tag will **not** appear on that device.

Access to both a valid Push Notification Tag and the optional Security Tag for the Monitoring Device that sent the notification are necessary to receive and see a Push Notification message. Please note that it is **not possible** to query or control equipment using these Tags.

To prevent unauthorized viewing of push notification messages, there are several configuration settings in eKeypad that can be used to restrict access to various customization and configuration settings. These settings can be used to restrict access to the equipment configuration, push notification tags and security tags.

For monitoring devices we recommend:

- Disable Edits. Removes the ability to change Alerts used to trigger Push Notifications.
- Configuration Passcode. Restricts access to the configuration screens.

For receiving devices we recommend:

- Configuration Passcode. Restricts access to the configuration screens.

By using these recommended security settings in eKeypad a passcode will be created that is required to view and/or change the Push Notification Tags, the Security Tags or the Alerts that trigger the sending of Push Notification messages.

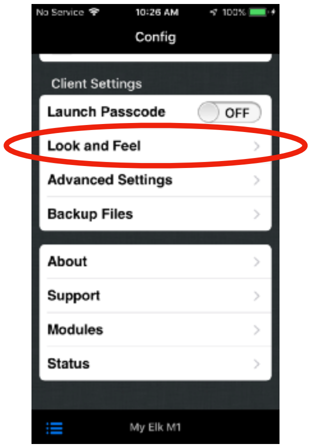
Disabling Changes to Push Notifications

This feature will hide the Customizations section on detail screens of capability items. Access to this section is necessary to make changes to the Alerts responsible for sending push notification messages.

To disable editing in eKeypad.

- Open the Config screen in eKeypad
- Touch on the Look and Feel link
- Turn the “Edit Interface switch to OFF

Changes to this setting take effect immediately.



No Service 10:26 AM 100%

Config

Client Settings

Launch Passcode OFF

Look and Feel

Advanced Settings

Backup Files

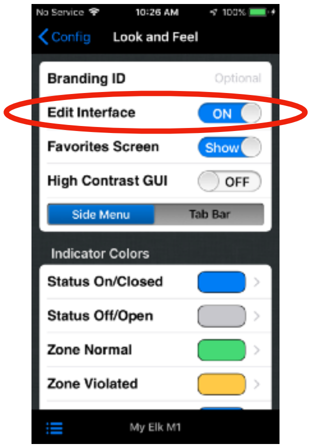
About

Support

Modules

Status

My Elk M1



No Service 10:26 AM 100%

Config Look and Feel

Branding ID Optional

Edit Interface ON

Favorites Screen Show

High Contrast GUI OFF

Side Menu | Tab Bar

Indicator Colors

Status On/Closed

Status Off/Open

Zone Normal

Zone Violated

My Elk M1

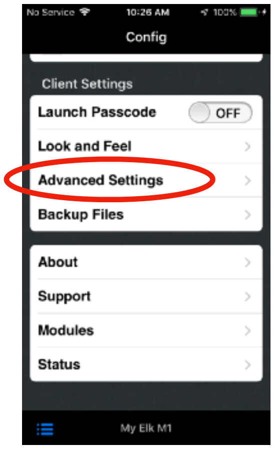
Restricting Access to Configuration

This feature allows a passcode to be setup which restricts access to all configuration screens in eKeypad.

To setup a passcode in eKeypad.

- Open the Config screen in eKeypad
- Touch on the “Advanced Settings” link
- Turn the “Secure Config” switch to ON

When you enable this setting a wizard will be displayed to guide you through the process of defining and verifying a passcode plus an optional hint to help in the recovery of forgotten passcodes.



No Service 10:26 AM 100%

Config

Client Settings

Launch Passcode OFF

Look and Feel

Advanced Settings

Backup Files

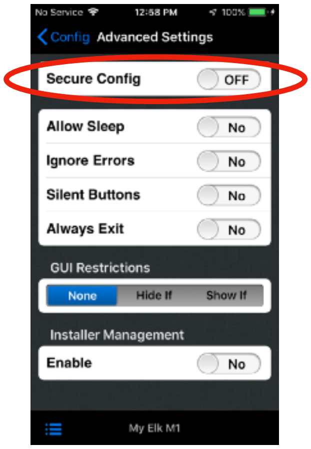
About

Support

Modules

Status

My Elk M1



No Service 12:58 PM 100%

Config Advanced Settings

Secure Config OFF

Allow Sleep No

Ignore Errors No

Silent Buttons No

Always Exit No

GUI Restrictions

None | Hide If | Show If

Installer Management

Enable No

My Elk M1

Place this passcode in a safe place. It is **not possible** to recover lost passcodes.

Setting up a configuration passcode will take effect immediately.

5. Push Notification Reliability

It is important to note that Push Notifications uses a “best effort” mechanism for delivery. There are numerous data networks and servers that participate in the notification mechanism that are outside the control of eKeypad. Because of this, we can not promise high reliability, timely delivery or that a message will be displayed by the target device.

You should **NOT** rely on Push Notifications exclusively. They are not a replacement for critical communications such as alarm system monitoring, medial personnel, law enforcement and/or other appropriate authorities.

Push Notifications do not deliver information. Notification messages only notify you that new information is available. You must launch eKeypad and establish an active connection to relevant equipment in order to view the real-time status.

Disclaimer

Push Notification support in eKeypad is provided as a supplemental communication method and should not be relied upon exclusively. This functionality uses a “best effort” mechanism for delivery and makes no claims of reliability or timely delivery of notifications.

eKeypad makes no warranties about the accuracy, completeness, or delivery of any message transmitted through Push Notifications. There is no guarantee that notification messages will: (a) be received in a timely manner; (b) ever reach their destination; or (c) be displayed by the device.

eKeypad is not responsible for any actions based on information provided in a Push Notification message; or for receiving a delayed message; or for messages that fail to arrive.

Several factors can delay or prevent the delivery of Push Notification Messages from being received or displayed on the receiving device. Following is a list of the most common reasons.

- **Guided Access is Not Running**

  Proper operation of a Push Notification Monitor requires that guided access is enabled and turned ON at all times.

  Always verify that Guided Access is enabled after working with the Push Monitor device.

- **Mobile Device is Offline**

  Apple servers must send the notification to the receiving device. Delivery of a Push Notification requires an active cellular or Wifi connection. Apple servers will not cache multiple Push Notifications.

  If multiple notifications are received while the receiving device is offline, all but the last Push Notification will be lost.

- **eKeypad is in the Foreground**

  Push Notifications will notify you when new information is available in eKeypad. It is not designed to inform you of status changes.

  If eKeypad is running in the foreground, there is no need to display notifications that the receiving device may receive. iOS will discard any messages received in this scenario. There are no iOS settings available to change this behavior.

- **Push Notifications are One-Way**

  Apple currently provides no mechanism to verify if a device has received a notification message. There is no way to verify that Push Notifications are received.

- **The Internet**

  Push Notification messages are sent from eKeypad to Apple using the internet. In some cases, Apple communications with the receiving device will also use the internet.

  If internet availability is down, there is no way for eKeypad to send the notification.

- **Device Configuration**

  Independent of eKeypad, end-users have complete control over Push Notifications. They have access to iOS configuration settings that can mute or disable messages received from eKeypad.

6. Appendix

The following sections provide additional detail, alternative and strategies for complicated installations.

Wired Ethernet Connection

One of the most common causes of issues, is the dynamic nature of Wifi connections. To increase reliability of monitoring devices, a wired Ethernet connection should always be used.

There are numerous options available for this purpose, but the most important thing is to **ALWAYS** use an Apple MFI (Made for iPhone) certified device. We can only provide support for installations using an MFI certified ethernet adapter.

The equipment we use in our testing includes the following. The prices listed are only for reference and may have changed.

- **Apple**. Lightning to USB3 Camera Adapter plus Belkin USB3.0 to Ethernet Adapter.
  - Model: Apple A1619 and Belkin B2B048A1277
  - Notes: Does not support IEEE 802.3af POE. Setup creates a tangle of wires and adapters.

- **Belkin**. Ethernet + Power Adapter w/ Lightning Connector.
  - P/N: F8J227dsWHT
  - Notes: Supports IEEE 802.3af POE. Physically small. Short, non-replaceable lightning cable on dongle.

- **Redpark**. POE and AC Powered solutions.
  - Model: L6-NETPOE or L6-NETAC
  - Notes: IEEE 802.3af POE option. Multiple, replaceable lightning cable options. Custom lightning cables sold separately. Longest lightning cable. Easiest solution to hide.

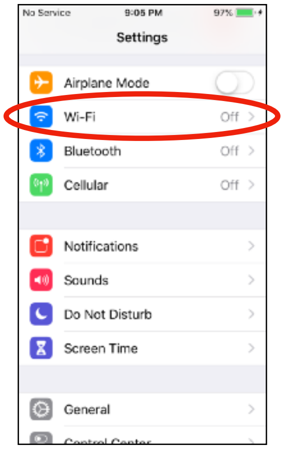
There is no special setup required to use these adapters; simply plug them in.

If eKeypad is running when the adapter is connected, it should be restarted.

When using an ethernet connection all other interfaces capable of serving as a network connection should be disabled. This includes Wifi, Bluetooth and Cellular Data functions. To properly disable these settings the changes must be performed in the iOS Settings app.

Turn Off Wi-fi in iOS

- Open the iOS Settings Application.
- Touch on the “Wifi” row.
- Turn the Wi-Fi switch to OFF


No Service 9:05 PM 97%

Settings

Airplane Mode ○

Wi-Fi Off >

Bluetooth Off >

Cellular Off >

Notifications >

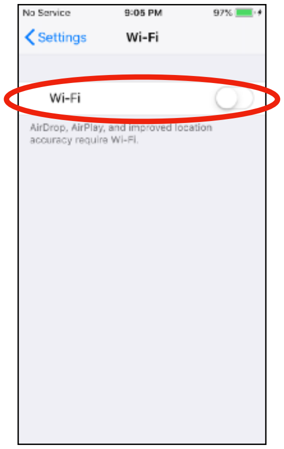
Sounds >

Do Not Disturb >

Screen Time >

General >

Control Center >


No Service 9:05 PM 97%

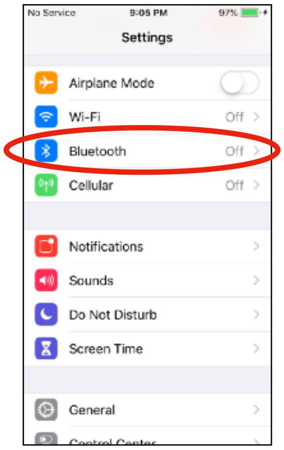
< Settings Wi-Fi

Wi-Fi ○

AirDrop, AirPlay, and improved location accuracy require Wi-Fi.

Turn Off Bluetooth in iOS

- Open the iOS Settings Application.
- Touch the “Bluetooth” row.
- Turn the Bluetooth switch to OFF.


No Service 9:05 PM 97%

Settings

Airplane Mode ○

Wi-Fi Off >

Bluetooth Off >

Cellular Off >

Notifications >

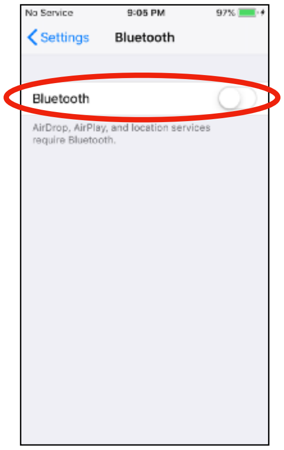
Sounds >

Do Not Disturb >

Screen Time >

General >

Control Center >


No Service 9:05 PM 97%

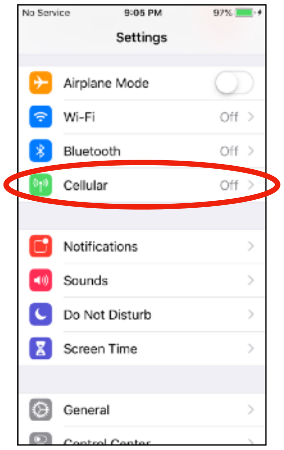
< Settings Bluetooth

Bluetooth ○

AirDrop, AirPlay, and location services require Bluetooth.

Turn Off Cellular Data in iOS

- Open the iOS Settings Application.
- Touch the “Cellular” row.
- Turn the “Cellular Data” switch to OFF.


No Service 9:05 PM 97%

Settings

Airplane Mode ○

Wi-Fi Off >

Bluetooth Off >

Cellular Off >

Notifications >

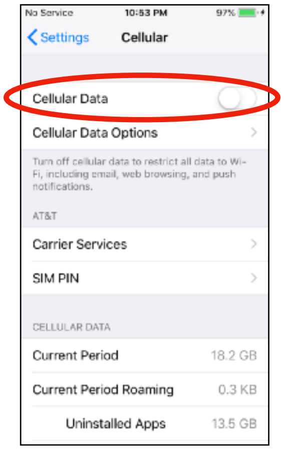
Sounds >

Do Not Disturb >

Screen Time >

General >

Control Center >


No Service 10:53 PM 97%

< Settings Cellular

Cellular Data ○

Cellular Data Options >

Turn off cellular data to restrict all data to Wi-Fi, including email, web browsing, and push notifications.

AT&T

Carrier Services >

SIM PIN >

CELLULAR DATA

Current Period	18.2 GB
Current Period Roaming	0.3 KB
Uninstalled Apps	13.5 GB

Guided Access

This is the preferred method. The “Guided Access” method can be configured and setup on the iOS device itself. There is no additional software, 3rd party services or internet connection requirements.

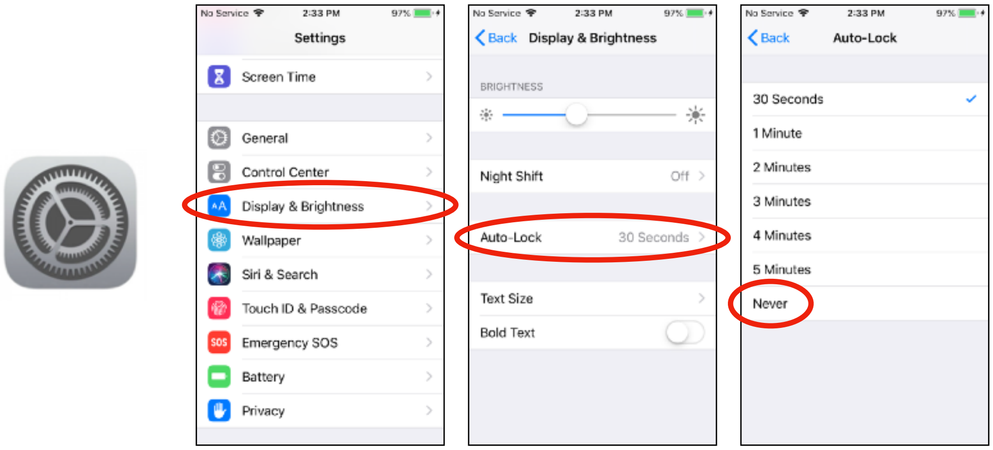
Details of how to setup Guided Access is detailed by Apple here:
https://support.apple.com/en-us/HT202612

Several iOS Settings are necessary for proper operation of guided access. All of these settings are located under the iOS Settings app.

Display Auto-Lock Setting

This setting determines if or when the iOS device automatically locks and the display enters sleep mode. For the purpose of using guided access with eKeypad this function should be disabled.

- Open the iOS Settings Application.
- Touch on the “Display & Brightness” row.
- Change the Auto-Lock setting to Never.



No Service 2:33 PM 97%

Settings

Screen Time

General

Control Center

Display & Brightness

Wallpaper

Siri & Search

Touch ID & Passcode

Emergency SOS

Battery

Privacy

No Service 2:33 PM 97%

Back Display & Brightness

BRIGHTNESS

Night Shift Off

Auto-Lock 30 Seconds

Text Size

Bold Text

No Service 2:33 PM 97%

Back Auto-Lock

30 Seconds ✓

1 Minute

2 Minutes

3 Minutes

4 Minutes

5 Minutes

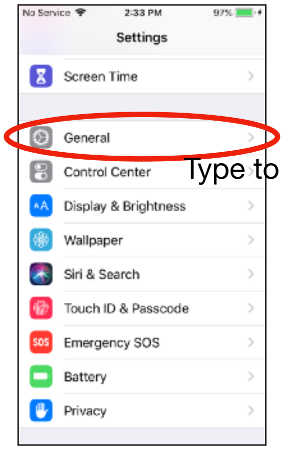
Never

Guided Access Auto-Lock Setting

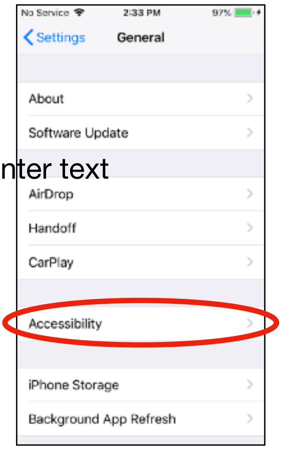
This setting determines whether guided access uses its own internal timeout for Auto-Lock or if it should use the Display value. For the purpose of using guided access with eKeypad guided access should use the Display value.

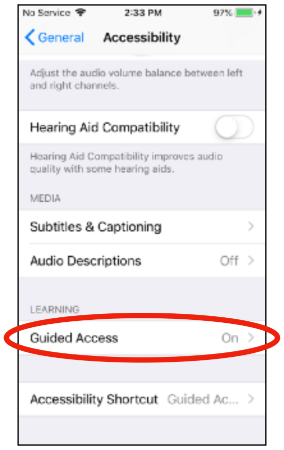
For iOS versions prior to iOS 13, Accessibility settings are located under the General section:

- Open the iOS Settings Application.
- Touch on the General row.
- Touch on the Accessibility row.
- Touch on the "Guided Access" row.
- Switch the "Mirror Display Auto-Lock" setting to ON.



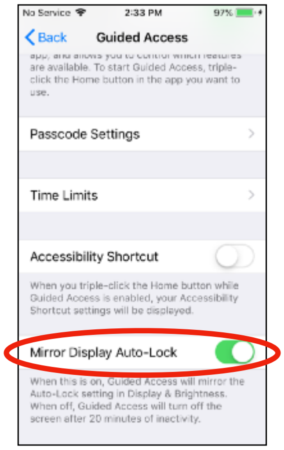
Type to enter text





Adjust the audio volume balance between left and right channels.

Hearing Aid Compatibility improves audio quality with some hearing aids.

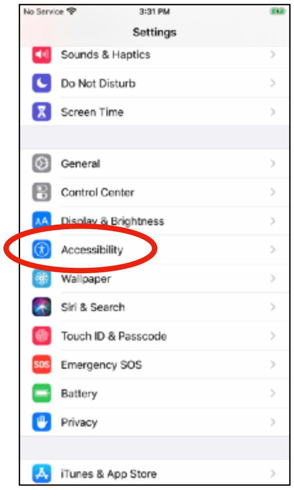


app, and allows you to control which features are available. To start Guided Access, triple-click the Home button in the app you want to use.

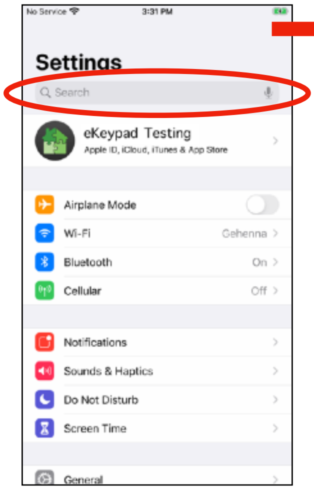
When you triple-click the Home button while Guided Access is enabled, your Accessibility Shortcut settings will be displayed.

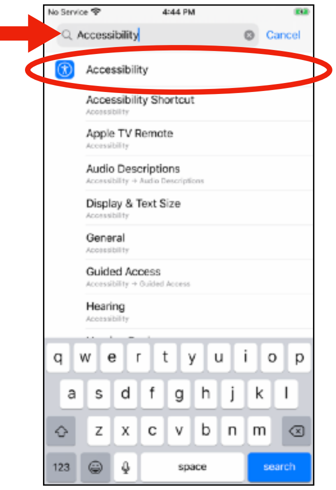
When this is on, Guided Access will mirror the Auto-Lock setting in Display & Brightness. When off, Guided Access will turn off the screen after 20 minutes of inactivity.

Starting in iOS 13, the Accessibility settings have been moved to the main Settings screen. If you have trouble locating the Accessibility screen you can use the Search field at the top of the main iOS Settings screen.



or





Common Issues

Some of the more common issues you may encounter.

Push Notifications not Received

Successfully receiving push notifications is dependent on matching the notification and security tags. Additionally, changes to the tags requires a restart to take effect.

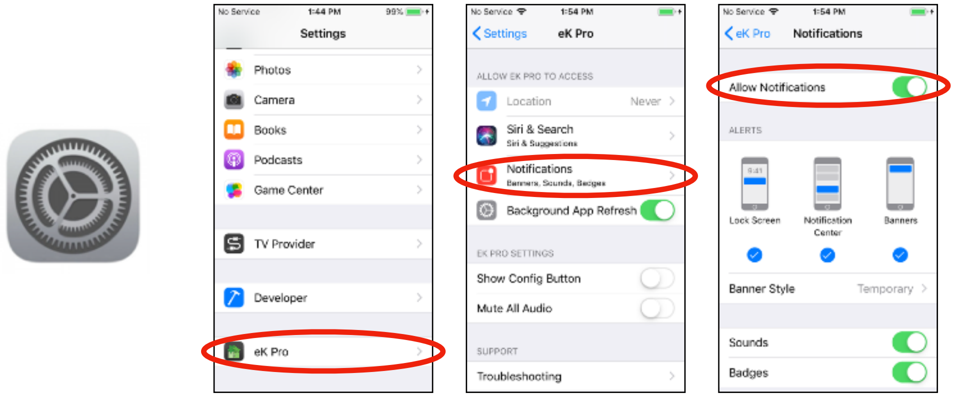
We recommend using the following checklist to troubleshoot this situation.

Troubleshooting Step	Why this can Help
1. Restart eKeypad on the Monitoring Device.	Notification and Security Tags are only registered at launch. Changes require a restart.
2. Restart eKeypad on the Receiving Device.	
3. Verify Tags on Monitor and Receiver match.	Tags are case sensitive and can look similar.
4. Verify Security Tag Configuration.	A Security Tag applies to **ALL** notifications.
5. Verify Receiver Device Allows Notifications	iOS can block notifications. See below for detail.

Apple provides a data privacy option that allows an end-user to hide Push Notification messages received for individual applications.

To change this behavior for eKeypad Push Notifications:

- Open the iOS Settings Application.
- Scroll down and tap on the “eK Pro” entry.
- Touch on the “Notifications” entry.
- Make sure the “Allow Notifications” switch is set to ON.

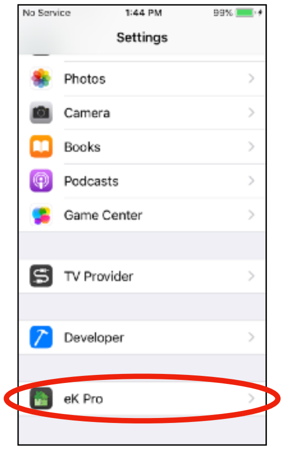


Notification Only Says, “Notification”

Apple provides a data privacy option that allows an end-user to hide Push Notification messages that may contain sensitive information. This configuration options will mask the message with the text, “Notification” in scenarios where the end-user has not been authorized.

To change this behavior for eKeypad Push Notifications:

- Open the iOS Settings Application.
- Scroll down and tap on the “eK Pro” entry.
- Touch on the “Notifications” entry.
- Make sure the “Allow Notifications” switch is set to ON.
- Change the “Show Previews” option to “Always”.



No Service 1:44 PM 99%

Settings

Photos

Camera

Books

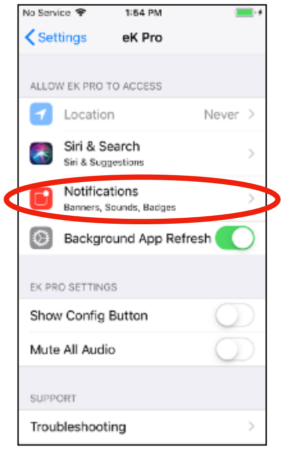
Podcasts

Game Center

TV Provider

Developer

eK Pro



No Service 1:54 PM

< Settings eK Pro

ALLOW EK PRO TO ACCESS

Location Never

Siri & Search
Siri & Suggestions

Notifications
Banners, Sounds, Badges

Background App Refresh

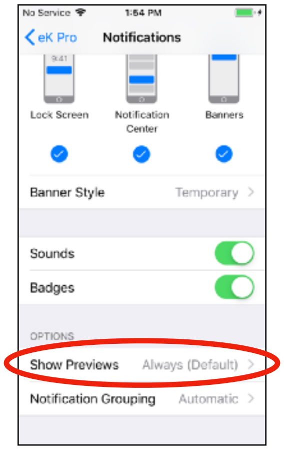
EK PRO SETTINGS

Show Config Button

Mute All Audio

SUPPORT

Troubleshooting



No Service 1:54 PM

< eK Pro Notifications

Lock Screen Notification Center Banners

Banner Style Temporary

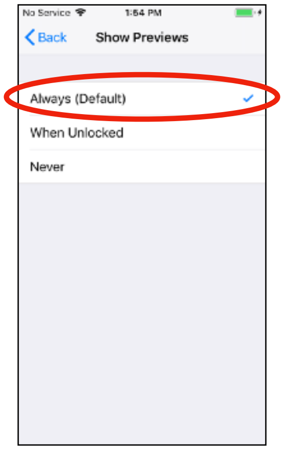
Sounds

Badges

OPTIONS

Show Previews Always (Default)

Notification Grouping Automatic



No Service 1:54 PM

< Back Show Previews

Always (Default) ✓

When Unlocked

Never

Push Notifications do not Appear when eKeypad Is Running

Push Notifications are designed to inform you when new information is available in eKeypad.

These messages do not appear if eKeypad running in the foreground. Under normal conditions, the eKeypad real-time connection will update the interface before any related notification message could possibly be received.

Advanced Configuration Help

Push Notification support in eKeypad was designed to allow for a wide range of flexibility in how it monitors equipment and distributes Push Notifications to end-users. This section shows a few examples of how to use eKeypad Push Notification support in more advanced configurations.

If you have a need to setup an advanced configuration we recommend that you contact eKeypad support for additional details and guidance. We will be glad to help.

Web Site:
https://www.ekeypad.net/

Help Articles:
https://www.ekeypad.net/help/

Document Downloads:
https://www.ekeypad.net/downloads/

Email Support:
support@ekeypad.net

PhoneSupport:
+1 (214) 497-4232

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

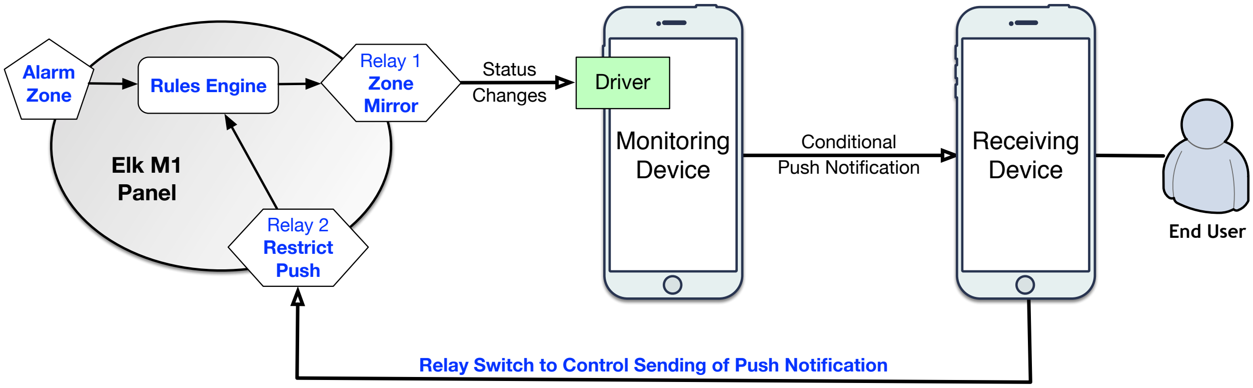
Below are a few examples of advanced push notification configurations.This is only a sampling of topics and does not cover all features of the eKeypad notification architecture.

End-User Disabled Notification

A common request is to allow end-users to enable and disable individual notifications. This ability is possible by using a special setup in the equipment being monitored.

The high level strategy is for the Monitoring Device not to monitor the primary item directly. Instead, a virtual item that mirrors the state of the primary should be monitored. The rules engine within the equipment is used to keeping the state of the two items synchronized. The additional of an additional push restricting relay is used to selectively control the synchronization rules and by extension sending push notifications.

Following is a more details example of this technique. It shows a setup that sends push notifications when an Alarm Zone changes to Violated on an Elk M1 panel. The end-user has access to a “Restrict Push” switch that will control if the push notification is sent.



1. Items that should be created in the M1 panel:

- A virtual relay named, “Zone Mirror”.
- A virtual relay named, “Restrict Push”.

Note

The “Zone Mirror” relay should only be visible to the Monitoring Device. See the “GUI Restrictions” functionality in eKeypad for more information.

2. Rules that should be setup in the M1 panel:

A. Zone not violated rule.
- Trigger: Alarm Zone changes to any state except Violated.
- Action: Change the Zone Mirror relay to OFF.

B. Zone violated rule.
- Trigger: Alarm Zone changes to Violated **and** Restrict Push relay is OFF.
- Action: Change the Zone Mirror relay to ON.

C. Push Restriction Enabled.
- Trigger: Restrict Push relay changes to ON.
- Action: Change the Zone Mirror relay to OFF.

3. Alert Manager Setup in the Monitoring Device:

The push notification alert configured in the monitoring device should **not** be triggered by changes in the state of the Alarm Zone itself. This alert should be triggered based on the state change of the Zone Mirror relay.

Once these items have been properly setup, the end-user will find a switch named, “Restrict Push” on the Outputs screen in eKeypad. Turning this switch to ON will prevent the push notifications from being sent; turning this switch to OFF will resume sending the push notifications.

Note

Using the setup described above, turning the Restrict Push switch to OFF while the Alarm Zone is already Violated will **not** send a push notification.

To have a push notification sent immediately, add the following rule.

D. Push Restriction Disabled.
- Trigger: Restrict Push relay changes to OFF **and** Alarm Zone state is Violated
- Action: Change the Zone Mirror relay to ON.

Consideration should also be given to the possibility that the Restrict Push toggle may be turned ON and unintentionally left in this state. There are a number of solutions to help manage this scenario, one of the most common is to use timers to automatically reset the push restriction switch to OFF after a period of time.

Monitoring Device Options

This document describes the recommended setup using a dedicated iPod Touch device as the monitoring device. There is technically no restriction on using a new iPod Touch device. In some scenarios it may be possible to alternatively use an iPhone or iPad. Following are the technical requirements that apply to monitor devices. We will only be able to provide support for monitoring devices that meet all of these requirements.

- **iOS Version**
  Push notification support in eKeypad require iOS 12 or higher. Older equipment that is only able to run older iOS versions will not be able to act as a monitors device.

- **Wired Ethernet**
  Wired ethernet adapters are only available for Lightning and USB-C connections. A wired ethernet adapter is a key requirement for a reliable monitoring device. Also, none of the iOS devices with the original 30-pin parallel connector support the minimum iOS version required to run versions of eKeypad supporting push notifications.

- **Dedicated Use**
  While it may be tempting to combine the monitoring device functionality with an existing device running eKeypad. This approach will cause reliability issues over time and is not supported. Monitoring devices should be dedicated ONLY for the purpose of monitoring and sending push notifications.

Multiple Receiving Devices

In this example, multiple end-users need to receive the same notification messages.

- There is no limit on the number of devices that can receive a Push Notification message.
- The optional Security Tag on Monitoring Devices must be setup on Receiving Devices.

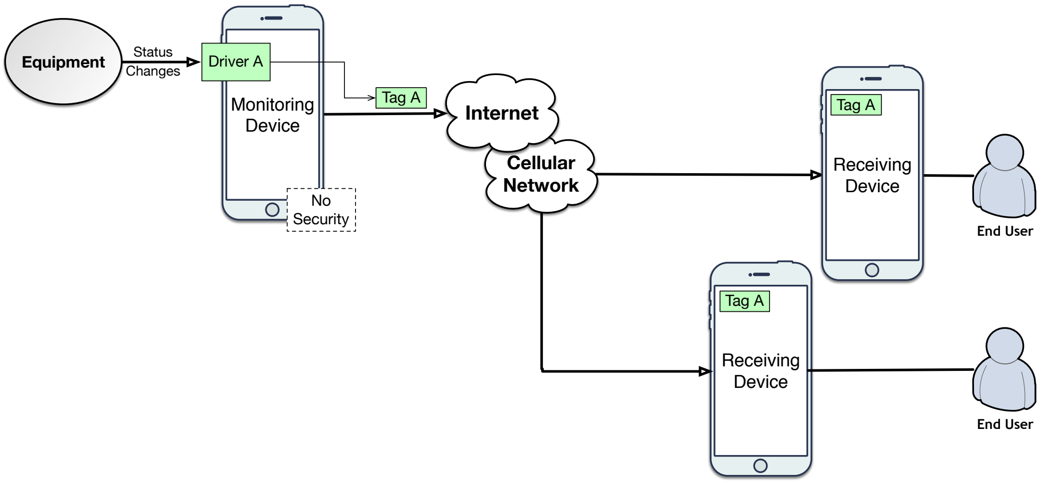


Diagram 2: Multiple devices receiving the same Push Notification message.

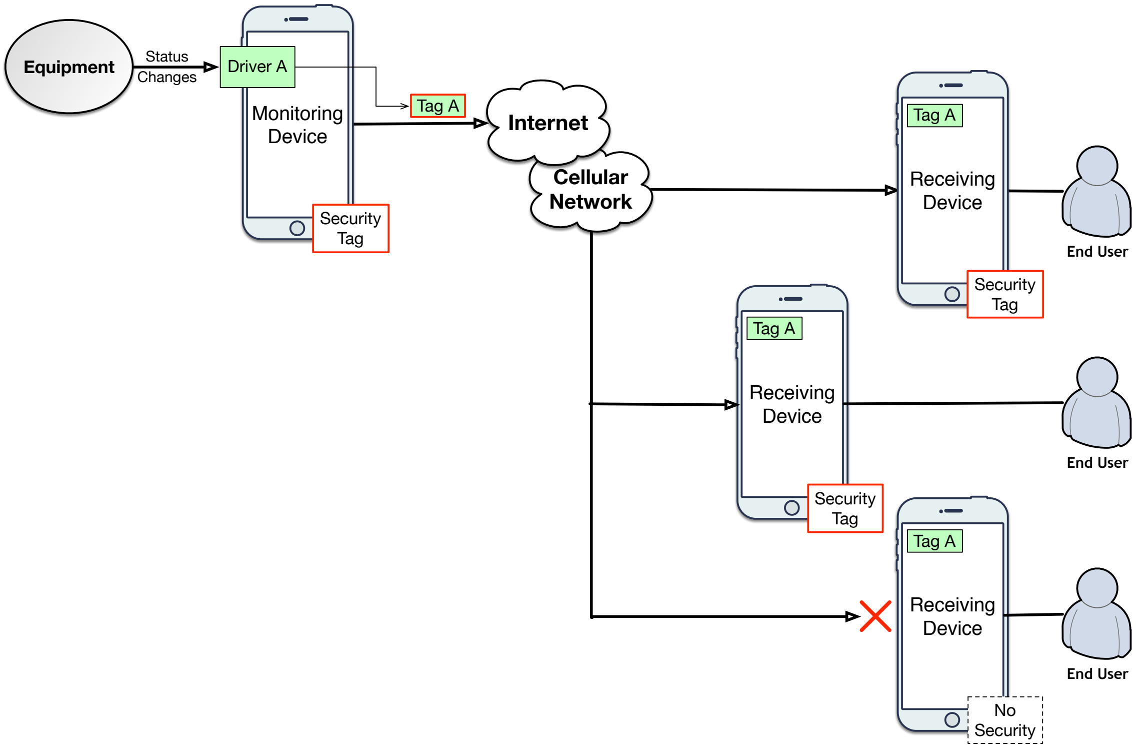


Diagram 3: Multiple devices with Security Tag restriction

Targeted Notification Delivery

This configuration example demonstrates how to divide Push Notifications so that different end-users can receive different notifications about the same equipment.

- When equipment is configured on a Monitoring Device the driver that is created is automatically assign a unique Push Notification Tag.
- Subsequently, configuring the same piece of equipment a second time will create a second driver with a different Push Notification Tag.
- The Alerts that define the triggers for Push Notifications are applied to a driver in eKeypad, not the equipment directly.

By using this information, Alerts can be configured for a single piece of equipment with different Tags. Properly configuring the end-users will allow you to select which notification they will receive.

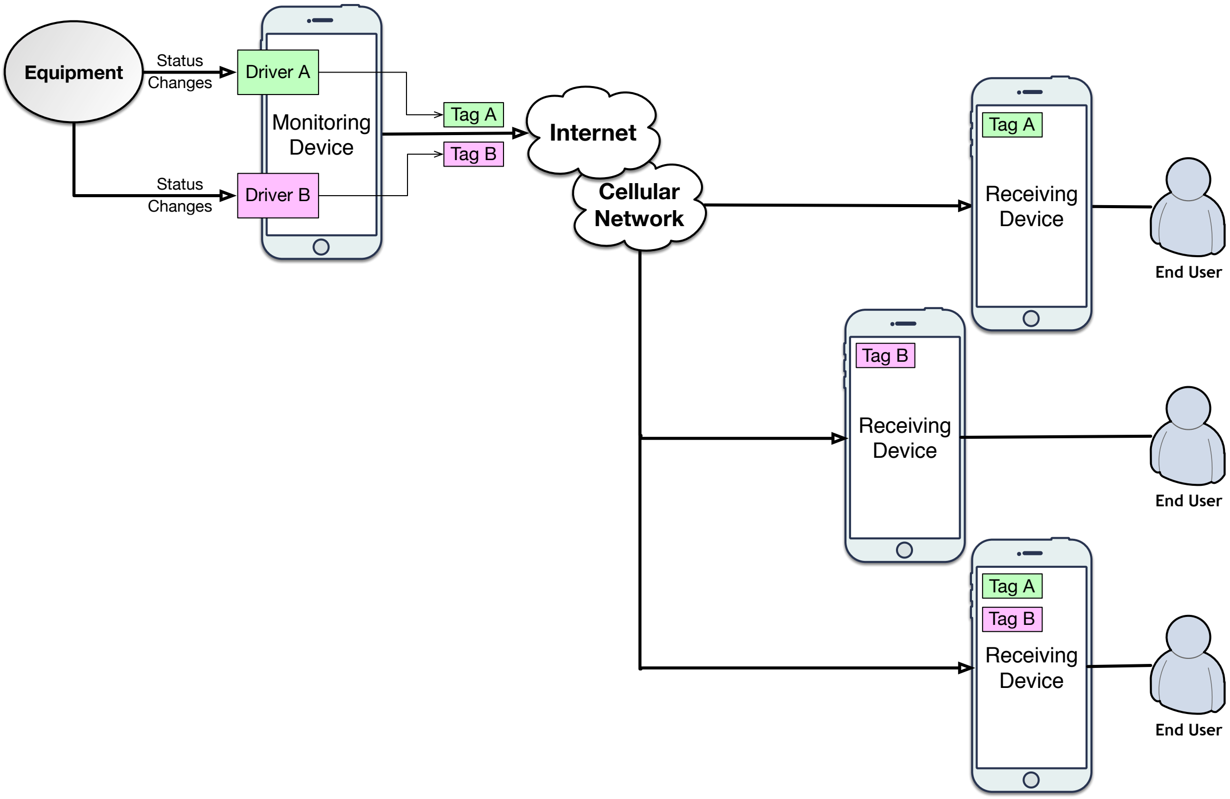


Diagram 4: Selective Push Notification Delivery

Multiple Equipment Locations

This example demonstrates an installer where the equipment that needs to be monitors is located in multiple physical locations.

- Monitoring Device should always be physically located in the same place as the equipment it is monitoring.
- For larger installs spread across multiple locations multiple Monitoring Devices will be required. Typically only one Monitoring Device is needed at each location.

Receiving Devices can receive notification messages from multiple monitors at the same time by configuring the appropriate Push Notification Tags. There is no limit on the number of Push Notification Tags that can be configured in a Receiving Device.

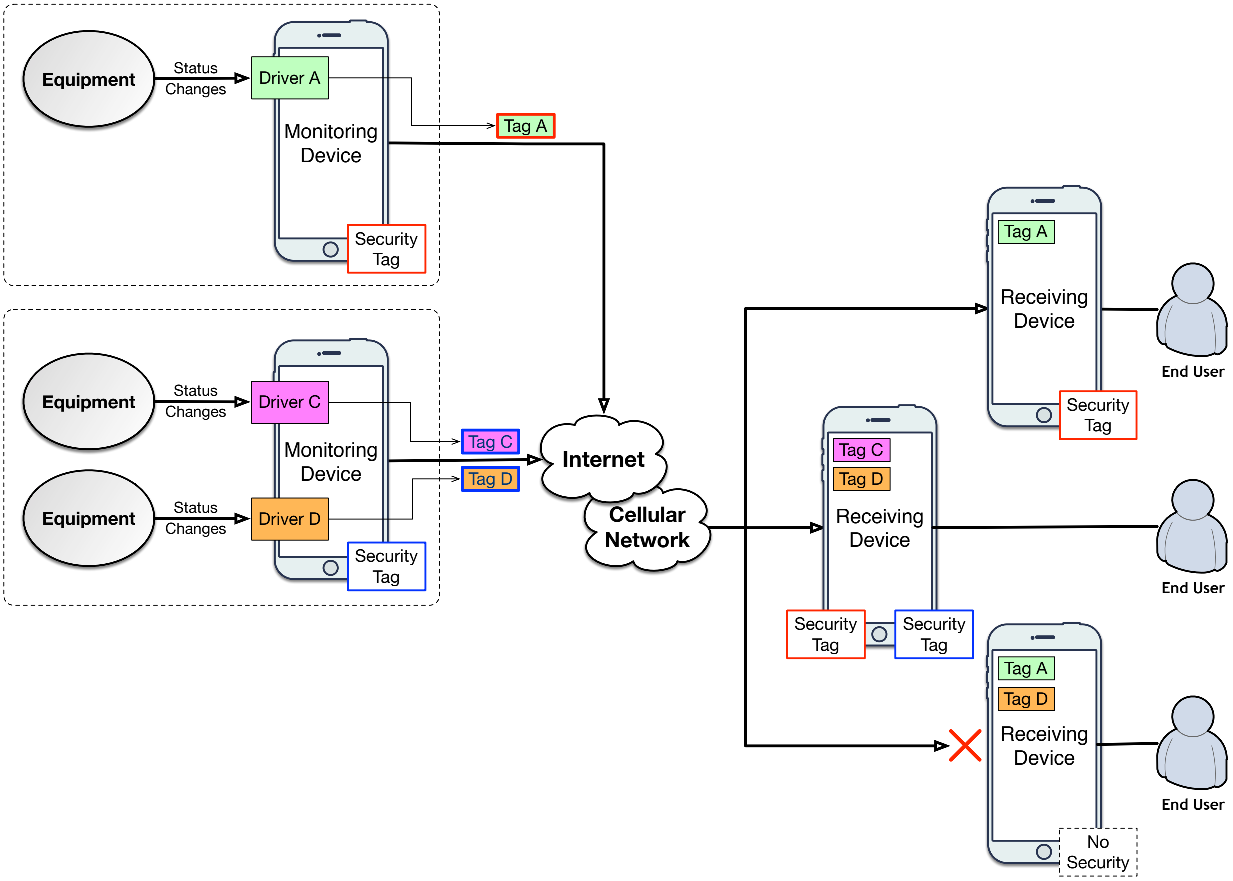


Diagram 5: Monitoring multiple equipment deployed in multiple locations

Document Change Log

Version	Notes
1.0	- Initial Version
1.1	- Added information about new Email Notification option - Changed best practice from Single Application Mode to Guided Access
1.2	- Updated screen shots for Configuration screens - Updated Push Monitor setup process - Updated Push Receiver setup process
1.3	- Updated with updated screen layouts - Updated with updated setup procedures - Removed Single Application Mode information