

# stages™ Release Notes 2.6.5

October 2018



- 2.....[Highlights](#)
- 7.....[System Administration](#)
- 9.....[Dispatch](#)
- 11.....[Signal Processing](#)
- 15.....[Setup](#)
- 18.....[External Application](#)
- 19.....[Miscellaneous](#)

## HIGHLIGHTS

### Opt In

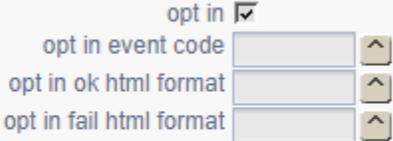
Stages™ can send out a notification for a subscriber to opt in to a service or feature. This will send out an email or SMS using an Auto Process with an Opt In URL. Clicking the URL will opt into the feature, and log an Event Code on the Site. That event code could generate an alarm or use an Auto Process to create a Memo.

The URL is built from variables including Site and Contact Info.

### Auto Process

A new field has been added for 'Opt In'. Once selected, pressing tab or saving will reveal more fields. 'Opt In Event Code' is the Event Code that will be logged to the Site when pressing the URL. 'Opt in HTML Format' defines which Email HTML Format houses the HTML Code that will display when the URL is pressed. 'Opt in HTML Fail Format' defines which Email HTML Format will be displayed if there is an issue with the URL link.

---



opt in

opt in event code  ^

opt in ok html format  ^

opt in fail html format  ^

In the Body of the Message, the variable '[OptInURL]' is entered to display the formatted URL with the Site and Contact Info imbedded.

If desired, the 'Opt In Event Code' can then be set up to trigger a Memo to the Data Entry department to update the account to enable the new feature.

### Email HTML Format

The HTML code for the URLs are defined in the Email HTML Format setup just as an outgoing email would be.

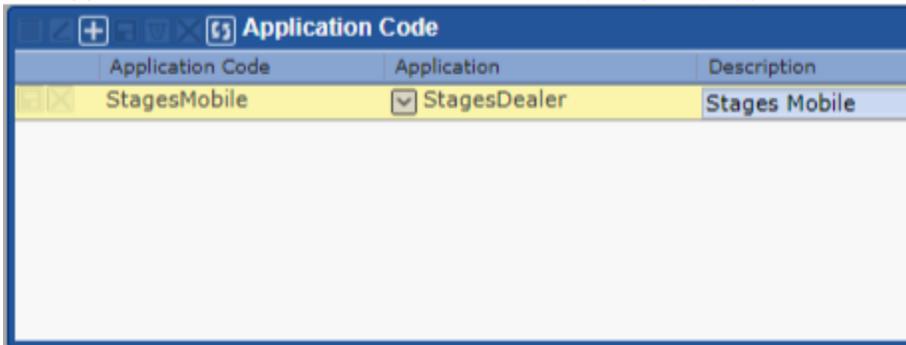
### Opt In URL Mask

A Task Parameter should be entered on Task 11 (Signal Processing) with a Parameter Name of 'OptInURLMask' and a value like 'https://server/path/{}' with 'Server' and 'Path' defined for where the Service is hosted. This will be used as the base for the [OptInURL] variable. The '{}' will be replaced by the Auto Process with specific data for that Site and Contact.

## Application Code – SQL Server Control

The Application Code represents a smaller group within an application #. For example, the Stages Mobile application is within Application #2. While Application #2 may be running on a specific SQL server, we can now define an application like the Stages Mobile application to run on a different SQL server. When switching an application code, the existing session will move to the new SQL server. Current users will move to the new SQL server automatically.

The Application Code must be defined. ([Utilities | stages™ | Application Code](#))



Application Code	Application	Description
StagesMobile	StagesDealer	Stages Mobile

## AppEngine.Config

The StagesGateway(s) servicing the Stages Mobile application must be used only for the Stages Mobile application.

The AppEngine.Config must list all SQL servers that may be designated to run this application.

The Application Code must be set. In this example, the Application Code is "DealerGroupA".

```
<AppEngine
  ApplicationNum="2"
  ApplicationCode="DealerGroupA"
  ApplicationName="Appengine Dev webservice"
  ApplicationTitle="Dealer Group A"
  GetWorkstationFlag="y"
  GoogleApiKey="AIzaSyCprQz1JInTmxs8iLpZmAeaPRpd1KxM_8o"
  MapApiKey="AIzaSyCprQz1JInTmxs8iLpZmAeaPRpd1KxM_8o"
  MapApiKeyType="key"
  ServerMessageType="http"
  HttpTimeoutSeconds="3600"
  SqlKeepAliveSeconds="30"
  SuppressChangePassword="N"
  IisTimeoutSeconds="30"
  SqlTimeoutSeconds="30"
  ValidateTypesFlag="Y"
  ClamServer="IDIIS01"
AllowServerPaths="N"
  >
  <Log LogAllErrors="N" />
```

## SQL Switching

(Utilities | Server Control | Server Application Control)

In the example below, Application #2 is running on Server #2 and the Stages Mobile application is following Application #2.

Applicat	App Name	Application Code	Application Code Descrip	Office	Active Server
1	StagesMonitoring			Secure Central Station	1-IDSQL1
▶ 2	StagesDealer			Secure Central Station	2-Beach
▶ 2	StagesDealer	StagesMobile	Stages Mobile	Secure Central Station	2-Beach(Application# 2)
3	StagesCustomer			Secure Central Station	1-IDSQL1
5	SGS Tickets			Secure Central Station	1-IDSQL1
7	SGSTicketsMobile			Secure Central Station	1-IDSQL1
9	Stages Guard			Secure Central Station	1-IDSQL1
10	Chat			Secure Central Station	1-IDSQL1
11	ExternalDispatch			Secure Central Station	1-IDSQL1

To move Stages Mobile to Server #1, press the button indicated below:

Applicat	App Name	Application Code	Application Code Descrip	Office	Active Server
1	StagesMonitoring			Secure Central Station	1-IDSQL1
▶ 2	StagesDealer			Secure Central Station	2-Beach
▶ 2	StagesDealer	StagesMobile	Stages Mobile	Secure Central Station	2-Beach(Application# 2)
3	StagesCustomer			Secure Central Station	1-IDSQL1
5	SGS Tickets			Secure Central Station	1-IDSQL1
7	SGSTicketsMobile			Secure Central Station	1-IDSQL1
9	Stages Guard			Secure Central Station	1-IDSQL1
10	Chat			Secure Central Station	1-IDSQL1
11	ExternalDispatch			Secure Central Station	1-IDSQL1

Application #2 is on Server #2 | Stages Mobile application is on Server #1.

Applicat	App Name	Application Code	Application Code Descrip	Office	Active Server
1	StagesMonitoring			Secure Central Station	1-IDSQL1
▶ 2	StagesDealer			Secure Central Station	2-Beach
2	StagesDealer	StagesMobile	Stages Mobile	Secure Central Station	1-IDSQL1
3	StagesCustomer			Secure Central Station	1-IDSQL1
5	SGS Tickets			Secure Central Station	1-IDSQL1
7	SGSTicketsMobile			Secure Central Station	1-IDSQL1
9	Stages Guard			Secure Central Station	1-IDSQL1
10	Chat			Secure Central Station	1-IDSQL1
11	ExternalDispatch			Secure Central Station	1-IDSQL1

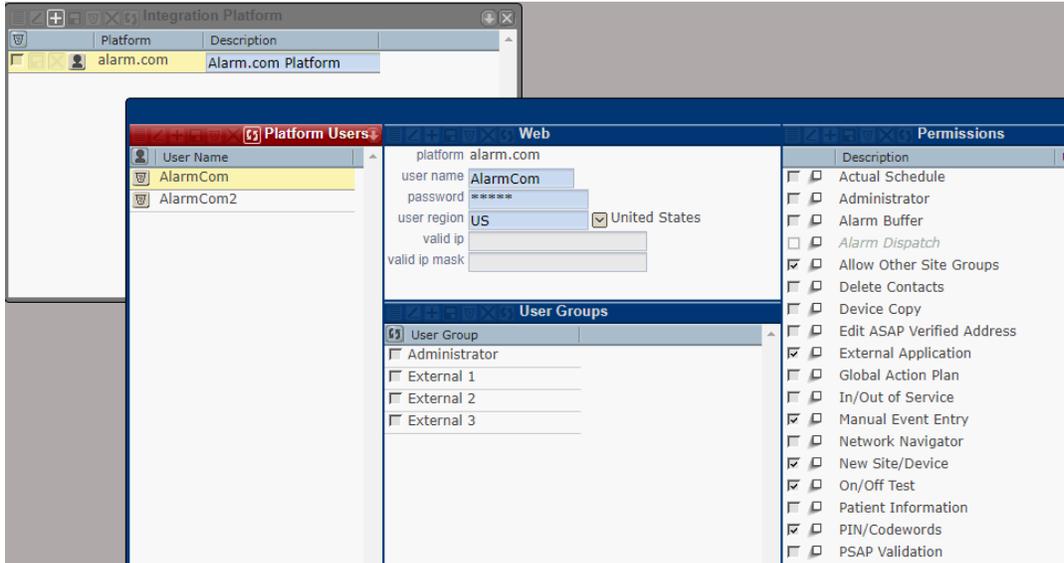
Reset the Application Code to follow the Application #. The Application Code must be on the same SQL server as the Application #. When connected to this SQL server, there is a function to reset the Application Code to follow the Application #.

Applications					
Applicat	App Name	Application Code	Application Code Descrip	Office	Active Server
1	StagesMonitoring			Secure Central Station	1-IDSQL1
2	StagesDealer			Secure Central Station	1-IDSQL1
2	StagesDealer	StagesMobile	Stages Mobile	Secure Central Station	1-IDSQL1
				Secure Central Station	1-IDSQL1
				Secure Central Station	1-IDSQL1
7	SGSticketsMobile			Secure Central Station	1-IDSQL1
9	Stages Guard			Secure Central Station	1-IDSQL1
10	Chat			Secure Central Station	1-IDSQL1
11	ExternalDispatch			Secure Central Station	1-IDSQL1

**Follow Application #.**  
 From now on this Application Code will follow the Application Number.

## External Application – Integration Platform Users

Users can be defined on the Integration Platform Setup window ([Setup | Device Setup | Integration Platform](#)). These users will have access to the External Application – Application #2 and will be able to access **any** accounts where the Device is assigned to the Integration Platform. For example, if 'alarm.com' is defined as an Integration Platform, any users defined on the alarm.com Integration Platform will have access to all alarm.com accounts.

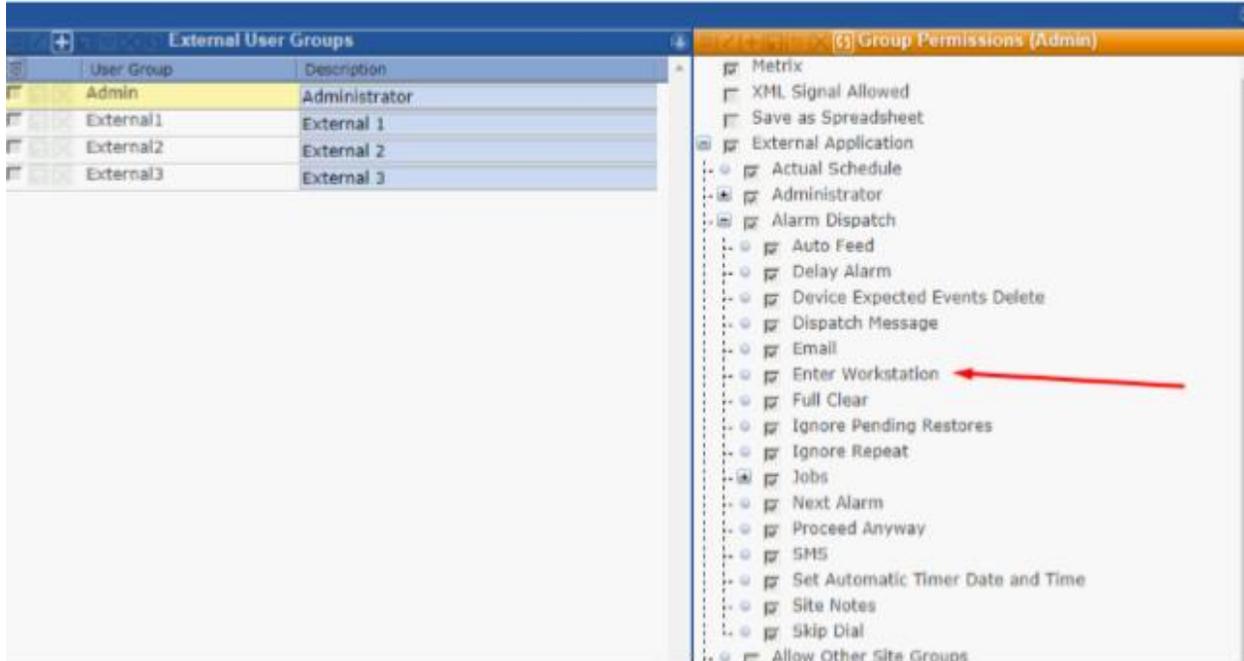


## SYSTEM ADMINISTRATION

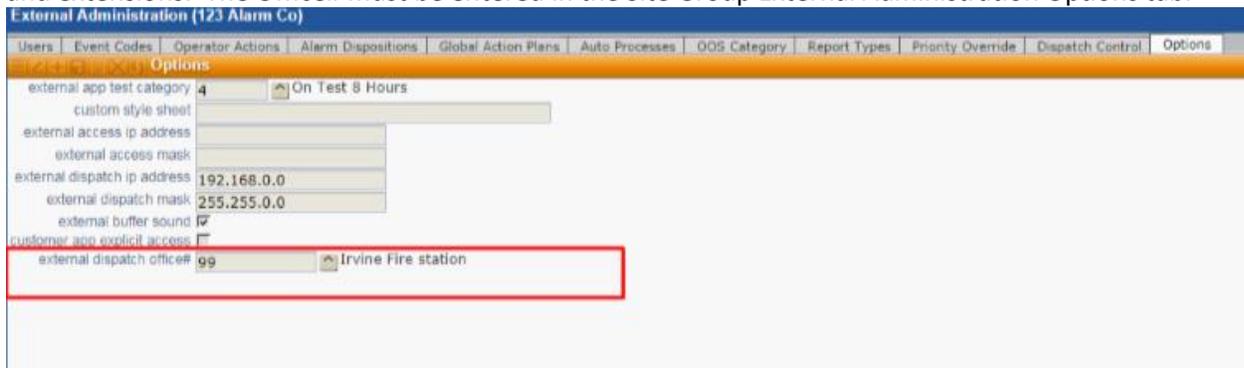
### External Application – Manually Enter Workstation

For alarm dispatching in the external application, the autodial feature requires that the application know which workstation/extension is running the application. If this cannot be determined by reverse DNS, stages™ can be configured to allow the user to manually identify the workstation.

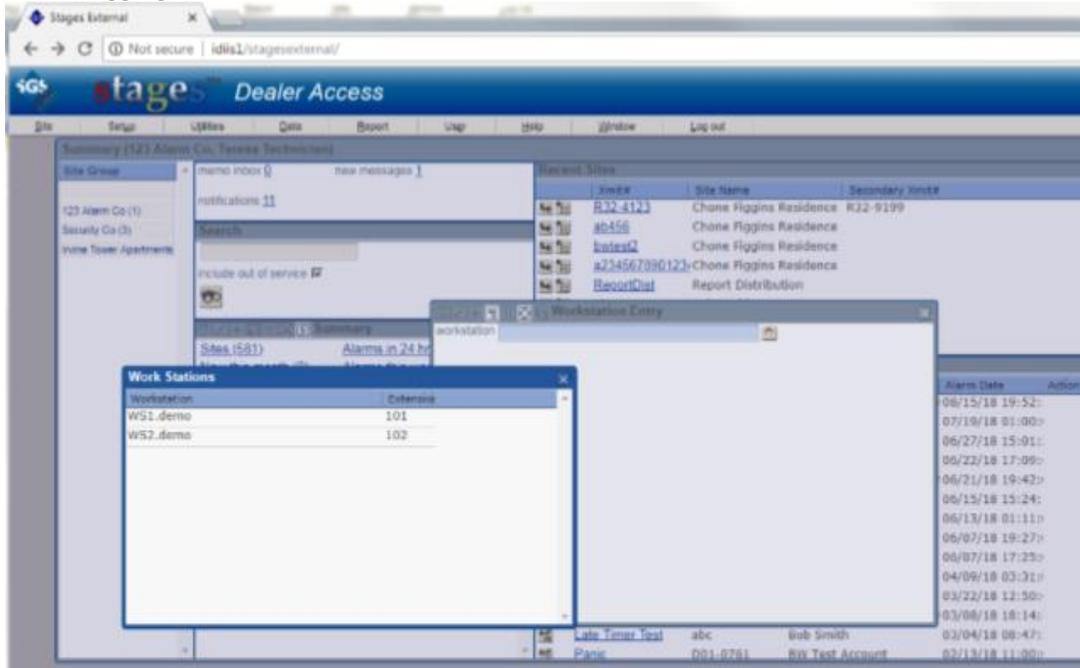
User Permission – The user must have the ‘Enter Workstation’ permission.



Office – An Office must be defined for the Site Group. This office must have a list of workstation names and extensions. The Office# must be entered in the Site Group External Administration Options tab.



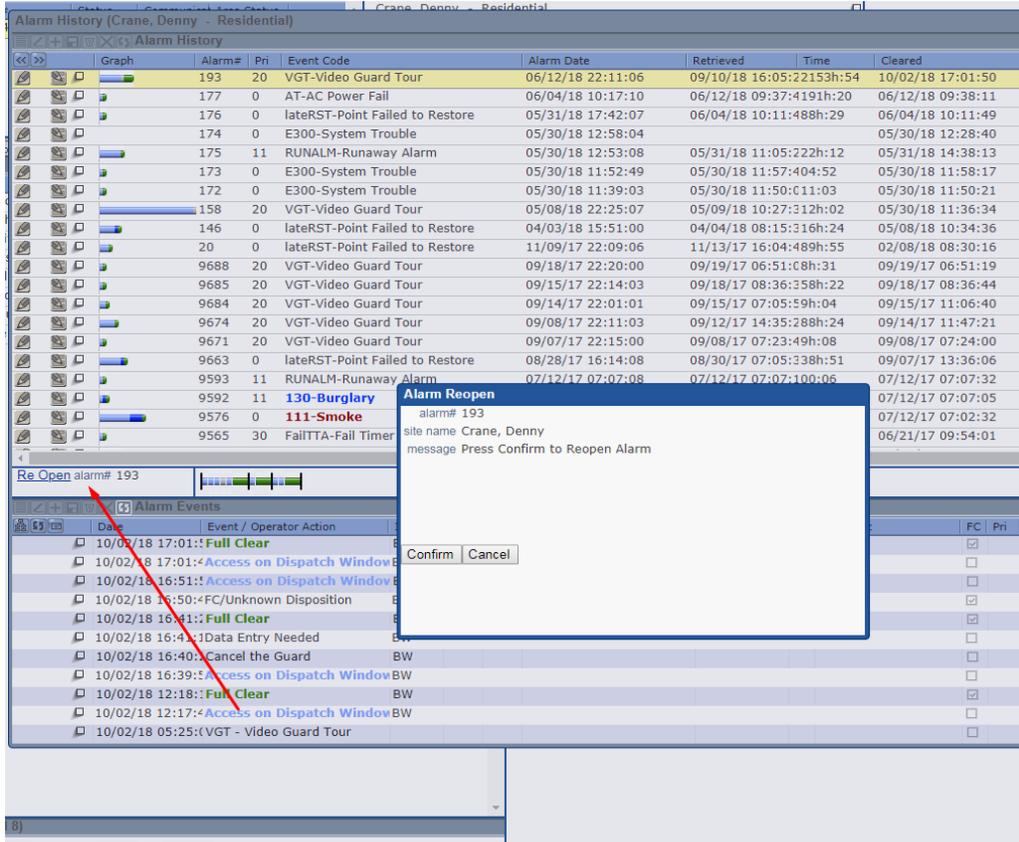
When logging in, the user is able to select the workstation.



# DISPATCH

## Reopen Alarm

There is a new stages™-generated operator action, 'Reopen', which allows a previously full-cleared alarm to be reopened. As an example, after an alarm has been cleared, an operator may receive an inbound call from an agency, dealer, or end user requesting some specific further action. All actions taken will still be associated with the originating Alarm#. If there is a Partial Clear Priority set on this operator action, alarms will be reopened with this priority. Otherwise, the alarm will be reopened with the priority of the original alarm.



This feature has a new securable:

[SiteAccess](#) / [SiteInformation](#) / [AlarmHistory](#) / [AlarmReopen](#)

## **Event Code**

Three new Event Code Options have been implemented:

- 1) OnTestCat=xxx (where 'xxx' represents the Test Category)
- 2) ClearTestCat=xxx (where 'xxx' represents the Test Category)

When an event with either of these options is logged, the Device will be placed on test or cleared from test.

- 3) AddDispatchType=xxx (where 'xxx' represents the Dispatch Type)

When an event with this option is logged, the Dispatch Type will be added to the Site.

## **ASAP Address Override**

A Mail Address with an "ASAP" usage can override fields when sending dispatch to ASAP. The Name field has been added as a field that can be overridden; in this case it will override the Site Name.

## SIGNAL PROCESSING

### XML Signal Service

Additional security methods have been added to the XML Signal Service.

All XML Signal Service tasks must have one of the following Task Options:

[LoginApp2] = An Application #2 Username and password is required with each signal.

[Login] = An Application #1 Username and password is required with each signal.

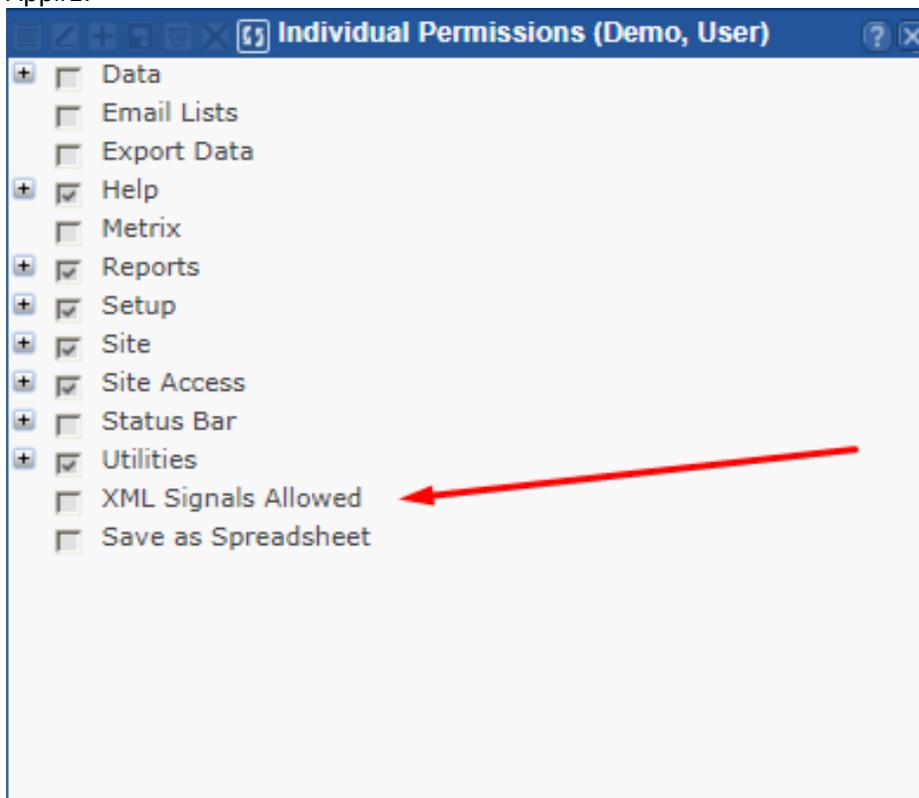
[Nologin] = No Login required.

**Warning:** The Nologin option should only be used when access to the Signal Service webservice is controlled by a VPN (or other network configuration) limiting access to a known party.

After the Task Option is set, the task parameters of Login and LoginApp2 can be removed.

For the LoginApp2 and Login options, the user sending in XML signals must have permission to send signals.

App#1:



## App#2:

The screenshot displays the 'External Administration (Dana's Site Group)' interface. The top navigation bar includes tabs for Users, Event Codes, Operator Actions, Alarm Dispositions, Global Action Plans, Auto Processes, OOS Category, Report Types, Priority Override, Dispatch Control, and Options. The 'Users' tab is active, showing a table with columns for Name, User Name, PIN, Effective Date, and Expire Date. A user named 'Lucky Thirteen' with User Name '13' and PIN 'shamrock' is listed.

Below the table, there are sections for 'Web' (user name, password, user region, valid ip, valid ip mask), 'User Groups' (Administrator, External 1, External 2, External 3), and 'Notification Subscriptions' (Subscription, Memos to Me, etc.).

The 'Permissions' section on the right lists various actions and their associated User Groups (all 'Administrator'). A red arrow points to the 'XML Signals Allowed' permission, which is currently unchecked.

If the user is an App#2 login, the signal must be for a Site that the user is allowed to access. When the user does not have access to the account, Event Code '!013' will be generated on the Task### account.

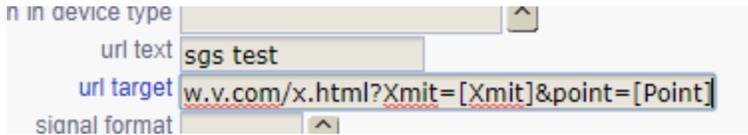
The screenshot shows the 'Detail' view for an event code '!013'. The fields are as follows:

- event code: !013
- description: Account Access not allowed
- priority: 0 (Priority 0)
- signal status: [dropdown menu]
- service type: [dropdown menu]
- delay seconds: [input field]
- alarm: [checkbox]

## Build URL from Signals

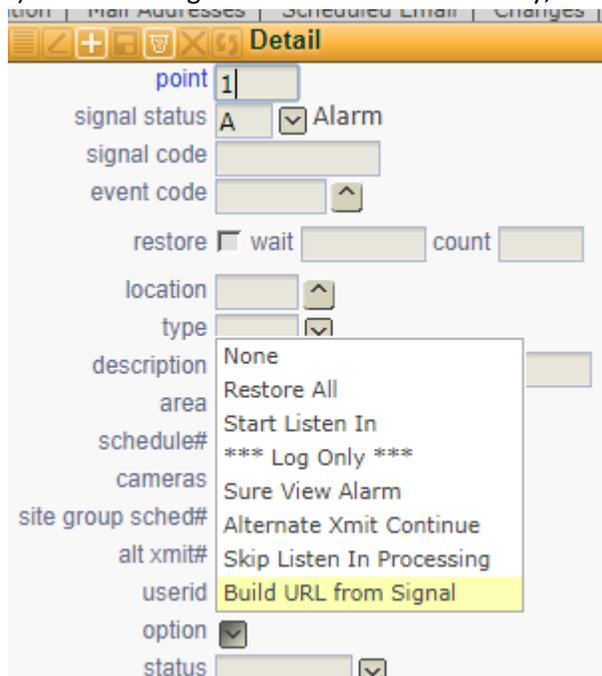
stages™ can build a targeted URL to display or launch to a Video Platform from an Incoming Signal using the Xmit# and Zone when the Signal does not send a URL. This has been done specifically for Chekt Video, but may be potentially used for other platforms as well.

- 1) In the Device tab in Site Data Entry, the 'URL Target' field supports the [Xmit] and [Point] variables.



The screenshot shows the 'Device' tab in Site Data Entry. The 'url target' field is highlighted and contains the text: `w.v.com/x.html?Xmit=[Xmit]&point=[Point]`. Other fields visible include 'url text' with 'sgs test' and 'signal format'.

- 2) In the Configuration tab in Site Data Entry, a new Option, 'Build URL from Signal', is available.



The screenshot shows the 'Configuration' tab in Site Data Entry. A dropdown menu is open for the 'option' field, showing several options. The option 'Build URL from Signal' is highlighted in yellow. Other options include 'None', 'Restore All', 'Start Listen In', '\*\*\* Log Only \*\*\*', 'Sure View Alarm', 'Alternate Xmit Continue', 'Skip Listen In Processing', and 'userid'.

- 3) In Site Summary and the Action Plan, the URL will be built from the first signal of the Alarm:

[www.v.com/x.html?Xmit=sgs888&point=1](http://www.v.com/x.html?Xmit=sgs888&point=1)

- 4) In History, the URL will be built for each signal that matches a zone with the Option to 'Build the URL', using the format in the Device URL Target.



The screenshot shows the 'Recent History' table in Site Data Entry. The table has columns for Xmit#, Initials, Event / Operator Action, Signal, Point, Description, and User Name. The first row shows a signal with Xmit# 'sgs888', Initials 'SGS', Event 'Operator Accessed', Signal 'BA', Point '1', and Description 'test'.

Xmit#	Initials	Event / Operator Action	Signal	Point	Description	User Name
sgs888	SGS	Operator Accessed	BA	1	test	

**Auto Process – Serial Notifications**

A new field, 'Serial Notify Expire Event Code' has been added. Use this field to log an event when there is no response to any of the serial notifications.

**Operator Action – Ignore Repeat Trips**

A new Operator Action Option, 'ClearIgnoreRepeat' has been implemented. When an operator action with this option is logged, all Ignore Repeat entries for the Device will be removed. When the Point is null, matching Event Code/Signal Code combinations will be ignored.

## SETUP

### Jurisdiction Requirements

[\(Setup | stages™ Setup | Jurisdiction\)](#)

The Locality Requirements window introduced in the 2.6.4 release to allow the defining of permits at the Locality level has been replaced with the Jurisdiction Requirements window.

New securables are **Jurisdiction** and **JurisdictionWrite**.

Jurisdiction Type	Jurisdiction Name	City	State	Zip	County
Unincorporated County	Orange County Ca		CA	92705	Orange

Agency Type
Police

agency type Police

permit required: PREQ1 (PREQ One)

permit instruction: [dropdown]

ordinance phone#: [text]

broadcast and file:  No

private response only:  No

ecv option: [dropdown]

sia cp01 panel:  No

multiple trips requirement: [dropdown]

permit responsible: [dropdown]

verified response: [dropdown]

permit rule: [dropdown]

rp response time: [text]

agency permit comment: [text area]

alarm coordinator: [dropdown]

renewal responsible: [dropdown]

subscriber list frequency: [dropdown]

subscriber list from: [dropdown]

ordinance uri: [text]

permit uri: [text]

Jurisdiction Types are defined in the corresponding setup window.

[\(Setup | stages™ Setup | Jurisdiction Type\)](#)

Jurisdiction Type	Description	Order#	Ignore City
Borough	Borough	2	<input type="checkbox"/>
City	City	4	<input type="checkbox"/>
Township	Township	3	<input type="checkbox"/>
Unincorporated	Unincorporated County	1	<input checked="" type="checkbox"/>

A Site can be assigned a Jurisdiction and its corresponding requirements.

Site

site name Chone Figgins Residence

address 12651 Dunas Rd  
Santa Ana, CA 92705 USA

region CA ^ California

time zone 5 ^ (GMT-08:00) Pacific Time (US & Canada); Tijuana

site type R v Residential

language [ ] v

runaway threshold [ ] ^

info Lots of Seats, "Big Scoreboard". Very crowded for a few hours on some days in the summer. Fireworks on Fridays. more wtf. this works a b

jurisdiction ^ Orange County Ca [Requirements](#)

Clicking on the 'Requirements' hyperlink will display the Jurisdiction Requirements for the Site.

Jurisdiction Requirements (Orange County Ca)

Jurisdiction Requirem Detail

Agency Type	
Police	agency type Police
	permit required PREQ One
	permit instruction
	ordinance phone#
	broadcast and file No
	private response only No
	ecv option
	sia cp01 panel No
	multiple trips requirement
	permit responsible
	verified response
	permit rule
	rp response time
	agency permit comment
	alarm coordinator
	renewal responsible
	subscriber list frequency
	subscriber list from
	ordinance url
	permit url

The existing Site Audit for Permits will also consider applicable Jurisdiction permit requirements.

## Site Group Setup

Email Addresses can now be entered for a Site Group.

Phones			
	Phone	Ext	Phone Type
<input type="checkbox"/>	213.333.1113		Work

Email Addresses	
Email Address	Auto
yourdealer123@gmail.com	<input checked="" type="checkbox"/>

## SMS Vanity Numbers

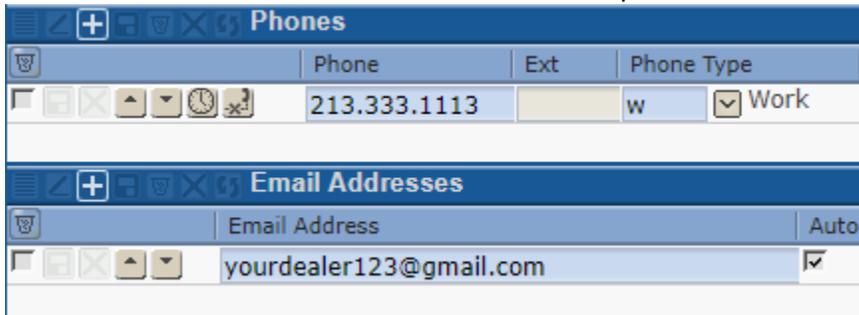
Stages™ now allows for separate phone numbers for sending SMS messages for a Site Group. This requires the SMS phone numbers to be established with the SMS service. Refer to the field help text for more information.

sms from phone#	1-800-ALARMCO
sms service	ABC

## EXTERNAL APPLICATION

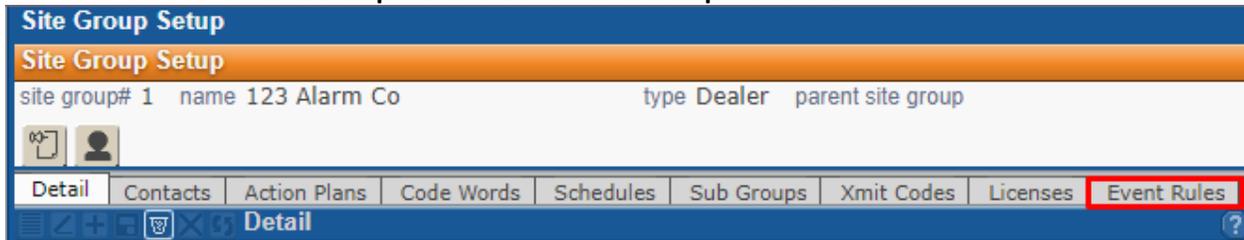
### Site Group Setup

Email Addresses can now be entered for a Site Group.



Event Rules can now be entered for a Site Group.

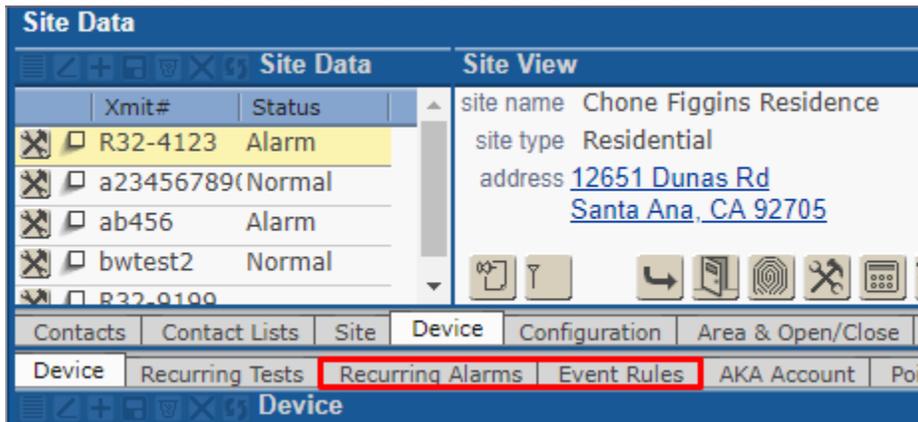
New securables are **XtSiteGroupEventRule** and **XtSiteGroupEventRuleWrite**.



### Device

Recurring Alarms and Event Rules can now be entered for a Device.

New securables are **XtDeviceEventRule** and **XtDeviceEventRuleWrite**.



## MISCELLANEOUS

### New Search Windows

The 'Additional Site Groups' field, ([Xmit Code Control](#) | [Xmit Assignment](#) | [Create Xmit Codes](#)), now utilizes a complex search window with input parameters.

**Site Group Multiple Select**

 site group#   
site group   
site group type

Selected	Site Group#	Site Group	Site Group Type
<input type="checkbox"/>	1	123 Alarm Co	Dealer
<input type="checkbox"/>	3	Security Co	Dealer
<input type="checkbox"/>	4	Taco Bell Restaurants	Franchise
<input type="checkbox"/>	5	Woodbridge Home Owners Assoc	Home Owners Association
<input type="checkbox"/>	9	Joe's Installer Company	Installing company

The 'Zip Select' field ([Mail Address Detail](#), [Site Address](#), [Site Address No Service](#)), now utilizes a complex search window with input parameters.

**Zip Select**

city   
state    
zip code   
county   
township



**Zip Select**

City	State	Zip	County	Township
Irvine	CA	92603	Orange	
Irvine	CA	92604	Orange	Woodbridge
Irvine	CA	92618	Orange	

## Alarm Statistics Detail

The address fields for the Site have been added to the Flyout on the list results.

The screenshot displays the 'Alarm Statistics' interface. On the left, there are various filters and controls: start date (09/01/18), end date (10/11/18), bucket minutes (60), group by (Priority), dispatch groups (10), priorities (0-), operators (Ad), interval set, site group, time format (M), and alarm time (checked). A magnifying glass icon is visible at the bottom left.

The main area shows a table of alarm statistics. A flyout menu is open over the first row, displaying the following details:

Alarm#	Pri	Event Code	Alarm Date
3500020901	1	GA-GAS ALARM	09/12/18 16:4

The flyout menu also includes the following address information:

- address: 37 Corporate Park
- address2: Suite 100
- city: Irvine
- state: CA
- zip code:

Below the main table, there is a section for 'Alarm Statistics' with a 'Priority Group' dropdown. The 'First Response' is set to 'Co'.