



# PassagePoint Global Administrator's Manual

---

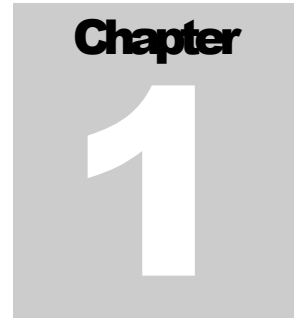
The information in this document is subject to change without notice. No part of this document may be reproduced without the express written permission of STOPware, inc.

Copyright © 2017 STOPware, inc. All rights reserved.

## Table of Contents

Chapter 1 – Introduction.....	4
WHAT IS PASSAGEPOINT GLOBAL? .....	4
USES FOR THE SOFTWARE .....	4
SUPPORTED HARDWARE .....	4
Badge Printer .....	4
Business Card, ID/License & Passport Scanners .....	4
Photo Capture Devices .....	5
Barcode Scanners.....	5
Signature Capture Devices .....	5
Biometric Fingerprint Scanners.....	5
INSTALLATION OPTIONS .....	5
CONFIGURE SYSTEM .....	5
OPERATING SYSTEM REQUIREMENTS .....	6
Chapter 2 – User Administration .....	8
ABOUT USER ADMINISTRATION.....	8
AUTHENTICATION RULES .....	9
Rule Options .....	11
USER ROLES .....	11
USER ACCOUNTS .....	13
Chapter 3 – Communication Settings.....	15
E-MAIL SERVER SETUP .....	15
E-MAIL TEMPLATES .....	15
ALERT CONFIGURATION.....	17
Chapter 4 – System Lists .....	19
AGREEMENTS.....	19
DESTINATIONS & PLACES.....	23
DESTINATION RULES.....	24
PEOPLE CATEGORIES.....	25
WATCH LISTS .....	28
WORKGROUP .....	30
LISTS.....	31
Chapter 5 – Badge Designer .....	35
Stock Sizes.....	35

- Badge Designs ..... 36
- Chapter 6 – Policy Manager ..... 43
  - Screen Policy..... 43
  - Barcode Scan Policy..... 45
  - Badge Printing Policy..... 47
  - Sign-in Kiosk Profiles..... 48
- Chapter 7 – External Systems ..... 58
  - Data Migration ..... 58
  - External Watch Lists ..... 59
  - Import Mappings..... 61
- Chapter 8 – System Administration ..... 63
  - Global Settings ..... 63
  - Database Tools ..... 64
- Chapter 9 – Station Preferences ..... 66
- Addendum – Screens, Options and Fields ..... 68
  - Screens ..... 68
  - Options ..... 83
  - Fields ..... 85



## Chapter 1 – Introduction

### WHAT IS PASSAGEPOINT GLOBAL?

PassagePoint visitor badging and lobby security software represents many years of pioneering product development. It was conceived to meet customer requests for computerized visitor logs and temporary visitor badges, and has evolved into the most comprehensive visitor management software available.

### USES FOR THE SOFTWARE

- For signing in and badging visitors - walk-in, pre-registered and authorized
- To pre-register individuals and groups
- For checking visitor names against U.S. sex offender lists
- As a people tracking tool
- To notify visitors and hosts of pre-registrations and arrivals
- For viewing and printing visit reports

### SUPPORTED HARDWARE

Below is a short description of the hardware devices that may be used with PassagePoint. Many of the supported device require USB 2.0 ports. For a full description on how to configure these devices within PassagePoint, see the chapter on Station Preferences and Devices.

#### Badge Printer

Practically any printer with a Windows driver can be used by PassagePoint. In most cases, small, direct-thermal style printers are best since they require little desk space, do not require ink and quickly print one badge at a time. The printer commonly used with PassagePoint is Dymo's Label Writer 450 Turbo.

#### Business Card, ID/License & Passport Scanners

The Card Scanning Solutions (CSSN) hardware works with PassagePoint to scan business cards, driver's licenses, ID cards and passports. The data and photo captured from a scan is automatically entered into the current visit record. Currently, PassagePoint works with the ScanShell 800, 800N, 1000, ScanShell 900DX, and SnapShell models. USB 2.0 ports are required for these devices to be accessible. Please refer to the CSSN documentation for questions about specific requirements.

### Photo Capture Devices

PassagePoint can capture photos using a TWAIN or WIA driver for an USB 2.0 web camera. Various web cameras will work with PassagePoint, including Logitech QuickCam line of cameras.

### Barcode Scanners

Barcodes printed on badges or sent via Email may be used to sign in/out people. When a barcode is scanned, PassagePoint can either open a tab containing that person's visit or automatically sign in/out that person.

### Signature Capture Devices

Agreements that people need to agree to can be signed electronically with a Topaz signature capture device. The Signature is captured and displayed on the agreement window when using the SignatureGem 1x5 model. The Topaz 4x5 model has the added ability of showing the agreements on the screen of the signature pad device.

### Biometric Fingerprint Scanners

When identifying a person, a fingerprint scanner can be used to access a person's current visit record or link to their previously record person data. A new person can be enrolled into the fingerprint device database and used later for sign-out or starting a new return visit. Currently, the M2-Hamster device from M2Sys is supported.

## INSTALLATION OPTIONS

PassagePoint can be installed two ways, i.e. as networked or standalone. Networked requires installing PassagePoint Client locally and configured to access PassagePoint Server software running on a remote server. Standalone assumes that the server/client application resides on a single machine. All these options are available in the installation options.

## CONFIGURE SYSTEM

After PassagePoint Global is installed, you will need to configure the program to work with your visitor management procedures. Configuration is done under The Home |Configure System.

Here you can configure the following: Badge designer, Communication Settings, External Systems, Policy Manager, System Lists, User Administration, Web Module (if installed) and System Administration.

Clicking on these menu groupings will expand and contract a list of setting options which can be independently configured. Multiple configurations can typically be defined for each setting. Some configurations can also be identified as a default setting. Some settings cannot be deleted once created, but can be disabled to maintain historical information relating to that setting.

NOTE – these menu groupings are listed in the program in alphabetical order, the order in this manual is the recommended implementation order.

## OPERATING SYSTEM REQUIREMENTS

Before installing PassagePoint, please assure that the Windows Operating System meets the following requirements:

### PassagePoint Server

- Windows Server 2008\R2 (64 bit)
- Windows Server 2012

### PassagePoint Client

- Windows 10 (64 bit)
- Windows 8.1
- Windows 7 (32 bit or 64 bit), update to Service Pack level:
  - ❖ Microsoft Windows 7 Service Pack 1 (SP1) or newer

NTFS partition is recommended for installing PostgreSQL. Otherwise, special installation steps are required.

For Logitech QuickCam support, you must have DirectX 9.x or higher and Internet Explorer 9 or higher installed prior to installing Logitech's software.

During install of Standalone or Server, Local admin rights are required for installing PostgreSQL.

## PassagePoint Components

PassagePoint installs and uses Java 8, PostgreSQL database and Apache Tomcat web server. Below are the components that are installed with each installation package:

*Standalone:* Tomcat, Java, PostgreSQL, and hardware drivers

*Server:* Tomcat, Java, and PostgreSQL

*Client:* Java and hardware drivers

## RAM Storage and Application Requirements

The table below lists the RAM, storage, and application requirements by install option.

**Table 1 – Client Workstation (including Kiosk) Requirements for Windows**

	Minimum	Recommended
Processor	Intel iCore3 or equivalent	Intel iCore5 or better
RAM	4 GB	4 GB or more *
Hard Disk Space	1 GB	1 GB or more
Monitor	SVGA (1366x768)	XVGA (1366x768) or higher
CD-ROM	Required for installation via CD	Required for installation via CD
Serial Ports	USB 2.0 ports for devices	USB 2.0 ports for devices

**Table 2 – Standalone/Server (up to 5 users) Requirements for Windows**

	Minimum	Recommended
Processor	Xeon processor or iCore5 or better	Xeon processor or iCore5 or better
RAM	4 GB	6 GB or more *
Hard Disk Space	2 GB	30 GB **
Monitor	SVGA (800x600)	XVGA (1024x768) or higher
CD-ROM	Required for installation via CD	Required for installation via CD
Serial Ports	USB 2.0 ports for devices	USB 2.0 ports for devices

**Table 3 – Server (up to 25 users) Requirements for Windows**

	Minimum	Recommended
Processor	Xeon processor or iCore5 or better	Xeon processor or iCore5 or better
RAM	4 GB	6 GB or more *
Hard Disk Space	5 GB	30 GB **
Monitor	SVGA (800x600)	XVGA (1024x768) or higher
CD-ROM	Required for installation via CD	Required for installation via CD

\* **Additional RAM and a powered hub may be required when using multiple USB devices, such as license scanner, printer, barcode scanner, camera, biometric scanner, etc.** USB 2 ports offer the best performance.

\*\***Hard disk space is based on moderate data growth. Please contact your PassagePoint representative for larger deployment requirements.**

### Port Requirements

PassagePoint Server requires TCP ports **5431, 2080, 2443, 9876, and 9875** be available. Ports are used for communication from PassagePoint Client, Kiosk, Web Pre-Reg, and Mobile to the PassagePoint Server.

Tomcat administration ports 8005, 8009, and 8082 may also be needed.

The SQL default port is 1433.

## Chapter 2 – User Administration

### ABOUT USER ADMINISTRATION

The User Administration option under Home | Configure System allows an administrator to define rules for user authentication, define user roles, and create user accounts and passwords.

When PassagePoint Global is launched, a login screen appears which allows users to specify their login name and password. Both fields are case sensitive.

#### Login Screen



PassagePoint ships with an Administrator User already configured with a login name of “admin” (all lowercase). There is no password assigned to Admin. It is recommended that you give Admin a password after successfully logging in the first time. Be sure to keep the password somewhere for reference. If you lose all passwords and are not able to login, you can contact STOPware Technical Support for assistance.

If a user fails to login after a specified number of attempts, or if their account has expired, the user account will become disabled. Once disabled, an administrator will need to reactivate the account in the User Accounts section.

A Login requires that a PassagePoint Client license is available. Client licenses are shared based on concurrent client connections.



To create user accounts:

1. Create the Authentication Rule
2. Create the User Roles
3. Create the User Account

## AUTHENTICATION RULES

User Authentication Rules allow administrators to specify login and password parameters for PassagePoint Clients. Authentication Rules are applied by assigning them to User Roles.

To create an Authentication Rule:

1. From Home | Configure | User Administration | Authentication Rules, select the Add Button to create a new account or select the rule and the Edit Button to modify an existing role.
2. The Setting Details screen for Authentication Rules appears.

**Setting Details**

**Rule Name**

**Rule Options**

Use PassagePoint Authentication  
 Use LDAP Authentication  
 Use Windows Single Sign On

**Password Rules**

**PassagePoint Client**

PassagePoint Login Name must match Windows login  
 Limit to one session per user

**Authentication Rule**

Allow users to change password  
 Passwords must not contain the Login Name  
 New users must change password on first login

**Account lockout attempts**

**Minimum length (# characters)**

**Maximum length (# characters)**

**Expires after # days**

**Disallow re-using # previous passwords**

**Historical passwords re-usable after # days**

Set a default password

**Regular Expressions Password Filter**

Regular Expressions are evaluated when a password is entered. Any passwords not matching an expression will cause the new password to be rejected.

Save Cancel

3. Enter a name for the Rule.
4. Choose a Rule Option. The choices are: PassagePoint Authentication, LDAP Authentication, or Windows Single Sign On.

## RULE OPTIONS

Depending on the edition of PassagePoint you have purchased, the list of Rule Options available to choose from will be different. Rule Options are the authentication schemes for maintaining login security. Select the Rule Option that is appropriate for the users.

**Use PassagePoint Authentication** – This option is selected by default. By choosing PassagePoint Authentication, you are using PassagePoint's security rules to manage client and web logins and password parameters.

**Use LDAP Authentication** – By choosing LDAP Authentication, you are using LDAP security rules to manage web logins.

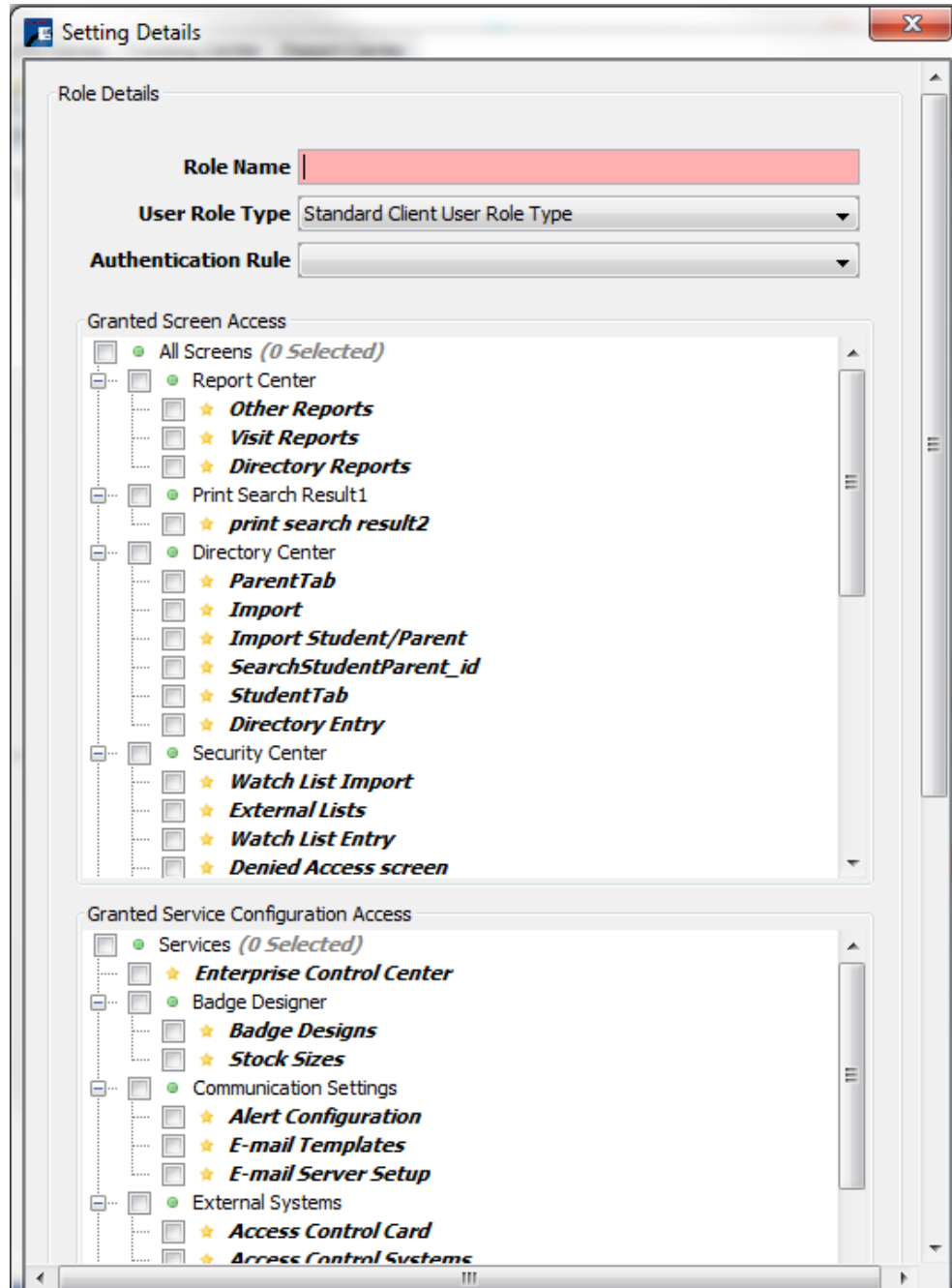
**Use Windows Single Sign On** – By choosing Windows Single Sign On, you are using Windows Single Sign On security rules to manage client and web logins and password parameters.

## USER ROLES

Roles are a logical grouping of users that share the same access rights to screens and login rules. Administrators can define a screen access policy and authentication rule with User Roles.

To configure roles:

1. From Home | Configure | User Administration, select the Add button to create a new account or the Edit button to modify an existing role.
2. The Setting Details screen for User Roles appears.



3. Role Name - Enter a name for the role. This is a free form text field to name the role. Use names that reflects the logical grouping of users, such as Receptionists, Security or Administrators. When configuring multiple roles for the same group of people, you might add other user categorizations to the name, such as a location – ‘Receptionists in Bldg. 5’
4. User Role Type - Select a User Role Type from the drop down list. Examples are: Standard Client User, Kiosk, Web User, Client and Web Access, Handheld User, and Client Admin.

5. Authentication Rule – Select the authentication rule to use with a User Role by choosing a rule from the drop down list. Rules listed are those configured from within the User Authentication Rules option under User Administration settings for Configure System.
6. Granted Screen Access – The listing of screens is organized hierarchically by PassagePoint Centers, also known as Center Tabs. By checking the box next to the name of a screen, you are granting the user access to that screen for viewing.
7. Granted Service Configuration Access – You can specify what the user has access to in Configure System. By checking the box next to the name of a screen, you are granting the user access to that screen for editing.
8. Set Opening Screen – You can specify the screen that displays by default after successfully logging in. To set the opening screen, select a screen from the hierarchical list of screens in the 'Grant Screen Access' frame and click the Set Opening Screen button.
9. Web Module Options – With the Web User Role Type, you can configure a role setting for users who will pre-register visitors using the PassagePoint Web Pre-Registration Module. You can specify if users can pre-register visits for hosts other than themselves. Additionally, users may be granted the ability to approve web pre-registrations in advance of a visit.
10. Disable – Checking the disable box makes the current role un-assignable. Roles cannot be deleted since removing roles would effectively grant user full rights to screens and unrestricted login access. Accounts with no assigned rules are treated as admin users.
11. Select the Save button.

## USER ACCOUNTS

User Accounts allow Administrators to define PassagePoint login accounts and grant rights based on a user role. For account security, each User Account should be assigned a User Role, which incorporate User Authentication Rules settings. By assigning a User Role, you are limiting access to screens that each user will be able to access.

To create a User Account,

1. From Home | Configure | User Administration, select User Accounts.
2. Select the Add Button to add a new User Account. The Setting Details for User Accounts appears.


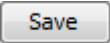
3. User Role - Select a User Role from the drop down list. User Roles are defined in the User Roles configuration option. Defined roles appear in the drop down list. Assigning a User Role to an account allows you to specify the screens which this user can access. Within the role definition, you can assign a User Authentication Rule that specifies password format rules and login limitations.
4. User Name – This is a free form text field to name the account.
5. Login Name –When logging into PassagePoint, this is the name that the user enters.
6. Password – Specify a password that conforms to the associated password rules. Passwords are case-sensitive. For security, passwords are encrypted and stored within the PassagePoint system. If a user account password needs to be reset, you can use this screen to specify a new password.
7. Language – Specify the language for this user.
8. Web Interface Allowed – Specify the web interface for this user (used with the Web Pre-Registration Module).
9. Linked Person – Allows you to associate a user to a person in the directory. This is for informational purposes. Click search to launch a directory search window that allows you to select the person who owns this account.
10. Disable – Accounts can only be disabled, not deleted. This maintains the integrity of past transactions. If a user account becomes disabled by the system because of an authorization rule, it can be reactivated here by un-checking the Disable box.

Warning: By not assigning a User Role, you effectively grant the user access to ALL screens and unrestricted password login.

## Chapter 3 – Communication Settings

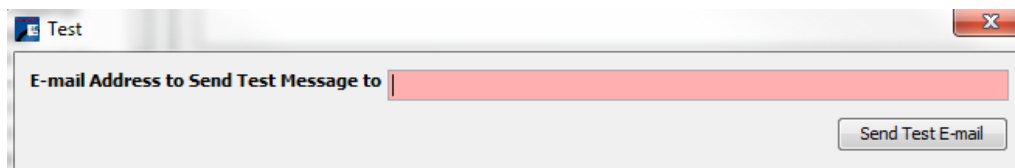
Communications Settings under Home | Configure System allows an administrator to configure the email templates, the email server, and the pop-up notifications for internal and external watch list matches.

### E-MAIL SERVER SETUP

1. To set up the E-Mail Server, from Home | Configure | Communication Settings, select E-Mail Server Setup.
2. Select the Edit button. 
3. Enter a name in the E-mail Setting Name field.
4. Specify the Outgoing E-mail Server by entering the IP address of DNS name of the server.
5. Enter the SMTP Port. The default port is 25.
6. Check if the SMTP server requires: TLS, SSL, and/or Authentication. If Authentication is required, specify the user name and password for logging into the SMTP server.
7. Select the Save button. 

Consult your E -mail administrator for the correct email settings for your organization.

To test that the SMTP server settings are correctly configured, click the “Test” button from E-Mail Server Setup. A test E-mail message will be sent to the address that you specify in the Test dialog window.



### E-MAIL TEMPLATES

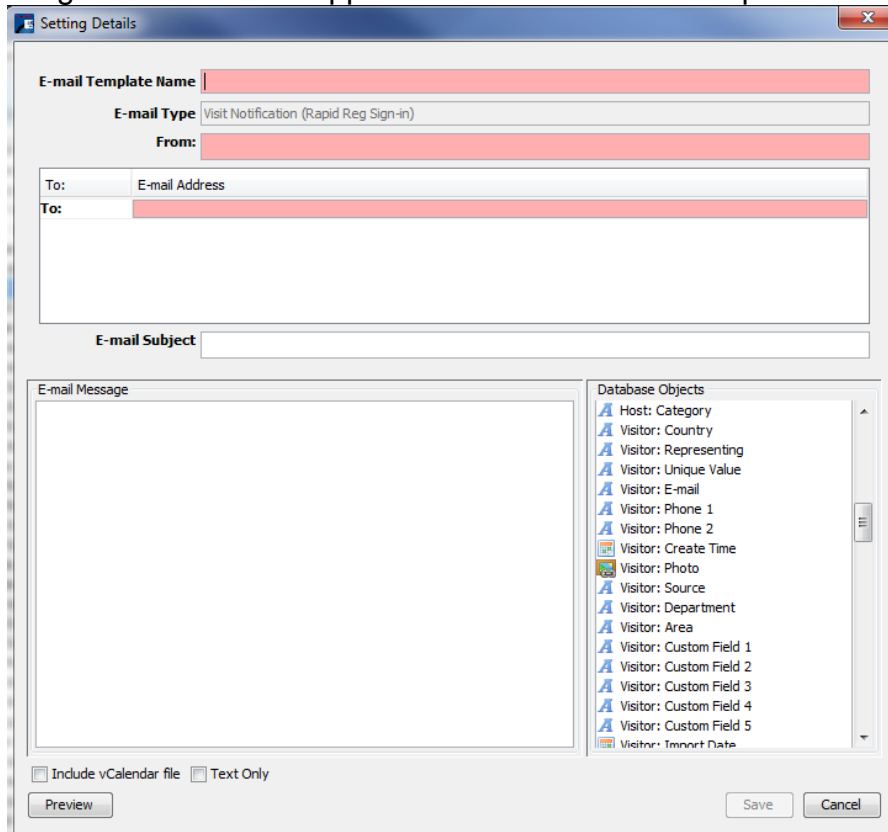
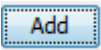
PassagePoint uses E-mail Templates when sending E-mail notifications. In addition to the pre-defined templates, you may create as many E-mail templates as you need. The E-Mail template types are:

- Visit Notification (Rapid Registration Sign-in)
- E-Visit Pass (Visitors)

- Pre-Registration Receipt (Hosts)
- Evacuation Report
- Internal Watch List Match Notifications
- Sex Offender Match Notifications
- Denial Match Notification

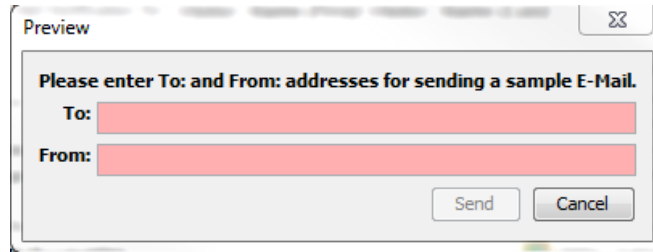
To add a template:

1. Select the desired template type and the Add button.
2. The Settings Details screen appears. The red fields are required.

A screenshot of a "Setting Details" dialog box. The dialog has a title bar with "Setting Details" and a close button. It contains several fields: "E-mail Template Name" (red background), "E-mail Type" (set to "Visit Notification (Rapid Reg Sign-in)"), "From:" (red background), "To:" (red background), and "E-mail Subject". Below these is a large "E-mail Message" text area. To the right is a "Database Objects" list with items like "Host: Category", "Visitor: Country", "Visitor: E-mail", etc. At the bottom are checkboxes for "Include vCalendar file" and "Text Only", and "Preview", "Save", and "Cancel" buttons.

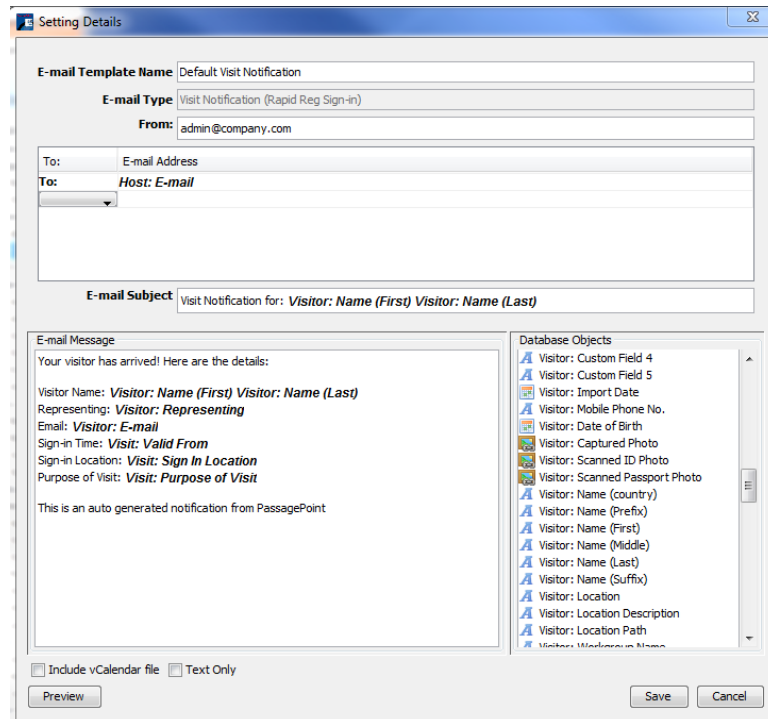
3. Name the E-Mail Template.
4. Select a From: and a To: email address. You may manually enter the email address or you can drag them from the Database Objects. For example, you could choose the Visitor: E-mail field and drag it into the From: and/or To: fields.
5. Enter the E-mail Subject.
6. Create the E-mail Message by typing the desired message into the box and dragging and dropping the desired Database Objects into the box. The Database Objects are replacement fields and will be replaced with the actual value. For example, Visitor: Name (Last) will display the visitor's last name. Database Objects will appear on the template as bold-italicized text.
7. Select to include a vCalendar file and/or if Text Only email, if desired.
8. You can preview the email by selecting the Preview button and entering the To: and From: addresses for the sample email.





To edit an existing template:

1. Select the desired template type and the Edit button.
2. The Settings Details screen for the template appears.



3. Make the desired changes to the template and select the Save button.

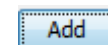
## ALERT CONFIGURATION

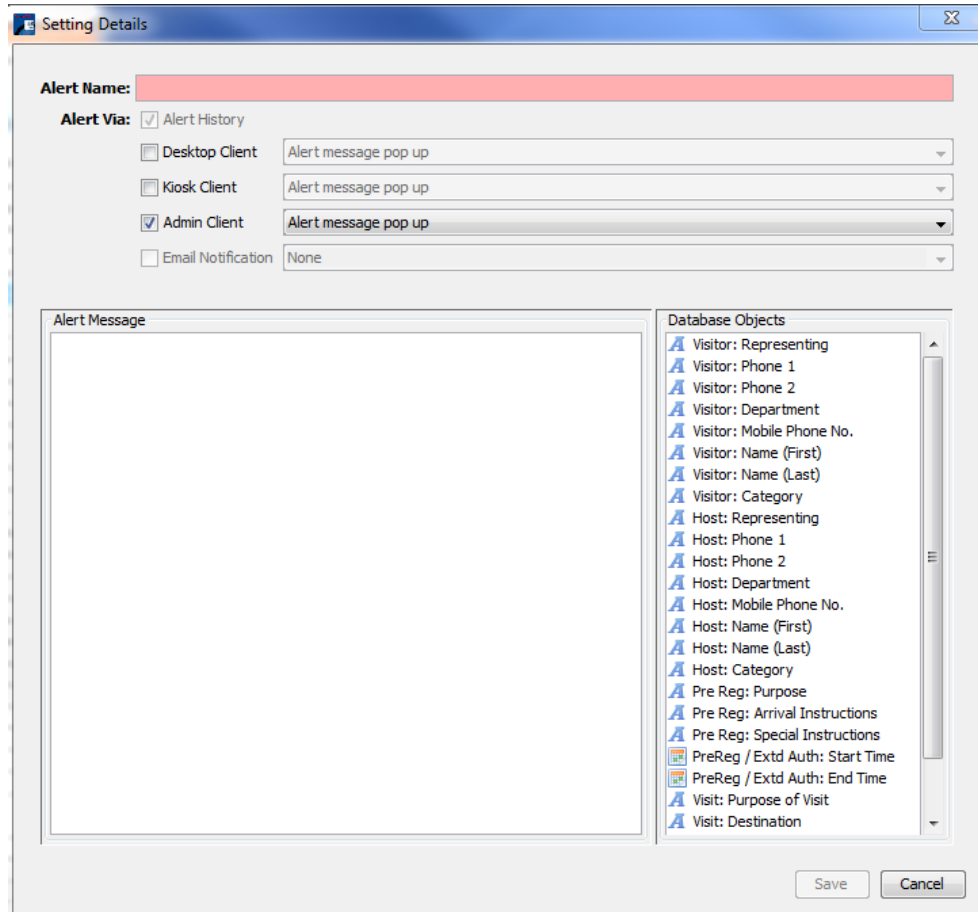
Use Configure alerts for External and Internal Watch lists to determine the alert message and where the alert displays. The alert types are:

- Desktop Client
- Kiosk Client
- Admin Client
- Email Notification

To add an alert configuration:


1. Select the desired watch list alert and the Add button.
2. The Settings Details screen appears. The red fields are required.





3. Name the Alert.
4. Select the desired Alert deliveries. NOTE – email Notification may not be available if you haven't set up an E-Mail template
5. Create the E-mail Message by typing the desired message into the box and dragging and dropping the desired Database Objects into the box. The Database Objects are replacement fields and will be replaced with the actual value. For example, Visitor: Name (Last) will display the visitor's last name. Database Objects will appear on the template as bold-italicized text.
6. Select the Save button.

To edit an existing template:

1. Select the desired template type and the Edit button. 
2. The Settings Details screen for the template appears.
3. Make the desired changes to the template and select the Save button.

## Chapter 4 – System Lists

System Lists under Home | Configure System allows an administrator to configure the dropdown lists for Agreements, Destinations & Places, Destination Rules, People Categories, Watch Lists, Workgroup, and Lists. The System Lists configuration screens allow you to define, sort, set a default item, and in some cases, customize the list items usage.

### AGREEMENTS

Agreements are contracts or documents legal or otherwise that visitors have to sign or agree to when they are at your facility. The steps to creating agreements in PassagePoint are:

1. Create agreement types in the Lists section of System Lists
2. Create the agreement
3. Assign the agreement to People Categories

To create Agreement Types:

1. From Home | Configure System | System Lists | Lists, select agreementTypes and the Edit button.

Setting Details

List Type: Agreement Types (single list)

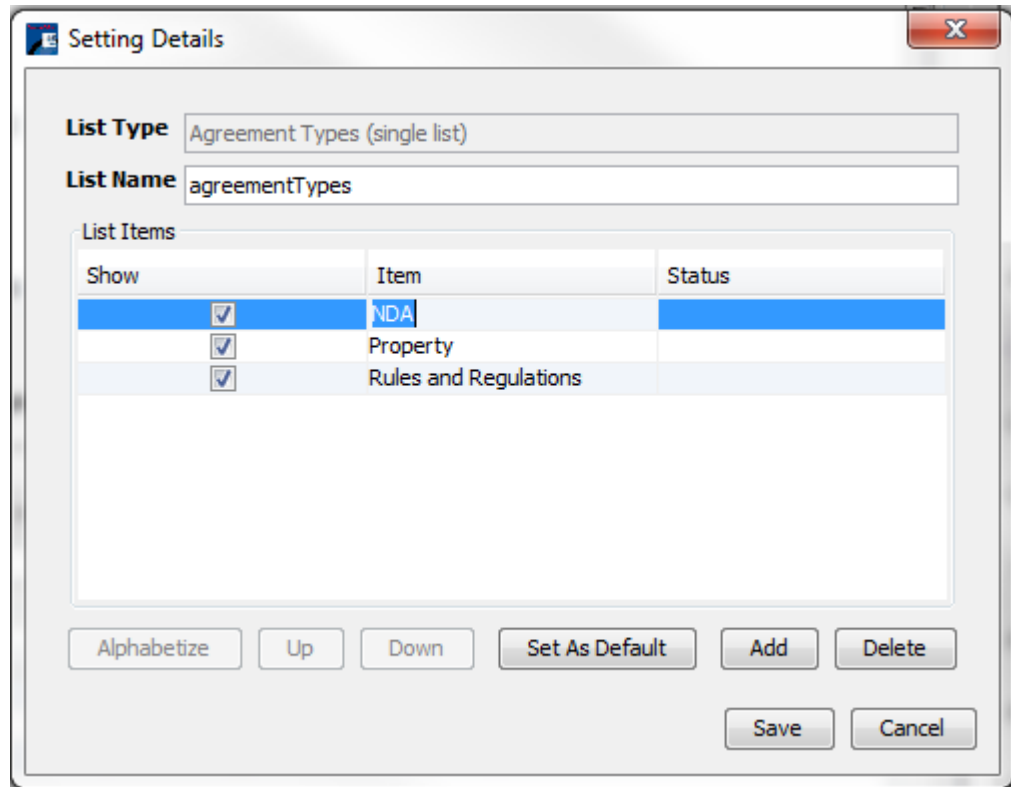
List Name: agreementTypes

List Items

Show	Item	Status
------	------	--------

Alphabetize Up Down Set As Default Add Delete Save Cancel

2. Select the Add button and type in the name of the Item (agreement). Repeat to enter all desired agreements.



3. To set a default, click on the desired Item, it will highlight in blue, and select the Set As Default button.
4. You may also change the order of the items by using the Up, Down, and Alphabetize buttons.
5. Once you have created the desired items, select the Save button.

To create Agreements:

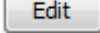
1. From Home | Configure System | System Lists | Agreements and the Add button.
2. The Settings Details screen appears. The red fields are required.

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

- Agreement Name:** A text input field.
- Agreement Type:** A dropdown menu.
- Agreement Text:** A large text area with an 'Import' button below it.
- New Acceptance Required After Every:** A numeric spinner set to '0', with radio buttons for 'Days', 'Months' (selected), and 'Every Sign In'.
- Accept Methods:** Radio buttons for 'Signature' (selected) and 'Click Accept'. Checkboxes for 'Signature On File Allowed', 'Can Bypass', and 'Disable On Kiosk'.
- Decline Methods:** A checkbox for 'Can Decline and complete sign-in on Kiosk' and a text input field below it.
- Disabled:** A checkbox at the bottom left.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

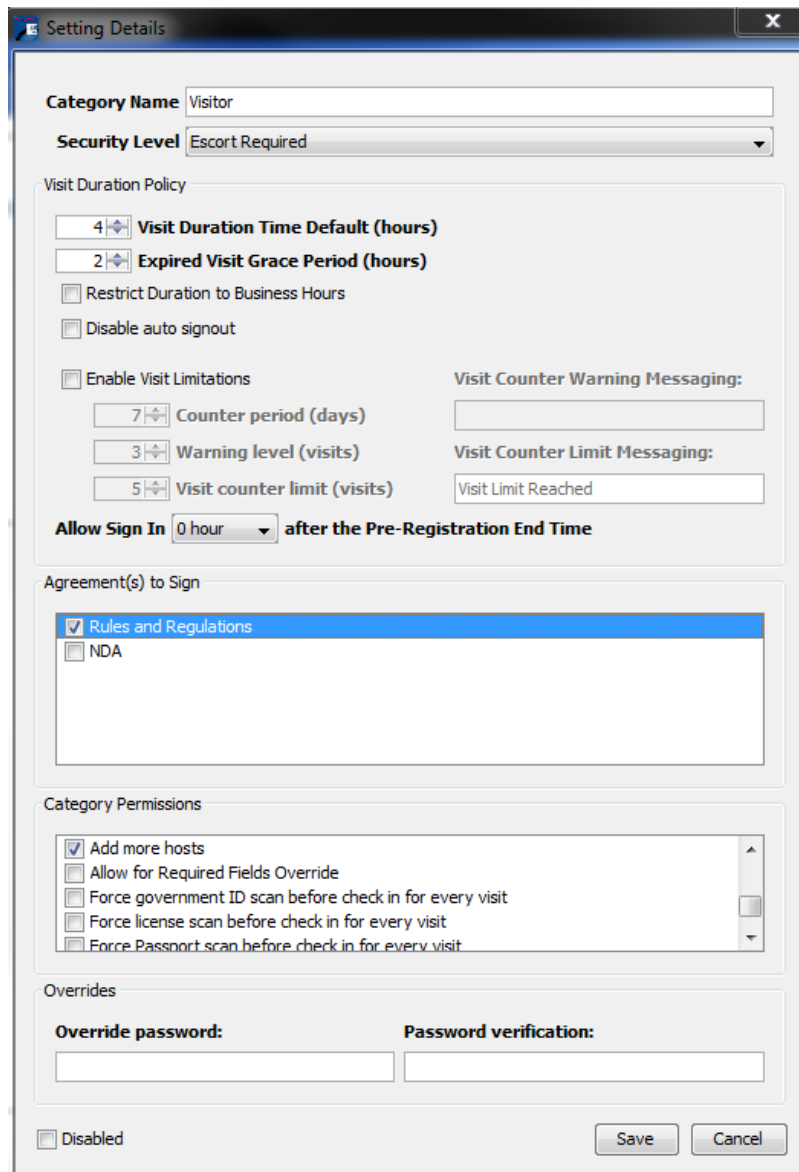
4. Name the Agreement.
5. Select the Agreement Type from the dropdown list.
6. Create the E-mail Message by typing the desired text into the box or importing the text with the Import button. The file must be a .txt file.
7. Determine the frequency for the agreement by setting the number of days or months or if agreement is for every sign in.
8. Indicate the Acceptance Method.
  - Signature: If you select Signature, you will be given the option of allowing a signature on file as a proxy for the actual signature. This means that the visitor doesn't have to sign a signature pad, the operator can choose Signature on File.
  - Click Accept – an accept agreement button displays for the operator
  - Can Bypass – the visitor does not have to agree to the agreement. If you select Can Bypass, the Disable on Kiosk option is active. This allows you to indicate that this will not be an option in Kiosk mode.
9. Decline Methods – selecting this option, allows the visitor to decline the agreement and continue to sign in in the Kiosk mode.
10. Disabled – if checked, indicates that this Agreement is disabled.
11. Select the Save button.

To edit an existing Agreement:

1. Select the desired Agreement and the Edit button. 
2. The Settings Details screen for the Agreement appears.
3. Make the desired changes to the Agreement and select the Save button.

To assign Agreements to People Categories:

1. From Home | Configure System | System Lists | People Categories and select the desired Configured People Category and the Edit button.
2. In the Agreement(s) to Sign section, place a checkmark by clicking on the desired agreement(s).



The screenshot shows the 'Setting Details' window for a 'Visitor' category. The 'Security Level' is set to 'Escort Required'. Under 'Visit Duration Policy', the 'Visit Duration Time Default (hours)' is 4, and the 'Expired Visit Grace Period (hours)' is 2. There are checkboxes for 'Restrict Duration to Business Hours', 'Disable auto signout', and 'Enable Visit Limitations'. Under 'Enable Visit Limitations', there are spinners for 'Counter period (days)' (7), 'Warning level (visits)' (3), and 'Visit counter limit (visits)' (5). There are also text boxes for 'Visit Counter Warning Messaging:' and 'Visit Counter Limit Messaging:' (Visit Limit Reached). The 'Allow Sign In' is set to '0 hour' after the Pre-Registration End Time. In the 'Agreement(s) to Sign' section, 'Rules and Regulations' is checked, and 'NDA' is unchecked. Under 'Category Permissions', 'Add more hosts' is checked, and other options are unchecked. The 'Overrides' section has text boxes for 'Override password:' and 'Password verification:'. At the bottom, there is a 'Disabled' checkbox and 'Save' and 'Cancel' buttons.

3. Select the save button.

## DESTINATIONS & PLACES

Destinations & Places are the areas of your facility where visitors visit.

To create Destinations & Places:

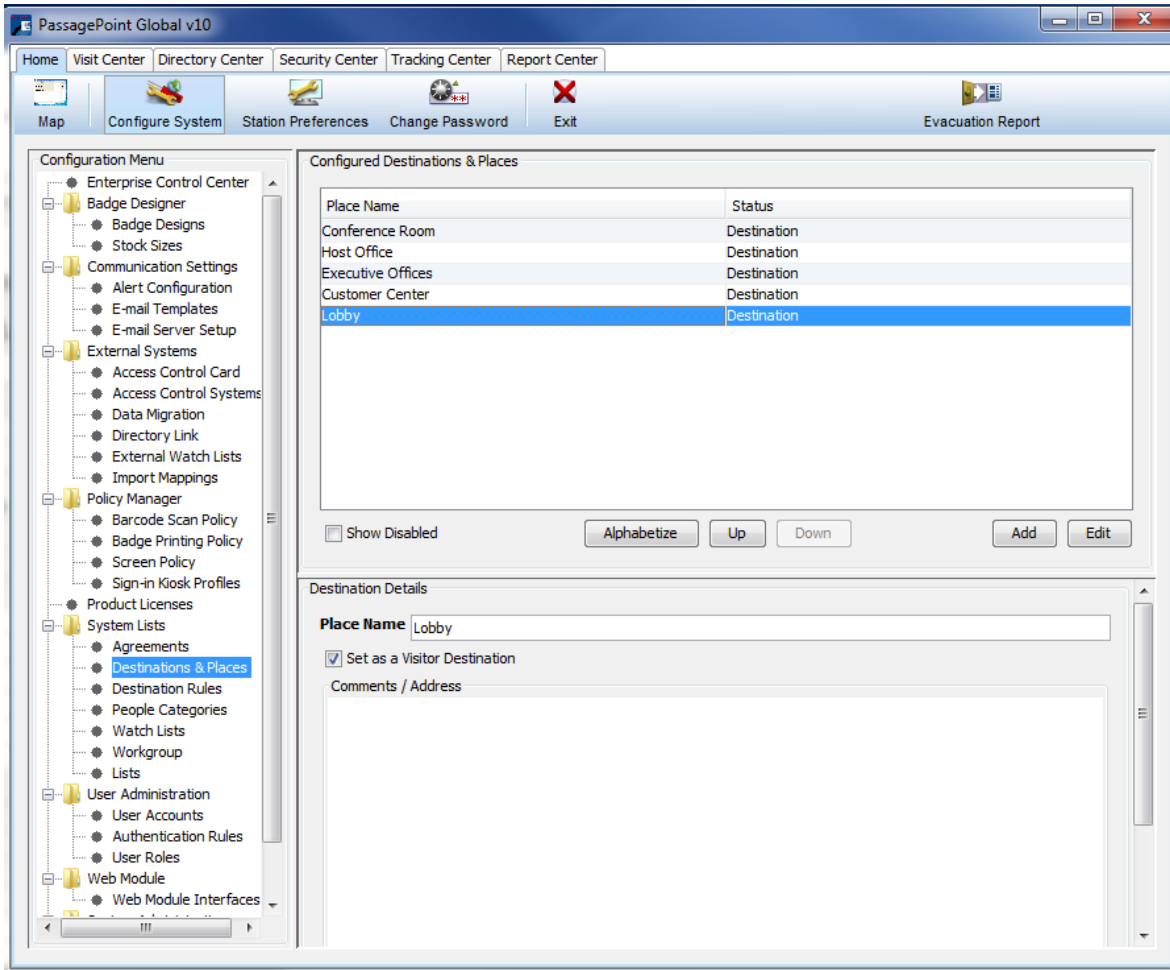
1. From Home | Configure System | System Lists | Destinations & Places and select the Add button.
2. The Settings Details screen for Destinations appears.

The screenshot shows a 'Setting Details' dialog box. At the top, there is a title bar with the text 'Setting Details' and a close button. Below the title bar, the dialog contains the following elements: a 'Place Name' text input field with a red background; a checked checkbox labeled 'Set as a Visitor Destination'; a large text area labeled 'Comments / Address'; a 'Disabled' checkbox; and two buttons labeled 'Save' and 'Cancel' at the bottom right.

3. Name the Place.
4. Type in any Comments about the place and/or address.
5. Disabled – if checked, indicates that this Place is disabled.
6. Select the Save button.

To view and organize Destinations & Places:

1. From Home | Configure System | System Lists | select Destinations & Places.
2. The Settings Configured Destinations & Places screen appears.



3. You may change the order of the items by using the Up, Down, and Alphabetize buttons.
4. When you check the Show Disabled check box, destinations that were disabled display and are indicated as a Disabled Destination.

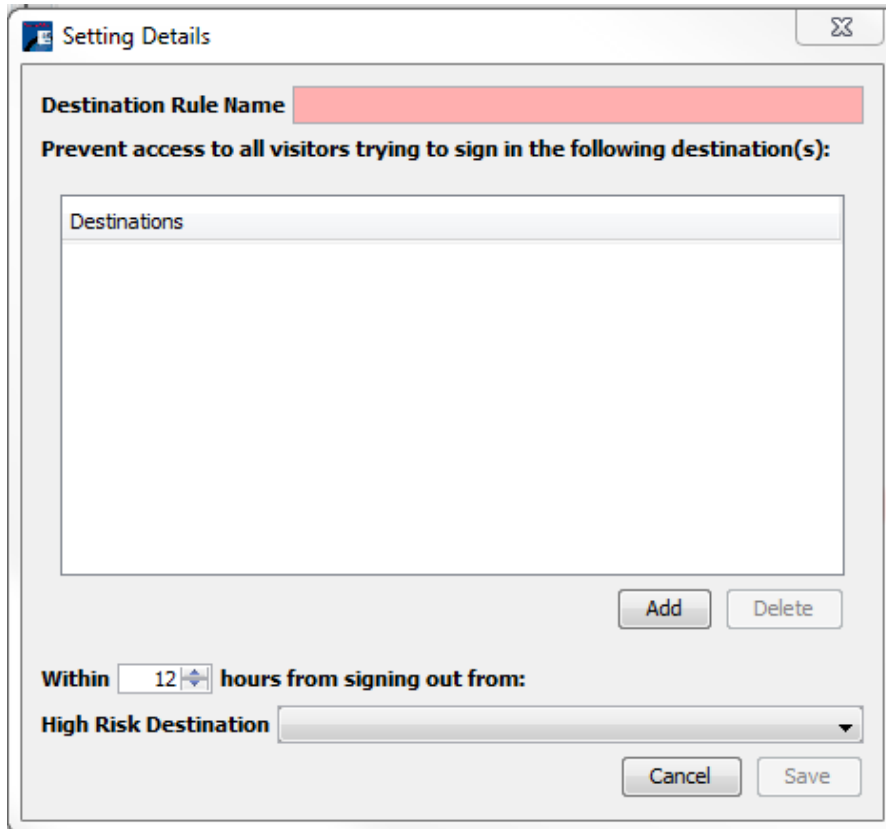
## DESTINATION RULES

Destination Rules allow you to restrict visitors from signing into a destination after they sign out of another destination. For example, you may want to prevent visitors from signing into the ICU after signing out of the Emergency Room.

To create Destination Rules:

1. From Home | Configure System | System Lists | Destination Rules, select the Add button.
2. The Settings Details Destination Rule screen appears.





3. Enter a name for the Destination Rule.
4. Add a Destination by selecting the Add button. Select the Down arrow after the Destination to change the destination from the default to the desired destination. Continue this step for all desired destinations.
5. Determine the desired time interval by selecting the up or down arrows.
6. Chose the desired sign out destination using the down arrow on the High Risk Destination field.
7. Select the Save button.

## PEOPLE CATEGORIES

People Categories are used to group individuals, both visitors and employees. Categories allow you to set visit durations, visit limitations, agreements to sign, permissions, collect different information, print different badges, and use reports by category.

PassagePoint Global is pre-configured with the following categories:

- Staff
- Faculty
- Volunteer
- Student
- Visitor
- Vendor

You can modify or delete these categories and create additional categories.

To create People Categories:

1. From Home | Configure System | System Lists | People Categories, select the Add button.
2. The Settings Details screen for People Categories appears.

**Setting Details**

**Category Name**

**Security Level** Escort Required

**Visit Duration Policy**

**Visit Duration Time Default (hours)**

**Expired Visit Grace Period (hours)**

Restrict Duration to Business Hours

Disable auto signout

Enable Visit Limitations

**Visit Counter Warning Messaging:**

**Counter period (days)**

**Warning level (visits)**

**Visit Counter Limit Messaging:**

**Visit counter limit (visits)**

**Allow Sign In** 0 hour **after the Pre-Registration End Time**

**Agreement(s) to Sign**

Rules and Regulations

NDA

**Category Permissions**

Allow as Valid Sponsor of Visitors

Allow to be included in Directory

Visitor must be from Directory

Allow to receive Deliveries

Allow to checkout Property

Require Host Signature

**Overrides**

**Override password:**

**Password verification:**

Disabled

Save Cancel

3. Enter a name for the Category.

4. Select the Security Level from the drop down list of levels. (If a desired level is not shown, create the security level in Home | Configure System | System Lists | Lists.)
5. Set the Visit Duration Policy. There are two parts to the Duration Policy – the Visit Duration and the Grace Period.
  - a. The Visit Duration is the number of hours for the visit for this category. For example, a Contractor may have a duration of 8 hours, where a Visitor may only have 1 hour. The visit duration can be between 0 and 24 hours.
  - b. The Grace Period is the time the visitor is allowed to remain after the visit duration ends. The Grace Period can be between 0 and 72 hours
  - c. You can restrict the Duration to only Business hours by selecting the check box.
  - d. Auto signout automatically signs the visitor out after the Visit Duration/Grace Period ends. You can disable the auto signout by selecting the check box.
6. To enable Visit Limitations, select the check box. Visit limitations allow you to restrict the number of visits during a period of time. You can set:
  - a. Counter Period in days. The Counter Period can be between 2 and 365 days.
  - b. Warning Level in number of visits. The Warning Level can be between 1 and 100 visits.
  - c. Visit counter limit in number of visits. The Counter Period can be between 2 and 100 days.
  - d. You can enter text for a Warning that visits will near the end and a Limit has been reached messages.
7. You can set the time the visitor can sign in after the Pre-Registration time has ended. For example, if a visitor is pre-registered for 11am to 2pm, and the Sign in is set in the Category for 1 hour after the end time, the visitor will be able to sign in until 3pm.
8. You can determine the Agreement(s) the visitor has to sign by checking the desired check box for the agreement. Set up agreements under Home | Configure System | System Lists | Agreements.
9. You can set the Category Permissions by checking the desired check boxes. The Category Permissions are:
  - Allow as Valid Sponsor of Visitors (for employees)
  - Allow to be included in Directory
  - Visitor must be from Directory
  - Allow to receive Deliveries
  - Allow to checkout Property
  - Requires Host Signature
  - Add more hosts
  - Allow for Required Fields Override
  - Force government ID scan before check in for every visit
  - Force license scan before check in for every visit
  - Force passport scan before check in for every visit
  - Force PIV card scan before check in for every visit

10. You can set an Override Password.
11. Disabled – if checked, indicates that this Category is disabled.
12. Select the Save button.

To edit People Categories:

1. From Home | Configure System | System Lists | People Categories and select the Edit button.
2. The Settings Details screen for selected People Category appears. Make the desired changes.
3. Select the Save button.

## WATCH LISTS

Watch lists are used to let the operator know that a specific visitor requires attention. You can create as many types of watch lists as you need. See Security Center or Importing for adding people to the watch lists created.

To create Watch Lists:

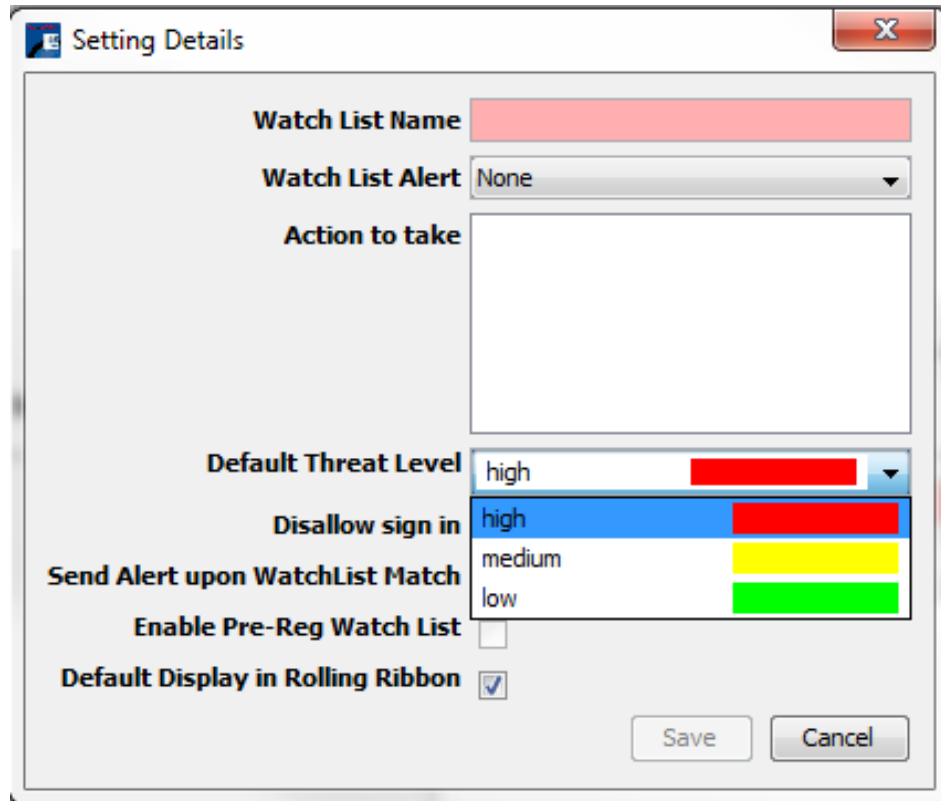
1. From Home | Configure System | System Lists | Watch Lists select the Add button.
2. The Setting Details for the Watch List screen appears.

The screenshot shows a 'Setting Details' dialog box for configuring a Watch List. The fields are as follows:

- Watch List Name:** A text input field, currently empty and highlighted in red.
- Watch List Alert:** A dropdown menu with 'None' selected.
- Action to take:** A large text area for entering the alert message.
- Default Threat Level:** A dropdown menu with 'high' selected, highlighted with a red bar.
- Disallow sign in:** An unchecked checkbox.
- Send Alert upon WatchList Match:** An unchecked checkbox.
- Enable Pre-Reg Watch List:** An unchecked checkbox.
- Default Display in Rolling Ribbon:** A checked checkbox.

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

3. Enter a name for the watch list.
4. Select the desired Watch List Alert from the drop down list.
5. Enter the Action to take for this watch list. What you type in will appear on the alert for the operator.
6. Assign a Default Threat Level for the Watch List. The choices are high, medium, and low and are color coded.



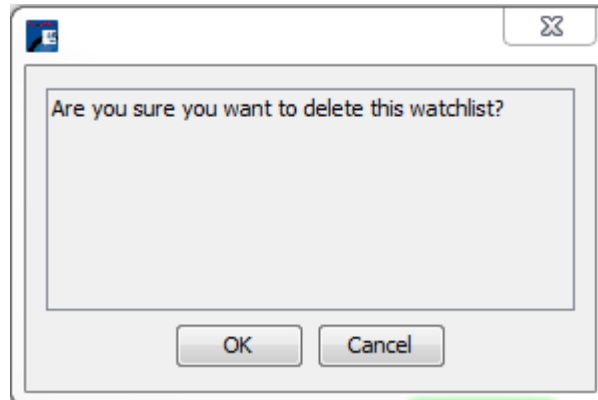
7. Select the checkmark on Disallow sign in, to prevent sign in for visitors on this type of watch list.
8. Select the checkmark on Send Alert upon WatchList Match, to automate an alert when a visitor is matched to a name on the Watch List.
9. To enable watch list matching when pre-registering visitors, select the check mark on Enable Pre-Reg Watch List.
10. To display the Watch List Type entries on the Rolling Ribbon, select the checkmark on Default Display in Rolling Ribbon. The Rolling Ribbon displays next to the Evacuation Report on the Visitor Center. This allows the operator to have a visual reminder of the people to be on the lookout for, otherwise known as BOLO.
11. Select the Save button.
12. Repeat for all desired Watch Lists.
13. To set a Watch List Type as the default type when adding a visitor to a watch list, highlight the desired Watch List Type and select the Set as Default button.

To Edit Watch Lists:

1. From Home | Configure System | System Lists | Watch Lists select the Edit button.
2. The Setting Details for the Watch List screen appears. Make the desired changes and select the Save button.

To Delete Watch Lists:

1. From Home | Configure System | System Lists | Watch Lists select the Delete button.
2. A confirmation screen appears. To delete, select the OK button.

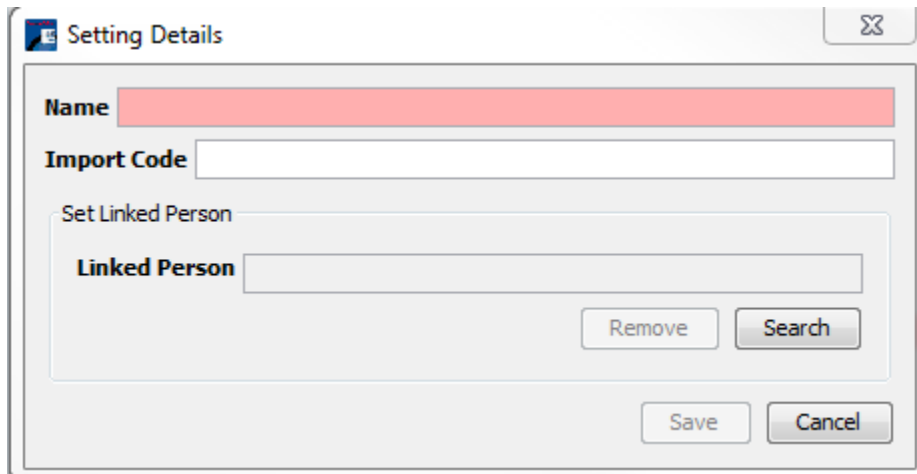


## WORKGROUP

Workgroup is used to define a group of workers that share resources and responsibilities.

To create a Workgroup:

1. From Home | Configure System | System Lists | Workgroup select the Add button.
2. The Setting Details for the Workgroup screen appears.



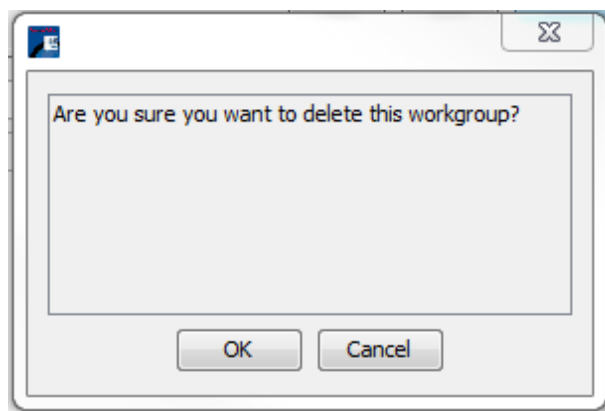
3. Enter a name for the Workgroup.
4. You may enter an Import Code if you are importing employees by workgroups.
5. Set the Linked Person to the Workgroup by selecting the Search button and searching for the desired employee.
6. Select the Save button.

To edit a Workgroup:

1. From Home | Configure System | System Lists | Workgroup select the Edit button.
2. The Setting Details for the Workgroup screen appears. Make the desired changes and select the Save button.

To delete a Workgroup:

1. From Home | Configure System | System Lists | Workgroup select the Delete button.
2. A confirmation screen appears. To delete, select the OK button.



## LISTS

The Lists are used to create the drop down list choices for:

- Arrival Instructions - steps to follow at sign-in
- Purpose of Visit - reasons for visiting location
- Security Levels - security interaction information, such as escort required (single list)
- Agreement Types - contracts or documents legal or otherwise that visitors have to sign or agree to when they are at your facility (single list)
- Threat Levels – indicates the risk level of the visitor (single list)
- Delivery Items – choices for delivered items, such as, box, envelope, flowers, etc.
- Courier Names - list of shipping carriers, such as FedEx, UPS, etc.
- Property Items - list of property types loaned out or brought in by visitors
- Country Codes - 2 letter code for countries (single list)
- Classifications - classifications for visitors such as, immigration and visa classifications. For example, US Green Card and H1B Visa (single list)

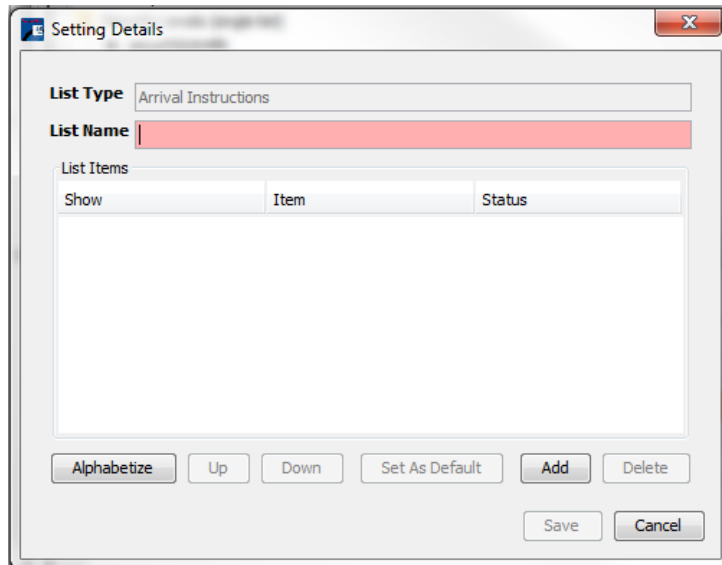
Security Levels, Agreement Types, Threat Levels, Country Codes, Classifications are all single lists, which means that all options are under one list. For these Lists, you will only be able to Edit to add options, for the other lists you will be able to add. Multiple

lists are used in the Enterprise Control Center (an Add-on software) Allocation Tree to assign custom lists by location.

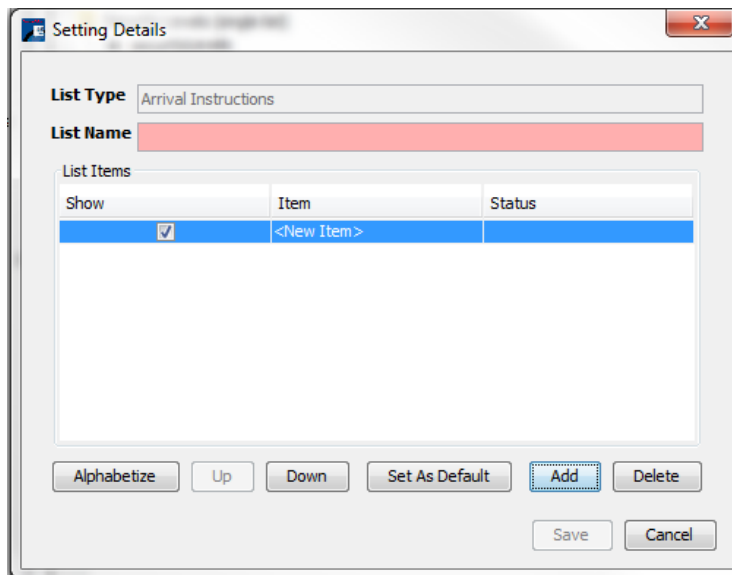
A list with a dot icon indicates that this list can be expanded, similar to a folder. To open dot icon lists, double-click on it.

To create Lists:

1. From Home | Configure System | System Lists | Lists.
2. Select the desired List and the Add button. The Setting Details for the Lists screen appears.



3. Enter a name for the list.
4. Select the Add button to add an item to the new list.

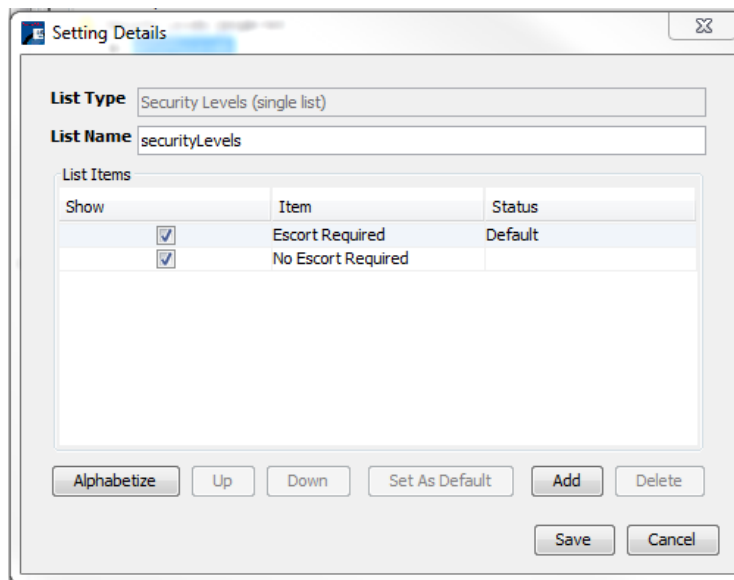




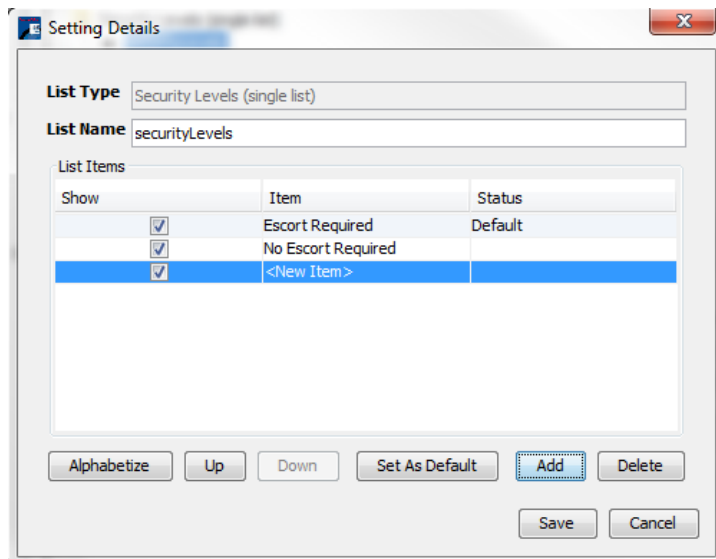
5. Replace <New Item> with the desired option.
6. You may change the order of the items by using the Up, Down, and Alphabetize buttons.
7. You may set an item as the default item by selecting the item and the Set as Default button.
8. Select the Save button.

To create Single Lists:

1. From Home | Configure System | System Lists | Lists select the Add button.
2. Select the desired List and the Edit button. The Setting Details for the Lists screen appears.



3. Select the Add button to add an option.



4. Replace <New Item> with the desired option.
5. You may change the order of the items by using the Up, Down, and Alphabetize buttons.
6. You may set an item as the default item by selecting the item and the Set as Default button.
7. Select the Save button.

## Chapter 5 – Badge Designer

PassagePoint includes an integrated badge design tool that allows complete control over how a badge or label looks and the information to be printed on a badge or label. The Badge Designer screen is used to create templates for both badges and labels. Once a template is complete, data is populated into the pre-defined template fields when a badge prints. The size of a badge used in a template is based on a user-defined stock size.

### STOCK SIZES

Before a badge template can be created, you must have a badge stock size defined. If your badge stock size isn't in the pre-defined stock size list you can create a new stock size.

To define stock sizes:

1. From Home | Configure System| Badge Designer | Stock Sizes, select the Add button.
2. The Setting Details for the Stock Size screen appears.

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

- Name:** A text input field with a red highlight.
- Stock Number:** A text input field.
- Units:** A dropdown menu currently set to 'in'.
- Badge Label Dimensions for Portrait Orientation:**
  - Badge Width:** A text input field with '0'.
  - Height:** A text input field with '0'.
- Badge label in landscape orientation**
- Badge Sheet Layout:**
  - Badge sheet dimensions same as badge label**
  - Sheet Width:** A text input field with '0'.
  - Sheet Height:** A text input field with '0'.
  - # Badges Across:** A text input field with '1' and a double-headed arrow.
  - Down:** A text input field with '1' and a double-headed arrow.
  - Left Margin:** A text input field with '0'.
  - Top Margin:** A text input field with '0'.
  - Horizontal Gap:** A text input field with '0'.
  - Vertical Gap:** A text input field with '0'.
- Disable**
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

3. Enter a name for the Stock Size and the Stock Number (from the manufacturer). Choose the Unit for the badge measurements, either inches (in) or centimeters (cm).
4. Enter the badge width and height for Portrait Orientation (where the longest side goes from top to bottom).
5. Check the box if you want the badge in Landscape Orientation (where the longest side goes from right to left side).
6. Check the box if you are using a sheet of labels where the badge label is the same size as the sheet i.e 1 label per sheet.
7. Enter the following:

Sheet Width & Height – Specify the physical dimensions in inches or centimeters of each badge on a sheet or roll.

#Badges Across and Down – Enter the number of badges across and down on a badge print sheet. For badge label rolls, such as labels for Dymo printers, enter “1” for both Across and Down.

Left and Top Margin – The Margin is the edge of a sheet that is not printable. It is assumed that left and right are the same dimensions, as well as top and bottom.

Horizontal and Vertical Gap – Gap is the measurement of space between badges on a sheet. Enter “0” for badge rolls.

8. Disabled – if checked, indicates that this Stock Size is disabled and will not be listed in the stock size list.
9. Select the Save button.

## BADGE DESIGNS

Badges print based on a customized design template created in Badge Designs. Pre-defined badges for Visitor, Visitor Barcode, and Employee are included in the software. You may change the pre-defined badges and/or make your own badges. When a visitor is signed in from the Visit Center (Pre-registration, Extended Authorization, or Rapid Registration screens), a badge for that visitor can be printed by selecting a badge design from the dropdown list and checking Print Badge. You can also set up a badge printing policy to have badges automatically print when checking in a visitor.

Objects placed on a badge are layered based on a set priority. The objects on a layout canvas are ordered as follows, starting from furthest back to front:

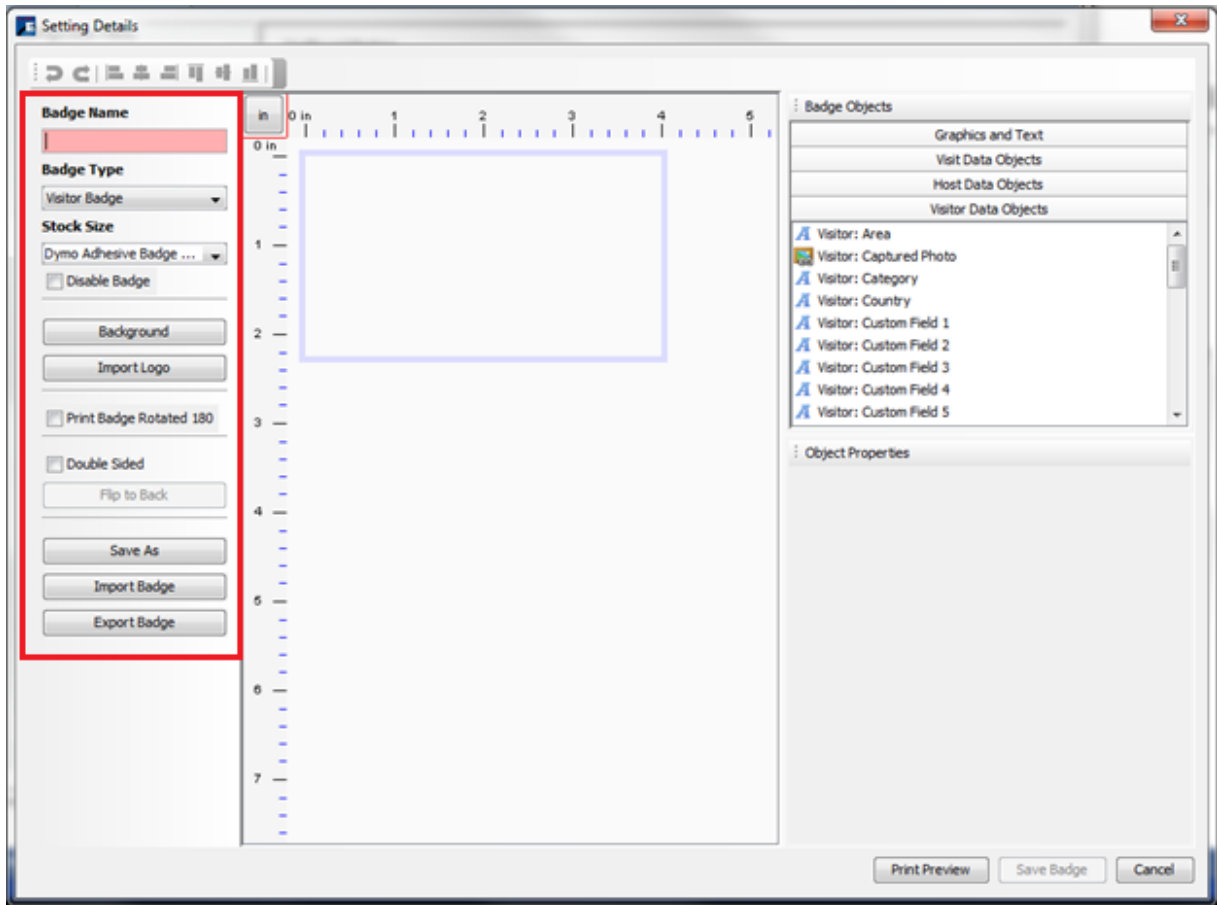
- Background: image or color
- Graphics: rectangles and lines
- Import logo images
- Text: data objects and text area

- Barcodes: linear and 2D barcodes

To create a Badge Design:

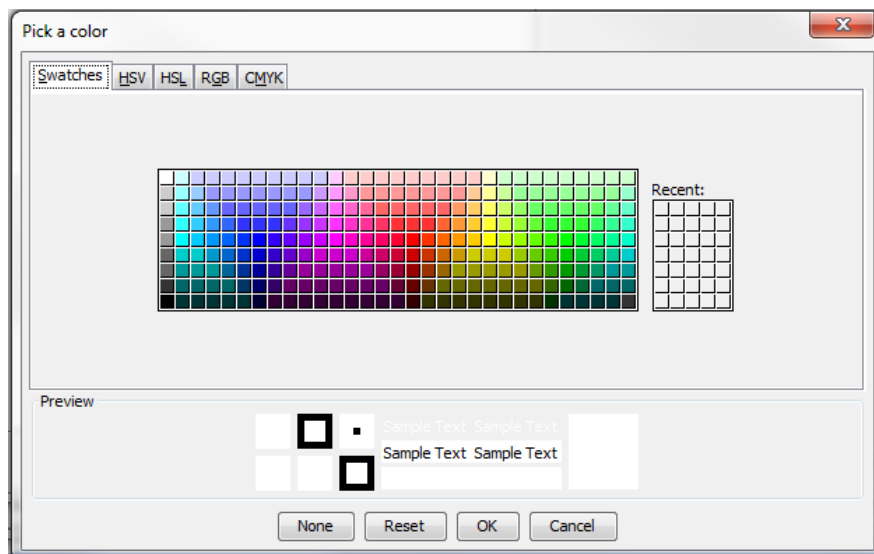
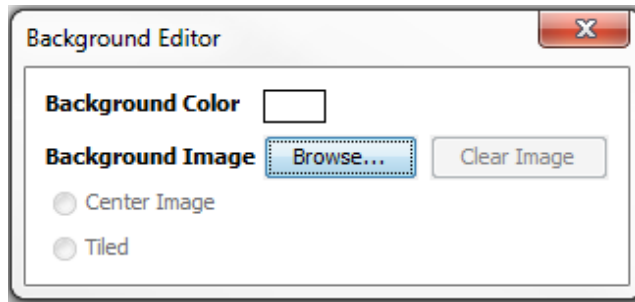
1. From Home | Configure System| Badge Designer | Badge Design, select the Add button.
2. The Setting Details for the Badge Design screen appears. The Badge Design Setting Details screen has a few sections. On the top is the Toolbar, on the left is the file naming and configuration, in the middle is the image of the badge, which updates as you make additions and changes, on the right is the Badge Objects and Object Properties sections. Each Section is explained below.

### Badge File Naming and Configuration



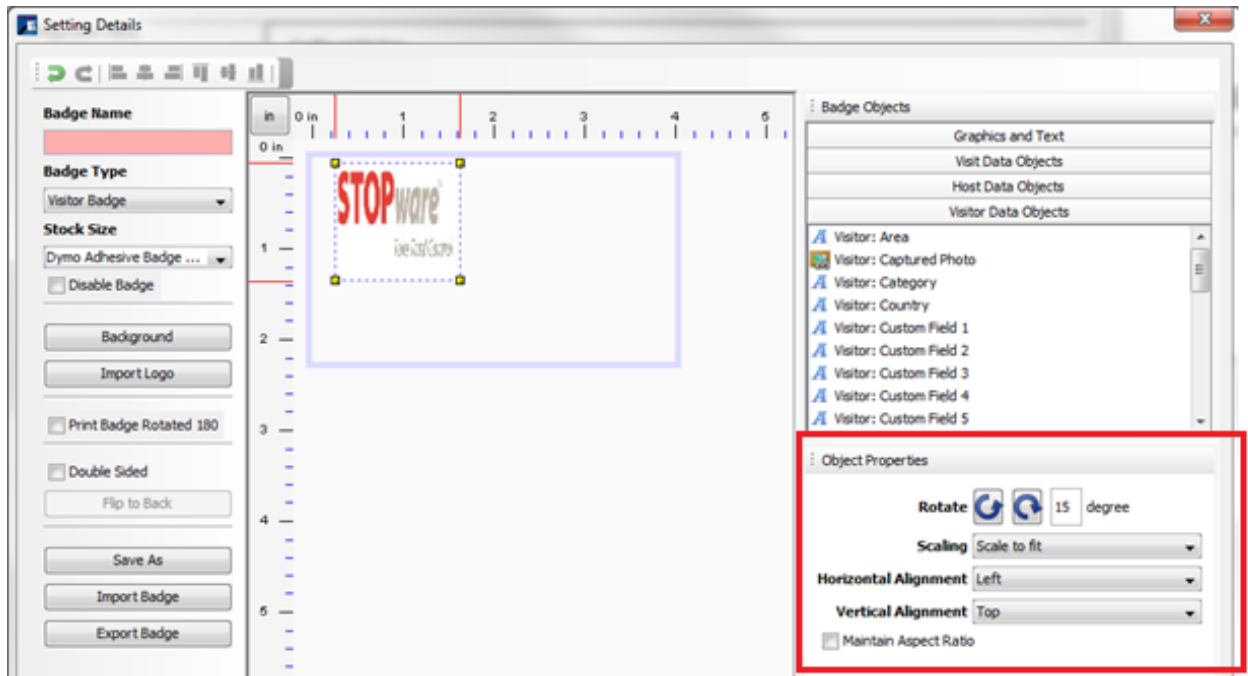
1. Enter a name for the badge.
2. Select the Badge Type. The choices are: Visitor, Delivery, Property, and Lost and Found.
3. Select the Stock Size from the list. (If your stock size isn't on the list, create the desired size in the Home | Configure System| Badge Designer | Stock Size)

4. You can set the badge background color and/or image with the Background button. To change the color, click in the color field and the Pick a color screen appears.



To change the background image select the Browse button and select the desired image file. The supported image file formats are: .jpeg, .jpg, .gif, .png, .tiff, and .tif. Use the radio buttons to Center or tile the background image.

5. Import a logo with the Import Logo button. The supported image file formats are: .jpeg, .jpg, .gif, .png, .tiff, and .tif.
6. The logo displays on the badge image in the middle of the screen. To move the logo, click it to highlight and drag and drop it to the desired location. To resize the log, mouse over the corner points and drag it to the desired size.

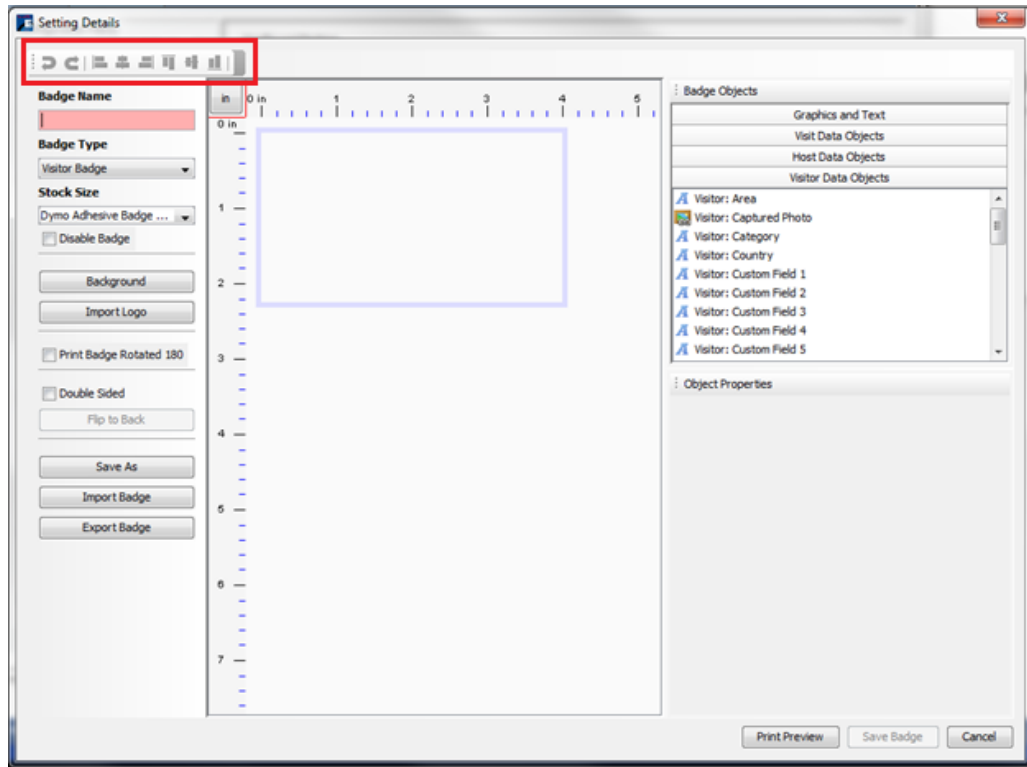










When you highlight the logo, the Object Properties display in the lower right corner of the screen. You can determine the rotation direction and degree of the image, the image scaling, the horizontal and vertical alignment and whether to maintain the image's aspect ratio (of width to height).

7. To Print Badge Rotated 180, select the check box. This will print the badge rotated 180 degrees.
8. For a Double Sided badge, select the check box. This will create a badge with front and back sides. Select the "Flip to Back" button to lay out the backside of the badge. When printing, two consecutive badge labels will print with one for front and the second for back.
9. Use the Save As button to create a new badge based on the current badge.
10. Import & Export Badge – Badges can be imported into PassagePoint and/or saved externally.
  - To import a badge design, click Import Badges Button. The file chooser dialog window appears allowing you to select a file for import or specify a name and location to export a file to.
  - Use the Export Badge Button to save the current badge to an external file. The file chooser dialog window appears allowing you to specify a name and location for the file. Name your file with a .badge extension.

## Toolbar

The Toolbar is used to undo or redo the last action and align the objects on the badge layout.



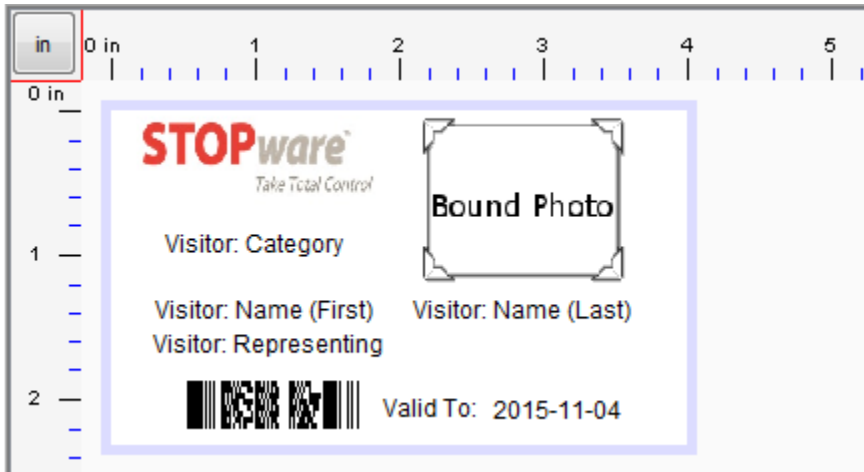
-  Undo the last action
-  Redo the last undo
-  Left align objects on the badge
-  Center align objects on the badge
-  Right align objects on the badge
-  Top align objects on the badge
-  Middle align objects on the badge
-  Bottom align objects on the badge

To align objects, select the objects you want aligned using the shift button on your keyboard to select all the objects and click on the desired alignment button.



## Badge Layout

The Badge Layout section shows you what is on the badge template.



## Badge Objects

Objects listed in Badge Objects may be added to the badge layout canvas by dragging the object directly onto the canvas. To delete any items on the canvas, select it and press the <Delete> key. The Objects are displayed with their object names, these names are replaced automatically with the actual data from the PassagePoint database at the time that the badge or label is printed.

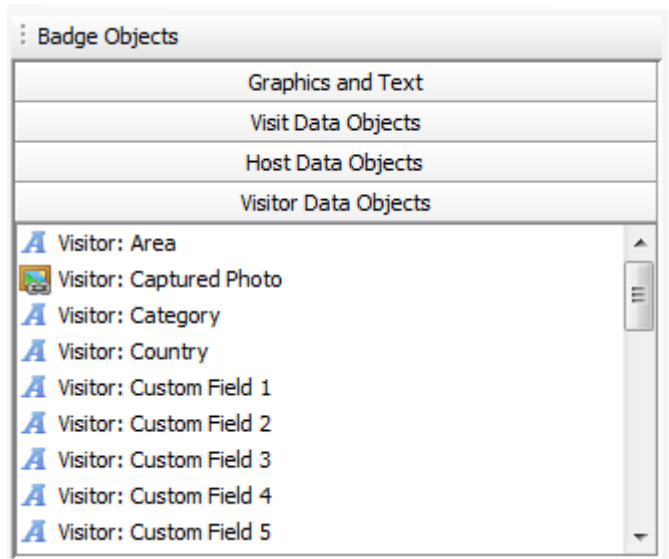
There are four sections of Badge Objects:

Graphics and Text – contains barcodes, signature image, rectangle, and text box

Visit Data Objects – contains visit information – includes purpose of visit, valid from/to, destination, access card information, and pre-registration information, etc.

Host Data Objects – contains host information – includes name, photo, department, email, etc.

Visitor Data Objects – contains visitor information – includes name, photo, category, email, phone, etc.



### Object Properties

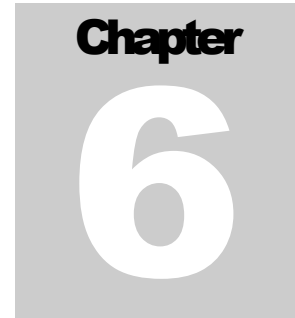
When you select an object on the Badge Layout section, the Object Properties display. The Object Properties allow you to configure how an object displays on the badge. Each object type has its unique property settings.

- All objects can be rotated 90 degrees by clicking on the rotate counter -clockwise or clockwise icon.
- Text fonts listed are those which are installed on the local Windows machine.
- Set justification of text with the Alignment dropdown.
- Color of text and background for an object can be set by clicking sample color box.
- For photos, check Maintain Aspect Ratio to keep the image from being stretched.
- The corners of rectangles can be curved by setting a corner radius.
- Dates can be formatted by selecting the example format from the Date Format dropdown list.
- Barcode encoded information can be mapped by selecting the appropriate field from the list.

### Print Preview

A sample of how the badge or label will appear can be viewed by clicking “Print Preview”. This may not be an accurate representation of your printed badge since length of data will vary.

Save the Badge with the Save Badge button.



## Chapter 6 – Policy Manager

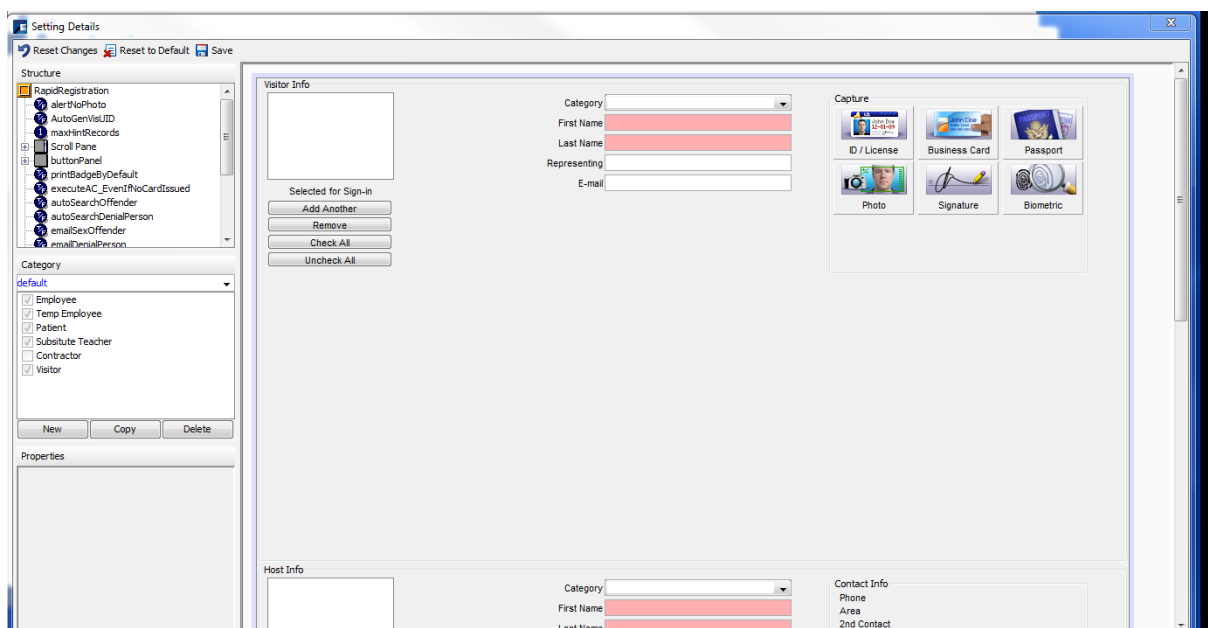
The Policy Manager is used to configure screens for each center, barcode scanning processes, badge printing processes, and screen configuration for the Kiosk. There are four policies in PassagePoint Global.

### SCREEN POLICY

The Screen Policy is where you define what elements are on the screens for the centers: Security, Directory, Visit, Home, Deletion Policy, Report, Print Search Result1, Tracking, and the Kiosk.

To configure screen policies:

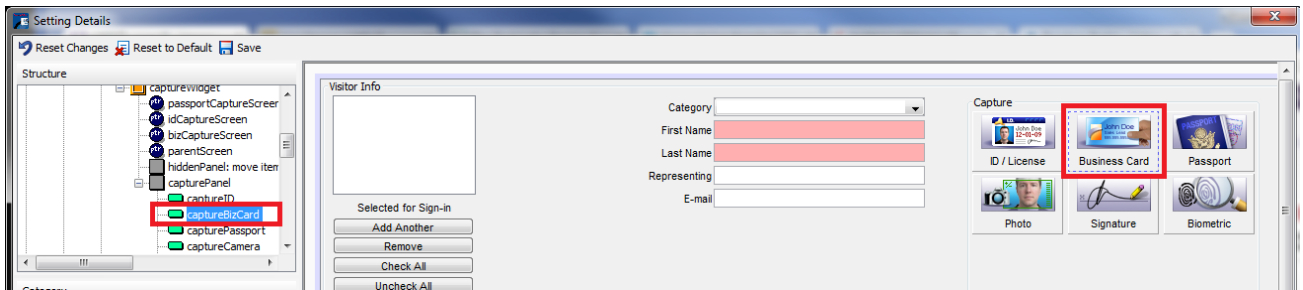
1. From Home | Configure | Policy Manager | Screen Policy
2. From the Configured Polices screen, select the Screen Type from the drop down list. The choices are Main Center Screens and Kiosk screens. You can also filter the screens to display only configured screens or only un-configured screens or all screens.
3. From the list of Screens, using the Plus sign navigate to and chose the desired screen to configure. To add a new policy, select the Add button. To edit an existing screen policy, select the Edit button.
4. The Setting Details for the Screen Policy screen appears.



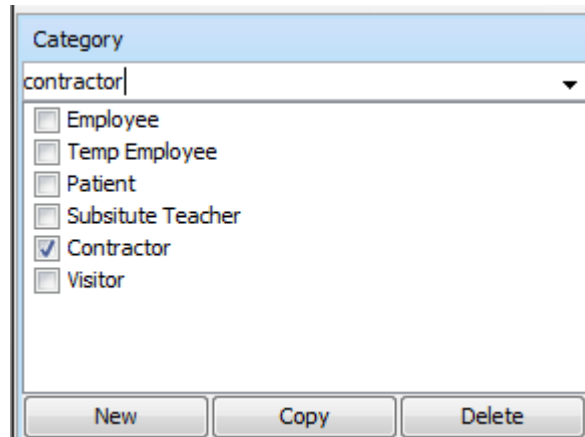
You can use the Setting Details screen to add/remove fields, change field titles, add fields, enable/disable fields, hide/show fields, and make fields required.

The Setting Details for the Screen Policy Screen is comprised of four sections: Structure, Category, Properties, and a mock-up of the actual screen layout.

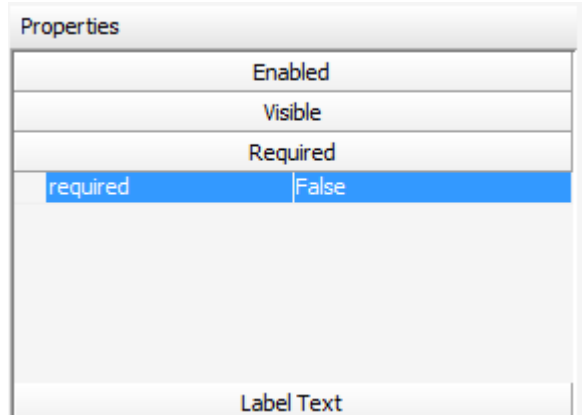
- **Structure:** displays the hierarchy of the all the items on the screen layout.
  - **Category:** allows you to assign the Screen Policy to a specific category or several categories or to the default of all categories.
  - **Properties:** allows you to determine whether an object is enable, visible, required, or if you can change the value.
  - **Screen Layout:** displays the layout of all the objects on the screen
5. To add/change an object on the screen, select the object. The Structure box automatically expands to the location of the object.



6. In the Category box, select the desired category/categories for the change by selecting it from the drop down list. If the desired category/categories is not listed, create a new one with the New button.
7. Change the Category label from Untitled# to the desired label by highlighting it and typing the desired name.
8. Select the desired category/categories by selecting the checkbox next to the category.
9. Make sure that the desired category is showing at the top of the Category box.



10. In the Properties box make the desired change:



- a. To Enable/disable: select Enabled. The setting for enabled appears. Click on the setting, the options appear. Chose True to enable the field and False to disable the field.
- b. To hide a field or make it visible: select Visible. The setting for enabled appears. Click on the setting, the options appear. Chose True to show the field and False to hide the field.
- c. To make required: select Required. The setting for required appears. Click on the setting, the options appear. Chose True to make the field required and False to make the field optional.
- d. Other options are dependent on the object selected.

They include: Label Text

- Title
- Input Mask
- Input Regex
- value Change Event Delay MilliSecs
- selected (if the object is a checkbox)

11. Select the Save button on the top right to save changes to the screen. If desired you may, reset the changes to the last saved change or reset to the default settings or you can exit the screen to void all changes you made.

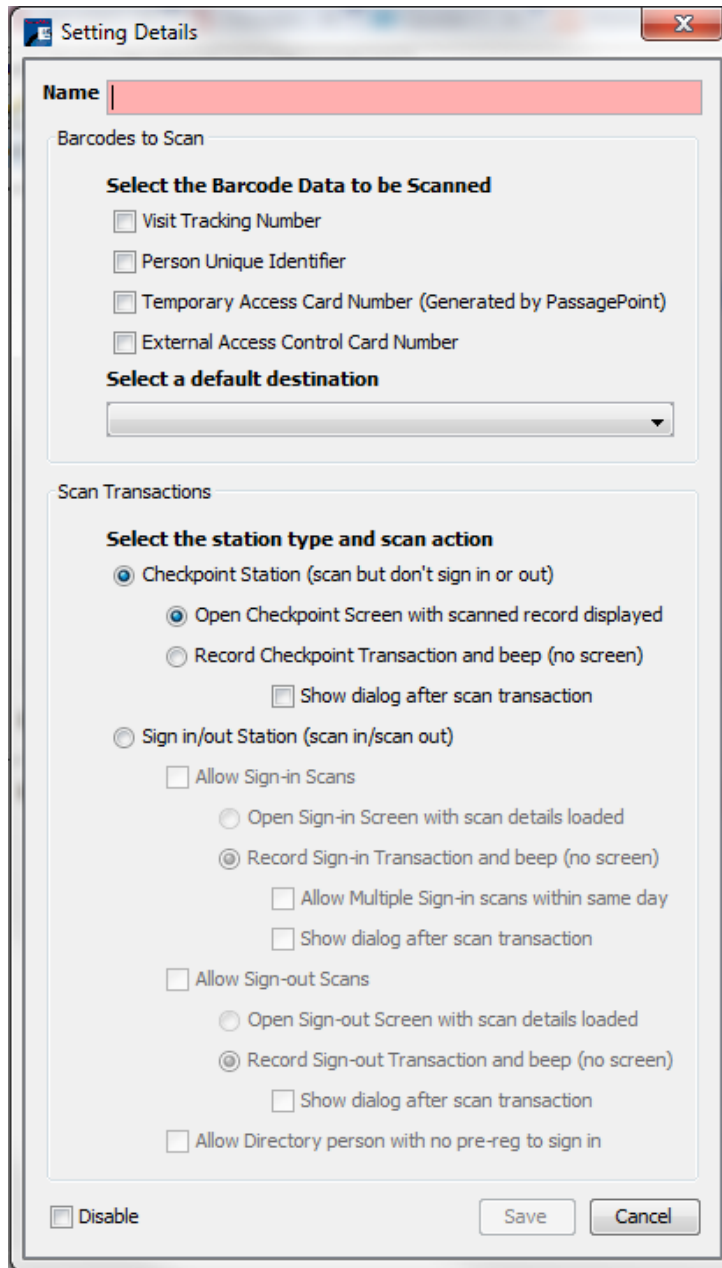
See Addendum for a listing of the Main Center Screens, Options and Fields.

## BARCODE SCAN POLICY

The Barcode Scan Policy allows you to determine which barcode types are scanned and for which transactions.

To configure a Barcode Scan Policy:

1. From Home | Configure | Policy Manager | Barcode Scan Policy
2. The Setting Details for the Barcode Scan Policy screen appears.



3. Enter a name for the Barcode Scan Policy.
4. Select the type of data to be scanned. The choices are:

- Visit Tracking Number – the number of the visit
- Person Unique Identifier – the visitor's number
- Temporary Access Card Number (generated by PassagePoint)
- External Access Control Card Number

5. Select the default destination from the drop down list.
6. Select the station type and scan action.

- a. Checkpoint Station. This will scan the barcode, but not check the visitor in or out.
  - Open Checkpoint Screen with scanned record displayed
  - Record Checkpoint Transaction and beep
    - Show dialog after scan transaction
- b. Sign in/out Station. This will scan the barcode and check the visitor in/out.
- c. Allow Sign-in Scans
  - Open Sign-in Screen with scan details loaded
  - Record Sign-in Transaction and beep
    - Allow Multiple Sign-in scans within same day
    - Show dialog after scan transaction
- d. Allow Sign-out Scans
  - Open Sign-out Screen with scan details loaded
  - Record Sign-out Transaction and beep
    - Allow Multiple Sign-out scans within same day
    - Show dialog after scan transaction
- e. Allow Directory person with no pre-reg to sign in. This allows a person who is in the PassagePoint Directory to sign in with a barcode scan without having been pre-registered.

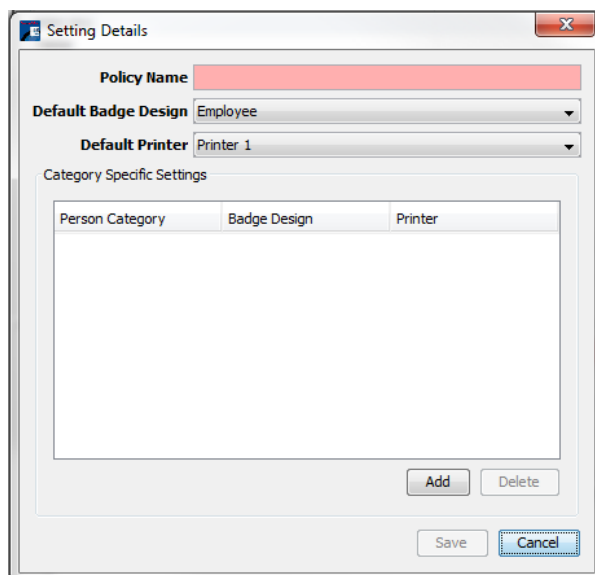
7. Select the Save button.

## BADGE PRINTING POLICY

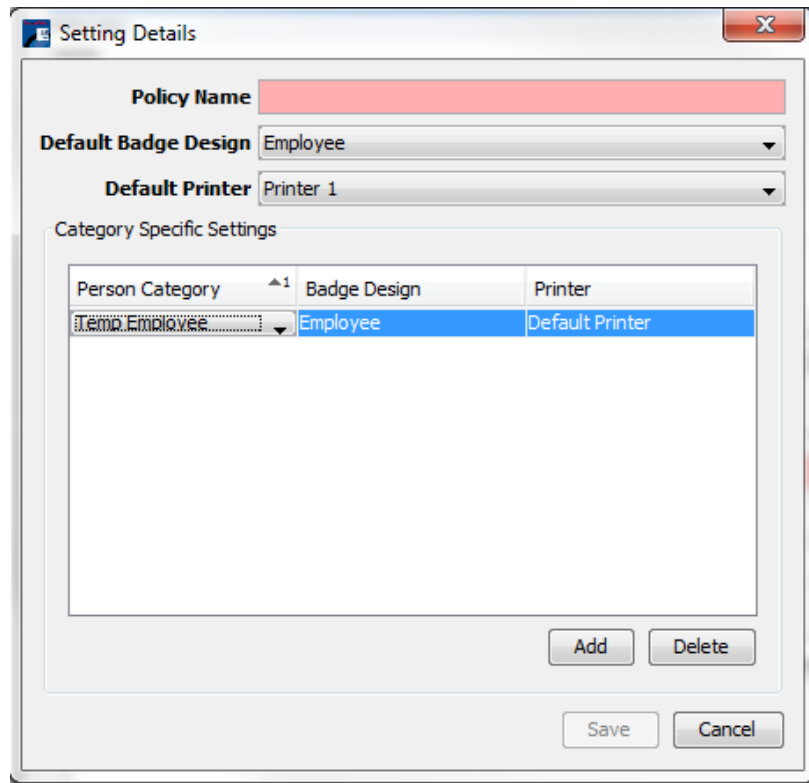
The Badge Printing Policy allows you to determine which badge will automatically print for a specific category.

To configure a Badge Printing Policy:

1. From Home | Configure | Policy Manager | Badge Printing Policy
2. The Setting Details for the Badge Printing Policy screen appears.



3. Enter a name for the Badge Printing Policy
4. Select the system defaults for the badge design and printer.
5. Set Category specific badge designs and printers, select the Add button.



6. The default category, badge design, and printer display.
7. Use the down arrow on the fields to select the desired category, badge design and printer for that category. Repeat to add all desired category badge printing combinations.
8. Select the Save button.

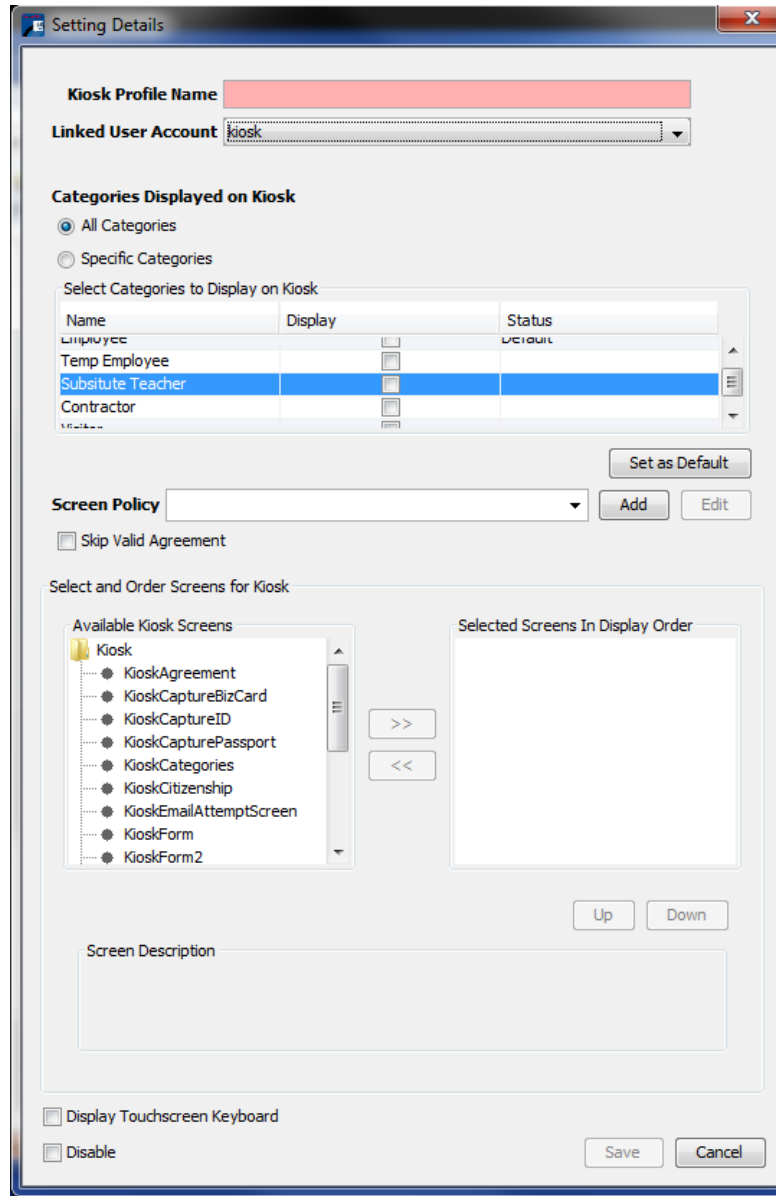
## SIGN-IN KIOSK PROFILES

The Sign-in Kiosk Profiles is where you define the screens and screen order for the Kiosk.

To configure a Kiosk Profile:

1. From Home | Configure | Policy Manager | Sign-in Kiosk Profiles
2. The Setting Details for the Sign-in Kiosk Profile screen appears.





3. Enter a name for the Kiosk Profile.
4. Choose a user account from the drop down list for the Kiosk.
5. Choose if all Categories or only specific categories display on the kiosk by selecting the Specific Categories radio button and then the desired category check box in the display column. If you select more than one category, you can set one as a default by selecting the Set as Default button. In the Status column, you will see the category selected as Default.

**Categories Displayed on Kiosk**

All Categories  
 Specific Categories

Select Categories to Display on Kiosk

Name	Display	Status
Temp Employee	<input checked="" type="checkbox"/>	
Substitute Teacher	<input checked="" type="checkbox"/>	
Contractor	<input checked="" type="checkbox"/>	
Visitor	<input checked="" type="checkbox"/>	Default

6. Select the Screen Policy for use on the Kiosk (the default is kiosk screens, you may have created another kiosk screen policy) by selecting it from the drop down list or clicking the Add button to add a new one. You may also edit the screens with the Edit Button.
7. Select the desired screen and add it to display screens by selecting the  button. To re-order the screens, click the screen name in the Selected Screens in Display Order box and select the Up or Down buttons to move the screen to the desired order.

The available kiosk screens are:

**Kiosk Agreement –**  
Agreement form for signing with the signature pad

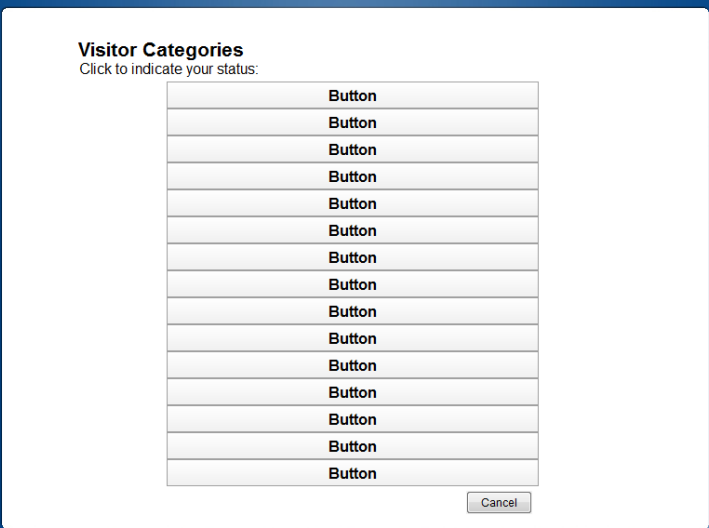
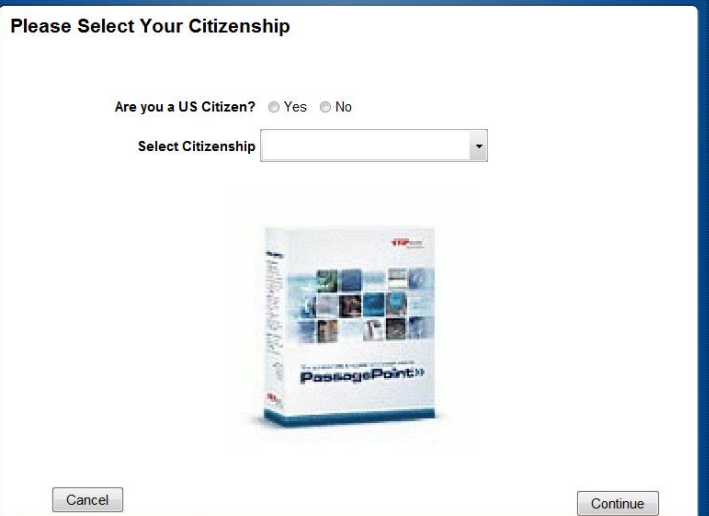
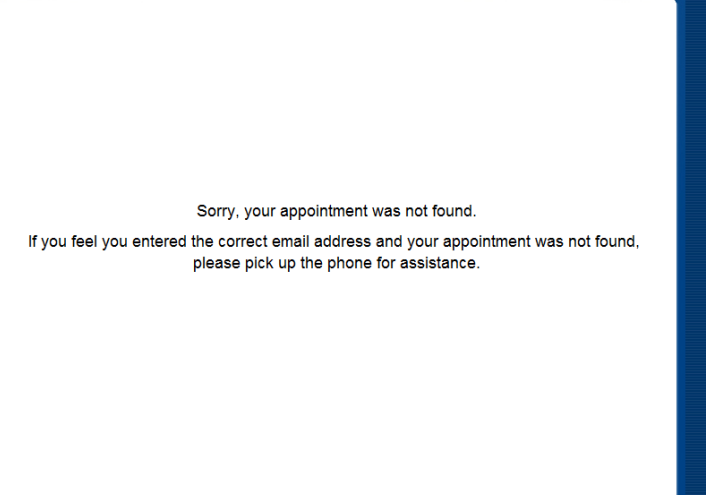
**Agreements**  
Please accept the terms and conditions:

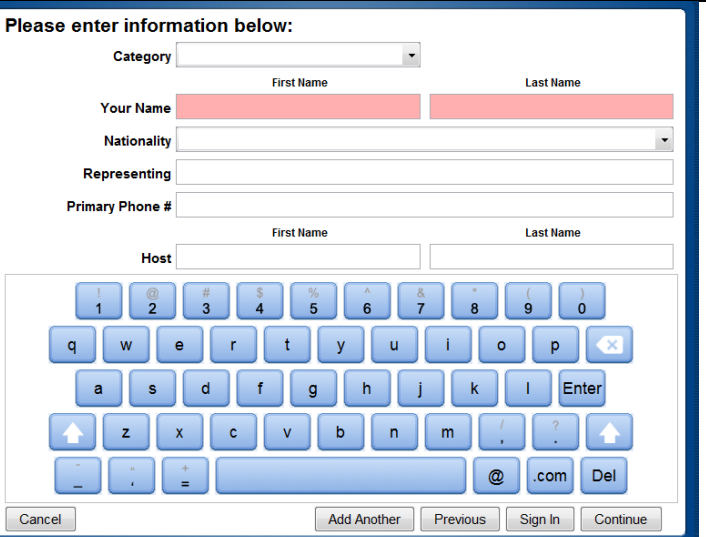
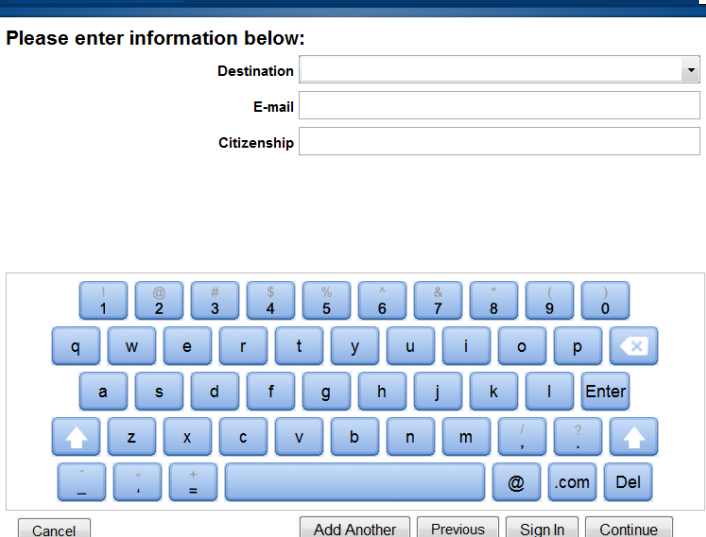
Agreement

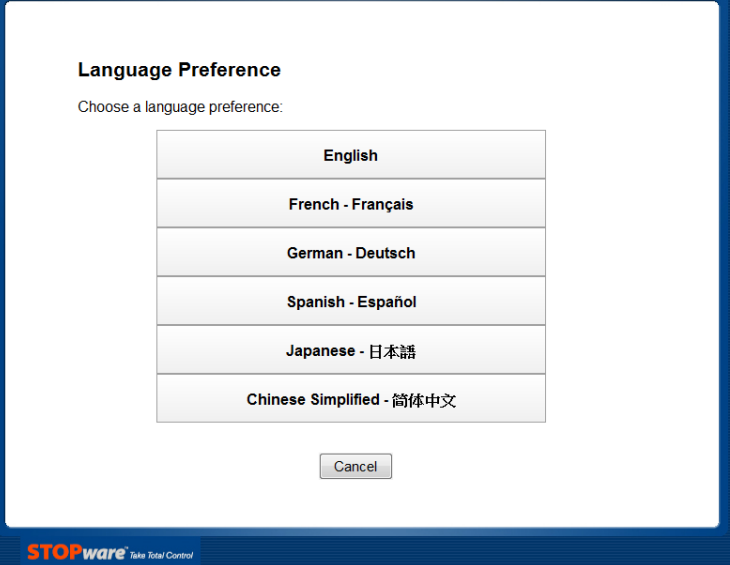
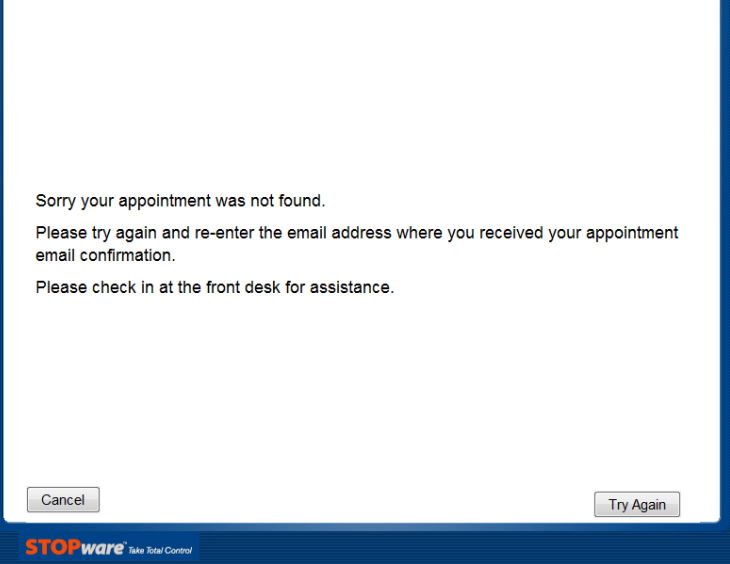
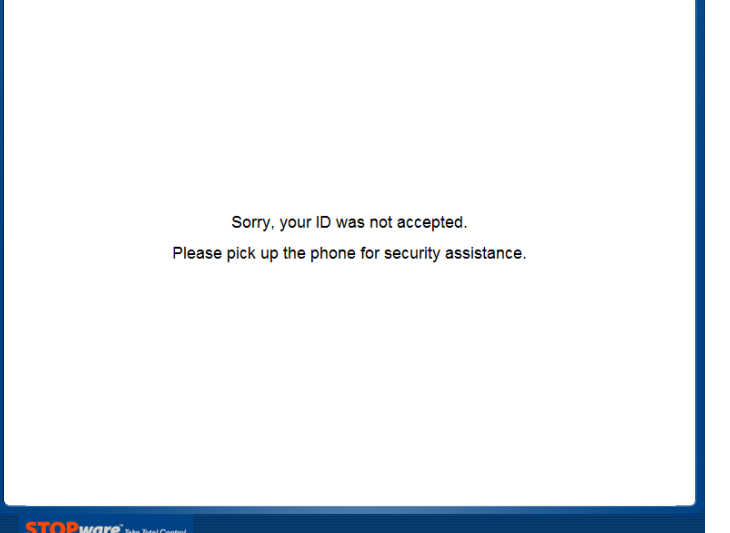
Use the signature pad to sign the above agreement

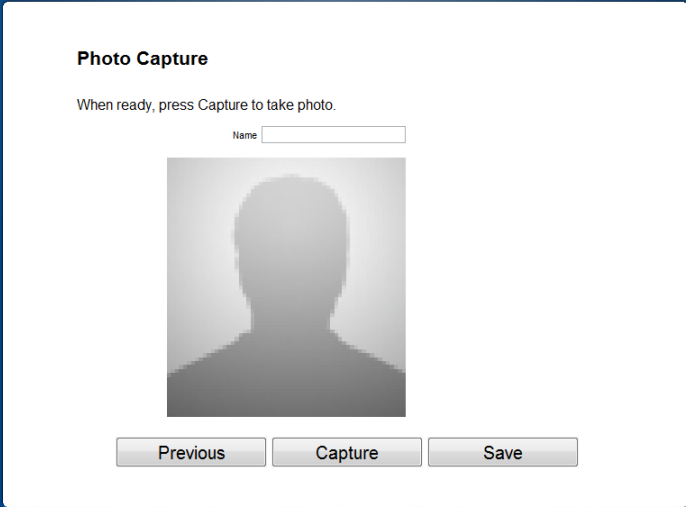

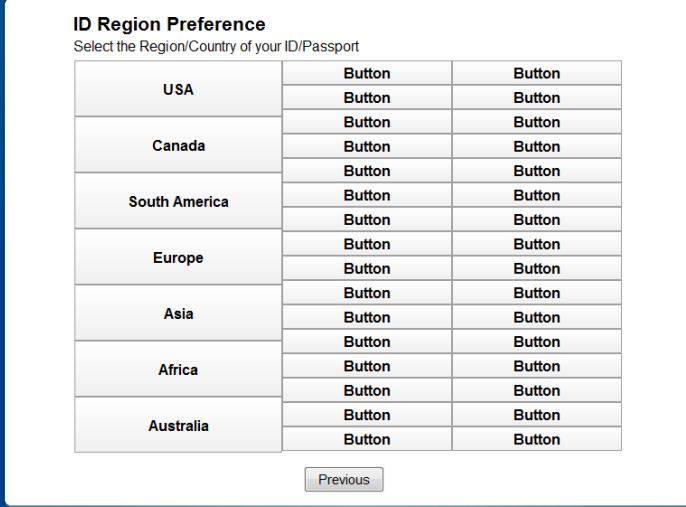
**STOPware** Take Total Control

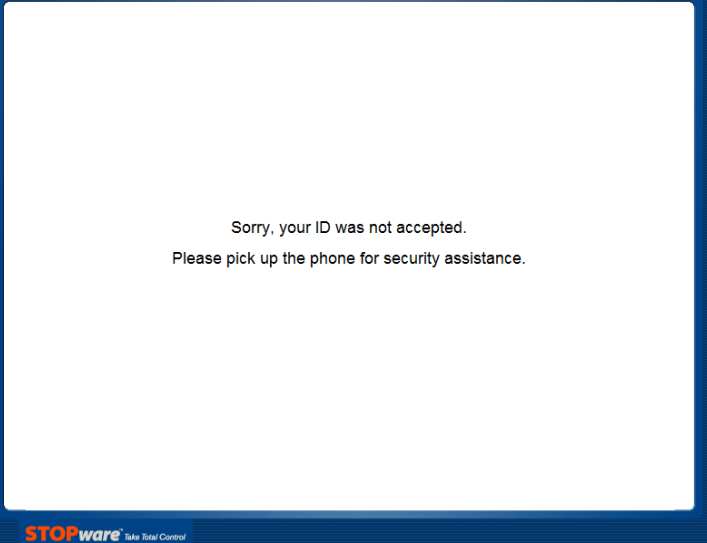
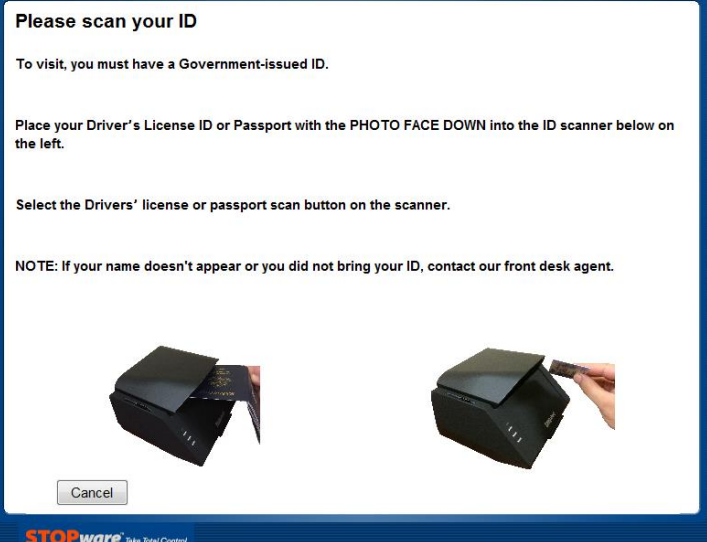
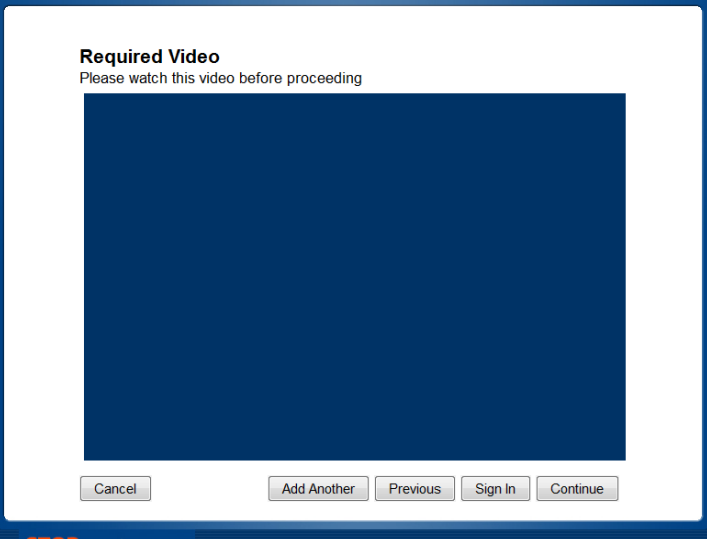
<p>Kiosk Capture Biz Card – Capture business card with a scanner</p>	
<p>Kiosk Capture ID – Capture ID or Driver License with a scanner</p>	
<p>Kiosk Capture Passport – Capture Passport with a scanner</p>	

<p>Kiosk Categories – Select Visit Categories</p>	
<p>Kiosk Citizenship – Select citizenship</p>	
<p>Kiosk Email Attempt Screen – notification to kiosk visitor that their visit was not found by searching by their email address.</p>	

<p>Kiosk Form – input name, representing, host</p>	 <p>The screenshot shows a kiosk form titled "Please enter information below:". It contains the following fields: "Category" (dropdown), "Your Name" (split into "First Name" and "Last Name" with red input boxes), "Nationality" (dropdown), "Representing" (text input), "Primary Phone #" (text input), and "Host" (split into "First Name" and "Last Name" with white input boxes). Below the fields is a blue virtual keyboard with buttons for numbers, letters, symbols, and navigation. At the bottom are buttons for "Cancel", "Add Another", "Previous", "Sign In", and "Continue". The STOPware logo is at the bottom left.</p>
<p>Kiosk Form 2 – input destination, email, citizenship</p>	 <p>The screenshot shows a kiosk form titled "Please enter information below:". It contains the following fields: "Destination" (dropdown), "E-mail" (text input), and "Citizenship" (text input). Below the fields is a blue virtual keyboard with buttons for numbers, letters, symbols, and navigation. At the bottom are buttons for "Cancel", "Add Another", "Previous", "Sign In", and "Continue". The STOPware logo is at the bottom left.</p>

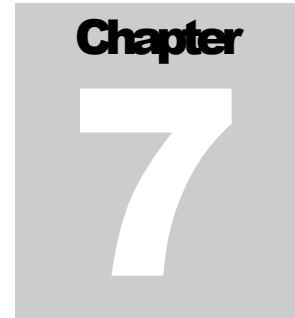
<p>Kiosk Language – select kiosk interface language</p>	
<p>Kiosk Message no Email Match –</p>	
<p>Kiosk Message no Scan Match - notification to kiosk visitor that their ID was not accepted by the scanner</p>	

<p>Kiosk Photo – capture photo using a digital cam</p>																																				
<p>Kiosk Prereg Look up</p>																																				
<p>Kiosk Region – select region for ID/Passport scanning</p>	 <table border="1" data-bbox="755 1375 1299 1764"> <tr> <td rowspan="2">USA</td> <td>Button</td> <td>Button</td> </tr> <tr> <td>Button</td> <td>Button</td> </tr> <tr> <td rowspan="2">Canada</td> <td>Button</td> <td>Button</td> </tr> <tr> <td>Button</td> <td>Button</td> </tr> <tr> <td rowspan="2">South America</td> <td>Button</td> <td>Button</td> </tr> <tr> <td>Button</td> <td>Button</td> </tr> <tr> <td rowspan="2">Europe</td> <td>Button</td> <td>Button</td> </tr> <tr> <td>Button</td> <td>Button</td> </tr> <tr> <td rowspan="2">Asia</td> <td>Button</td> <td>Button</td> </tr> <tr> <td>Button</td> <td>Button</td> </tr> <tr> <td rowspan="2">Africa</td> <td>Button</td> <td>Button</td> </tr> <tr> <td>Button</td> <td>Button</td> </tr> <tr> <td rowspan="2">Australia</td> <td>Button</td> <td>Button</td> </tr> <tr> <td>Button</td> <td>Button</td> </tr> </table>	USA	Button	Button	Button	Button	Canada	Button	Button	Button	Button	South America	Button	Button	Button	Button	Europe	Button	Button	Button	Button	Asia	Button	Button	Button	Button	Africa	Button	Button	Button	Button	Australia	Button	Button	Button	Button
USA	Button		Button																																	
	Button	Button																																		
Canada	Button	Button																																		
	Button	Button																																		
South America	Button	Button																																		
	Button	Button																																		
Europe	Button	Button																																		
	Button	Button																																		
Asia	Button	Button																																		
	Button	Button																																		
Africa	Button	Button																																		
	Button	Button																																		
Australia	Button	Button																																		
	Button	Button																																		

<p>Kiosk Scan Attempt Scan</p>	
<p>Kiosk Scan Passport ID -</p>	
<p>Kiosk Video – show a video clip</p>	



8. Select the checkbox to display a keyboard on the touchscreen, if desired.
9. Select the Save button.



## Chapter 7 – External Systems

External Systems is where you specify the settings to connect PassagePoint Global to other information systems. This includes importing information such as employees, visitors, and watch lists.

### DATA MIGRATION

Data Migration allows you to migrate data from the earlier version of PassagePoint, 4.5 into PassagePoint Global.

The image shows a "Data Migration Configuration" dialog box with the following fields and controls:

- Data Migration Name:** A dropdown menu with "PassagePoint 4.5 Data Migration" selected.
- Auto-Create Missing Data (Locations, Categories):** An unchecked checkbox.
- Watch List for imported entries:** A dropdown menu.
- Access Control System for imported Cards:** A dropdown menu.
- User Role for all imported Users:** A dropdown menu.
- Web Interface for all imported Users:** A dropdown menu.
- Filename containing Exported Data:** A text field with a red background and a "Browse ..." button to its right.
- Authorizer for Web Pre-Registrations:** A section titled "Set Linked Person" containing:
  - Linked Person:** A text input field.
  - Remove:** A button.
  - Search:** A button.

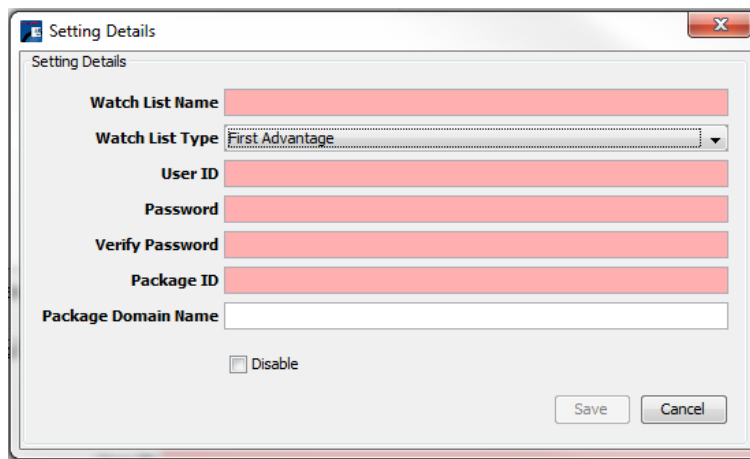
At the bottom right of the dialog are "Save" and "Cancel" buttons.

## EXTERNAL WATCH LISTS

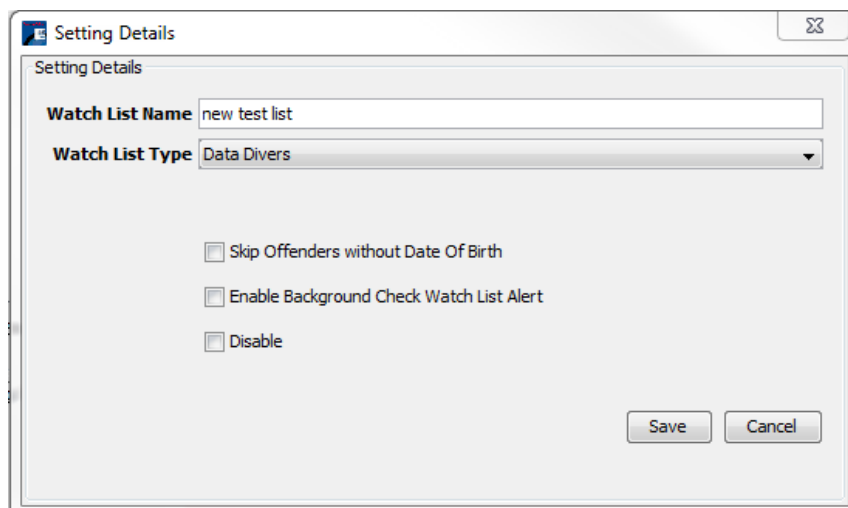
The External Watch Lists allows you to configure the screening services compatible with PassagePoint Global. The current screening services are Sex Offender Screening via Data Divers and Government Denied Party via MK Data. Previous providers are First Advantage and BCG Direct.

To add a screening service:

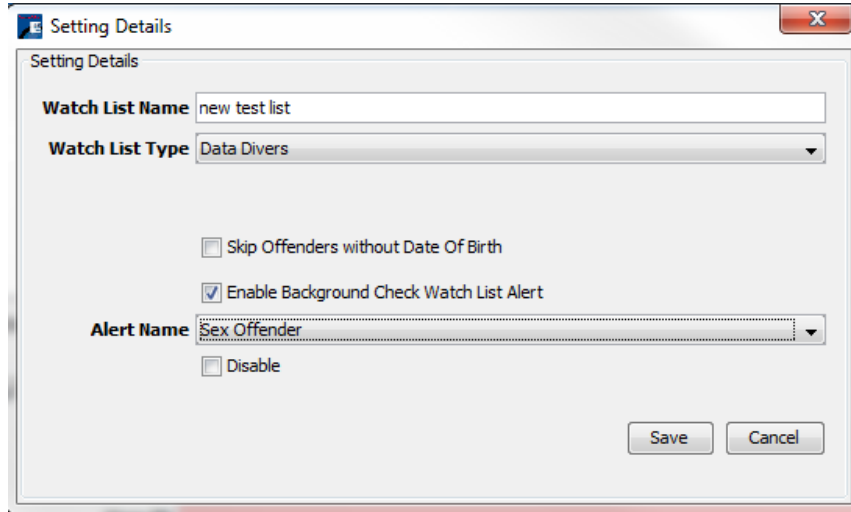
1. From Home | Configure System| External Systems | External Watch Lists, select the Add button.
2. The Setting Details for the Watch List screen appears.



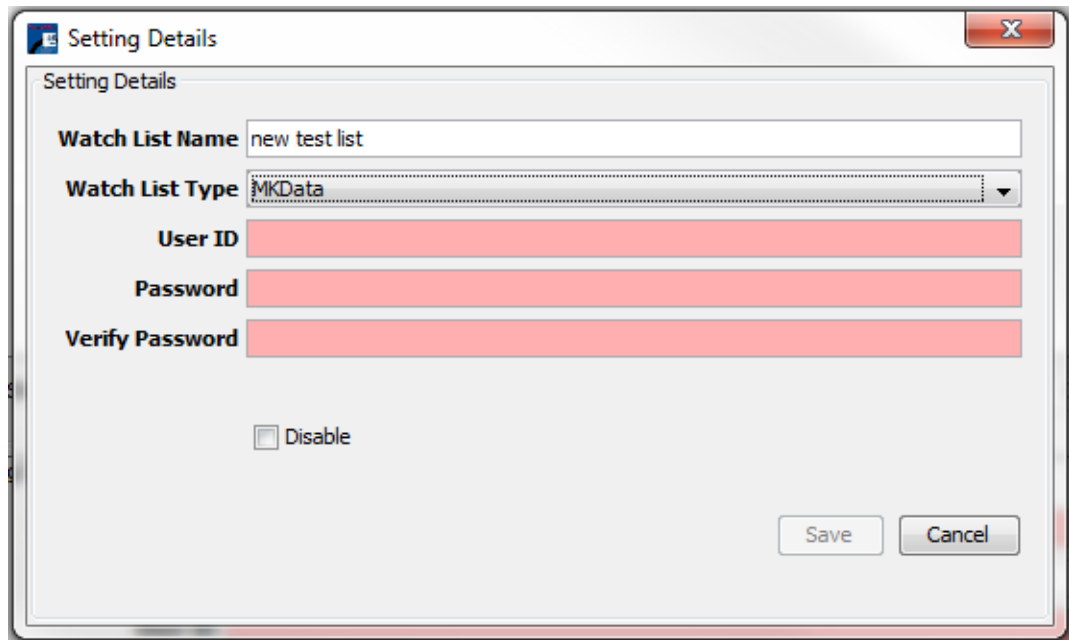
3. Enter a name in the Watch List Name field and select the Watch List Type from the dropdown list. The screen will change dependent on the Type chosen.
4. If you chose DataDivers for the Sex Offender Screening, the following screen appears: NOTE: you must purchase a license and the screening service in order to use Sex Offender Screening.



5. Select the desired options:
  - a. Skip Offenders without Data of Birth
  - b. Enable Background Check Watch List Alert  
When this option is selected, you are given the option to choose the Alert Type.



- c. Disable
6. Then select the Save button.
7. If you chose MK Data for the Sex Offender Screening, the following screen appears:



8. Enter your User ID, Password and Verify the Password.
9. Select the Save button.

## IMPORT MAPPINGS

The Import mappings allow you to configure the Data Set, File Format, and Column Mapping for importing People, Watch Lists, or Access Cards into PassagePoint Global.

To add a mapping:

1. From Home | Configure System| External Systems | Import Mappings, select the Add button.
2. The Setting Details for the Import Mappings screen appears.

**Setting Details**

**Import Name** [Redacted]

**Data Set**

- Import People (Directory, Visitors, etc)
  - Category** Visitor
  - Import Watch List
    - Watch Lists** Internal
    - Threat Level** medium
    - Configure Web Link Roles
  - Import Access Card

**File Format**

- Column Separator** Comma
- Column Enclosed By** None
- Duplicates** Append
- Start Import with Row** 0
- Key Field**
- Key Field**
- Photo Folder** [Browse...]

**Column Mapping**

[Redacted]

Test Add Column Delete Column Save Cancel

3. Enter a name in the Import Name field.
4. Choose a Data Set – the choices are: People, Watch List, or Access Card.
5. Choose the Column Separator – the choices are: Comma, Tab, Space, Semicolon
6. Choose the Column Enclosed By – the choices are: None, Single Quote, Double Quote. None is the default.
7. Choose a method to deal with Duplicates – the choices are: Append, Replace, Skip. **Append** will add the information into PassagePoint even if someone similar already exists. **Replace** replaces existing information with the information from the import. **Skip** skips the information if it already exists.
8. Select the row using the up and down arrow to set the starting row for Start Import with Row.
9. The Key Fields can only be selected after you mapped the columns. **You must map at least one of the following fields in order to select a key field and to continue with the import.**
  - Person: Unique ID
  - Person: E-mail
  - Person: Phone 1
  - Person: Phone 2
  - Person: Mobile Phone No.
10. If applicable, use the Browse button to select the location for the Photo Folder.
11. Add columns to map by selecting the Add Column button. Add as many columns as you need.
12. Map the columns by selecting the column (default name on added columns is “Skip”) and choose the field to map/import from the drop down list.
13. Use the Test button to test your import mapping with a file to check if you selected the desired fields.
14. Select the Save button. You can now use the mapping when importing information in the Directory Center.

## Chapter 8 – System Administration

System Administration is where you configure settings for PassagePoint Global such as, clock format, time zone, and date format. You can also access tools for the database.

### GLOBAL SETTINGS

To configure Global Settings:

1. From Home | Configure | System Administration, select Global Settings.
2. The Configure Global Settings screen displays.

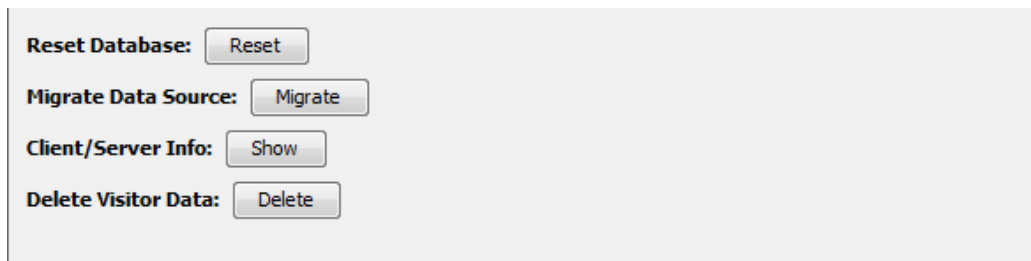
3. Select the desired settings for:
  - a. Clock Format – 12 hour or 24 hour
  - b. Time Zone – from the drop down list select your time zone
  - c. Date Format – from the drop down list select the desired date format
  - d. Destination UI – if Enterprise Control Center is enabled, select the checkbox to use the List Pane for Destination Selection
  - e. Intellihint – select the checkbox to use Intellihint by Category
  - f. Category – select this box to force the user to choose a category

- g. Auto Refresh Rate – Select Global Configuration for the refresh rate to affect all stations; select Per Station Preferences Settings and set the rate on each station under Home>Station Preferences. Enter the number of seconds for the refresh rate.
- h. Search Tabs – select the number of maximum number of records returned in a search. Two hundred is the default and 1000 is the max.
- i. List Result Tabs - select the number of maximum number of records returned in a search. Two hundred is the default and 1000 is the max.
- j. Select the checkbox to enable the Print Multiple Badge button on the Pre-Registration Search results.
- k. Custom Package Management – Acuant SDK – select the specific version or the Latest from the drop down list.

## DATABASE TOOLS

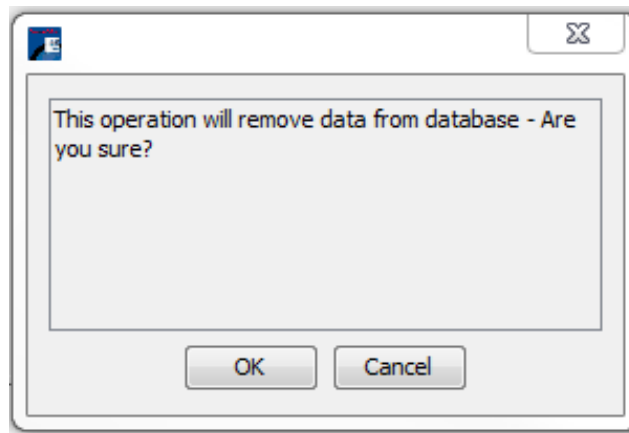
To access the Database Tools:

1. From Home | Configure | System Administration, select Database Tools.
2. The Database Tools display



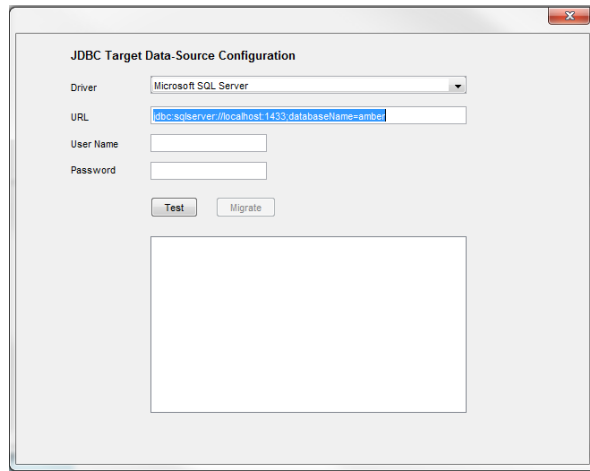
- a. Reset Database – allows you to reset the database to the default settings and removes data from the database.

NOTE: If you reset the database you will lose all visitor information and settings you have made to the database. Resetting the database was intended for new installs after testing. Use Delete Visitor data to remove visitor information and leave setting changes.

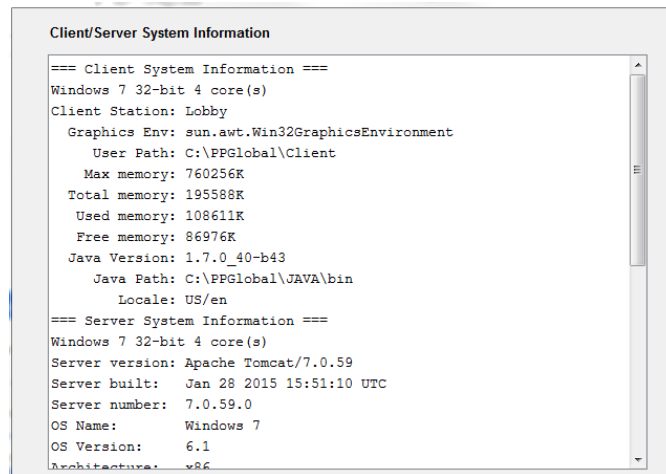




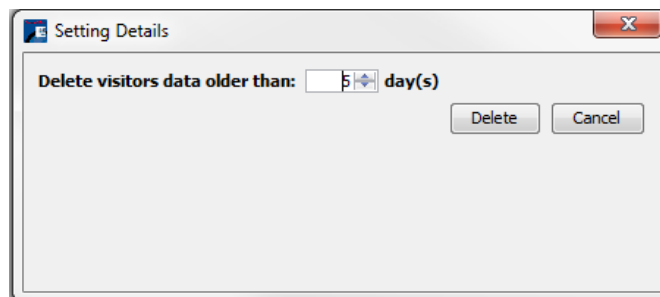
- b. Migrate Data Source - allows you to migrate from one SQL Database to a different SQL Database. For example, migrating data from PostgreSQL to Microsoft SQL.



- c. Client/Server Info – displays the information for the Client System and the Server



- d. Delete Visitor Data – allows you to delete data for visitors older than the selected number of days.

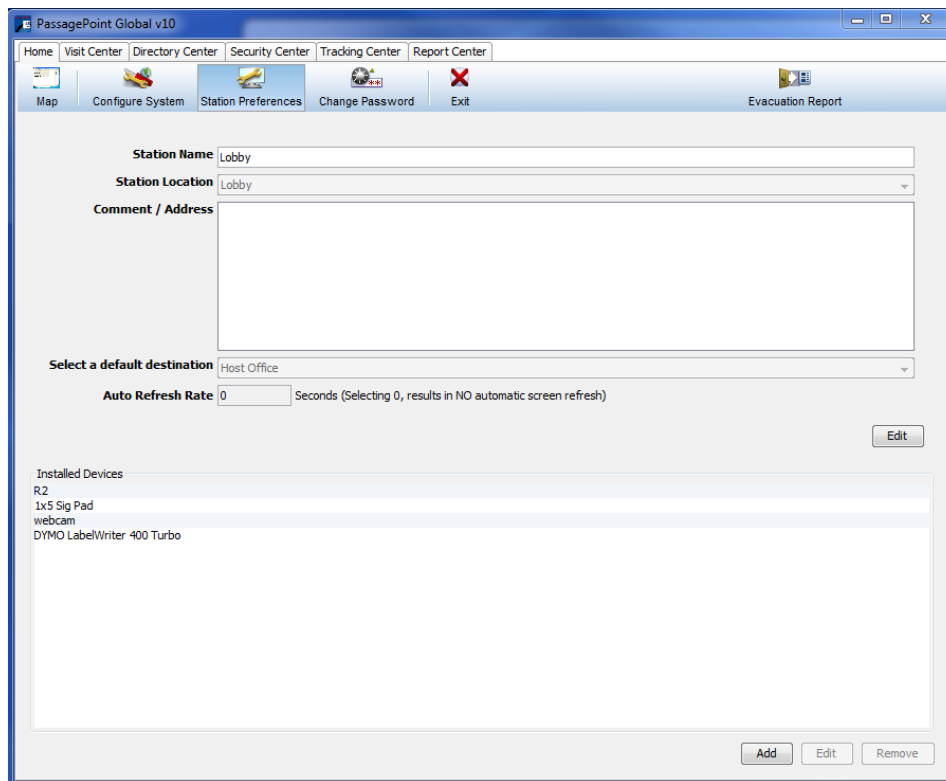


## Chapter 9 – Station Preferences

Station Preferences is where you configure settings for the PassagePoint Global client workstation. You can set the station name, location, address, and the hardware devices installed on the workstation.

To configure Station Preferences:

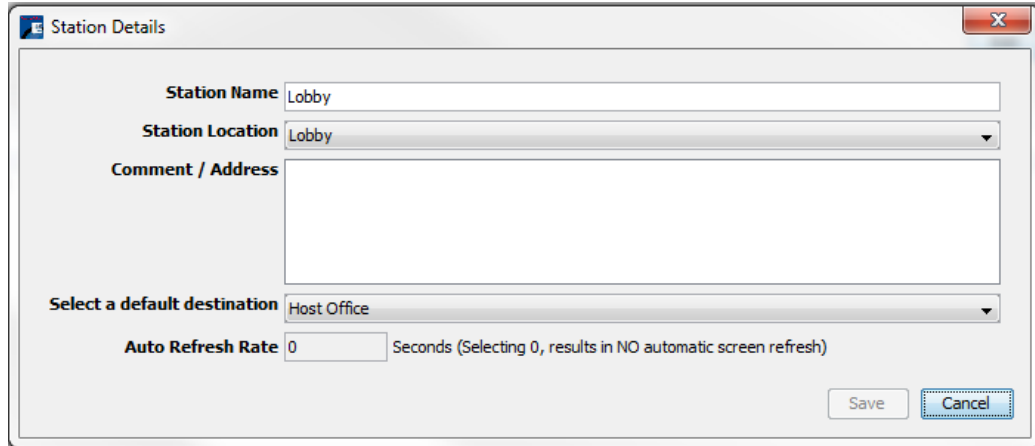
1. Navigate to Home | Station Preferences
2. The current Station preferences display.



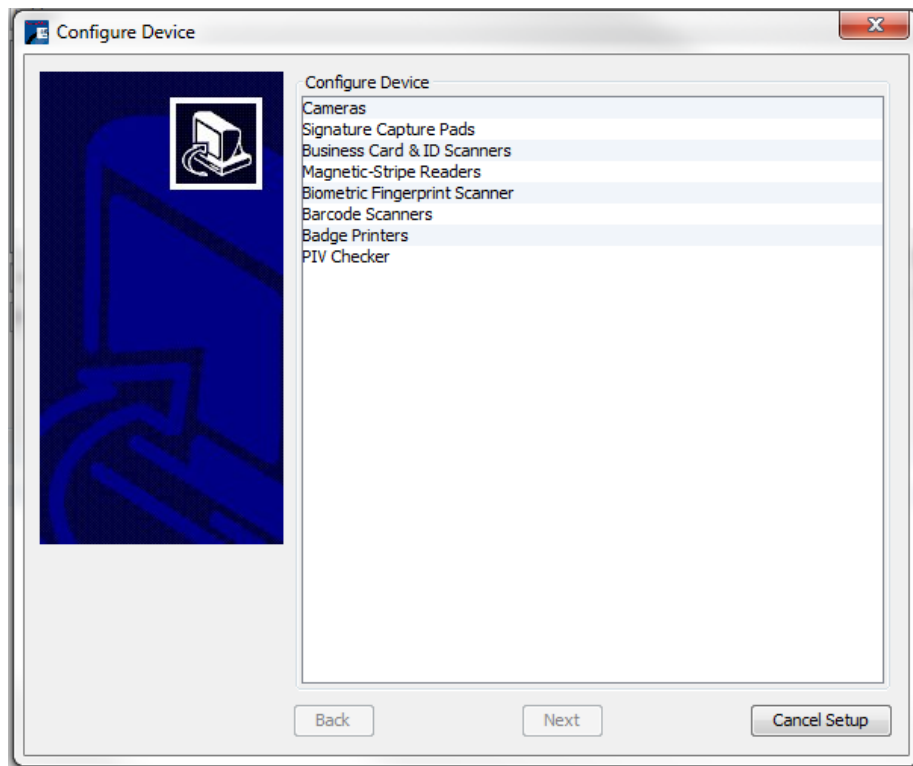
The screenshot shows the 'PassagePoint Global v10' application window. The 'Station Preferences' tab is active. The interface includes a navigation bar with options: Home, Visit Center, Directory Center, Security Center, Tracking Center, and Report Center. Below this is a toolbar with icons for Map, Configure System, Station Preferences, Change Password, and Exit. The main content area contains the following fields and controls:

- Station Name:** Text input field containing 'Lobby'.
- Station Location:** Dropdown menu showing 'Lobby'.
- Comment / Address:** Large text area for notes.
- Select a default destination:** Dropdown menu showing 'Host Office'.
- Auto Refresh Rate:** Input field set to '0' with the text 'Seconds (Selecting 0, results in NO automatic screen refresh)'.
- Edit button:** A button to modify the station settings.
- Installed Devices:** A list box containing:
  - R2
  - 1x5 Sig Pad
  - webcam
  - DYMO LabelWriter 400 Turbo
- Buttons:** 'Add', 'Edit', and 'Remove' buttons at the bottom right.

3. To change the station name, location, address, default location and auto refresh rate, select the Edit button.
4. The Station Details screen displays.



5. Make the desired changes and select the Save button.
6. To add hardware to the station, select the Add button at the bottom of the screen under the Installed Devices section.
7. The Configure Device screen displays.



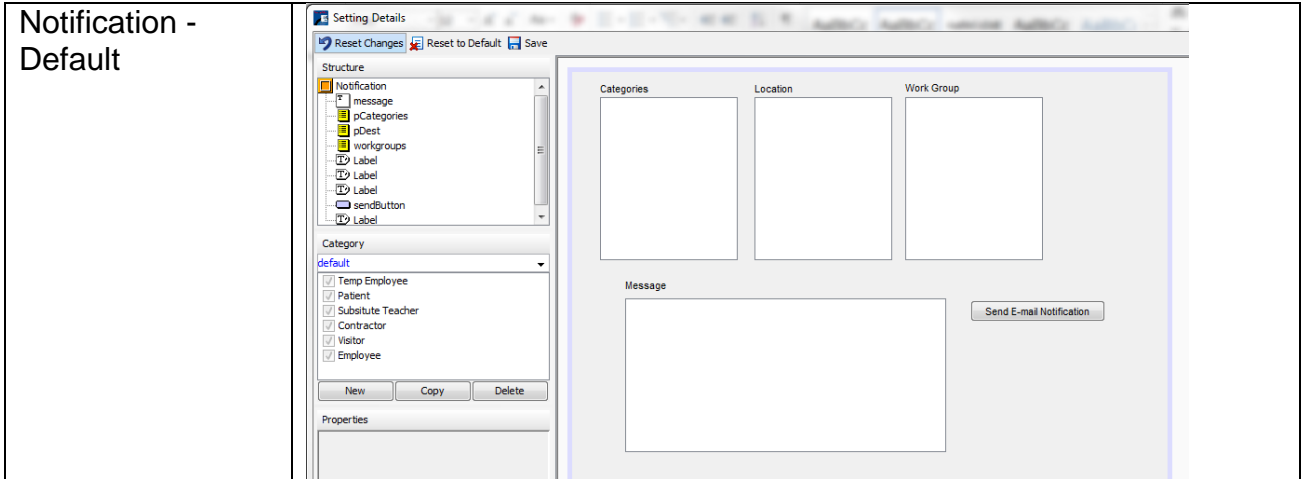
8. Select the desired device type and the Next button.
9. Select the desired model from the list and the Next button.
10. Enter associated information as requested and when finished, select the Finish button. The device is installed and is displayed in the Installed Devices list.

## Addendum – Screens, Options and Fields

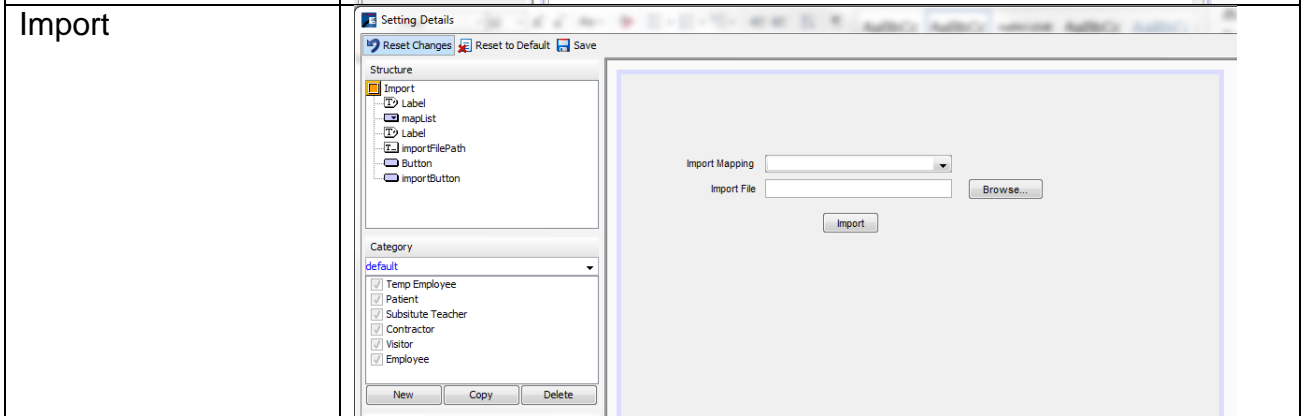
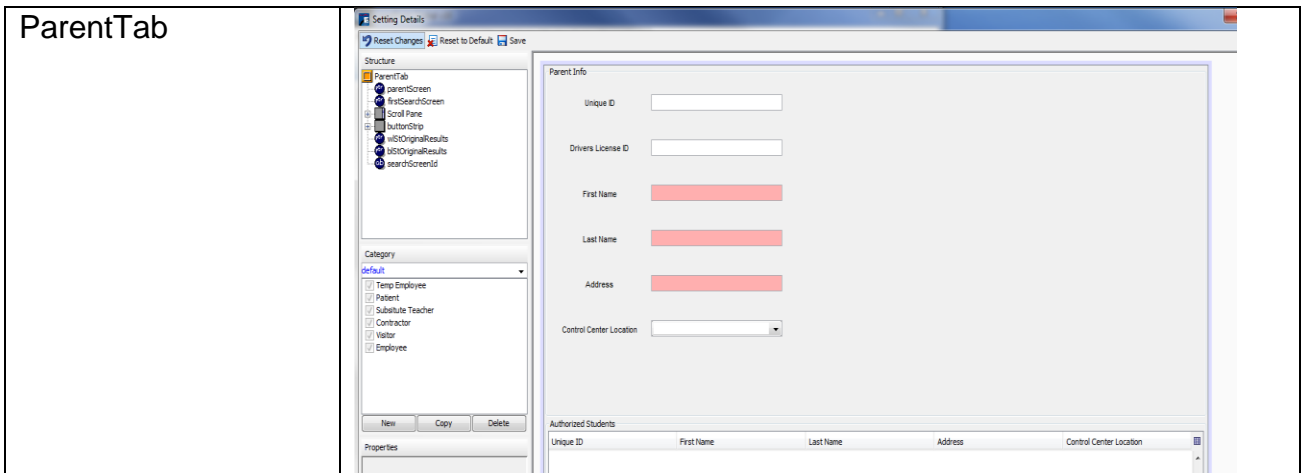
### SCREENS

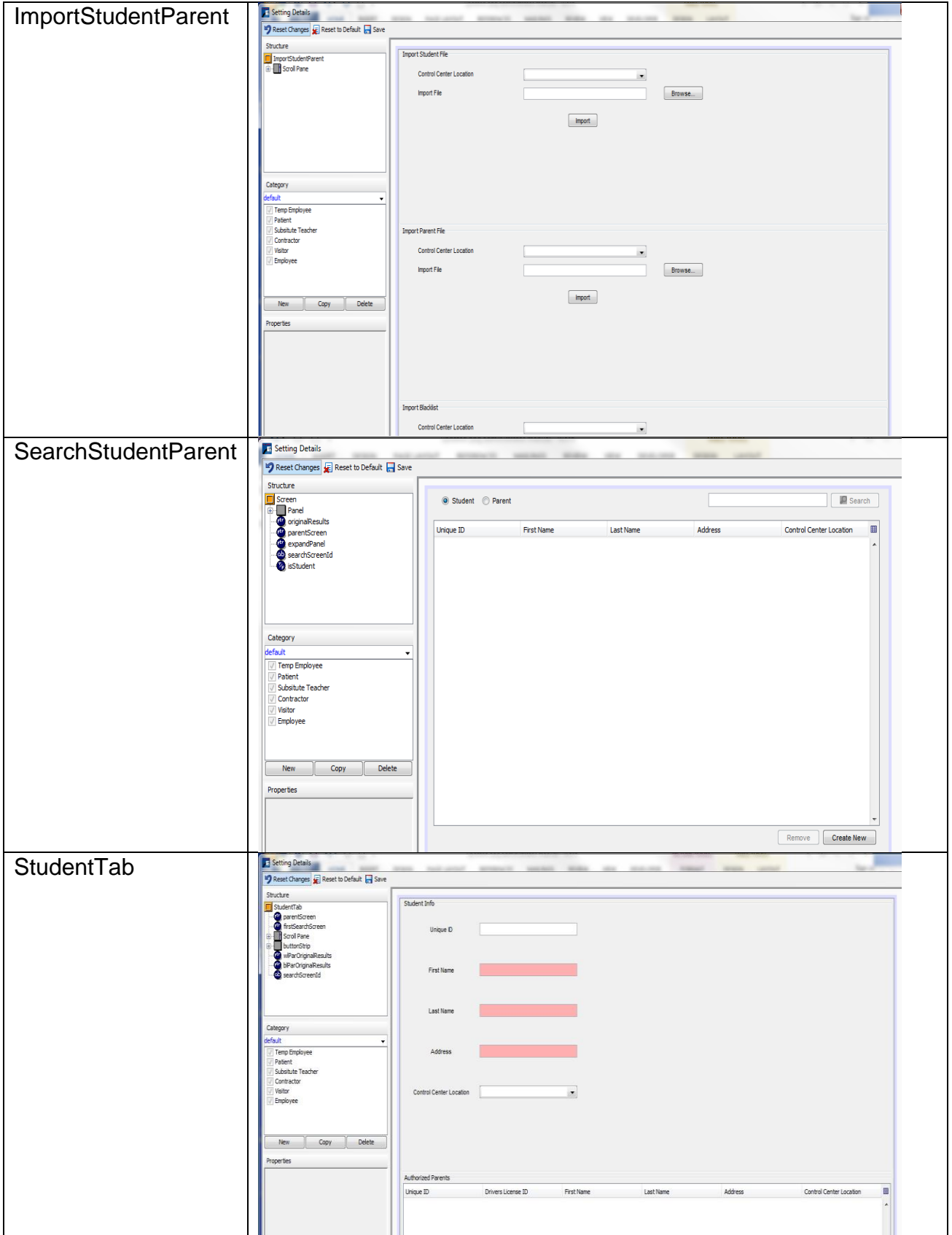
Security Center screens:

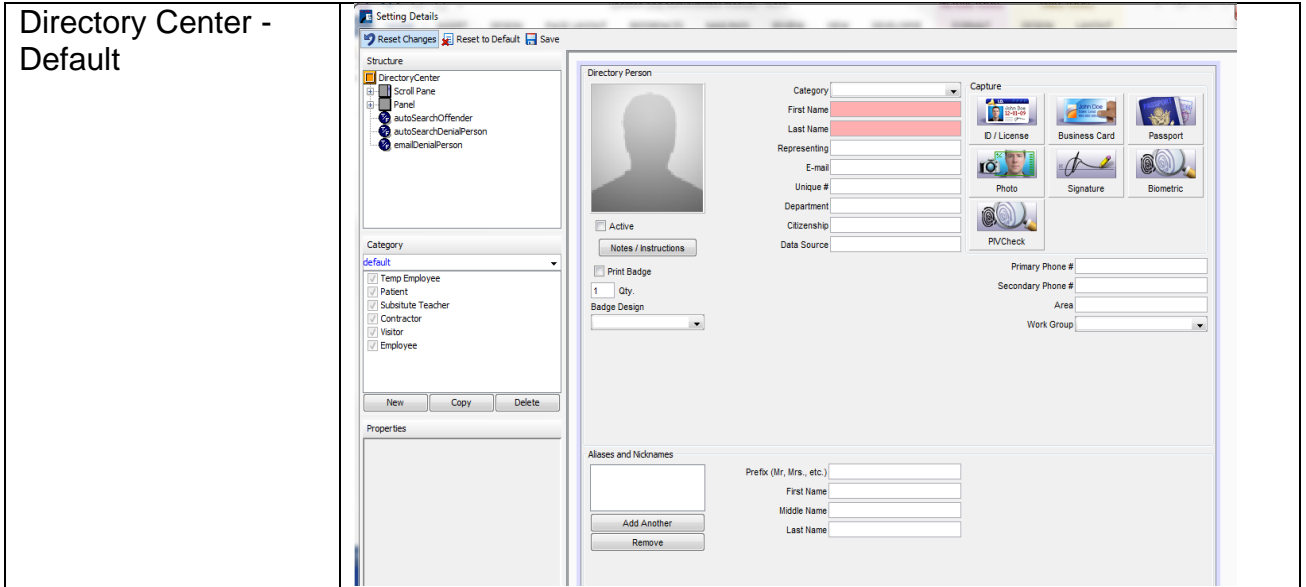
<p>External List</p>	
<p>Watch List</p>	
<p>TabScnDenied – Today's Denials Screen</p>	
<p>TabScnAlerts – Active and Historic Alerts Screen</p>	



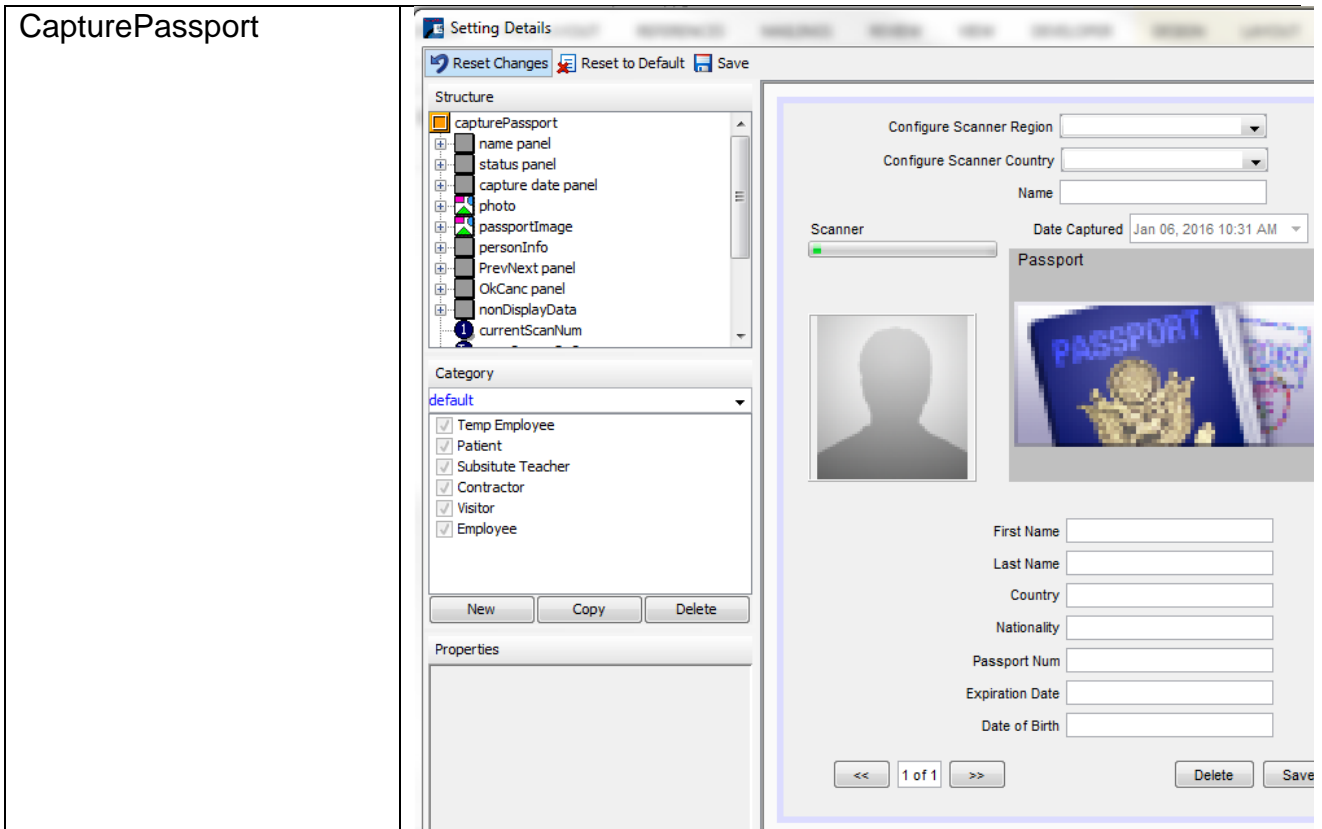
Directory Center screens:

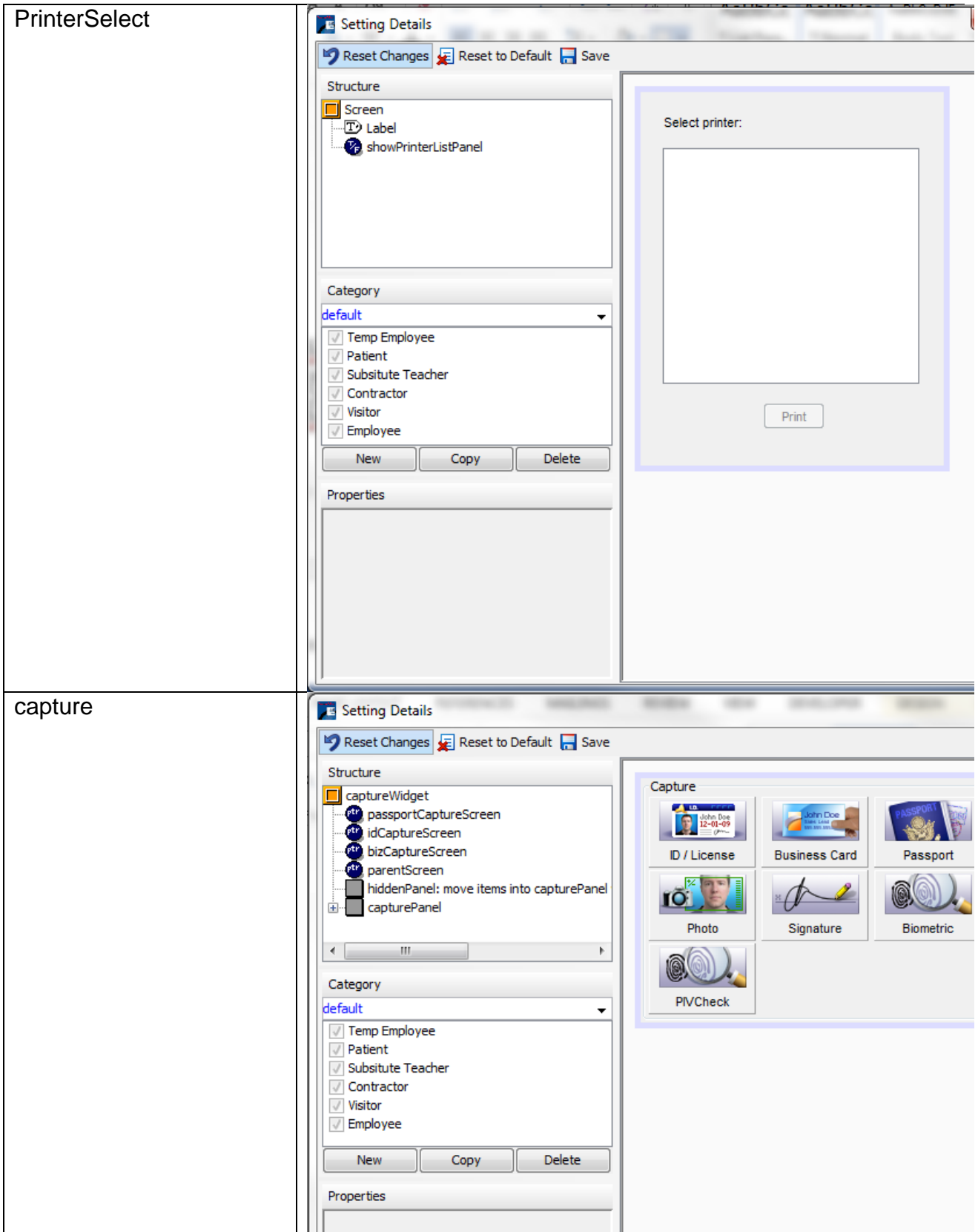




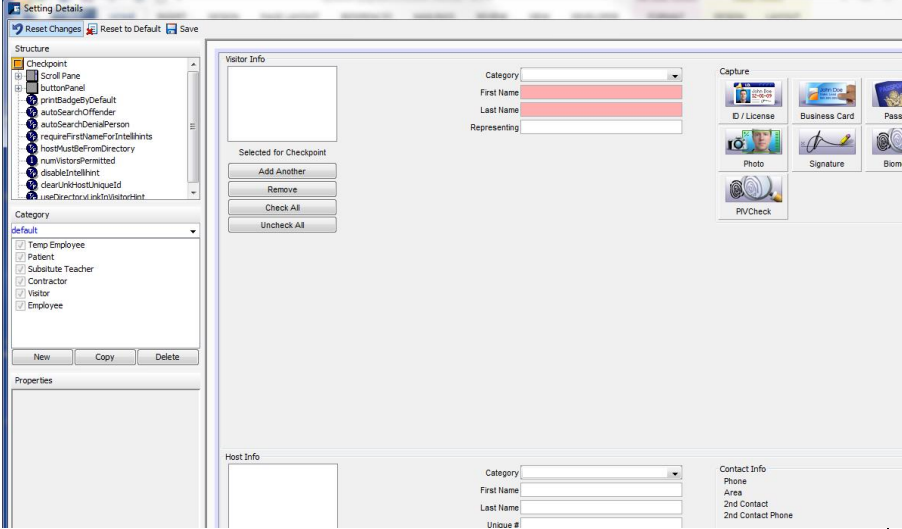
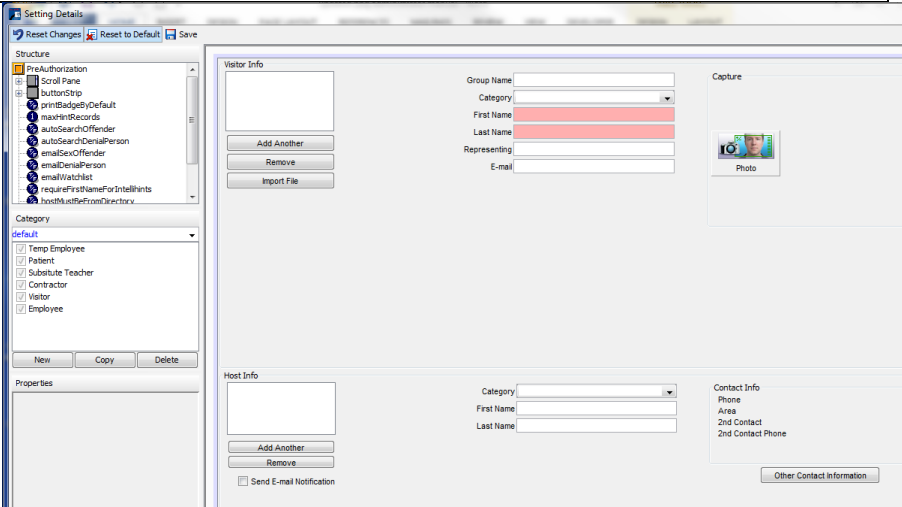


Visit Center screens:







<p>Checkpoint</p>	
<p>PreAuthorization</p>	

captureID

Setting Details

Reset Changes | Reset to Default | Save

Structure

- captureID
- personFullName
- status panel
- face
- licenseImage
- capture date panel
- personInfo
- PrevNext panel
- OkCanc panel
- nonDisplayData
- parentScreen

Category

default

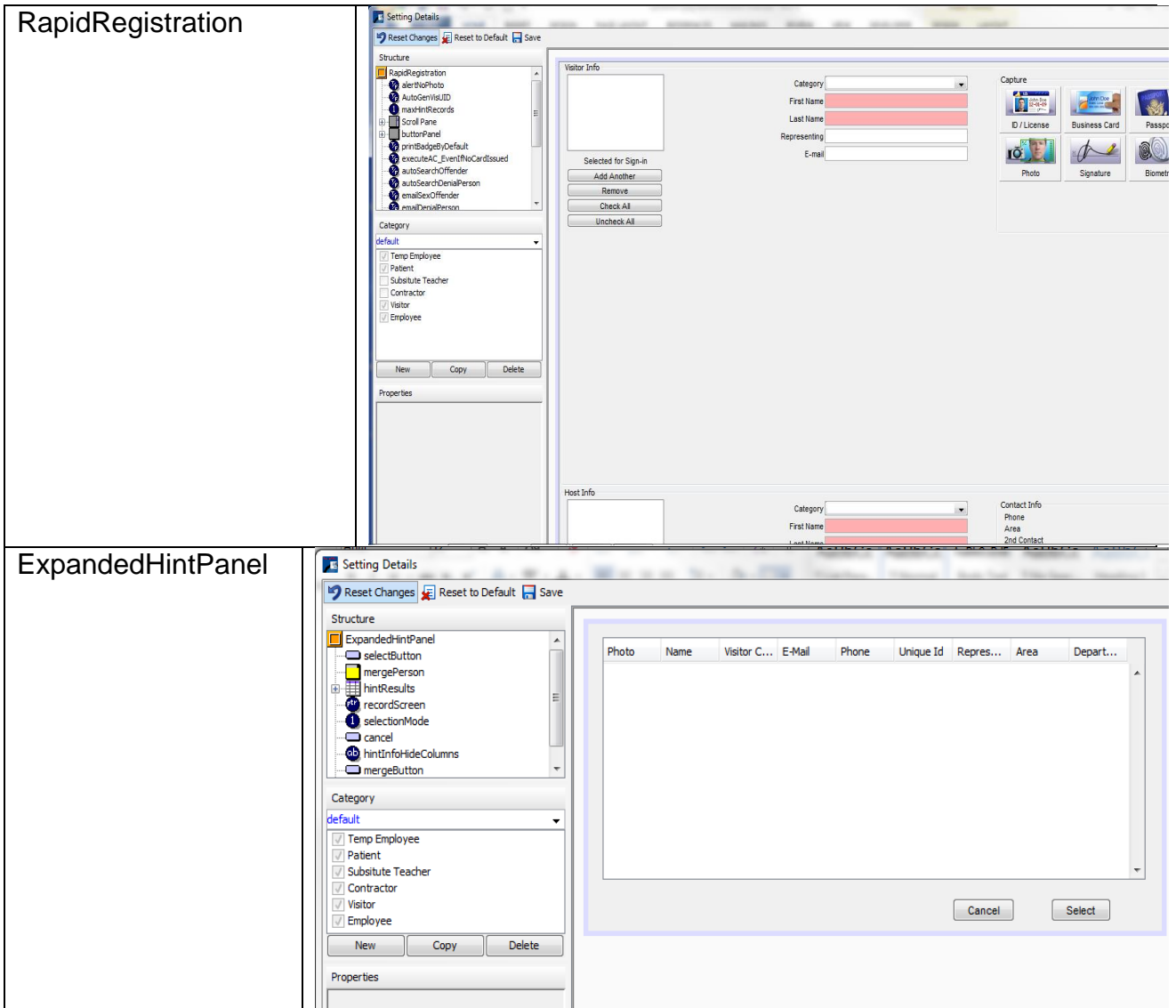
- Temp Employee
- Patient
- Substitute Teacher
- Contractor
- Visitor
- Employee

New | Copy | Delete

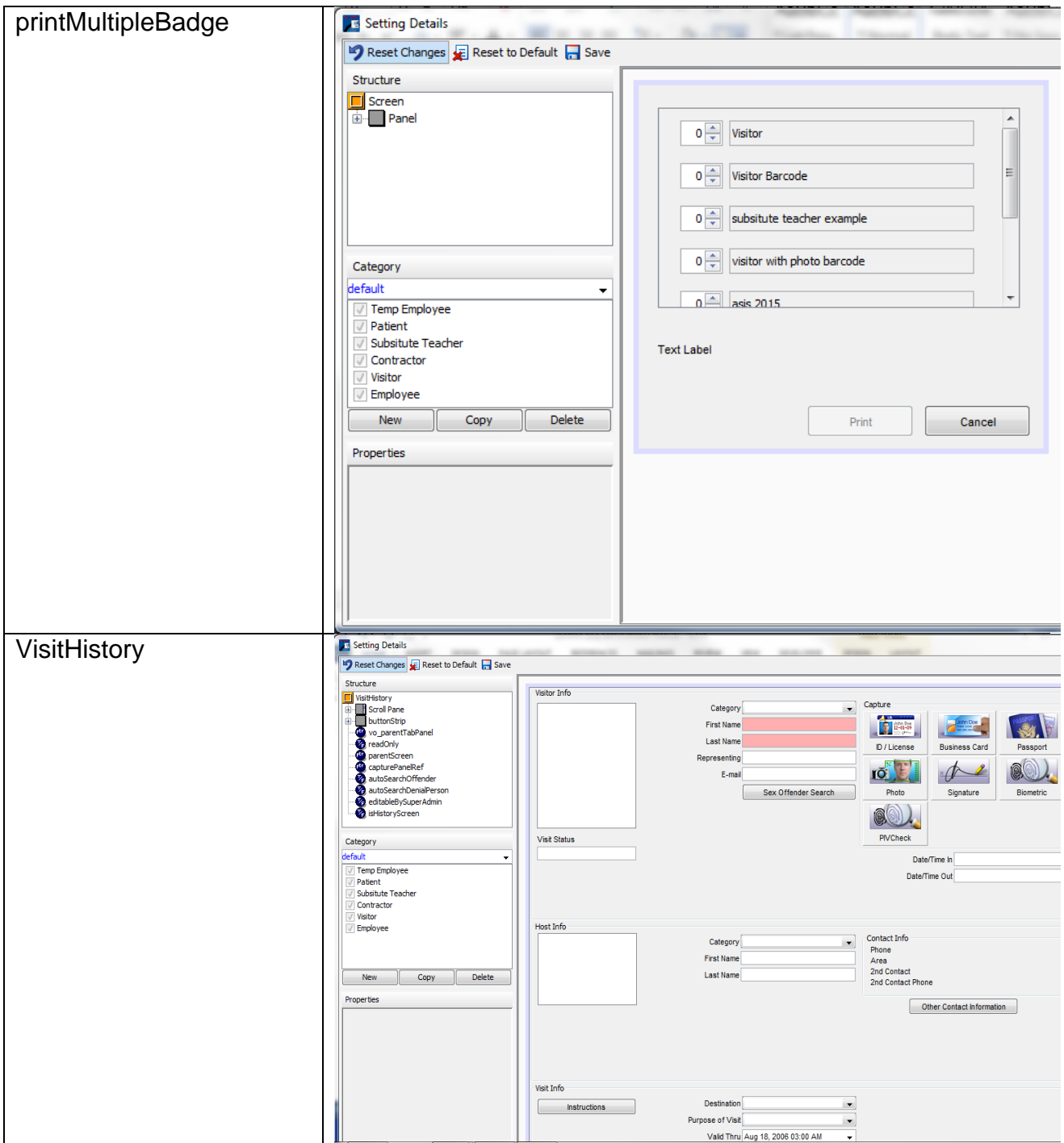
Properties

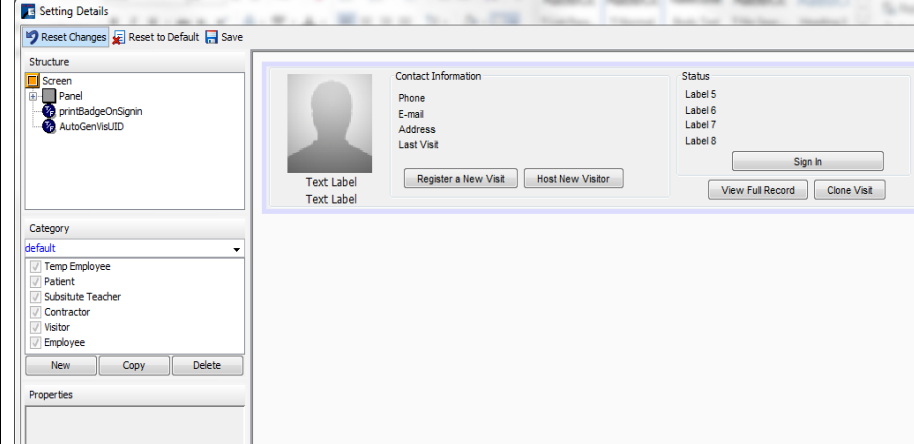
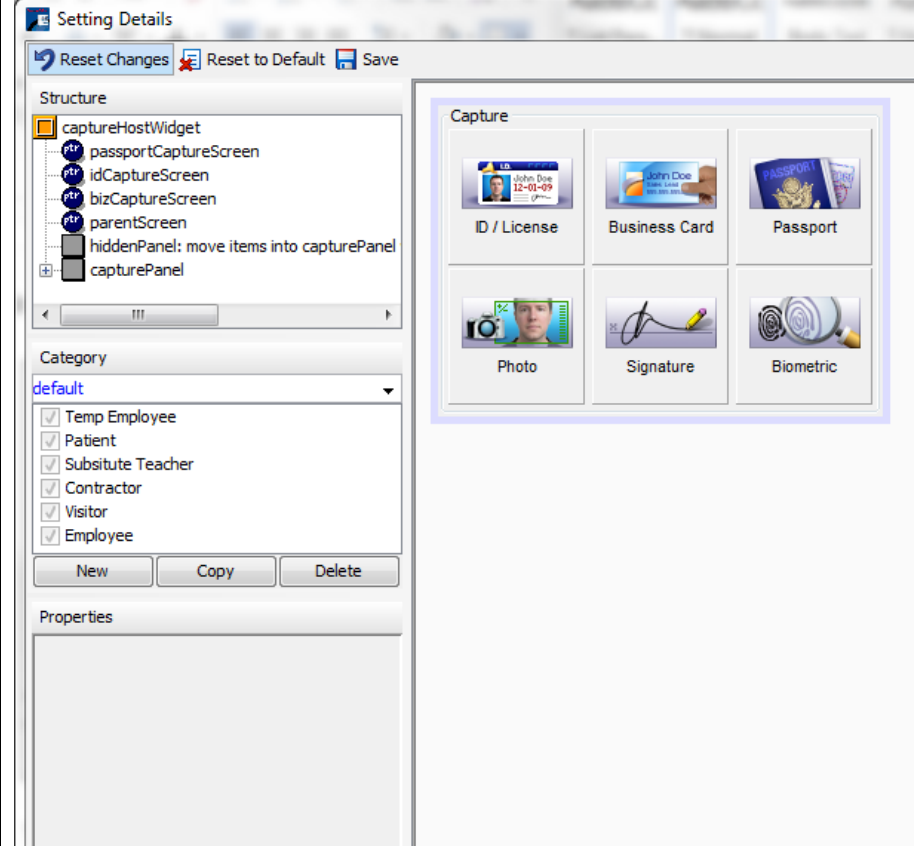
Configure Scanner Region [dropdown]  
Configure Scanner Country [dropdown]  
Name [text]  
Scanner [dropdown] | Date Captured [Jan 06, 2016 10:31 AM]  
ID / License  
[Photo Placeholder] [Sample License: John Doe, 12-01-09]  
First Name [text]  
Last Name [text]  
Address 1 [text]  
Address 2 [text]  
Issuing State [text]  
ID/License Number [text]  
Date of Birth [text]  
Date Issued [text]  
Expiration Date [text]  
<< 1 of 1 >> | Delete | Save

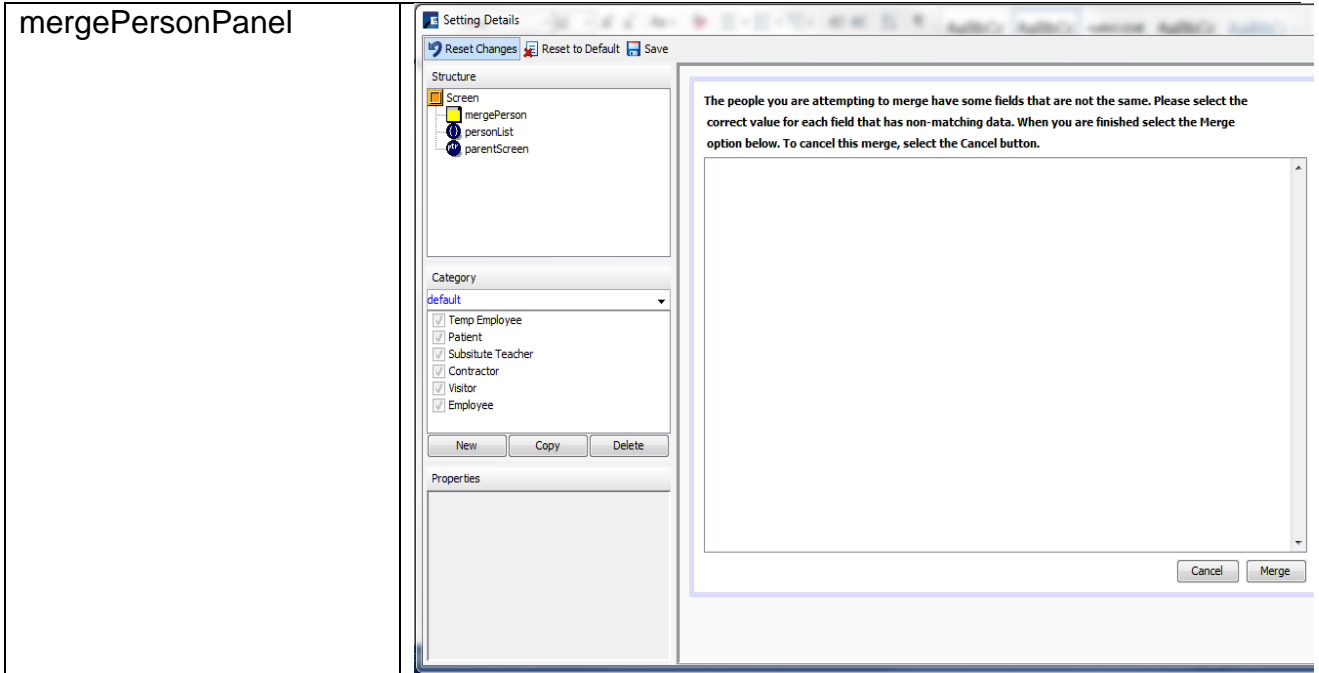
<p>access</p>	
<p>EvacReport</p>	



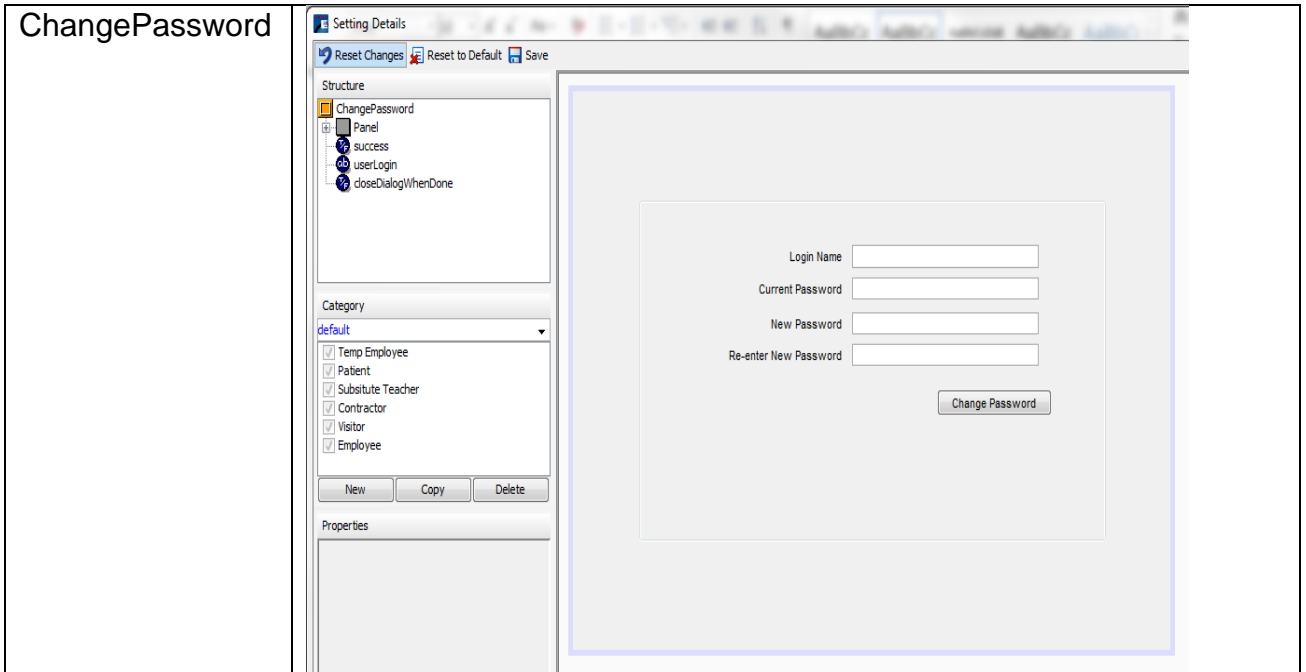
<p>captureBizCard</p>	
<p>PreRegistration</p>	



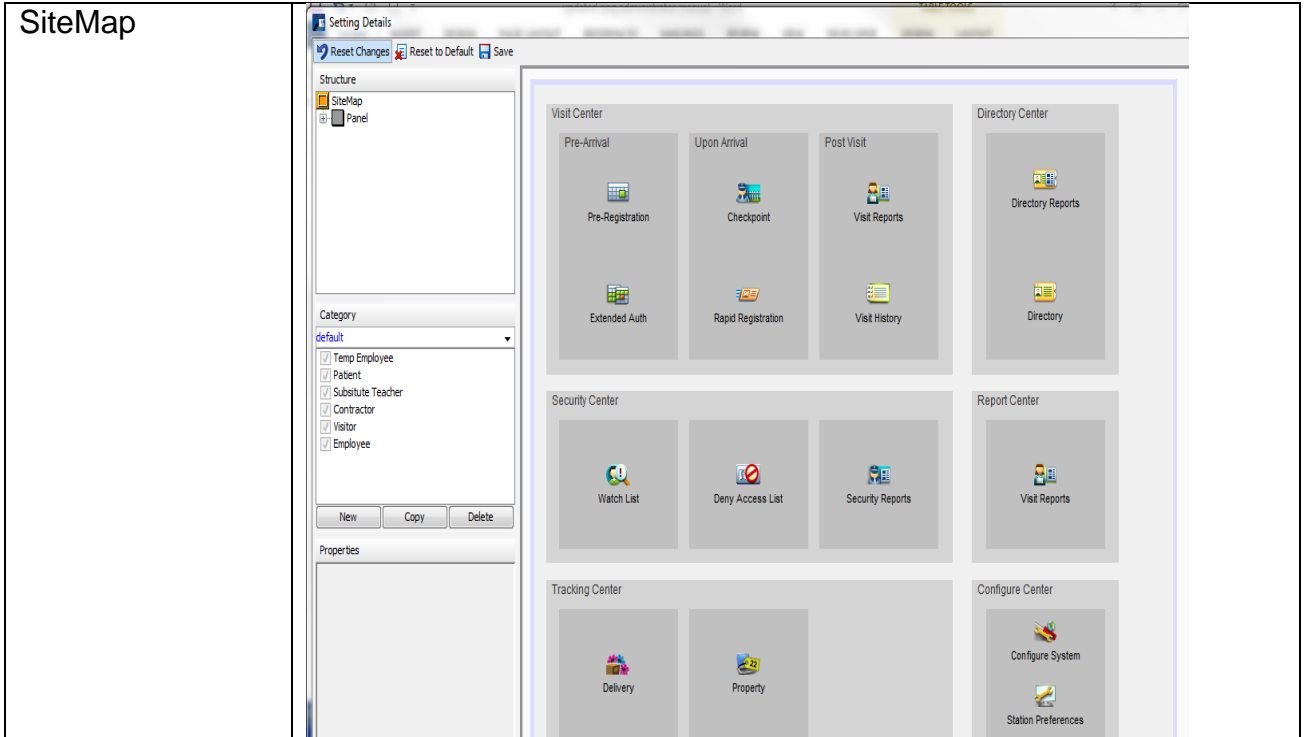
<p>RapidRegSearchOptions</p>	
<p>captureHost</p>	



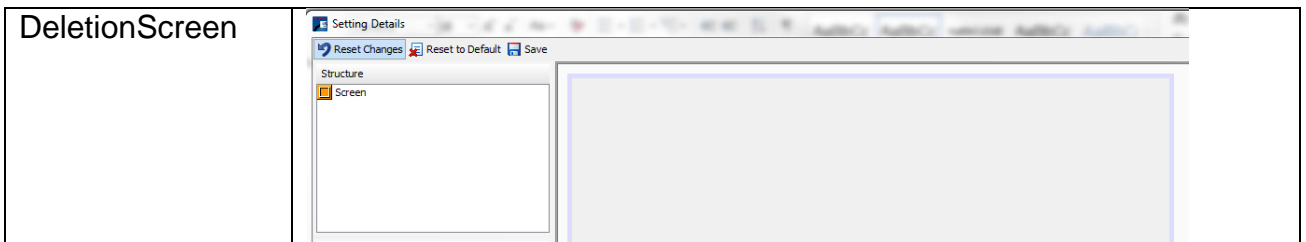
Home screens:





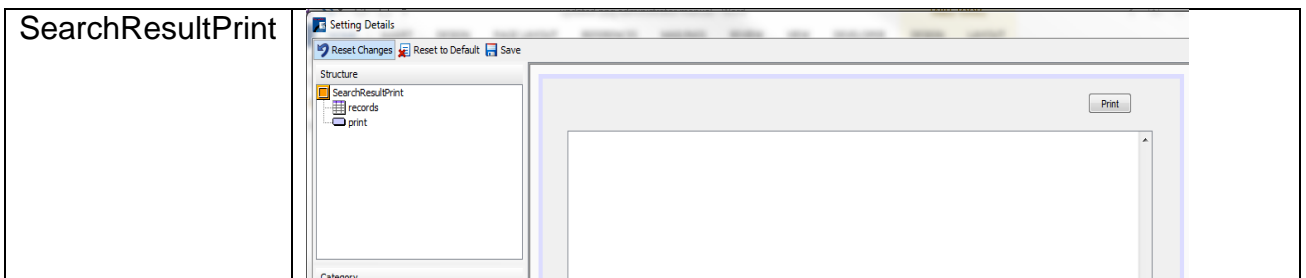


Deletion Policy screens:



Report Center screens: There are no Report Center screens.

Print Search Result1 screens:



Tracking Center screens:

**Property - Default**

**Delivery - Default**

## OPTIONS

The Options are located under the Structure section on the Setting Details for the screen. The Options differ by screen. The following are the Options for the most used screens: Rapid Registration, Pre-Registration, and Extended Authorization (Pre-Authorization).

Options key:

 = true or false. True turns the feature on; False turns the feature off.

 = a number value is required.

Options definitions:

AlertNoPhoto - when set to true the program shows an alert when there isn't a photo for the visitor.

AutoGenVisUID – when set to true the program auto-generates a permanent unique id for the Visitor. The unique ID must be greater than 15 characters to be able to scan it with a barcode scanner.

MaxHintRecords – when a value is entered, the number of matching names listed in the Intellihint pop up is limited to the value.

PrintBadgeByDefault – when set to true the program automatically prints a badge on visitor sign-in.

executeAC\_EventIfNoCardIssued - when set to true, even if access card number is blank, the program will still send the information to the access control system. The Access Control Integration is required.

autoSearchOffender – when set to true the program will automatically search for a sex offender after entering a name. A subscription to Sex Offender screening service is required.

autoSearchDeniaPerson - when set to true the program will automatically search for a denied person after entering a name. A subscription to Denied Party screening service is required.

emailSexOffender – when set to true the program automatically sends an email when there is a match for Sex Offender. NOTE: email templates must be configured. A subscription to Sex Offender screening service is required.

emailDenialPerson - when set to true the program automatically sends an email when there is a match for Denied Person. NOTE: email templates must be configured. A subscription to Denied Party screening service is required.

emailWatchList - when set to true the program automatically sends an email when there is a watch list match. NOTE: email templates must be configured.

requireFirstNameForIntellihint – when set to true Intellihint requires a first name in order to work. When set to false Intellihint works with just a last name.

hostMustBeFromDirectory – when set to true a host is always required and the host must be in the directory.

numVisitorsPermitted – when a value is entered, the number of visitors for the host is limited to the value.

useDirectoryLinkInVisitorHint – when set to true and using a category set in Directory Link, the program will look for a match in LDAP. Directory Link license is required.

noPhotoCropperScreen - if set to true, the screen that allows the operator to crop the photo doesn't appear.

disableIntellihint - when set to true, Intellihint is not enabled.

clearUnkHostUniqueId – when set to true the program searches for a match for the host and populates fields with the match. When set to false, the program allows you to assign a unique ID for the host.

### Rapid Registration

- alertNoPhoto
- AutoGenVisUID
- maxHintRecords
- Scroll Pane
- buttonPanel
- printBadgeByDefault
- executeAC\_EvenIfNoCardIssued
- autoSearchOffender
- autoSearchDenialPerson
- emailSexOffender
- emailDenialPerson
- emailWatchlist
- requireFirstNameForIntellihints
- hostMustBeFromDirectory
- numVisitorsPermitted
- useDirectoryLinkInVisitorHint
- noPhotoCropperScreen
- disableIntellihint
- clearUnkHostUniqueId

## Extended Authorization

- printBadgeByDefault
- maxHintRecords
- autoSearchOffender
- autoSearchDenialPerson
- emailSexOffender
- emailDenialPerson
- emailWatchlist
- requireFirstNameForIntellihints
- hostMustBeFromDirectory
- useDirectoryLinkInVisitorHint
- disableIntellihint
- clearUnkHostUniqueId

## Pre-Registration

- maxHintRecords
- printBadgeByDefault
- autoSearchOffender
- autoSearchDenialPerson
- emailWatchlist
- emailSexOffender
- emailDenialPerson
- requireFirstNameForIntellihints
- hostMustBeFromDirectory
- useDirectoryLinkInVisitorHint
- disableIntellihint
- clearUnkHostUniqueId

## Checkpoint

- printBadgeByDefault
- autoSearchOffender
- autoSearchDenialPerson
- requireFirstNameForIntellihints
- hostMustBeFromDirectory
- numVisitorsPermitted
- disableIntellihint
- clearUnkHostUniqueId
- useDirectoryLinkInVisitorHint

## FIELDS

Fields are located under the Structure section on the Setting Details for the screen, under Panels - . There are two parts to a field: the Label and the actual field. Here is an example of what the email field looks like in the Structure section:

