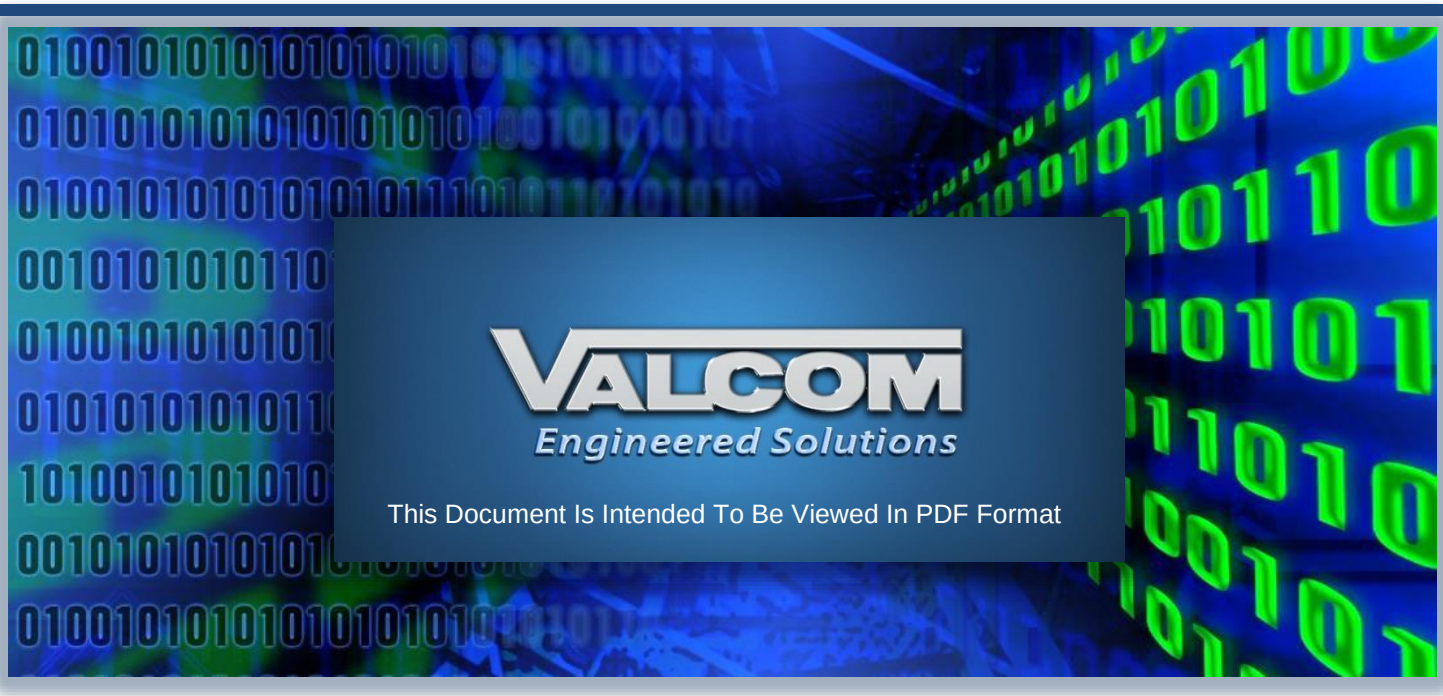


IP6000 Emergency Notification System

VE6024 Server Overview

rev. 2022-1.00

This document describes the functionality and set up of the VE6024 eLaunch Server and the VE6025 Application Server Pro. These 2 products form the core of Valcom's IP6000 Emergency Notification System. The products used in conjunction with the VE6024 and VE6025 vary from installation to installation.

This document was written around the following firmware revisions:

VE6024 2.4.0

The latest revision of this document may be found here.

Other important information including network requirements may be found here.

IP6000 initial system setup is accomplished with the VIP-102B IP Solutions Setup Tool. A video example may be found here and a reference manual may be found here.

Please submit corrections or suggestions to bfg@valcom.com

Table of Contents

A Practice You'll Never Regret

Make it a habit to backup all programming (VIP-102B Snapshots, all system server(s) backups, other system programming) whenever you begin work on an existing system *and* whenever you complete programming or maintenance of a system. Always save all backups with names identifying what they are and the date and time they were saved.

Include a text document with the backups describing the changes that were implemented. Keep copies of backups both on site, and off site.

Valcom's IP6000 Emergency Notification Communication System features an IP platform. The many benefits include unlimited system size, remote management and diagnostics, inherent supervision and deployment on any scale – single building, campus, town, state or global.

Valcom's IP6000 system works on the concept of IP endpoints connected through a properly configured network platform. These POE devices may be one way or two-way speakers/horns, audio gateways which can be used to interface with analog systems, clocks, LED signs, FXS or FXO ports allowing for staff generated announcements from the telephone system or input/output gateways to trigger, or receive triggers from, other systems for automated emergency or security messages.

Each Valcom IP endpoint must be programmed with a unique IP address (static or DHCP) and a unique "channel dial code". An unlimited number of audio groups may be created to facilitate simultaneous broadcast through multiple endpoints.

By design, each Valcom IP endpoint "remembers" all other endpoints so that there is no single point of failure. As long as proper network connectivity exists between endpoints, they will continue to interoperate.

There are a number of optional servers that allow the IP6000 system to be utilized in applications such as school intercom, hospitals, universities, manufacturing and other facilities requiring scalable emergency mass notification.

VE6024

The VE6024 eLaunch server provides single point, multimodal distribution of emergency information.

When an emergency occurs, users initiate the distribution of the intended emergency notification by selecting a "Scenario".

The information dispensed by Scenarios may be completely predefined, completely ad hoc (made on the fly), or a combination, where the predefined content can be modified just prior to launch. There is no practical limit to the number of scenarios that can be defined in a VE6024.

The **VE6024** eLaunch server Scenarios:

a) Generate one-line posts to HTTP addresses (websites, etc.)
b) Generate posts to Twitter™
c) Generate posts to Facebook™
d) Generate CAP 1.2 (Common Alert Protocol) formatted XML messages

These CAP messages:

1) May be pushed out via HTTP
2) May be polled as RSS feeds
3) May be polled as ATOM feeds
4) May be sent as e-mails

VE6025

The VE6025 Application Server Pro can turn CAP messages, like those generated by the VE6024, into audible and visual alerts.

The VE6025 Application Server Pro allows users to import WAV audio files, create WAV audio files via telephone dial codes or create WAV audio files from text (for example, CAP messages) via an onboard text-to-speech engine. The system can accommodate WAV files as large as 20MB.

The VE6025 can record Valcom VoIP group announcements. These recorded announcements:

a) May be archived for future use
b) May be immediately broadcast
c) May be delay broadcast for feedback prevention
d) Any combination of the above

Sequential announcements to the same recorded group may be stacked and played in the order of completion. This is ideal for high paging traffic in hospitals or airports.

Any action invoked by the VE6025 is in the form of an “event”. Events may:

Send an audio file to a group of VoIP endpoints.

Send a text file to a group of IP LED signs.

Pop up a message on Windows based computers.

Convert a text-based CAP message to audio via the onboard text-to-speech engine and send it to a group of VoIP endpoints (speakers, horns, LED signs, screen pop ups, speakers in select IP telephones)

Invoke a Scenario on a VE6024 eLaunch server.

Initiate or stop an audio stream (music and other program material) to a group of VoIP endpoints.

Operate a relay on a VE8048A I/O unit to control ancillary devices.

Cause a State Change Event allowing users to force VE8048A I/O gateway inputs or audio group recordings to be enabled or disabled. This is useful in situations where users wish

to ignore an VE8048A input during certain times of the day and or only wish to record announcements to audio groups at defined times.

Stop any currently active event, Play List item, audio stream or relay.

Define a delay in seconds (delays are used between chained events in Play Lists and Schedules)

Define a test room priority mask in order to dictate a priority level that must be exceeded for successful audio and/or text broadcast. This allows for scheduled “quiet time” where only high priority audio can broadcast.

Events may be controlled or chained for sequential operation:

a) by Schedules
b) by Play Lists

Schedules must be controlled by the Calendar. They may be automated by day of the week or calendar date.

Play Lists provide for non-scheduled triggering of events. Multiple events in a single Play List may be chained for sequential deployment.

Parallel Play Lists are combinations of single Play Lists that will operate simultaneously.

Play Lists/Parallel Play Lists may be controlled:

a) manually within the VE6025
b) by the text monitor. The text monitor can receive data from other network endpoints, Valcom or otherwise, and scan for specific content within that data. If found, the matched string will trigger a Play List item
c) by CAP filters. These filters process messages received from user defined CAP sources. If the filter rules are satisfied, then the filter will simultaneously start one or more Play List item(s). Multiple filters may be applied to CAP sources. As filter rules are satisfied, each associated Play List item will start and complete before the next filter is processed
d) by VE8048A inputs
e) by Icons on a VE6025 graphic

The VE6025 can provide 12 unique communication streams simultaneously.

VE6023

The VE6023 Telephone Application Server is an interface between an IP telephone system and Valcom VoIP groups. It allows the speakers in select IP telephones to receive Valcom group announcements. IP phones may be associated with any number of Valcom VoIP groups. This device also allows synchronization between the audio broadcast timing from the IP phone speakers and any other Valcom VoIP endpoints. The VE6023 has a separate installation manual.

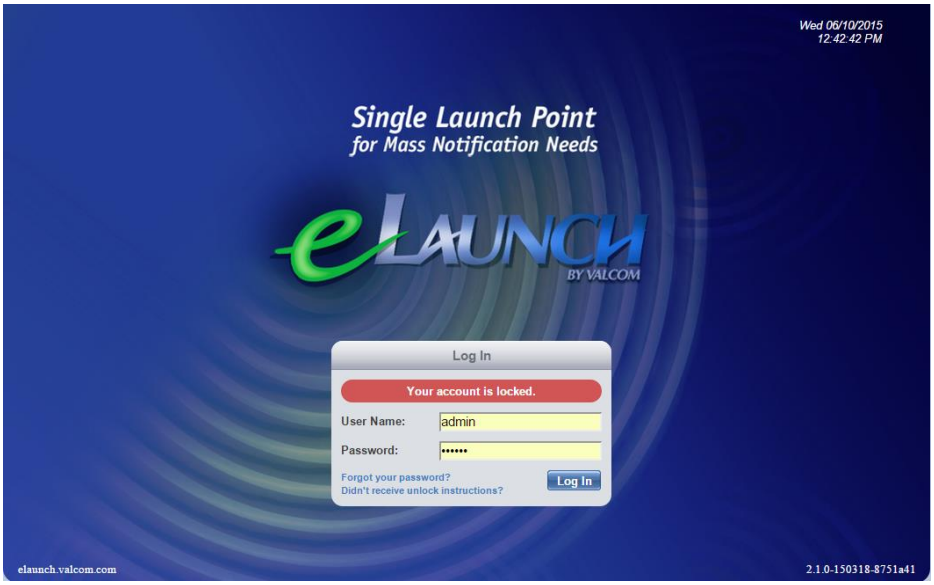
In all cases, initial server setup, device name, host name, domain name and IP address, is accomplished via the VIP-102B IP Solution Setup Tool. Once completed, subsequent setup is accomplished via browsing to those IP addresses.

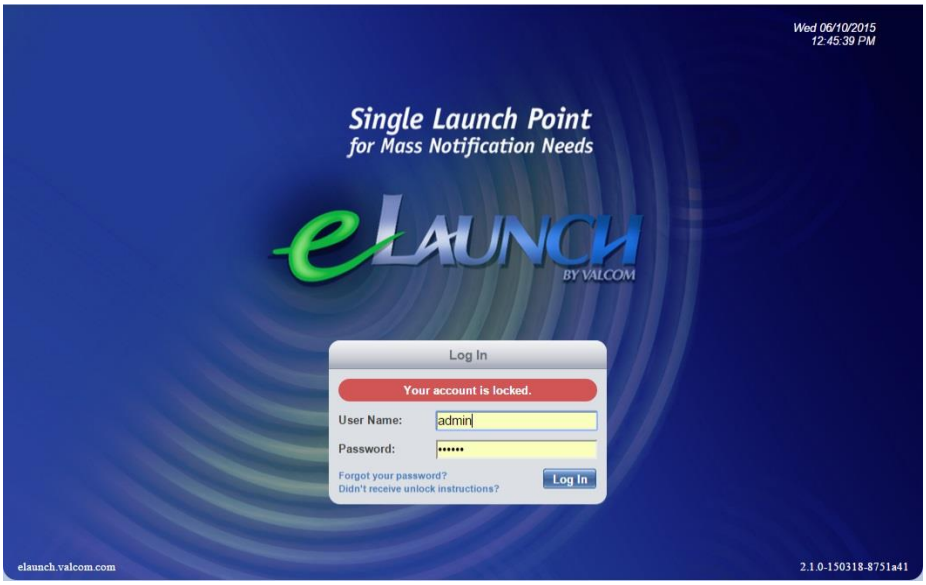
VE6024 eLaunch Server

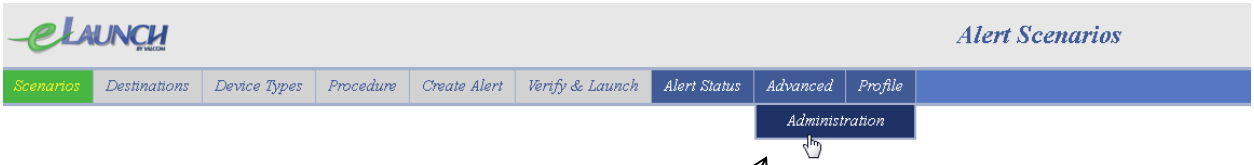
The VE6024 does not ship with a default username and password. A username and password are defined at initial setup.

eLaunch passwords must be a minimum of 6 characters. After 20 unsuccessful attempts to sign into a user's account, it will be locked. To unlock the account, the user must follow the instructions that were sent to the email address associated with their account. Unlock instructions will only be sent to the email address associated with the locked account.

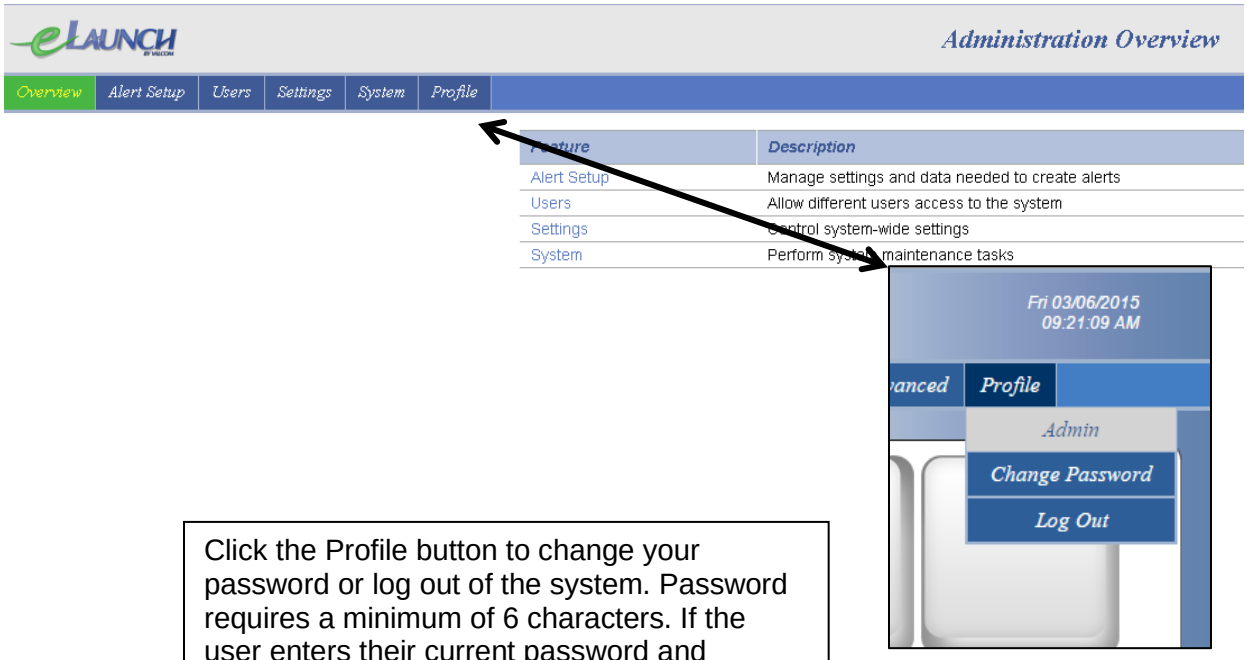
Attempting to resend the unlock instructions to another account will result in a warning message that the email was not found.





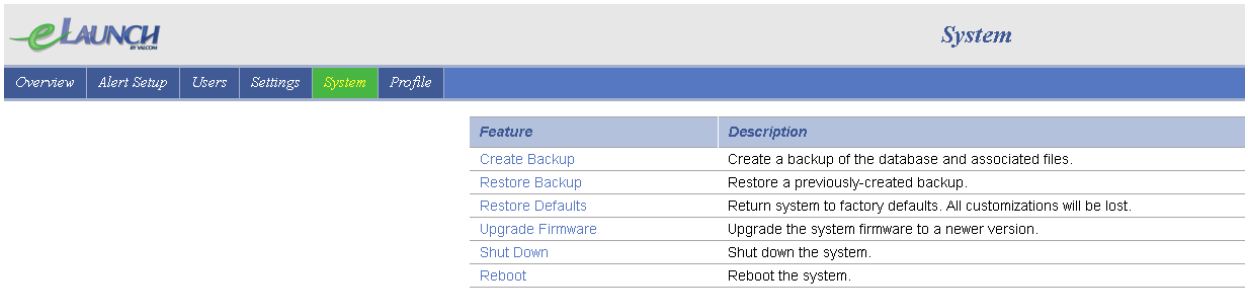


Once logged in, click on Advanced then click on Administration



Click the Profile button to change your password or log out of the system. Password requires a minimum of 6 characters. If the user enters their current password and submits without entering a new password, then no change will be recorded.

Advanced/Administration/System



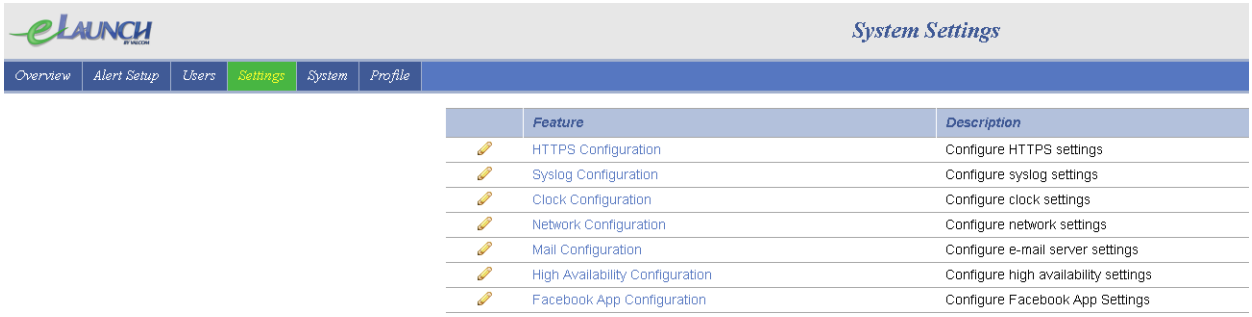
The System page allows users to perform routine server tasks. It is advisable to always maintain a current backup of the VE6024 programming.

The VE6024 must use the same NTP source as the system receiving the alerts (typically a VE6025 Application Server Pro). Variations in time and/or date can cause newly posted alerts to appear as expired.

Log File

The VE6024 log file is available in the zipped backup file. Unzip the backup to view the log file.

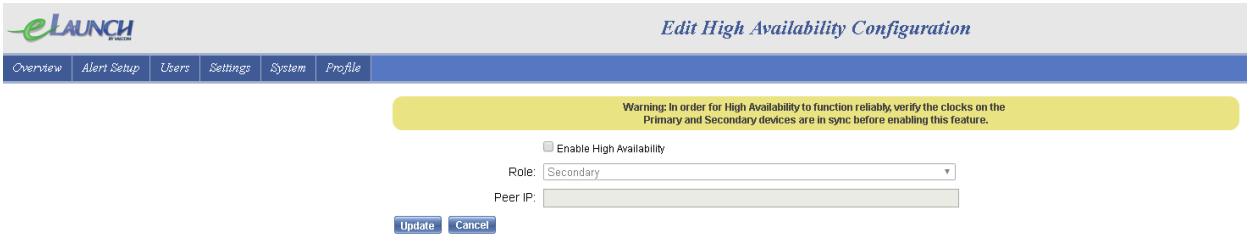
Advanced/Administration/Settings



The Settings menu allows setup of HTTPS secure server communications, defining a destination for server syslog messages, setting up the system clock (correction to an NTP server is strongly suggested), reviewing or altering the server network credentials, defining the mail client credentials used when eLaunch send e-mail alerts, setting up a High Availability server pair (for redundancy) and configuring the settings for posting to Facebook.

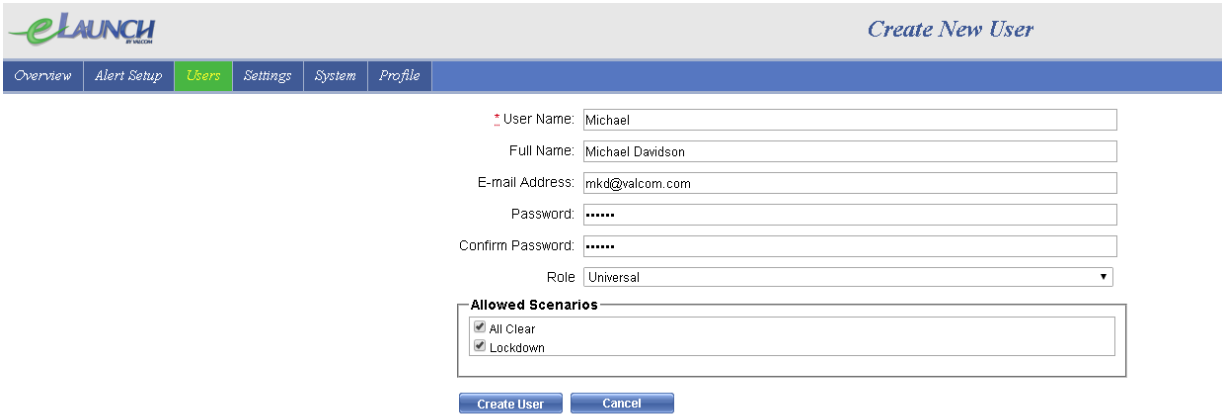
Setting up a High Availability Pair

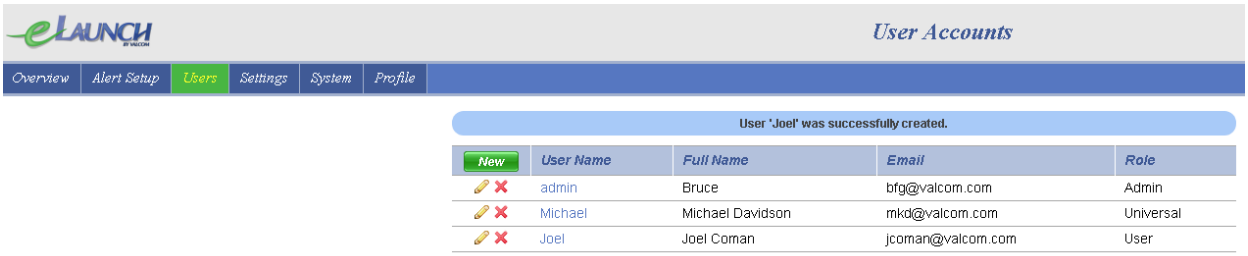
See High Availability Setup instruction in the Application Server setup section of this manual

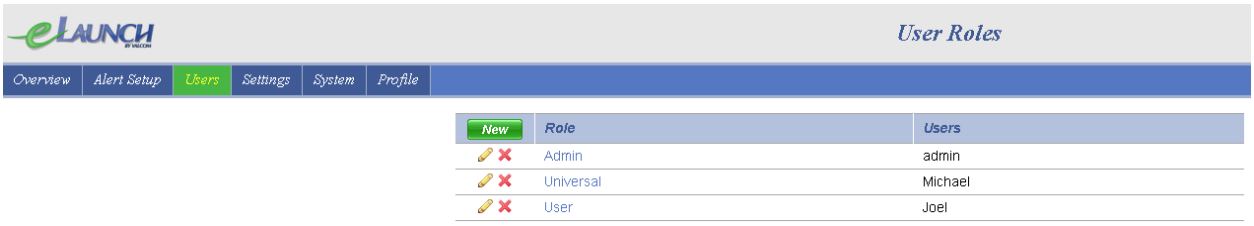


Advanced/Administration/Users

Multiple user accounts may be defined with unique passwords. Users are assigned roles which dictate their rights within the system.







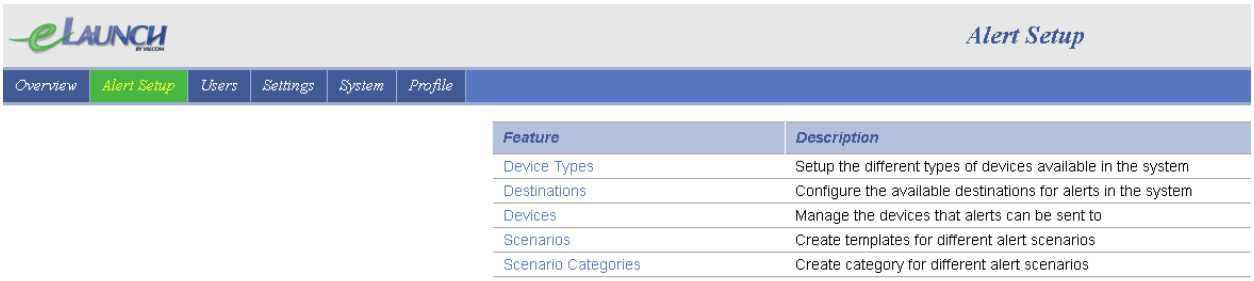
Roles Menu

User Access only allows launching Scenarios

Admin Access only allows access to Administrative functions

Universal Access allows both

Advanced/Administration/Alert Setup



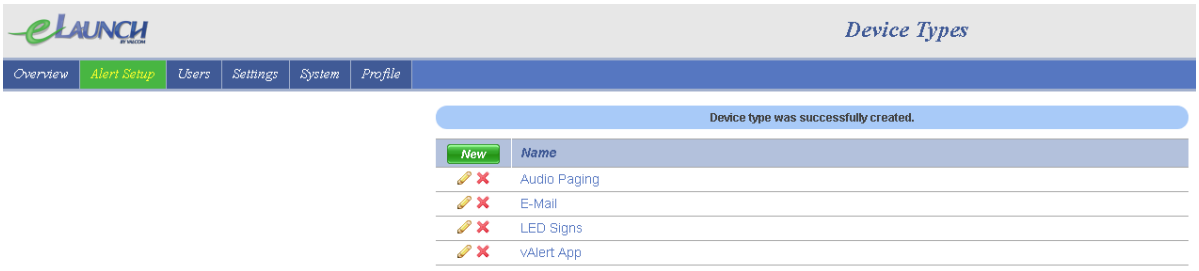
The VE6024 posts emergency messages.

These messages are either sent directly from the VE6024 as e-mails or may be broadcast, displayed or posted to other systems by use of **"Devices"**

Devices may be associated with one type of message delivery (e-mail, Facebook™), or may be associated with multiple modes of message delivery (VE6025 Application Server).

To simplify this for system users, labels known as "Device Types" are attached to the devices so that users do not have to have knowledge of which device is associated with each message delivery mode. In other words, it is easier for users to simply select a destination and how the alert should be delivered than to choose which systems will provide the delivery.

Note that Device Types are simply labels and may be easily created or removed.



Device Type CAP Parameter Mapping

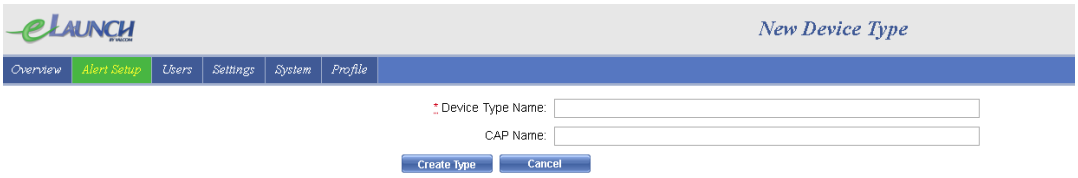
Occasionally, CAP recipient devices search the parameter section of the CAP message for specific names. If these names are not found, the device will not properly process the CAP message.

For this reason, the VE6024 provides an option to map a non-user-friendly CAP Name to a user-friendly Device Type Name. The users may specify these names when creating a new Device Type.

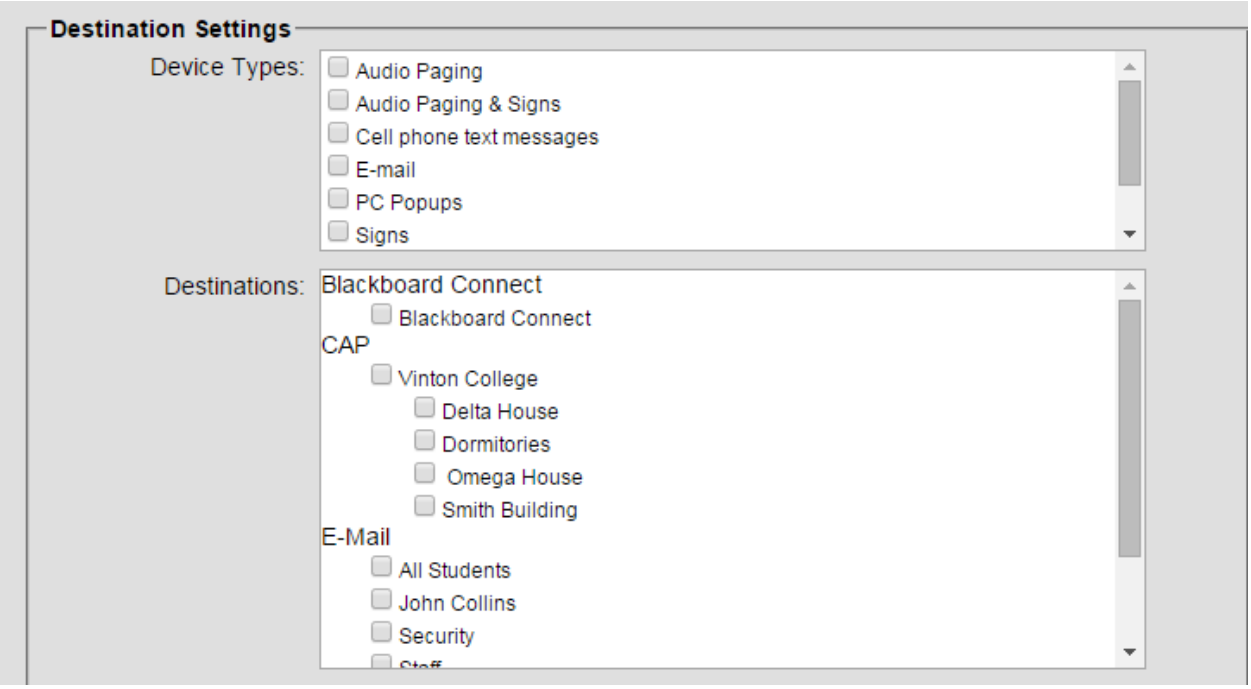
If populated, the CAP Name will replace the Device Type Name in the actual CAP message.

Example:

A third-party CAP recipient device's protocol requires specific CAP parameters names to function properly. When determining message delivery methods, this device searches the CAP parameters for "SMS". If there is no parameter in the CAP message matching "SMS" then the messages are not delivered. "SMS" may not be meaningful to users. Device Type parameter Mapping makes it provide a Device Type Name will be meaningful to VE6024 users, like "Text Message Delivery" and simultaneously provide a technical CAP field name like "SMS".



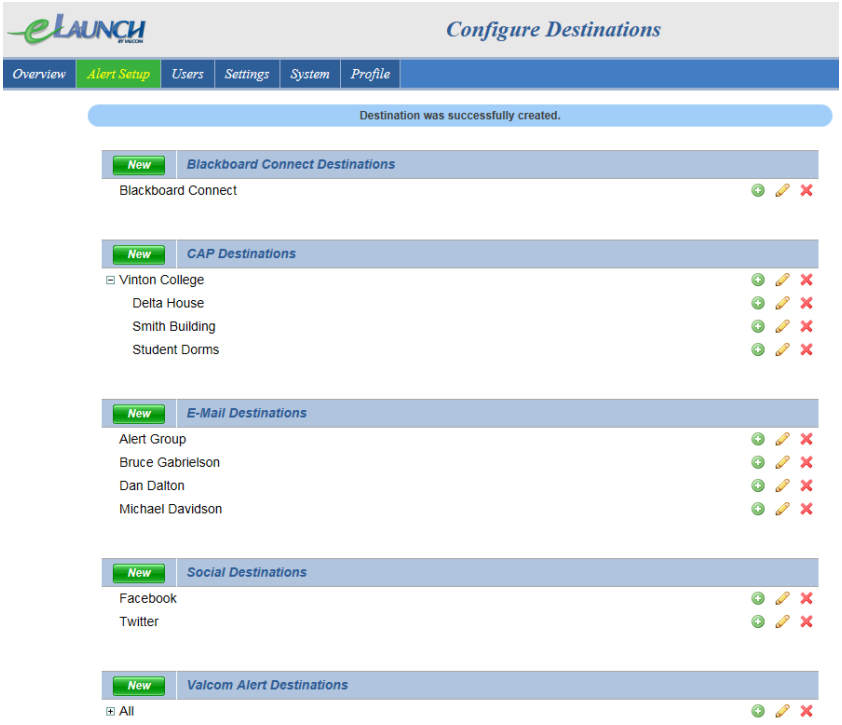
During the message creation process, users will only see the destinations and device types. Device type labels may be added and removed as required.



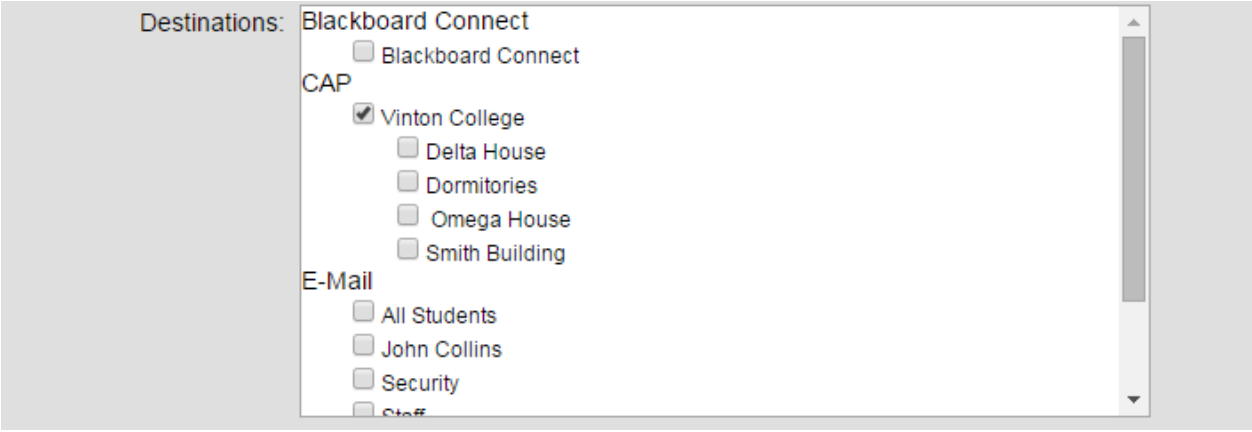
This can lead to some confusion. For example, one of the default device types in the VE6024 is e-mail. However, you would only use that device type if the VE6024 was relying upon an ancillary system (device) to send e-mails. If the VE6024 is the only device sending e-mails, those e-mails recipients will be shown as message Destinations. If this is the case, it is suggested that the “e-mail” device type be deleted to avoid any confusion.

Additionally, if your system has an ancillary device that is multifunctional, for example a VE6025 that delivers messages to LED signs, Audio Paging and Screen pop ups, then deleting those individual device types and creating a new device type called “LED signs, Audio Paging and Screen pop ups” would simplify message creation.

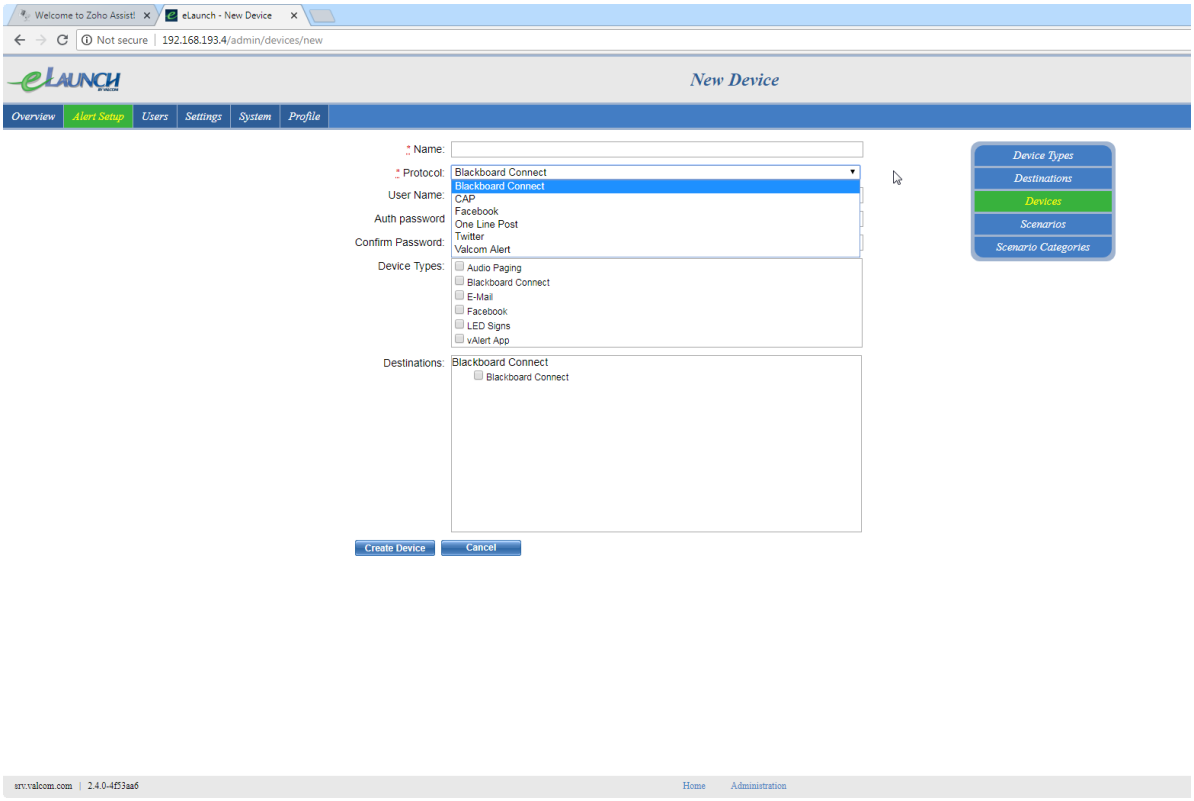
Destinations are simply labels to define areas or groups of message recipients. Without these destination labels, users would not be able to choose delivery locations for their emergency messages.



Ultimately, when the actual emergency messages are defined, there will be a selection of all the destinations which have been defined during initial setup. For privacy purposes, e-mail destinations may be sent using TO, CC or BCC.



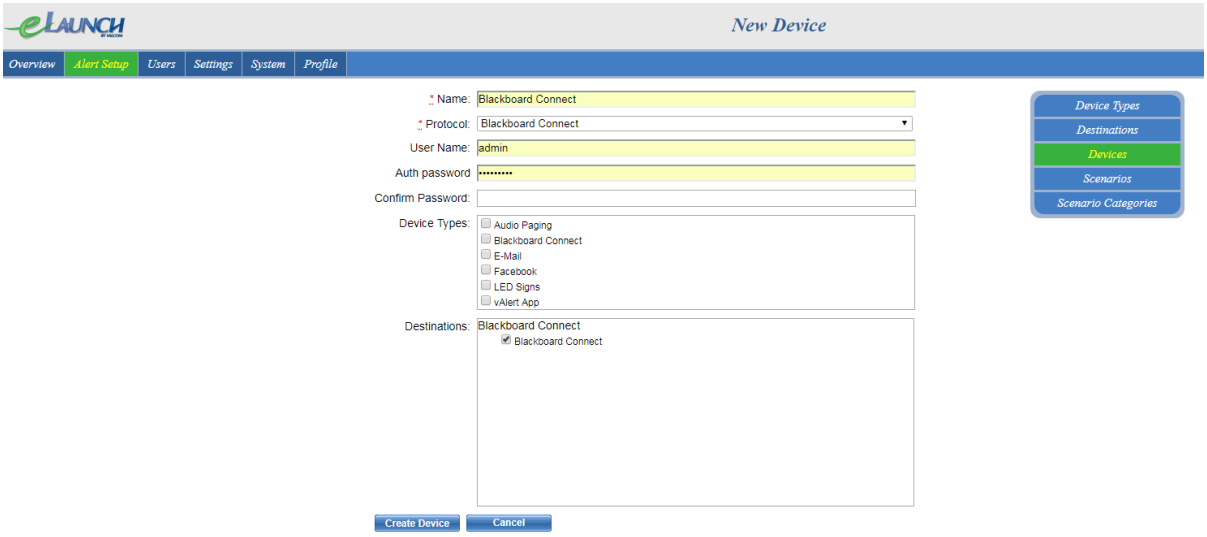
For destinations to receive emergency messages from the VE6024, ancillary devices or systems must be defined.



Device protocols are available to support:

a) Blackboard Connect,
b) Common Alert Protocol Receivers
c) Facebook™
d) One-line posts (for websites)
e) Twitter™
f) Valcom Locate

Blackboard Connect Destinations require a Blackboard connect system be in place. In order to post messages, the VE6024 will log into the Blackboard Connect system.



CAP Destination Devices can either poll the VE6024 for new messages or receive alerts pushed from the VE6024. Devices that are intended to receive "push" alerts from the VE6024 must be defined with their device specific post URL (refer to sample screen shot)

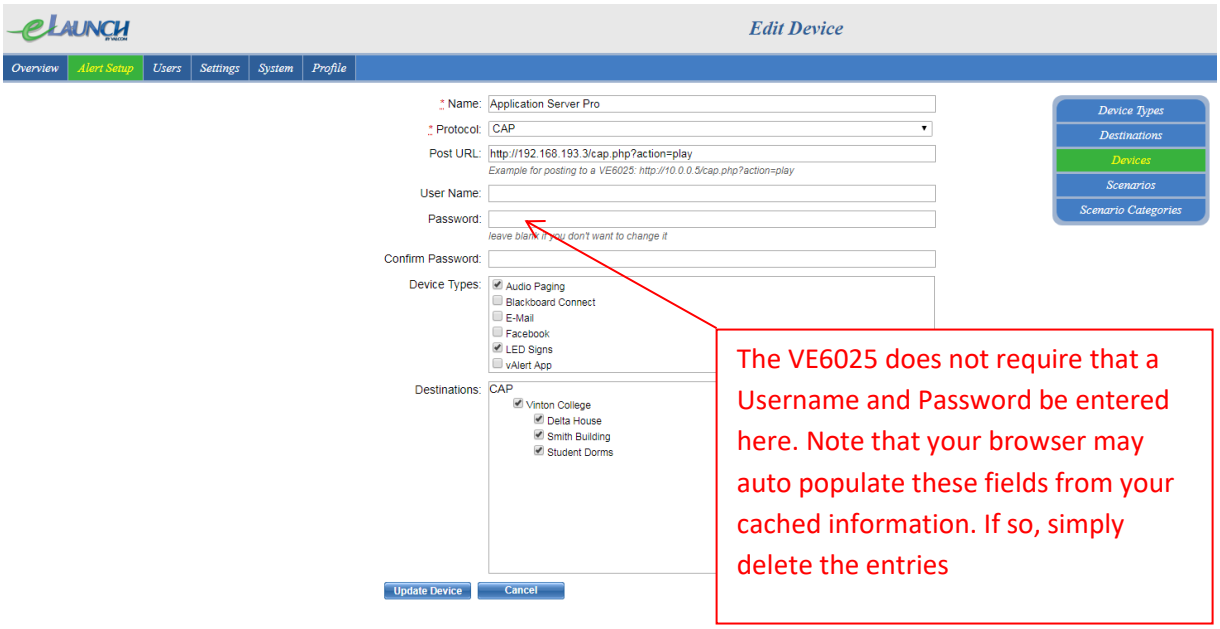
Notice that the screen shot for the sample CAP receiver, the VE6025, may be associated with any of the physical site destinations we previous defined. As you will see, the VE6025s will be able to deliver messages to any or all of these areas based upon the content of the received CAP message.

In other words, if the emergency message is only intended for Delta House, then the VE6025 will be able to deliver the content to Delta House exclusively.

If the emergency message is only intended for Delta House and Smith Building, then the VE6025 will be able to deliver the content to both the Delta House and Smith Building.

The VE6025 can filter the CAP message and route the message based upon the destination.

Therefore, the destination labels play a crucial role in the available granularity of content delivery.



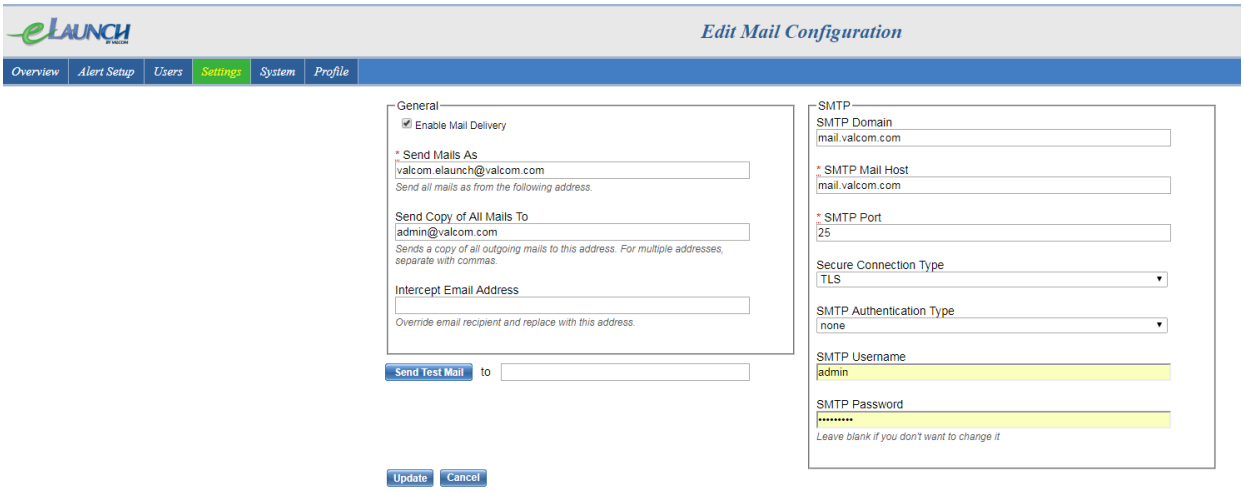
Some systems may not be able to receive push alerts and may rely upon information polled from CAP sources. The VE6024 automatically hosts an Alert List as well as CAP, RSS and ATOM feeds for each alert generated.

To poll the VE6024, the polling system should be directed to one of the following URLs:

http://<IP address of VE6024>/cap/alerts/feed.rss
http://<IP address of VE6024>/cap/alerts/feed.atom
http://<IP address of VE6024>/cap/alerts/feed.cap ***--or--***
http://<IP address of VE6024>/cap/alerts/latest ***(this link provides straight CAP XML)***

E-mail Destinations are simply e-mail addresses. However, for the VE6024 to send e-mails, it must be set up with the appropriate configuration.

Setup of the mail configuration is handled under the Settings tab in Mail Configuration page for an Admin User.



The default mail screen will look like the image above. To enable sending mail, select the checkbox for 'Enable Mail Delivery' under the General Section. The e-mail address that is used to send the mail to the user can be user configured. An address can also be defined that will receive all e-mails sent from the eLaunch.

To enable mail delivery, the SMTP section must be configured correctly. SMTP is short for Simple Mail Transfer Protocol and is a protocol designed for sending e-mail messages between servers.

Most e-mail systems utilize SMTP to send messages from one server to another server. Messages are then retrieved from the server using either Post Office Protocol (POP) or Instant Mail Access Protocol (IMAP). The SMTP Domain is the Domain of the SMTP server.

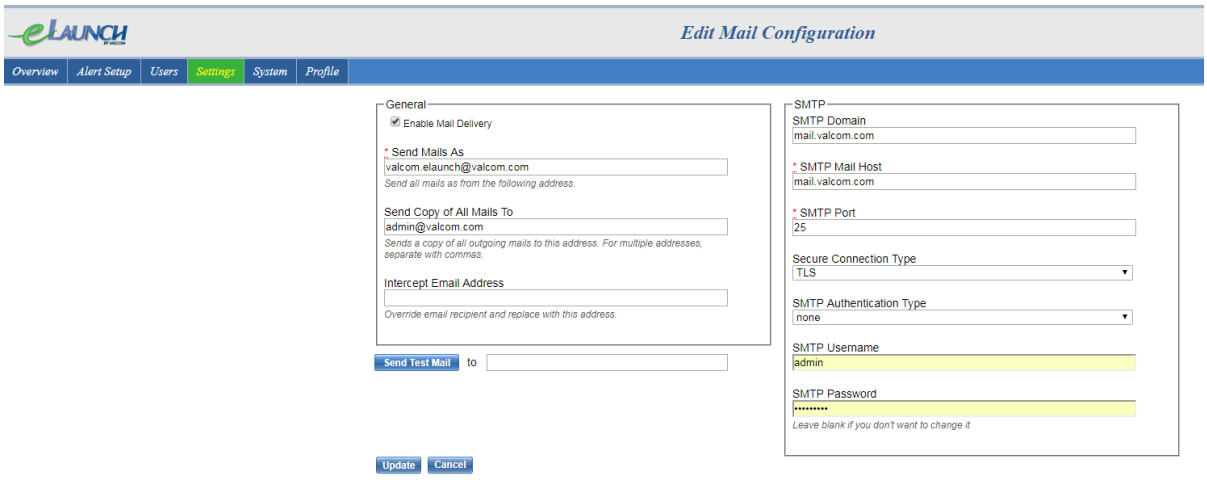
If a company uses the domain of company.com the SMTP Domain will be filled with company.com. The SMTP Mail Host will be the server address. In many cases it is something like mail.company.com. In other cases, like with Yahoo! Mail Plus
the SMTP server address is plus.smtp.mail.yahoo.com.

SMTP ports are usually set to 25 by default. If the SMTP connection is secured by SSL the default port is 465 instead. The Secure Connection Type is the type of connection used by the

Mail Server for security purposes and choices include None, SSL and TLS. SMTP Authentication Type allows for selection between none, plain, login and cram_md5 and an SMTP client may log in using one of those authentication mechanisms. The SMTP Username is the full e-mail address of a user on an SMTP server such as jsmith@company.com. Finally, is the SMTP Password. The SMTP Password will be the password of the e-mail account entered into the SMTP Username field above.

To test that the Mail has been configured properly enter an e-mail address into the line next to the 'Send Test Mail' button. The test e-mail address does not need to be the address entered into the SMTP Username field.

Users may choose which CAP fields are sent to each e-mail destination (Alert Setup/Destinations/E-mail Destinations)



Social Destinations are social media platforms such as Facebook™ and Twitter™.

Before creating a new Social Media Device it is important to add a Destination for any Social Media Devices (Advanced/Administration/Alert Setup). There is a category of Destination known as a *Social Destination*. The *Social Destination* is intended to be used as the destination category for all Social Media platforms going forward. Other than its use for Social Media there is nothing different between the *Social Destination* and any other destination.

The name of the Social Destination can be anything you would like. It does help to name the Social Destination after the Facebook™ Page or Twitter™ Profile that will be posted to using the eLaunch.

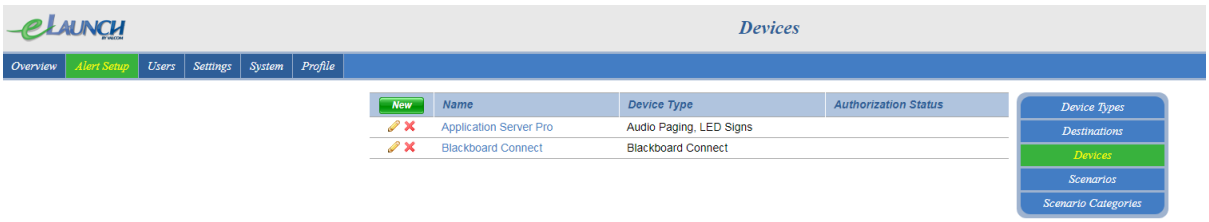
Typically, facilities utilize a single Facebook™ or Twitter™ account, so the social destinations users create would simply be called "Facebook" or "Twitter".

Technically, you could create a single destination called “Social Media” and assign all of the social media accounts to the single Social Media destination. Choosing this destination for an emergency message would cause the message to be delivered to all defined social media accounts.

When the Valcom Locate protocol is selected, fields become available to define your Valcom Locate server.

Devices

There is a column on the Devices index screen labeled as *Authorization Status*. This column will display either "Authorized" or "Unauthorized" for Social Media devices only. The column is useful for telling which Twitter™ and Facebook™ devices are properly authorized.



Twitter™

Instructions are in the web interface

Posting a Tweet

Once a Twitter™ account has been authorized it's time to try sending a Tweet using the eLaunch. Twitter™ restricts their Tweets to 140 characters so the SMS/Twitter™ field is being used to send to the Twitter™ service. When launching an alert either Ad-hoc or from a Scenario you simply need to select the Social Destination for the associated Device, the Device Type of the associated device and make sure that the SMS/Twitter™ field has been filled with a valid alert. Upon launching the alert, the user should see the Tweet appear on their feed within seconds, provided that the alert was sent properly.

Twitter™ API caveats

So far there is one issue to watch out for when using the eLaunch to post a Tweet to Twitter™. Built into Twitter's API is a program that will compare the content of your Tweet against the content of your previous Tweets. If you try to send the exact same message twice within a certain time period Twitter™ will reject the post entirely. Twitter™ does not release any information on what the time frame is for being able to post two messages of the same content, but it is most likely a few hours and may also change based on prior post history. To work around this issue, the best idea would be to put something like the time of the alert in the SMS field on the end of the message. Users will just have to be cautious that the addition of the time does not push their alert

to over 140 characters because Twitter™ will then reject the message since they do not provide any way to parse and post messages longer than 140.

Facebook™

Setting up the eLaunch to use Facebook™

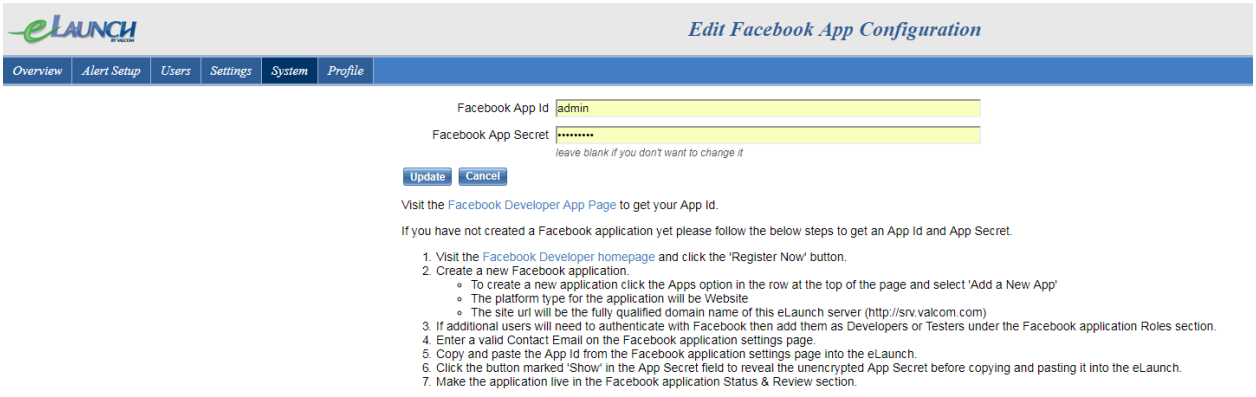
To allow a user to authorize and post to Facebook™ from the eLaunch it is necessary for an eLaunch administrator with a Facebook™ account sign up to be a Facebook™ developer. Users can sign up as a developer at https://developers.facebook.com. Once they have signed up as a Facebook™ developer the user should create a new Facebook™ App.

Creating an Application

When logged into Facebook™ as a developer there is a bar at the top of the screen. The items on the bar are Apps, Products, Docs, Tools and Support. To create a new application, click on the Apps column and select the option to 'Add a New App'. Select the option of Website as the platform for the new application and then select a name for the application. If asked by Facebook™ whether this app is a test version of another app select 'No'. As a category choose communication and then press the 'Create App ID' button. After creating the application, the user will be taken to the Quick Start screen for Websites. In the 'Tell us about your website' section enter the hostname of the eLaunch into the section labeled Site URL. The hostname should be the fully qualified domain name of the server.

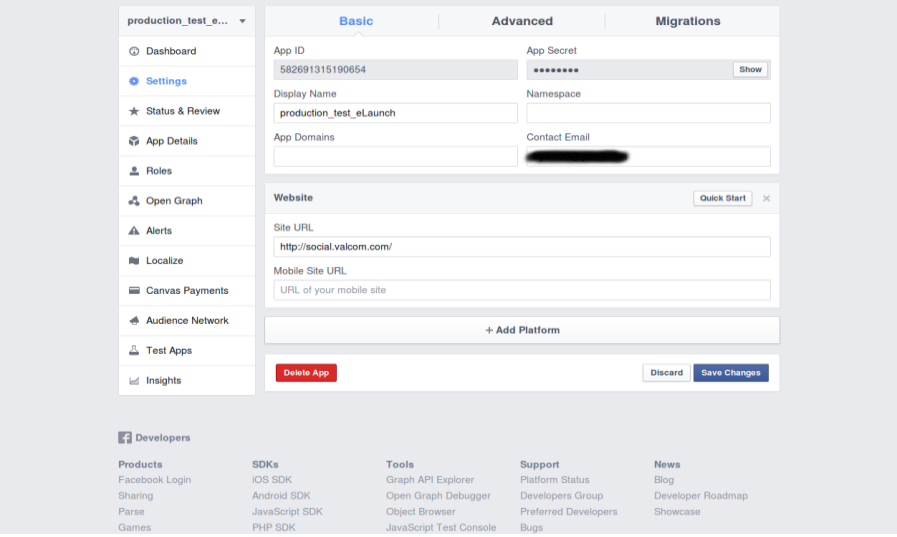
Click the 'skip Quick Start' button at the top of the Quick Start page when the application setup is finished. This will take you to the application dashboard. On the left column select 'Settings' to go to the application settings. In the 'Contact E-mail' field enter a valid contact e-mail and Save the Changes. On the left column select 'Status & Review'. At the top will be a toggle box labeled 'NO'. Toggle this to 'YES' to make your application live so general users can see any information posted by the eLaunch.

To copy the App ID and App Secret to the eLaunch visit the Settings section in the Facebook™ App. To properly copy and paste the App Secret for Facebook™ into the eLaunch you will have to click the 'Show' button in the App Secret field. You may be required to enter your Facebook™ password as a form of security. After that the user will be able to copy and paste the App Id and



App Secret from Facebook™ and put them into the eLaunch Facebook™ App Configuration screen found at Advanced/Administration/Settings/Facebook App Configuration.

Next go into the Advanced Tab, enable Web OAuth Login and enter a Valid OAuth redirect URI (http://oauth.net/) for the eLaunch to become fully authorized.



Facebook™ App Settings Page

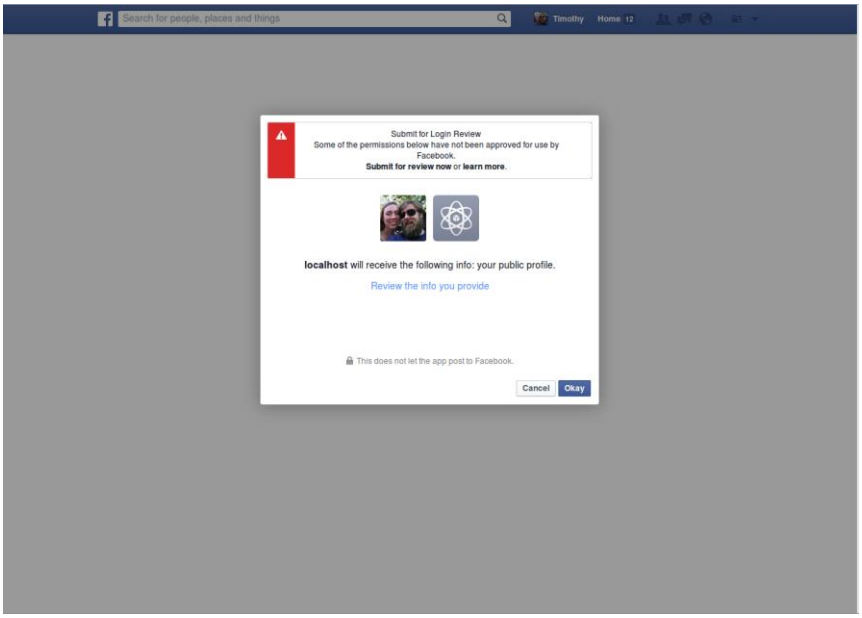
Before Authorizing with Facebook™ make sure that no one is logged in on that browser

Select the "Facebook™" option from the Protocol drop down menu. Upon selecting Facebook™ as the protocol the option to enter a User Name, Auth Password and Confirmation Password will be hidden since none of this is necessary for Authorizing with Facebook™. If any Social Destinations exist they will be displayed in the Destinations box.

There is a difference between posting to a Facebook™ User Profile and a Facebook™ Page. In order to post to a Facebook™ Page you must name your Device the same as your Facebook™ Page. If the Device name does not match the name of the Facebook™ Page you would like to post to then the Device will post directly to your User Profile.

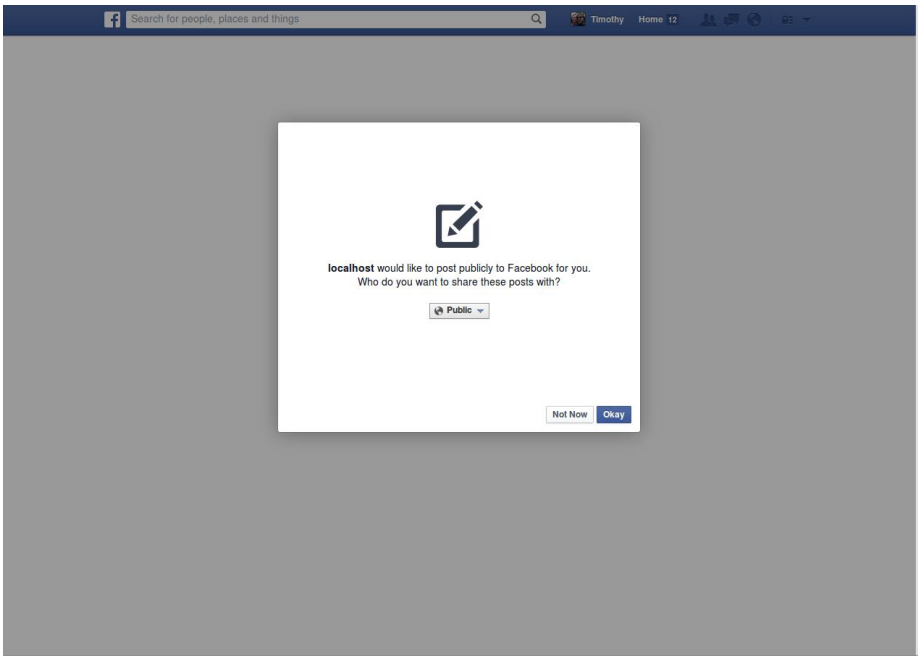
Upon clicking on the "Sign In" button the user will be automatically redirected to the Facebook™ website. If there is no Facebook™ user logged into that browser the login dialog will be displayed.

Once logged in on the proper account the user will be asked to accept the permissions to allow the eLaunch to post to their account. Since the eLaunch will be asking for permissions to post without having undergone a review process it will warn you that a review is required as shown in the image below. A review is not required since the application will not be in use by the general population so this warning may be ignored.



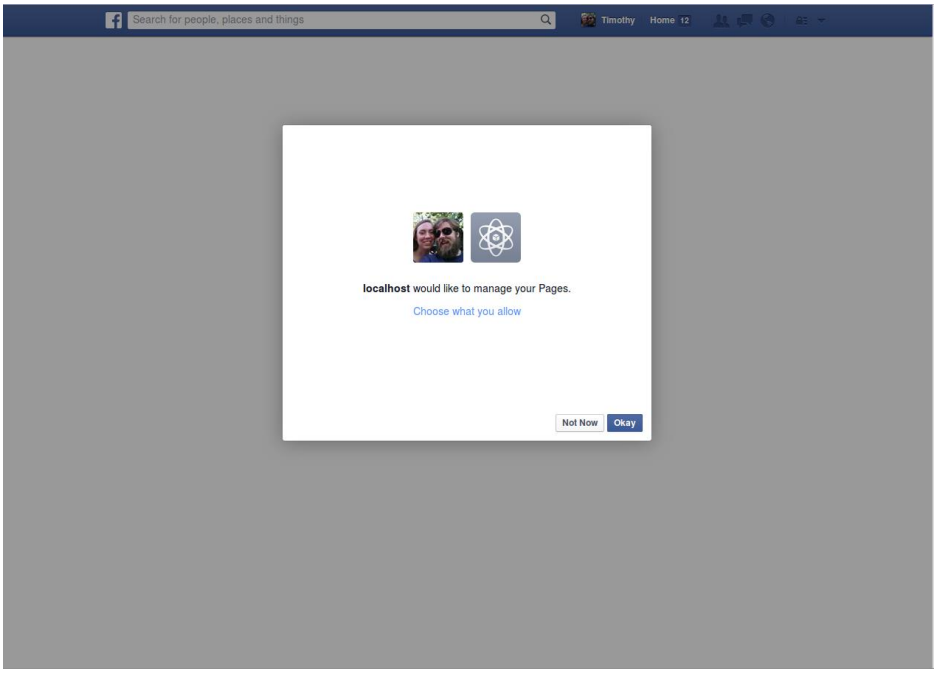
Review Process Requested

After selecting okay, the user will be forwarded to accept the permission required for the eLaunch app to be able to successfully post to a Facebook™ Page or Profile. Before accepting the permission, be sure to set who can view the posts made by the eLaunch. If posting to a public page the best option would be Public so anyone visiting the page will be able to see the post.



Permission to Post to Page

The next permission to accept is the permission for the eLaunch app to manage pages. This permission gives access to the eLaunch to post to pages managed by the user.



Permission to Manage Pages

If the user grants the permissions, they will be redirected back to the Devices screen. There will be a message alerting the user that the Facebook™ device has authorize successfully and the *Authorization Status* will be updated to show that Facebook™ has "Authorize".

Posting to Facebook™

Once a Facebook™ account has been authorized its time to try creating a new post on your Facebook™ feed. Facebook™ does not have the same post restrictions that are present in Twitter™ so messages posted to Facebook™ make full use of the headline, description and instructions field. If all three fields have information present, then all three fields will be combined and sent. Upon launching either an Ad-hoc alert or a pre-defined Scenario the user should see a message appear on their timeline within seconds.

Facebook™ API Caveat

If the server tries to send a message with the same exact content as the previous message within a minute or so, Facebook™ will reject the post of the message. Communicating with Facebook™ will also require the use of a Fully Qualified Domain Name or FQDN as the Site URL of the Facebook™ Application. A FQDN requires a device to have a local hostname and parent domain name such as *hostname.example.com* and be resolved by a DNS server. The IP address of the eLaunch cannot be safely used since it is often a private IP address behind a user's firewall and Facebook™ does not view private IP addresses as a valid Site URL.

Setting Up Emergency Messages

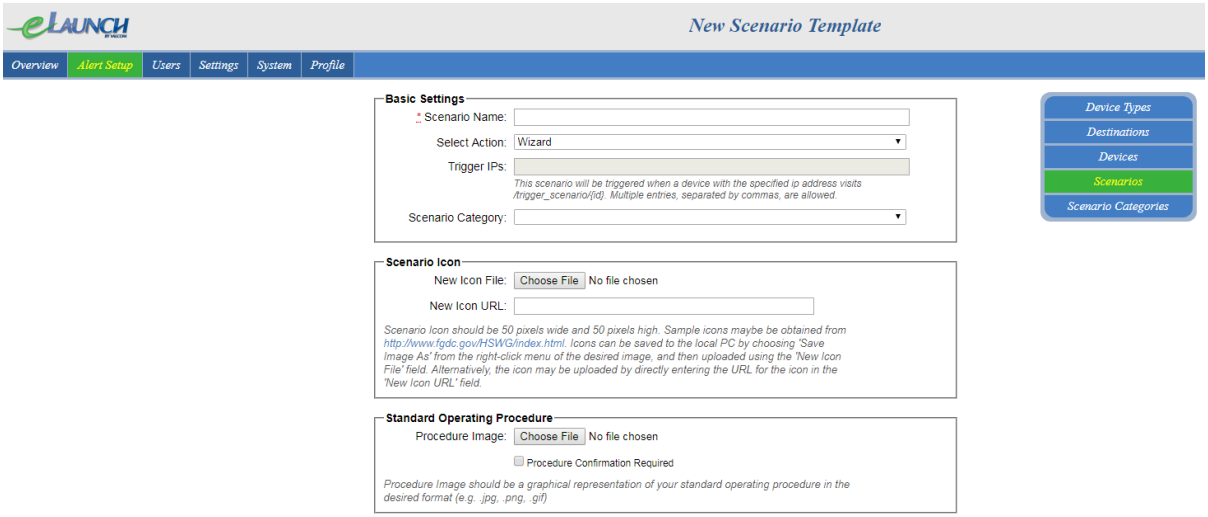
Before setting up emergency messages, or **Scenarios**, associating devices with destinations and labeled with device types should be completed. There is no practical limit to the number of scenarios that can be defined in a VE6024.

Scenarios must be given a name indicative of the alert (Fire, Take Shelter, etc.)

Select the action desired when the Scenario is launched. “Auto” launches the Scenario as is, “Wizard” allows prelaunch changes and “Choice” lets you choose between Auto and Wizard on a per launch basis.

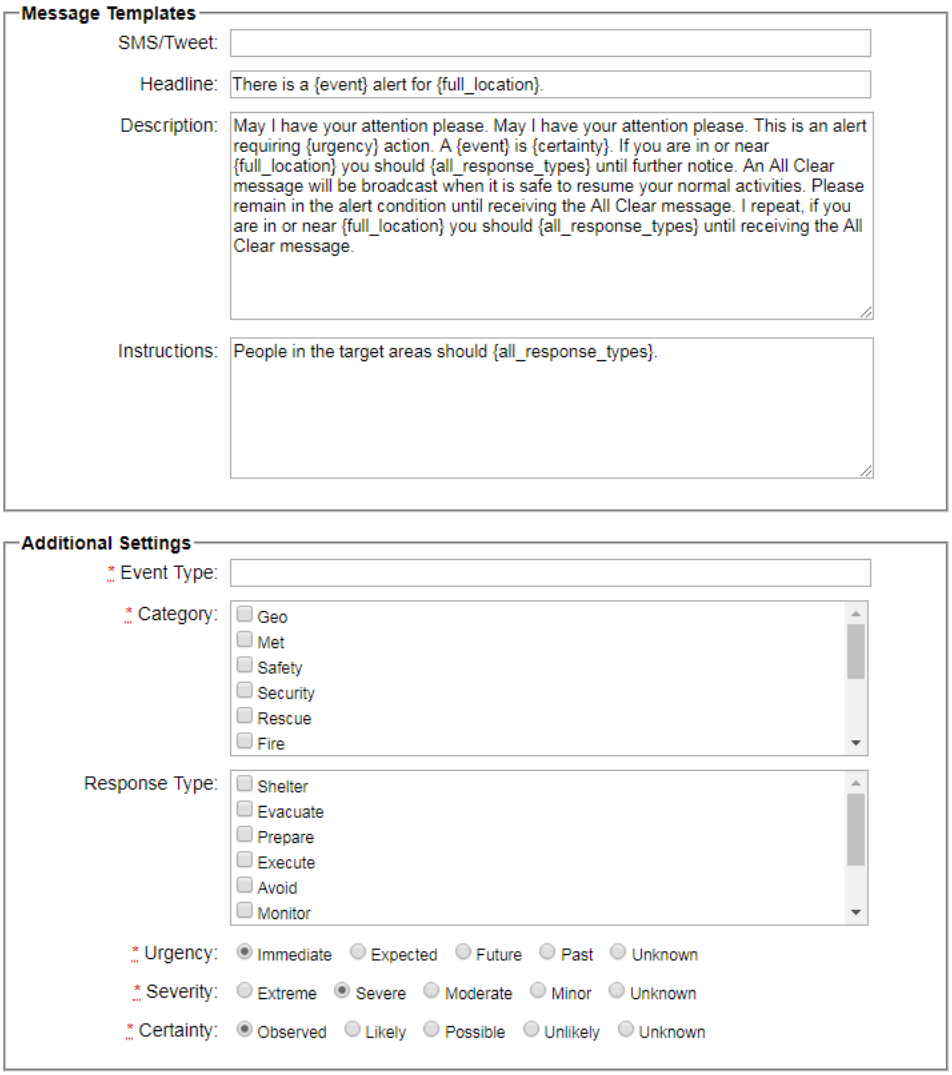
An ICON may be added for visual identification of the alert type.

An optional standard operating procedure image and confirmation may be added to describe steps that should be taken before message launch.



The Message Template may be used as is, with variables in place, or may be customized as desired. A 160-character SMS/Tweet of the message may be entered along with the Headline, Description and Instructions CAP fields.

Enter the Event Type (Fire, Take Shelter, etc.) and choose one or more Categories, Response Types, and Urgency, Severity and Certainty. These are all standard CAP fields and will be substituted for the variables in the Message Template.



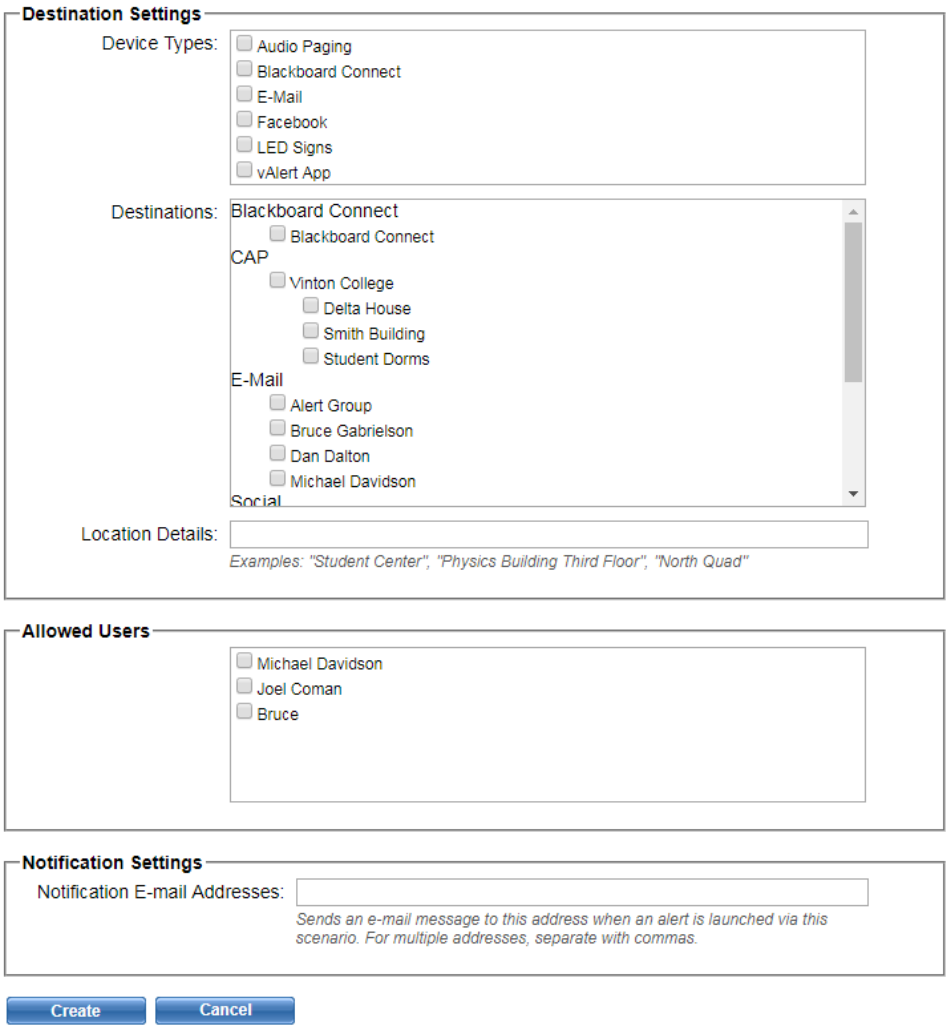
Including regex assigned variables in scenarios

When you trigger an eLaunch event from an Application Server text monitor, any variables assigned a value from Regex as a function of that text monitor, are automatically sent to the VE6024 and may be incorporated into the triggered scenario's headline, description or instructions.

Choose which Device Types should deliver the message, and where the message should be delivered (Destinations). **One Line Post devices use CAP destinations**.

You may also include location details, although this is typically only used with Auto launching.

Lastly, choose which users have permission to launch this Scenario and any message specific e-mail recipients.



You can have multiple comma separated email addresses in the Notification Settings section under the scenario. Notification email is just an email alerting a user to the fact that the scenario has been launched and doesn't contain the alert information.

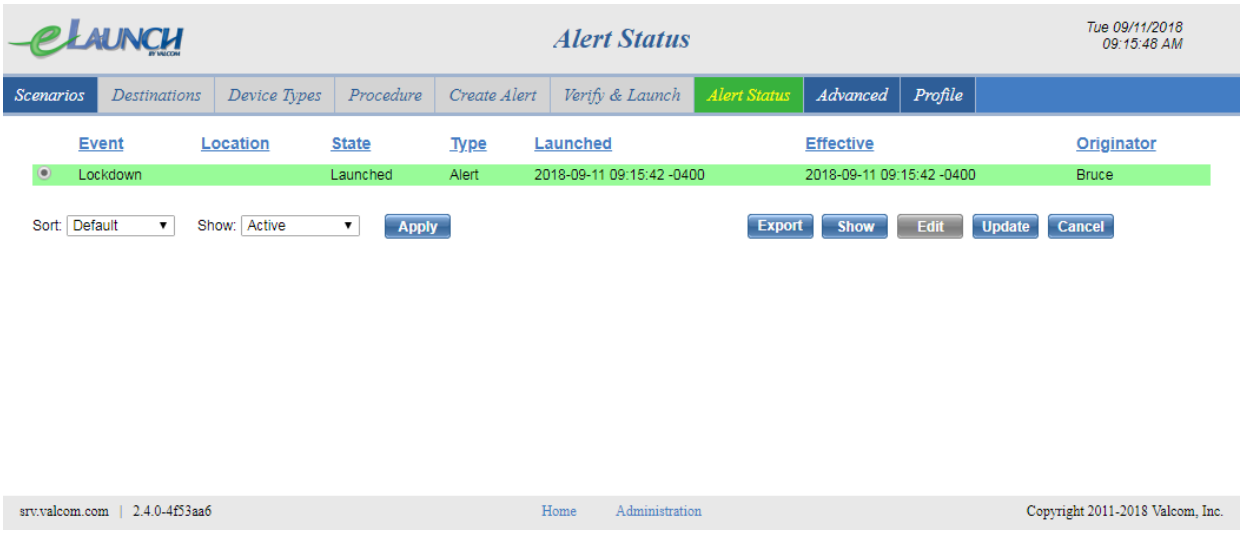
The default VE6024 Scenario headline, description and instructions contain variables that are populated based on other Scenario fields:

{full_location} = Location Details
{event} = Event Type
{urgency} = Urgency
{certainty} = Certainty
{all_response_types} = All Response Types Checked
{start_time} = Onset (only variable through Wizard)
{end_time} = Expires (only variable through Wizard – default is 5 hours after Onset/start time)

Click on the eLaunch Logo to go to the launch screen. You are ready to launch Scenarios.

The Ad-hoc button allows users to create custom Alerts "on-the-fly"

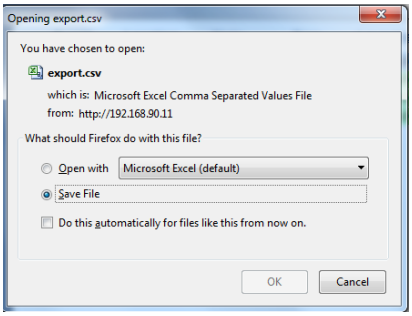
Once a Scenario is successfully launched, the Alert Status screen is displayed. From this screen users may view, cancel or update and re-launch alerts.



Alert status will show previous launched scenarios and scenario drafts (in progress, but not yet launched).

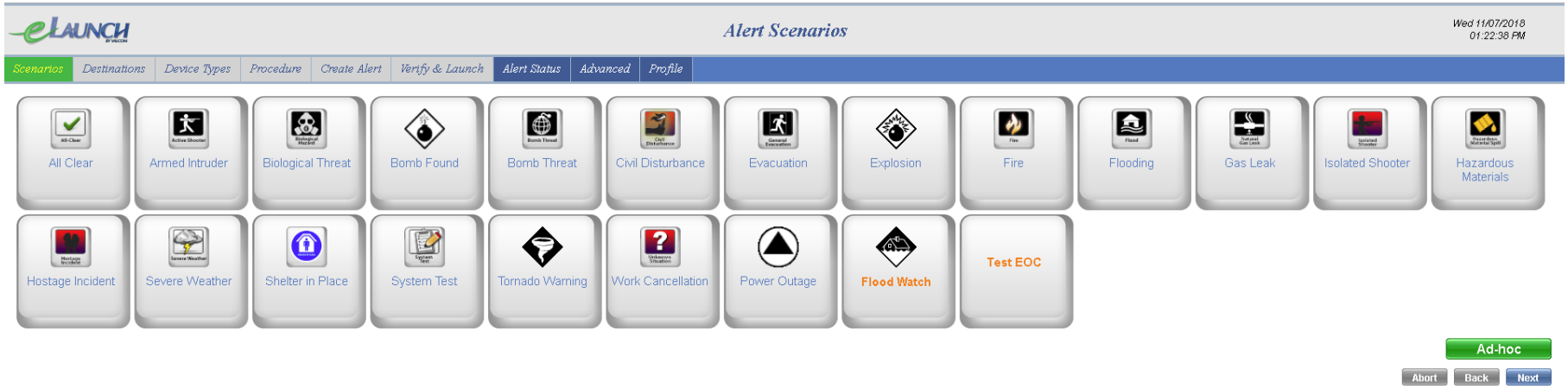
Users can select any scenario and either edit drafts or view and update previously launched scenarios. Updating allows users to edit and relaunch scenarios with updated information.

The export button allows users to export a CSV file containing alert status history.



Click on the eLaunch logo to return to the Alert Scenarios screen.

Sample eLaunch Screen



We'd like to hear from you!

Valcom, Incorporated

5614 Hollins Rd

Roanoke, VA 24019 U.S.A.

1-540-563-2000

Regular Business Hours are Monday – Friday

8:30 a.m. to 7:30 p.m. EST

Engineered, Built and Supported In The U.S.A!