



This Document Is Intended To Be Viewed In PDF Format

IP6000 VE6021/VE6025 Application Server Overview

rev. 2022-1.00

This document describes the functionality and set up of an VE6021 Application Server or VE6025 Application Server Pro. These products are used in many applications including advanced VoIP communication and Emergency Mass Notification systems. In this capacity, the VE6025 is used and is almost always paired with a [VE6024](#) eLaunch Server.

This document was written around the following firmware revisions:

Version 4.10 (with certain post release additions)

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](#).

If using a VE6021, disregard all sections pertaining to Common Alert Protocol and Text-to-Speech and eLaunch.

Please submit corrections or suggestions to bfg@valcom.com

Table of Contents

- VE6021/VE6025 APPLICATION SERVER 4**
- MENU TREE5
 - System Folder*.....6
- SSL CERTIFICATE INSTALLATION (OPTIONAL).....7
 - Sample files*.....8
 - Self-Signed Certificates*9
- USERS.....10
- SETUP OPTIONS12
 - Setup/Network*.....12
 - Setup/VIP Tab*13
 - Setup/SNMP Tab*.....14
 - Setup/Syslog Tab*.....15
 - Setup/Crisis Alert Tab*.....16
 - Setup/Paging Tab*.....19
 - Setup/Prayer Time Tab*20
 - Setup/High Availability Tab*21
- SETTING UP A HIGH AVAILABILITY PAIR.....22
 - Setup/Miscellaneous Tab*.....25
- ADMINISTRATION/SYSTEM/CLOCK26
- ADMINISTRATION/SYSTEM/LICENSE28
- EDITORS29
 - Editors/Audio Editor*.....29
 - Editors/Text Message Editor*.....35
 - Editors/Event Editor*36
 - Editors/Schedule Editor*.....55
- PLAY LIST.....58
 - Play List/Create Play List*.....58
 - Editors/CAP Editors*.....60
 - Editors/CAP Sources Editor*61
 - Editors/CAP Filters Editor*.....63
 - Editors/CAP Alerts Viewer*.....67
- ADMINISTRATION/CALENDAR68
- EDITORS/INPUT EDITOR70
- EDITORS/GROUP CODE EDITOR73
- EDITORS/CREATE NEW GRAPHIC.....74
- EDITORS/ICON EDITOR.....84
- EDITORS/TEXT MONITORS85
- PREFERENCES/PASSWORD91
- VALCOM DESKTOP ALERT INSTALL (OPTIONAL) 92**

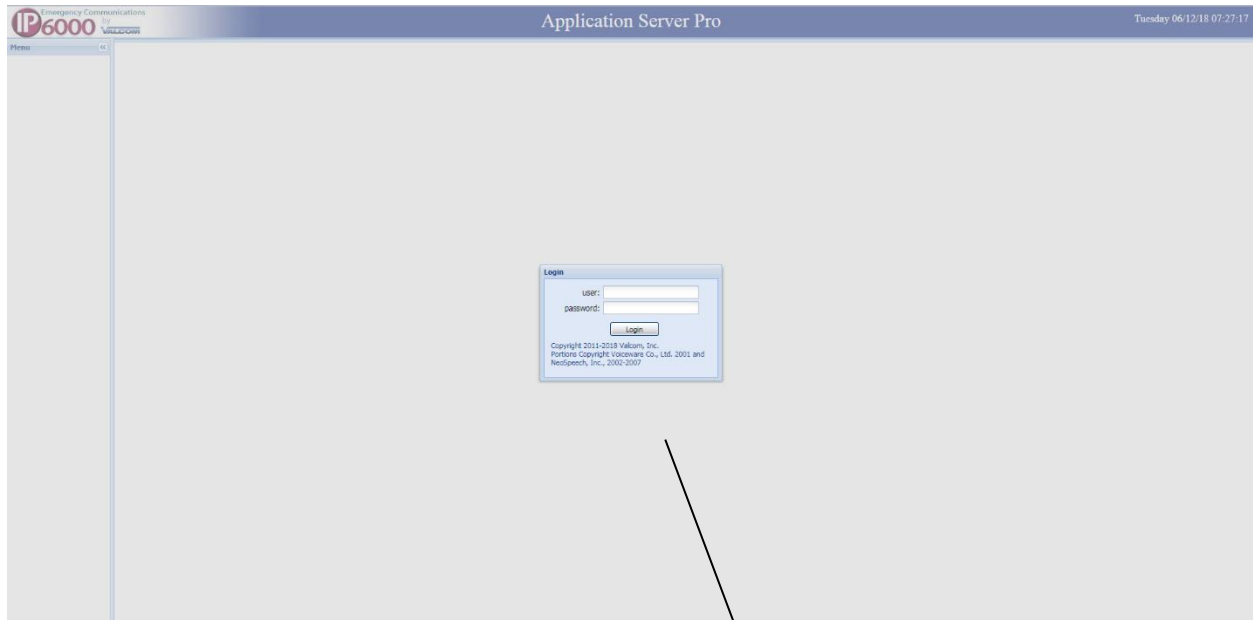
BASIC APPLICATION SERVER TROUBLESHOOTING.....	102
BROWSER COMPATIBILITY.....	102
USING THE VIP STATUS MONITOR	107
VOLUME OFFSET INTEROPERABILITY BETWEEN VALCOM DEVICES	108
POWER/MAINTENANCE.....	110
MODIFYING TEXT-TO-SPEECH	111
MANUALLY CONTROLLING APPLICATION SERVER AUDIO BROADCASTS	112
SCHEDULING AUDIO	123

VE6021/VE6025 Application Server

Initial server setup is accomplished via the VIP-102B IP Solution Setup Tool.

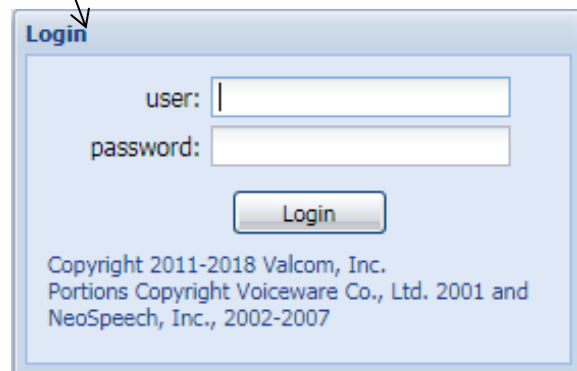
The VIP-102B will be used to assign IP addresses and channel dial codes to all the Valcom endpoints. It is also used to designate group dial codes and group membership. **The Application Server utilizes these groups to send audio and text announcements.**

Once the server has been assigned an IP address, subsequent setup is accomplished via browsing to that IP address.

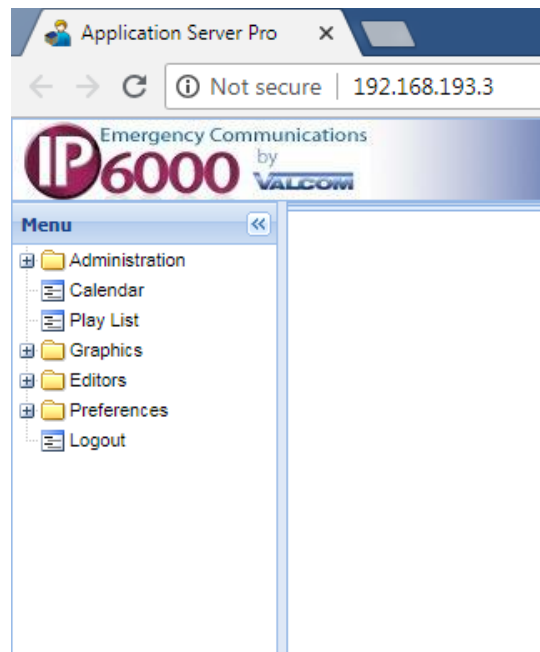


Default Login User Name: admin

Default Login Password: 4cc3ss

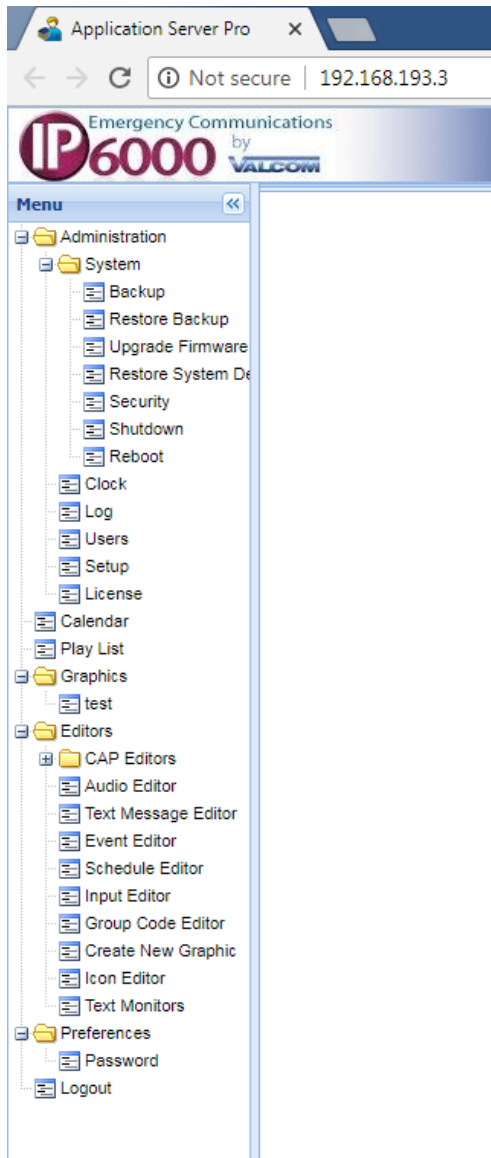


Menu Tree



Once logged in, initial users are presented with the menu tree. Clicking on the plus next to tree folders provides an expanded view of menu items.

System Folder



The System folder offers the ability to:

Backup* all Application Server programming

Restore Application Server programming from a previous backup

Upgrade Firmware

Restore the Application Server to factory defaults

Setup SSL secure communications**

Shut the server down

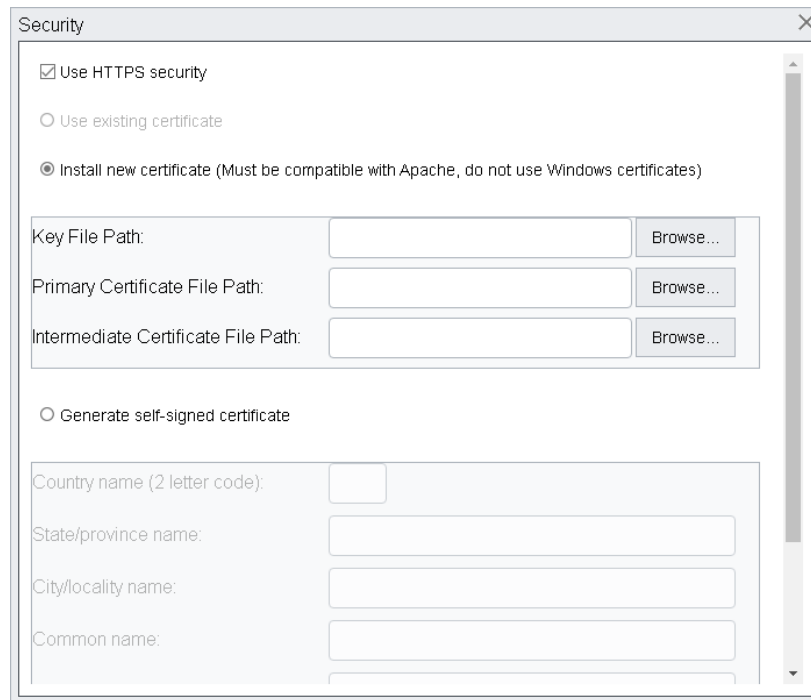
Reboot the server

Log provides a view of system syslog information

*The backups are saved as a “zip” file. Some browsers, Safari for example, have a default option to automatically unzip “safe” files. This should be disabled prior to performing a backup.

**allows for the use of HTTPS security for the web browser portal instead of HTTP. The user will be given the choice of using an existing certificate or installing a new certificate for use by the Server.

SSL certificate installation (Optional)



The screenshot shows a 'Security' dialog box with the following options and fields:

- Use HTTPS security
- Use existing certificate
- Install new certificate (Must be compatible with Apache, do not use Windows certificates)

Fields for certificate file paths:

- Key File Path: [Text Box] [Browse...]
- Primary Certificate File Path: [Text Box] [Browse...]
- Intermediate Certificate File Path: [Text Box] [Browse...]

Generate self-signed certificate

Fields for self-signed certificate details:

- Country name (2 letter code): [Text Box]
- State/province name: [Text Box]
- City/locality name: [Text Box]
- Common name: [Text Box]

Install

Installing an SSL certificate into any of the VE602x servers must follow this two-step process.

- 1) Generate a *Certificate Request* which is sent to the *Certificate Authority*.
- 2) Once you've received a response package (typically a zip file which will need to be extracted) from the *Certificate Authority*, upload the certificate to the server. You may or may not be provided, or require, the Intermediate Certificate.

Most common mistakes

The two most common made mistakes are:

- 1) When requesting the certificate make sure the certificate is either an *Apache*, or *Nginx* server. Do **not** get one for a Microsoft server. The VE602x servers are running Linux and will *never* work with a wrong certificate.
- 2) When generating the *Certificate Request* there are two files generated. The first, the actual certificate is sent to the *Certificate Authority*. The second, is used during the install process and is *needed* for the install to succeed. This file has a file extension of *.key*.

Sample files

Sample Certificate of Request

-----BEGIN CERTIFICATE REQUEST-----

MIIcUdCCAAACAQAawczELMAkGA1UEBhMCMVVMxETAPBgNVBAGMCFZpcmdpbmlhMRAwDgYDVQQHDAdSb2Fub2tlMRUwEwYDVQQKDAxWYWxjb20sEIOQy4xEzARBgNVBAsMCkVHSU5FRVJTTkcxZzARBgNVBAMMCnZhbGNvbS5jb20wggEiMA0GCSqGSIb3DQEB AQUAA4IBDwAwggEKAoIBAQCxhNgbFsqn9Mp+Xd/sLB6fEWL32JYLUXEEmsOGimOs RGQd1kRa6BjN3bIRPKII0Fr+yChQAFD5EstoTdcdbbBRx0e0K1DUalQWWbC31CUI MGhZ8xtPQdla5GgiCv8ygVb7JJzcGEY+RXDt+kLLGL73UNW16jvAYWAablAuJXa FdV0xLljzZY5erXFE/odvakeJJo6Vig8IXD4IMB2e+ZKRyRTmeIWkOh0CQskfNQD m4hQpkzH2yaQOMtdeya/zeQjHzUpbp/uBgsVzVVlp0Ma28fIkSf+xLcqGiDu5Ec+ P2Yt8UwqrOSLfmnwsJQq7AAxaWlBj21lI6wR7zf2Js9RagMBAAGgADANBgkqhkiG 9w0BAQUFAAOCAQEAA0gVKulgG/DQHAGQKNtTV1jhLQcgaqvwHuHtlfc+4fbC57o 43ZLSsUScySezTeOMCXceRC8xZiNqiNpff9EkzGAoSQ3bh7JJuFUFruNk8LN5AKy UMDr7tL4NtOrJ6b5kwbPatQvJWBIRxv5lyEtKE+D2AK0Su1fJ9TFZy3mcm9WtF+J YOaJgxb/nTgmr+sww3l9yHjPUTcrHZh+vmMU8U1VQlwnHQQbpcWgx850wDOozQrM bhJzTDYGBG0SjYIKQCkee51N+Q/hT0buUtUWbpyEPiSc8/G60xyMq5KCXTk/QlOl cSdKuxcgd4aoshpR3pQlhKKk07eoM1jR21iaxw==

-----END CERTIFICATE REQUEST-----

Sample Private Key

-----BEGIN PRIVATE KEY-----

MIIEvglBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQCxhNgbFsqn9Mp+ Xd/sLB6fEWL32JYLUXEEmsOGimOsRGQd1kRa6BjN3bIRPKII0Fr+yChQAFD5Esto TdcdbbBRx0e0K1DUalQWWbC31CUIMGhZ8xtPQdla5GgiCv8ygVb7JJzcGEY+RXDt +kLLGL73UNW16jvAYWAablAuJXaFdV0xLljzZY5erXFE/odvakeJJo6Vig8IXD4 IMB2e+ZKRyRTmeIWkOh0CQskfNQDm4hQpkzH2yaQOMtdeya/zeQjHzUpbp/uBgsV zVVlp0Ma28fIkSf+xLcqGiDu5Ec+P2Yt8UwqrOSLfmnwsJQq7AAxaWlBj21lI6wR 7zf2Js9RagMBAAEcggEBAIyoDfOo43qhY7EtALhJXRn81MY9PuZl6ZwUZMi97qwY pJtfo1nEfaLhBG1x9aiwpukp/4ckOQSh97n1s3N2IPa3SAFIMPGeLnJnLrb5yVKF uKIND16FdoumXzxaKksCYMEuCXv7X+0HaKunmDUErouX6T3zDwPh2L4fB0JY/6OE R3xho2vLZBBRlpfVx/0E6AQUgvpvOL2ZbBceCdv4BHHCLoFipKpBT2fPKgYux5ccY z4KWJGXsipaeYRJs/+F5ovwd8395Q8aft54KQ8TTlw3TcCQeJu5vEHlql/R7l0gV schwrkZohk9fmdoAlh3LTaiweQ5l2zh7mETISc6rwmECgYEA17E7rfWgyJtOPYh0 CHD1+X7BNtlqg7iX4N497krU7Vr0hnZBVdefEb3APXnnGhbiYdLRbljBKZwvja07 8hqMDLz8ChNMYIBTzpaOs1+z795SeZZFS8kwSI1K0MDIRzF37zf/qHiwclOqQdZ xK67MA/PpKdoD4STus28dCvI5P8CgYEA0rFjPan5xQB3w7dqvcxs83R1r+reP0Cx +hpgm/qMxdA+iaaOrpcPSeBYFFmtlGnAppLJCsh3VpVCRYhsO97UuwOI4ktabsGQ 9Wv0HEt0QN65i0uR0naKoT3WzOVTTTrBHgcwKrvQmKe0DwUNynVQS8MRqPEohuC+4 /rab1n1Hu68CgYBUxLwZiY3QN08AQxqD2zCwmT/Jih3AyinEIFL144oxbJGjX0ys 3KgCjuGXUxGBkuYAgbsxR+6GG0loB5SdmyG/vs8DZL52vhKjqQF/Rvg02lb4DgnU wgt/XnQaT668ID1W7rB5/GenHOEdcapn7bPPsrdG10uW3qvYWek1XVLBwKBgQCw cEBR7OavZR7mVVkclG8oyWQst4D6c1EX4rL4rC7rEOLuHv7pkjMJAMgZ8qd727ur Qsz9LLdTWJcw53fMA2UeX21oJDZM/ehlveilMULfeCTIU5mAKCkbsk+JMpo7EUaw oBBqRqcXARbd53+55MgfvDxC1Mm8FqrTE1UZn7xMnQKBGf4P/oVR8ISb9jrh7OTW wCDwmN9l9DsDdC8ifCFmo8foLBL9myyuAlafkWrW3rRODJTaVWQ9EzoOs9kRJZJQ /zu7W0Ew7ur66YkiFEFTZqA2veBs11dO5Y8WBHNp78EsChJFD9EpIKt4fnjrpHJR u+19+2EFT/mLCJ9kOBTl6ISf

-----END PRIVATE KEY-----

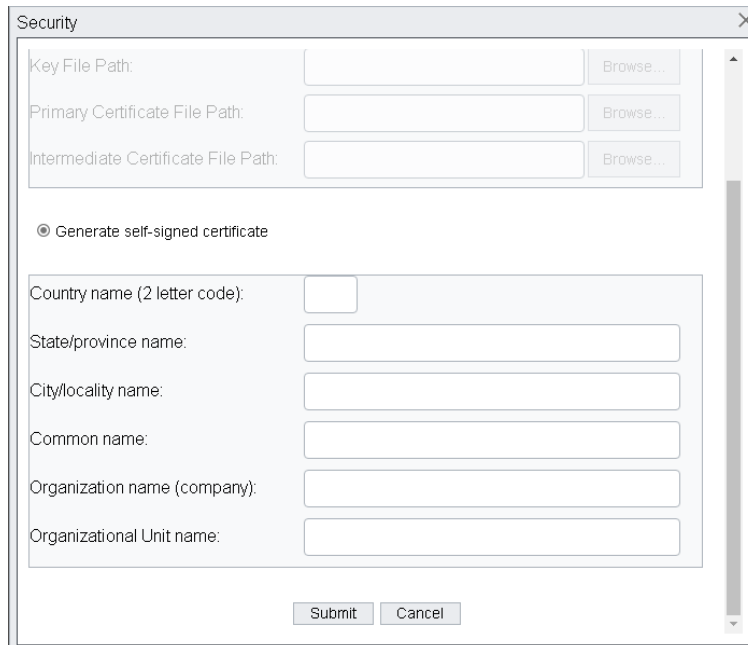
Sample Primary Certificate

-----BEGIN CERTIFICATE-----

```
MIICATCCAwoCCQDPufXH86n2QzANBgkqhkiG9w0BAQUFADBFMQswCQYDVQQGEwJu
bzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ210
cyBQdHkgTHRkMBA4XDTEyMDEwNDQwMFOxDTIwMDMxOTE0NDQwMFOwRTELMAkG
A1UEBHMCMm8xEzARBgNVBAgMCINvbWUtU3RhdGUxITAfBgNVBAoMGEludGVybmV0
IFdpZGdpdHMgUHR5IEEx0ZDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtrQ7
+r//2iV/B6F+4boH0XqFn7alcV9lpjvAmwRXNKnxAoa0f97AjYPGNLKrpkNXXhB
JROIdbRbZnCNc5fzX1a+JCo7KStzBXuGSZr27TtFmcV4H+9glRlcNHtZmJLnxBJ
sihkGR8yVYdmJZe4eT5ldk1zoB1adgPF1hZhCBMCAwEAATANBgkqhkiG9w0BAQUF
AAOBgQCeWBEHYJ4mCB5McvSSUox0T+/mJ4W48L/ZUE4LtrRhHasU9hiW92xZkTa7E
QLcoJKQiWfiLX2ysAro0NX4+V8iqLziMqvswnPzz5nezaOLE/9U/QvH3l8qqNkXu
rNbsW1h/IO6FV8avWFYVfOutUwOaZ809k7iMh2F2JMgXQ5EymQ==
```

-----END CERTIFICATE-----

Self-Signed Certificates



Security

Key File Path: Browse...

Primary Certificate File Path: Browse...

Intermediate Certificate File Path: Browse...

Generate self-signed certificate

Country name (2 letter code):

State/province name:

City/locality name:

Common name:

Organization name (company):

Organizational Unit name:

Submit Cancel

Enter the requested information

To find your country code for self-signed certificates, [click here](#).

Click Submit

In either case, if certificate installation is successful, reloading the browser will result in the browser using https.

Users

The default system has a single user login (admin). An Application Server login should be created for each user allowed to access the system, to control access to system features There are 3 levels of privileges that a user can be given.

The screenshot shows the 'Add New User' dialog box. It includes fields for Username, Password, and Confirm. There are checkboxes for 'Hide Menu' and 'Admin'. A 'Privileges' section lists various system functions with dropdown menus set to 'full'. A 'Startup Tabs' section shows 'Selected Items' and 'Available Items' panes with navigation arrows between them. 'Submit' and 'Cancel' buttons are at the bottom.

They are full, limited and disabled. The Users form allows specific rights to be assigned on a per user basis. Click “Users” and choose “Add User” to begin. For each system user, enter a user name and a password. User names must begin with a letter, must not contain spaces and must be less than 255 characters in length. Passwords must be between 6 and 31 characters in length and contain at least 2 numbers or symbols.

For each server function choose Full, Disabled or Limited access to each available system function.

Full = unrestricted view, modify and execute rights.

Disabled = function will not be shown

Limited = view and execute rights

Available Items for startup tabs include:

Calendar

Audio Editor

Event Editor

Input Editor

CAP Alerts Viewer

CAP Alerts Editor

CAP Sources Editor

Group Code Editor

Play List

Schedule Editor

Text Editor

Individual Graphics

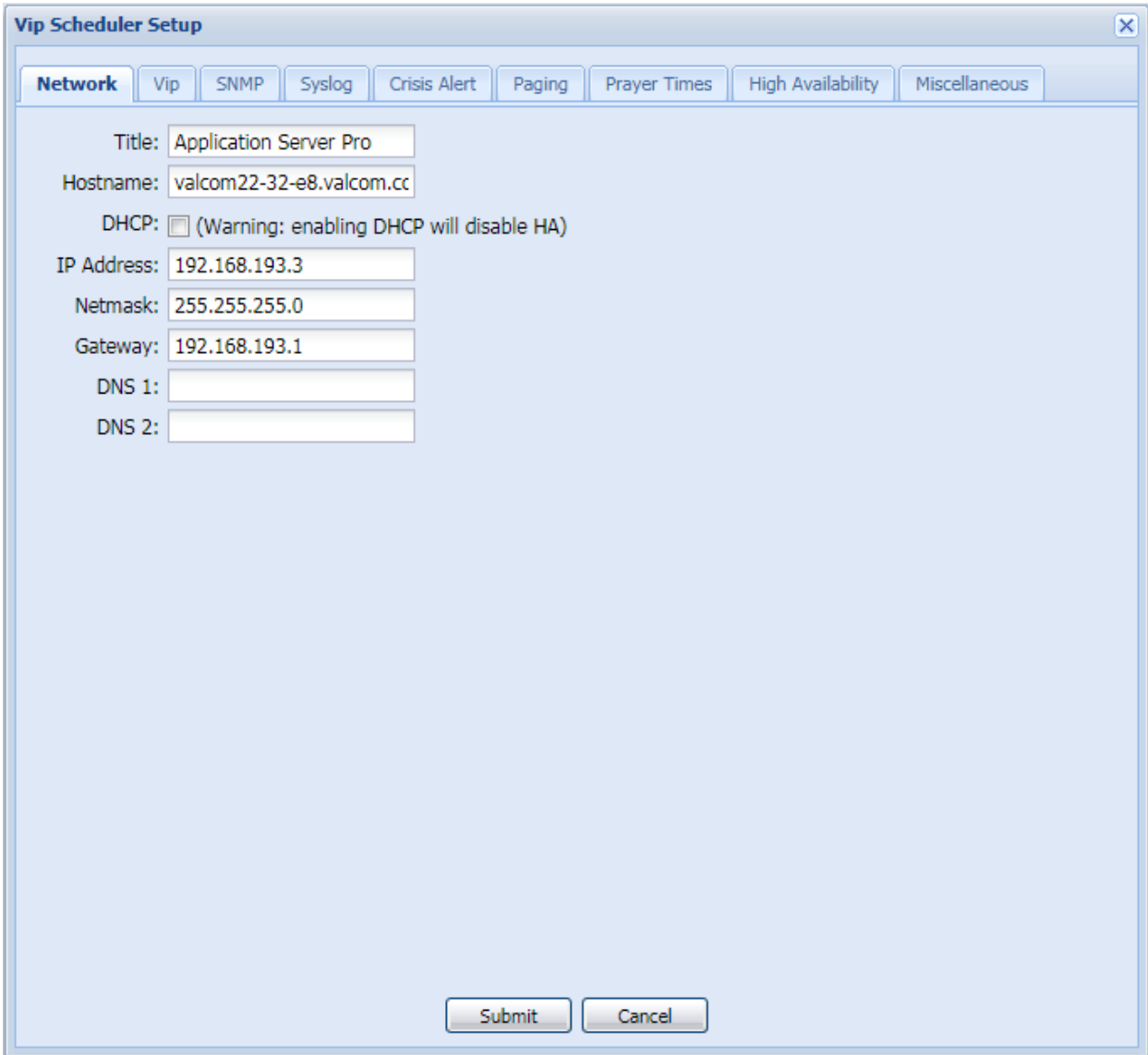
The “Hide Menu” checkbox provides an uncluttered user interface by hiding the left menu tree when not in use.

The “Admin” checkbox allows the creation of users with any level of access. When unchecked, factory predefined rights are enforced and any screens with a “hide” checkbox will not be available to the non-admin user.

Under Startup Tabs, Selected Items, define what screens will be immediately viewable upon login. Multiple Simultaneous Logins to an Application Server are permitted if the logins are to different user accounts. The same browser may not be used to login to two or more separate Application Server accounts at the same time.

Setup Options

Setup/Network



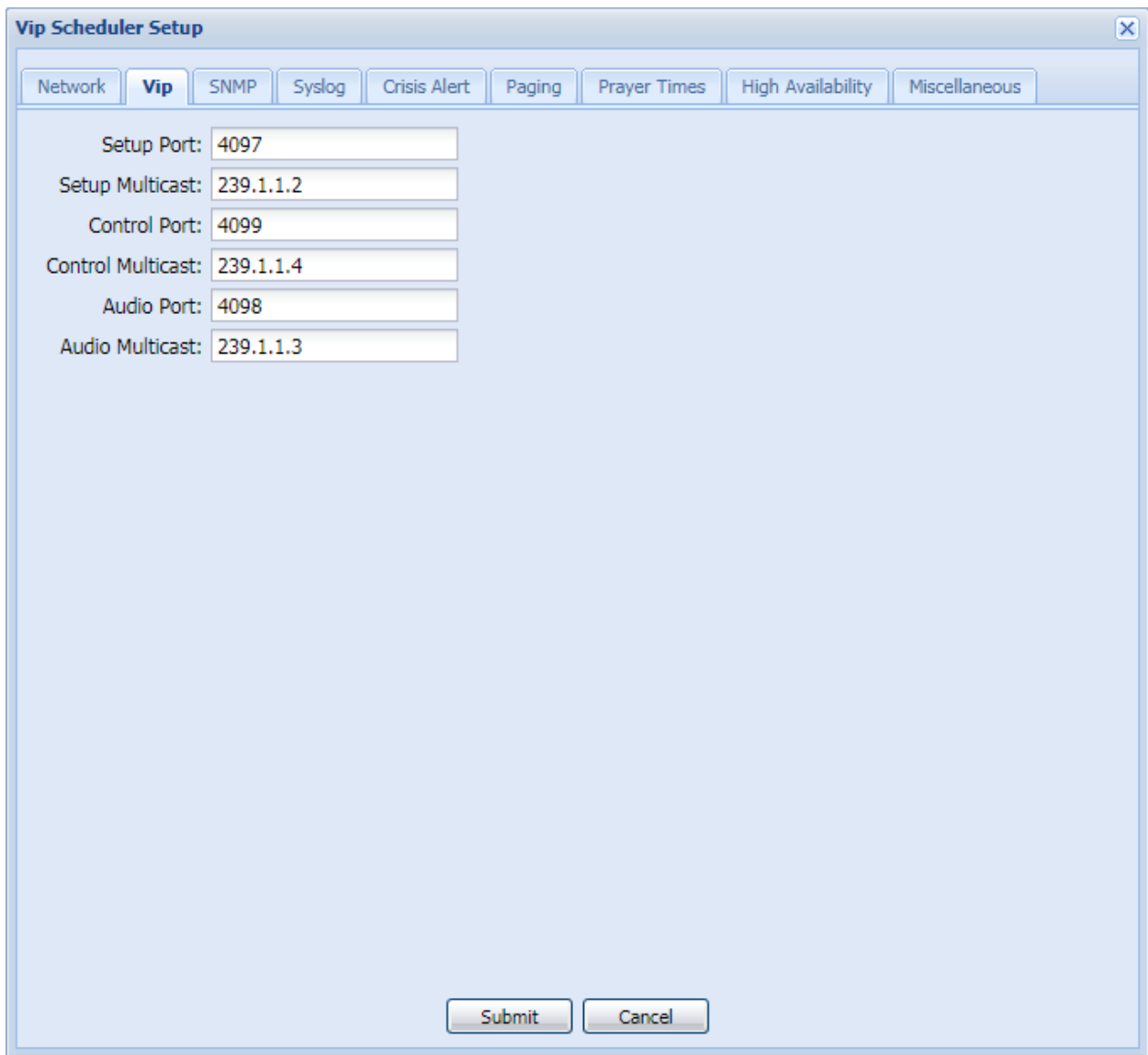
The screenshot shows a window titled "Vip Scheduler Setup" with a close button in the top right corner. Below the title bar is a row of tabs: "Network" (selected), "Vip", "SNMP", "Syslog", "Crisis Alert", "Paging", "Prayer Times", "High Availability", and "Miscellaneous". The main area contains the following fields:

- Title: Application Server Pro
- Hostname: valcom22-32-e8.valcom.cc
- DHCP: (Warning: enabling DHCP will disable HA)
- IP Address: 192.168.193.3
- Netmask: 255.255.255.0
- Gateway: 192.168.193.1
- DNS 1: (empty field)
- DNS 2: (empty field)

At the bottom of the window are two buttons: "Submit" and "Cancel".

The Setup/Network Tab displays and allows modification of the Application Server's Title, which is displayed on the top of the main browser screen, the network hostname and the IP address settings.

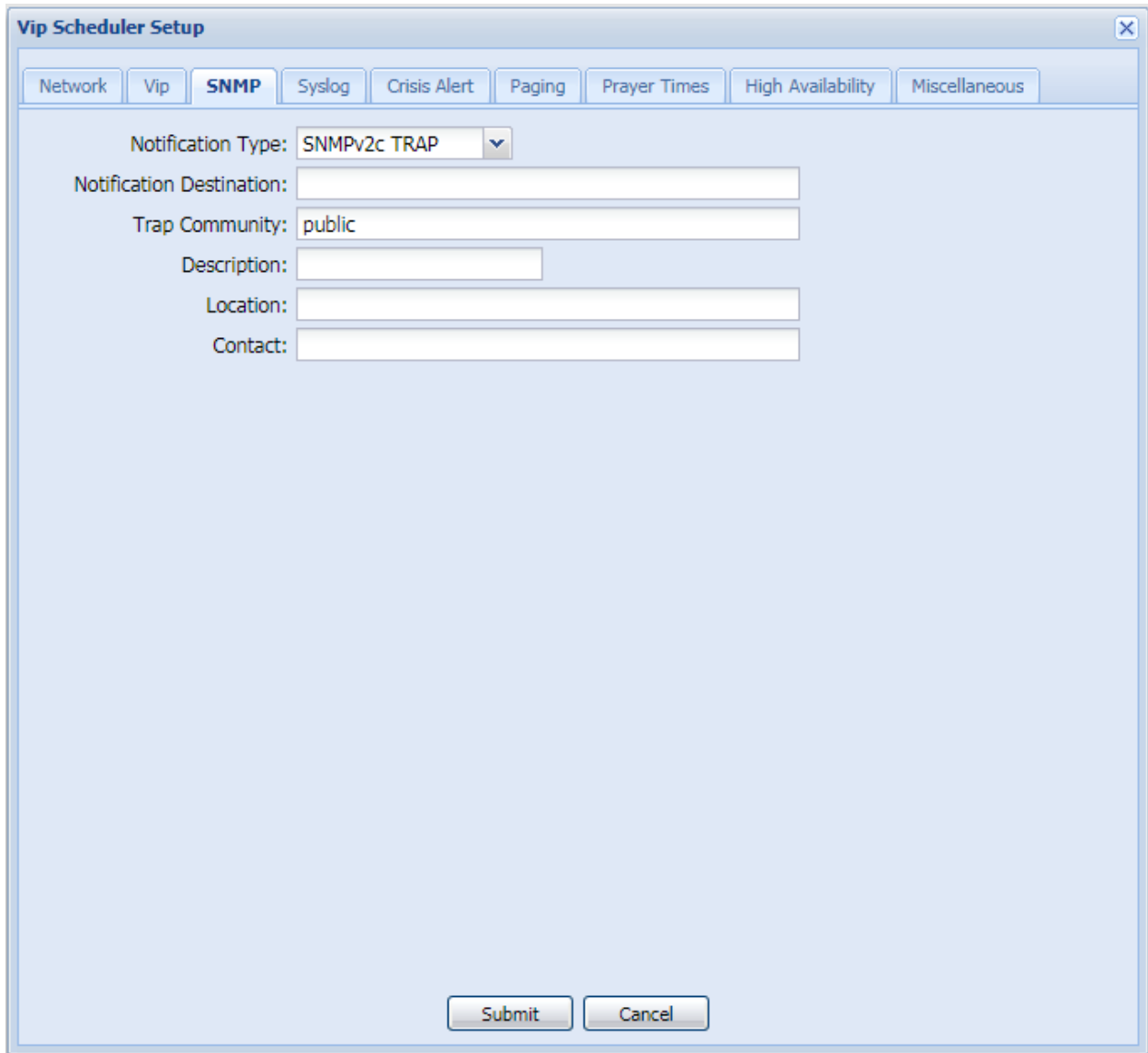
Setup/VIP Tab



The screenshot shows a web-based configuration window titled "Vip Scheduler Setup". At the top, there is a navigation bar with several tabs: "Network", "Vip" (which is selected and highlighted), "SNMP", "Syslog", "Crisis Alert", "Paging", "Prayer Times", "High Availability", and "Miscellaneous". Below the tabs, the "Vip" configuration section contains six input fields arranged in three rows. The first row contains "Setup Port:" with the value "4097". The second row contains "Setup Multicast:" with the value "239.1.1.2". The third row contains "Control Port:" with the value "4099". The fourth row contains "Control Multicast:" with the value "239.1.1.4". The fifth row contains "Audio Port:" with the value "4098". The sixth row contains "Audio Multicast:" with the value "239.1.1.3". At the bottom of the window, there are two buttons: "Submit" and "Cancel".

The Setup/VIP Tab displays and allows modification of the system's multicast addresses and associated ports. These should only be changed with factory direction.

Setup/SNMP Tab



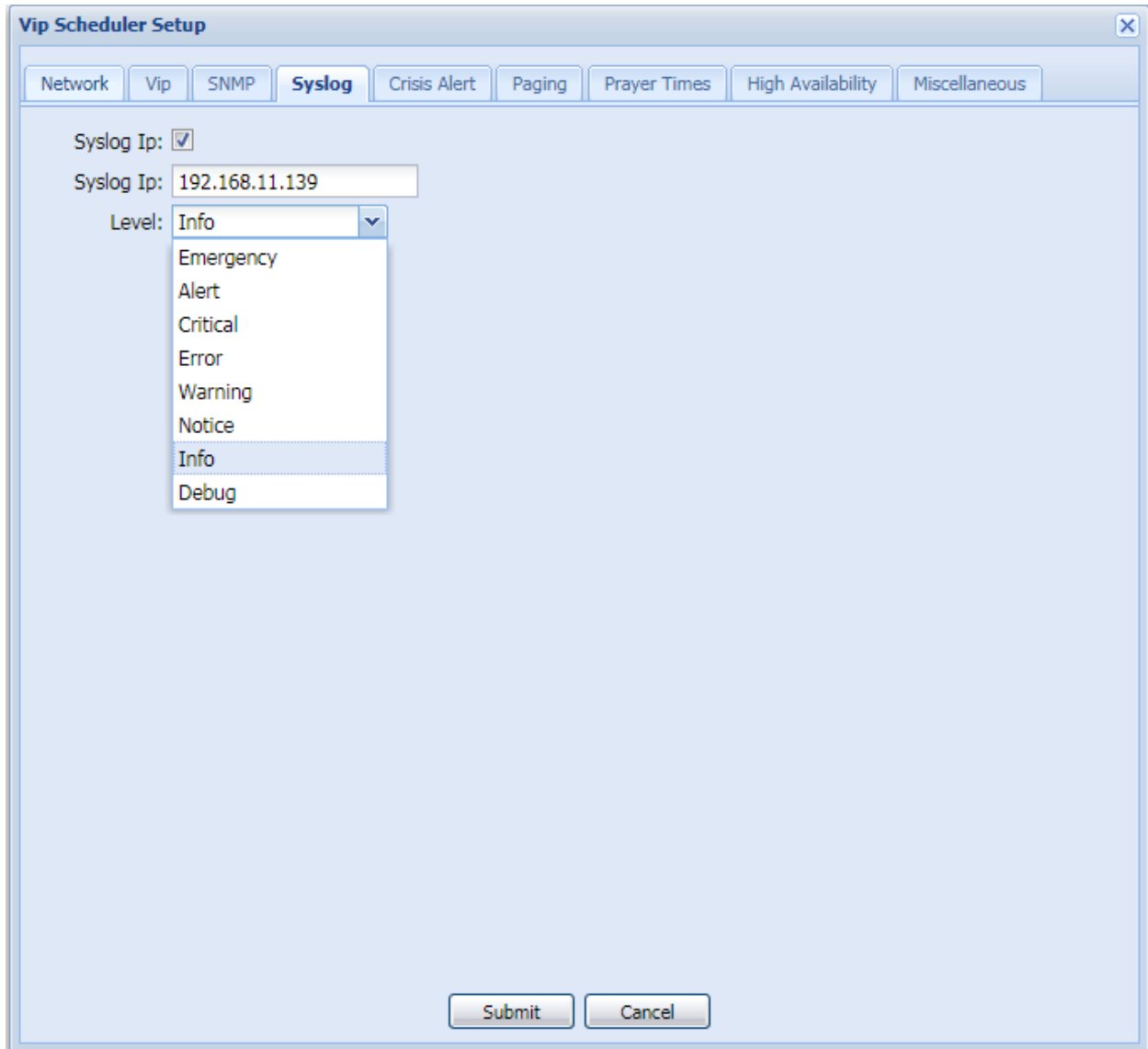
The screenshot shows a software window titled "Vip Scheduler Setup" with a close button (X) in the top right corner. Below the title bar is a tabbed interface with the following tabs: Network, Vip, **SNMP** (selected), Syslog, Crisis Alert, Paging, Prayer Times, High Availability, and Miscellaneous. The main area of the window contains the following fields:

- Notification Type: A dropdown menu with "SNMPv2c TRAP" selected.
- Notification Destination: An empty text input field.
- Trap Community: A text input field containing the value "public".
- Description: An empty text input field.
- Location: An empty text input field.
- Contact: An empty text input field.

At the bottom of the window, there are two buttons: "Submit" and "Cancel".

The Setup/SNMP Tab displays and allows modification of the system's SNMP settings.

Setup/Syslog Tab



The screenshot shows a window titled "Vip Scheduler Setup" with a close button (X) in the top right corner. Below the title bar is a tabbed interface with the following tabs: Network, Vip, SNMP, **Syslog**, Crisis Alert, Paging, Prayer Times, High Availability, and Miscellaneous. The "Syslog" tab is active. Inside this tab, there is a "Syslog Ip:" label followed by a checked checkbox and a text input field containing "192.168.11.139". Below this is a "Level:" label followed by a dropdown menu. The dropdown menu is open, showing a list of log levels: Emergency, Alert, Critical, Error, Warning, Notice, Info (highlighted), and Debug. At the bottom of the dialog box are two buttons: "Submit" and "Cancel".

The Setup/Syslog Tab displays and allows users to define a destination for the Application Server's syslog data along with the level of messages to be sent. At this point the only relevant levels are Info and Debug. Info provides basis system messages while Debug is intended for Valcom software developers.

Setup/Crisis Alert Tab

The screenshot shows the 'Vip Scheduler Setup' dialog box with the 'Crisis Alert' tab selected. The dialog has a title bar with a close button and a tabbed interface with the following tabs: Network, Vip, SNMP, Syslog, Crisis Alert (selected), Paging, Prayer Times, High Availability, and Miscellaneous. The 'Crisis Alert' section contains the following fields and options:

- Crisis Alert enabled:
- CM Software Version: 6.3.111 and later 6.3.xx and earlier
- CM Server IP: 192.168.97.137
- SNMP Community Name: everyoneRW
- CM Extension: 3101
- CM Password: ●●●●
- CM Confirm Password: ●●●●
- AE Server IP: 192.168.97.135
- AE Port: 4721
- AE Server UserName: AlertMonitorDE
- AE Server Password: ●●●●●●●●●●
- AE Confirm Password: ●●●●●●●●●●
- Text Monitor Port: 10065
- Text Monitor Protocol: TCP UDP
- Text Monitor Example: name=firstname lastname,ext=extension,building=build

At the bottom of the dialog are 'Submit' and 'Cancel' buttons.

The Setup/Crisis Alert Tab displays and allows users to define the information required for emergency call alerting with Avaya Communication Manager / Avaya Application Enablement Services. This setup tab is not used with Avaya IP Office.

Click the “Crisis Alert enabled” checkbox to enable the fields on this page and provide the information required to use Avaya Application Enablement Services for Crisis Alerting.

CM Software Version:

Select the version of the Avaya Communication Manager server to which SNMP queries will be submitted.

CM Server IP:

Enter the IP address of the Avaya Communication Manager server to which SNMP queries will be submitted and where the telephone extension with a Crisis Alert button is defined.

SNMP Community Name:

Enter the SNMP V1 community string that has been configured on the Communication Manager to allow access for this server to make SNMP queries. The access can be read-only for SNMP versions below 6.3.111 and read/write for versions greater than 6.3.111.

CM Extension:

Enter the extension number configured on the Communication Manager for use by this server to monitor for Crisis Alert notifications. This extension must have a Button Assignment as "crss-alert".

CM Password / Confirm CM Password:

Enter the password for the extension number entered above.

AE Server IP:

Enter the IP address of the Avaya Application Enablement Services server.

AE Port:

Enter the port number to which the AE server listens for service connections. This must be the unencrypted port on the AE server.

AE Server User Name:

Enter the user created on the Avaya Application Enablement Services server for this server to log in.

AE Server Password / AE Confirm Password:

Enter the password for the AE user entered above. Due to quirks with the Java programming language, do not use a semicolon character in the password.

Text Monitor Port:

Enter the port which will be used with a Text Monitor filter on this server to receive alerts. This port will also be entered in the Text Monitor configuration.

Protocol:

Choose TCP or UDP to match the protocol selected for the Text Monitor filter on this server.

Sample:

This read-only field presents a sample of a Text Monitor string that would be used with a Text Monitor to parse the text received by the Monitor. When creating a Text Monitor to receive the alerts, the following Regular Expression (regex) will parse the incoming text and assign variables to be used with a Text-to-Speech audio file:

```
name=(?<name>.*),ext=(?<ext>\d+)(,building=(?<bldg>[^,]*)?)?(,floor=(?<floor>[^,]*)?)?(,room=(?<room>.*))?
```

The regex above would be entered without line breaks. The variables available to the TTS engine would be:

- name – the name assigned to the telephone making the emergency call
 - ext – the extension number assigned to the telephone
 - building, floor, room – the building, floor and room assigned to the telephone
- Building, room and floor may be sent as empty fields if the corresponding fields in the station definition in Aura have not been entered.

Setup/Paging Tab

Vip Scheduler Setup

Network Vip SNMP Syslog Crisis Alert **Paging** Prayer Times High Availability Miscellaneous

System Volume Offset:

Default Priority:

Quick Page

Priority:

Audio Volume Offset:

Audio Repeat Gap (sec):

Sign Color:

Sign Duration (sec):

The Setup/Paging Tab:

- a) Displays and allows modification of the Application Server's default Event volume offset and priority.
- b) Allows users to define the priority, Audio Volume offset, Audio Repeat Gap, Sign Color and Sign Message Duration for messages originated through the Quick Page form.

Setup/Prayer Time Tab

Vip Scheduler Setup

Network Vip SNMP Syslog Crisis Alert Paging **Prayer Times** High Availability Miscellaneous

Prayer Times enabled:

Location

Country:

State/Province:

City:

Latitude: ° ' N

Longitude: ° ' E

Time Zone:

DST starts:

DST ends:

Qibla:

Prayer Time Calculation Parameters

Method: Univ. of Islamic Sciences, Karachi

Fajr: 18 ° below horizon

Isha: 18 ° below horizon

Asr Method: Standard

Dhuhr: 0 minutes after solar transit

Maghrib: 0 minutes after sunset

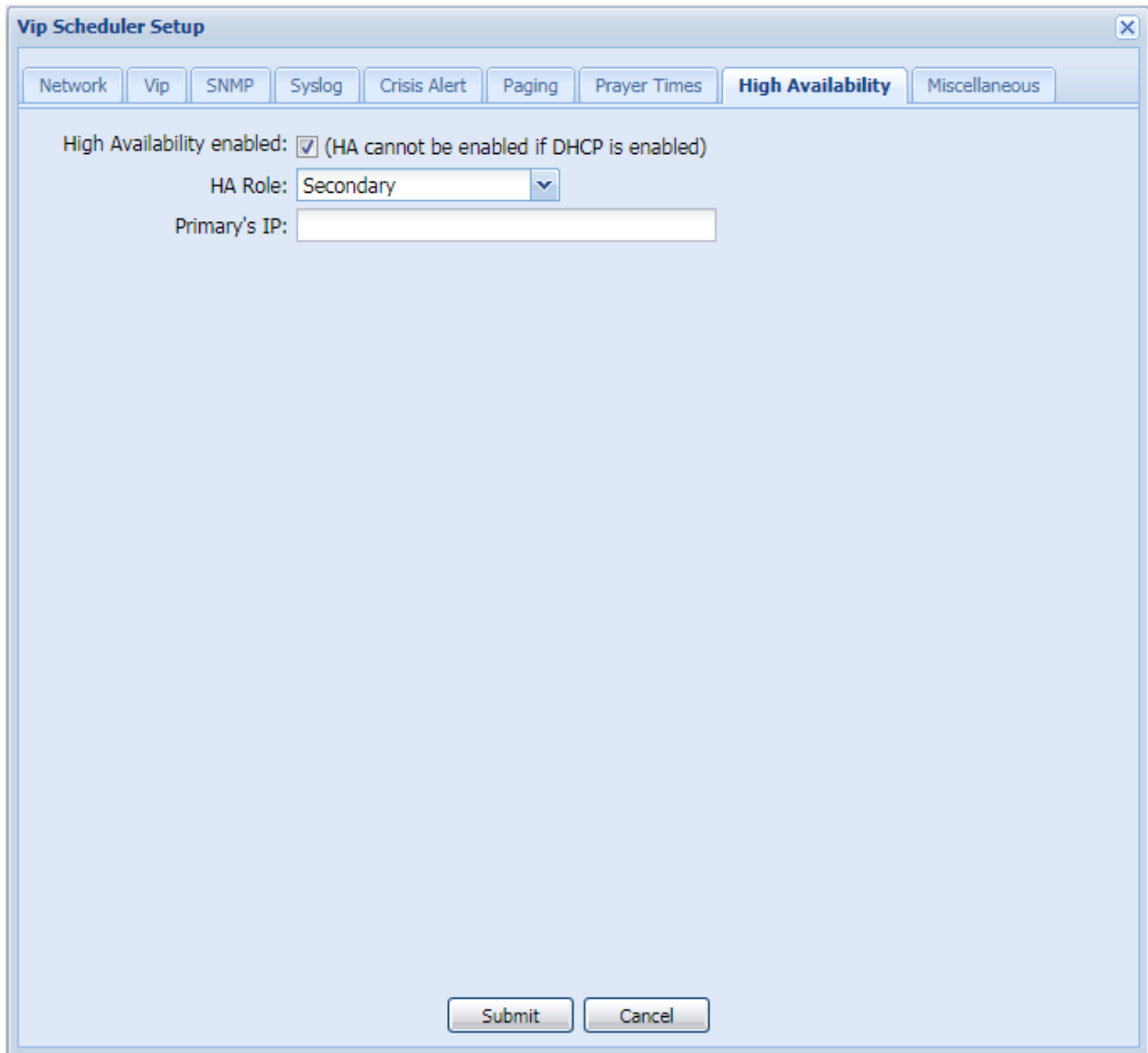
Events

	Event	Time today
Fajr:	<input type="text"/>	<input type="text"/>
Shuruq:	<input type="text"/>	<input type="text"/>
Dhuhr:	<input type="text"/>	<input type="text"/>
Asr:	<input type="text"/>	<input type="text"/>
Maghrib:	<input type="text"/>	<input type="text"/>
Isha:	<input type="text"/>	<input type="text"/>

Submit Cancel

The Setup/Prayer Times Tab displays and allows users to define the parameters governing automatic broadcast of audio Events as prayer time reminders.

Setup/High Availability Tab



The screenshot shows a software window titled "Vip Scheduler Setup" with a close button in the top right corner. Below the title bar is a tabbed interface with the following tabs: "Network", "Vip", "SNMP", "Syslog", "Crisis Alert", "Paging", "Prayer Times", "High Availability" (which is the active tab), and "Miscellaneous". The "High Availability" tab contains the following settings:

- High Availability enabled: (HA cannot be enabled if DHCP is enabled)
- HA Role: Secondary (selected in a dropdown menu)
- Primary's IP: [Empty text input field]

At the bottom of the window, there are two buttons: "Submit" and "Cancel".

The Setup/High Availability Tab displays and allows users to set up high availability mode as described on the next page.

Setting up a High Availability Pair

Introduction

High availability, which will be referred to as HA, is a system design intended to make certain that users can access the system without a loss of service. The purpose of HA is to minimize the down time or other periods where the system is unavailable, and to maximize run time and availability. One way to handle down time and system unavailability is to create a backup and failover system using two HA enabled servers. One of the HA servers will act as the Primary server or Master, while the other acts as the Secondary backup server or Slave. All changes made to the Primary will be replicated to the Secondary server so if the Primary goes down the Secondary will take over as the Master. This minimizes the down time and information loss.

Setup

To setup HA between two servers, it is important that the HA servers be two of the same VE602x servers. They must be identical in software as well as being up to date with the latest firmware installed on both. Both VE602x servers must also be set to the same subnet. If one server is on the 192.168.48.1 subnet and another server is on the 192.168.47.1 subnet they will not be able to be set into a HA pairing. If the VE602x servers are in two separate physical locations, they will still need to be on the same subnet. To do that, a VLAN or Virtual LAN will be used. A VLAN allows for devices to share a common subnet even if they are not on the same network switch. Putting the VE602x servers in different locations is recommended since a localized event will be less likely to affect both servers.

After ensuring that both servers are of the same type and on the same subnet; check to make sure that both servers are currently assigned a static IP address. **HA cannot be enabled if both or one of the servers is set to DHCP.** Once both servers have a static IP address it is time to set up the HA. Make sure to log into the server as the Admin to access this setting. Expand the Administration folder and select the Setup option located there. ***It's important to set HA up in the server that will serve as the secondary before setting up HA up in the server that will serve as the primary.***

Check the box labeled High Availability Enabled. Using the drop menu next to the label 'HA Role:' designate one of the servers as the Primary and one of the servers as the Secondary. For the setup of the Secondary the user is only required to select the role of Secondary for the server and enter the IP address of the server that will be acting as the Primary.

Once the information has been added into fields simply select "Submit" and return to the Primary server to finish the setup.

The Primary will require more information than the Secondary to set up properly. The form will look like the one posted above. To complete setup a Virtual IP Address must be assigned. This address will allow a user to log into whatever device is currently the Master without having to worry about knowing the static IP address for either device. The IP address of the Secondary will be required as well as the Hostname of the Secondary server. This information must be identical to the information shown on the Network tab/Setup option in the Secondary server. The CARP VHID is a unique number that is used to differentiate the HA pair from any other HA pair that may

be running on the same network. All HA pairs on the same network must have a different CARP VHID number. The final step is to assign a CARP password for the HA pair. The password must be between 6 and 31 characters in length and contain at least 2 symbols or numbers. When all the required information has been filled in on the form; select "Submit" for the Primary device.

Testing

After establishing HA, you will be able to access the server from the Virtual IP within approx. 1 minute but allow a minimum of 5 minutes before you attempt to test the HA mode.

Once the setup has finished it is important to test and see if the HA pair is functioning. A good first test is to try and log into the server using the Virtual IP address set for the HA pair. If it is reachable through the browser and the user can log on, then it is a good sign. Next try to log into the server using the IP address of the Primary. It should be reachable through the web browser and allow the user to log into the system. Finally, attempt to log into the server using the IP address of the Secondary. The IP address should give a 'cannot be found' message in the browser. This test should establish that the HA is functioning properly.

It is also recommended to test if the Secondary will properly assume the role of the Primary should the Primary go offline. To do this, it would be simplest to either unplug the Ethernet from the Primary device or shutdown the Primary. Either method will take it off the network. The Secondary should then realize that the Primary is no longer available and assume the role of the Primary. To make sure it is working, attempt to log into the server using both the Virtual IP address and the IP address of the Secondary after taking the Primary offline. Once the test is complete, connect the primary back to the network and temporarily remove the Secondary from the network. This should force the Secondary offline and force the Primary to take over the Virtual IP address.

If the user has the VIP Status Monitor then they can check to see if the HA pair is working by entering the information into the VIP Status Monitor. If the status of the HA pair does not yield any error messages or warnings then the HA pair should be functioning correctly. If the VIP-102B tool is in use, it will also change when using HA. The Secondary device will no longer be visible in the VIP-102B tool and the Primary will have information about the Failover System in the Summary tab. This is shown in the image below. This is another way to test if a HA pair is functioning.

User Instructions

Once HA has been set up and tested for proper functionality, it is time to allow the users access to the system. For the standard user the unit will operate the same as any VE602x server. The system admin will create the user accounts and then distribute the accounts and passwords to the users. The users will also be required to know the Virtual IP address of the HA pair. The users will enter the Virtual IP address into the browser and use their user name and password on the

login screen to log into the system. The user does not need to know the static IP address for either server or even know that there are two servers acting in a HA pair.

If for some reason you need to power down a HA pair, you will need to do so from the power button on the front of each server. Use a straightened paperclip to momentarily press the power button.

When powering up two servers configured for HA, it is best to start the primary server first.

If you need to disable HA mode, disable it from the setup tab in the primary. The secondary should be accessible from its own IP address after approx. 1 minute. The primary server will require a power reset. Do so using the power button of the front. Push it once. After approx. 10 seconds the alarm will sound. Turn off the alarm with the "Silent" button. Then push the power button again to restart the server. After approx. 2 minutes you should be able to access the server using it's IP address. HA will be disabled.

Setup/Miscellaneous Tab

The screenshot shows a window titled "Vip Scheduler Setup" with a close button (X) in the top right corner. Below the title bar is a tabbed interface with the following tabs: Network, Vip, SNMP, Syslog, Crisis Alert, Paging, Prayer Times, High Availability, and Miscellaneous. The "Miscellaneous" tab is selected and active. The main area of the dialog contains the following settings:

- Pre-page Delay(ms): 500
- Post-page Delay(ms): 250
- Pre-record Trim(ms): 800
- Post-record Trim(ms): 800
- Classic Calendar Mode:
- User Timeout:
- Minutes: 15

At the bottom of the dialog are two buttons: "Submit" and "Cancel".

The Setup/Miscellaneous Tab displays and allows users to define:

- the default pre and post page delays for audio originating from the Application Server
- The amount of recorded audio that will be trimmed from audio recorded using the Application Server recording capabilities.
- When the Application Server will automatically logout inactive users

Administration/System/Clock

Clock Setup

Country: United States - US

Cities/TZone_ID: America/New_York

Comments: Eastern (most areas)

External NTP Server Enable:

Is Server Group:

-
-
-
-
-
-

Ntp Server Addresses:

0.us.pool.ntp.org

Date: 06/12/2018

Time: 08 : 11 : 37

Valcom Internal NTP Server:

Submit Cancel Ignore Address Errors

The clock form is used for defining NTP time sources for the Application Server.

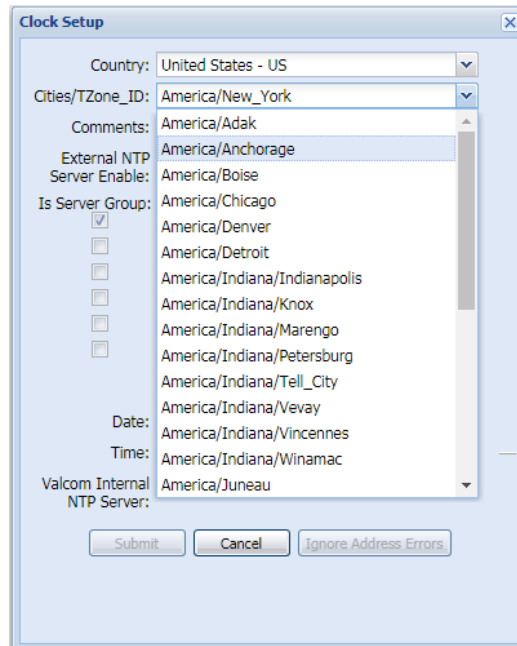
When External NTP Server Enable is checked, and at least one valid NTP Address is entered, the Application Server will periodically poll the NTP server for current time information.

If you know that an NTP server address that you've entered is directed to a pool of servers, then check the "Is Server Group" checkbox. If the NTP Server is a stand-alone server, or if you are uncertain, then do not check the "Is Server Group" check box. *Only check the box if the address/hostname is a pool (i.e. 3.pool.ntp.org).*

If an NTP server is not available for some reason, it is simply disregarded until the next time check interval. The frequency at which the Application Server checks for time updates is a function of NTP and is dependent upon the recent history of time response stability.

When “Valcom Internal NTP Server” is checked, then the Application Server will respond to requests for NTP time from other devices. However, when both NTP Enable and NTP Server are checked, then the Application Server will only respond to requests for NTP time from other devices if the Application Server can, itself, obtain valid time.

Note that changes to clock settings may force a system log out.



Administration/System/License

License

Current License

Expiration(days):

Model:

New License

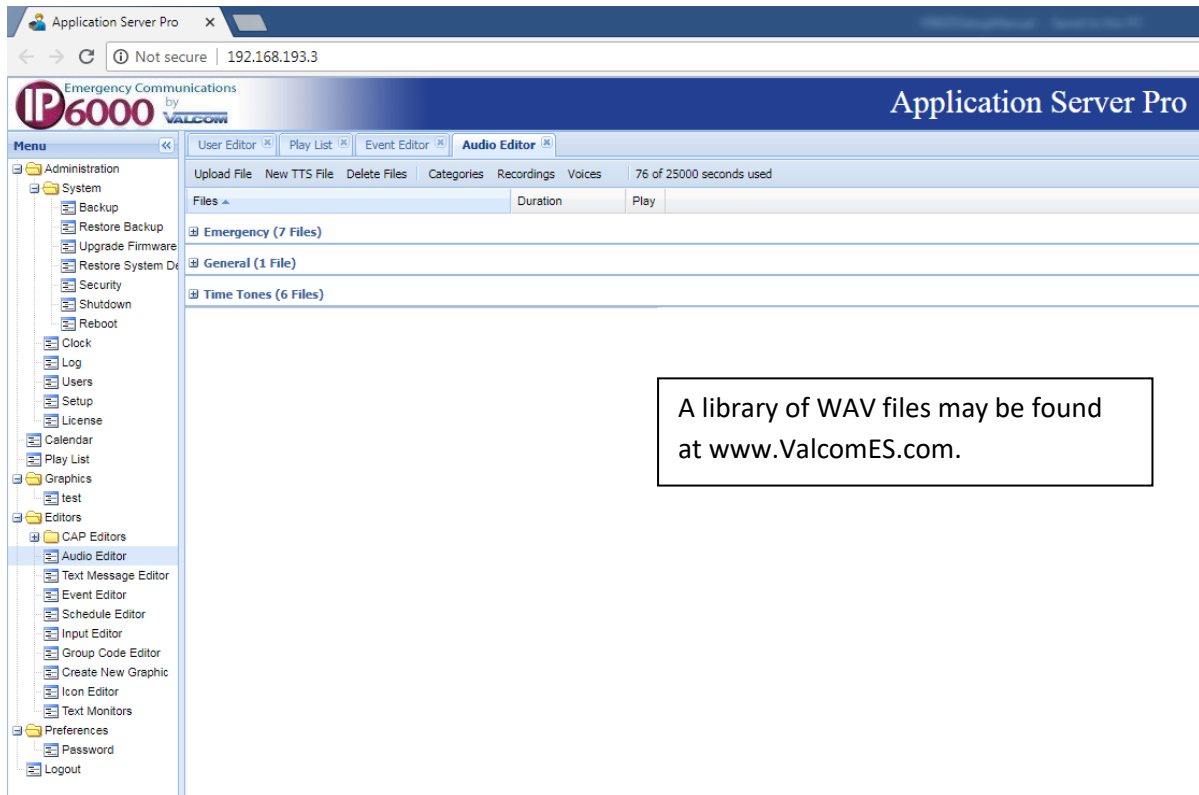
Registration Key: (send to Valcom)

License Key: (get from Valcom)

Currently, Application Servers are shipped from the factory with a license preinstalled for your application.

Editors

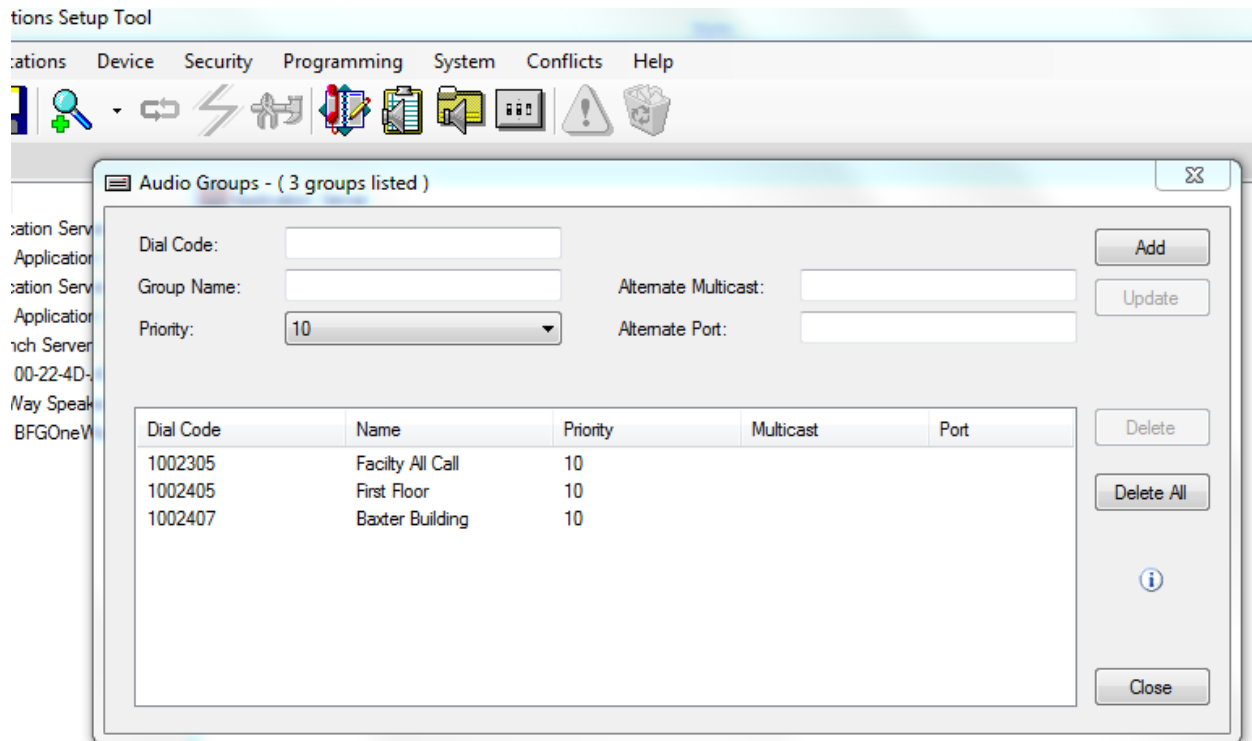
Editors/Audio Editor



The audio editor allows users to:

- a) Upload, categorize and process up to 20MB WAV files. Processing is an option that modifies uploaded files for higher sound quality.
- b) Create and categorize audio files from text (new TTS File)
- c) Delete existing audio files
- d) Manage audio file categories
- e) Record new audio files (refer to Editors/Audio Editor/Recordings)
- f) Manage text-to-speech voice options

The Application Server can create WAV audio files of any announcement sent to a group. The groups are created in the VIP-102B IP Solutions Setup Tool.



The groups may have membership (IP speakers or gateway channel assigned) or may be empty. To record the audio, the Application Server is programmed to “listen” for the group and, if the priority level of the group audio is higher than or equal to a defined priority mask, record the audio content and save it as a WAV file.

WAV files may be archived or overwritten with each new group announcement.

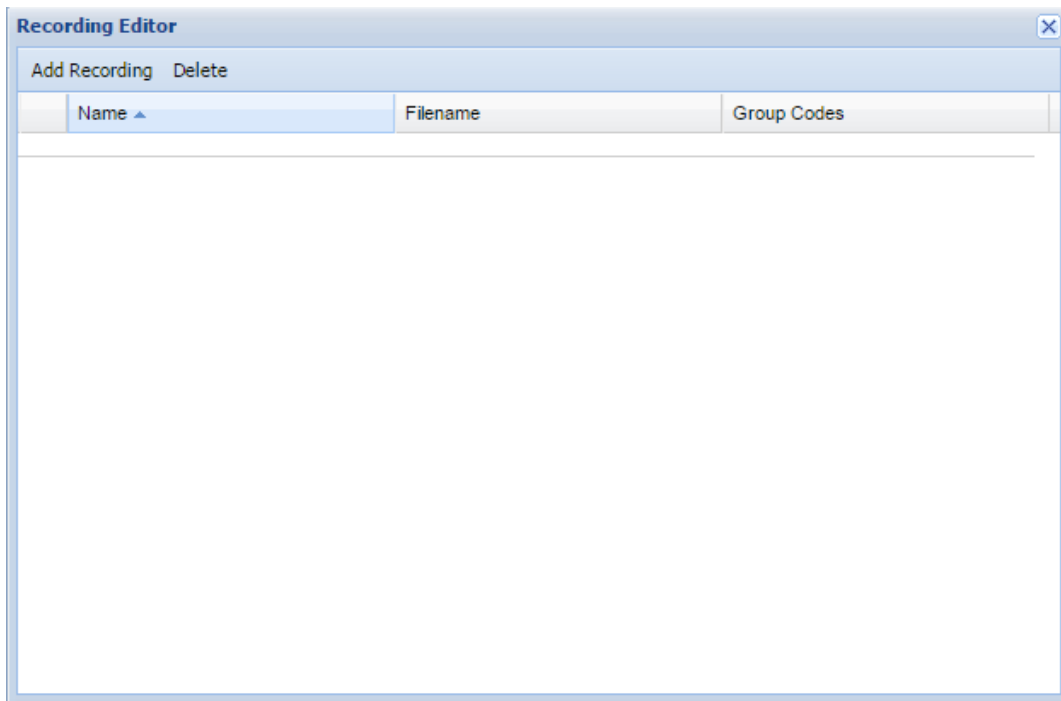
WAV files may be automatically broadcast after recording for call stacking, feedback elimination or as part of a Play List so that the announcement can automatically trigger other events.

If the group being recorded has membership, the members will receive the announcement while it is being recorded.

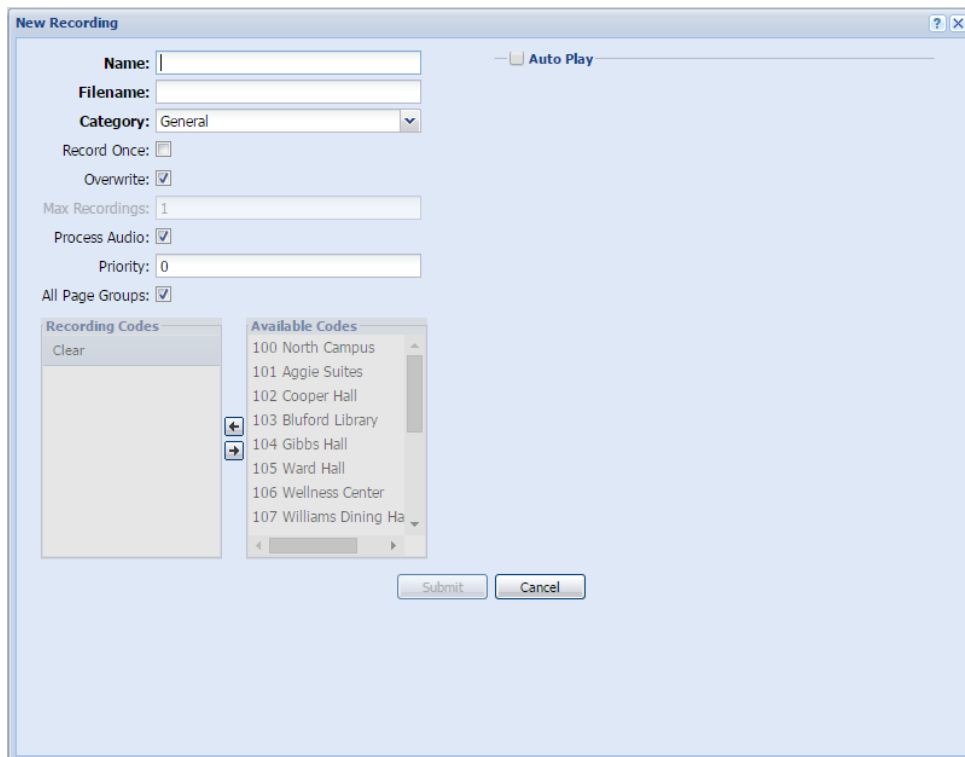
This feature can be used to create custom WAV files that may be played on a schedule or manually controlled (refer to the “**Manually Controlling Application Server Audio Broadcasts**” section of this manual).

It can also be used to record and store copies of high priority announcements such as Code Blue announcements.

Editors/Audio Editor/Recordings



Click Add Recording



Explanation of “Add Recording” Fields [Watch it here.](#)

Name:

This is the name of the recording event.

Filename:

The name of the file generated from the recording. There are 2 naming conventions for Recordings. Record Once and Overwrite use the filename for naming the audio file while Max Recordings uses the filename-page group-date-time for naming the generated file.

Category:

Recordings are saved under the selected Category in the Audio Editor.

Record Once:

If Record Once is checked then the Recording will be used once and then the event will delete itself. The resulting audio file will remain on the server.

Overwrite:

If Overwrite is checked then the Recording will create one audio file. That audio file will be overwritten with each recorded page.

Max Recordings:

Both Overwrite and Record Once must be unchecked. Max Recordings should be set between 1 and 9999. Max Recordings will create an audio file up to the number of Max Recordings selected. Once that number has been reached the oldest existing Max Recording Audio File will be replaced.

Process Audio:

Process the Audio for the Recording for higher sound quality. This setting can only be used with Record Once or Overwrite.

Priority:

This sets a priority for recorded audio announcements. Announcements made that equal or exceed the set priority will be recorded.

All Page Groups:

Any Page made to a known Page group that equal or exceed the set priority will be recorded if box is checked. If box is not checked only selected page groups will be recorded.

If All Page Groups is not checked, then users may select which group code to record. All groups are created in the VIP-102B IP Solutions Setup Tool.

Audio sent to groups allocated as “Recording Codes” will both record a WAV file under the selected category *and* broadcast to channels included in the group’s membership. If the real time live broadcast is not desired, then the groups allocated as recording codes may be empty.

Click Auto Play

New Recording

Name: Announcement 1
Filename: Announcement 1
Category: General

Record Once:
Overwrite:
Max Recordings: 1
Process Audio:
Priority: 0
All Page Groups:

Recording Codes
Clear
300 Record Page

Available Codes
107 Williams Dining Ha
108 Emergency Station
200 South Campus
203 music
400 All Call Bells
501 Page Play Group
600 Entire Campus Emk
700 North Campus

Auto Play

Record Play List: None
Number of plays: 1
Gap (sec):
Repeat Interval: 00:00:00
Total Time: 00:00:00
Priority: 25
Volume Adj.: 0 dB
Cancel Code:
Pre-tone File:

Auto Play Codes
Clear

Available Codes
100 North Campus
101 Aggie Suites
102 Cooper Hall
103 Bluford Library
104 Gibbs Hall
105 Ward Hall
106 Wellness Center
107 Williams Dining Ha
108 Emergency Station

Submit Cancel

Auto Play:

If checked, after a Recording is made it will be automatically played. This option is only usable with Overwrite and Max Recordings.

Record Play List:

This allows the Auto Play of the recording to be done within a Play List thus allowing other events to be “chained” to the recorded audio file for sequential operation (i.e. recorded audio plays followed by a relay activation and an emergency tone).

The steps to create a Record Play List are as follows:

- 1) Create the initial recording (Overwrite checked, Auto Play Unchecked)
- 2) Create an Audio Event and corresponding Play List Item from the recording
- 3) Check Auto Play and choose the Play List Item from the “Record Play List” pull down menu.

The Play List will be invoked to play all new instances of the recorded audio file.

Number of plays:

Select a number between 1 and 59. The number is how many times the recording will be auto played.

Gap (sec):

The Gap between plays of the recording when set to any number of plays greater than 1.

Repeat Interval:

This is how often the auto play will repeat. Set with Hours:Minutes:Seconds. For example, setting 11:45:30 will cause the Auto play to Repeat every 11 hours, 45 minutes and 30 seconds. This option requires a Total Time value to be defined.

Total Time:

This is the total amount of time that the auto play will repeat. Set with Hours:Minutes:Seconds. Setting to 24:00:00 will cause the auto play to run for 24 hours. It will repeat base on the Repeat Interval.

Priority:

This is the priority of the auto play. This setting defaults to 25.

Volume Adj:

The adjusted volume of the auto play broadcast.

Cancel Code:

Select a Cancel Code to Cancel an Auto Play that is currently playing. Dial the Cancel Code to stop the announcement.

Pre-tone File:

Select an audio file to be played before the Recording is Auto played.

Auto Play Codes:

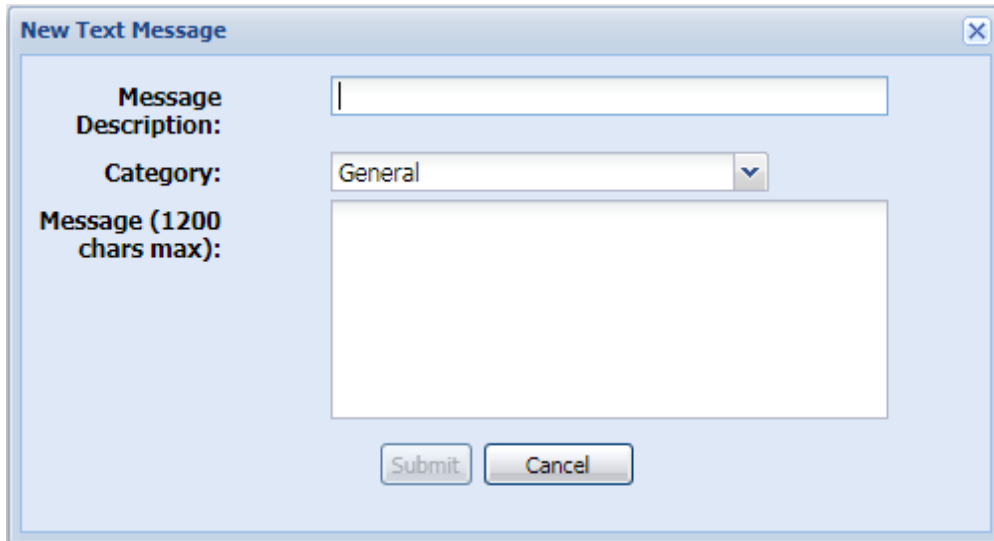
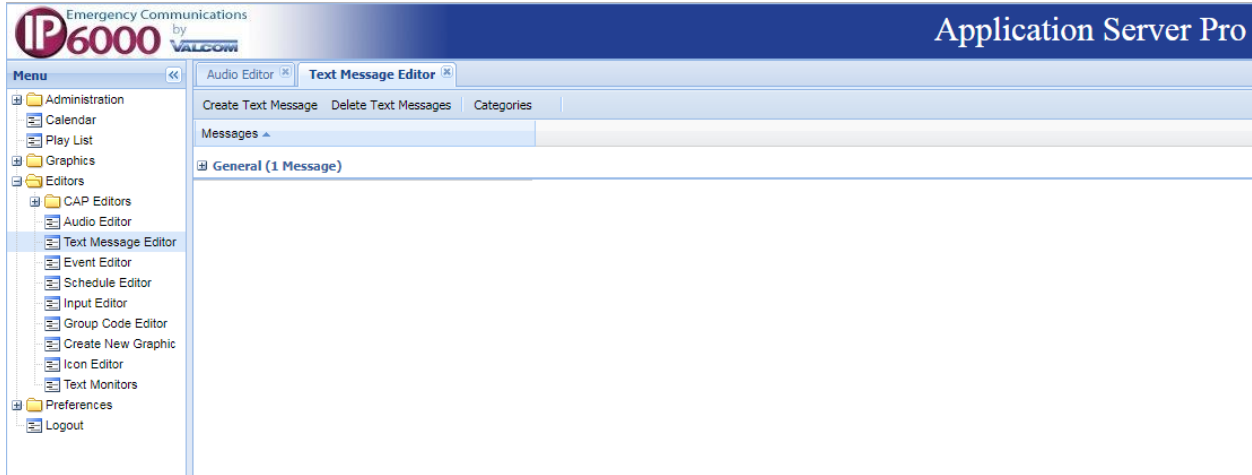
The Recording will be played to the selected group

Stacking Recordings (record and play multiple simultaneous announcements):

To stack recordings to be played the Recording Event must be set to Max Recordings with the number of max recordings exceeding the number of pages expected to be made simultaneously. No other setup is needed.

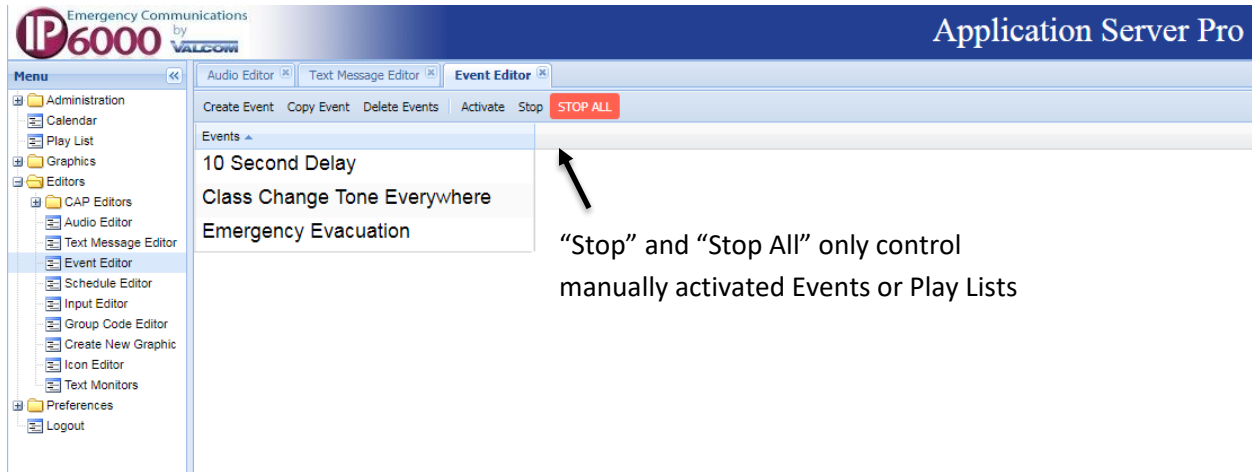
Editors/Text Message Editor

Text message editor allows users to create and categorize text messages for LED signs and screen pop ups.



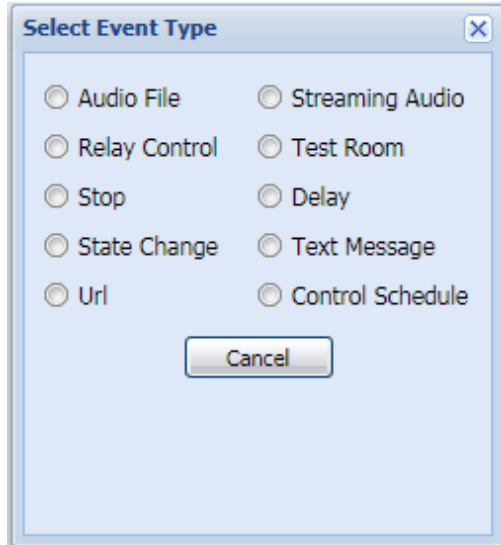
Editors/Event Editor

Event editor allows users to create events. ***Any action invoked by the Application Server is in the form of an “event”.***



“Stop” and “Stop All” only control manually activated Events or Play Lists

Click Create Event:



There are checkbox selections to **automatically create a Play List** from new Events. There is also a **Hide** checkbox to hide Events from non-admin level users (refer to the Users menu).

The following pages describe each possible event type.

Audio File Events

Audio File Events allow users to play audio files to groups. Audio file events are invoked by:

- a) A Schedule
- b) A Play List

If the Text-to-speech check box is checked, the audio file will be created from the selected fields of a CAP message. In this case:

- a) The CAP message was received by the Application Server
- b) The received CAP messages matched the applied CAP filter
- c) The applied CAP filter triggered a Play List item
- d) This Audio File Event was triggered by the Play List Item

If “Send text also” is checked the text of the CAP message will be sent to LED signs and screen pops that are part of the recipient group.

The screenshot shows a 'Create New Audio File Event' dialog box with the following fields and options:

- Event Name: [Text Input]
- Hide:
- Create Playlist:
- Text to Speech:
- Audio File: [Dropdown]
- Voice: paul [Dropdown]
- CAP field: [Dropdown]
- Send text also:
- Duration (sec): [Text Input]
- Number of plays: 1 [Text Input] 0 -> Infinite
- Gap (sec): [Text Input]
- Page Delay (sec): [Text Input]
- Volume Adj.: 0 dB [Dropdown]
- Override from CAP:
- Priority: 25 [Text Input]
- Selected Codes: [List with Clear button]
- Available Codes: 000 Emergency All Call, 600 All Call, 601 Outside
- Submit and Cancel buttons at the bottom.

Otherwise, users may define the audio file to play. In any case, users may define duration for the audio file. If not defined, the audio file will play to completion.

Users may also choose to have the audio file play multiple times and define the gap between plays.

“Page Delay” delays the audio for a defined number of seconds after the event is initiated to allow secondary systems time to prepare.

Users may offset the audio file’s volume and priority. Higher numbered priority audio overrides lower numbered priority audio.

Override from CAP allows the page group and priority to be decided from the received CAP Alert. On the VE6024 eLaunch Scenario, in the Area Desc field, entering the desired group and priority in the format valcom:page_group:priority. For example, entering valcom:687:50 in the Scenario’s Area Desc field would send a priority level 50 page to group 687.

The inactive options become available when Text to Speech is checked. Paul is the default voice; others are available for addition charge. CAP Field defines which CAP field(s) text will be rendered to speech. Send text also automatically generates and invokes a text event to display the text from the selected CAP fields on LED signs or PCs hosting the Desktop Alert TSR.

Selected Codes are user selected destinations (audio groups) for the event. Groups are comprised of VoIP endpoints (speakers, gateways, LED signs, etc.) and are defined in the VIP-102B IP Solutions Setup Tool.

Relay Control Events

Relay control events allow users to control the relay outputs on VE8048A/VE8048AR I/O units.

Users may select a single relay and any relay control groups (defined in the VIP-102B IP Solutions Setup Tool)

Selected relays/control groups may be set to cycle for a finite number of times or turned on steady state.

Priority defines how relays will respond should multiple events be sent to the same relay(s) simultaneously. The event with the higher priority will prevail.

Relays or control groups that have been turned on steady state must be stopped with a stop event.

Create New Relay Control Event

Event Name:

Hide:

Create Playlist:

Dial Code:

Relay #:

Priority:

Relay Action:

On Duration:

Off Duration:

Number of Cycles: 0 -> Infinite

Selected Codes

Clear

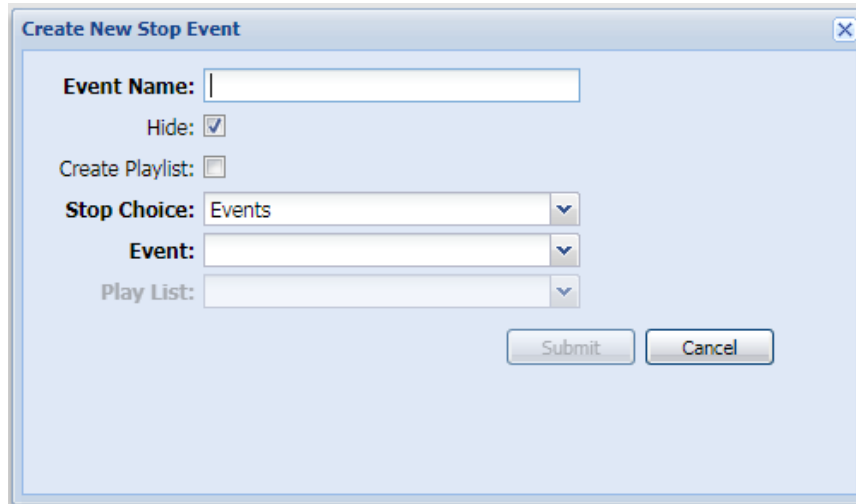
Available Codes

- 500 Control Group 1
- 501 Control Group 2

Submit Cancel

Stop Events

Stop events allow users to stop active relays, streaming audio, test rooms or any active Play List item.

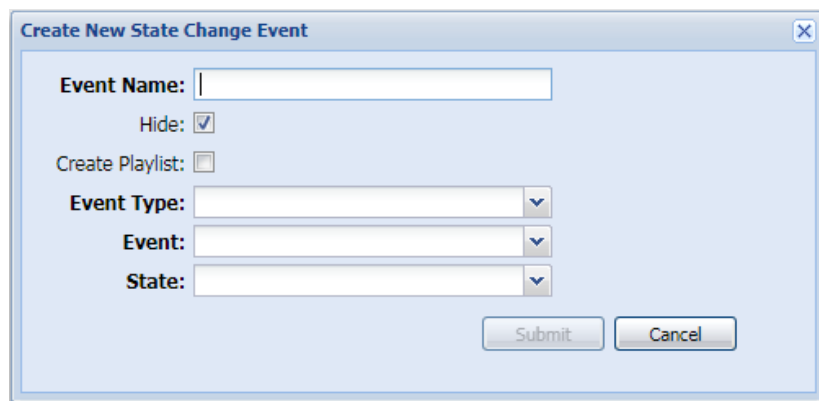


The screenshot shows a dialog box titled "Create New Stop Event". It contains the following fields and controls:

- Event Name:** A text input field.
- Hide:** A checked checkbox.
- Create Playlist:** An unchecked checkbox.
- Stop Choice:** A dropdown menu with "Events" selected.
- Event:** A dropdown menu.
- Play List:** A dropdown menu.
- Submit** and **Cancel** buttons at the bottom right.

State Change Events

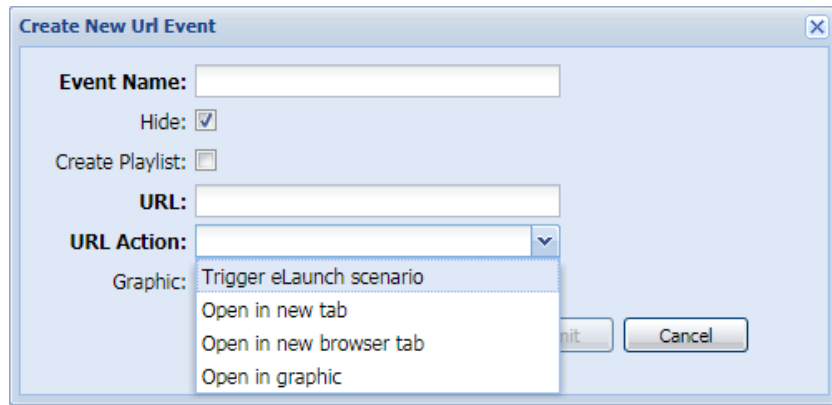
Choosing a **State Change Event** allows users to force VE8048A I/O Unit inputs or audio group recordings to be enabled or disabled. This is useful in situations where users wish to ignore an VE8048A input during certain times of the day and or only wish to record announcements to audio groups at defined times. If a state change event disables an input or recording, a second state change event will be required to reactivate the input or recording.



The screenshot shows a dialog box titled "Create New State Change Event". It contains the following fields and controls:

- Event Name:** A text input field.
- Hide:** A checked checkbox.
- Create Playlist:** An unchecked checkbox.
- Event Type:** A dropdown menu.
- Event:** A dropdown menu.
- State:** A dropdown menu.
- Submit** and **Cancel** buttons at the bottom right.

URL Events



Create New Url Event

Event Name:

Hide:

Create Playlist:

URL:

URL Action:

Graphic:

- Trigger eLaunch scenario
- Open in new tab
- Open in new browser tab
- Open in graphic

URL events launch URLs. This can be used to trigger eLaunch Scenarios, browse to an IP camera, a website, a browser interface of another system or any URL.

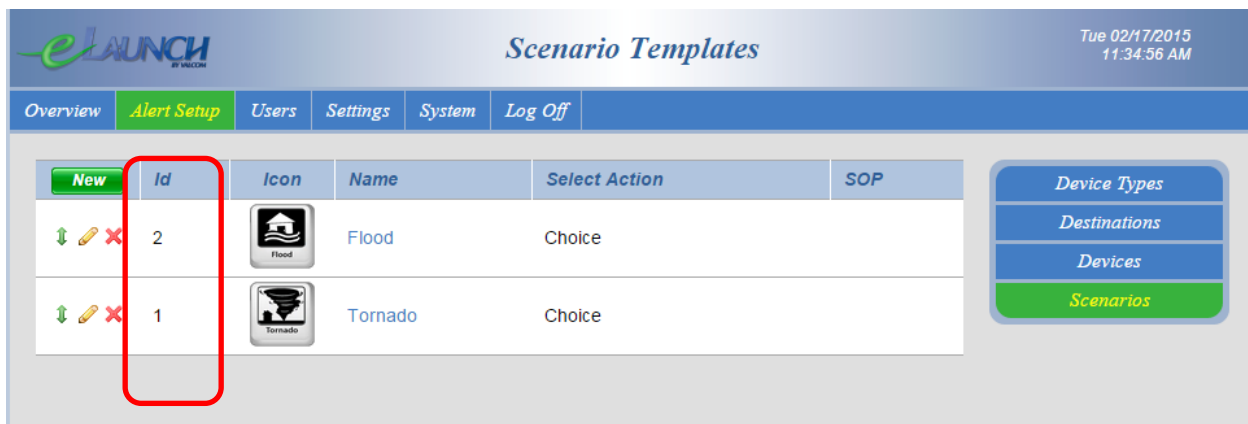
URLs may be opened in a new tab within the Application Server, a new browser tab or in any graphic. In order a the graphic to be available as a selection, a URL window must be “placed” in the graphic via the “place node/place URL window” operation.

Triggering eLaunch Events

Users may define URL events to launch Scenarios in one or more VE6024 eLaunch servers.









Users simply name the event and enter a launch URL. If the eLaunch server’s IP address is 192.168.2.5, and the Scenario with ID number 2 is to be launched, then the launch URL would be http://192.168.2.5/trigger_scenario/2.

Scenario IDs may be found in the VE6024 eLaunch server’s alert set up screen.



eLAUNCH Scenario Templates Tue 02/17/2015 11:34:56 AM

Overview **Alert Setup** Users Settings System Log Off

New	Id	Icon	Name	Select Action	SOP
  	2		Flood	Choice	
  	1		Tornado	Choice	

Device Types
Destinations
Devices
Scenarios

Additionally, the Application Server's IP address must be entered in the Scenario as a trigger IP in the VE6024.

eLAUNCH *Edit Scenario Template* Tue 02/17/2015 11:36:57 AM

Overview **Alert Setup** Users Settings System Log Off

Basic Settings

* Scenario Name: Flood

Select Action: Choice

Trigger IPs:

This scenario will be triggered when a device with the specified ip address visits /trigger_scenario/2. Multiple entries, separated by commas, are allowed.

Device Types
Destinations
Devices
Scenarios

Streaming Audio Events

[Streaming audio](#) allows users to play program material from external audio sources (CD, MP3, Radio) to system audio groups. External audio sources are connected to the system through dedicated audio gateway channels.

Users may name the streaming audio event.

Choose the source audio gateway channel by its assigned dial code.

Choose a priority for this streaming audio event (in the case of multiple audio events being sent to the same group(s) simultaneously).

Choose which group(s) will receive the streaming audio.

Volume Adjust allows users to preset the volume of the streaming audio.

Streaming audio events used in schedules must have corresponding Stop events.

The screenshot shows a dialog box titled "Create New Streaming Audio Event". It contains the following fields and options:

- Event Name:** CD Player
- Hide:**
- Create Playlist:**
- Dial Code:** 311 CD Player (dropdown menu)
- Priority:** 25
- Volume Adj.:** 0 dB (dropdown menu)
- Selected Codes:** 600 All Call
- Available Codes:** 000 Emergency All Call, 601 Outside
- Buttons:** Submit, Cancel

Note: A streaming audio source can only be distributed to one group at a time.

Test Room Events

Test Room events designate a priority “mask” which must be exceeded before server generated audio will play to selected audio channels (selected by their channel dial codes)

Users may name the Test Room event. The selected name may indicate the areas defined in the event (i.e. Testing in all Senior Rooms).

Choose a priority mask.

Choose which audio groups or channel codes will be masked (only events higher than the selected mask will play into the channels that are selected or the channels that are members of the selected audio groups).

Test Room events must have corresponding Stop events.

The screenshot shows a window titled "Create New Test Room Event". It contains the following fields and controls:

- Event Name:** SAT Tests
- Hide:**
- Create Playlist:**
- Priority Mask:** 40
- Selected Codes:** A list box containing "412 Testing Rooms". A "Clear" button is above the list.
- Available Codes:** A list box containing "000 Emergency All Call", "311 CD Player", "312 MP3 Player", "600 All Call", "601 Outside", and "810".
- Navigation arrows (left and right) are positioned between the two list boxes.
- Buttons:** "Submit" and "Cancel" are located at the bottom right of the dialog.

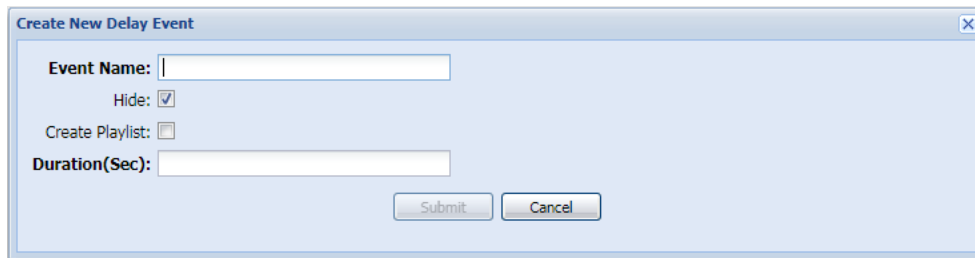
For example, when a Test Room event with a priority Mask of 50 is active in a system that has:

- 1) an All Call Group set to priority 40
- 2) a Scheduled Bell Tone Group set to priority 45
- 3) an Emergency All Call Group set to priority 60

Server generated all call and bell tone audio would be blocked from reaching the channel dial codes or members of groups that have been added to the Selected Codes column (aka Test Room Members). Only audio with a priority of 51 or higher would reach the Test Room Members.

Delay Events

Choosing a **Delay** event allows users to define delays that may be used in between chained events in schedules or in Play Lists. If the desired delay is the same between all chained events, then Event Interval is a better option. Event Interval appears wherever events may be chained.



The screenshot shows a dialog box titled "Create New Delay Event" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Event Name:** A text input field.
- Hide:** A checked checkbox.
- Create Playlist:** An unchecked checkbox.
- Duration(Sec):** A text input field.
- Submit** and **Cancel** buttons at the bottom right.

Text Message Events

Users may define text message events for distribution to LED signs and PC screen pop ups. This is also useful if users wish to send a CAP alert to LED signs and PC screen pops exclusively (no text-to-speech)

If “From CAP Alert” is checked, users choose fields from the triggering CAP alert to display.

Changing the sign Layout requires users to press Submit and then edit the event in order to view the additional fields.

Despite the appearance of other modes, LED signs currently support Red and Green lettering and scroll or hold display modes.

Create New Text Message Event

Event Name: Tornado Take Shelter

Hide:

Create Playlist:

Layout: 1 line

Priority: 90 (use -1 to set idle message)

Display time: 360 (seconds)

Display count: 1

Include icon:

Icon: [Dropdown]

Selected Codes

Clear

000 Emergency All Call

Available Codes

412 Testing Rooms
600 All Call
601 Outside

Whole sign

From CAP Alert:

Message: Tornado Tak Shelter

CAP field: headline

Font size: 15/16 Row

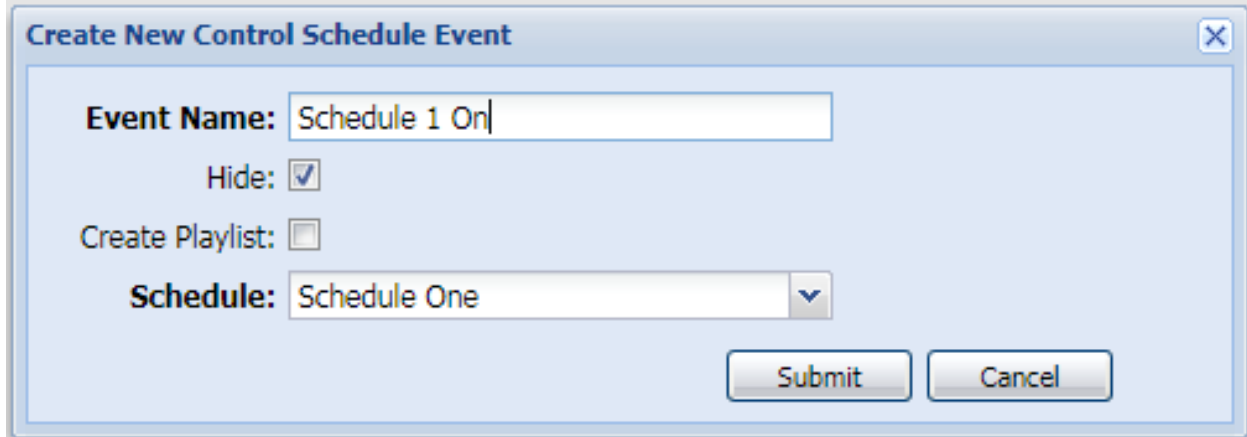
Color: Red

Display mode: Scroll

Submit Cancel

Control Schedule Events

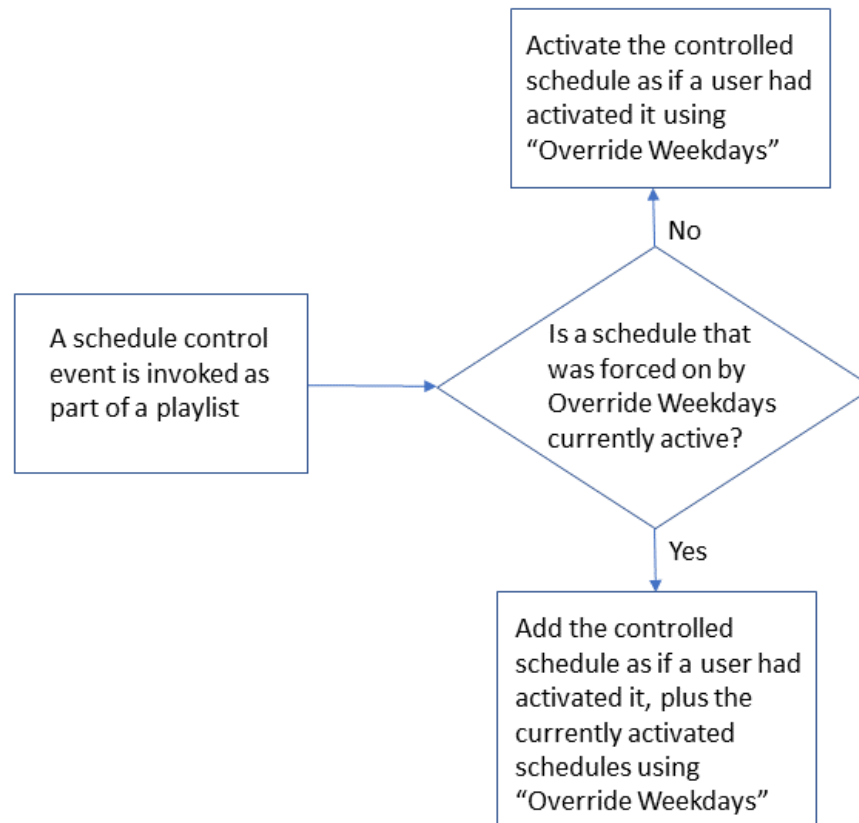
Users may create Events to manually turn schedules on. Corresponding Stop Events must be created to manually turn the schedules back off,

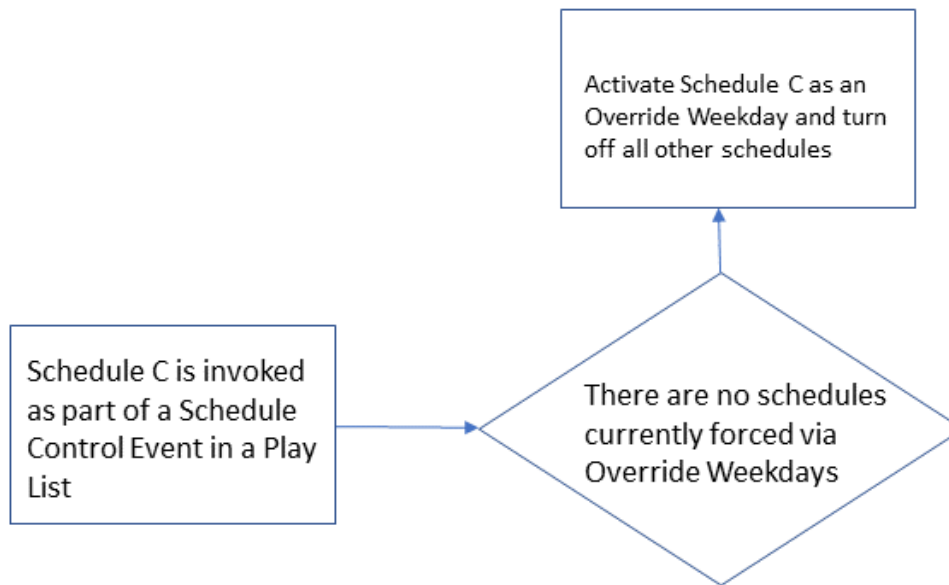


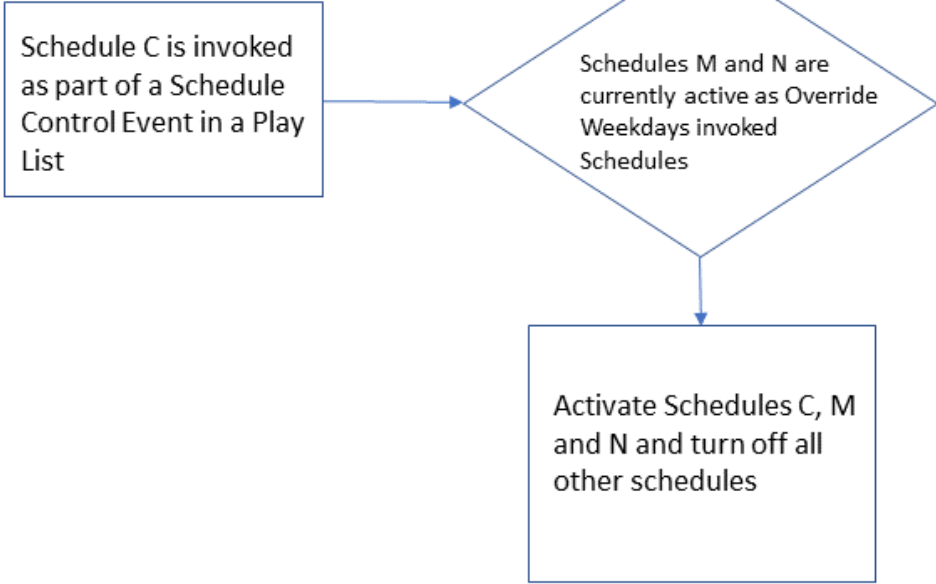
The image shows a dialog box titled "Create New Control Schedule Event" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

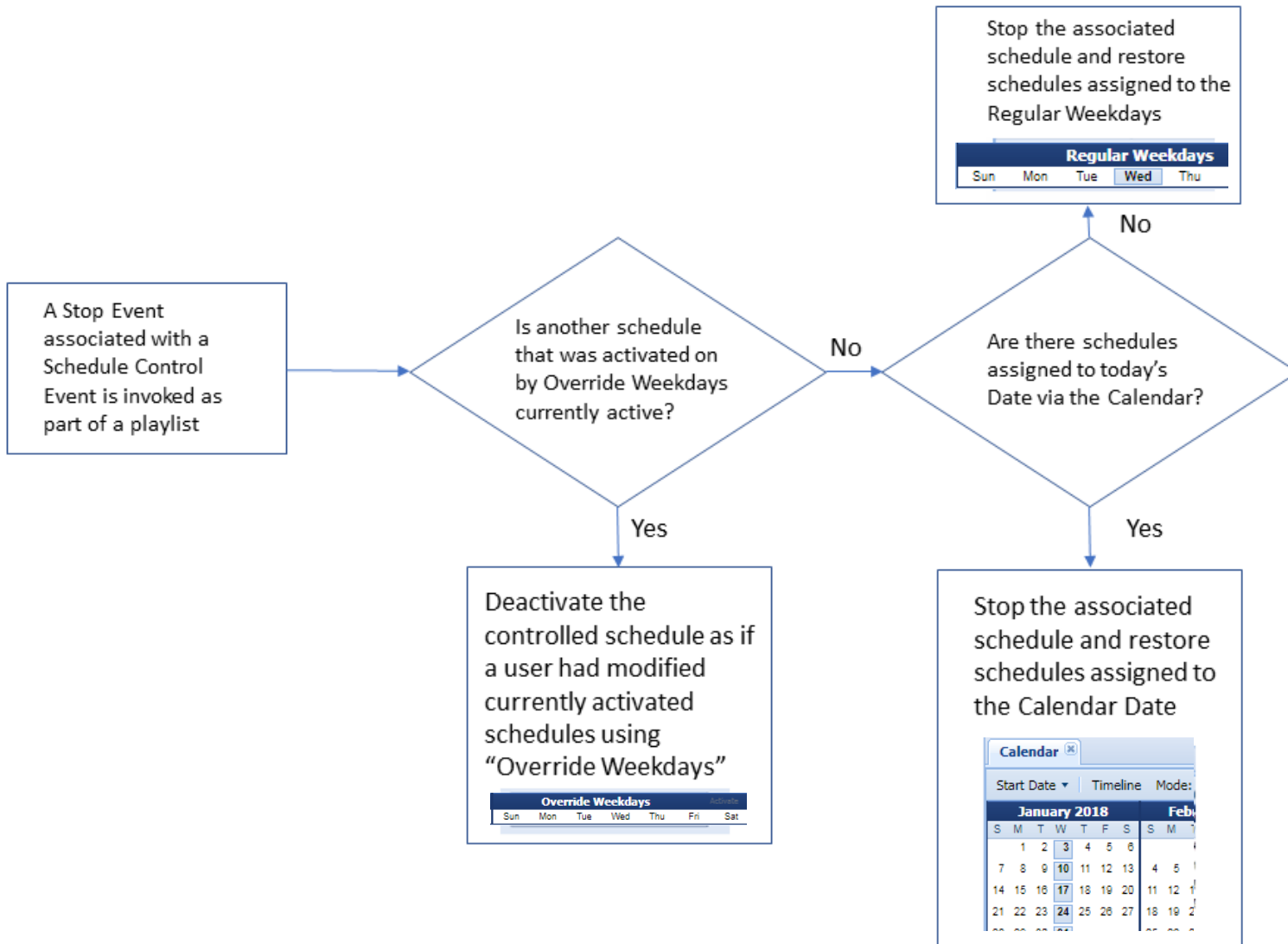
- Event Name:** A text input field containing "Schedule 1 On|".
- Hide:** A checked checkbox.
- Create Playlist:** An unchecked checkbox.
- Schedule:** A dropdown menu showing "Schedule One" with a downward arrow.
- Submit** and **Cancel** buttons at the bottom right.

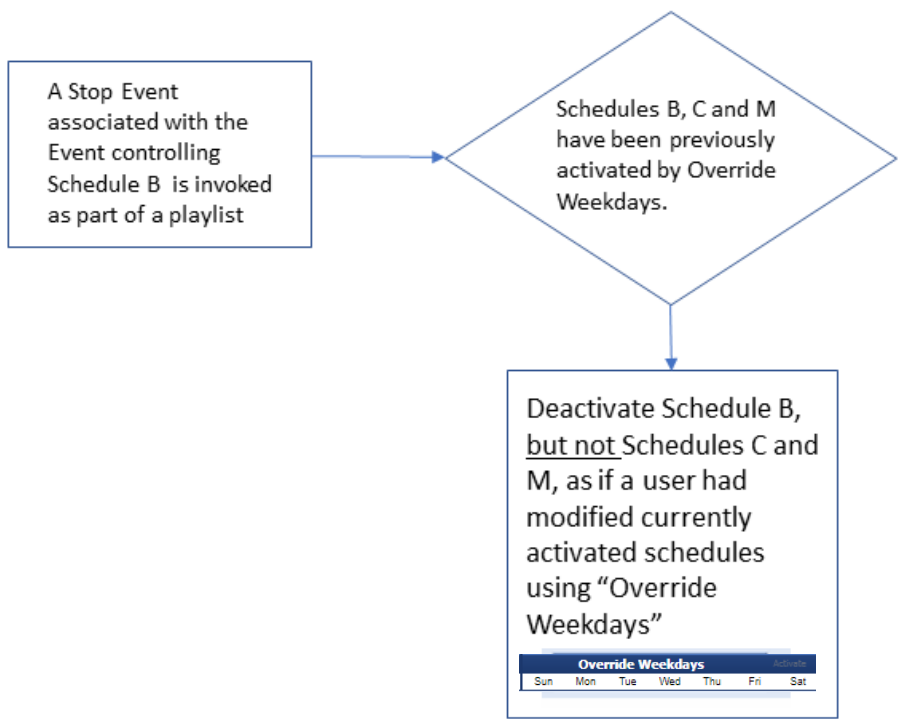
Refer to the following flowcharts for the schedule control event algorithm.



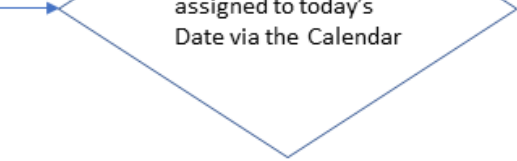






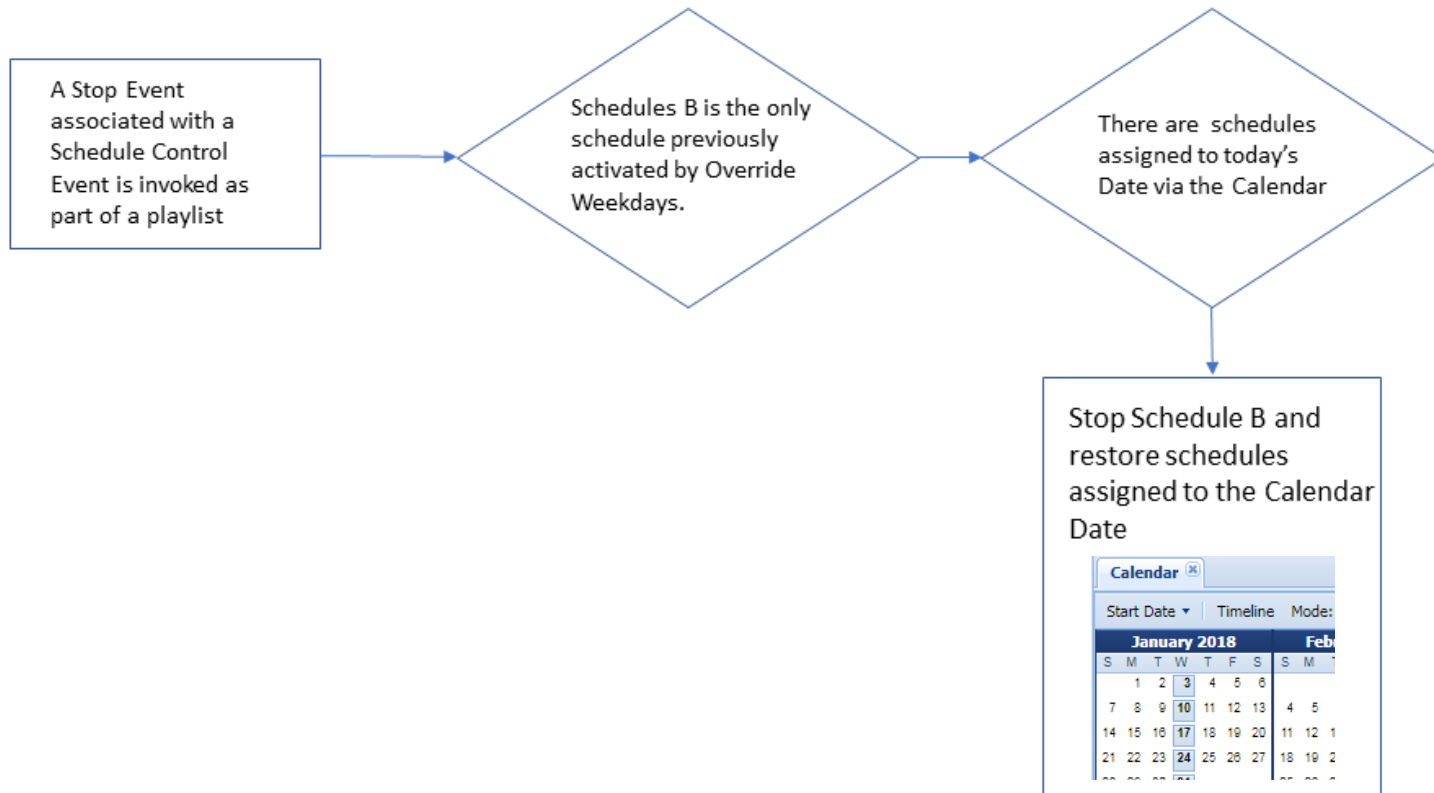


A Stop Event associated with a Schedule Control Event is invoked as part of a playlist



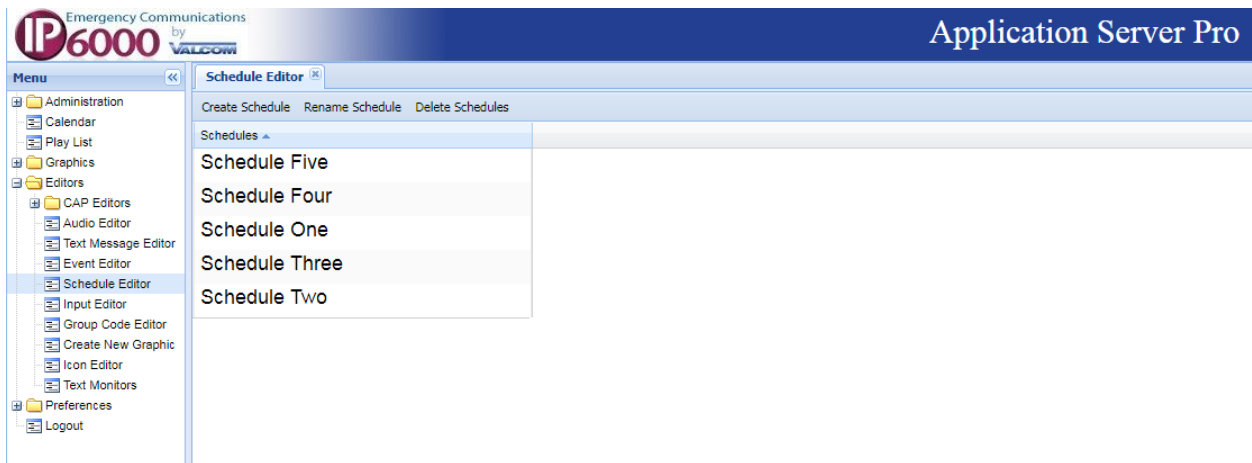
Stop Schedule B and restore schedules assigned to the Regular Weekdays

The screenshot shows a software interface with a table of schedules. The first row is highlighted. The table has columns for 'Schedule Name', 'Status', and 'Action'. The 'Action' column contains a button labeled 'Stop'. Below the table, there are several buttons: 'Stop Schedule B', 'Restore Schedules', and 'Apply'. The 'Stop Schedule B' button is highlighted.

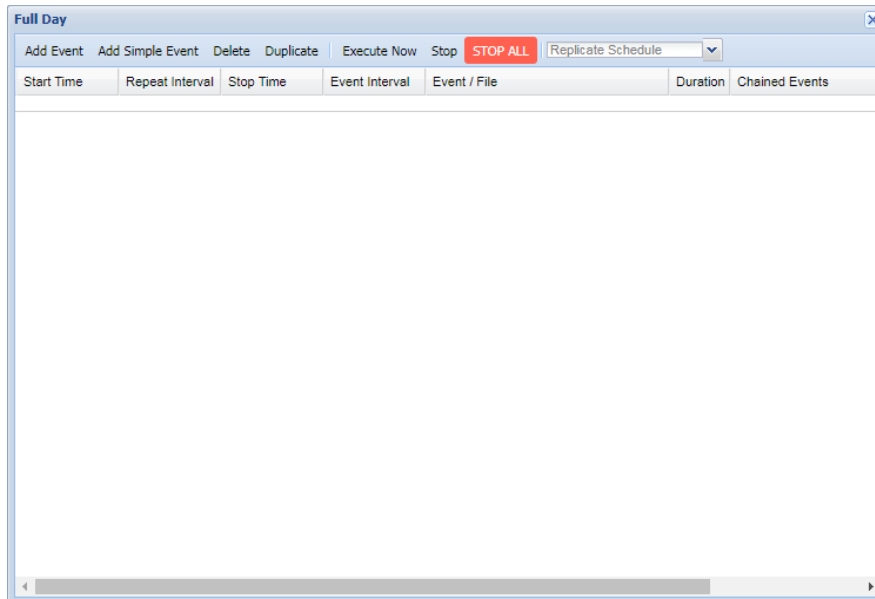
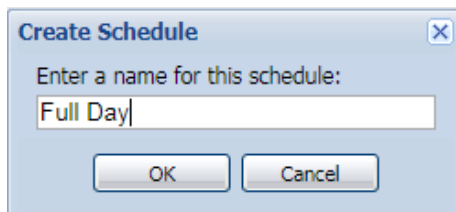


Editors/Schedule Editor

[Schedules](#) may be used to automatically control the execution of events. Schedules may be automatically controlled by the Calendar.



To create and name a schedule, users click create schedule.



Schedules may either be comprised of events created using the event editor or of simple events. If choosing events created by the event editor:

- a) Choose the primary event in the top event pulldown menu
- b) Choose the time that the event should occur in 24-hour format
- c) Choose a repeat interval and stop time (if applicable)
- d) Choose subsequent "chained events"

If chained events are selected, users have the option of defining an event interval to pace the execution of those events.

The screenshot shows a 'New Schedule Event' dialog box. At the top, there is a title bar with the text 'New Schedule Event' and a close button. Below the title bar, there is a dropdown menu labeled 'Event:'. Underneath, there are four rows of time selection controls, each consisting of three spinners for hours, minutes, and seconds. The rows are labeled 'Start Time:', 'Repeat Interval:', 'Stop Time:', and 'Event Interval:'. Below these controls are two panels. The left panel is titled 'Chained Events' and contains a 'Clear' button and an empty list. The right panel is titled 'Available Events' and contains a 'Create Event' button and a list of four events: '9th Grade Tardy Bell', 'Bell Tone Everywhere', 'LED Sign Class Change mE', and 'Unlock Doors Relay'. At the bottom of the dialog are two buttons: 'Submit' and 'Cancel'.

Repeat interval will cause the primary event and all chained events to repeat until the stop time. Timing for the repeat interval starts when the primary event starts (a 10 second event with a 15 second repeat interval will repeat every 5 seconds). If the repeat interval is less than the time for all events to complete, then the event or series of event and chained events will continuously loop until the stop time. Event sequences initiated before the stop time will complete past the stop time if necessary.

Event Interval is the period of time between the execution of the primary event and each chained event. Repeat Interval and Stop Time must be used together and should only be used with audio events that invoke fixed duration WAV files.

Simple event allows users to add “one off” events a schedule. Event editor should be used to create recurring events.

Users simply choose the time when they want the audio event to occur, the desired audio file and duration to play, the event priority, volume offset and the groups(s) to receive the audio file.

New Schedule Event

Start Time: 00 : 00 : 00

Audio File: [dropdown]

Duration (sec): [text]

Priority: 25

Volume Adj.: 0 dB

Selected Codes

Clear

Available Codes

000 Emergency All Call
412 Testing Rooms
600 All Call
601 Outside

[Submit] [Cancel]

Additional schedule creation functions allow users to click an event and make an exact copy by clicking duplicate or to replicate a previously defined schedule. This allows users copy and edit to facilitate making similar schedules.

Full Day

Add Event Add Simple Event Delete Duplicate Execute Now Stop STOP ALL Replicate Schedule

Start Time	Repeat Interval	Stop Time	Event Interval	Event / File	Duration	Chained Events
08:30:00				Bell Tone Everywhere	0	
00:00:00				Bell Tone Everywhere	0	

Play List

Play List/Create Play List

Create Play List allow users to choose a primary and chained events to invoke.

Users must name the Play List item and, using the Event pulldown menu, choose a primary event to control.

Optionally, users may choose a repeat interval and total time to repeat the primary and all of the chained events.

Event Interval is the period of time between the execution of the primary event and each chained event.

Chained events play sequentially. Refer to Parallel Play Lists for simultaneous event activation.

Create New Play List

Name:

Event:

Hide:

Repeat Interval: : :

Total Time: : :

Event Interval: : :

Chained Events

Clear

Available Events

Create Event

- 9th Grade Tardy Bell
- Bell Tone Everywhere
- LED Sign Class Change mE
- Unlock Doors Relay

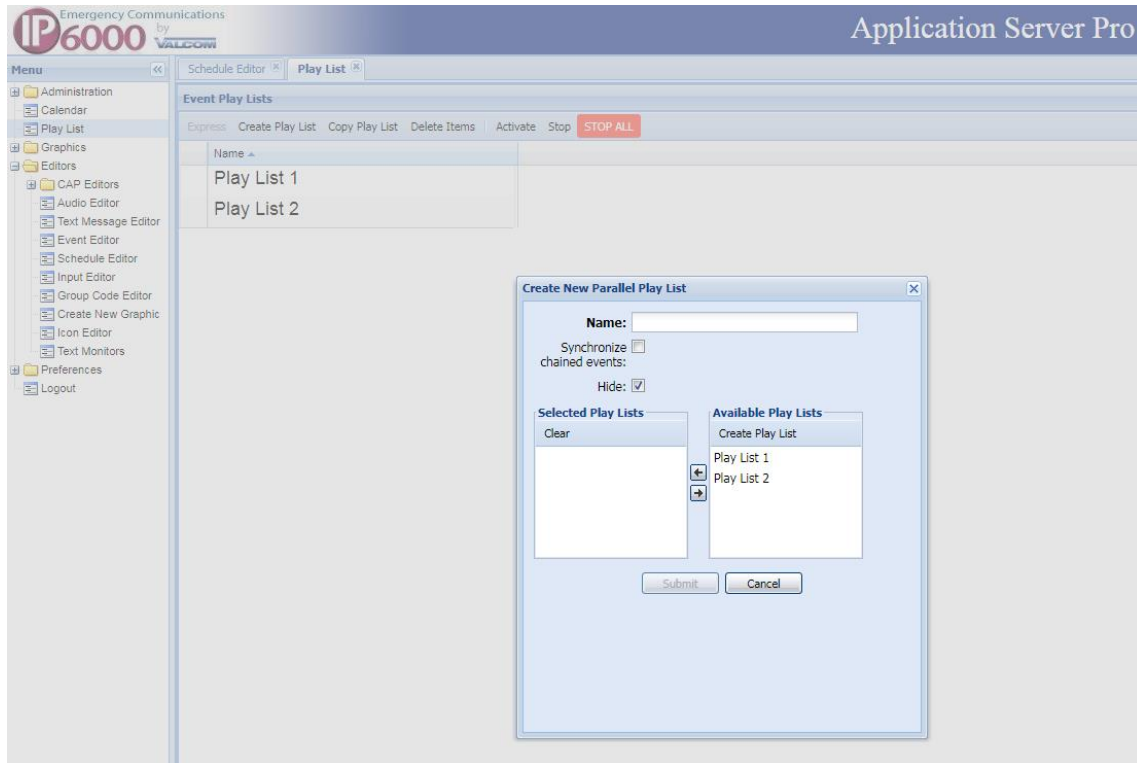
Submit Cancel

Repeat Interval and Total Time should only be used with audio events that invoke fixed duration WAV files.

Play List/Parallel Play Lists

Parallel Play Lists are simply Play Lists comprised of other Play Lists. The advantage of parallel Play Lists is simultaneous operation. Parallel Play Lists appear wherever Play Lists appear and are invoked in the same manner as Play Lists.

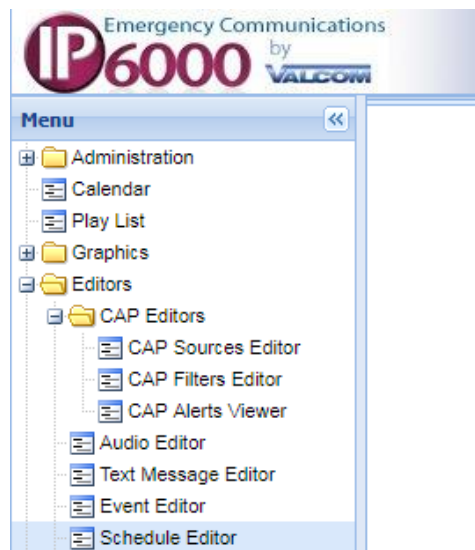
The Synchronize Chained Events checkbox will cause any chained events in the Play Lists to sequentially operate in tandem.



Editors/CAP Editors

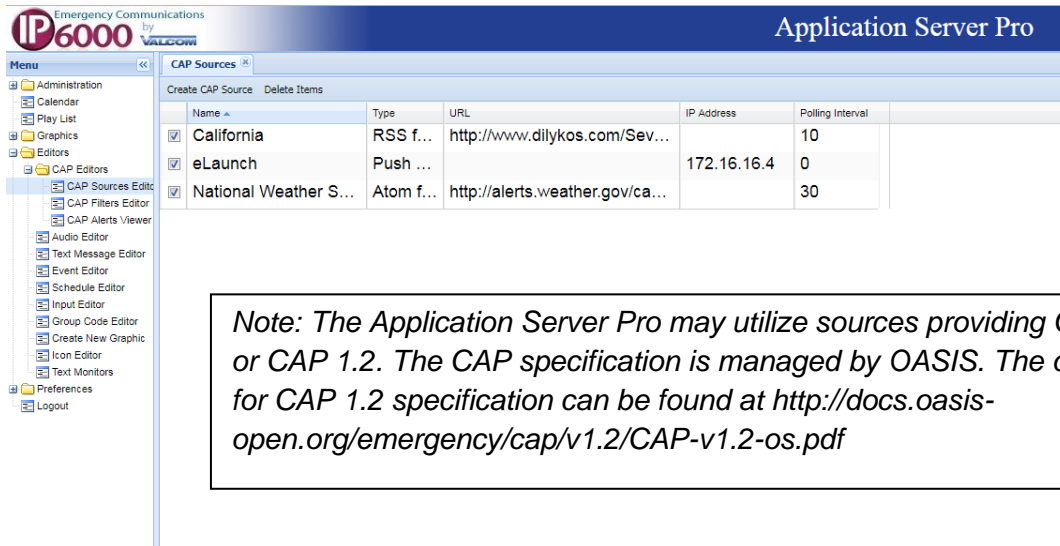
As mentioned previously, the VE6025 can utilize Common Alert Protocol (CAP) XML messages to broadcast audio and text alerts. It can periodically poll RSS/ ATOM feeds or Alert Lists for the same purpose. Once a CAP source is qualified (Editors/CAP Sources Editor), or an RSS/ATOM List feed or Alert List is identified, any messages received from those sources are processed by applying CAP filters. If the content of the received message matches **all** the rules defined in the filter, the filter will invoke a Play List item. The Play List item will, in turn, invoke events. The events are typically used to process the text of the message to audio (text-to-speech) and/or to direct the text directly to groups for display on LED signs or PC screen pop ups.

However, the events are not limited to processing the text from the received message and may be used for a myriad of other functions (See Editors/Event Editor).



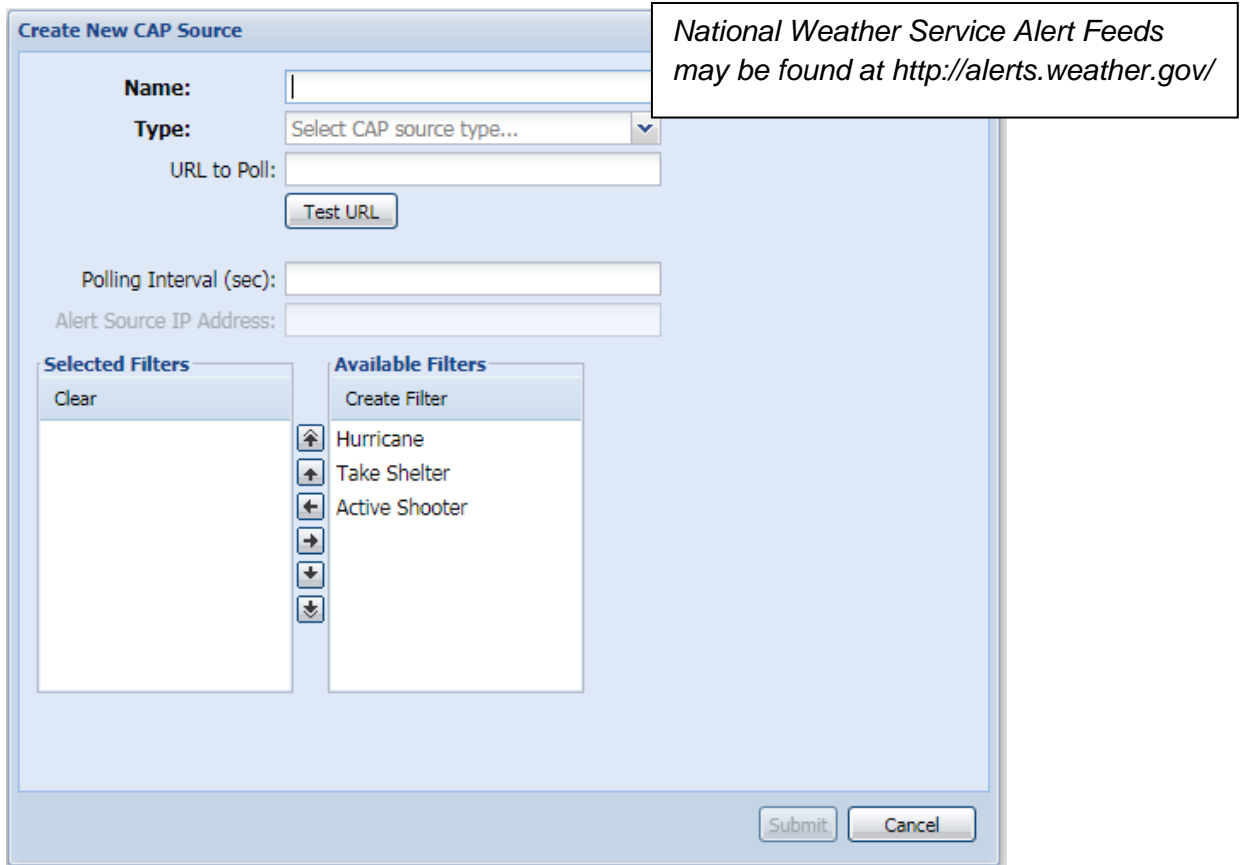
Editors/CAP Sources Editor

Users may qualify external sources of emergency messages by clicking Create CAP Source.



Name	Type	URL	IP Address	Polling Interval
<input checked="" type="checkbox"/> California	RSS f...	http://www.dilykos.com/Sev...		10
<input checked="" type="checkbox"/> eLaunch	Push ...		172.16.16.4	0
<input checked="" type="checkbox"/> National Weather S...	Atom f...	http://alerts.weather.gov/ca...		30

Note: The Application Server Pro may utilize sources providing CAP 1.1 or CAP 1.2. The CAP specification is managed by OASIS. The document for CAP 1.2 specification can be found at <http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf>



Create New CAP Source

Name:

Type:

URL to Poll:

Polling Interval (sec):

Alert Source IP Address:

Selected Filters

Clear

Available Filters

Create Filter

- Hurricane
- Take Shelter
- Active Shooter

National Weather Service Alert Feeds may be found at <http://alerts.weather.gov/>

Create New CAP Source

Name:

Type: ▼

URL to Poll:

Polling Interval (sec):

Alert Source IP Address:

Selected Filters

Clear

Available Filters

Create Filter

↑ Hurricane

↑ Take Shelter

← Active Shooter

→

↓

↓

Submit Cancel

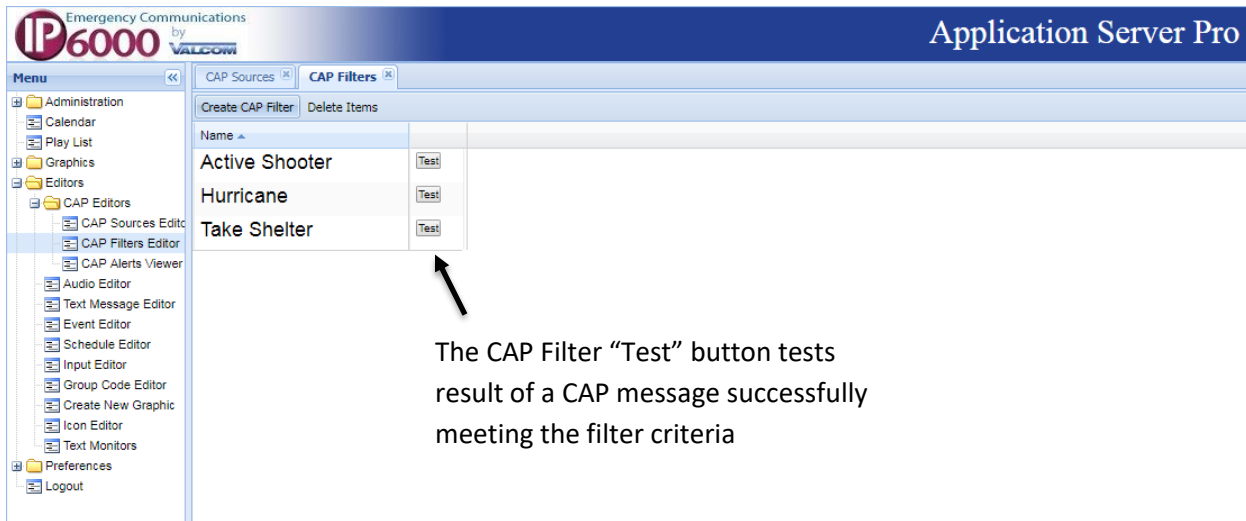
Users name the CAP source, choose the type of CAP source (Atom feed, RSS feed, Alerts List or Push alert)

For push alerts, users enter the Alert Source IP Address. For others, users enter the URL to poll and the polling interval. Some services will block systems that poll too frequently. Typical polling intervals are 60 to 180 seconds.

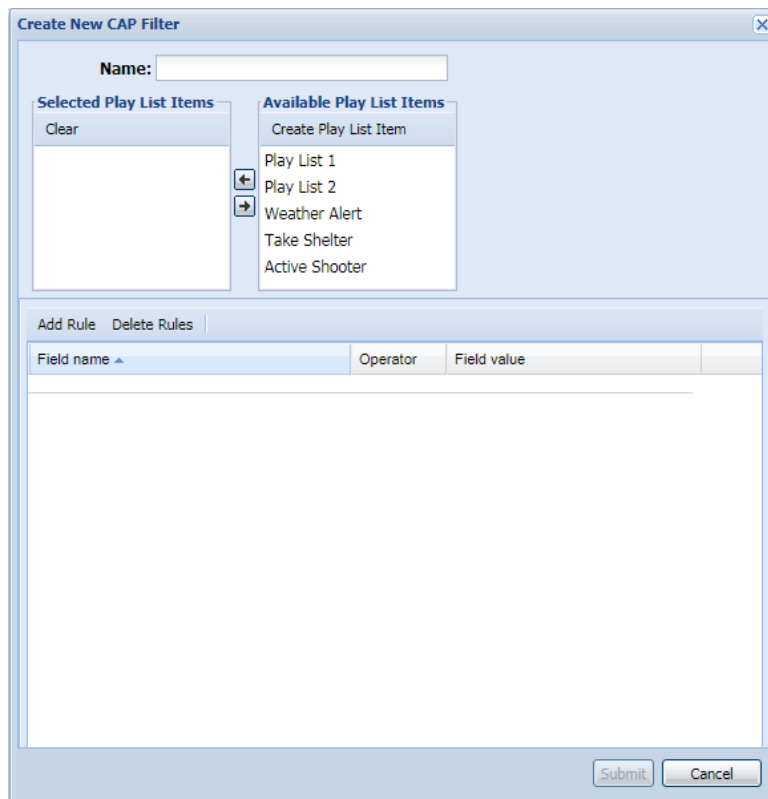
Atom/RSS Feeds and Alert Lists are typically polled at a defined interval. CAP XML sources may also be polled, however, typically push alerts to the Application Server.

Editors/CAP Filters Editor

Filters must be applied to emergency messages in order to activate Play Lists. The filters are comprised of rules which identify text within the fields of the received message and apply operators (Matches, Does not match, Includes, Does not include) to determine a course of action. If the filter rules are not met, then no action takes place. If **all** the filter rules are met, then the filter will activate its associated Play List item(s) simultaneously.



The CAP Filter "Test" button tests result of a CAP message successfully meeting the filter criteria



Field name	Operator	Field value
------------	----------	-------------

Create New CAP Filter Rule

Field name:

Create New CAP Filter Rule

Field name:

Operator:

Field value:

If utilizing the VE6024 eLaunch Server as the message source, field names correlate to information entered in Scenarios as follows:

<u>CAP Filter Field Name</u>	<u>VE6024 Scenario Field</u>
area_desc	Top Levels selected as CAP destinations
event	Event Type
headline	Headline
description	Description
instruction	Instructions
category	Category
response_type	Response Type
urgency	Urgency
severity	Severity
certainty	Certainty

The VE6024 Scenarios may contain headline and description 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)

Note: You can see a feed by pointing your browser to the appropriate address:

eLaunch Latest: <http://your.elaunch.IP/cap/alerts/latest>

eLaunch CAP: <http://your.elaunch.IP/cap/alerts/feed.cap>

eLaunch RSS: <http://your.elaunch.IP/cap/alerts/feed.rss>

eLaunch Atom: <http://your.elaunch.IP/cap/alerts/feed.atom>

Sample Filter

Edit CAP Filter

Name: Bomb Threat

Selected Play List Items

- Clear
- Bomb Threat
- Bomb Threat LED
- Bomb Threat Phones

Available Play List Items

- Create Play List Item
- Fire Message
- Hurricane
- Earthquake
- Hurricane eLaunch

Add Rule Delete Rules

Field name	Operator	Field value
event	matches	bomb threat

Submit Restore Cancel

Sample CAP source with filters applied

Edit CAP Source

Name: eLaunch

Type: Push alert

URL to Poll:

Test URL

Polling Interval (sec): 0

Alert Source IP Address: 172.16.16.14

Selected Filters

- Clear
- Hurricane
- Evacuation
- Bomb Threat
- Gunman
- take shelter
- eLaunch Earthquake
- eLaunch Fire
- Active Shooter

Available Filters

- Create Filter
- Hurricane
- Gunman
- take shelter
- Weather
- eLaunch Earthquake
- Active Shooter
- Evacuation
- eLaunch Fire

Submit Restore Cancel

Each filter that is applied to a CAP source is evaluated sequentially, and if its rules allow, the filter will immediately invoke its associated Play List item(s). If more than one Play List item is associated with a filter, the Play List items will play simultaneously.

Users may find it advantageous to name CAP Filters, the Play List Item they activate, the Event invoked by the Play List as well as the audio/text file broadcast by the event with the same or similar names.

CAP filters applied to CAP sources are evaluated sequentially. Each validated CAP filter will complete its associated Play Lists SIMULTANEOUSLY before subsequent CAP filters are evaluated.

Editors/CAP Alerts Viewer

All accepted CAP Alerts can be viewed in this section. It gives information on the Identifier of the Alert as well as the state of the alert, the time it was sent and the time it expires.

Administration/Calendar

The screenshot displays the Administration/Calendar interface. At the top, there is a 'Start Date' dropdown, a 'Timeline' button, and a 'Mode' selector with 'View' selected and 'Build' unselected. Below this is a 12-month calendar grid for 2018, organized into four rows of three months each. The months shown are January, February, March, April, May, June, July, August, September, October, November, and December. Each month's calendar shows days of the week (S, M, T, W, T, F, S) and dates. Some dates are highlighted with a blue background, indicating they are selected. To the right of the calendar grid are two panels: 'Selected Schedules' and 'Available Schedules'. The 'Selected Schedules' panel contains a 'Clear' button and is currently empty. The 'Available Schedules' panel contains a 'Create Schedule' button and a list of schedule names: Full Day, Schedule Five, Schedule Four, Schedule One, Schedule Three, and Schedule Two. Below the calendar grid, there are two tabs: 'Regular Weekdays' and 'Override Weekdays'. The 'Regular Weekdays' tab is active, showing a row of buttons for Sun, Mon, Tue, Wed, Thu, Fri, and Sat. The 'Override Weekdays' tab is inactive.

The Calendar form is used to define when system schedules will operate.

Individually click on Sun, Mon, Tue, Wed, Thu, Fri or Sat and move the desired default schedules for these days from Available Schedules to Selected Schedules.

Users may also choose to operate select schedules based upon calendar dates. If Classic Calendar Mode is checked under the Setup/Miscellaneous Tab, this is accomplished by creating date groups. This is accomplished as follows:

Choose one or more dates from the Calendar by clicking Build and then clicking the desired dates. Once all dates have been selected, click View and choose one or more schedules to operate on the selected dates. Up to 365 date groups may be defined.

Calendar date groups may be modified as follows:

- a) **Remove a date from an existing date group** - Click Build and then double click the dates within a defined group. Once the date's background color is gone, the date is removed from the group. Click View to exit.
- b) **Add dates to an existing date group** – Click Build and then single clicking a date in any defined group, the background color will turn yellow and additional dates may be added to the date group. Click View to exit.

If Classic Calendar Mode is unchecked under the Setup/Miscellaneous Tab, individual dates may be selected for schedule assignment without building date groups.

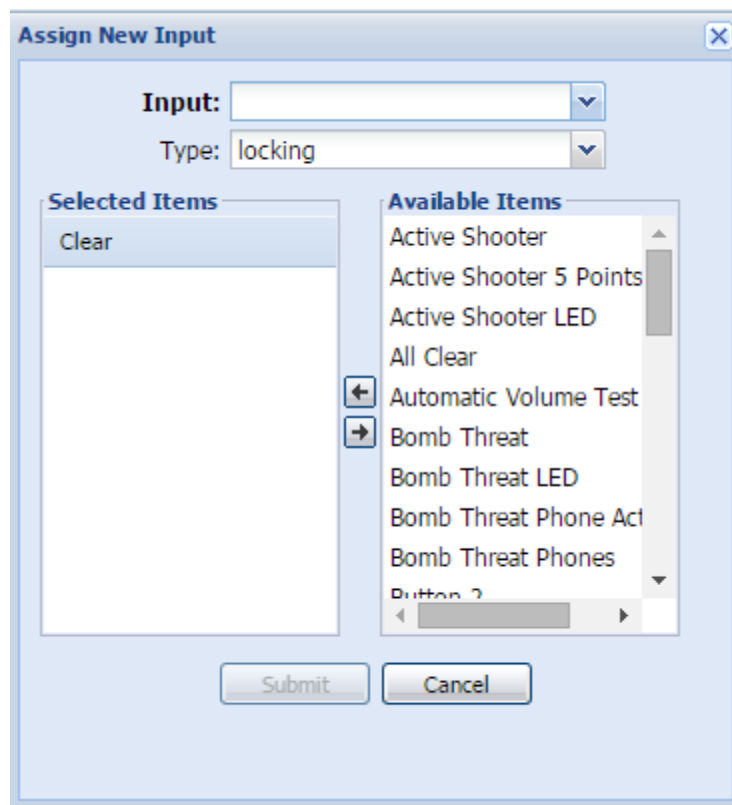
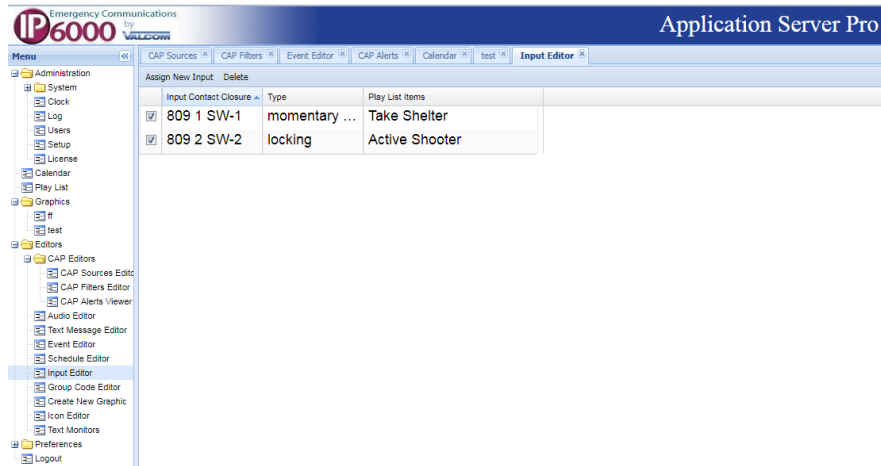
One-time overrides may be enabled up to seven days in advance may be selected using Override Weekdays. Individually click on Override Weekdays Sun, Mon, Tue, Wed, Thu, Fri or Sat and move the desired Override schedules for these days from Available Schedules to Selected Schedules, then click activate. Override Weekdays schedule selections deactivate once complete.

Examples:

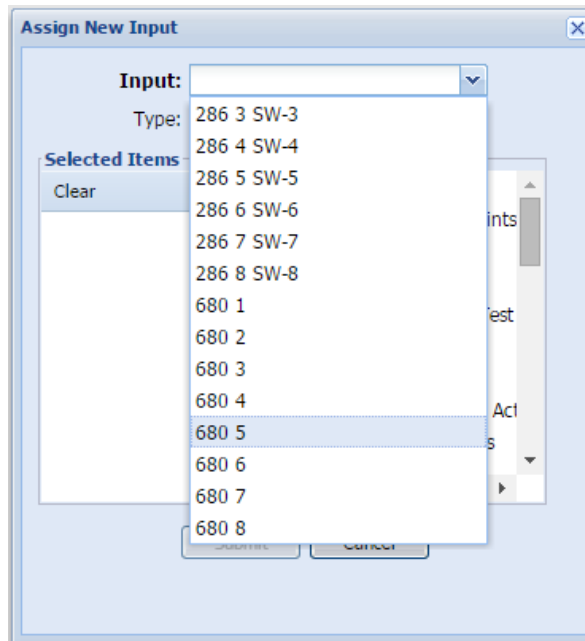
Schedules Assigned to Current Day of the week (Regular Weekdays)	Schedules Assigned to Current Day of the week (Override Weekdays)	Schedules Assigned to Current Date by way of a Calendar Date Group	Which Schedules actually operate?
2 and 3	none	none	2 and 3
2 and 3	none	1	1
2 and 3	4 and 5	1	4 and 5

Editors/Input Editor

The input editor allows users to assign VE8048A inputs (that are programmed to control the server) to activate or deactivate any combination of Play List items.



Users may choose a VE8048A I/O unit switch input:

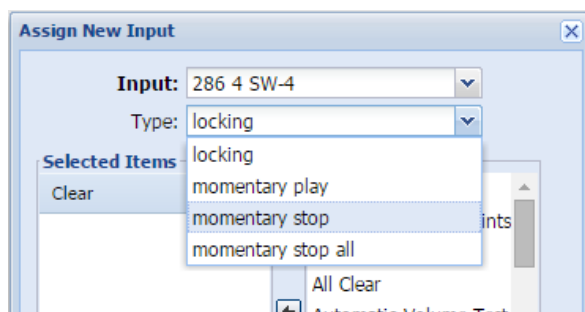


Select the switch type (locking or momentary). Locking switches activate the selected Play List items when the switch is locked on. If those Play List Items are actively distributing an audio file, delay, text message event or relay control “on” event, opening the locked switch will terminate the activity.

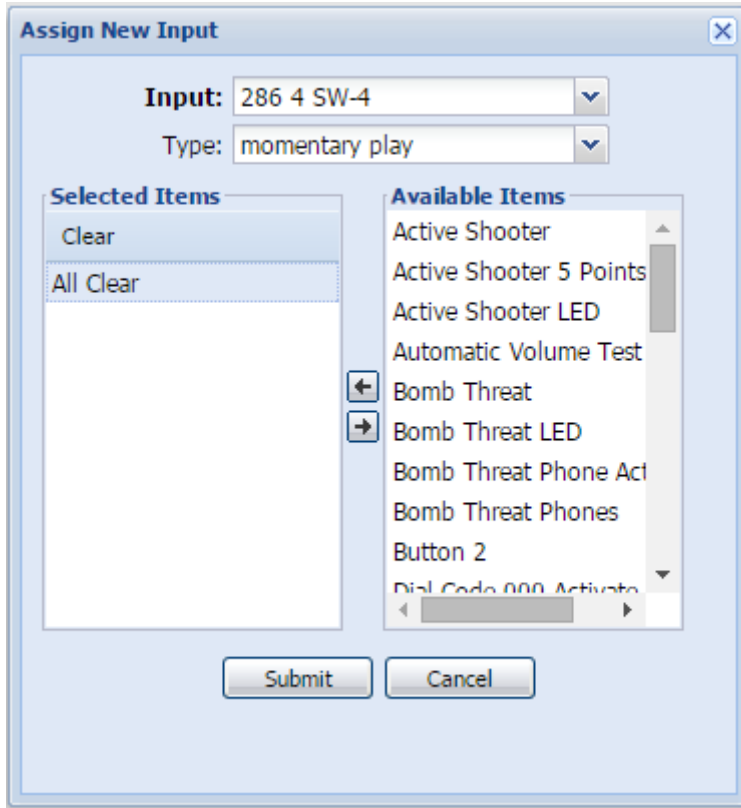
Play List Items controlling streaming audio, state change, stop, eLaunch, schedules or test rooms will not terminate when the locking switch is opened.

Momentary switches will play a play list item for its duration (if applicable) or until a stop command is received.

Momentary Stop All only controls manually activated Playlists and Events.



Once the switch and switch type are selected, choose the Play List item(s) to be controlled from the Available Items list. Multiple play lists, if selected, will operate in tandem much like Parallel Play lists.

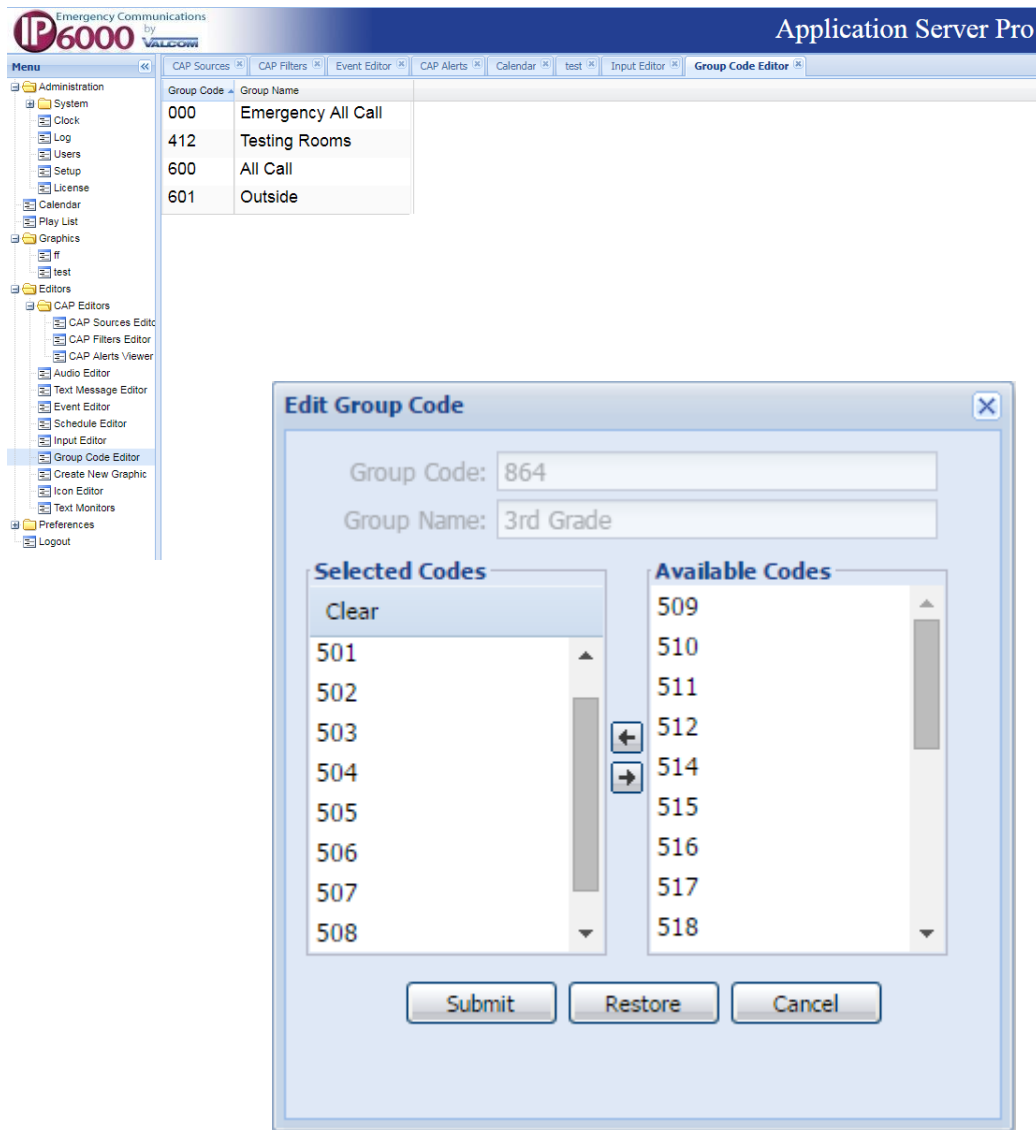


Editors/Group Code Editor

Group Code Editor allows users to modify the audio group membership that was initially defined in the VIP-102B IP Solutions Setup tool. Users may add or remove channels (defined by their dial codes) to or from any group. New groups may only be defined in the VIP-102B.

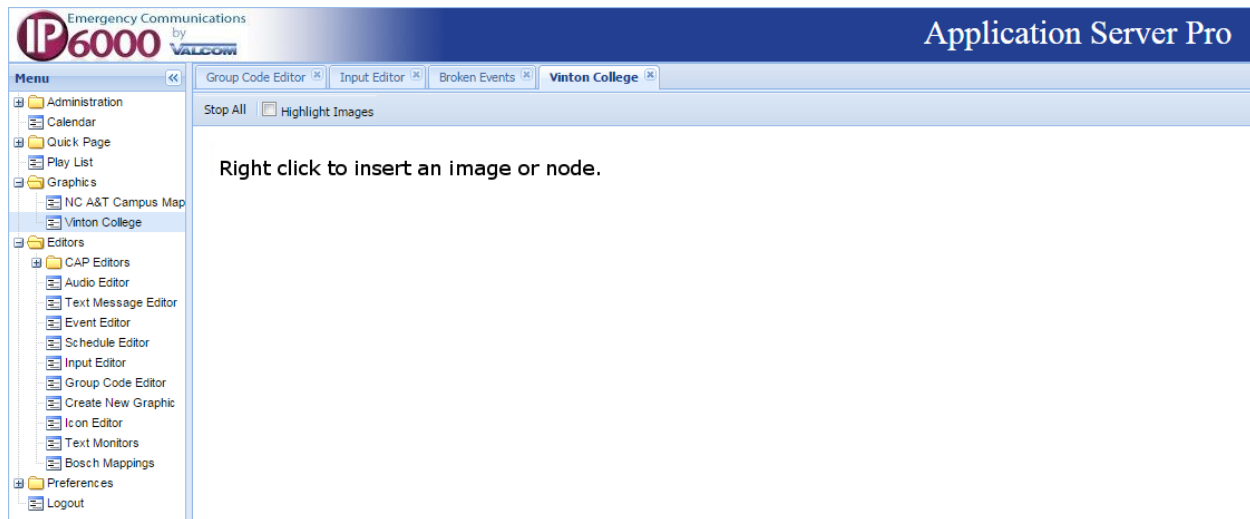
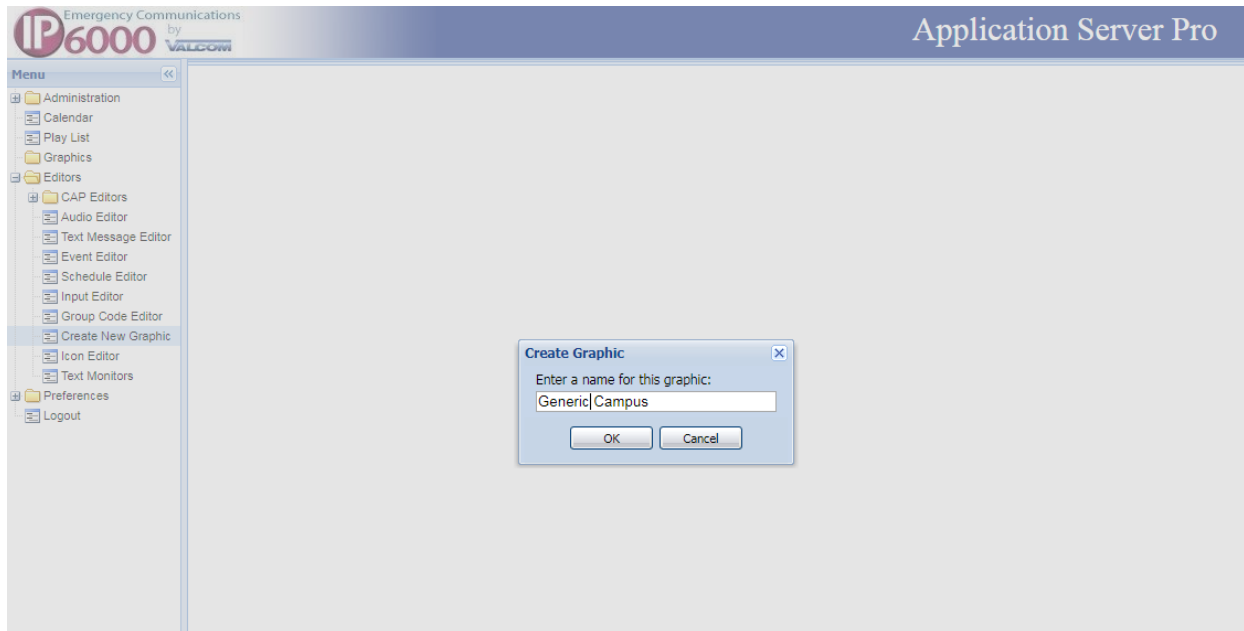
The preferred method of updating group membership is through the VIP-102B.

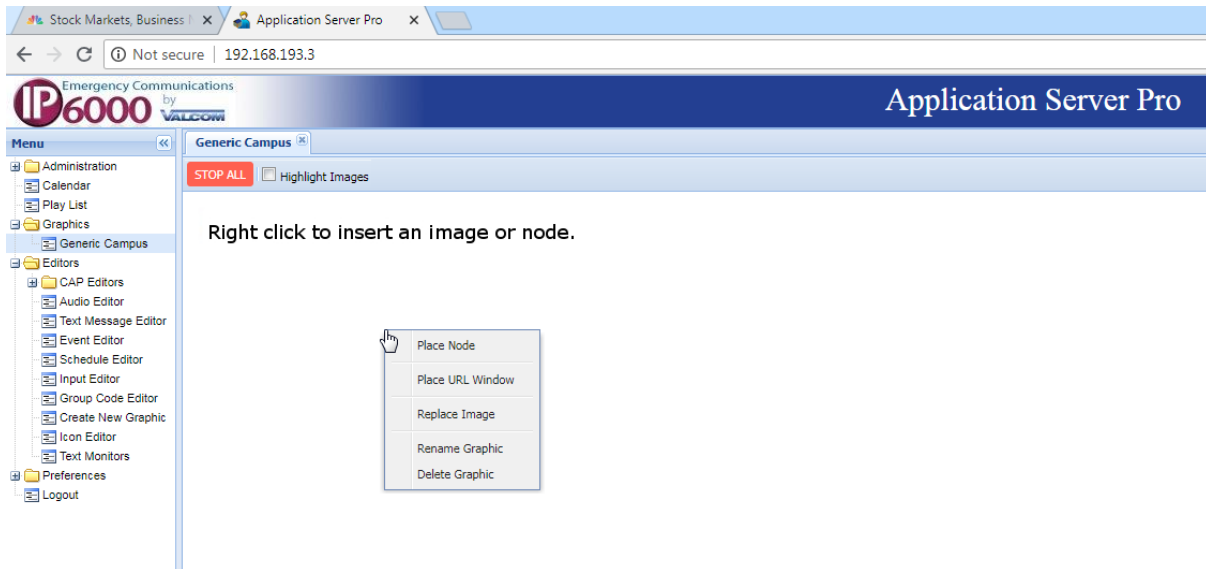
To edit the membership of a group, double click the group and add or remove channel dial codes as desired.



Editors/Create New Graphic

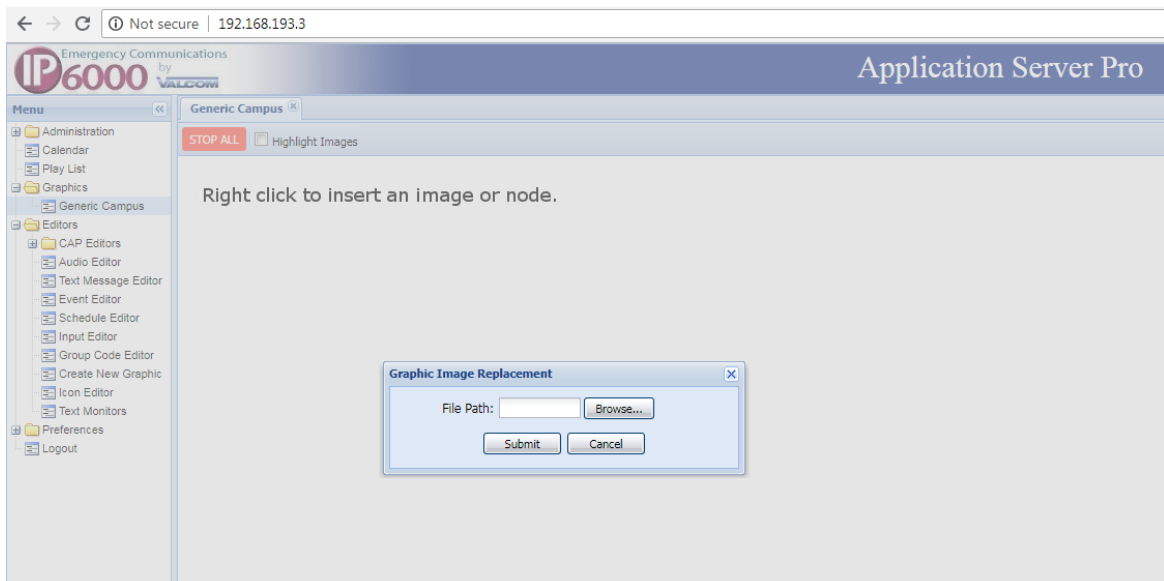
Graphics can be created to represent a map of a campus or a school. On the Graphic several different nodes can be placed. Nodes can lead to other maps, URLs or trigger Quick Page or Play Lists when a node is selected.





To create a window for displaying URL events, click “Place URL Window” The resizable URL window will open when a URL event selected to display within the graphic is active. The URL window will close when the URL event stops.

To import a graphic (JPG, PNG or GIF), right click and choose replace image

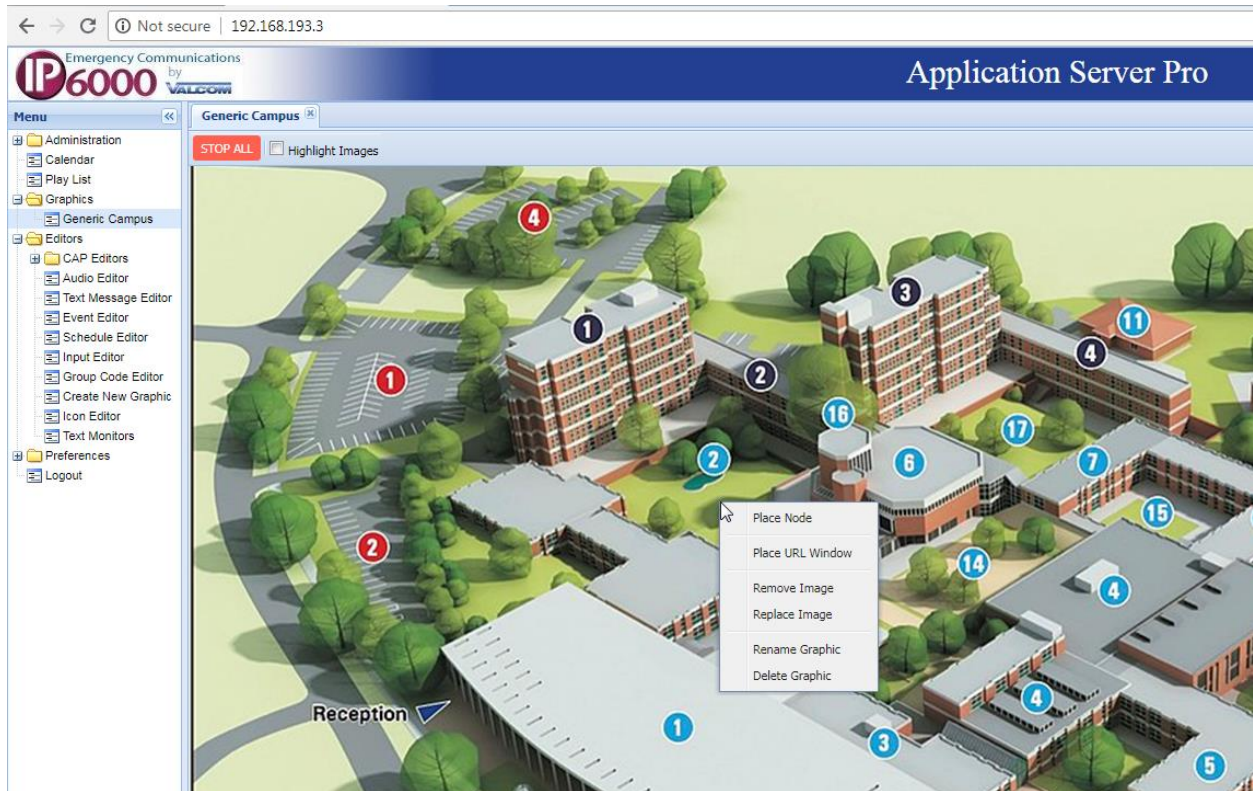


Choose an image file and click submit

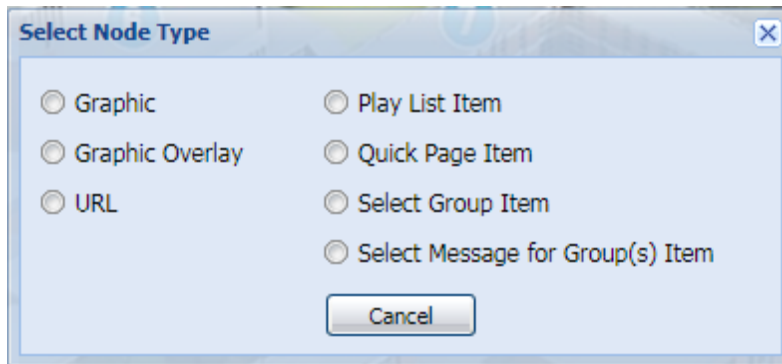


Note: The **Stop All** button only controls manually activated Playlists and Events.

Right click on the imported image to place nodes. Nodes may be dragged to the desired location on the graphic.



Node Types

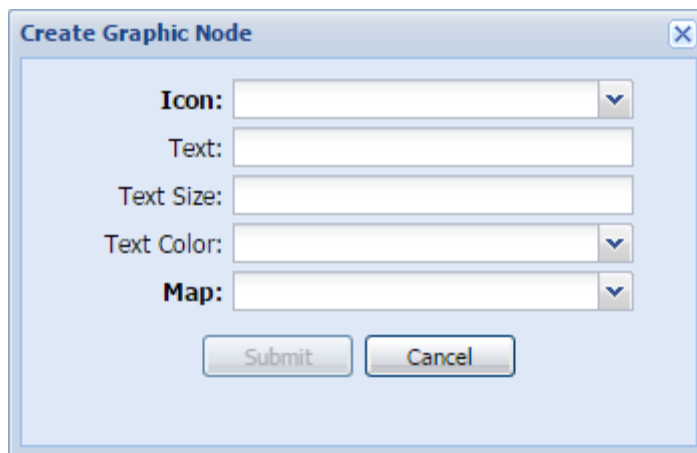


A dialog box titled "Select Node Type" with a close button (X) in the top right corner. It contains seven radio button options arranged in two columns. The first column includes "Graphic", "Graphic Overlay", and "URL". The second column includes "Play List Item", "Quick Page Item", "Select Group Item", and "Select Message for Group(s) Item". A "Cancel" button is located at the bottom center of the dialog.

<input type="radio"/> Graphic	<input type="radio"/> Play List Item
<input type="radio"/> Graphic Overlay	<input type="radio"/> Quick Page Item
<input type="radio"/> URL	<input type="radio"/> Select Group Item
	<input type="radio"/> Select Message for Group(s) Item

Graphic Nodes

A graphic node allows users to place an icon on a graphic which will navigate to another graphic or 'map'. This is useful for selecting a detailed view of an area or building.

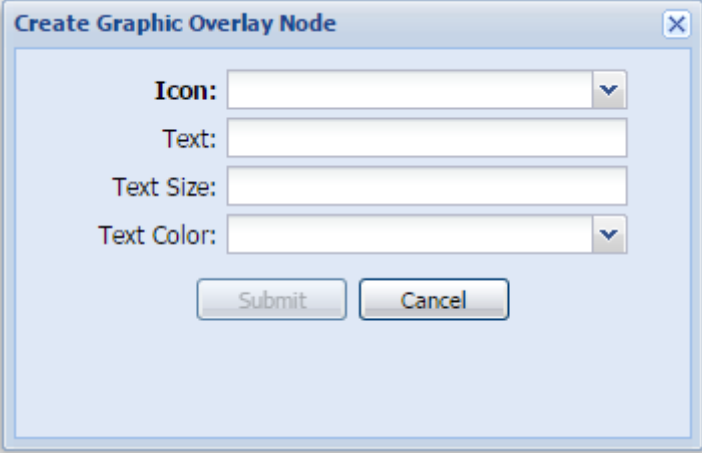


A dialog box titled "Create Graphic Node" with a close button (X) in the top right corner. It contains five input fields: "Icon" (a dropdown menu), "Text" (a text box), "Text Size" (a text box), "Text Color" (a dropdown menu), and "Map" (a dropdown menu). At the bottom, there are two buttons: "Submit" and "Cancel".

Icon:
Text:
Text Size:
Text Color:
Map:

Graphic Overlay Nodes

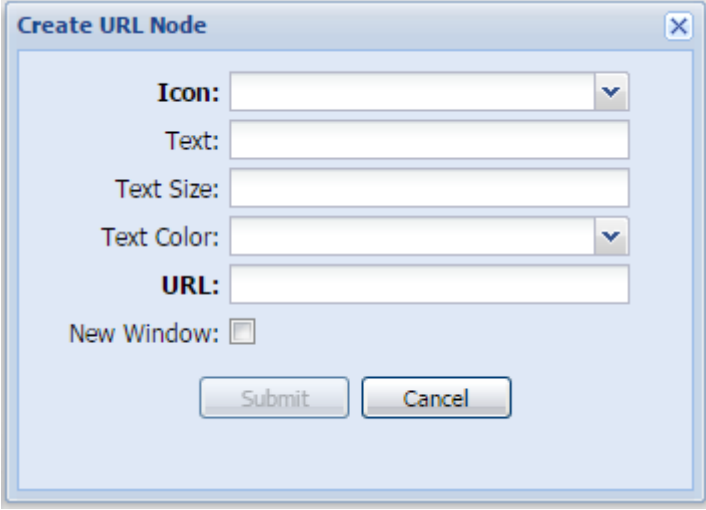
A graphic overlay node allows users to place a nonfunctional icon on a graphic. This is useful for marking locations on maps or aerial views.



The 'Create Graphic Overlay Node' dialog box features a title bar with a close button (X). The main area contains four input fields: 'Icon' (a dropdown menu), 'Text' (a text box), 'Text Size' (a text box), and 'Text Color' (a dropdown menu). At the bottom, there are two buttons: 'Submit' and 'Cancel'.

URL Nodes

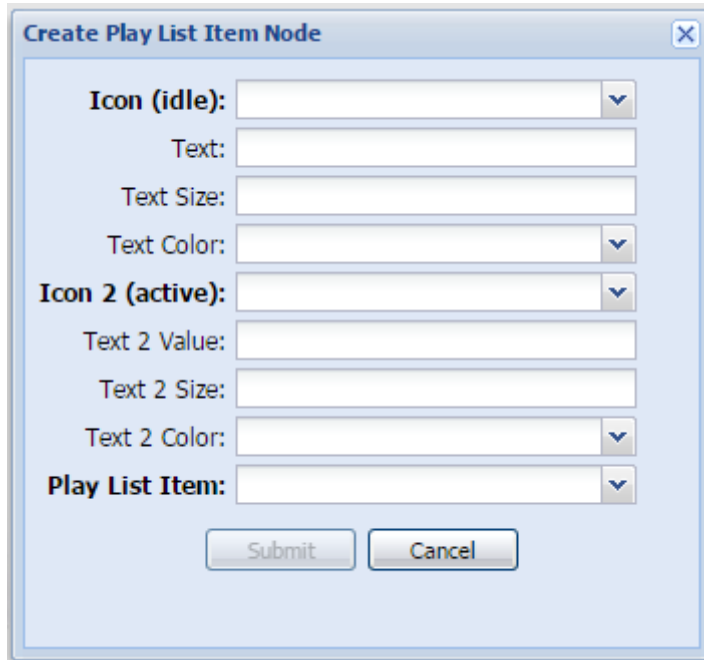
A URL node allows users to place an icon on a graphic which will navigate to a URL. This is useful for opening a web interface of another system. URL Actions include Open in new tab, Open in new browser tab and open in this graphic (in a resizable window).



The 'Create URL Node' dialog box features a title bar with a close button (X). The main area contains five input fields: 'Icon' (a dropdown menu), 'Text' (a text box), 'Text Size' (a text box), 'Text Color' (a dropdown menu), and 'URL' (a text box). Below the 'URL' field is a checkbox labeled 'New Window'. At the bottom, there are two buttons: 'Submit' and 'Cancel'.

Play List Item Nodes

A Play List item node allows users to place an icon on a graphic which will invoke an Application Server Play List item. Two icons may be added to indicate an active or idle state of the Play List item (regardless of how it was invoked).



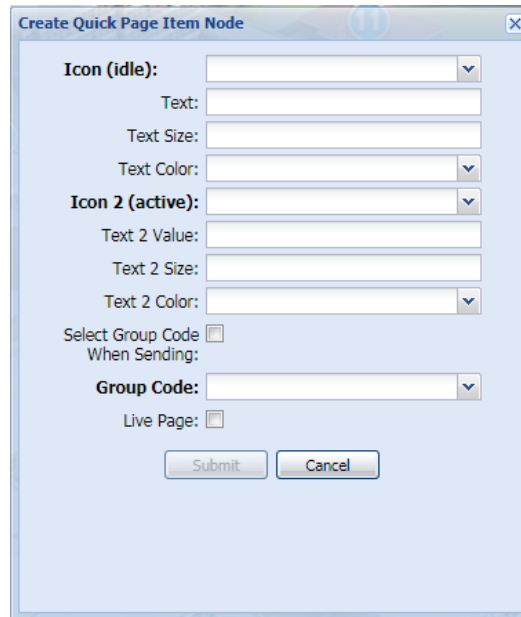
The image shows a dialog box titled "Create Play List Item Node" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Icon (idle):** A dropdown menu.
- Text:** A text input field.
- Text Size:** A text input field.
- Text Color:** A dropdown menu.
- Icon 2 (active):** A dropdown menu.
- Text 2 Value:** A text input field.
- Text 2 Size:** A text input field.
- Text 2 Color:** A dropdown menu.
- Play List Item:** A dropdown menu.

At the bottom of the dialog are two buttons: "Submit" and "Cancel".

Quick Page Item Nodes

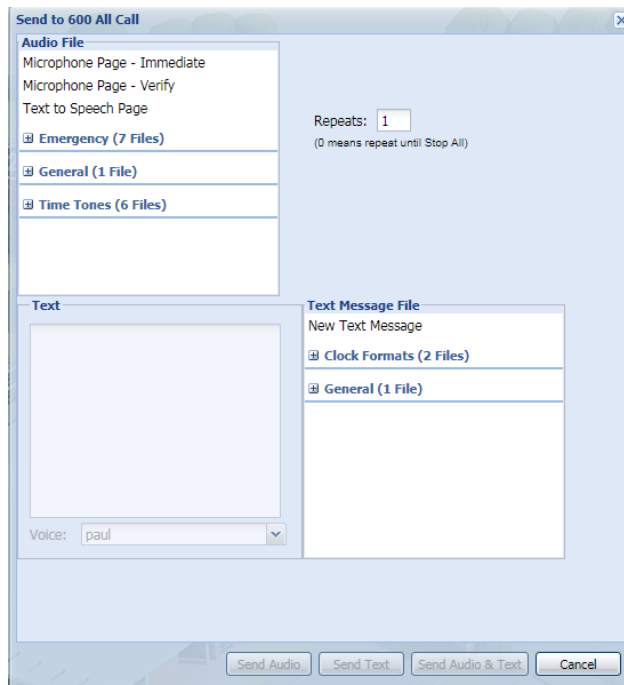
A quick page item node allows users to place an icon on a graphic which will send custom quick page audio to the selected group. If Live Page is selected, the PC's microphone is used as the audio source.



The 'Create Quick Page Item Node' dialog box contains the following fields and controls:

- Icon (idle):** A dropdown menu.
- Text:** A text input field.
- Text Size:** A text input field.
- Text Color:** A dropdown menu.
- Icon 2 (active):** A dropdown menu.
- Text 2 Value:** A text input field.
- Text 2 Size:** A text input field.
- Text 2 Color:** A dropdown menu.
- Select Group Code When Sending:** A checkbox.
- Group Code:** A dropdown menu.
- Live Page:** A checkbox.
- Submit** and **Cancel** buttons.

When clicked, create quick page items node will allow the user to choose the message to be sent:

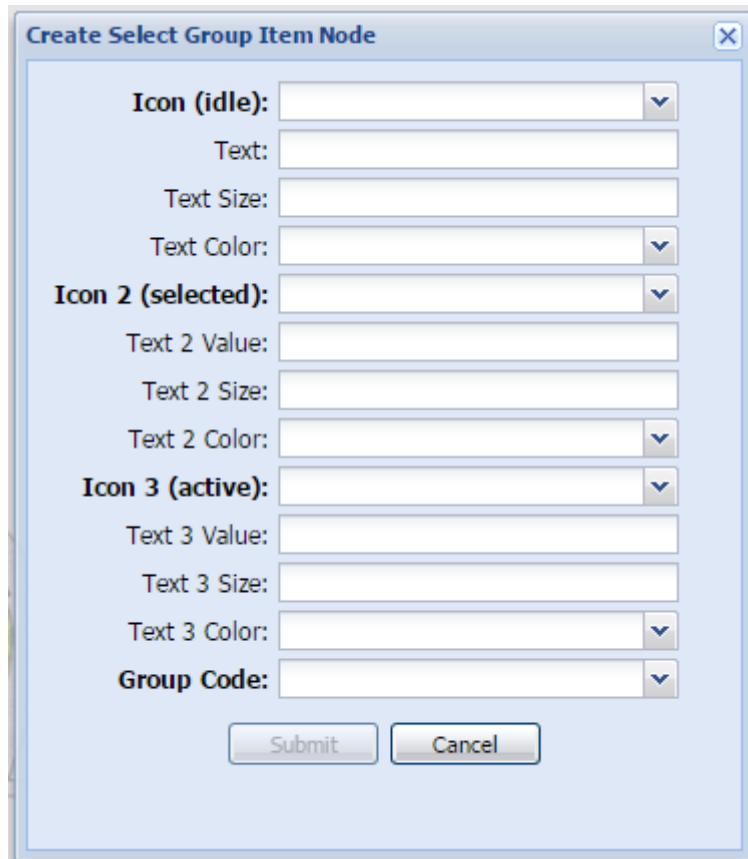


The 'Send to 600 All Call' dialog box contains the following sections and controls:

- Audio File:** A list of audio files including 'Microphone Page - Immediate', 'Microphone Page - Verify', 'Text to Speech Page', 'Emergency (7 Files)', 'General (1 File)', and 'Time Tones (6 Files)'. A 'Repeats: 1' field is present with a note '(0 means repeat until Stop All)'.
- Text:** A large text area for entering a message.
- Text Message File:** A list of text message files including 'New Text Message', 'Clock Formats (2 Files)', and 'General (1 File)'.
- Voice:** A dropdown menu currently set to 'paul'.
- Send Audio**, **Send Text**, **Send Audio & Text**, and **Cancel** buttons.

Select Group Item Nodes

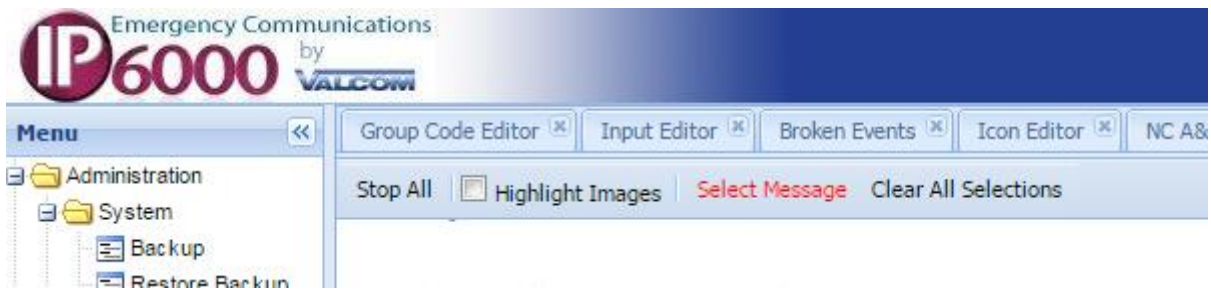
Select Group Item nodes allow users to select multiple icons, each of which adds a group to receive an impending message (see below).



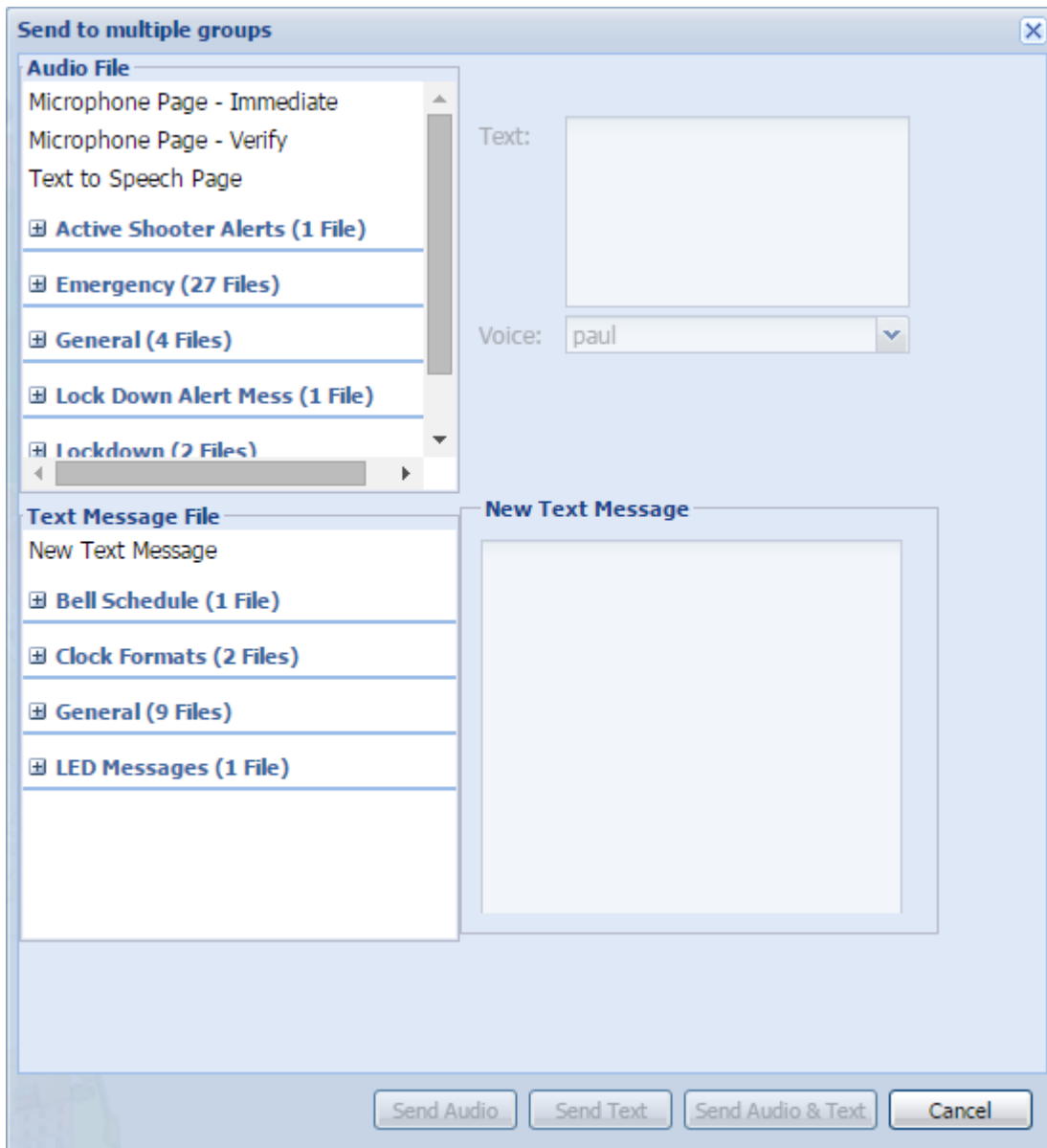
The dialog box, titled "Create Select Group Item Node", contains the following fields and controls:

- Icon (idle):** A dropdown menu.
- Text:** A text input field.
- Text Size:** A text input field.
- Text Color:** A color selection dropdown menu.
- Icon 2 (selected):** A dropdown menu.
- Text 2 Value:** A text input field.
- Text 2 Size:** A text input field.
- Text 2 Color:** A color selection dropdown menu.
- Icon 3 (active):** A dropdown menu.
- Text 3 Value:** A text input field.
- Text 3 Size:** A text input field.
- Text 3 Color:** A color selection dropdown menu.
- Group Code:** A dropdown menu.
- Submit** and **Cancel** buttons at the bottom.

Once one or more Select Group Item icons are clicked, a Select Message and Clear All Selections menu item becomes available. (Node type "Select Message for Group(s) Items" creates a node which emulates the Select Message menu item)

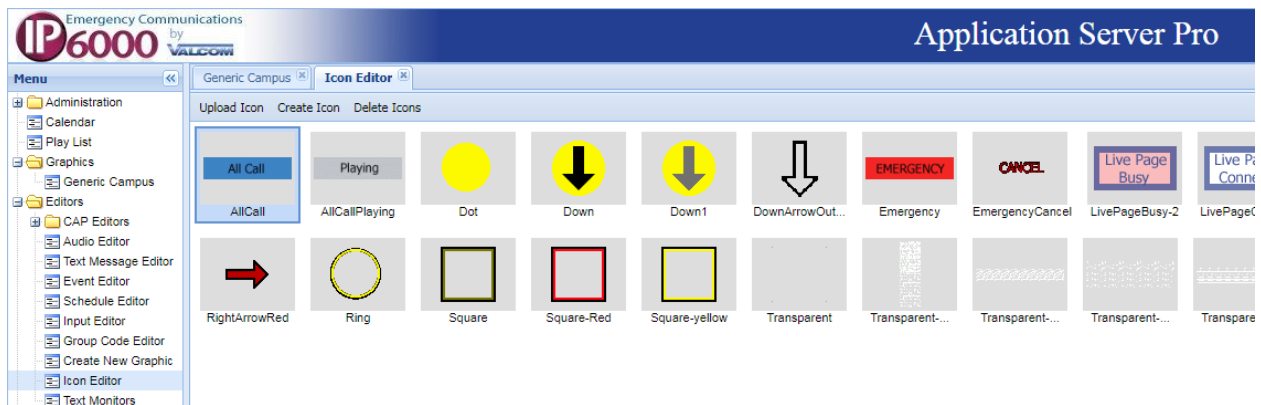


Clicking Select Message allows user to pick a message to send to all the groups selected.



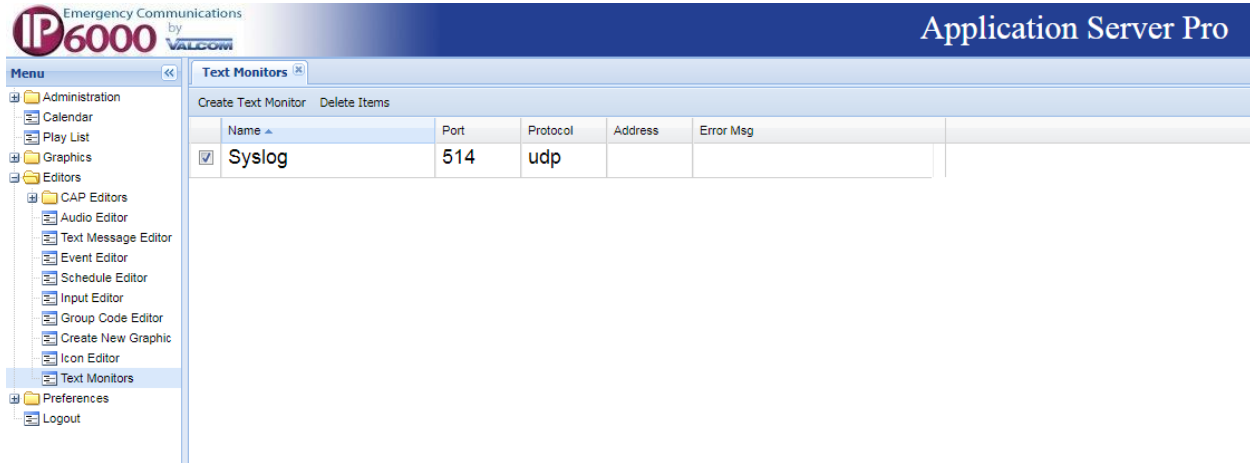
Editors/Icon Editor

Icon Editor allows users to add, create or delete icons that may be used for the nodes. Adding icons allows users to import jpeg, png, bmp, tif or gif files to be used for icons. If transparency is desired for indication of active status, only png or gif files may be used. Imported graphics to be utilized as icons should be approximately 100 x 100 pixels in size. . Valcom maintains a library of ICONs here: <http://www.class-connection.com/icons.htm>.

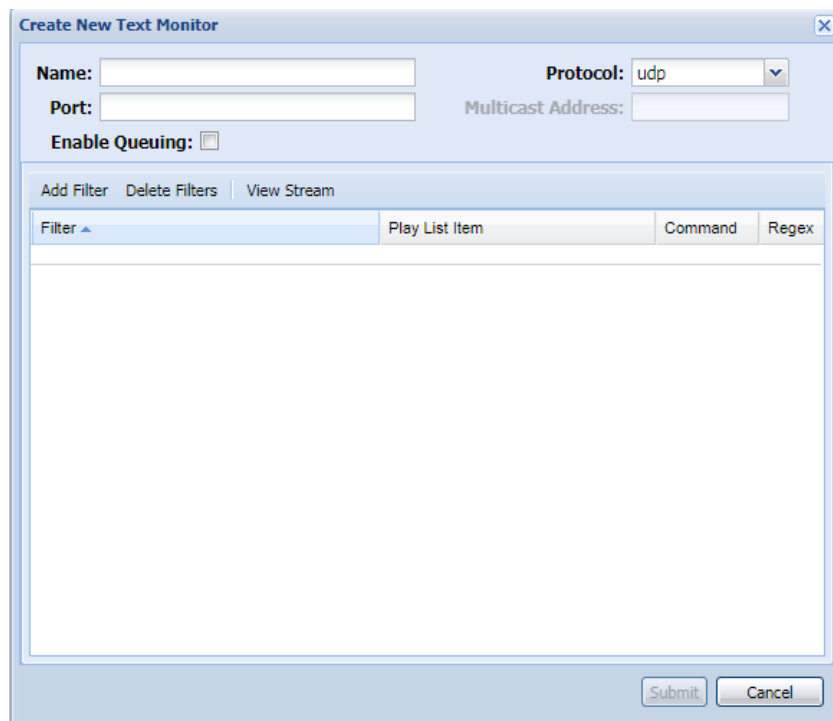


Editors/Text Monitors

The Application Server can monitor data outputs, such as syslog, from other devices and scan for text strings. If the defined text string exists, the Application Server can invoke a Play List item.



Name the text monitor to identify the type of data being monitored, identify the port number, protocol (UDP, TCP or Multicast) and, if applicable, the multicast address to monitor. Once accomplished, add one or more filters for the defined port. (Hint: View stream may be clicked to sample the incoming data).



Enter the trigger text string under filter, choose a Play List item to control and choose a command. Commands are start, stop, or stop all active Play List items.

Create New Filter

Regex:

Filter: PAGE STOP ORIG, 000, 24,

Test String:

Test Result:

Play List Item: All Clear

Command: start

Save Cancel

Create New Text Monitor

Name: **Protocol:** udp

Port: **Multicast Address:**

Enable Queuing:

Add Filter Delete Filters View Stream

Filter	Play List Item	Command	Regex
PAGE START ORIG, 000, ...	Play List 1	start	0

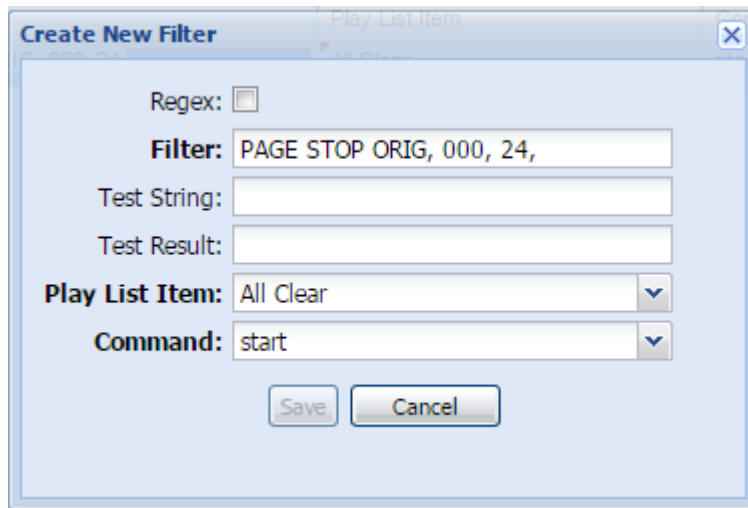
Submit Cancel

If you need to capture variable information from a text monitor, use [capture groups](#) or refer to the following section.

Common Uses of Regex in Text Monitor

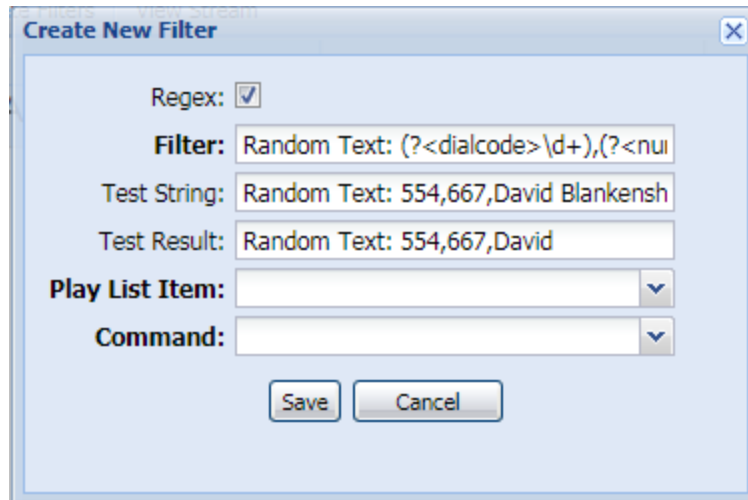
This process is used to extract information from incoming data (syslog, etc.) and use that message specific data to create custom text to speech and text messages for LED signs and other text message recipients.

The Regex Box in Text Monitor must be checked when using Regular Expressions.



The screenshot shows a dialog box titled "Create New Filter" with a close button in the top right corner. The "Regex" checkbox is unchecked. The "Filter" text box contains the text "PAGE STOP ORIG, 000, 24,". The "Test String" and "Test Result" text boxes are empty. The "Play List Item" dropdown menu is set to "All Clear". The "Command" dropdown menu is set to "start". At the bottom of the dialog are "Save" and "Cancel" buttons.

Note that once enabled, a Test String may be entered to test the results of the Regex filter.



The screenshot shows the same "Create New Filter" dialog box, but now the "Regex" checkbox is checked. The "Filter" text box contains the regular expression "Random Text: (?<dialcode>\d+),(?<nui". The "Test String" text box contains "Random Text: 554,667,David Blankensh". The "Test Result" text box contains "Random Text: 554,667,David". The "Play List Item" and "Command" dropdown menus are empty. The "Save" and "Cancel" buttons are at the bottom.

Assigning variables to received data

Syslog String used as an example = **Random Text: 554,667,David Blankenship**

Apply Text Monitor Filter =

```
Random Text: (?<dialcode>\d+), (?<number>\d+), (?<callerID>.\S*)
```

554 is dynamically assigned to variable *dialcode*

667 is dynamically applied to variable *number*

David is dynamically assigned to variable *callerID*

Explanation:

(?*dialcode*\d+) finds sequential digits and assigns variable “*dialcode*” to those digits

(?*number*\d+) finds the next set of sequential digits assigns variable “*number*” to those digits

(?*callerID*.\S*) finds sequential letters and assigns variable *callerID* to those sequential letters

(If you wanted to assign another variable, like “*lastname*” to Blankenship, you would modify the Text Monitor Filter to:

```
Random Text: (?<dialcode>\d+), (?<number>\d+), (?<callerID>.\S*) (?<lastname>.\S*)
```

The commas and the space between the bracketed expressions are matched literally and form the boundaries of the text or numbers to be included in the variables.

For example, you get the same results if the Syslog String was:

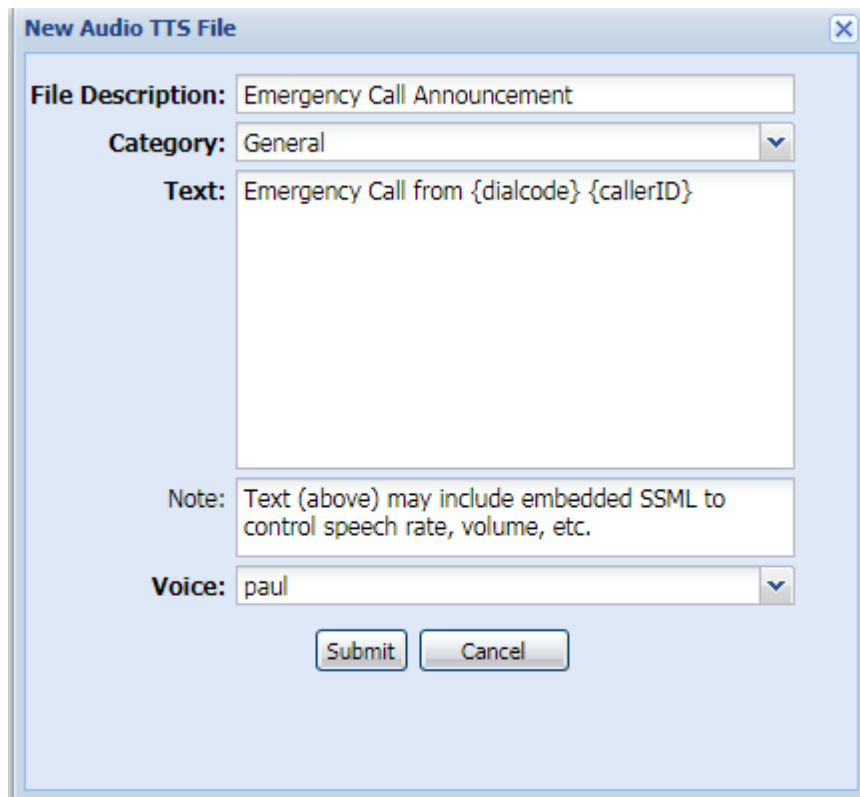
Random Text: 554 red 667 white David blue Blankenship

And the Text Monitor Filter was:

Random Text: (?<dialcode>\d+) red (?<number>\d+) white (?<callerID>.\S*) blue (?<lastname>.\S*)

Using the variables in TTS files

Variables are entered in curly brackets {variable}. When the text-to-speech is rendered as part of an event, the number and word represented by the variable will be inserted.



New Audio TTS File [X]

File Description: Emergency Call Announcement

Category: General [v]

Text: Emergency Call from {dialcode} {callerID}

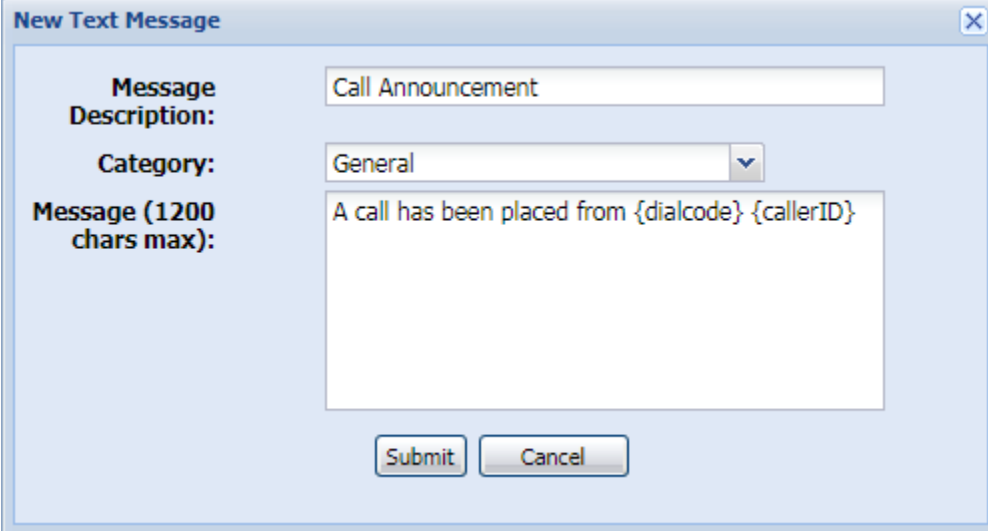
Note: Text (above) may include embedded SSML to control speech rate, volume, etc.

Voice: paul [v]

[Submit] [Cancel]

Using variables in the Text Message Editor

Variables are entered in curly brackets {variable}. When the text is displayed as part of an event, the number and word represented by the variable will be inserted.



The screenshot shows a 'New Text Message' dialog box. It has a title bar with the text 'New Text Message' and a close button. The dialog contains three main sections: 'Message Description:' with a text input field containing 'Call Announcement'; 'Category:' with a dropdown menu currently set to 'General'; and 'Message (1200 chars max):' with a larger text area containing the text 'A call has been placed from {dialcode} {callerID}'. At the bottom of the dialog are two buttons: 'Submit' and 'Cancel'.

Accepting random text/numbers/spaces in Text Monitor

If you receive a syslog message such as Call Started 101, 300 and you want the text monitor filter to match any Call Started message that ends in 300 (Call Started 101, 300 or Call Started 102, 300 or Call Started 201, 300) Then use the wildcard `.*?` as follows:

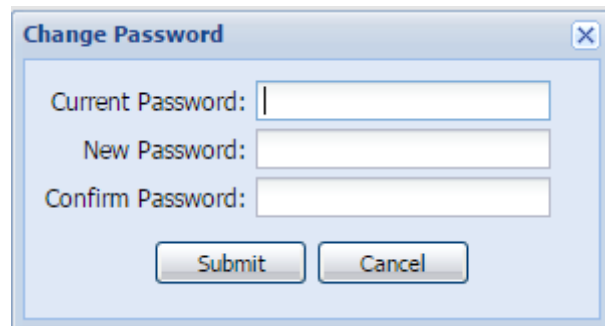
(Call Started).*(300)

`.*?` matches any character (except for line terminators)

You may also test your regular expressions at <https://regex101.com/>

Preferences/Password

Preferences/Password allows user to change the default 4cc3ss admin password.



A dialog box titled "Change Password" with a close button (X) in the top right corner. It contains three text input fields: "Current Password:", "New Password:", and "Confirm Password:". Below the fields are two buttons: "Submit" and "Cancel".

Valcom Desktop Alert Install (Optional)

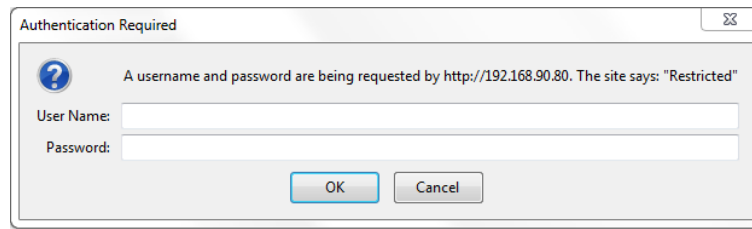
Introduction

The Valcom Desktop Alert is a tool that can be used to help spread word of any dangers by displaying a desktop alert on the screen of any computer running the Windows operating system. The purpose of the Valcom Desktop Alert is to capture any text message sent out by Valcom VE602x Application Servers on the network. The Valcom Desktop Alert will utilize the same ports and multicast addresses as the other devices on the system.

Server Side Setup

Once enabled with the Valcom Desktop Alert option, the VE602X Application Servers are able to deliver the executable install file for the Desktop Alert, a custom logo graphic as well as .INI files. This is handled through a separate screen located at the URL address http://<my_server>/popup.

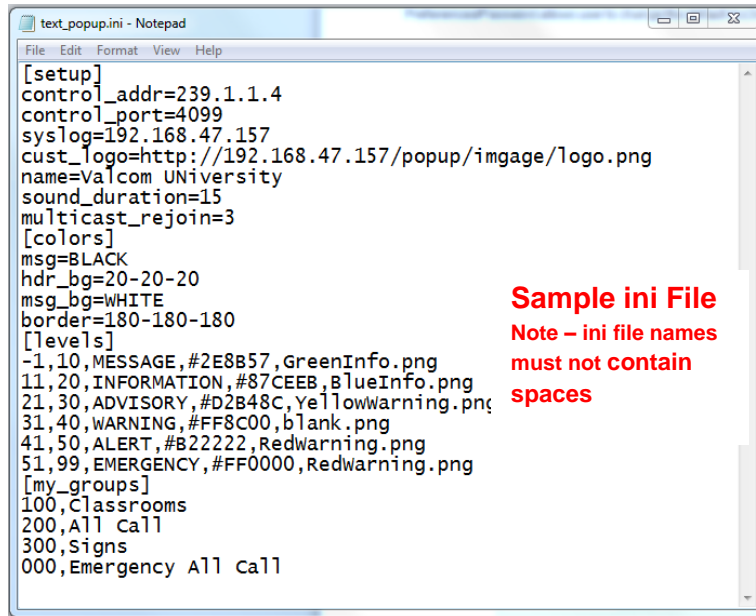
The default log in credentials are user name = "popupadmin" and password "PopupAdmin_pwd"



The screen allows the IT department or user in charge of setup and distribution of the Desktop Alert to upload a custom .INI file and custom JPG logo file to the server for distribution. Several .INI files and logos can be uploaded for different classes of users and the specific links can be

distributed through email, or may alternately be entered during installation in the “**Enter the URL of the configuration server**” field. The logo JPG file should be 120 x 75 pixels. A sample.ini file has been provided that will show how to set up the .INI file to contain the proper group codes. The executable can be received by visiting the URI listed under Valcom Desktop Alert Install URI.

Configuration Ini files can be uploaded and made available through http://<my_server>/popup.



```
text_popup.ini - Notepad
File Edit Format View Help
[setup]
control_addr=239.1.1.4
control_port=4099
syslog=192.168.47.157
cust_logo=http://192.168.47.157/popup/imagage/logo.png
name=Valcom University
sound_duration=15
multicast_rejoin=3
[colors]
msg=BLACK
hdr_bg=20-20-20
msg_bg=WHITE
border=180-180-180
[levels]
-1,10,MESSAGE,#2E8B57,GreenInfo.png
11,20,INFORMATION,#87CEEB,BlueInfo.png
21,30,ADVISORY,#D2B48C,Yellowwarning.png
31,40,WARNING,#FF8C00,blank.png
41,50,ALERT,#B22222,Redwarning.png
51,99,EMERGENCY,#FF0000,Redwarning.png
[my_groups]
100,Classrooms
200,All Call
300,Signs
000,Emergency All Call
```

Sample ini File
Note – ini file names
must not contain
spaces

Anatomy of the Ini File

setup section

The *control_addr* and *control_port* items specify the multicast IP address and port on which the Desktop Alert receives messages from the VE602x Application Server. The values must match those of the Control Multicast and Control Port values in the Vip tab of the Setup screen on the VE602x Application Server.

```
control_addr=239.1.1.4
```

```
control_port=4099
```

The *syslog* item is optional. If present, it provides the address of a Syslog server to log information about messages received, etc. Each instance of Valcom Desktop Alert with a defined Syslog server will post to the Syslog server independently.

```
syslog=192.168.42.151
```

The *cust_logo* item specifies the URL of the file for the logo that appears in the top right corner of alerts.

```
cust_logo=http://Server_IP_Address/popup/images/cclogo.jpg
```

The *sound_duration* item is the default timeout for the audible PC alert in seconds.

```
sound_duration=30
```

The *multicast_rejoin* item is how often, in minutes, the Valcom Desktop Alert will make a network request to rejoin the multicast group. Minimum acceptable value is 3 minutes.

```
multicast_rejoin=3
```

The *name* item provides the name that appears in the top center (and also in the frame captions and the right-click menu).

```
name=Name of this University Notification System
```

colors section

The *colors* and *levels* sections allow the display colors to be customized. Colors may be entered in three formats:

Certain common colors may be entered by name. These are: BLACK, WHITE, RED, BLUE, GREEN, CYAN, LIGHT_GREY, and YELLOW.

Red, green, blue values can be entered as 3 decimal numbers (between 0 and 255) separated by dashes, e.g., 250-180-0 (http://www.rapidtables.com/web/color/RGB_Color.htm)

Red, green, blue values can be entered as a # followed by three 2 digit hexadecimal numbers, e.g., #FAC81E (<http://www.color-hex.com/>)

The items in the *colors* section are:

name – the color of the name text in the top center area

msg – the color of the message text

hdr_bg - the background color for the name area in the top center, and the message type area directly below it

msg_bg - the background color for the message area

border – the initial color for the border. (The border color will change when messages are displayed.)

Here is an example of a *colors* section:

name=BLUE

msg=BLACK

hdr_bg=20-20-20

msg_bg=250-180-0

border=180-180-180

levels section

The *levels* section defines the message types, based on the Valcom message priority levels - provide a name and color for each type. Each item consists of a lower and upper limit for a range of priority levels, followed by the name and color for that level. When a message is received, its priority level is used to determine the message type. The name for that message type is displayed in the message type area, in the specified color. The border is also changed to that color. **The message types should cover all priority levels between -1 and 99.** Here is an example *levels* section:

-1,10,Message,GREEN

11,20,Information,GREEN

21,30,Advisory,180-180-0

31,40,Warning,#FAC81E

41,50,Alert,250-30-30

51,99,Emergency,RED

(Note that all text messages sent from Quick Page have the same priority level. This level can be set in the Paging tab of the VE602x Application Server Setup screen. For Text Message events, the priority can be set per event.)

my_groups section

The *my_groups* section specifies which Valcom group codes the Desktop Alert will respond to. Each item contains a group number and group name. Only the group number appears in the Valcom text message. The name is effectively just a comment. Here is an example *my_groups* section:

002,Classrooms

004,Test Emergency

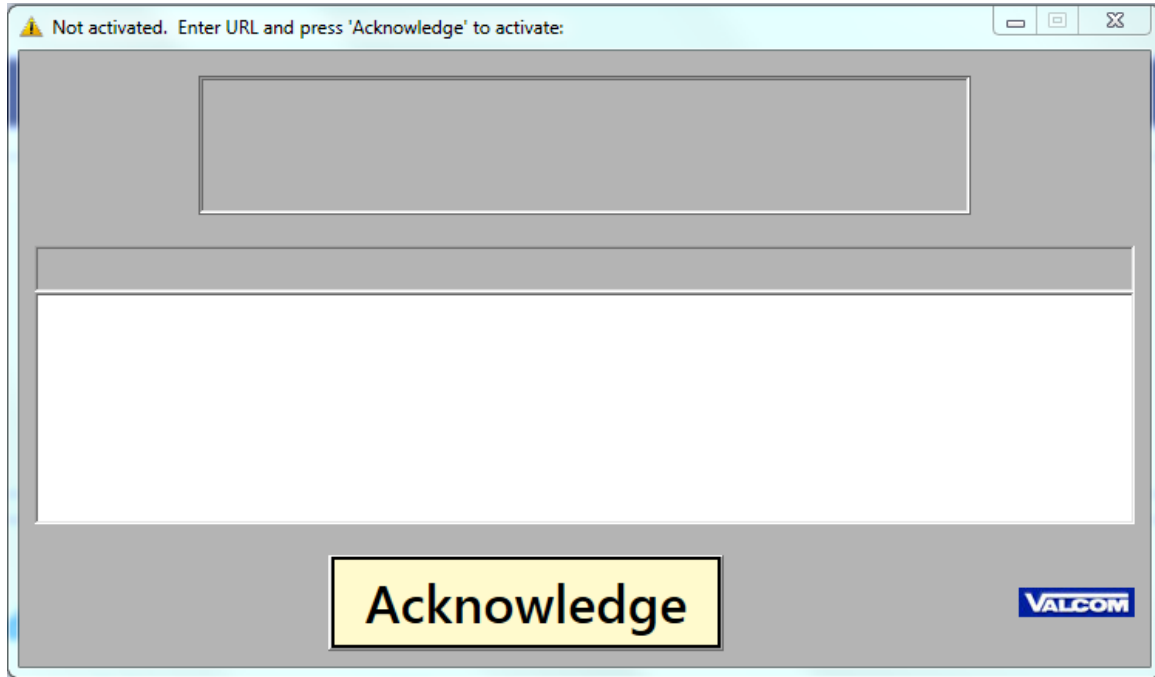
010,signs

730,test

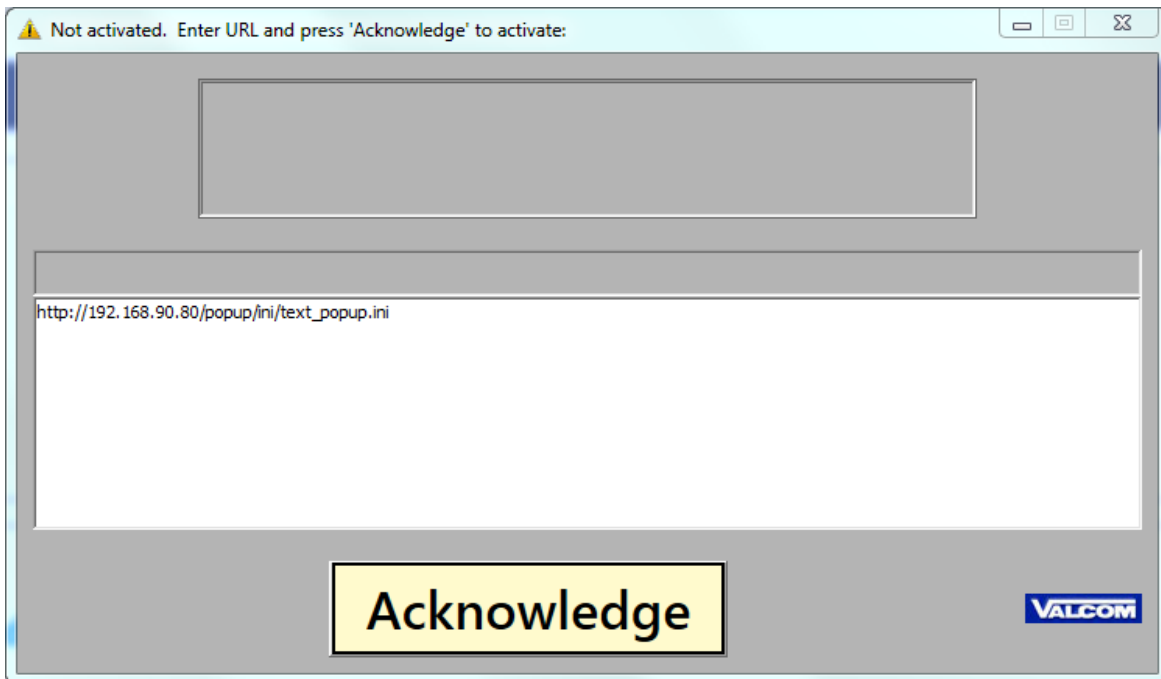
Install

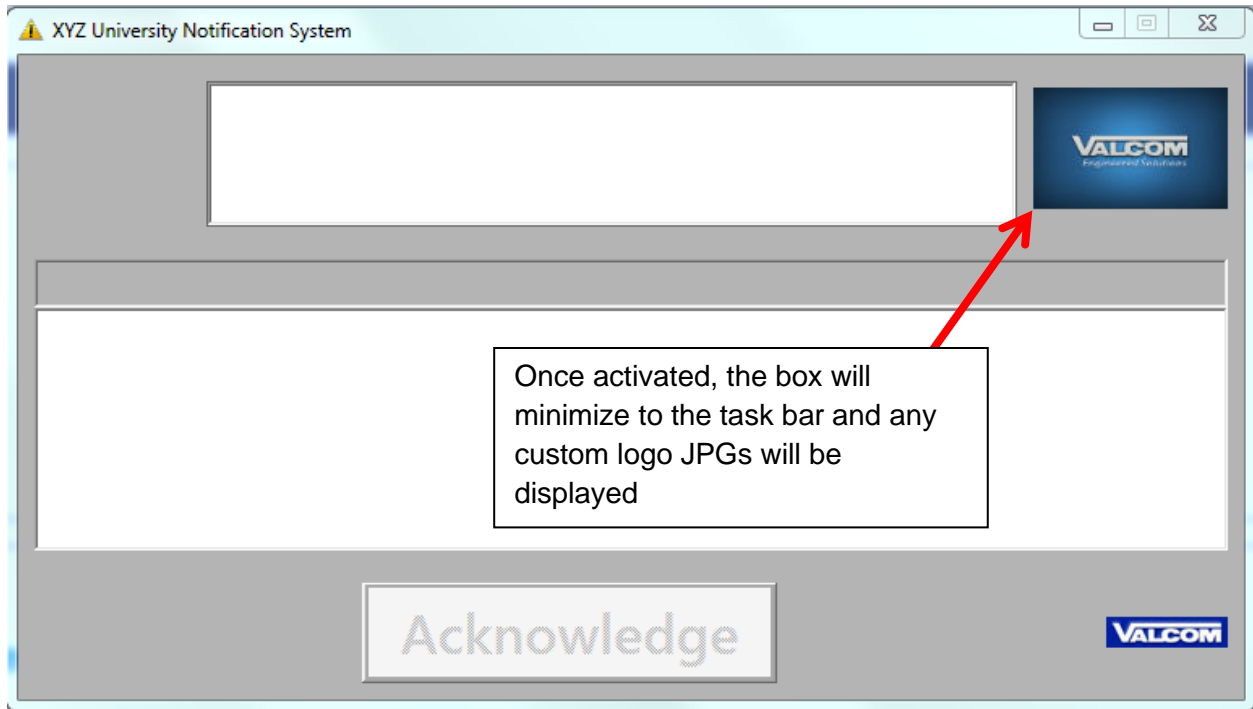
There are several options available for installing the Valcom Desktop Alert.

The materials needed to install the Valcom Desktop Alert may be sent through email to all the intended users. The email will include two separate links. The first link will be a link for the Valcom Desktop Alert itself while the second link will be a link to the .INI file that contains the page groups. Click the first link to download the installer to the computer. Once downloaded, invoke the installer. The default settings that the InstallShield Wizard program uses will work fine for the install so nothing needs to be changed. After installation of the program has completed click the Start Menu and All Programs and open the Valcom Desktop Alert. If this is the first time the program has been opened, the user will be prompted with a screen that looks like the one below:



At this point, if the URL of the .INI file was not entered during install of the Valcom Desktop Alert, copy and paste the second link in the email into the large gray box and press the Acknowledge button to activate the Valcom Desktop Alert.





Installation Options

The Valcom Desktop Alert can be provided as either an EXE or MSI to be installed.

exe Install

The exe is used for guided installs. Since the Valcom Desktop Alert was built using InstallShield it would also be possible to create a response file for silent installation. It is recommended that any silent or mass installs be done using the MSI instead.

The Customer Information screen has a field for User Name and Organization. The User Name is the name that is used to register the install. The Organization is the company named used to register the product.

The Server URL is the location on the network of the configuration INI file. The program will go out and fetch the INI from this url to configure the Valcom Desktop Alert.

msi Install

The msi can accept a number of switches for silent installs. A basic install can be performed via the /i switch followed by the msi file name using the command:

```
msiexec /i ValcomDesktopAlert1_08_0001.msi
```

An uninstall can be performed via the /x switch using the command: `msiexec /x ValcomDesktopAlert1_08_0001.msi`

A silent install can be performed without the need for a response file via the /qn switch using the command:

```
msiexec /i ValcomDesktopAlert1_08_0001.msi /qn
```

Other silent options are:

/qb = Displays a basic interface - mostly silent but with a progress bar

/qr = Displays a reduced user interface - also automatic, but displays a little more

There are several other options that can be used as well. See documentation on msiexec for all the possibilities: <https://technet.microsoft.com/en-us/library/cc759262%28v=ws.10%29.aspx>

Additional parameters can be passed to the installer. Note that these parameters can be provided even if a silent install is not being run. Doing so will initialize the dialog boxes in the install UI with the values. Parameters should be enclosed in quotation marks. A command using these parameters will take the following form:

```
msiexec /i ValcomDesktopAlert1_08_0001.msi /qn PARAMETERNAME="value"
```

For example, to run silently and provide the server url, use the following command:

```
msiexec /i ValcomDesktopAlert1_08_0001.msi /qn SERVERURL="https://path/to/text_popup.ini"
```

Available options include:

- SERVERURL: URL to configuration ini file. The application will download this file each time it starts up and will keep a local copy in case it can't reach the URL on a subsequent launch. If the server url is not provided, it will retain the current value if one has already been defined on a previous installation. Also note that the install can be run a second time with a different URL (which is like a modify or repair) and it will update the url to the new value.
- USERNAME = Name used to register the install.
- COMPANYNAME = Company name used to register the install.
- INSTALLDIR = Directory to install the product to.
- LAUNCHPROGRAM = By default, the program will launch after a silent install (1). To prevent the program from launching pass an empty string (i.e. ""). This parameter does not need to be used if you are NOT running silently, since a checkbox at the end of the install controls whether or not the program launches. Technically, however, this parameter can be used to set the default value of the checkbox to off, like so:
 - msiexec /i ValcomDesktopAlert1_08_0001.msi LAUNCHPROGRAM=""

Caveats of install

- A rule needs to be added to the firewall to allow ValcomDesktopAlert.exe to listen on the port specified in the configuration ini file (default 4099). If using Windows Firewall, this needs to happen prior to deployment so the application doesn't ask the user on launch.
- If you make changes to the configuration ini file after the application has been deployed, the changes will not take effect until the deployed instances are restarted.
- You may want to set up a syslog monitor to watch the application and restart it if someone closes it or in the unlikely event that it crashes.
- If a user is logged in and the application is running, and they switch accounts without logging out of the first one, the application will fail to launch for the second account and they will not receive any alerts. This is because the application is run at the user level and needs to bind to an address/port. Since the application launched from the first account is already bound, the second instance will not bind and will silently fail to launch.

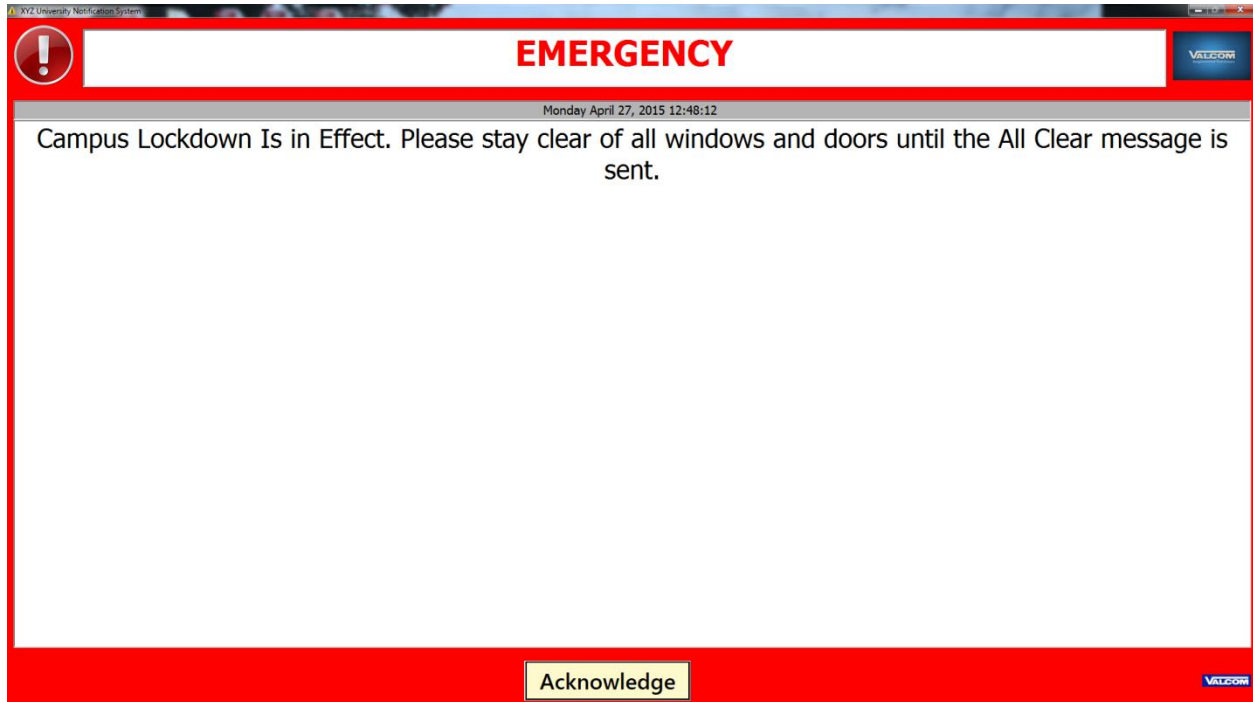
Usage

Once the Desktop Alert is up and running it requires very little attention. Minimizing the Desktop Alert will move it to the taskbar. Closing the Desktop Alert will remove the icon from the task bar and close the window; however, the Desktop Alert will still reside in the notification area in the lower right of the desktop. Double clicking on the icon will bring the Desktop Alert window back. Right clicking on the icon in the notification area will give the user several options:



- 'Close XYZ University Notification System' will close the application until it is opened under the Start Menu again
- 'Restore XYZ University Notification System' will bring the Desktop Alert back to the screen
- 'Show History' will open a new window showing a history of all messages received, with timestamps.
- 'Test' will cause the program to wait for 10 seconds before returning the number of other devices running the Desktop Alert and a source number.

If the Desktop Alert is invoked by a group message, it will pop up to the forefront of the screen and display the message. If sound is active it will continue to beep until the Acknowledge button is pressed or the timeout period defined in the ini file has passed. The icon in the taskbar will also blink until the Acknowledge button is pressed.



Troubleshooting

Windows 8 install

There is currently an issue where the Install will not proceed on Windows 8 and 8.1. A program known as Windows SmartScreen prevents the app from running. This is happening because Windows 8 sends app information on every program you try to download and install to the Microsoft Servers. If Microsoft doesn't know about the program either because it is new or few people use it then the Server will respond that the program is unsafe and prevent immediate execution. To get around this issue the user has to select 'More info' and then the option to 'Run Anyway' will appear. Use 'Run Anyway' to install the program on your machine.

Using a new ini file

There is no easy way to reset or change the Ini file used by the Valcom Desktop Alert at this time. If a change of the ini file is required, the user must go and delete the url and ini file located inside the mnt directory of the program. The full path to the ini file on a windows machine is *C:/Program files(x86)/Valcom/DesktopAlert/mnt*.

Basic Application Server Troubleshooting

If the Application Server is not communicating, verify that the front panel power LED is illuminated. Also, be sure to check network connections, cables and VLAN port.

Ascertain if any network changes have occurred and verify all [network settings](#).

To aid in problem resolution, please provide Technical Support with:

Is there any change if you close your browser, then bring it up and log in again?

Are you using the latest, currently supported version of your browser of choice?

A summary of the problem and the troubleshooting done so far

A screen shot showing the error message and what was happening at the time

A current system backup file

A VIP-102B system “snapshot” of the installed system

A screenshot of the VIP-102B “Network Diagnostics” screen

The VE6025 log file and/or syslog file from the VE6024

Power failures will cause an audible alert which may be silenced via the front panel “silent” button.

The fault LED will also illuminate if there is a power failure or internal power circuit failure.

The battery LED will illuminate while the internal battery is not fully charged.

Best Practices & General Troubleshooting procedures may be found here.

Browser Compatibility

Internet browsers are not created equally and often vary in functionality, permissions, and visual display characteristics/capabilities.

Valcom strives to maintain compatibility with the latest, actively supported, versions of mainstream browsers such as those provided by Apple, Microsoft, Google and Firefox. Browser updates often occur without notice and may affect the experience of using browser-based products.

Outdated browser versions should be avoided.

If experiencing issues with our browser interface, using a different browser may yield more acceptable results.

Please report any browser issues to esd@valcom.com.

The Syslog

The system can be set up to send syslog messages to an IP address such as a computer with the 102B tool installed. The syslog can be saved into a file.

To setup the Syslog for an Application Server

Go to Administration / Setup

Go to the Syslog tab

Enable Syslog IP

Enter a Syslog IP address

Set level to Debug

To setup the Syslog for a VE6024

Go to Settings / Syslog Configuration

Set log level to Debug

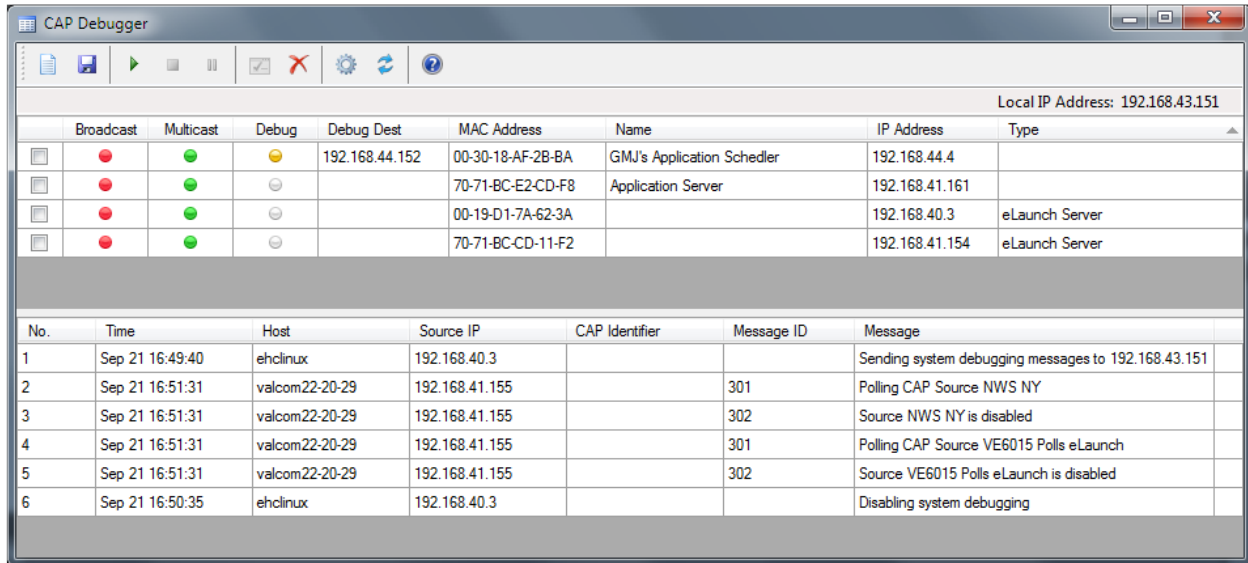
Enable Use Syslog

Enter a syslog Server / IP address

The syslog messages can be viewed by going to the 102B tool, selecting communications and selecting the option to 'View Syslog Messages'

The CAP Debugger Tool

The CAP Debugger, automatically installed with the VIP-102B, is used to trace the progress of an alert generated by the eLaunch system and handled by the Application Server Pro devices.



The top section of the tool will list all of the eLaunch and Application Server Pro devices that have been detected on the network from the beacons they are sending. The bottom section will display syslog messages from selected devices as alerts are generated.

To use the tool, put checks beside all the devices that you wish to debug and click the Start button.



The selected devices will enter debugging mode as indicated by the Debug status indicator. The destination of their debug messages will be set to the IP address of the local PC.

Debug	Debug Dest
<input checked="" type="checkbox"/>	192.168.44.152
<input type="checkbox"/>	
<input checked="" type="checkbox"/>	192.168.43.151
<input type="checkbox"/>	

A green indicator tells us that debug messages are being sent to our local PC. A yellow indicator tells us that the device is sending debug messages to some other PC on the network. A white indicator tells us that the device is not currently in debug mode.

At this point, an alert can be generated from the eLaunch system and debug messages should appear in the lower section of the tool. If both an eLaunch system and an Application Server Pro were selected for debugging, messages should be seen from both devices as the alert is generated and then received and acted upon.

When debugging is finished, the Stop button can be pressed which will cause any device that is sending debug messages to the local PC to exit debug mode.



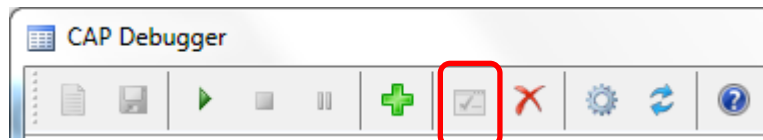
the Stop ALL Debugging button stops ALL devices that are sending debug messages, even those that are sending to other destinations:



The Pause button can be used to temporarily halt receiving messages while debugging without actually telling the devices to exit debugging mode:



While a capture is running, the Change Selected Devices button can be used to modify the devices that should be sending messages without having to stop the current capture first. Simply adjust the necessary check marks beside the desired devices and click the button to change the devices that will be sending debugging messages to the local PC:



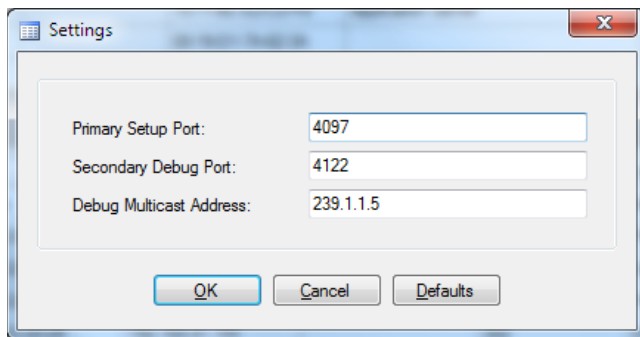
The New button can be used to clear the list of messages received and start a new capture using the selected devices:



The Save button can be used to save the messages from the current capture to a text file:



The Settings button can be used to change the address and ports that the tool is communicating on if these settings have been modified in the actual VIP devices using the VIP-102B tool:



The Restart Communications button can be used to restart communications if some error occurred during startup and communications could not be initialized. This could be caused by problems such as other tools running that are already using the specified ports or by network connectivity issues:



If there were issues on startup, the button may appear with a **red background** to indicate that there were problems, and the other buttons might be disabled due to the restricted functionality until the problem is resolved.

Using the VIP Status Monitor

Introduction

Originally created to monitor the status of critical servers installed in a High Reliability Automatic Failover configuration, the VIP Status Monitor (VSM) has evolved into a powerful tool that can be used in conjunction with any device with a valid IP address on the network. The software is available [here](#) and a manual can be found [here](#).

Volume Offset Interoperability between Valcom Devices

Currently there are several areas to modify the volume offset of an IP6000 system. Through the VIP-102B IP Solutions Setup Tool, users can set a volume offset for each IP Speaker and Audio Gateway channel and may assign an additional volume offset based upon group priorities.

From the server, users can assign a global volume offset in the setup menu, and may also assign individual volume offsets to audio events.

Volume Offset on the Server

The 'System Volume Offset' is located under the 'Paging' tab found under Administration/Setup. The threshold for the volume is between -40 volume units and +20 volume units. The 'System Volume Offset' is applied to any audio being originated from the Application Server.

On the same 'Paging' tab in the setup menu is an 'Audio Volume Offset' for the Quick Page section. The 'Audio Volume Offset' can be set in the same threshold between -40 volume units and +20 volume units.

The last area to set a volume offset is when you create an Audio File Event, a Streaming Audio Event or a Recording. This field is labeled as 'Volume Adj'.

To determine what volume offset to send to the Speakers when making a page, the server will take into consideration both the 'System Volume Offset' and the 'Audio Volume Offset' (Quick Page) or the 'Volume Adj.' (Audio File Event, Streaming Audio Event or a Recording).

Before sending out a message the server will add these two numbers together. If the total offset exceeds +20 volume units, the server will set the offset to +20 volume units. Likewise, if the total offset is less than -40 volume units the server will set the offset to -40 volume units.

For example, if the 'System Volume Offset' is +10 volume units and the 'Volume Adj.' of an Audio File Event is set for +15 volume units; the Volume Offset sent to the Speakers is +20 volume units. If the 'System Volume Offset' is -20 volume units and the 'Volume Adj.' of an Audio File Event +5 volume units, then the volume offset sent to the speakers is -15 volume units.

Speakers/Audio Gateway Channels

If the speaker/audio gateway channel is set to an audio output volume of -25 volume units and receives a packet to start an audio page with a volume offset of +13 volume units, then the speaker will broadcast at an audio output volume of -12 volume units.

Speakers and audio gateway channels can be set within a threshold of -48 volume units and +28 volume units. Settings are changed by using the VIP-102B IP Solutions Setup Tool.

Volume Offsets for Audio Group Priorities

Volume offsets for audio group priorities are set in the VIP-102B IP Solutions Setup Tool under 'System' and then 'Volume Offsets'. This menu gives the option to set volume offsets based upon audio group priority levels. The levels can be set between -12 volume units and +12 volume units. Speaker and audio gateway channels that receive group audio simply add/subtract any group priority offset to their own volume unit setting.

Putting it all together

For example: a server with 'System Volume Offset' of -5 volume units and invokes an Audio Event that is set to +12 volume units. This Audio Event is sent to a group with a priority of 20. Priority 20 has been assigned a volume unit offset of -2. A speaker in that group has a volume unit offset of +12.

Leaving the server: $-5 + 12 = +7$ volume units

The group volume offset subtracts 2 volume units = $7 - 2 = +5$

The speaker in the group adds its volume offset of +12 to the group priority volume offset $5 + 12$, and the resulting audio is broadcast at +17 volume units.

In Practice

When setting up a new system, it's best to leave all offsets/volume adj set to 0. Set speaker and audio gateways channel output volumes as desired. Then apply offsets, only as needed.

VIP-102B Group Priorities vs. Server Group Priorities

The VIP-102B IP Solutions Setup Tool allows volume offsets to group audio based upon the group's priority. If the group is receiving audio from an Application Server event, then the group's priority and its associated volume offset is overridden by the event's priority and volume offset.

For example, an announcement to a group that has an assigned volume offset of +6 will result in the group members broadcasting the audio with an offset of 6 above their individual channel output volume presets.

An Application Server sending an audio event with an assigned volume offset of +2 to a group with an assigned volume offset of +6 will result in the group member broadcasting their audio with an offset of 2 above their individual channel output volume presets.

Priority Overrides

Although the server sets the priority of audio events on per event basis, higher priorities still prevail. For example, if group 999, assigned a priority of 50 in the VIP-102B IP Solutions Setup Tool, is currently receiving a live voice announcement, and the server sends audio to that group at a priority of 25, the audio sent from the server will not override the live voice announcement. If the audio from the server is still in progress at the conclusion of the live voice page, the group members will join the server audio stream at a new priority of 25.

Higher priority audio overrides lower priority audio. If multiple audio streams have the same priority, then they are processed on a first come/first serve basis.

Once higher priority audio has completed, any lower priority audio still in progress will be broadcast mid-stream.

Power/Maintenance

Power failures will cause an audible alert which may be silenced via the front panel “silent” button. The fault LED will also illuminate if there is a power failure or internal power circuit failure.

The battery LED will illuminate while the internal battery is not fully charged.

Power off

There are two methods to powering off a VE602x device. The first method is to power off the device through the User Interface in the browser. This method requires the user to log into the VE602x device through the browser as the admin. Next expand the Administration folder then expand the System folder. Select the Shutdown command and confirm that you would like to power off the device. The server will continue to operate for 20 minutes after the shutdown command is selected. The second method is to use the power button located on the VE602x device itself. There will be a small hole located to the right of the silent button. Use a paper clip to press the power button. Once the green power light is off unplug the power cord from the device.

Power on

To power on the VE602x device plug the power cord into the device. If the power light does not show green it means that the device still hasn't powered on. If that is the case take a paper clip and press the power button located in the small hole to the right of the silent button.

System servers should be powered through an adequately sized uninterruptable power supply. As of this writing, the bump in line switching power supplies for the servers each require 2 amps of current @ 100 – 240vac 50/60 Hz. The server should be installed in a climate and environment-controlled location. Periodically wipe the enclosure with a clean dry cloth to remove any dust and debris. A current backup of system programming should always be maintained in a secure location. Specifications are subject to change.

Modifying Text-To-Speech

There is a screen for editing the speed and pitch of the text-to-speech renditions. It may be accessed by visiting <http://<IP address of the Application Server>/neotts>.

SSML (Speech Synthesis Markup Language)

These settings are applied to all text-to-speech conversions performed by this unit, including eLaunch Alerts, Quick Page, and Audio File creation.

Paul

<p>Prefix:</p> <input type="text" value="<prosody volume = '50' rate = '1' pitch = '100'>"/>	<p>Suffix:</p> <input type="text" value="</prosody>"/>
--	--

The system defaults are:

Default Prefix: <prosody volume = '50' rate = '1' pitch = '100'>

Default Append: </prosody>

	Range	Default
Volume	0 - 100	50
Rate	.5 - 4	1
Pitch	50 - 200	100

For more information about SSML you can download [SSML-Manual](#).

Manually Controlling Application Server Audio Broadcasts

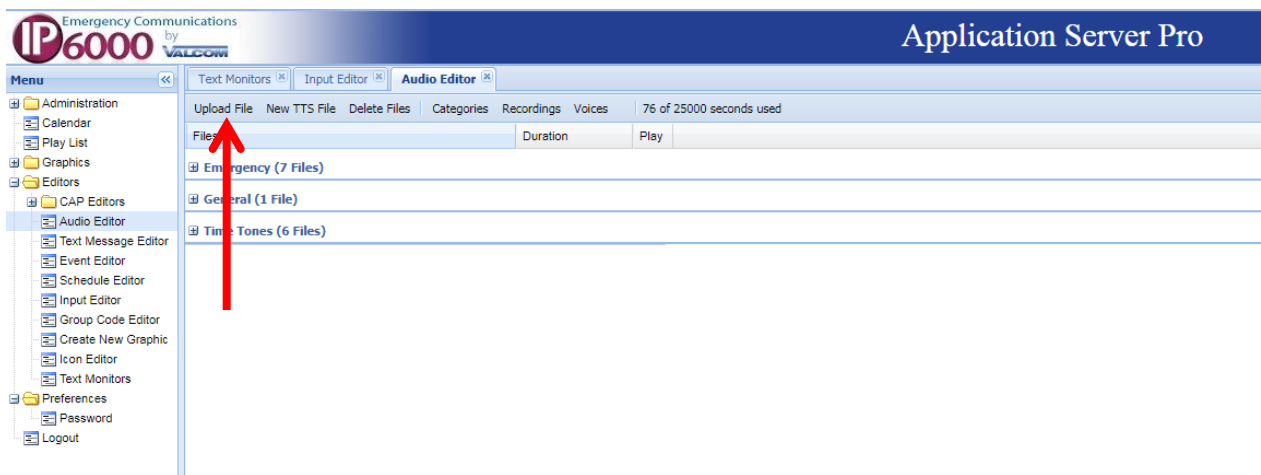
Manual triggering of audio from the Application Server may be accomplished via an external switch/button, and/or via another network device's data stream, such as [syslog](#).

Either of these external trigger options may be used to invoke a server Play List and therefore any audio events contained within that Play List.

The first step is to either upload a suitable audio file or create an audio file using the Server's text-to-speech capabilities.

Open Audio Editor

Upload the desired audio file (Upload File):



Upload New Audio File

File Description:

File Path:

Category:

Process Audio:

Audio files may also be created by recordings.
Refer to the Audio Editor section of this manual.

Or, create an audio file from text-to-speech (New TTS File):

New Audio TTS File

File Description: Evacuate the building

Category: Emergency

Text: All personnel evacuate the building immediately.

Note: Text (above) may include embedded SSML to control speech rate, volume, etc.

Voice: paul

Submit Cancel

Once you have completed adding the audio file, open Event Editor and create a new event (Create Event). Choose "Audio File" as the Event Type.

Emergency Communications by VALCOM

Application Server Pro

Menu: Administration, Calendar, Play List, Graphics, Editors (CAP Editors, Audio Editor, Text Message Editor, Event Editor, Schedule Editor, Input Editor, Group Code Editor, Create New Graphic, Icon Editor, Text Monitors), Preferences (Password, Logout)

Text Monitors | Input Editor | Audio Editor | Event Editor

Create Event Copy Event Delete Events Activate Stop STOP ALL

Event List:

- 9th Grade Tardy Bell
- Active Shooter
- Bell Tone Everywhere
- LED Sign Class Change Message
- Take Shelter
- Unlock Doors Relay
- Weather Alert

Select Event Type

Audio File Streaming Audio

Relay Control Test Room

Stop Delay

State Change Text Message

Uri Control Schedule

Cancel

Name the Event

Choose the audio file you created

Choose the groups(s) where you want the audio to broadcast

Click Submit

Create New Audio File Event

Event Name:

Hide:

Create Playlist:

Text to Speech:

Audio File:

Voice: paul

CAP field:

Send text also:

Duration (sec):

Number of plays: 1 0 -> Infinite

Gap (sec):

Page Delay (sec):

Volume Adj.: 0 dB

Override from CAP:

Priority: 25

Selected Codes

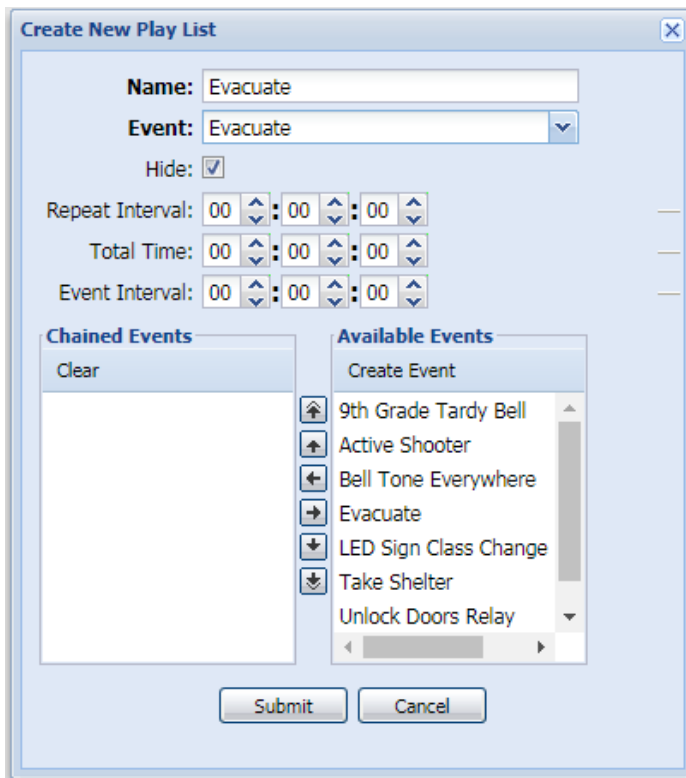
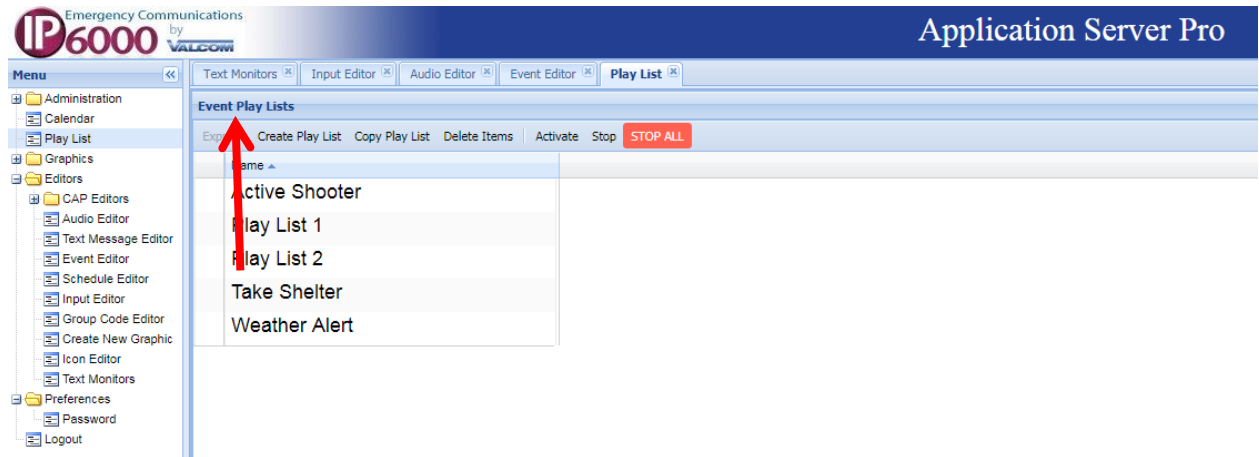
Clear

Available Codes

- 000 Emergency All Call
- 412 Testing Rooms
- 600 All Call
- 601 Outside

Submit Cancel

Create a Play List



For convenience sake, name the Play List with the same name you used for the controlled Event.

Choose the Event you wish to control.

Optional Steps

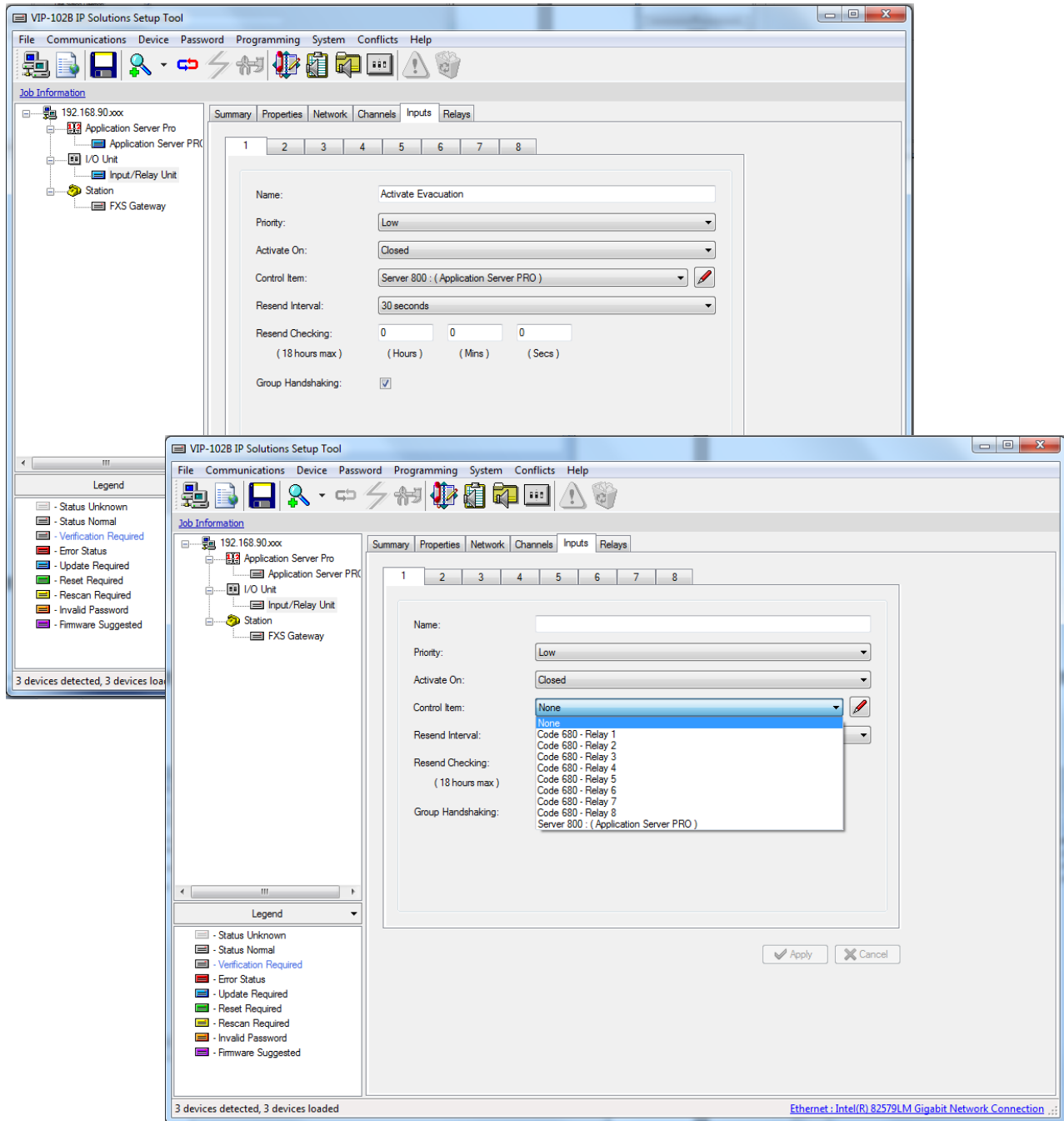
Define any desired Repeat Interval and Total play time.

Choose any chained events that will play sequentially after the initial event completes. If you choose chained events, you may define an Event Interval between chained events.

Click Submit to save your Play List

VIP-102B Steps

If manually triggering via external switches/buttons, those switch/button will connect to the IP6000 system via I/O gateways. The inputs on these gateways that will be used to trigger Play Lists on the server will need to have the server selected as the “Control Item”.

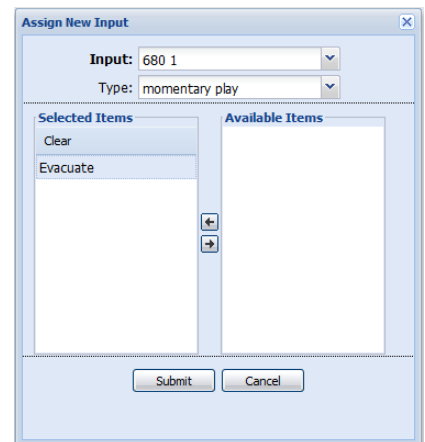
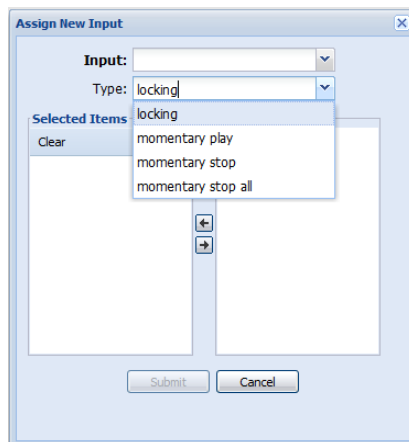
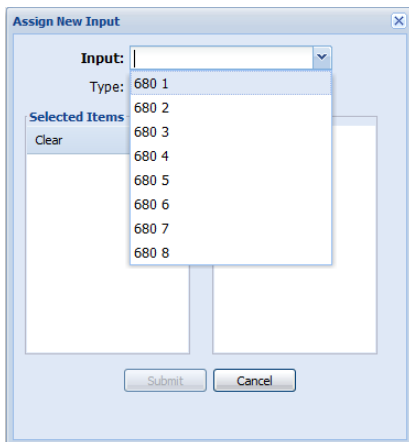
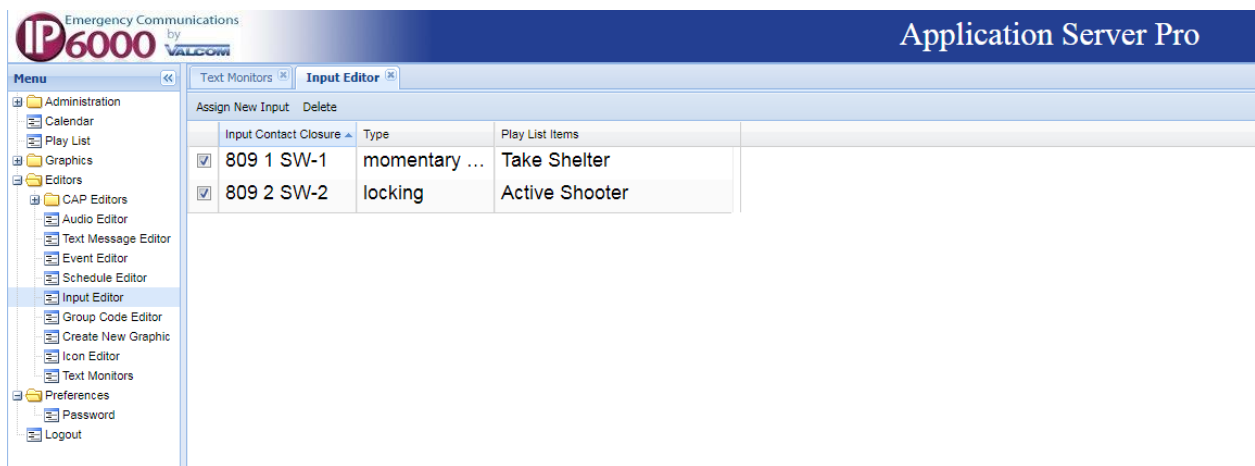


In the Application Server, use “Input Editor” to select the input, switch type (locking or momentary), and Play List(s) to activate. Locking switches activate the selected Play List items when the switch is locked on. If those Play List Items are actively distributing an audio file, delay, text message event or relay control “on” event, opening the locked switch will terminate the activity.

Play List Items controlling streaming audio, state change, stop, eLaunch, camera control or test room will not terminate when the locking switch is opened.

Momentary switches will play a play list item for its duration (if applicable) or until a stop command is received.

After these steps, the switch trigger should be functional.



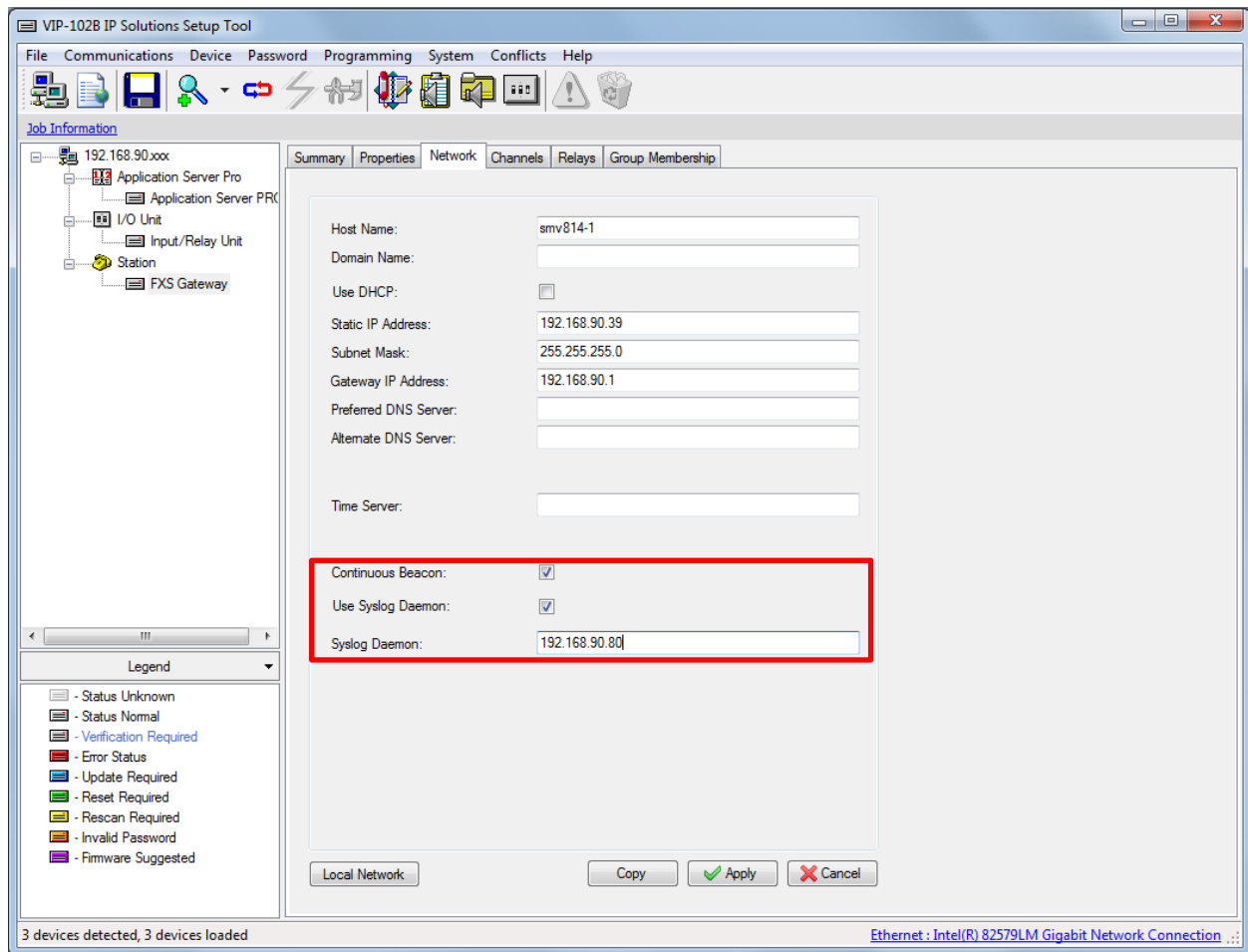
Manually Triggering Via Another Network Device's Data Stream

If manually triggering [via another network device's data stream](#), such as syslog, The triggering system must have its syslog data directed to the Application Server's IP address.

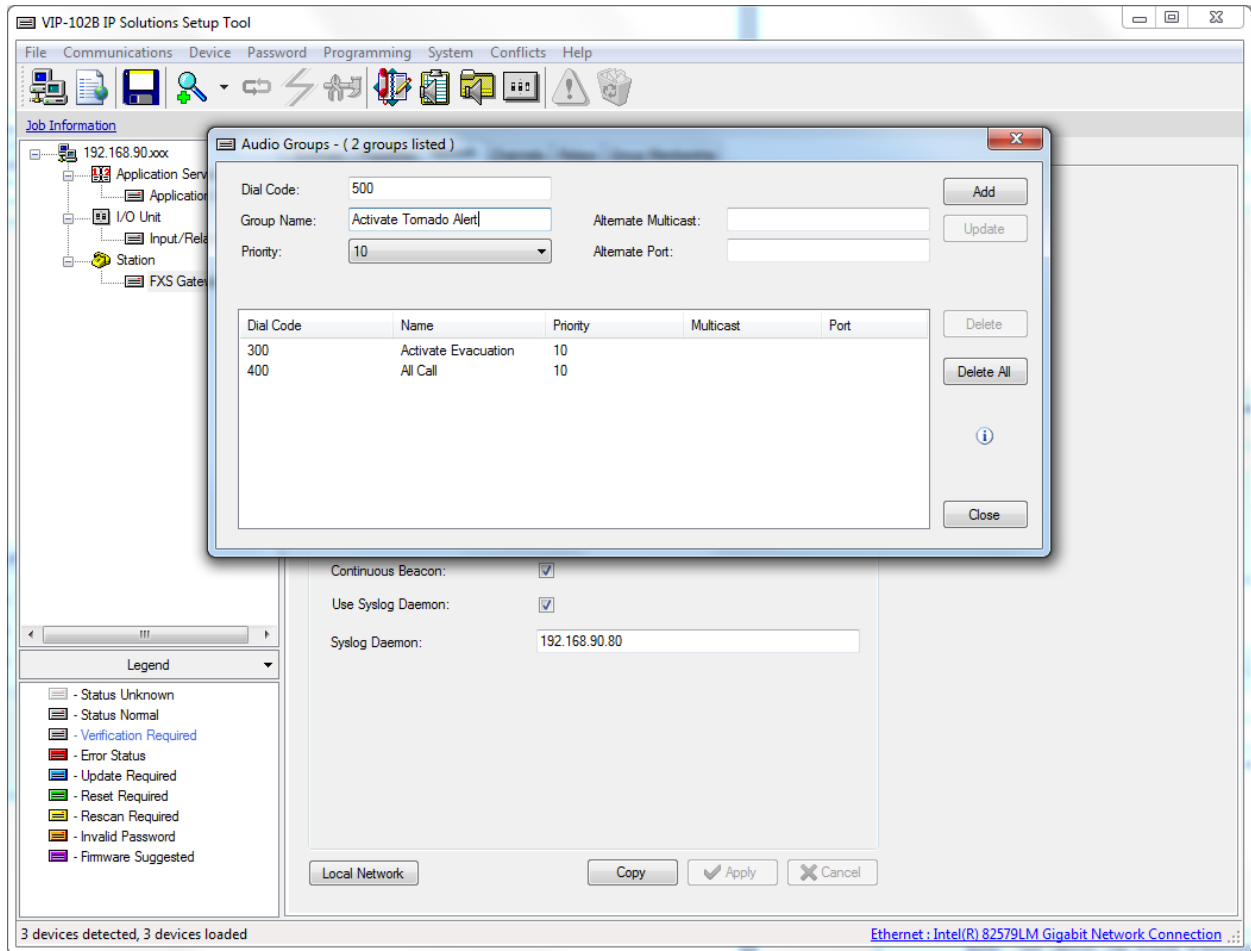
In this example, case, we will be monitoring an FXS gateway for group dial codes. When a phone connected to the FXS gateway channel dials the group code the Play List item will be triggered.

These group dial codes will be defined and allocated for the sole purpose of triggering a Play List.

In order to send data to the Application Server, the Syslog Daemon field of the FXS gateway's network tab must contain the Application Server's IP address. "Use Syslog Daemon" must be checked.

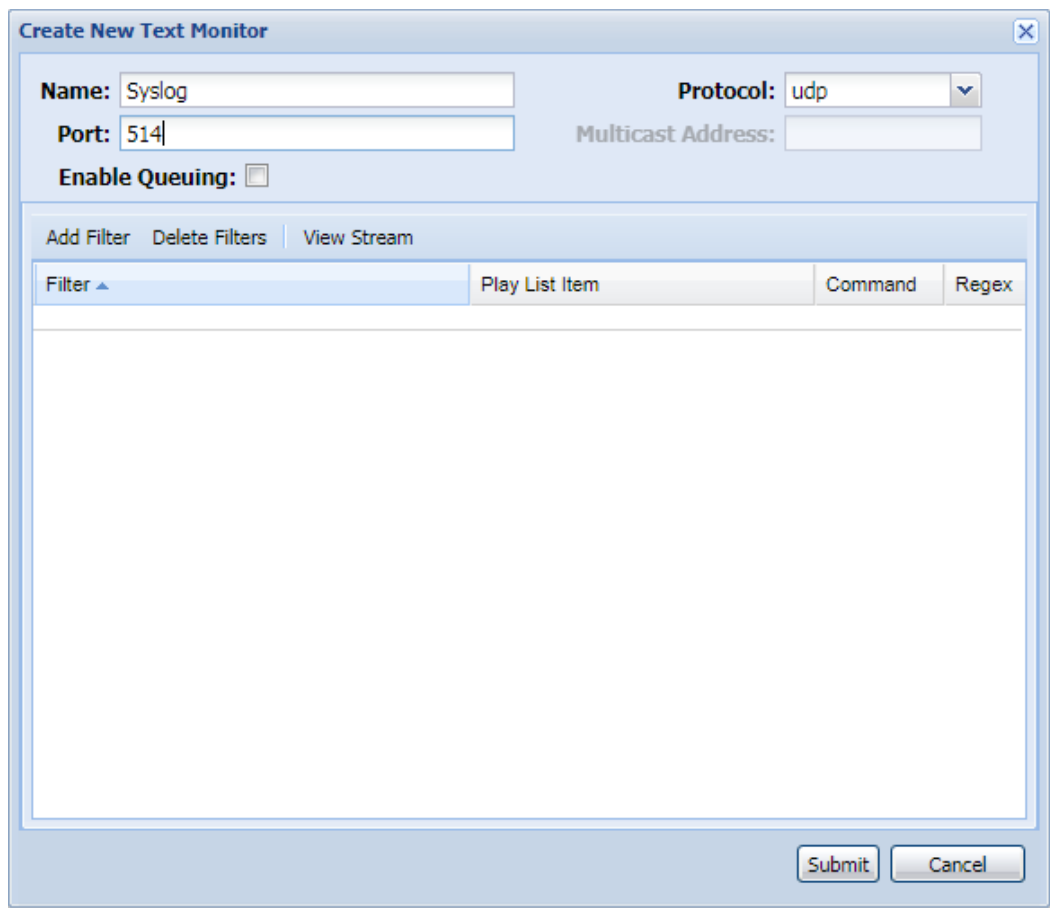
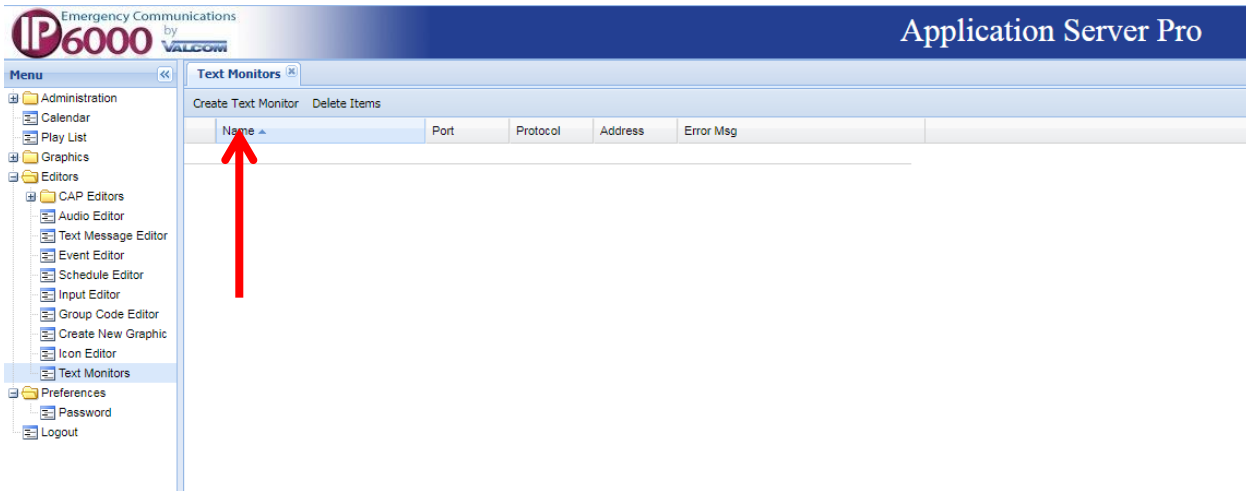


Then, create a group dial code to used as a trigger for each Play List.



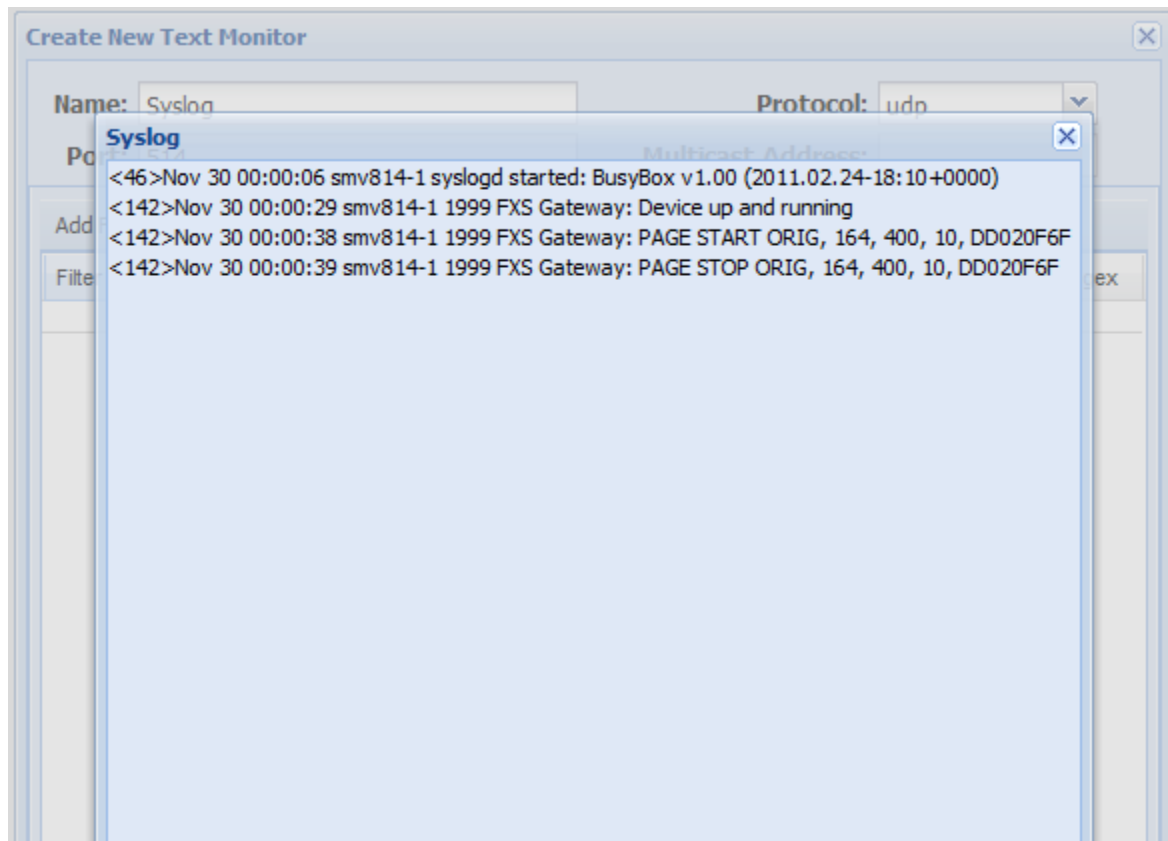
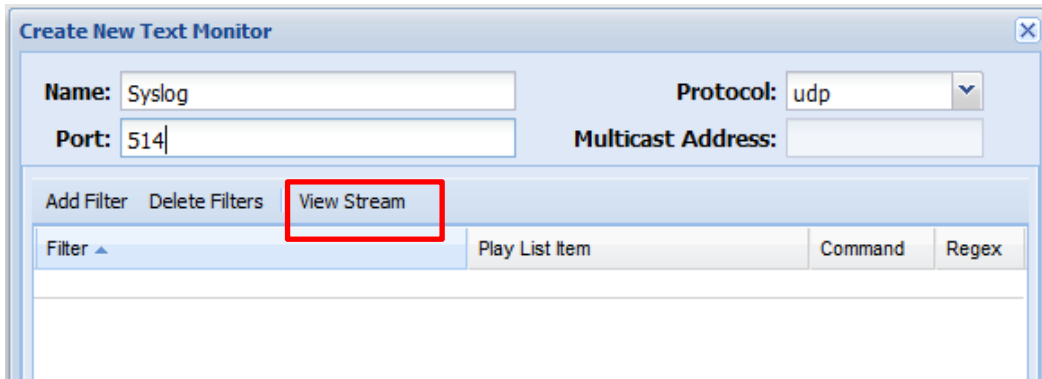
In the Application Server, go to Text Monitors

Click Create Text Monitor



Each text monitor is defined for a port number and a protocol. Then one or more filters are applied to monitor all incoming text data on the specified port, and in the specified format, for triggering phrases.

After creating the text monitor, generate some data from the triggering system and click “View Stream” (on the Create New Text Monitor screen) to identify a unique text string that may be used for triggering the Play List.



Once a unique text string is identified, click Add Filter and copy the trigger text to the Filter field. Choose the desired Play List item and Command.

The image shows two overlapping windows from a software interface. The background window is titled "Create New Text Monitor" and contains the following fields: "Name" (Syslog), "Port" (514), "Protocol" (udp), and "Multicast Address". Below these fields are buttons for "Add Filter", "Delete Filters", and "View Stream". The foreground window is titled "Create New Filter" and contains: a "Regex" checkbox (unchecked), a "Filter" text field containing "PAGE START ORIG, 164, 400", "Test String" and "Test Result" text fields (both empty), a "Play List Item" dropdown menu set to "Evacuate", and a "Command" dropdown menu set to "start". At the bottom of the "Create New Filter" window are "Save" and "Cancel" buttons. At the bottom of the "Create New Text Monitor" window are "Submit" and "Cancel" buttons.

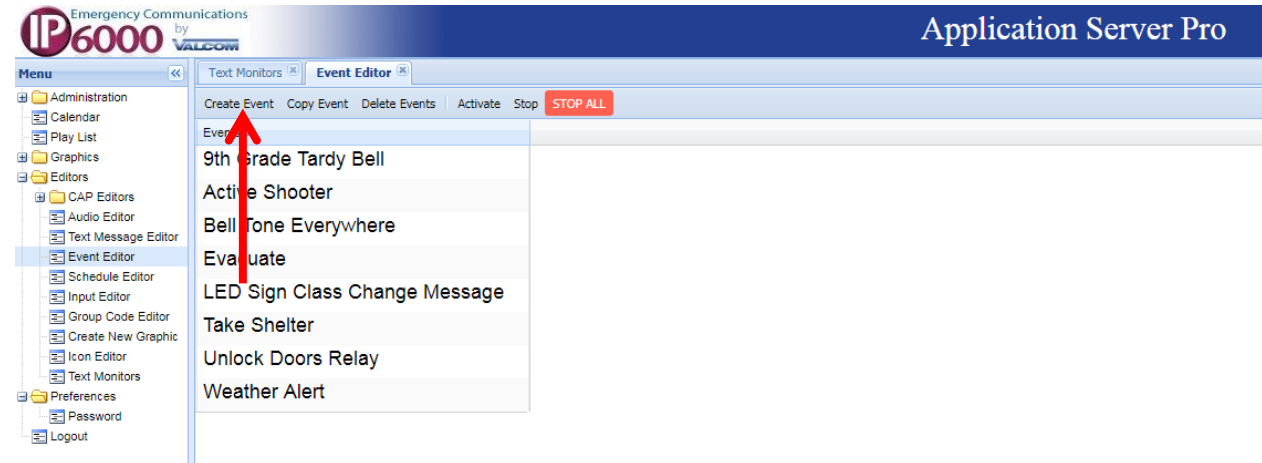
NOTE: "PAGE START ORIG, 164, 400" IS ONLY USED AS AN EXAMPLE. The actual text string captured from the data stream (generally syslog) will vary depending upon the gateway being monitored.

Click Save.

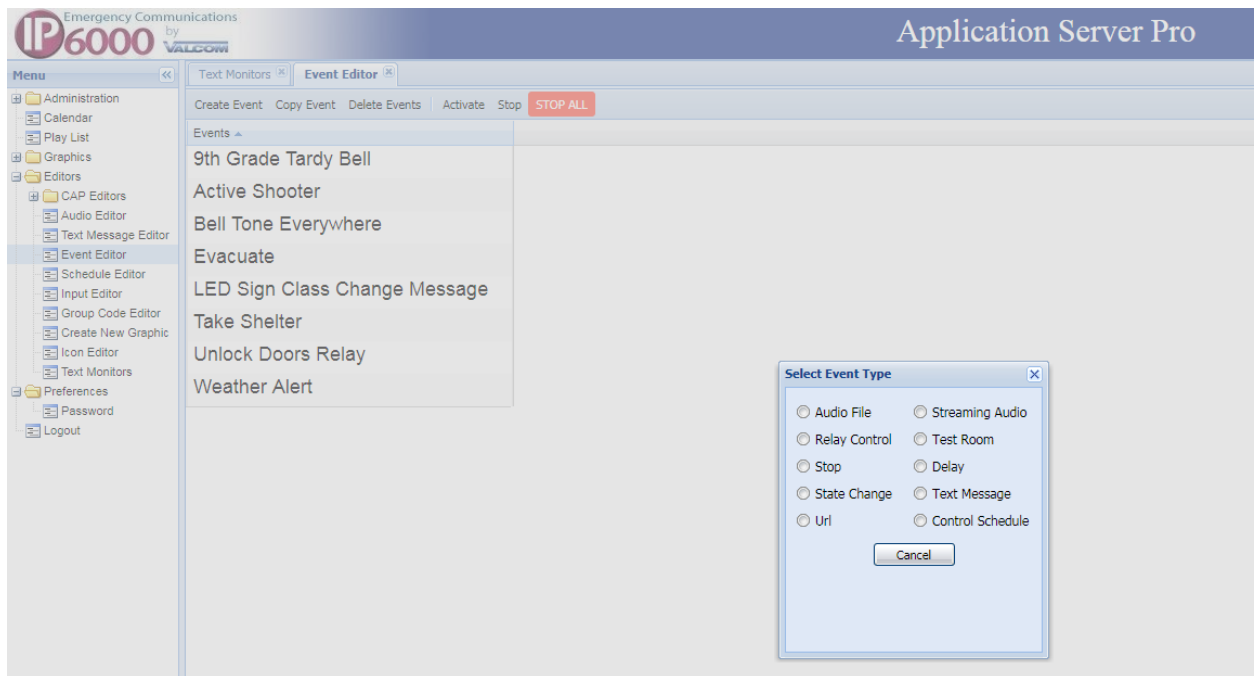
Repeat these steps as necessary. Note that a filter entry will be required for each unique trigger location. In our example, a trigger has been defined such that a specific endpoint channel, with dial code 164, must originate a broadcast to group 400 in order to trigger the Evacuate Play List Item. Additional filters may be added to trigger the Evacuate Play List Item from other endpoint channels.

Scheduling Audio

To [schedule audio](#), one or more Audio File Events should be created. Go to Event Editor and click Create Event.



Click select "Audio File" as the Event Type



On the “New Audio File Event” form, provide an Event Name comprised of the Event purpose and destination –i.e. “Tardy Bell Everywhere” or “Lunch Bell 1st Floor”

The screenshot shows a window titled "Create New Audio File Event". It contains the following fields and options:

- Event Name: [text input]
- Hide:
- Create Playlist:
- Text to Speech:
- Audio File: [dropdown menu]
- Voice: paul [dropdown menu]
- CAP field: [dropdown menu]
- Send text also:
- Duration (sec): [text input]
- Number of plays: 1 [text input] 0 -> Infinite
- Gap (sec): [text input]
- Page Delay (sec): [text input]
- Volume Adj.: 0 dB [dropdown menu]
- Override from CAP:
- Priority: 25 [text input]

At the bottom, there are two lists:

- Selected Codes:** [empty list with a "Clear" button]
- Available Codes:** 000 Emergency All Call, 412 Testing Rooms, 600 All Call, 601 Outside

Navigation arrows are between the lists. "Submit" and "Cancel" buttons are at the bottom right.

Then choose:

- 1) an audio file
- 2) a duration for the audio file (leave blank to play the file for its duration)
- 3) the number of times the audio file will play
- 4) the gap in seconds between plays (if applicable)
- 5) a delay to start the audio a few seconds after the event starts
- 6) any desired volume offset
- 7) the desired audio priority
- 8) which audio groups will receive the audio

Sample:

Create New Audio File Event [X]

Event Name:

Hide:

Create Playlist:

Text to Speech:

Audio File: [v]

Voice: [v]

CAP field: [v]

Send text also:

Duration (sec):

Number of plays: 0 -> Infinite

Gap (sec):

Page Delay (sec):

Volume Adj.: [v]

Override from CAP:

Priority:

Selected Codes

Clear

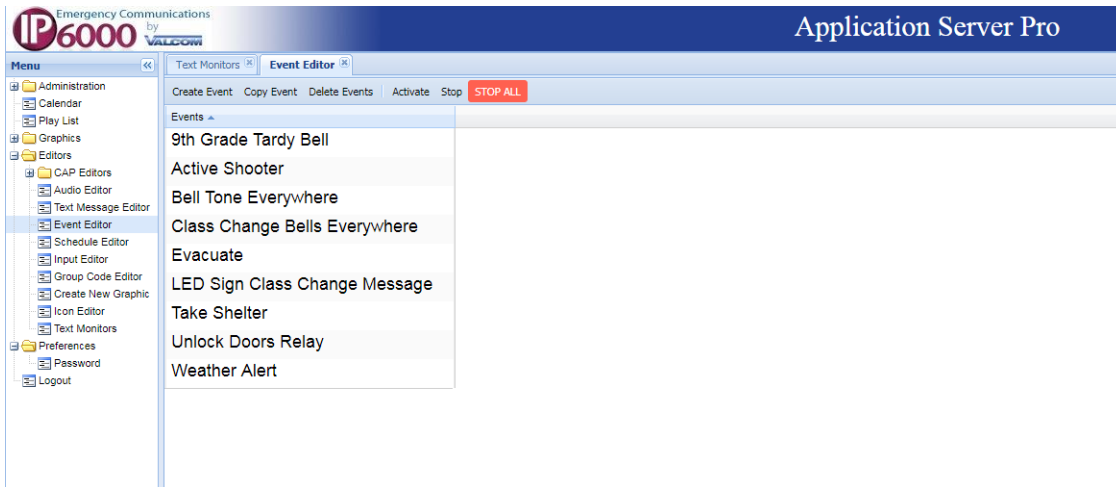
600 All Call

Available Codes

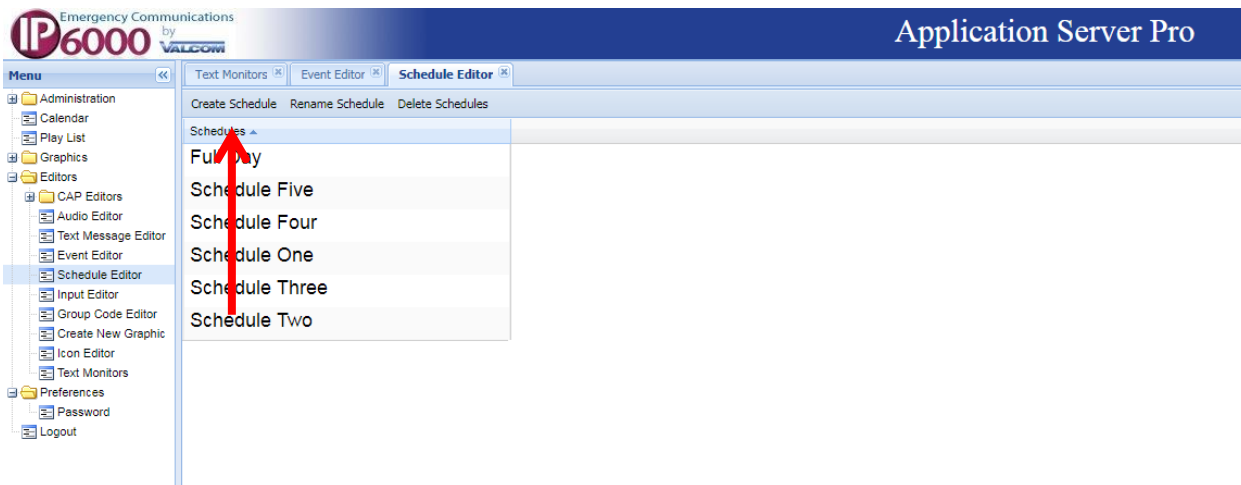
000 Emergency All Call
412 Testing Rooms
601 Outside

[←] [→]

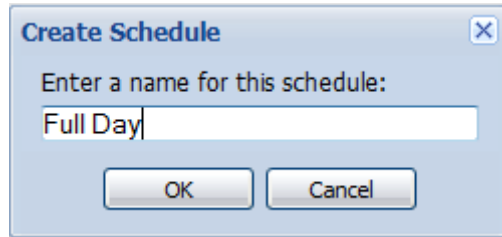
Repeat these steps as necessary to create additional Events.



Open Schedule Editor and click "Create New Schedule"

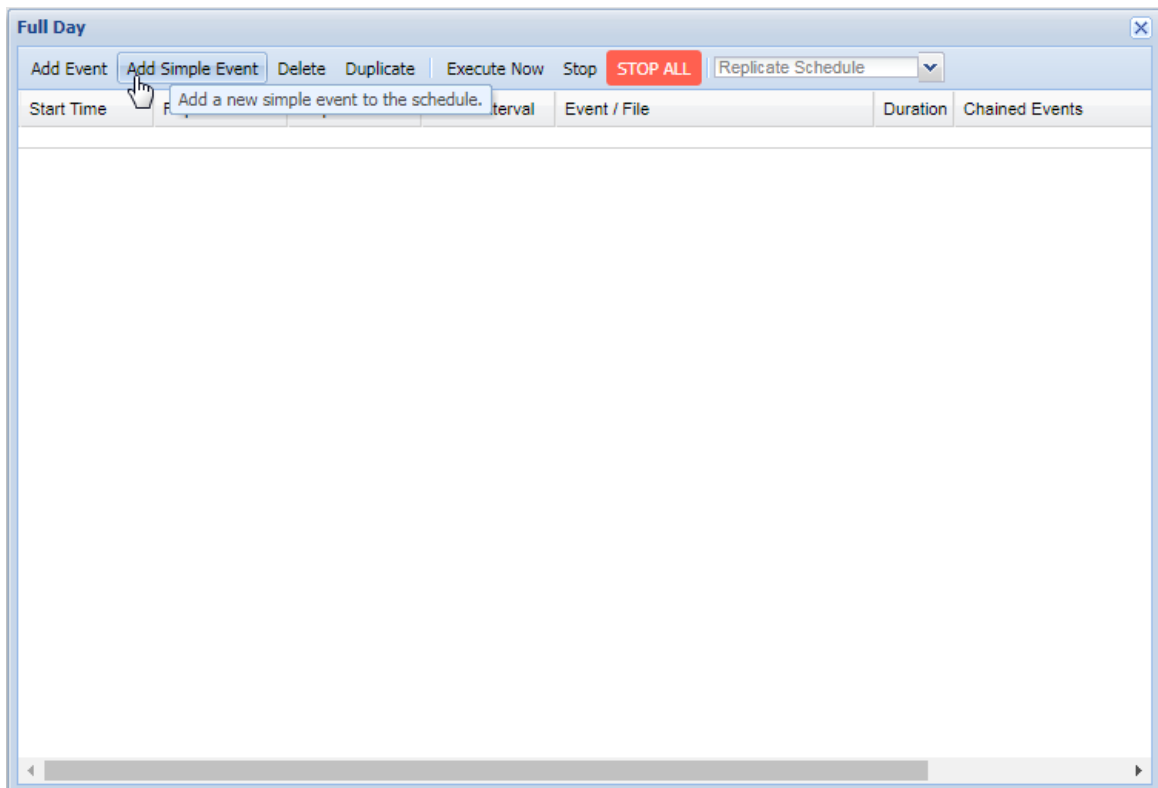


Name the schedule

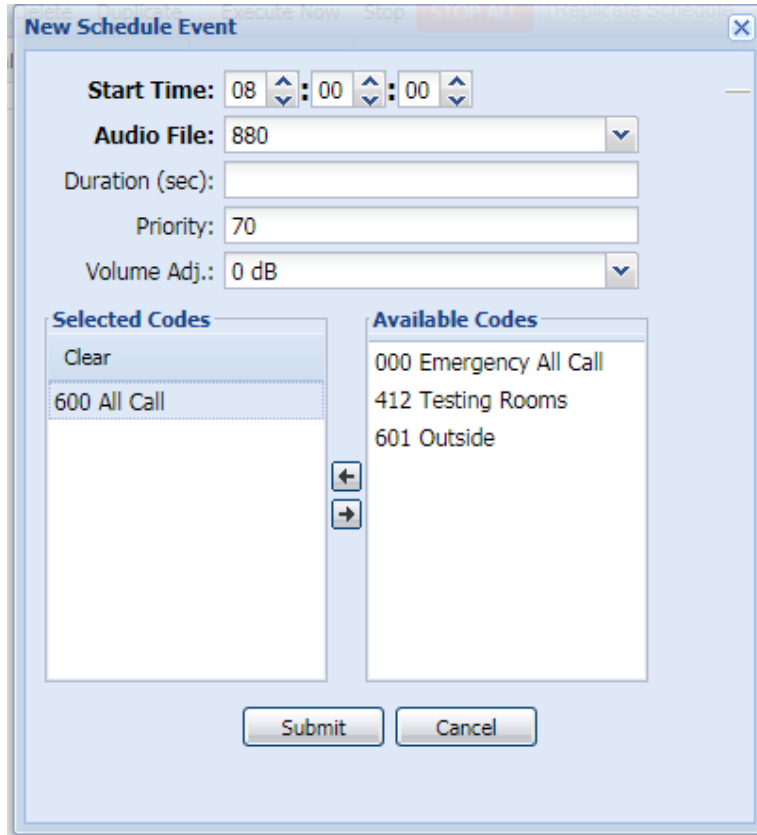


There are 2 ways to add Events to schedules.

There are 2 ways to add Events to schedules. Note that Simple Events should only be used to create “one off” events.

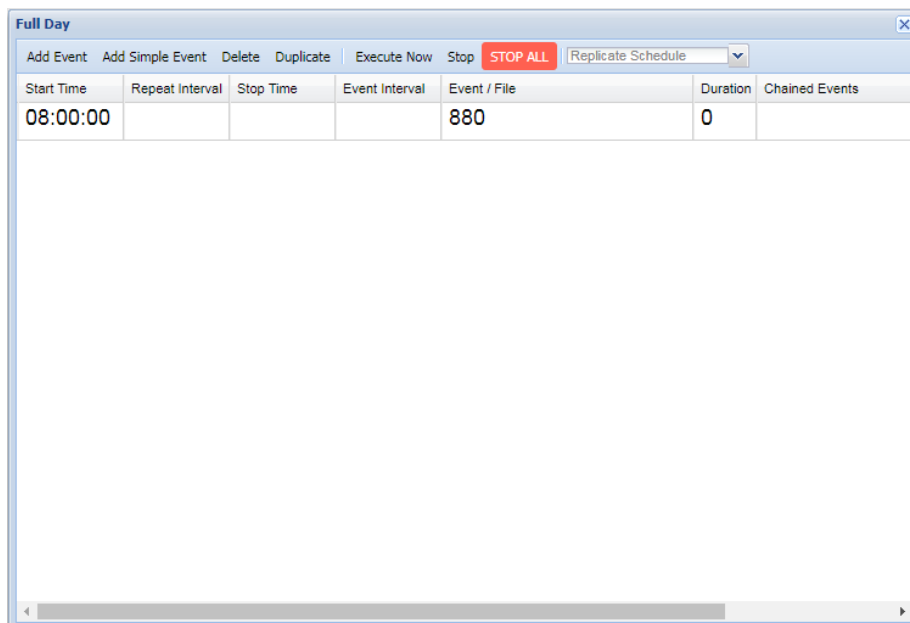


With "Simple Events", the Start Time, Audio File, Duration, Priority, Volume Offset and destinations are selected for each Event - **all times are entered using 24 hour format**



The 'New Schedule Event' dialog box contains the following fields and sections:

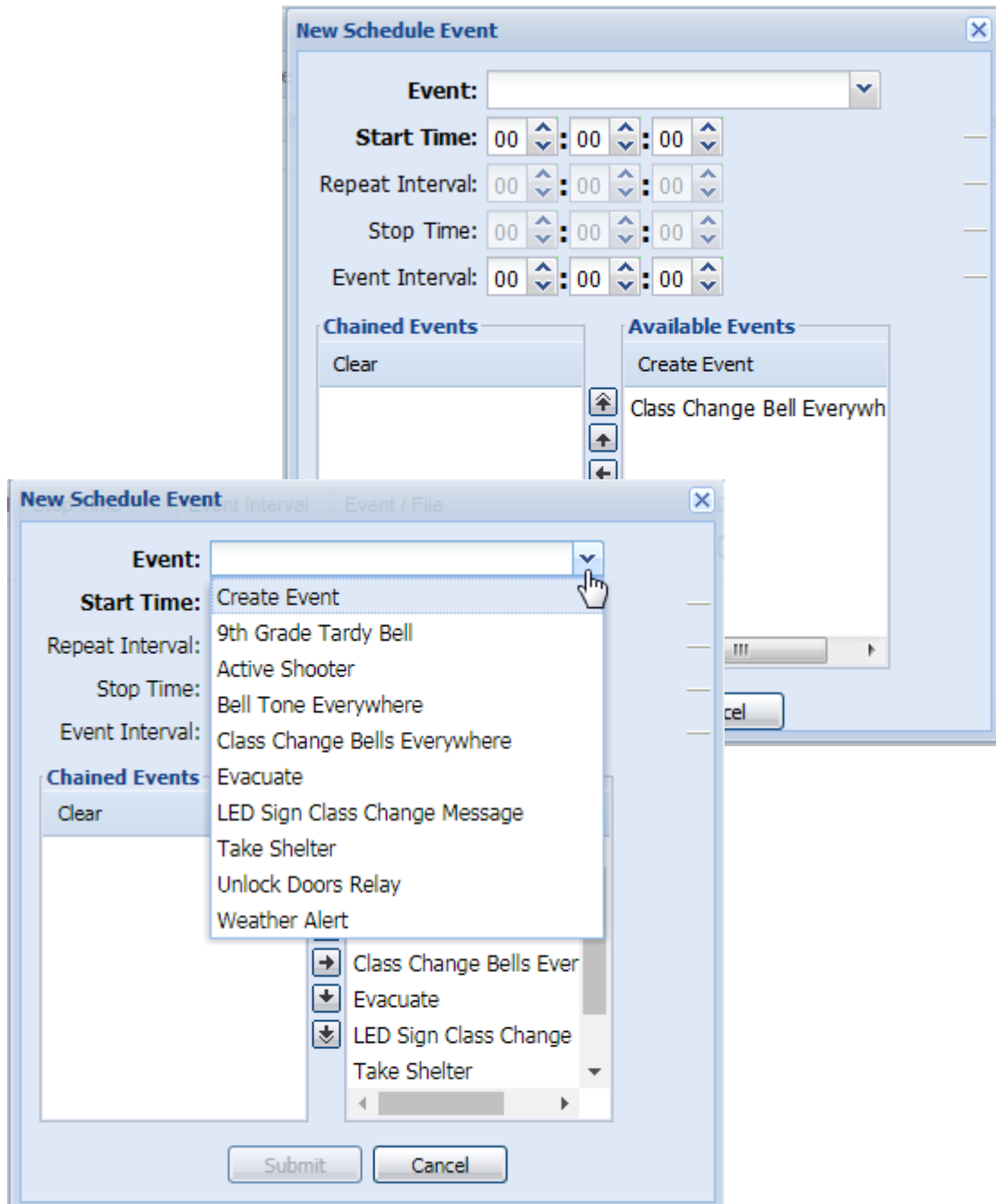
- Start Time:** 08 : 00 : 00
- Audio File:** 880
- Duration (sec):** (empty)
- Priority:** 70
- Volume Adj.:** 0 dB
- Selected Codes:** Clear, 600 All Call
- Available Codes:** 000 Emergency All Call, 412 Testing Rooms, 601 Outside
- Buttons:** Submit, Cancel



The 'Full Day' window displays a table with the following data:

Start Time	Repeat Interval	Stop Time	Event Interval	Event / File	Duration	Chained Events
08:00:00				880	0	

The easier method involves pre-defining the Events (as accomplished in our previous example) and simply adding those pre-defined Events to the schedule. Click “Add Event” and choose one of the previously defined Events



Enter the time that the Event will occur - **all times are entered using 24-hour format**

New Schedule Event Interval Event / File

Event: Class Change Bells Everywhere

Start Time: 08 : 15 : 00

Repeat Interval: 00 : 00 : 00

Stop Time: 00 : 00 : 00

Event Interval: 00 : 00 : 00

Chained Events

Clear

Available Events

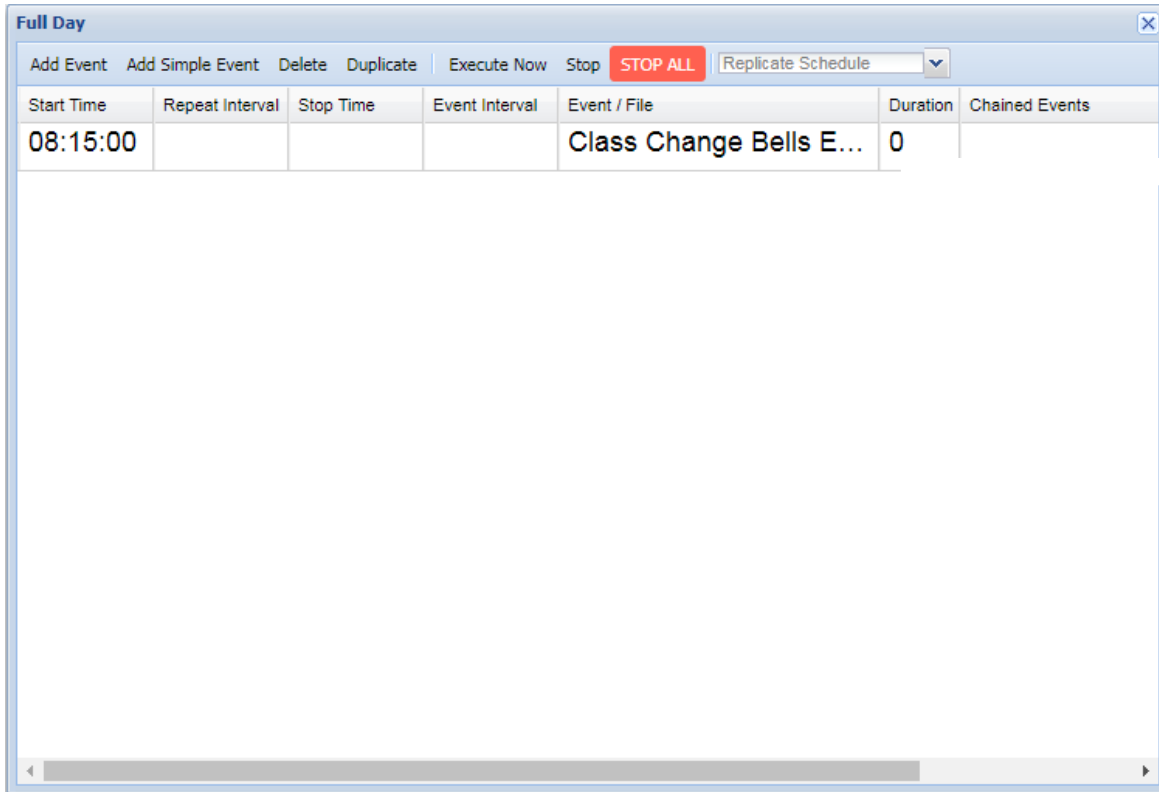
Create Event

- 9th Grade Tardy Bell
- Active Shooter
- Bell Tone Everywhere
- Class Change Bells Ever
- Evacuate
- LED Sign Class Change
- Take Shelter

Submit Cancel

Note: If Chained Events are selected from Available Events, they will play sequentially. The use of Chained Events in schedules is not typically required.

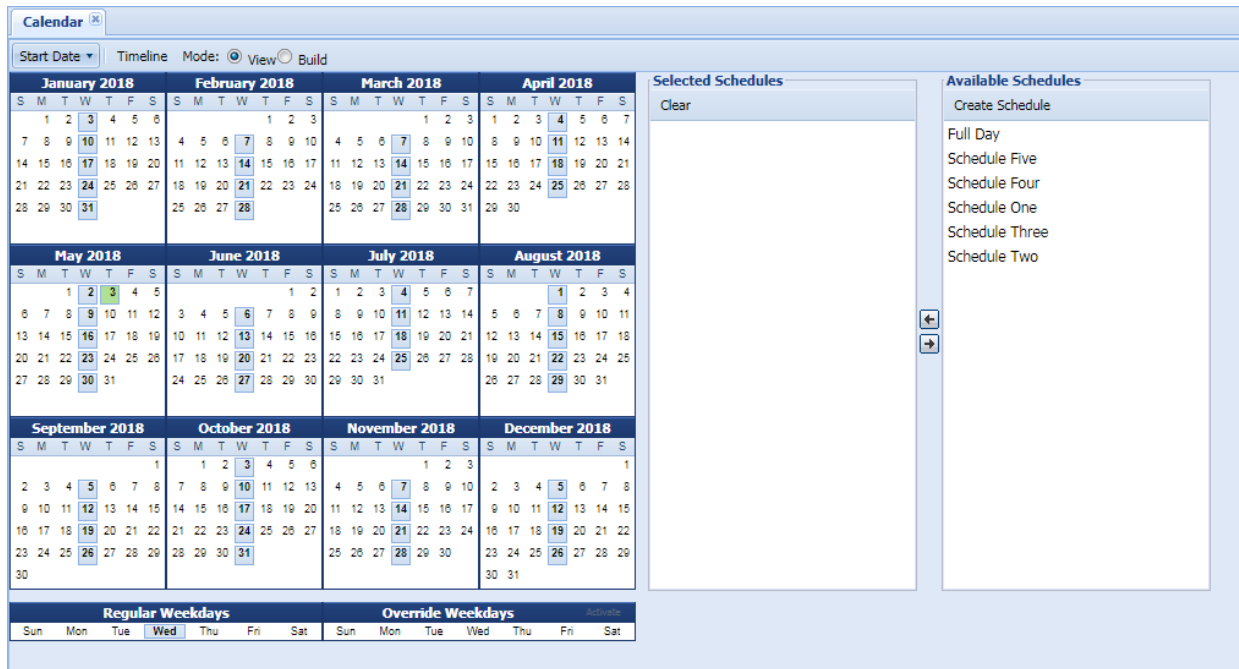
Example of Event successfully added



The screenshot shows a software window titled "Full Day" with a close button in the top right corner. Below the title bar is a menu bar with the following items: "Add Event", "Add Simple Event", "Delete", "Duplicate", "Execute Now", "Stop", "STOP ALL" (highlighted in red), and "Replicate Schedule" (with a dropdown arrow). Below the menu bar is a table with the following columns: "Start Time", "Repeat Interval", "Stop Time", "Event Interval", "Event / File", "Duration", and "Chained Events". The table contains one row of data:

Start Time	Repeat Interval	Stop Time	Event Interval	Event / File	Duration	Chained Events
08:15:00				Class Change Bells E...	0	

Choose "Calendar" from the menu tree



The Calendar form is used to define when system schedules will operate.

Individually click on Sun, Mon, Tue, Wed, Thu, Fri or Sat and move the desired default schedules for these days from Available Schedules to Selected Schedules.

Users may also choose to operate select schedules based upon calendar dates. This is accomplished by creating date groups. This is accomplished as follows:

Choose one or more dates from the Calendar by clicking Build and then clicking the desired dates. Once all dates have been selected, click View and choose one or more schedules to operate on the selected dates. Up to 365 date groups may be defined.

Calendar date groups may be modified as follows:

- a) **Remove a date from an existing date group** - Click Build and then double click the dates within a defined group. Once the date's background color is gone, the date is removed from the group. Click View to exit.
- b) **Add dates to an existing date group** – Click Build and then single clicking a date in any defined group, the background color will turn yellow and additional dates may be added to the date group. Click View to exit.

One time overrides may be enabled up to seven days in advance may be selected using Override Weekdays. Individually click on Override Weekdays Sun, Mon, Tue, Wed, Thu, Fri or Sat and move the desired Override schedules for these days from Available Schedules to Selected Schedules, then click activate. Override Weekdays schedule selections deactivate once complete.

Examples:

Schedules Assigned to Current Day of the week (Regular Weekdays)	Schedules Assigned to Current Day of the week (Override Weekdays)	Schedules Assigned to Current Date by way of a Calendar Date Group	Which Schedules actually operate?
2 and 3	none	none	2 and 3
2 and 3	none	1	1
2 and 3	4 and 5	1	4 and 5