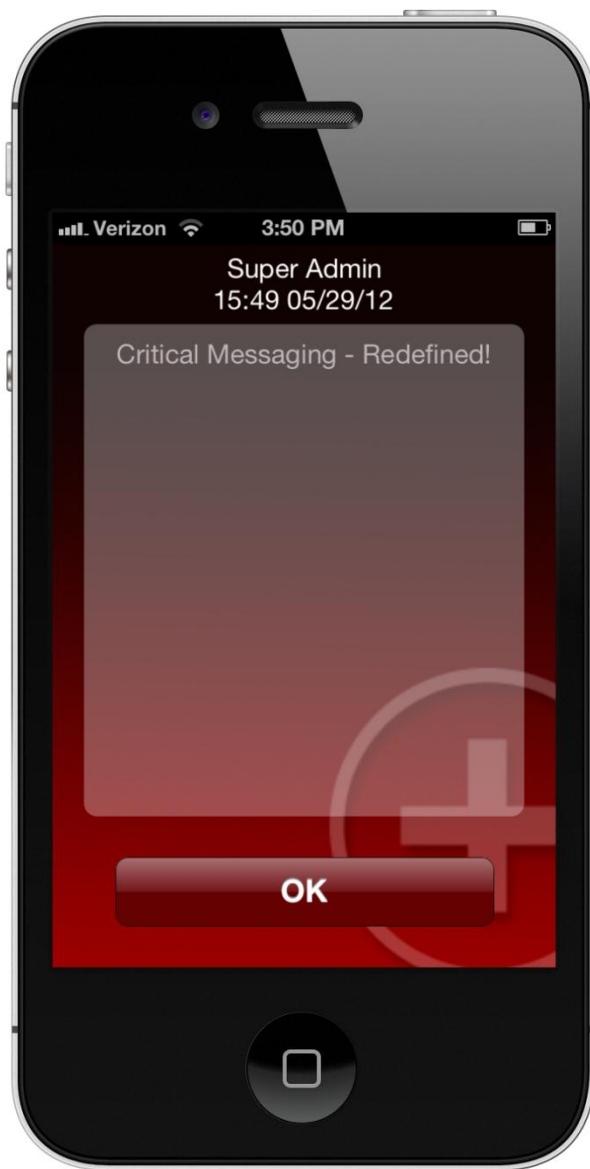


Zipit® Enterprise Critical Messaging Solution™
Zipit Confirm™ User Guide
for iOS Devices



Legal Notice

The software in the “Zipit products” which make up the Zipit® Enterprise Critical Messaging Solution™, and include the Zipit Now™, Zipit Confirm™ mobile application, and Zipit RAP™ console is Copyright © 2003-2013 Zipit Wireless, Inc. All rights reserved. Please visit <http://www.zipitwireless.com/legal/> for any updates to this notice, patents and/or trademarks.

Software Copyright Notice: Zipit products may include copyrighted Zipit and third-party software. Laws in the United States and other countries preserve for Zipit and third-party software providers certain exclusive rights for copyrighted software, such as the exclusive rights to distribute or reproduce the copyrighted software. Accordingly, any copyrighted software contained in Zipit products may not be modified, reverse-engineered, distributed, or reproduced in any manner to the extent allowed by law. Furthermore, the purchase of Zipit products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents, or patent applications of Zipit or any third-party software provider, except for the normal, non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Patent Notice: The Zipit products and/or technologies are covered by various U.S. and/or foreign patents. These patents include: US7,292,870; US7,894,837; US8,086,678; US8,190,694; AUS2005251096; AUS2009251161; JP5031556. Additionally, other U.S. and/or foreign patent applications are pending.

Trademark Notice: The “Z” logo, and Zipit are registered trademarks, and Zipit Enterprise Critical Messaging Solution, Zipit Now, Zipit Confirm and Zipit RAP are trademarks of Zipit Wireless, Inc.

Zipit® Enterprise Critical Messaging Solution™
Zipit Confirm™ User Guide
for iOS Devices



- **What's Included?**
- **Data Usage**
- **Battery Usage**
- **Installing Zipit Confirm on your Mobile Device**
- **Logging in for the First Time**
- **Configuring Your Mobile Device**
- **Application Features and Layout**
- **Receiving and Responding to a Critical Message (Page)**
- **Sending a Critical Message (Page) from your Smartphone**
- **Receiving a Zipit Chat or a ZText**
- **Sending a Zipit Chat or a ZText**
- **Message Inbox**
- **Accessing and Managing Contacts in Your Contacts List**
- **Enterprise Control and Security Features**
- **Using Zipit Confirm on Additional Mobile Devices**

What's Included?

Zipit's service pricing includes unlimited critical messages (pages), unlimited Zipit Chats, unlimited ZTexts, online access to a corporate directory, as well as administrative access to the Remote Administration Portal otherwise known as the RAP.

Receive Critical Messages:

- Enables delivery of critical messages with 4 levels of priority that require a response and can be tracked in real time by a dispatcher to determine if an event is being properly addressed by the recipients.
- All critical messages are encrypted for security and logged in the RAP so that they can be reviewed at any time.

Send Critical Messages:

- Enables the initiation of critical messages from the Smartphone to Paging Groups and/or Users with expiration options, 4 priority levels, multiple response options, and a free form message.
- Once a message is sent, a status screen is updated in real time showing how long it took to send (process), deliver, and respond to the message, along with each user's response.
- All critical messages are encrypted for security and logged on the cloud-based server (RAP) so that they can be reviewed at any time.

Zipit Chat:

- Enables text-based communication with Zipit Now devices and other Zipit Confirm mobile application users.
- All Zipit Chat communication is encrypted for security and logged in the RAP.
- Sent and delivery status is tracked for each message sent.
- The enterprise can control which contacts can be reached and which can be blocked.

ZText:

- Enables text-based 2-way communication with standard cell phones via text (SMS), even when your device is connected to Wi-Fi. (Typical SMS communications occurs over a cellular voice network.)
- All ZText communication is logged in the RAP.
- The enterprise can control which contacts can be reached and which can be blocked.

Enterprise Contacts List:

- Ability to search for and add corporate users and address books.
- Address books of contacts can be pushed by the administrator to your device.
- Automatic updates to all contacts if the corporate directory changes.

Data Usage

The Zipit service uses bandwidth provided from your cellular provider and will contribute to data usage. Typical data usage for a single month is approximately 10.5 MBs of data based on 2,000 pages received and responded to, 1,000 Zipit Chat messages sent, 1,000 Zipit Chat messages received, 1,000 ZText

Zipit® Enterprise Critical Messaging Solution™

Zipit Confirm™ User Guide

for iOS Devices



messages sent, 1,000 ZText messages received, 100 contacts added to the address book, and 100 address book updates. All Zipit services also work when using a Wi-Fi data connection and, during such a connection, do not affect cellular data usage charges. Software updates, if provided while connected to cellular, may consume up to an additional 20 MBs.

The Zipit Confirm mobile application does not use your cellular provider's standard SMS (text messaging service) and therefore has no impact on your cellular provider's SMS charges.

Battery Usage

Battery usage will vary depending on how often you use the Zipit Confirm mobile application. However, simply having the application installed and running on your device will have very little, if any, impact on your battery life.

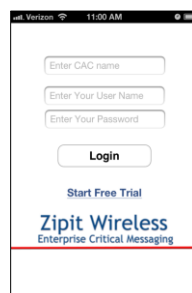
Installing Zipit Confirm on your Mobile Device

The Zipit Confirm mobile application can be downloaded for free from the iTunes Store to any iOS device including iPhone, iPad, and iPod. Search for Zipit Confirm and select the "Download" button and follow the instructions.



Logging in for the First Time

First time use of the Zipit Confirm mobile application requires you to enter a Customer Access Code (CAC), a Username, and a Password and then select the Login button. The login information should be provided by your system administrator that manages users of the Zipit Enterprise Critical Messaging Solution. This administrator must designate your device type as a "Smartphone". Login information is only required again if the application is removed and then re-installed or if you login to the application on a different mobile device.



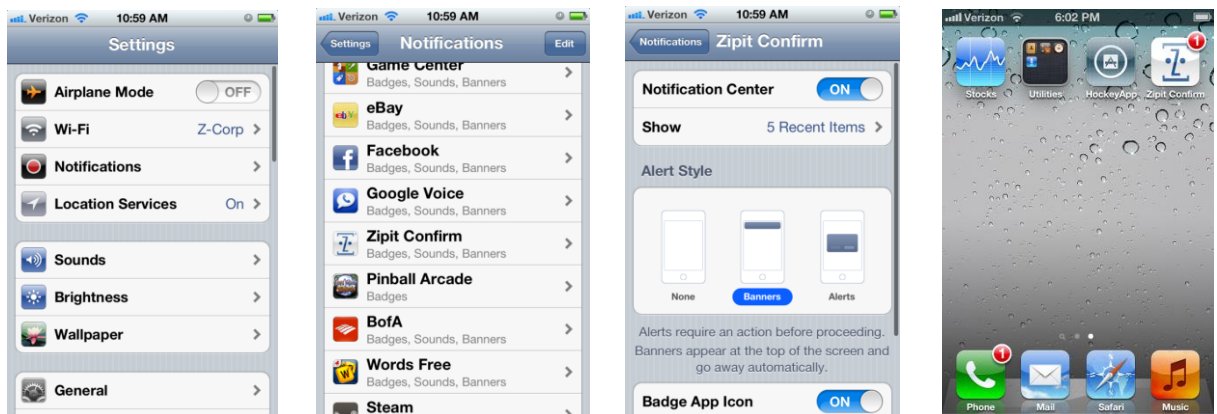
Configuring Your Mobile Device

There are two keys to ensure that your Zipit Confirm mobile application performs as intended.

1. **Notifications:** If you don't know that a new message has arrived, the solution is not going to meet your expectations. Therefore, it is critical that you receive notifications when a critical message, Zipit Chat, or ZText is delivered.

For iOS mobile devices, the device settings (not the application's settings) need to be properly configured in order to receive notifications. Choose these options in Settings > Notification > Zipit Confirm:

- **Notification Center:** Set this to "On".
- **Alert Style:** Select Banners or Alerts.
- **Badge App Icon:** Set this to "On". Allows the message count to appear on your application icon.
- **Sounds:** Set this to "On". This will allow notifications to make a sound based on your volume settings. If this is Off, notifications will never make a sound.
- **View in Lock Screen:** Set this to "On". This setting allows you to see an alert on screen even if your device is locked.



In addition, we recommend placing your Zipit Confirm mobile application icon on your Main Screen so that you can see a count of the number of incoming messages that have been delivered. A small badge with the count will appear at the upper corner of your application icon (as shown above).

2. **Wi-Fi Connectivity:** One of the benefits of the Zipit Confirm mobile application is that all communications, including ZText, work on Wi-Fi just as they work when your mobile device is connected to a cellular data network. In many facilities, especially larger facilities and hospitals, cellular coverage may not be available in all areas. It is important that your mobile device is configured to support Wi-Fi so that the Zipit Confirm mobile application can receive critical messages even when cellular coverage is not available.

Please contact your IT staff to make sure that your device is enabled to connect to your enterprise's Wi-Fi infrastructure.

Application Features and Layout



Messages – Provides access to all message types including critical messages, Zipit Chats, and ZText messages. You can delete a message, filter messages by type, and initiate a critical message or Zipit Chat from this screen.



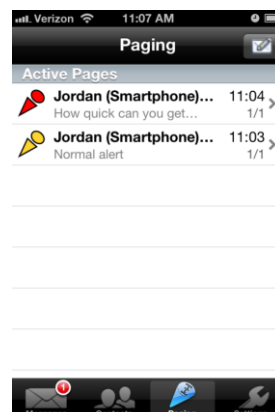
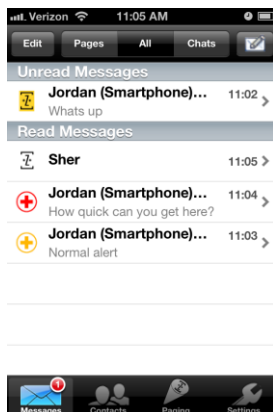
Contacts – Provides access to all address books and individual contacts stored locally with your application as well as providing access to contacts that can be searched and retrieved from your enterprise's database.



Paging – Provides ability to initiate critical messages and Zipit Chats from your Smartphone. This feature can be enabled or disabled by your administrator. If disabled, the Paging tab will not appear in the tab bar at the bottom of the screen.



Settings – Provides access to application settings such as Team invite/sharing, sounds, stats, timeout, require paging confirmation, paging defaults, network status, user information (CAC, Username, Email2Page address), Logging Out, software version, ZText number, and feedback.



Receiving and Responding to a Critical Message (Page)

Critical messages can be sent to your Mobile Device with one of four priorities. The priority of the message determines how you are notified.

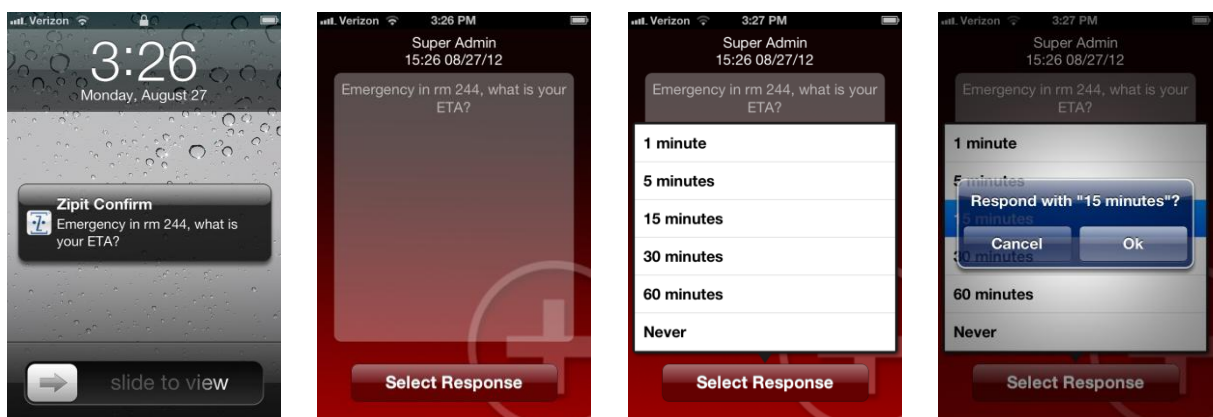
- **Priority 1 - Mayday Alerts:** If the Zipit Confirm mobile application is not open, Mayday Alert messages generate a push notification that displays a banner or alert pop-up. The device will use your notification volume and vibration settings for the alert. The push notification and its associated

alerts will repeat until the application is opened. When the application is opened, the alert sound repeats at the application volume setting and the device vibrates until you provide a response. If the Zipit Confirm mobile application is open when the message is initially delivered, the alert sound repeats at the application volume setting and the device vibrates until you provide a response. Mayday Alerts block all other Zipit Confirm mobile application activities until a response is provided.

- **Priority 2 - High Priority Alerts:** If the Zipit Confirm mobile application is not open, High Priority Alert messages generate a push notification that displays a banner or alert pop-up. The device will use your notification volume and vibration settings for the alert. The alert sound is distinct from P1 alert. The push notification and its associated alerts will repeat until the application is opened. When the application is opened, the alert sound repeats at the application volume setting and the device vibrates until you provide a response. If the Zipit Confirm mobile application is open when the message is initially delivered, the alert sound repeats at the application volume setting and the device vibrates until you provide a response. High Priority Alert messages block all other Zipit Confirm mobile application activities until a response is provided.
- **Priority 3 - Normal Priority Alerts:** If the Zipit Confirm mobile application is not open, Normal Priority Alert messages generate a push notification that displays a banner or alert pop-up. The device will use your notification volume and vibration settings for the alert. The alert sound is distinct from P1 and P2 alerts. The push notification and its associated alert will only play once. When the application is opened, the alert sound plays once at the application volume setting. If the Zipit Confirm mobile application is open when the message is initially delivered, the alert sound plays once at the application volume setting. Normal Priority messages are accessible in the Message Inbox.
- **Priority 4 - Mailbox Alerts:** If the Zipit Confirm mobile application is not open, Mailbox Alert messages generate a push notification that displays a banner or alert pop-up. The device will not make any sound and will not vibrate. Mailbox Alert messages will be accessible in the Message Inbox when the Zipit Confirm mobile application is next opened. If the Zipit Confirm mobile application is open when the message is initially delivered, the message appears in your Message Inbox without any sound or vibration.

One or more response options will be provided with each critical message. Select the desired response, or, if allowed, enter a custom response and then confirm the choice.

P1 and P2 Page Alerts:




Zipit® Enterprise Critical Messaging Solution™

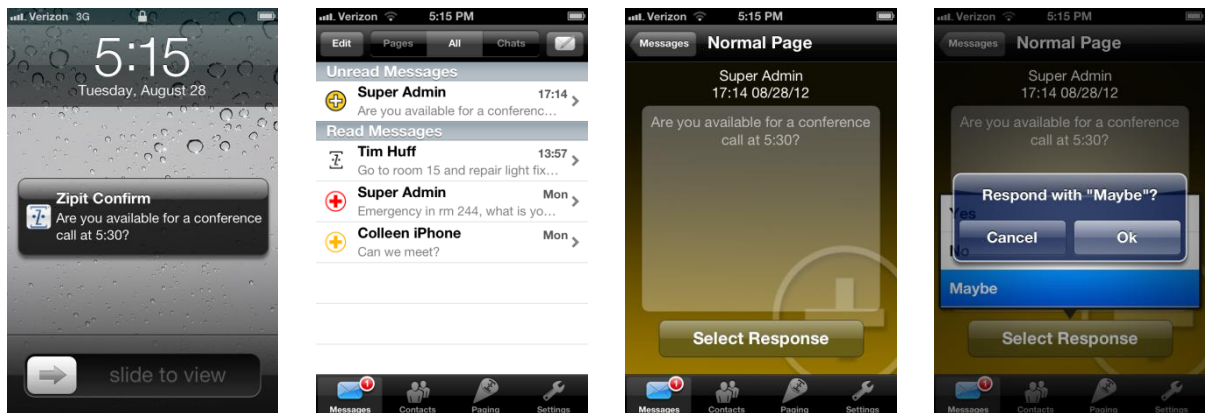
Zipit Confirm™ User Guide

for iOS Devices




Priority 1 and Priority 2 messages only appear in the Message Inbox after you have responded to the message and therefore never appear in the Message Inbox as “Unread”. Priority 3 and Priority 4 messages that are sent to the Message Inbox will appear as “Unread” until a response is provided, even if the message has been opened and viewed. The number of unread messages will also be displayed in the top right hand corner of the Message Inbox icon  at the bottom of your device.

P3 and P4 Page Alerts:



All critical messages are logged in the Remote Administrative Portal (RAP). The maximum incoming critical message length is 250 characters.

Sending a Critical Message (Page) from your Smartphone

If your administrator has enabled you to have rights to send critical messages, selecting the Create New Message icon  will allow you to choose between sending a Page Alert and sending a Zipit Chat/ZText Message.

Select the Create New Message icon from the top right of the screen and then select the “Send Page” option. You can then select the Paging Group(s) and/or User(s) that you want to send the page to; select the Priority Level of the page with “P1 – Mayday” being the highest priority and “P4 – Mailbox” being the lowest priority (your administrator may have restricted the priority levels you can use); select the expiration time (the time after which a response is no longer required or allowed); select from a list of canned Response Options (defined by your administrator); select if a Custom (Free) Response is allowed, not allowed, or optional; and enter your message. To send the message, press the Send icon in the top right corner of the screen. You can cancel this message at any time by pressing the Cancel option in the top left hand corner of the screen.

As soon as the message is sent, you will be provided with a summary screen that is updated in real time with the status of the message for each intended recipient (sent, delivered, and response information).


Press the Paging icon  to view your paging history (a list of messages in the order they were sent –

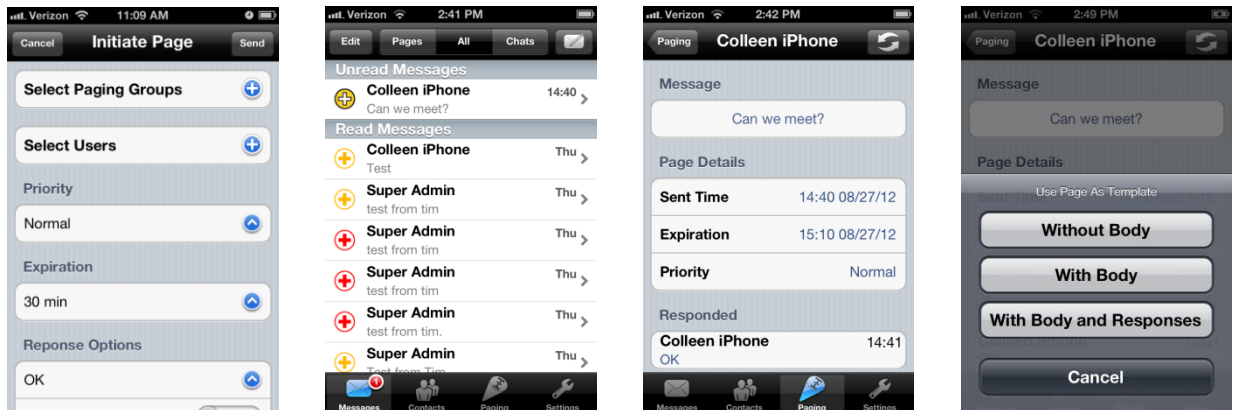
Zipit® Enterprise Critical Messaging Solution™

Zipit Confirm™ User Guide

for iOS Devices

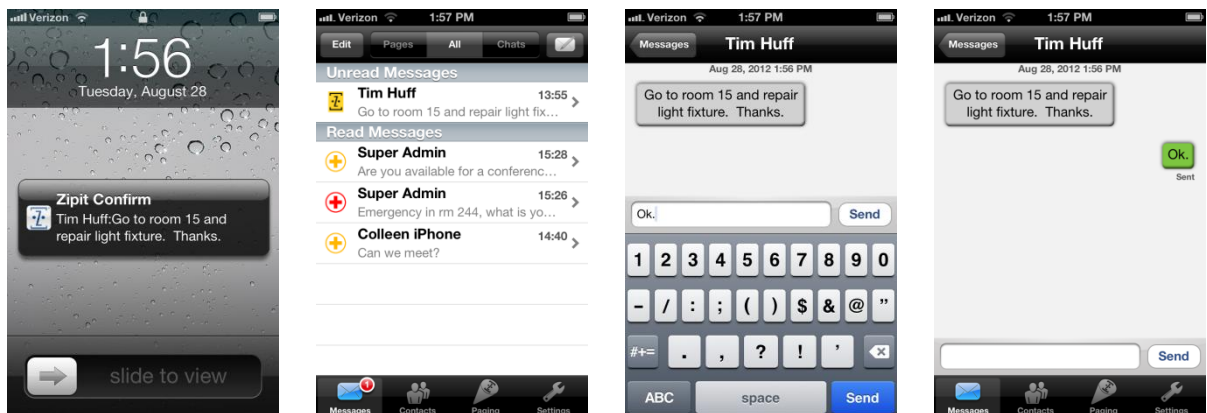


most recent to oldest). Select any page to review the status of each recipient. If you ever need to send a second page using the same options as in a previously sent page, simply pull up the page that was sent, and click on the create Template icon . You can choose to use the existing page as a template “Without Body”, “With Body”, or “With Body and Responses”. Click the Cancel option to return to the previous screen.



Receiving a Zipit Chat or a ZText

An incoming Zipit Chat or ZText will generate a push notification that displays a banner or alert pop-up. The device will use your notification volume and vibration settings for the alert. The push notification and its associated alert will only play once. Go to your Message Inbox to view the message.



Sending a Zipit Chat or a ZText

You can compose a message three ways:



- 1) Open an existing conversation from the Message Inbox and type in a new message (as shown above).

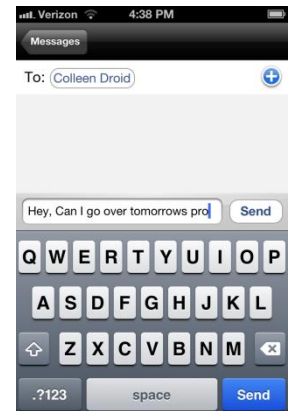
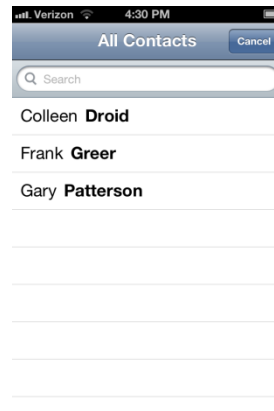
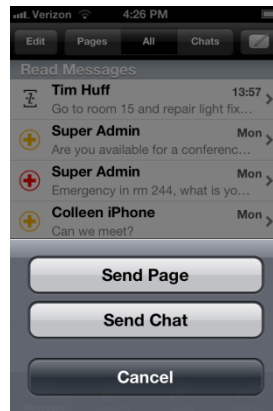
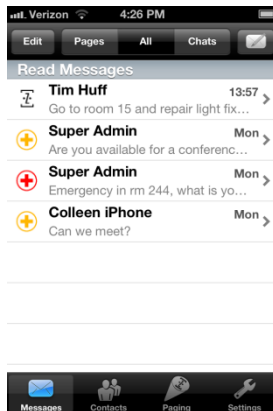
Zipit® Enterprise Critical Messaging Solution™

Zipit Confirm™ User Guide

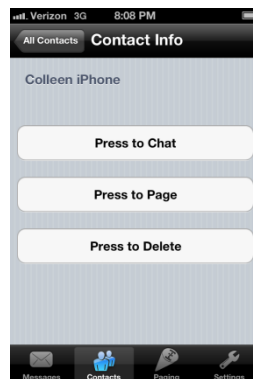
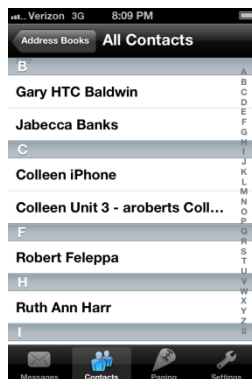
for iOS Devices



- 2) Select the Create New Message icon  in the top right hand corner of the Message Inbox screen, choose “Send Chat” option. Press the Blue Plus Sign icon  at the top right if you want to select a recipient from your Contacts List, or click on the Search criteria field, and enter a user’s name or a 10-digit phone number in the “recipients” field. If the message is being sent to multiple recipients (you can include a combination of Zipit Chat users as well as ZText users), enter multiple names or numbers in the “recipients” field.



- 3) Select a contact from the Contacts List  and choose the desired action from the available options (such as “Press to Chat”, “Press to Page” or “Press to Delete”).



Note: All Zipit Chats and ZText conversations are logged in the Remote Administrative Portal (RAP). The maximum Zipit Chat or ZText message length is 140 characters.

Message Inbox

Messages are always displayed in order of the time they were sent or received, with the newest message appearing at the top of the Message Inbox. Messages that have not been read or, in the case of critical messages, have not been answered are grouped at the top of the Message Inbox in Unread Messages.


Zipit® Enterprise Critical Messaging Solution™

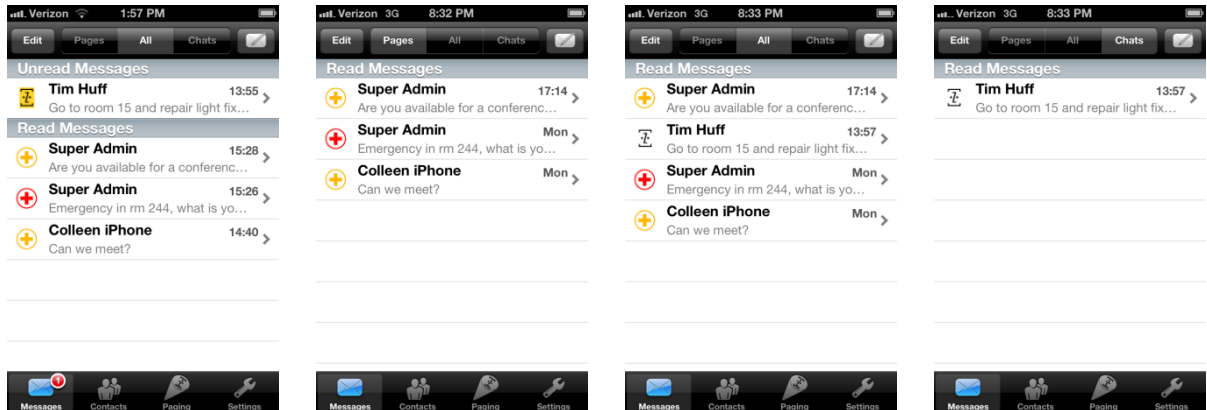
Zipit Confirm™ User Guide

for iOS Devices






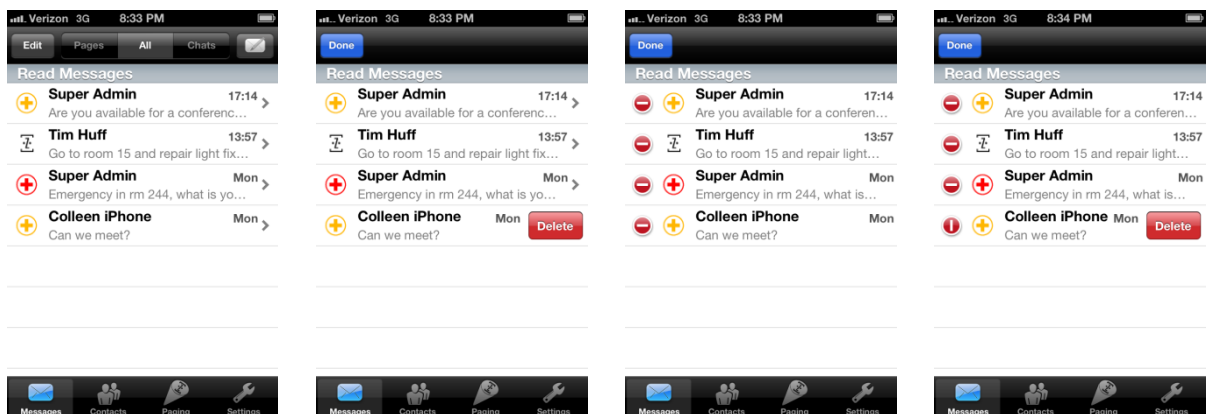
Filtering Messages:

- 1) By default, all message types are displayed within the Messages Inbox. Unread messages are grouped at the top of the Message Inbox and Read messages at the bottom.
- 2) Filtering allows you to view a subset of the messages in the Message Inbox.
- 3) Messages can be filtered by type (Pages only, All Messages, Chats only) by selecting the desired filter from the filter bar  that is provided just above the list of messages.



Deleting Messages:

- 1) Messages can be deleted from the Message Inbox by swiping a conversation to the right. A Delete button  will appear. Tap the Delete button to delete the message or touch elsewhere to cancel. Once completed, tap  to return to the Messages Inbox view.
- 2) Messages can be deleted by tapping the Edit icon  on the top left of the Message Inbox. A minus sign appears beside each conversation. Tap the minus sign and then the Delete button to delete the message.
- 3) Messages are automatically deleted based on settings controlled by your administrator.




Accessing and Managing Contacts in Your Contacts List

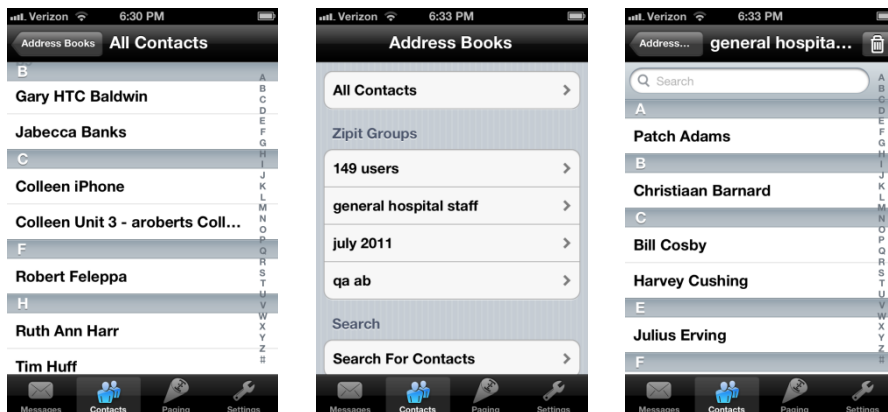
Contacts can be managed entirely by your administrator, by you, or a combination of both. Your administrator can:

- 1) Push address books to your application so that your contacts appear in your Contacts List automatically.
- 2) Lock your Address Book so that you can only access contacts that are pushed your device.
- 3) Block Personal Contacts so that you can't add your own contacts.

Your contacts are accessible by selecting the Contacts tab at the bottom of your screen. Contacts are always displayed in alphabetical order by the user's first name. You can do a quick search of your contacts by entering the first few characters of a user's first or last name in the search field at the top of the Contacts List. You can also scroll through the list to find a contact.

Filtering Contacts:

- 1) Your Contacts List view can be filtered to show only contacts that are included in a selected address book. Select the Address Books icon  at the top left of the All Contacts screen and select the address book to view.



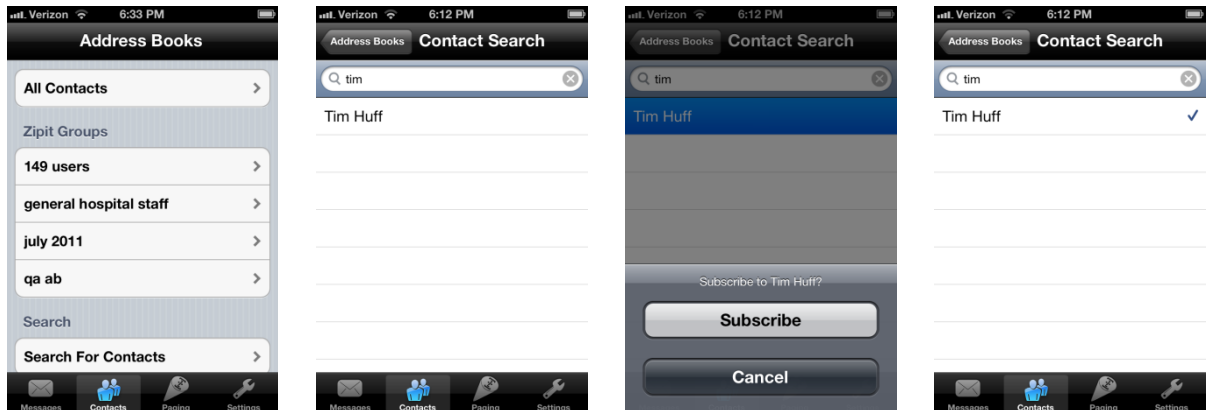
Adding Contacts (if your administrator allows it):

- 1) Contacts can be added from your enterprise's database of contacts by selecting Search For Contacts at the bottom of the Address Books view. Enter as many characters as you wish to match the name of the desired user or address book. Tap the Search icon to initiate the search. All users and address books that match your search will be displayed. A check mark to the right of an entry let's you know that user and/or address book is already added to your Contacts List. If no check mark is visible, you can touch on the entry and a Subscribe option will appear allowing you to add this user or address book to your Contacts List. Once added it will now be displayed with a check mark. If you add an address book, all users that are included in the address book will be added to your Contacts List and you will also be able to filter your Contacts List view by the address book.

Zipit® Enterprise Critical Messaging Solution™


Zipit Confirm™ User Guide

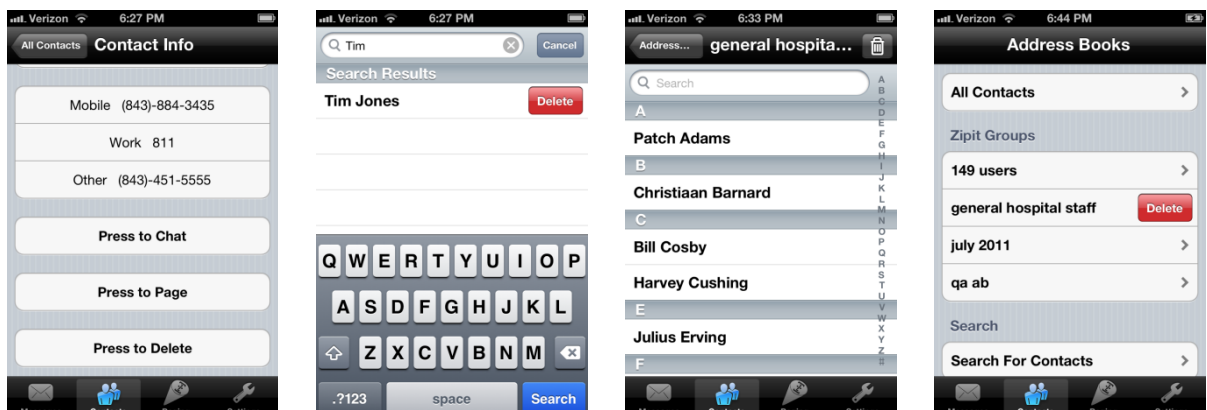
for iOS Devices



- 2) Personal Contacts cannot be added to your Zipit Confirm Contacts list. However, if your administrator has enabled Personal Contacts, a Blue Plus sign will be available when creating a new message so that your personal contacts stored within your device's personal contact address book can be messaged via ZText.

Deleting Contacts:

- 1) Contacts can be deleted by selecting a contact and then tapping the Press to Delete option at the bottom of the screen.
- 2) Contact can be deleted from the contact list by swiping a contact to the right. A Delete button will appear. Tap the Delete button to delete the contact or touch elsewhere to cancel.
- 3) Address books can be removed by selecting the address book and then tapping the Trashcan icon  in the upper right corner of the screen.
- 4) Address books can be deleted from the Address Books view by swiping an address book to the right. A Delete button will appear. Tap the Delete button to delete the address book or touch elsewhere to cancel.



Enterprise Control and Security Features

Zipit Confirm is designed to allow your enterprise to manage your application remotely. The following capabilities are managed by your administrator.

- **Require Password after Timeout** – allows the administrator to enforce security. If it is enabled by the administrator, you will be required to use one of the four time intervals provided in Settings/Lock Timeout and then provide your password prior to accessing the application (the same password that you logged into the application with on your first login).
- **Lock Address Book** – allows the administrator to lock your address book so that you can't add enterprise or personal contacts. Only contacts that are in address books that are pushed to your device by the administrator will be available in your Contacts List.
- **Allow Personal Contacts** – if enabled by the administrator, you will be able to access your device's personal contact address book.
- **Enable ZText** – if enabled by the administrator, a 10-digit cellular number will be assigned to the application, and you will be able to SMS text message cellular users.
- **Lock Application / Unlock Application** – if Locked by the administrator, your application will be unusable until the administrator Unlocks it. This can be useful if you misplace your device and want the administrator to lock the device until it is found.
- **Wipe Application** – if this command is issued by the administrator, your application will be wiped of all user data and will be reset to the state of a brand new download.

Using Zipit Confirm on Additional Mobile Devices

Each Zipit Confirm license can be assigned to only one user and cannot be shared by multiple users (unless the users share a username – such as a role).

Using the Application with Multiple Devices:

The Zipit Confirm mobile application can be run on as many devices as you choose – but only one device at a time per user. If you access the application from another device, you will be required to Login with your CAC, Username, and Password – just like with your initial login. Once you login, your original application will be wiped of all user data. Don't worry, when you login again on a second device, your contacts, settings, and unanswered critical messages will be restored. Previously read messages will not be restored but are available to view from the Remote Administration Portal (RAP).

Replacing Your Mobile Device:

If you ever replace your mobile device, the license will automatically transfer to the new device once the application is installed and you have logged in. All of your contacts, settings, and unanswered critical messages will be restored. Previously read messages will not be restored but are available to view from the Remote Administration Portal (RAP).