PassagePoint Global v10

Administrator's Manual

Disclaimer

STOPware, inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. STOPware, inc. reserves the right to revise this publication and to make changes to its contents, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, STOPware, inc. reserves the right to make changes to any part of the PassagePoint product, at any time, without any notification to any person or entity of such changes.

STOPware, inc.
1710 Zanker Road, Suite 100
San Jose, CA 95112

PassagePoint Global v10 Administrator's Manual
August 2008

Table of Contents

Chapter 1 – Introduction

About User Administration

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

PassagePoint Global expands on the business logic in PassagePoint 4.5 and uses a newly developed platform. Screens have been redesigned for ease of use, borrowing from the latest Internet browser look.

This manual includes chapters that review administrator configuration options. The User Administration chapter covers logging into PassagePoint, setting up user accounts, granting users access to screens, and managing passwords. The System Lists chapter describes configuring People Categories, Lists, Agreements and Import Mappings. In the Badge Designer chapter, creating badge templates and specifying stock sizes is described.

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. In the Global edition, PassagePoint has been tailored for the corporate, government and other large environments.

How the Software Can be Used

- For signing in and badging walk-up visitors
- To pre-register individuals and groups
- For checking visitor names against national sex offender and criminal lists
- As a people tracking tool
- To notify visitors and hosts of pre-registrations and arrivals
- For viewing and printing visit reports
- To grant card access within Access Control Systems

Hardware Support

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 LabelWriter 400 Turbo* (www.dymo.com).

Business Card, ID/License & Passport Scanners

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

Photo Capture Devices

PassagePoint can capture photos using a TWAIN or WIA driver for an USB 2.0 camera. Various 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. Signature can be captured from a SignatureGem 1x5 model and shown simultaneously on the PassagePoint Client agreement window. Topaz's 4x5 LCD model has the added ability of displaying the agreements text on the LCD 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 used to retrieve a person's previously saved data to create a new visit. 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 on the installation CD.

CONFIGURE SYSTEM

The Configure System option under the Home tab allows administrators to define system settings. Settings have been grouped into 'Badge Designer', 'Communication Settings', 'External Systems', 'Policy Manager', 'System Lists', 'User Administration' and 'Web Module'. 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 deactivated to maintain historical information relating to that setting.

HARDWARE AND OPERATING SYSTEM REQUIREMENTS

System Requirements

For details on system requirements, see the "Getting Started Guide".

Chapter 2 – User Administration

The User Administration chapter covers the login process and user account administration, including authentication rules, user roles and changing user passwords. Security of the PassagePoint system begins with creating secure user accounts that are tied to User Roles and Authentication Rules. For advanced security, consider implementing Allocation tree to control data access.

Login

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

Figure 1 - 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 highly 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 *User Accounts*.

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

User Accounts

User Accounts allows administrators to define PassagePoint login accounts and grant rights based on a user role. You can link a User Account to a person who appears in the Directory. For account security, each User Account should be assigned a User Role, which incorporates User Authentication Rules

settings. By assigning a User Role, you are limiting access to screens that each user will be able to access. Within a role, you assign User Authentication Rules to enforce password rules and login restrictions. Below are descriptions of some of the fields on the User Accounts configuration screen:

User Name – This is a free form text field to name the account.

Login Name – When logging into PassagePoint, this is the name that the user enters.

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.

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 pick the person who owns this account.

User Role – 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. User Roles may be defined with the User Roles configuration option. Defined roles will appear in the pick list.

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

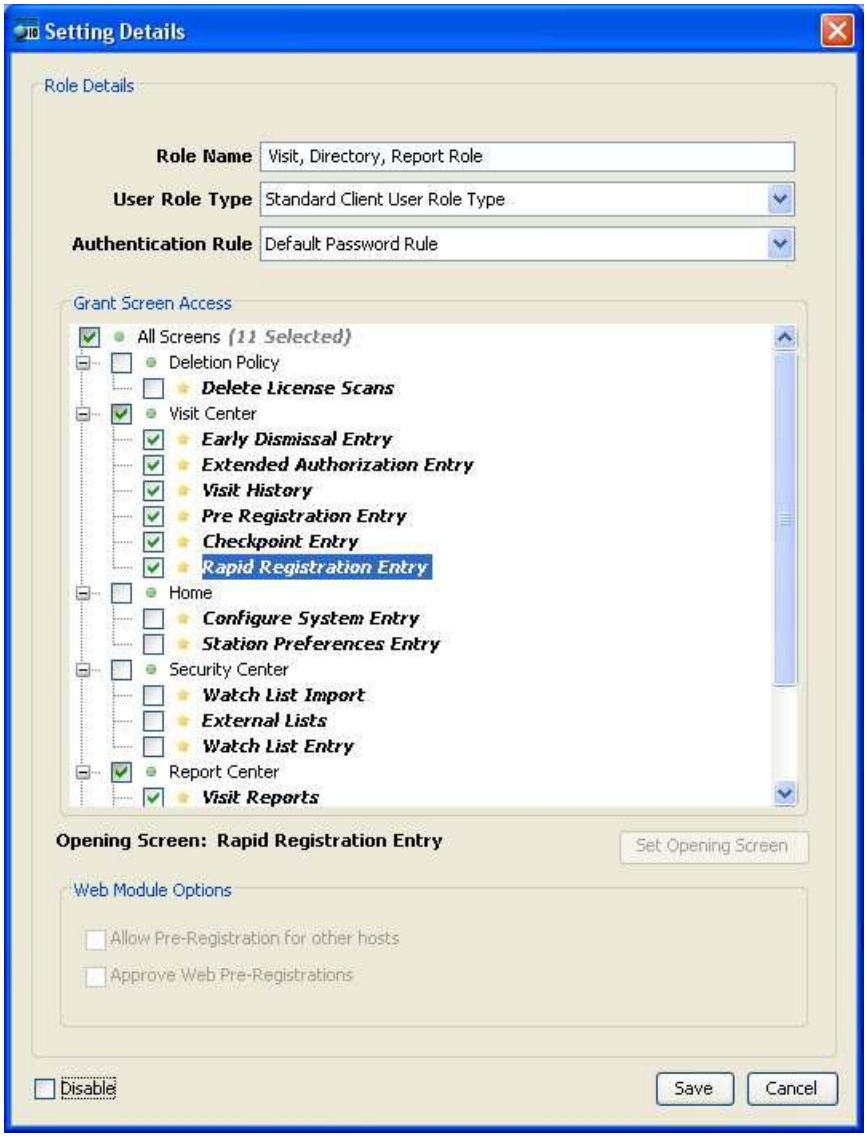
Disable – Accounts can only be disabled, not deleted. This maintains the integrity of past transactions. If a user account becomes disabled by the system because of an authorization rule, it can be reactivated here by un-checking the Disable box.

User Roles

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

To configure roles, click either "Add" to create a new account or "Edit" to modify an existing role. From within the Setting Details screen, you will specify a name for the role. This is a descriptive name of the user role being configured. We suggest that you use names that reflect 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 categorization to the name, such as a location – 'Receptionists in Building 5'.

Figure 2 - User Roles



Authentication Rule – Specify the authentication rule to use with a User Role by choosing a rule from the pick list. Rules listed are those configured from within the *User Authentication Rules* option under User Administration settings for Configure System.

Grant 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 and editing.

Set Opening Screen – You can specify the screen that will displayed 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.

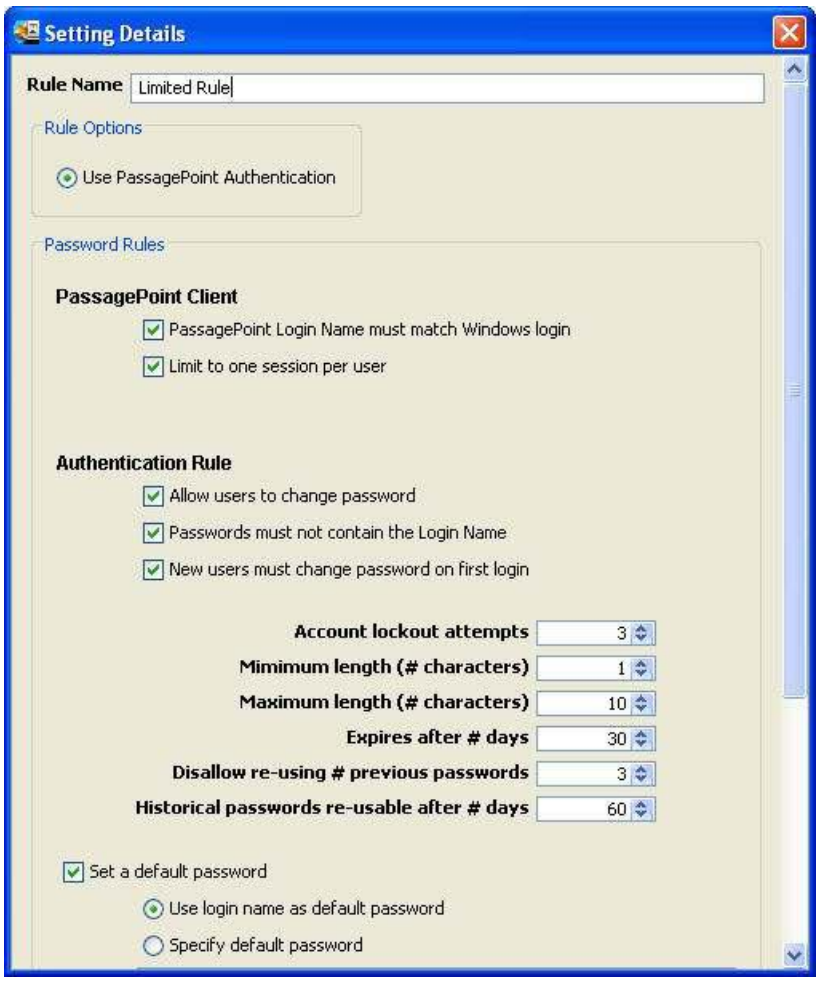
Web Module Options – When a Web User Role Type is configured, you can configure a role setting for users who will pre-register visitors using the PassagePoint Web Pre-Registration Module. You can specify if users can pre-register visits for hosts other than themselves. Additionally, users may be granted the ability to approve web pre-registrations in advance of a visit.

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.

User Authentication Rules

User Authentication Rules allows administrators to specify login and password parameters for PassagePoint Clients. Authentication Rules are applied by assigning them to User Roles. Click "Add" in the Configured User Authentication Rules panel to add a new User Authentication Rule. To edit a configured rule, select the rule and click "Edit".

Figure 3 - User Authentication Rule



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 for Authentication – Selecting this option bypasses PassagePoint Authentication and uses LDAP for login authentication. To use LDAP authentication, you will also need to configure LDAP support on the PassagePoint Server.

Comment [EC1]: need info here about LDAP config

Use Third-Party Web Password System – This option is only applicable to authentication with PassagePoint Web Pre-Registration system. It bypasses any password authentication and trusts the user information being sent to the Web client. To use this option, you will need to configure Microsoft IIS single sign-on options and PassagePoint Directory Link.

PassagePoint Password Rules

PassagePoint Client

PassagePoint login must match Windows login – Checking this option will enforce a rule that the login name specified for PassagePoint is the same as the Windows machine login name.

Limit to 1 session per Login Name – Enabling this option will enforce unique logins for clients logging into PassagePoint server. If a second client attempts to use a login name that is currently logged in, they will get an error message and not be allowed to login. Logging in with the user Admin is excluded.

Web Pre-Registration Module Logins

Allow Internet users to choose login & password – If this option is checked, you are allowing users who login over the internet to specify their own unique login name and password. This option is only available with the Web Pre-Registration module.

Password Rules

Allow user to change passwords – This option allows users to access the "Change Password" screen under the Home tab. From within Change Password, they will be able to assign a new password to a user account with a valid login name and current password.

Passwords must not contain login name – Enabling this password rule forces a password that contain a user's login name to be rejected. The user will be asked to enter a new password.

New user must change password – This option will require that a user change their password upon the first successful login to PassagePoint. A password dialog will appear on login asking them for a new password.

Account lockout attempts – If this rule is checked, an account will be locked after a specified number of unsuccessful attempts to log into PassagePoint. The account will need to be reactivated by an administrator from the User Accounts.

Minimum / Maximum length of password – Specify the minimum or maximum number of characters that a password may be set to. Setting this to "0" means do not check for password length.

Expires after # days – Enabling this rule forces passwords to automatically expire after a specified number of days. Upon expiring , users will be asked to enter a new password on their next successful login.

Disallow re-using last # previous passwords – This option will disallow a user to set their password to previous passwords. The number specified is the number of passwords that the system remembers and checks against.

Historical password re-usable after # days – Setting a number of days here will determine when a password may be reused. Number of days is counted from the day that the password was changed.

Set a default password – To set default passwords for new user accounts, check the "Set a default password" box to display the default password options. For security, it is important that this option be used with the "New users must change password" option. Click on one of the radio buttons to make a selection between the two options:

> **Use login name as default password** – Choosing this option will set the password to be the same as the login name.
>
> **Specify default password** – Choosing this option will allow a user to enter a default password that is used by all new users

Regular Expression Password Filter

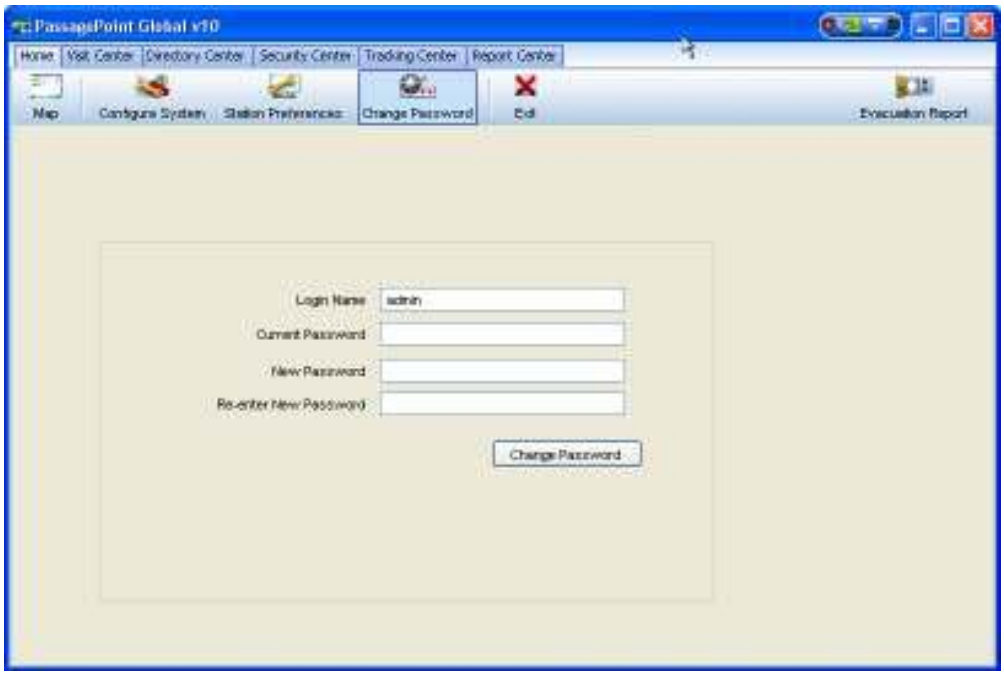
You may use regular expression (also known as RegEx or RegExp) to specify a text pattern that is not acceptable as a password. When a user account password is being set, it will be checked against the RegEx filters for a pattern match. If the new password matches a RegEx filter, the password will be rejected and the user will be required to enter a new password.

CHANGING PASSWORDS

User passwords can be changed from the *Change Password* ribbon button under the Home tab. If a user is granted access to this screen, they can change a user password by entering the Login Name and current and new passwords. If the Login Name and current password matches a user account, the account will be updated with the new password.

In the event that a password needs to be reset, it can be changed without knowing the current password from within the *User Account* option.

Figure 4 - Change Password



Chapter 3 – Communication Settings

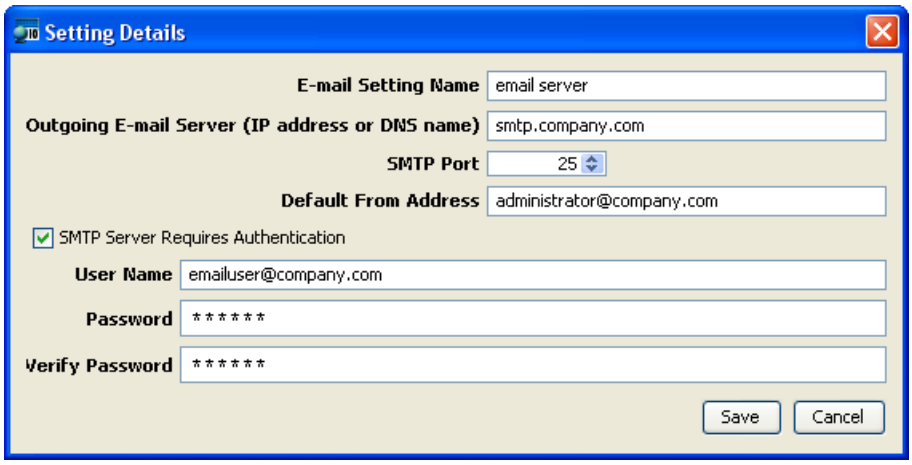
In this Communication Settings chapter, information about how to configure E-mail Templates and E-mail Server Setup is provided. These lists screens are accessible under *Home | Configure System | Communication Settings*.

Communication Settings contains configuration screens for sending notifications and visit information via E-mail. Additional communication channels such as Instant Messaging will be supported in future releases.

E-MAIL SERVER SETUP

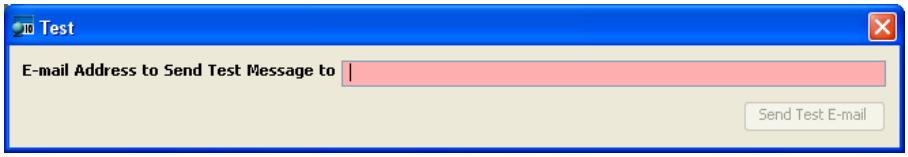
Setting up the E-mail server configuration entails specifying the SMTP server and port. By default, the SMTP port number is 25. A default From: address can be entered for sending E-mails. If SMTP server authentication is required, check the Requires Authentication box and specify the user name and password for logging into your SMTP server. Your E-mail administrator should be consulted for the proper settings on any of these settings.

Figure 5 - E-mail Server Settings



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

Figure 6 - Send test E-Mail

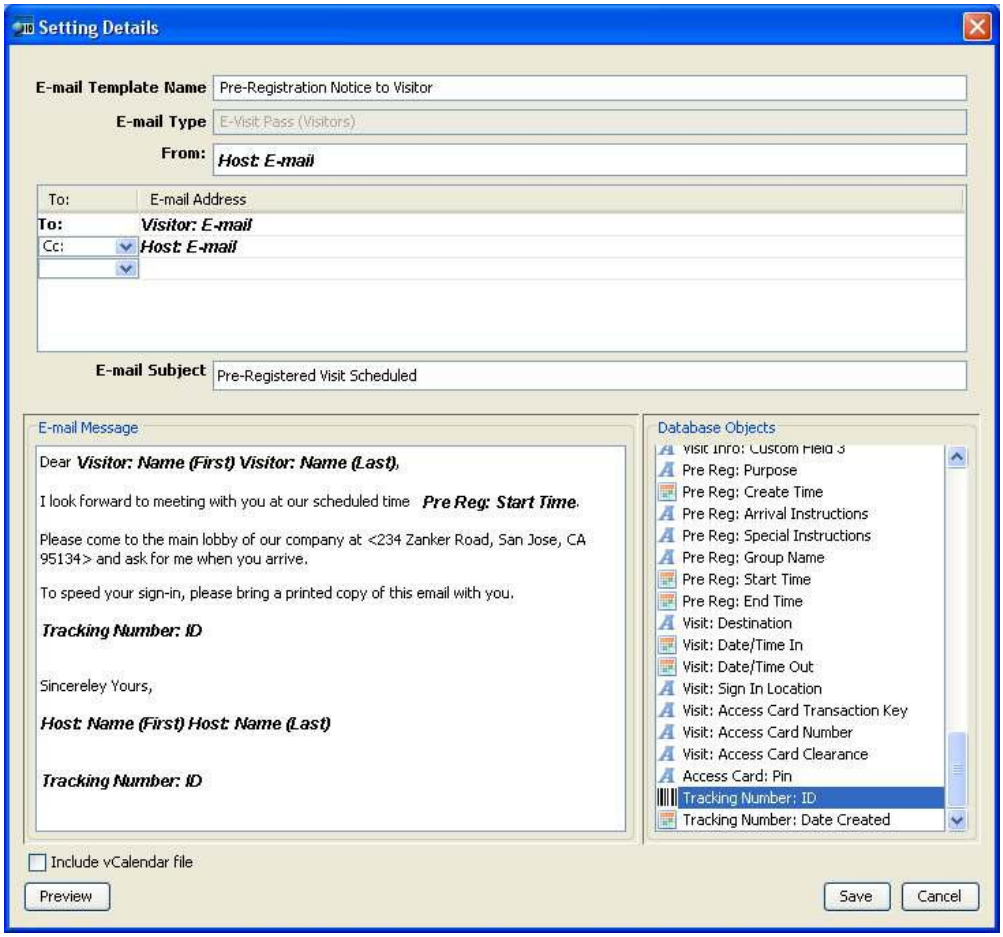


E-MAIL TEMPLATES

PassagePoint uses E-mail Templates when sending E-mail notifications. Several template types have been pre-defined.

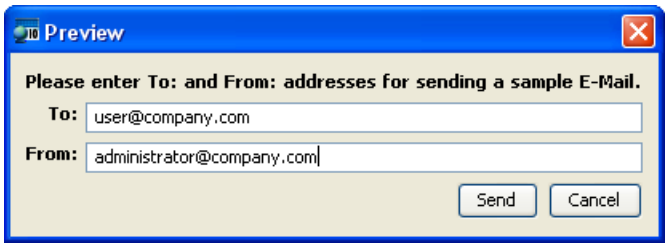
To modify a template, add a new template by selecting a template type and clicking Add. Existing templates can be edited by selecting the template and clicking the Edit button. Within the Setting Details screen that opens, elements stored within the database can be drag and dropped from the Database Objects listing onto the template fields and message body. Database Objects will appear on templates as bold-italicized text. The From: and To: fields are required and can be set to a E-mail database object or a hardcoded address may be entered.

Figure 7 - E-mail Template



To test the layout of the E-mail, you can send a test E-mail message by clicking the "Preview" button. A message will be sent to the people that you specify in the To: field on the Preview dialog box. Both the To: and From: fields are required.

Figure 8 - Send E-mail template test



Chapter 4 – System Lists

In the System Lists chapter, information about how to configure Agreements, Destination Places, Lists and People Categories is provided. These lists screens are accessible under *Home | Configure System | System Lists*.

System Lists are administrator configurable items that typically appear as dropdown lists on Entry screens. The System Lists configuration screens allow you to define the list items, sort items, set a default item, and in some cases, customize their usage.

AGREEMENTS

Agreements in the System Lists configuration screen allows you to enter legal and contract documents that visitors will need to agree to as part of their sign-in. Agreements are applied by associating them to appropriate People Categories. Visitors will see those agreements that have been assigned to their category when they sign-in at a PassagePoint Visitor Sign-in Station.

Before you begin to configure the NDA features, you should consider the different ways to setup this feature. Agreements may be presented to visitors through the PassagePoint Sign-in Station or manually by a receptionist.

Using a Visitor Sign-in Station

If you are using a Visitor Sign-in Station, then the agreement text will be displayed to the visitor on the screen after the visitor enters the required information.

The text can vary depending on which category (Volunteer, Visitor, etc.) they select. Once the NDA is displayed, you can require that the visitor simply clicks the "Accept" button or you can require that they sign a digital signature pad and then click Accept. The captured signature is stored electronically in the visitor's record within PassagePoint and can be printed as an agreement document.

You can also either require that the agreement be accepted to complete the entry or allow the visitor to decline the agreement and still complete the sign-in.

Reception Administration of Agreements

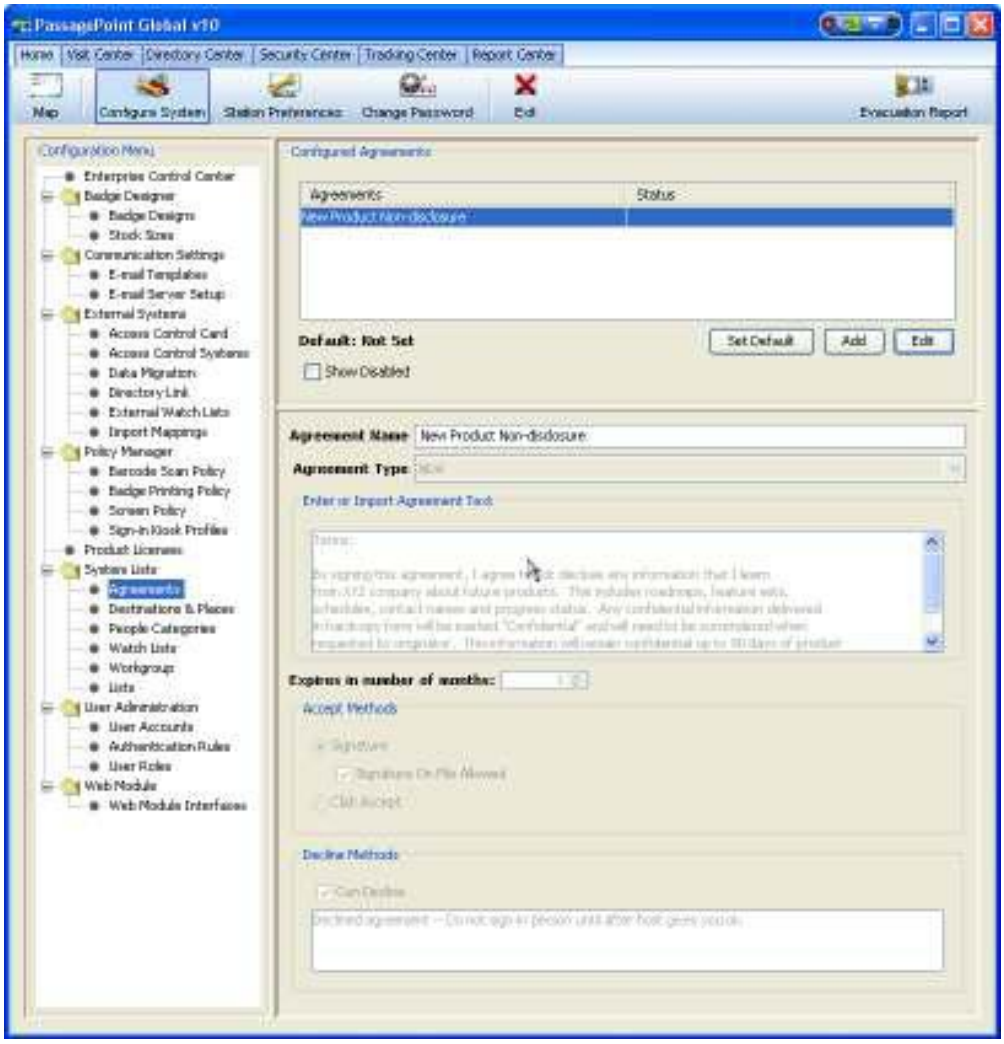
If a receptionist administers agreements manually, the visitor's name and contact information are entered on a Visit Entry screen. Then the receptionist clicks the "Capture" button which activates the signature capture pad. The visitor should be shown and allowed to read the agreement text in hardcopy form. The receptionist can view the signature on screen before completing the entry.

Configuring Agreements

To configure Agreements, click "Add" or "Edit" on the Configured Agreements screen under *Home | Configure System | System Lists | Agreements*. In the Setting Details screen that opens, you can specify

a name for this agreement, the type of agreement, the text for this agreement, and accept and decline methods.

Figure 9 - Agreement Configuration Screen



Enter or Import Agreement Text

In the text box, you can type in the text for the agreement. You can also paste in text from the clipboard by placing your cursor in the box and hitting Ctrl-V.

Alternatively, you can import the agreement text by clicking the "Import" button. In the Open window, navigate to and select the text file for the agreement. Import only plain text files since formatting code will not be interpreted.

Accept Methods

Choose whether to accept agreements with a signature or with an accept button.

Acceptance Methods supports capturing a signature electronically with a signature pad such as those from Topaz Systems. Once captured, the signature will be stored electronically in PassagePoint and may be viewed and printed with agreements as legal documents. If an agreement covers a period of time, say twelve months, you can set PassagePoint to recapture a new signature from that visitor after the twelve month period.

Comment [EC2]: where do we configure signature durations?

If signature capture device is not used, you may store signatures on paper and indicate that a signature is on file with the "Signature On File Allowed" option. The receptionist will be able to designate that the agreement was accepted by checking "Signature On File" in the Visit Entry screen.

Alternatively, agreements may be accepted with clicking an "Accept" button that appears on the agreement screen.

Decline Methods

If an agreement can be declined, visitors can click a "Decline" button. You can allow visitors to decline the agreements and still complete the sign-in process. If the Visitor Sign-in Station is used without a receptionist verifying the entry, it is recommended to require acceptance of the agreement, i.e. do not enable "Can Decline".

Destination Places

Places that a visitor can go to are configured under the Destination Places. The configuration screen can be found under *Home | Configure System | System Lists | Destination Places*.

Configured Destination Places will appear in Entry screens as a dropdown list. The first item on the list will be selected as the default destination.

To Add / Edit a Destination

Destination Places can be added or deleted from the Configured Destination screen. Click the "Add" button to add a new destination. To edit an item, select it and click "Edit". In the Setting Detail screen, enter the name of the location and any comments or address for the location.

Destinations cannot be deleted since historical information may require it for data consistency. Instead, you are allowed to disable destination items. Select the destination and click "Edit" to open it. In Destination Setting Details, check the "Disabled" box to make this destination no longer appear in Destination dropdown lists.

Sorting the Destination Places List

The list of Destination Places may be sorted manually or alphabetically. To manually sort the list, select a Destination and click the "Up" or "Down" buttons to reposition its location in the list. The entire list can be resorted alphabetically in ascending order by clicking the "Alphabetize" button.

LISTS

PassagePoint uses lists to provide easy-to-use menus. These lists can be modified to include your own custom menu options. Lists are maintained from within *Home* | *Configure System* | *System Lists* | *Lists*:

- Classifications –immigration and visa classifications, such as US Green Card and H1B Visa (multiple lists)
- Citizenships – countries of citizenship (multiple lists)
- Arrival Instructions – steps to follow at sign-in (multiple lists)
- Purpose of Visit – reasons for visiting location (multiple lists)
- Threat Levels – indicates the general risk levels and is displayed in Secure View
- Security Levels – security interaction information, such as escort required (single list)
- Agreement Types – classifications of legal agreements (single list)

Some List Types support multiple lists. The reason for multiple sub-lists is to allow administrators to create custom lists which can be assigned to locations in the Allocation Tree (a Enterprise Edition feature).

To modify a list, select the list or sub-list from Configured Lists screen and click "Add", "Edit" or "Delete". 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 Add / Edit Lists Items

From within the Lists Setting Details screen, you can name each list, add / edit / delete items, set item visibility, sort items, and set an item as default. Having a Show box checked indicates that this item will appear in the dropdown list on Entry screens. Setting an item as default makes it the automatically selected item in the dropdown list on Entry screens.

To Sort a List

The order of the list can be set manually by using the "Up" and "Down" buttons on the Lists Setting Details screen. Select the item that you would like to move and click either buttons to reorder the list.

You can automatically sort the list in alphabetical ascending order by clicking the "Alphabetize" button.

PEOPLE CATEGORIES

PassagePoint uses Categories to help organize individuals within the system and for setting preferences. People Categories are used for both your in-house staff, as well as your visitors. Each category may have its own name and its own preferences. For example, you may want to set the Staff category to have a temporary badge for a full 8 hour duration, while visitors may only have 4 hours.

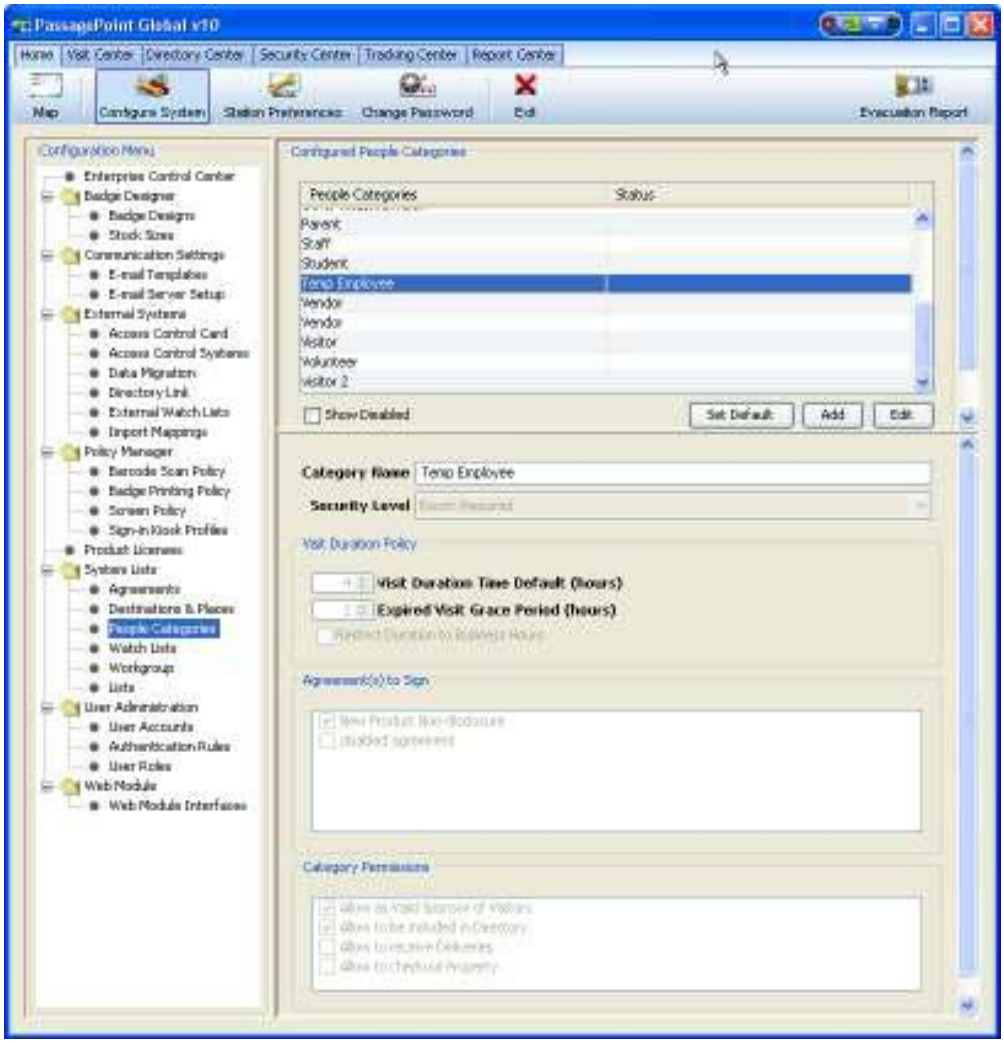
PassagePoint Global is preconfigured with the People Categories. Categories can be modified or deleted, and additional categories may be added.

Table 1 - People Categories

EDU Edition	Global v10 Edition
Faculty	Visitor
Parent	Employee
Staff	Temp Employee
Student	Contractor
Visitor	
Volunteer	

To add or edit People Categories, open the People Categories configuration screen under *Home | Configure System |System Lists | People Categories*. Within this screen, you can click "Add" to enter new categories or select a category and click "Edit" to change parameters.

Figure 10 - People Categories



From within the People Category settings screen, specify the default duration for a visit. These are times for determining the length of a visit. Additionally, you can assign contractual agreements that each category of people need to agree to before they are allowed to complete sign-in. Categories can be designated as a host and or to be included in directory.

Security Level

This sets the default security level for this category. The list of security levels which appear have been configured on the Security Levels screen under *Home | Configure System | System Lists | Lists*. Examples of Security Level setting are: Escort Required, No Escort Required, etc.

Visit Duration Policy

This policy allows you to set a default duration time for visits which will help in calculating the expected sign-out time, when a badge expires, and when to automatically sign-out visitors.

Visit Duration Default (hours) – The number of hours specified in this setting is a default length of time for this category of people. Indicate the number of hours that a typical visit usually lasts in hours. For example, you may want to have visitors to have access for only one-half of a day, while your in-house people may need a full day badge.

Expire Visit Grace Period (hours) – Specify the number of hours after the visit end time that the system will wait before automatically signing out a visitor with this category. The PassagePoint system is designed to automatically sign-out visitors after a visit end time. The grace period specifies the number of hours before the auto sign-out process occurs after the specified visit end time found in the visit record.

Agreement(s) to Sign

Contractual and legal agreements may be assigned to People Categories. As visitors arrive to sign-in, they will be presented with the agreements that have been assigned to their category. If a signature pad has been added to PassagePoint, visitors can use the signature pad to sign acceptance of the agreement terms.

Before assigning any agreements, you will need to enter the agreements under *Home | Configure System | System Lists | Agreements*. To associate an agreement with a category, check the box of the agreements that apply.

Here is an example of using agreements with people categories. You have decided to classify parents with a category of Visitor. Within the Visitor category, you have specified that a set of agreements, such as a Code of Conduct and/or a Non-disclosure Agreements, must be signed in advance of entering the location. When a parent arrives to sign in, PassagePoint will show the agreements on the screen of the PassagePoint Visitor Sign-in Station. Using a signature pad, they can sign that they agree to the terms.

Category Permissions

Allow as Valid Sponsor of Visitors – People with this permission have the ability to host visitors. When a visit transaction is being entered, only people with categories that have this setting enabled will appear as hosts.

Allow to be included in Directory – People with this category setting will appear under PassagePoint's Directory Center. Directory people are typically your in-house people, such as staff and teachers. Students may optionally be included in the directory.

Allow to be receive deliveries – This category option indicates that people with this category will be able to receive delivery items.

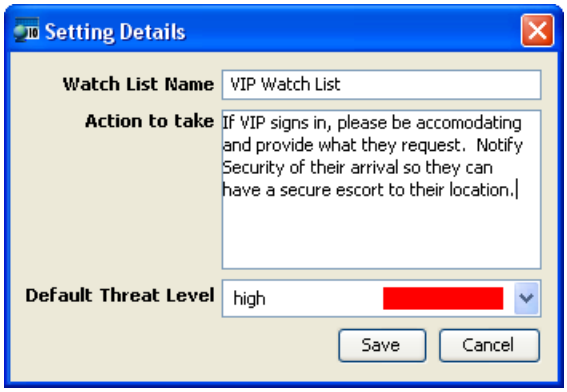
Allow to be checkout property – Checking this option specifies that the people with this category are authorized to check property out from your organization.

Watch Lists

Watch Lists manage people who you want to be on the lookout for. Multiple lists can be created to organize the various people. When PassagePoint is installed, the "Internal" Watch List is automatically created. Internal is the default list used for manually entered Watch List data.

To create additional lists that may be allocated through Control Center, click <Add> below the Configured Watch Lists table. On the Setting Detail screen, specify the name of the Watch List, enter text for the appropriate action to take, and pick a Threat Level from the dropdown list.

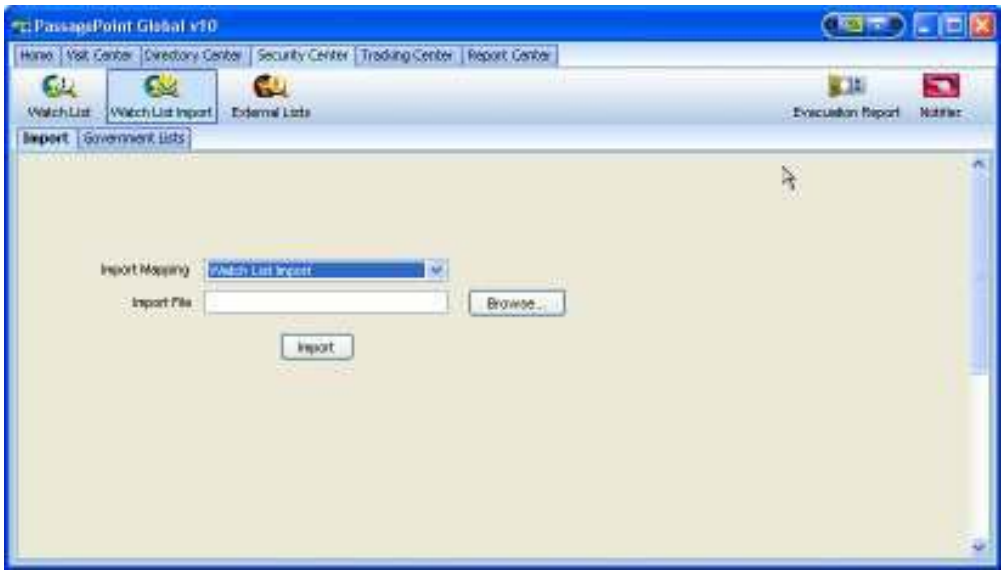
Figure 11 – Creating a Watch List



Importing Watch Lists

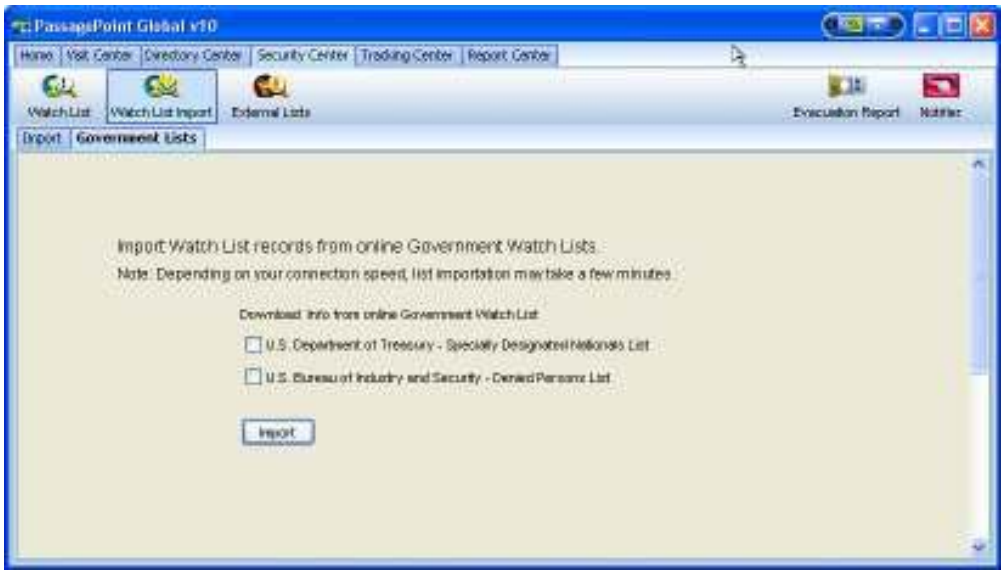
People can be imported into a Watch List by creating an Import Mapping in Configure System and running Watch List Import from the Security Center. From the Watch List import screen, click on "Browse…" to indicate the location of the import file.

Figure 12 – Importing Watch Lists



Watch List Import also includes the option for downloading U.S. Government Watch Lists.

Figure 13 – Importing Government Watch Lists



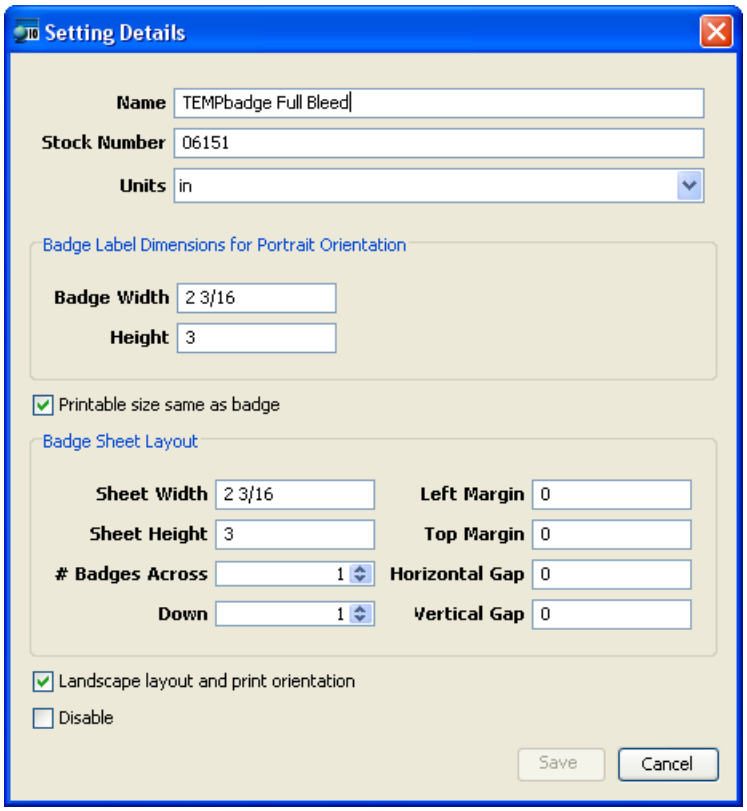
Chapter 5 – Badge Designer

PassagePoint provides 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 printing templates for both badge 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 at least one badge stock size defined. To define stock sizes, choose *Home | Configure System | Badge Designer | Stock Sizes*.

Figure 14 - Badge Stock Sizes



A list of pre-defined stock sizes is list in the Configured Badge Stocks table. Click "Add" or "Edit" to manage stock sizes. In the Setting Details screen, you can enter information about badge size, page

layout of badge sheet, and separate printable size dimensions. To save edits, you must provide a Name for this badge stock configuration.

Units – From the dropdown, pick whether the dimensions for this stock are in inches or centimeters.

 # Badges Across & 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.

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

Left & Top Margin – 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 & Vertical Gap – Gap is the measurement of space between badges on a sheet. Enter "0" for badge rolls.

Stock Print Size: Badge Width & Height – Specify the dimensions for the printable area of a badge. If the print size is the same as the physical label dimensions, then check the "Printable size same as badge" box.

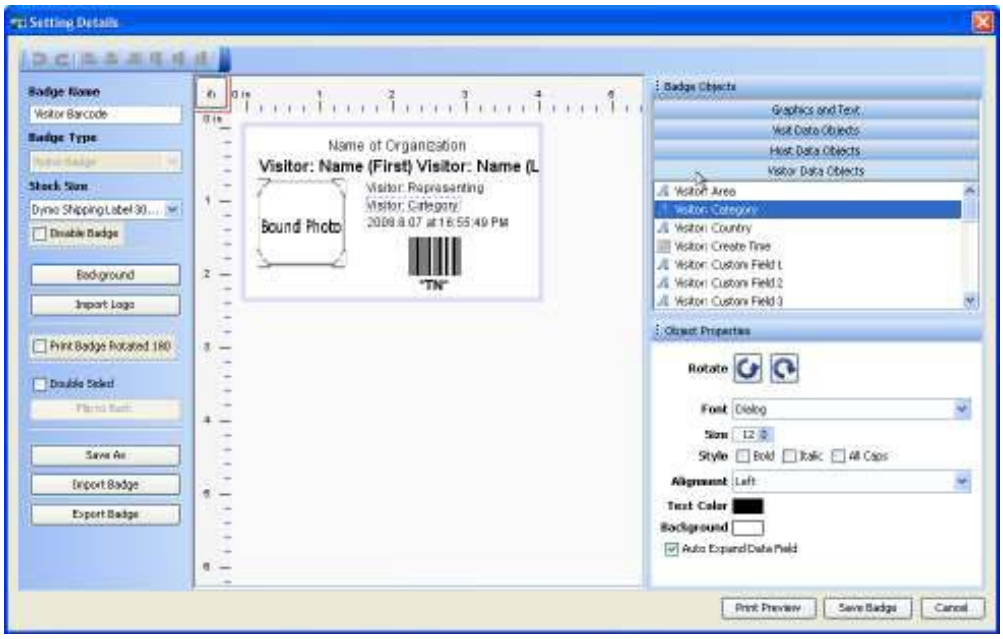
Landscape Layout – Check this box if the badge prints in landscape mode, i.e. where the badge width is greater than height. When landscape is checked, a badge based on this stock will be shown in Badge Design with a wide orientation. If the same stock is used for both portrait and landscape badges, create two stock configurations with the same dimension. Set one with landscape selected and the other without.

Disable – Check the disable box if you do not want this stock size to be listed in Badge Design.

BADGE DESIGNS

Badges for visitors and Labels for deliveries and properties can be customized to your corporate identity using Badge Designer. Before a badge or labels can be printed, a badge template must be created that defines how information and graphics is laid out. Manage badge designs by opening *Home | Configure System | Badge Designer |Badge Designs*. From the list of Configured Badges, you can click on "Add" or "Edit" to design a badge layout template.

Figure 15 - Badge Designer



Badges print based on a customized design template created in Badge Designs. Information that you want printed on a badge is added by simply dragging and dropping objects onto a badge layout canvas and configuring their properties. Similarly, objects on a layout can be removed by selecting it and pressing the <Delete> key. When a visitor is signed in on the Rapid Registration screen, a badge for that visitor can be printed by selecting a badge design from the dropdown list and checking Print Badge.

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

Badge Type – Classify a badge or label by selecting the appropriate badge type from the dropdown list. The selection will determine what data can be placed on the design.

Badge Name – To be able to save a badge design, a Badge Name must be entered. This is a general name to identify this badge and will be used on PassagePoint Entry screens that allow for printing badges and labels.

Stock Size – When creating a badge, choose a stock size from the dropdown list. This list is populated from the Stock Sizes configuration screen. The orientation of the badge is dependent on whether or not "Landscape Layout" was checked for this stock size.

Disable Badge – Badges which are disabled will not appear in the badge dropdown list on the Rapid Registration screen. Check the Disable Badge box to inactivate this badge design.

Background – Click the "Background" button to specify a background style for this badge. The color or image that you select will remain in the very back of the badge layout as objects are placed on top of it.

If you choose to use an image, the image can be placed on the badge centered (one image centered) or tiled (image repeated to fill badge layout). Click "Browse…" to select a file to import an image file as a background. Supported image files types are: .bmp, .jpg, .gif, .png and .tif

Import Logo – Images can be placed on the layout by clicking the "Import Logo" button. Any text or barcodes that are placed on the badge layout will appear over the logo image. The difference between background and logo images is logo cannot be tiled and is one level above background.

Select "Import Logo" to specify the logo file to insert. The supported image file formats are: .bmp, .jpg, .gif, .png and .tif

Double Sided & Flip to Back – To design badges to have front and back sides, check the Double Sided box. When printing, two consecutive badge labels will print with one for front and the second for back. Click on the "Flip to Back" button to lay out the backside of the badge.

Import & Export Badge – Badges can be saved externally and imported into PassagePoint. Use the "Export Badge" to initiate saving the current badge to an external file. To initiate an import of a badge design, click "Import Badges". 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. We recommend that you name your files with a .badge extension.

Toolbar

Your last action can be undone with the Undo arrow icon on the toolbar. To redo the last undo, click on the Redo arrow icon.

Additionally, objects placed on a badge can be aligned with the six toolbar buttons for aligning left, center, right, top, middle and bottom. Select the various objects you want aligned on the badge canvas, and click on one of the six alignment buttons.

Figure 16 - Badge Designer Toolbar

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.

Database Objects

The list of data objects represent data items from the PassagePoint database. For visitor badges, objects are categorized as host, visitor, visit and pre-registered. Similar categorizations will be shown as you select different Badge Types.

Properties for each badge object can be changed within the Object Property panel. Select an object on the badge canvas to modify its settings in Object Properties.

Objects that appear on the badge canvas 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.

Graphics and Text

These are static and graphical objects which can be placed on a badge. Again, to add the object to your badge design, select the object and drag it onto the badge layout canvas. Delete objects on canvas with the <Delete> key.

Text Area: Drag this object onto the badge layout canvas to specify a fix line of text. Text that appears on the printed badge is modified within its "Text" Object Properties.

Linear Barcode: A Linear Barcode can configured to represent one of the following information: Access Card, Visit Number, Directory Number or a static value. The barcode value can be also be displayed on the badge either above or below the barcode by choosing a setting from the "Text" dropdown in Object Properties.

2D Barcode: Information contained in a 2D Barcode can be mapped to multiple PassagePoint data field. To assign data to the barcode, select the barcode and double-click on a blank field below the PDF417 Barcode label in Object Properties. Additional data items can be added to the 2D barcode by double-clicking on the next blank line and selecting a data field. Similarly, double-click a line to change its

assigned field. When creating a 2D Barcode with multiple data fields, allot extra room for it to expand for varying amounts of data.

Object Properties

To configure how an object displays on the badge, select an object on the badge layout canvas and set its properties in the Object Properties panel. Each object type has its unique property settings. Highlights of various object properties follow.

- 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. See the Other Objects section above for details.

Print Preview

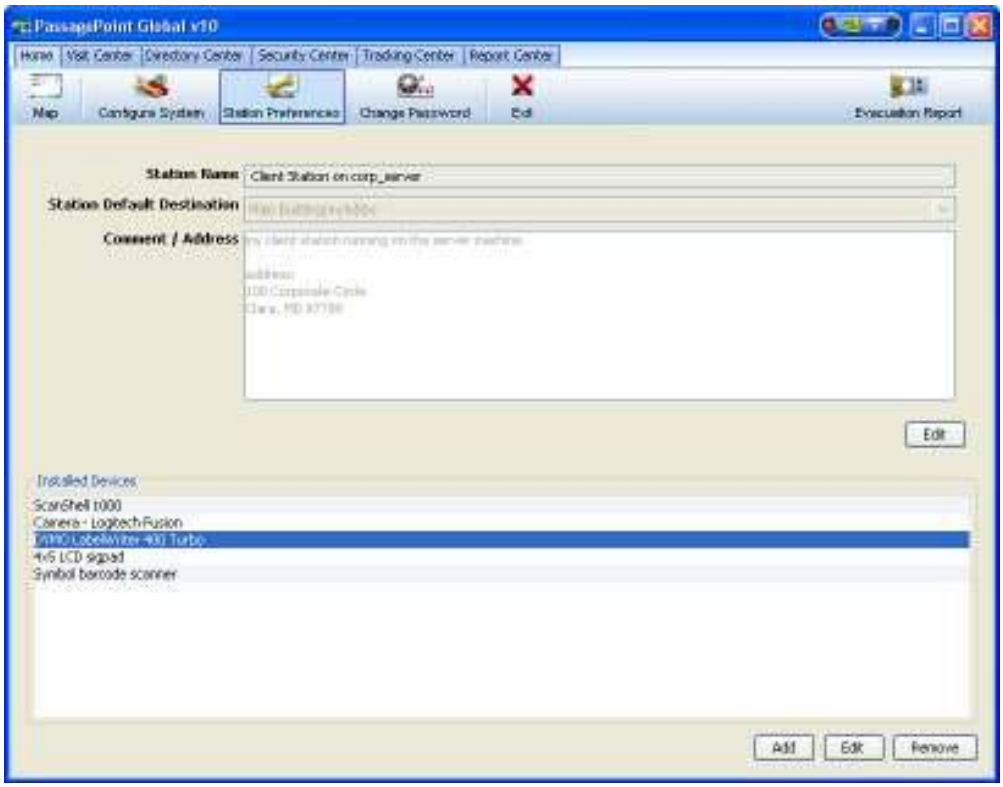
A sample of how the badge or label will appear can be viewed by clicking "Print Preview". This may not be an accurate representation of your printed badge since length of data will vary.

Chapter 6 – Station Preferences & Devices

Hardware devices that are supported at a PassagePoint Station is configured from within the Station Preferences screen. Supported hardware for Global includes printers, Logitech cameras and Card Scanning Solutions scanners. To access the Station Preferences screen, open *Home | Station Preferences*.

In the Station Preferences Screen, you can name the current station by clicking "Edit" in the top panel for Station. In the Station Details screen, you can also add a comment about the station and/or add address information.

Figure 17 - Station Preferences



Managing Hardware Devices

To access the device configurations for this station, click the "Add", "Edit" or "Remove" button in the bottom panel for Installed Devices.

When adding a device, you first select the type of device you want to create a configuration for. In subsequent screens, you will typically specify the manufacturer, model and configuration for the device. For devices that are manufacturer and/or model independent, such as barcode scanners, you may only see a configuration screen. Before adding a device, install the driver from the device manufacturer.

After adding device configurations to your station, we suggest that you close PassagePoint and restart it before trying to perform capture scans.

Editing a device allow you to only edit the configuration for the device. You will not be able to specify the make and model within edit. To specify a new manufacturer and model, we recommend that you add a new device configuration.

Cameras

When adding a Logitech camera, you first need to install the drivers. Logitech cameras are connected via a station's USB 2.0 port. Logitech camera drivers will install as a generic Logitech Camera, a WIA Logitech QuickCam, or both.

PassagePoint installs and uses a generic camera driver named Video DataSource. The Video DataSource driver is used to easily select the camera source type and configure settings such as resolution. Camera settings can be specified when the Photo Capture is activated from PassagePoint Client data entry screens.

Figure 18 – Camera Setup

Business Card / ID / Passport Scanners

Several Card Scanning Solution scanners are supported with PassagePoint, including SnapShell, ScanShell 800, 800N and 1000. Depending on the model, you will be able to capture data from either business cards, driver's licenses, ID cards, or passports. Additionally, a Magshell 900 scanner can be added for scanning magnetic strip information on the back of licenses.

On the Device Configuration screen for some scanner models, there is a "Calibrate" button that allows you to reset the scanner. When calibrating ScanShell flatbed scanners, Card Scanning Solutions recommends that you have the cover open during the calibration procedure. For some scanners, you will need to insert a calibration sheet into the scanner. Consult your hardware documentation for calibration instructions.

Figure 19 - Scanner Setup

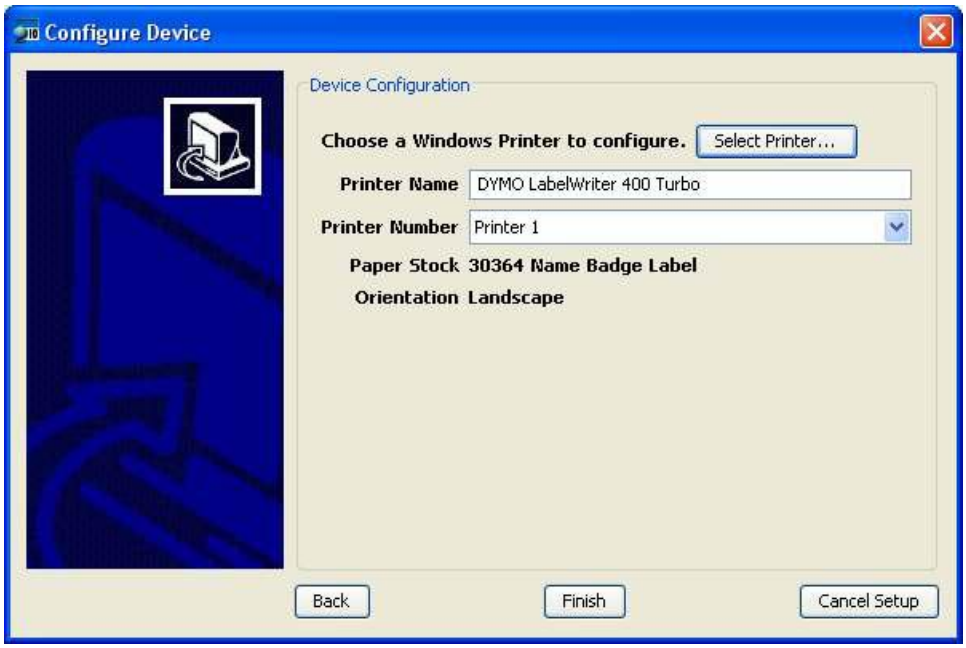
Whenever a scanner doesn't seem to correctly capture major portions of data, use the "Calibrate" button to re-calibrate and initialize the scanner. This will typically resolve most scanner issues. To re-calibrate a scanner, select the scanner configuration from Installed Devices in *Home | Station Preferences* and click "Edit". From the Device Configuration screen, click "Calibrate".

Badge Printers

Printers for printing badges are configured in Station Preferences. Printers for reports do not need to be configured within PassagePoint. When reports are printed, a Print Setup dialog will appear that allows users to select the printer to use.

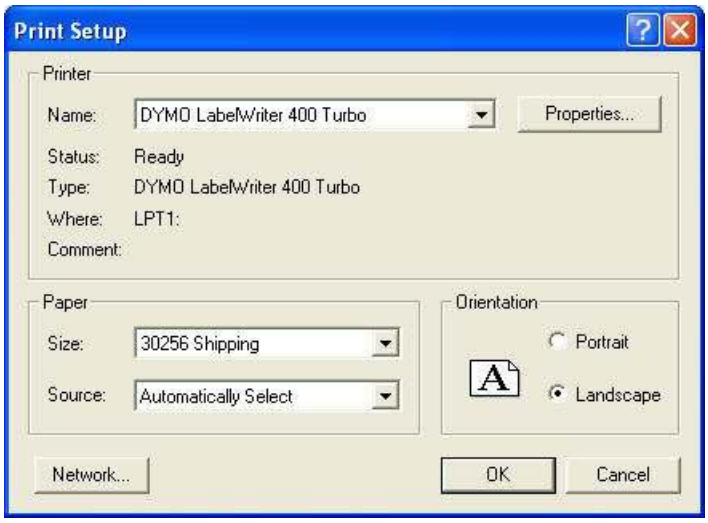
Printer queues for your badge printers need to be configured in Windows Printers and Faxes before adding it to PassagePoint. When adding and editing a printer configuration, you will find that the Device Configuration screen has a "Setup Printer…" button. Clicking this button will open the Windows Print Setup screen.

Figure 20 – Printer Device Configuration



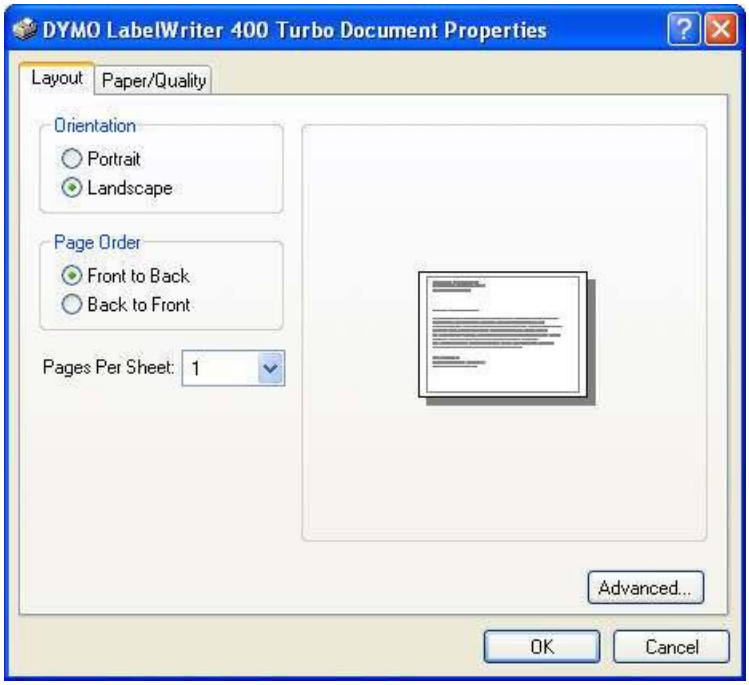
Specify the printer you are configuring by selecting the printer from the "Printer Name:" dropdown. The size of badge stock can be selected in the Paper section. Specify the orientation of your badge by selecting landscape or portrait layouts. If portrait and landscape badges are printed, then create a second printer configuration to handle the second layout format.

Figure 21 - Print Setup



Click "Properties…" to specify additional printer settings. This includes settings such as Page Ordering which would be applied when printing badges for multiple visitors in a group. In the Paper/Quality tab, specifying Black & White or Color has similar print results.

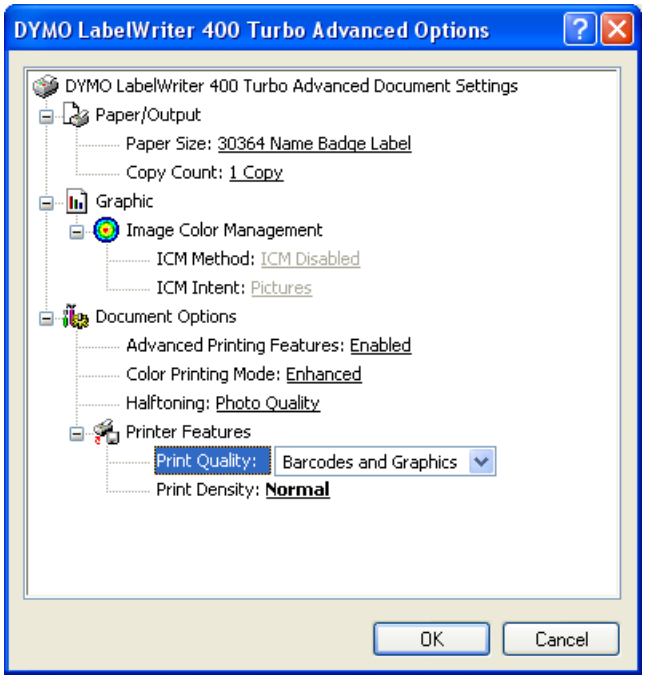
Figure 22 - Printer Properties



For Dymo printers, you can specify the print quality, density and halftone settings and by clicking "Advanced…" from the Properties screen. We suggest using these settings:

- Halftoning: Photo Quality
- Print Quality: Barcodes and Graphics
- Print Density: Dark

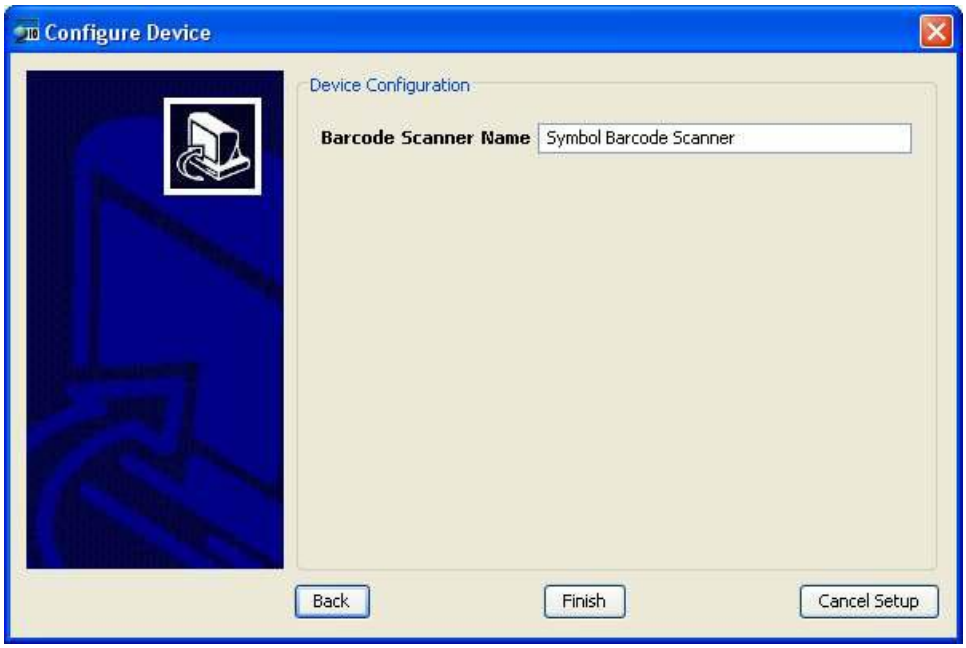
Figure 23 - Printer Advanced Options



Barcode Scanner Devices

Signing people in and out can be drastically sped up by scanning barcodes printed on badges or sent via Email. When configuring barcode devices, choose Symbol/Motorola when configuring one of their barcode scanners. For scanners from other manufacturers, choose *Generic serial barcode scanner* and configure your scanner as a COM port device. Barcode Scanners must be able to configured for OPOS/JPOS (Point of Sales) for it to properly run with PassagePoint Client. After selecting the manufacturer, specify a name for your device on the Device Configuration screen.

Figure 24 – Barcode Scanner Configuration



Additionally, you will need to configure a Barcode Scan Policy to set how barcodes are handled when scanned.

Signature Capture Devices

Using a Topaz signature capture pad, people can electronically sign agreements. Any agreements may added to PassagePoint for people to sign during registration time, including non-disclosures, personal releases and acknowledgments.

To configure a signature pad, select Signature Capture Pads from Station Preferences' Configure Device screen. Select one of the supported models of the Topaz signature pad, i.e. either SignatureGem 1x4 or 4x5. On the Device Configuration screen, enter a name for the signature pad and specify the port. Typically, Topaz will appear as a HID1 port device.

Figure 25 – Signature Capture Configuration

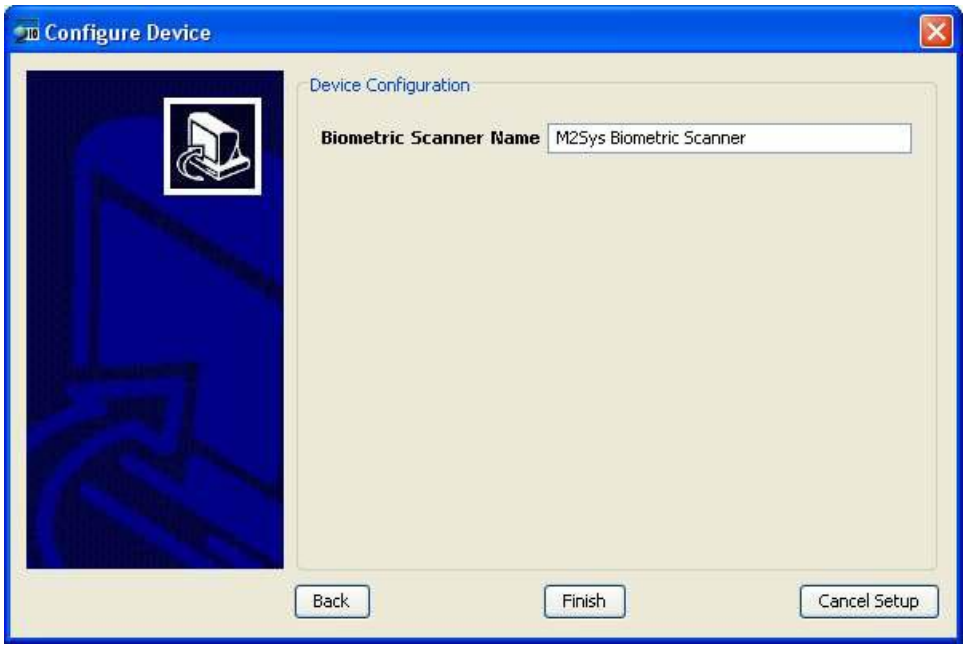
Biometric Fingerprint Scanner Devices

Fingerprint scans can be used to identify a person for easy registration. A new person can be enrolled into the biometric database on their first sign-in. On return for sign-out or subsequent registrations, their fingerprint can be scanned to identify them and bring up their record.

Currently, PassagePoint supports the M2-Hamster scanner from M2Sys. Additional scanners will be supported in the future.

To configure a fingerprint scanner, choose "Biometric Fingerprint Scanner" from the list of Configure Device screen when clicking Add or Edit from Station Preferences. On the second configuration screen, specify the name of the device.

Figure 26 – Biometric Scanner Configuration



Chapter 7 – External Systems

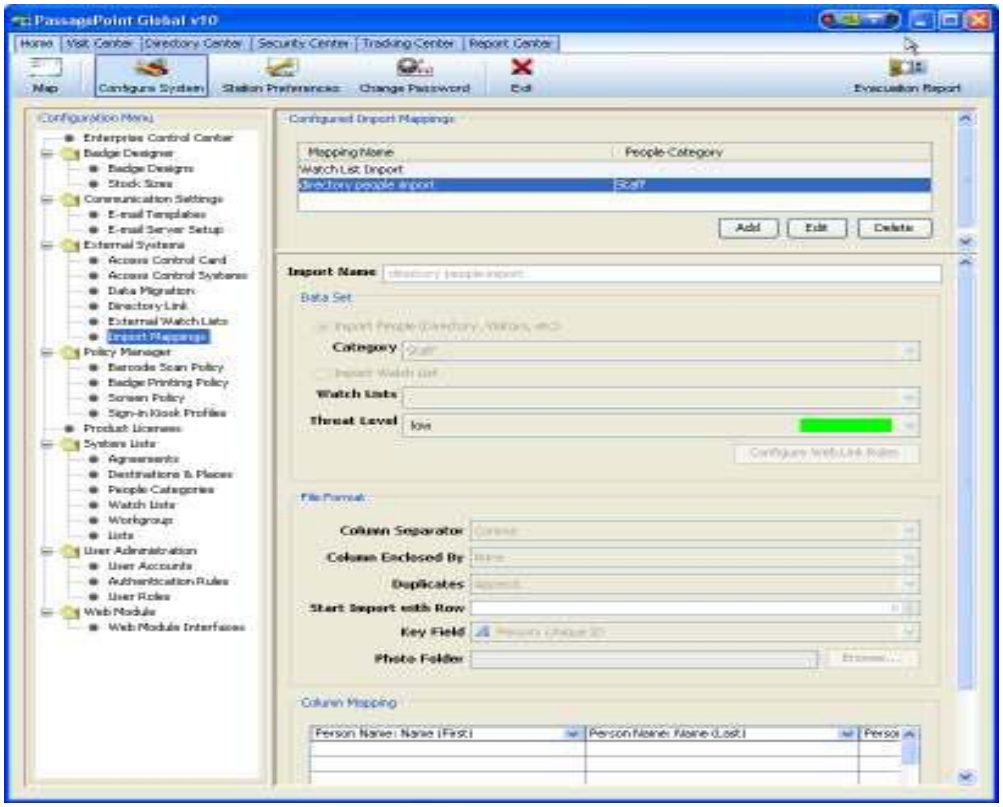
People data from external systems can be imported into PassagePoint. This includes importing people into Directory, Visit Pre-Registration and Extended Authorization.

Additionally, PassagePoint allows for verifying visitors against an on-line Megan's Law Sex Offender database.

Import Mappings

The import process entails creating an Import Mapping and running it against a text import file in a Center screen. To import people or Watch List data into PassagePoint, first create an Import Map. A map defines the format of the import file and the data fields that the import data gets saved to. To define or edit an Import Map, open *Home | Configure System | External Systems | Import Mappings*.

Figure 27 - Import Mapper Screen



In this section, we will use standard relational database terminology, such as rows and columns. Imagine data in the import file as a grid where rows are each new data record, e.g. each person in the import file is a row. A column represents a data value of a particular type, e.g. city data for people is a column.

To create an Import Map, click "Add" from the Configured Import Mappings panel. If the configuration of the map changes, such as a change to people category, file format setting, or column ordering, you will need to either edit or add a new mapping before attempting to run the import.

Data Set

You can either import Directory people or Watch List people. Choose between either to import People or Watch List in the Data Set panel. With people, select the category for the data set that you will import. Watch List requires specifying a Threat Level for the import data set. The category or threat level that you select will be used for all records imported in a single import session. If your one import file contain multiple category of people or multiple threat level for Watch List, you will need to split the file into multiple files based on category or threat level and create multiple Import Maps for each.

File Format

Under File Format, specify the delimiters for columns. Columns may be separated by space, tab, comma or semicolon. Each column can also be enclosed with single or double quotes.

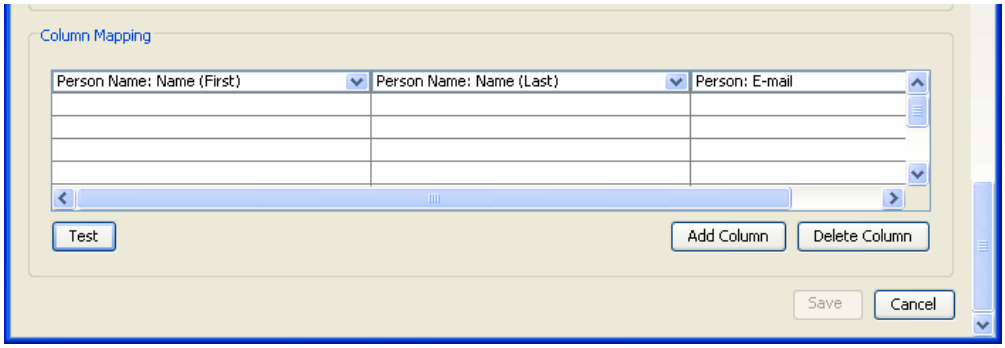
For cases where an import record is already found in PassagePoint, you can specify to have the import record added as a duplicate by picking Append in the Duplicates dropdown. Alternatively, you can replace the PassagePoint record with the import data by selecting Replace. This is useful if a previous import was not successful and you want to re-import the data. One last choice is to skip import of the record and have the data already in PassagePoint remain as is.

After adding column mappings, use Key Field to specify the column to use for checking for duplicates. Key Field is only active when Duplicate is set to skip or replace, since append means to always add regardless of duplicates. Columns listed for key fields are is unique to a person, such as E-mail, phone number or a unique ID.

Column Mapping

Columns to be imported are mapped to fields within PassagePoint in the Column Mapping panel. This correlate data from the import file to the data fields within PassagePoint.

Figure 28 - Column Mapping in Import Mapper



Click "Add Column" to insert a column into the mapping. New columns are added at the end on the right. From the column dropdown, select the PassagePoint field that this data will be saved to. Skip indicates to ignore data in that particular import column. To delete a column, select the column by clicking the column map dropdown and clicking "Delete Column".

Test the import map by clicking the "Test" button and specifying an import file. PassagePoint will display the first nine lines of data that would be imported from the specified file.

Running Imports

After defining an Import Map, you can import data into PassagePoint by using the import features within the Visit and Directory Centers.

External Watch List – Sex Offender

PassagePoint has the ability to check visitors against a Megan's Law Sexual Offender database. When a visitor arrives, you can check the person against a national sex offender database by entering the person's full name and optionally their date of birth. When matches are found, you will be able to view details on the matching offenders including their physical description, address, offense and photo.

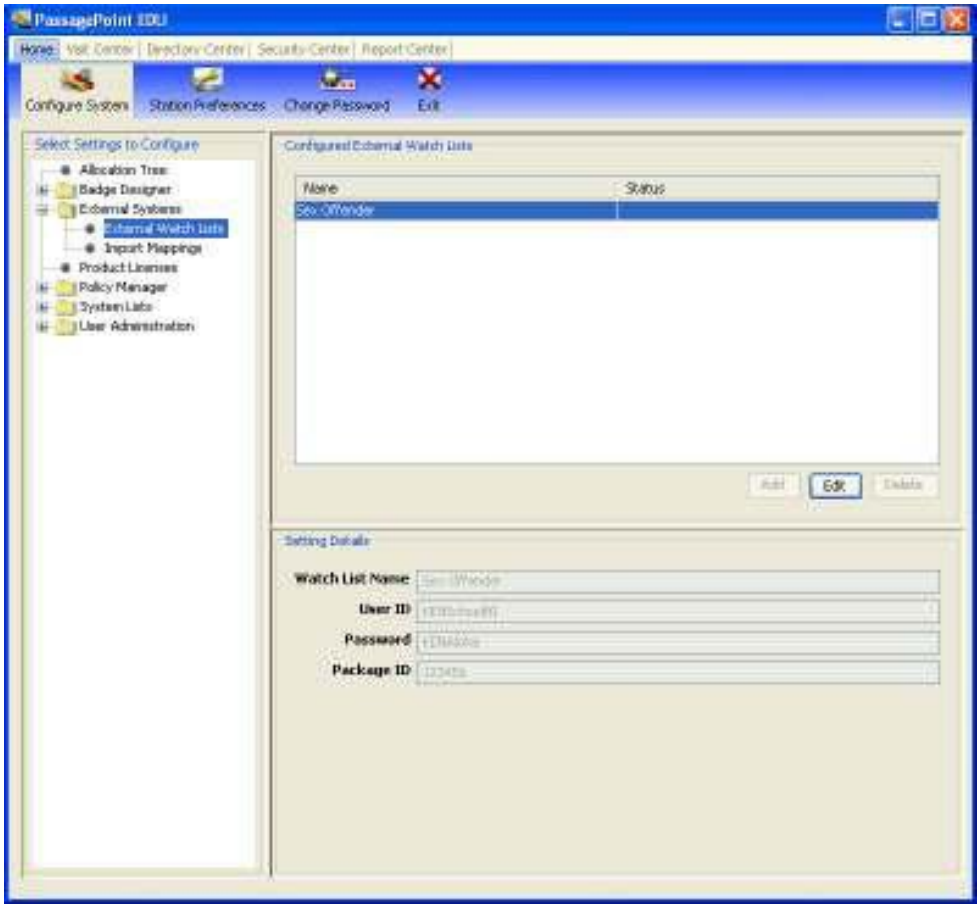
This feature requires that you purchase a subscription from The Safe School Project. For information about The Safe School Project, access their website at http://www.safe-schools.com.

Configuring Sex Offender Account

To be able to conduct Sex Offender searches, you need to configure your Sex Offender account. Account information will be provided to you directly from The Safe School Project.

Configure the Sex Offender Watch List interface by accessing *Home | Configure System | External Systems | External Watch List* and select "Sex Offender". Click "Edit" to enter the account information you received from The Safe School Project.

Figure 29 - Sex Offender Watch List Settings



In the Setting Details screen, specify the User ID, Password and Package ID information that you received from The Safe School Project. Note that the account information is case sensitive.

To test your account, conduct a search for an offender under *Home | Security Center | Sex Offender Search*. A search result of either "No matches found" or "Match found" indicates that your account has been correctly configured. If it returns an error, then the account information is either incorrect or your Safe Schools account is not active. In this case, please contact The Safe School Project for account inquires.

Searching the Sex Offender Database

In the Visit Center, you will find a "Sex Offender Search" button on various screens. After entering a visitor name or after scanning a driver's license, state ID or passport, you can click this button to conduct an offender search. Search queries are sent over the Internet to The Safe Schools Project web database.

When the search completes, a dialog screen will display whether a match was found or not. If a match is found, click "OK" to display detailed information about matching offenders. If an error message is displayed, check your account configuration and make sure the Safe Schools account is active.

Alternatively, you can use the Sex Offender Search screen under *Security Center | External Lists*. Enter the person's full name and optionally their date of birth and click "Search" to query The Safe Schools Project.

Figure 30 - Sex Offender Search

Directory Link

Instead of importing people into the Directory of the local PassagePoint database, Directory Link can be used to access live data from a remote company directory database. Connecting to a remote directory instead of maintaining people locally allows you to avoid extra maintenance within PassagePoint such as adding new people who have joined your organization.

People data such as name, Email, ID number, etc can be linked from the remote directory to corresponding data fields within PassagePoint. Connection to the remote directory uses the following standard protocols:

- Lightweight Directory Access Protocol (LDAP)
- Open Database Connectivity (ODBC)
- Java Database Connectivity (JDBC)

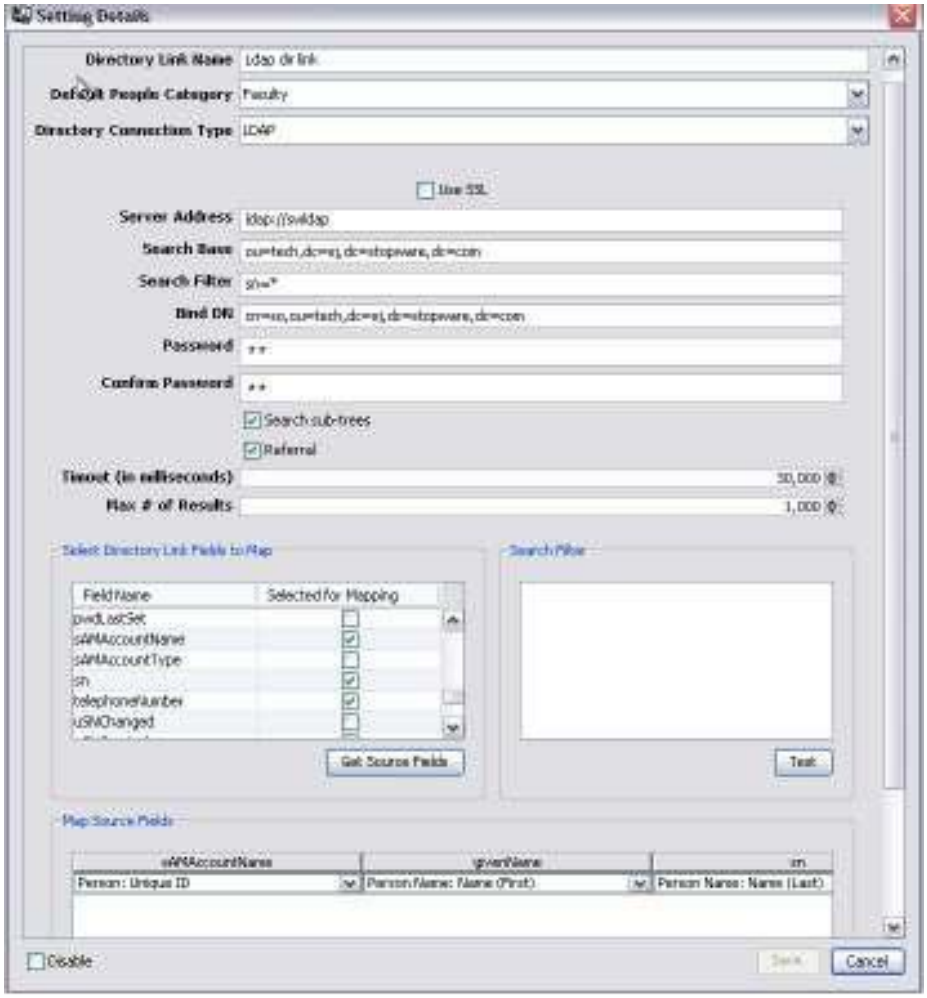
Configuring Directory Link for LDAP

A directory administrator should be able to provide the LDAP server settings, such as server address, search base (location in LDAP tree to start looking for people) and bind DN.

After entering directory database / LDAP connection information, click "Get Source Fields" to access a list of fields from the directory server. Within the "Select Directory Link Fields to Map" section, check the fields for data that you want to transfer into PassagePoint. These fields will then need to be mapped to a corresponding PassagePoint field in the "Map Source Fields" panel.

To configure PassagePoint Directory Link to access a remote directory using LDAP protocol:

1. Launch the client application and login as an Administrator user.
2. Select Home | Configure System | Directory Link. If the option is not listed, check that a Directory Link license has been installed under Product Licenses.
3. Click Add to create a new Directory Link definition.



4. Pick the category for the directory people from the Default People Category drop-down list.
5. Select LDAP from the Directory Connection Type drop-down. Check SSL if it is needed for connecting to the LDAP server.
6. In Server Address, enter the LDAP server connection string.
7. In Search Base, enter the fully-qualified organizational unit in which you want PassagePoint to pull directory people from.
8. Enter a Search Filter string. To pull all records, use sn=*
9. In Bind DN, enter the LDAP context to use.
10. Enter the Password used to connect to the LDAP server.
11. Check Search Sub-trees to include branches in the tree contained within the specified context.
12. Check Referral to pull people data that are referenced in other tree locations outside of the current context.

13. Timeout sets the number of milliseconds to wait for directory search results to return.
14. Max # of Results sets the upper limit for large directory query results.
15. Click the "Get Source Fields" button to load the table columns from the Directory database.
16. Select the Directory data that you want linked to PassagePoint by checking the data column names. For distinguishing between people with the same name, we suggest that columns representing a unique value be included, such as an Email address, phone number or employee ID be included.
17. In the Map Source Fields panel, choose the corresponding PassagePoint field name. Note that the Unique # field may be used for quick sign-in with barcodes.
18. Click Preview to view a sample of data that will be mapped.
19. If data in the table needs to be filtered,
20. Click Save to save the configuration.
21. To verify the LDAP Directory Link, enter a name of a person who is in the directory on a Visit Center entry screen's Host name fields.

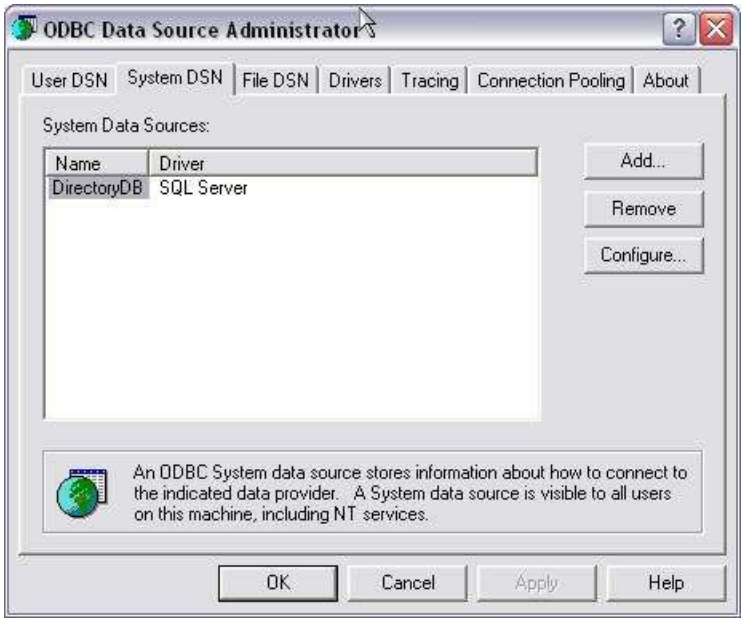
Configuring Directory Link for ODBC and JDBC Connections

PassagePoint Directory Link has the ability to connect to a remote database using an ODBC or JDBC driver. Unlike LDAP, ODBC and JDBC requires that the database connection be configured from within Windows. If you already have an ODBC connection defined to the Directory database on the PassagePoint Server machine, you can skip this set of steps. For JDBC, you may need to installs JDBC drivers based on the database type(SQL Server, Oracle, etc) your Directory is running on.

Setting up the ODBC Data Source

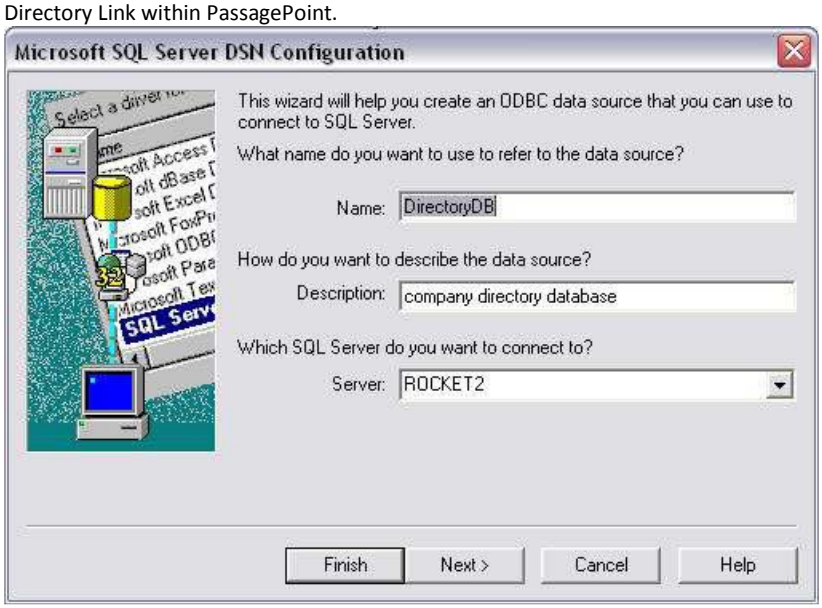
Below are steps for configuration an ODBC connection to a SQL Server database as an example. Consult with your company DBA for assistance with configuring other database connections.

1. On the PassagePoint Server machine, open Windows Control Panel – Administrative Tools. Launch the Data Sources (ODBC) utility.
2. Click on the System DSN tab. Click Add.

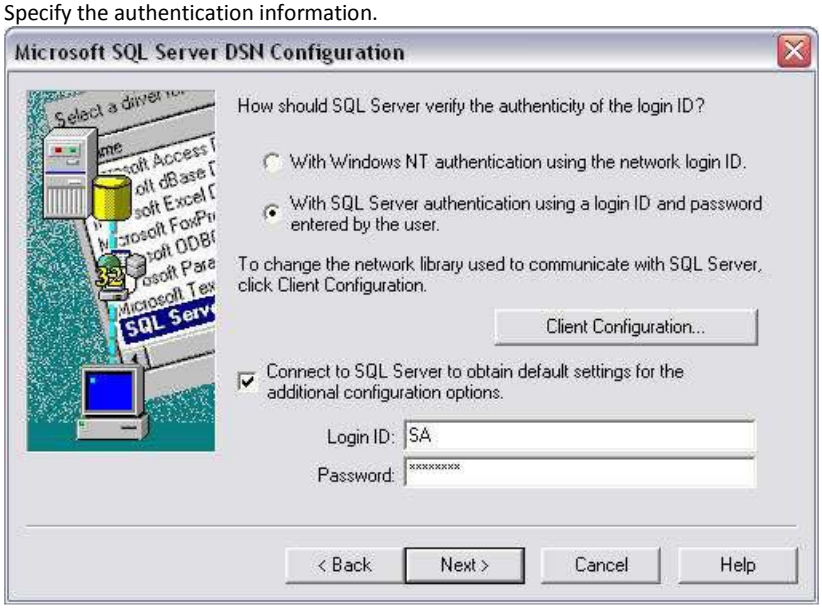


3. Select SQL Server from the list of ODBC drivers and click Finish.

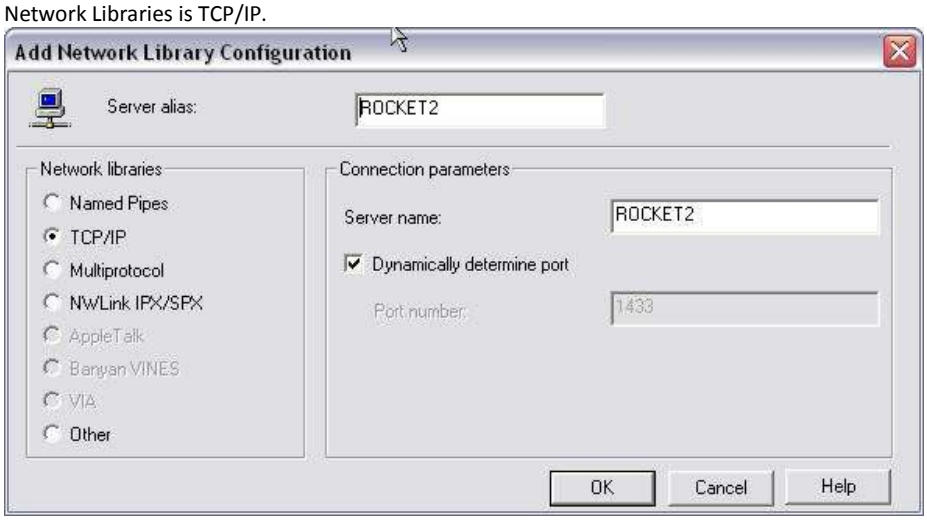
4. Assign a Data Source Name (can be set to any name). This name will be used later in configuring Directory Link within PassagePoint.



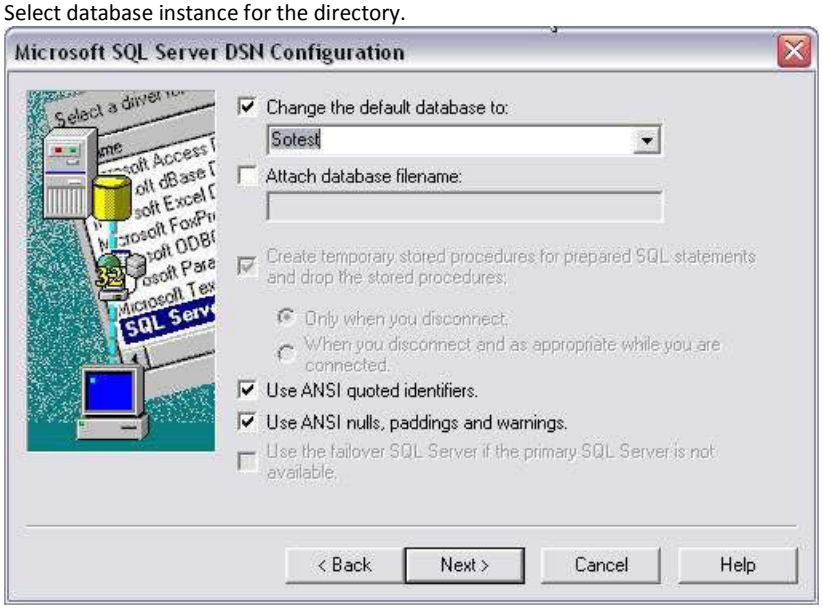
5. Select the server pick list where the system where the directory database is located. Click Next to continue.
6. Specify the authentication information.



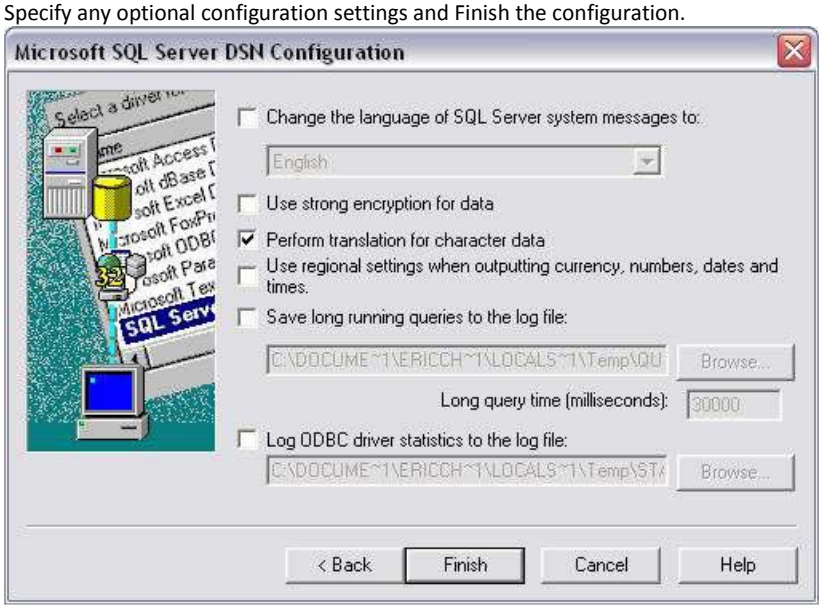
7. Click Client Configuration and verify that the network settings are correct. Typically, the Network Libraries is TCP/IP.



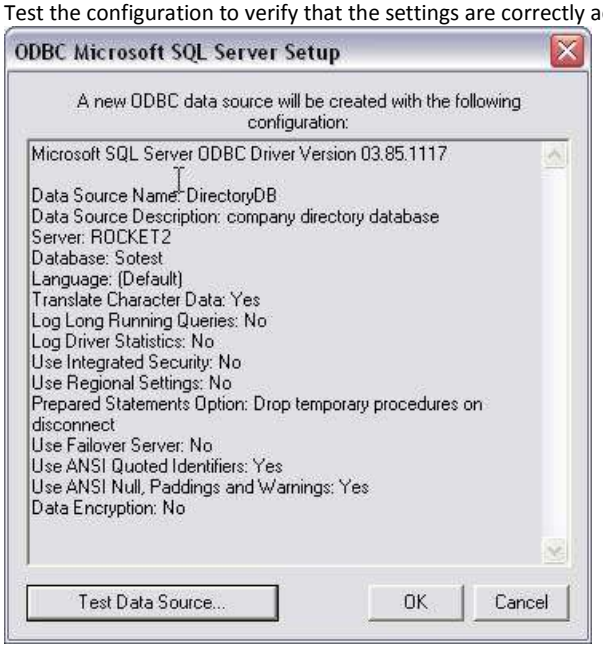
8. Select database instance for the directory.



9. Specify any optional configuration settings and Finish the configuration.



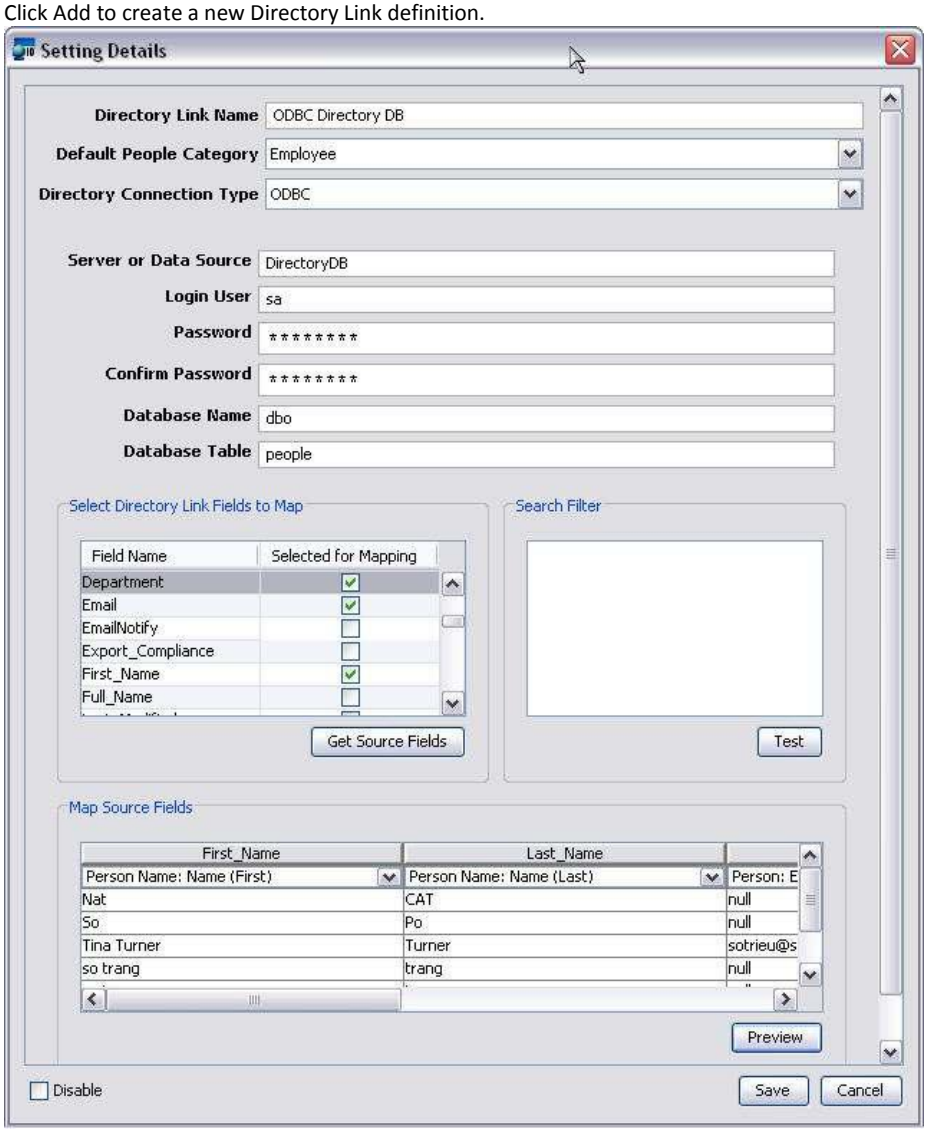
10. Test the configuration to verify that the settings are correctly accessing the Directory database.



11. This completes the configuration of the ODBC DSN.

Configuring ODBC Connection in Directory Link

1. Launch the client application and login as an Administrator user.
2. Select Home | Configure System | Directory Link.
3. Click Add to create a new Directory Link definition.



4. Pick the category for the directory people from the Default People Category drop-down list.
5. Select ODBC from the Directory Connection Type drop-down.
6. In Server or Data Source, enter the DSN Name that was specified in step 4 in the previous section.
7. Enter the Login Name and Password used to connect to the Directory database.
8. Enter the Database Name to connect to.
9. Enter the name of the Table in the database to pull directory data from.
10. Click the "Get Source Fields" button to load the table columns from the Directory database.
11. Select the Directory data that you want linked to PassagePoint by checking the data column names. For distinguishing between people with the same name, we suggest that columns representing a unique value be included, such as an Email address, phone number or employee ID be included.
12. In the Map Source Fields panel, choose the corresponding PassagePoint field name. Note that the Unique # field may be used for quick sign-in with barcodes and for Web User Account authentication.
13. Click Preview to view a sample of data that will be mapped.
14. If data in the table needs to be filtered,
15. Click Save to save the configuration.
16. To verify the ODBC Directory Link, enter a name of a person who is in the directory on a Visit Center entry screen's Host name fields.

Access Control System

Below is an example configuration for a C-Cure Access Control System from Software House. Similar steps are performed with other Access Control System.

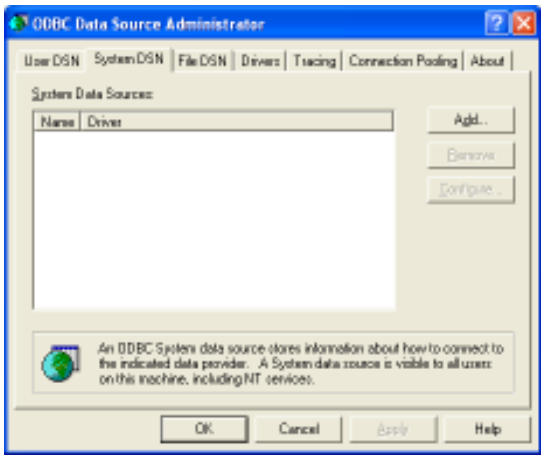
Install MDB files on the C-Cure server:

1. Locate the CCure.mdb file located on the PassagePoint CD
2. Copy the file to the CCure server within a folder like C:\ccureMdb\
3. Share the ccureMdb folder

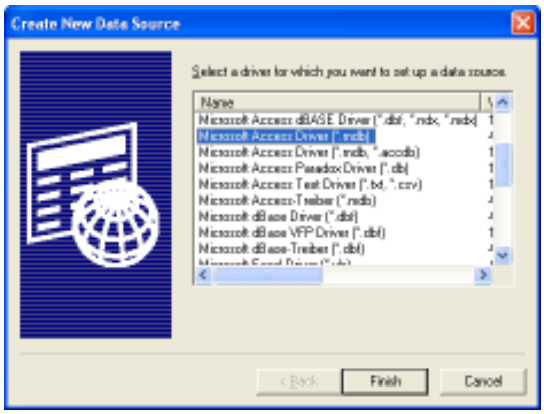
Configure the C-Cure server:

1. To create an ODBC source. Go to control panel>Admin tools.

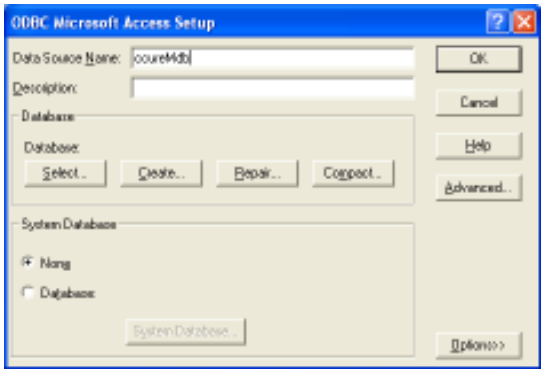
2. Click on Data source ODBC, click on the System DSN tab and then click on Add.



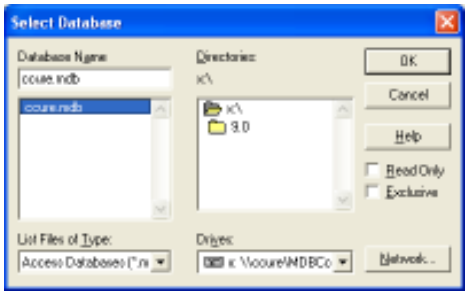
3. Select the Microsoft Access Driver, and Finish.



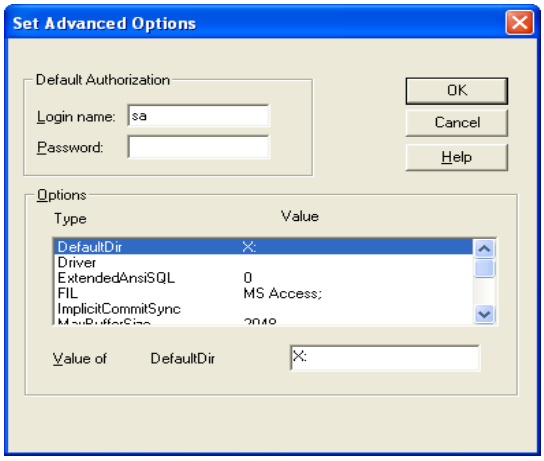
4. Enter an ODBC name (e.g. ccureMdb.)



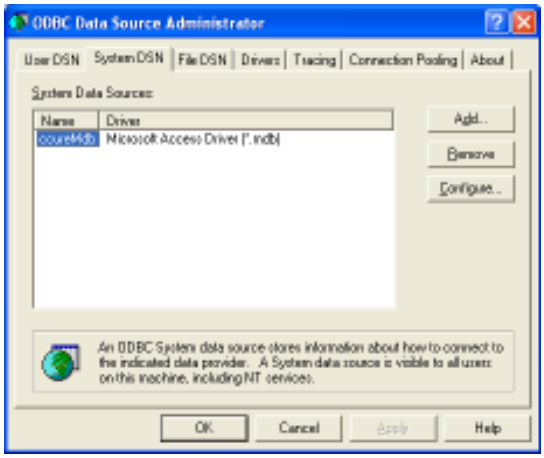
5. Click on Select, select the drive to the MDB file (e.g. x: drive), select the ccure.mdb file and click OK.



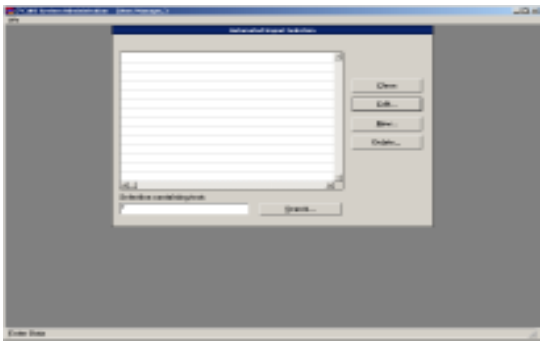
6. Create a login name. Click on the Advance button, enter a user name (e.g. sa), and click on OK.



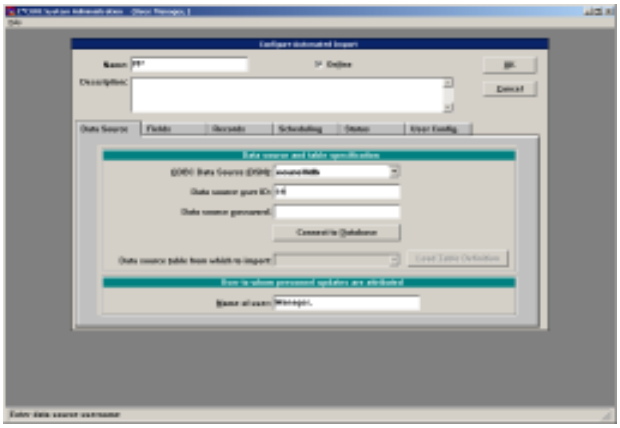
7. Click on OK again, the ODBC should now be created.



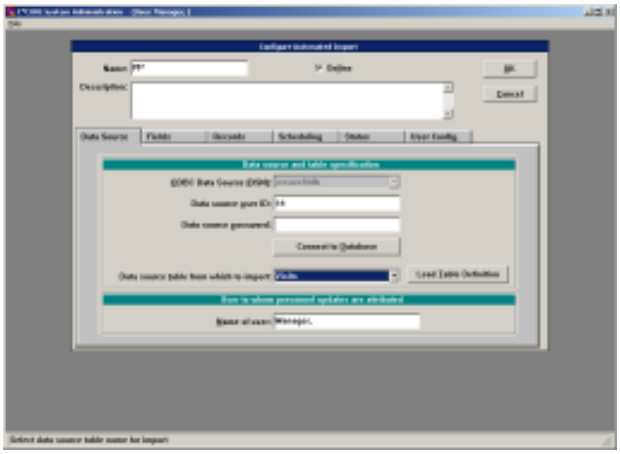
8. Log into your CCure client, click on Personnel>Automated Import to set the automated import.



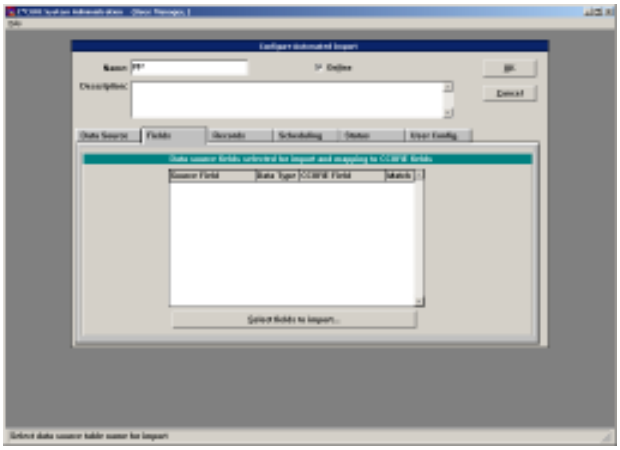
9. Click on New. Enter a name for the Name field, select your ODBC source, enter the data source user ID (e.g. sa), and enter a password (if available).



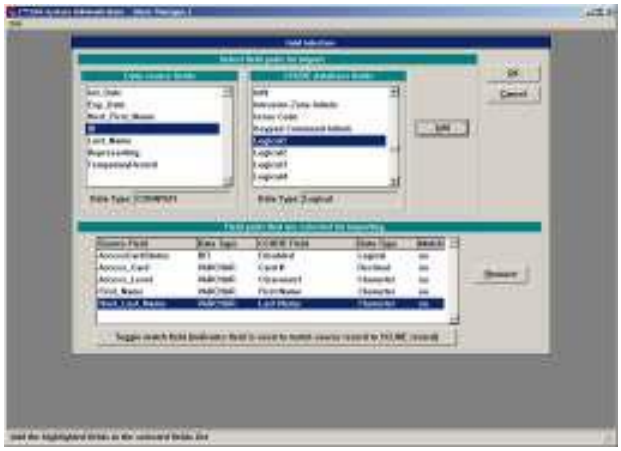
10. Connect your database by clicking on Connect to Database, the Data source table from which to import will enable. Select the Visits table. Load the fields by clicking on Load Table Definition



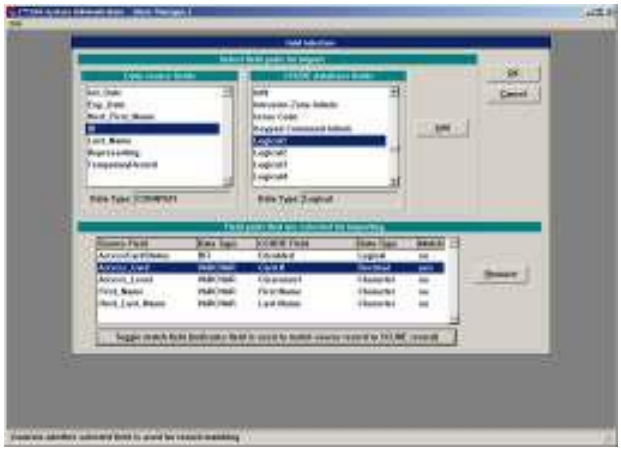
11. Map the PassagePoint fields to CCure fields so that CCure can import data by clicking on the fields tab, and then click on the Select fields to import button.



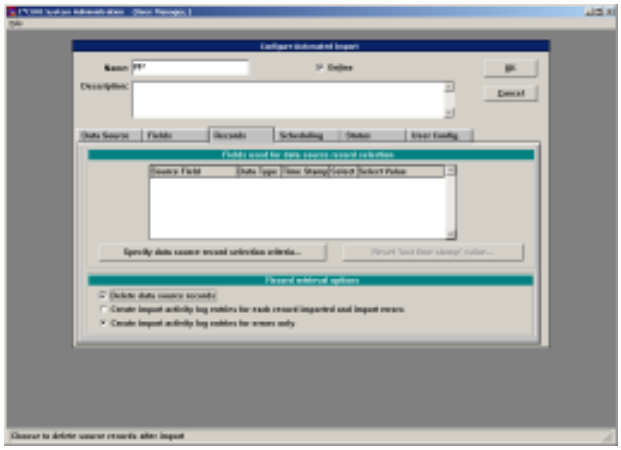
12. To map the fields you must select Data source fields and a CCure database fields and Click on Add. Below are some of the critical fields that need to be mapped.



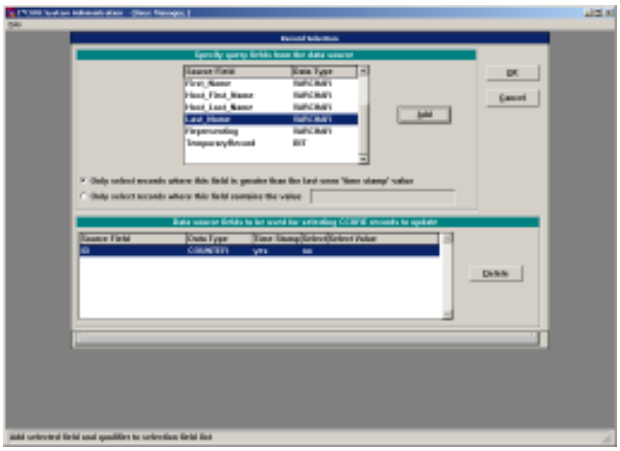
13. To match the access card field, select the Access Card and click on Toggle match field.



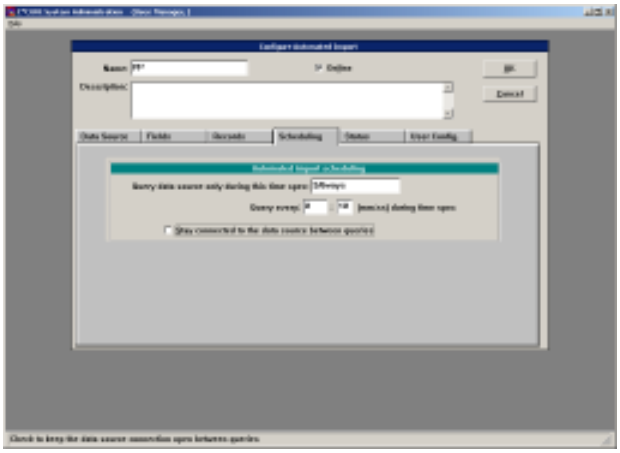
14. Click on the records tab, select the Delete data source record box, and click on Specify data source record selection criteria.



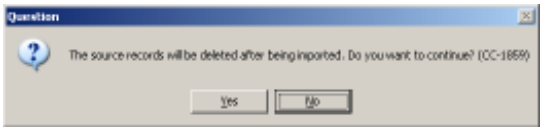
15. Select the ID source field, click on Add, and click on OK



16. Click on the scheduling tab, and change Query every field to 10 seconds



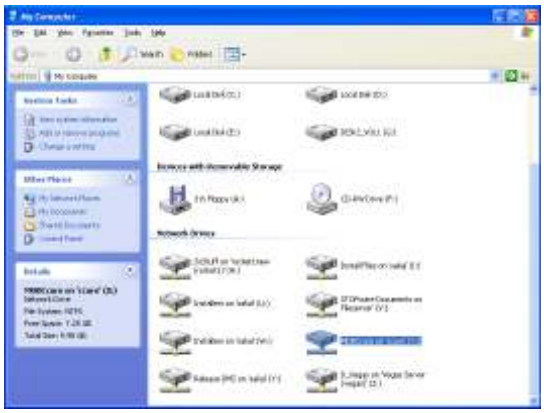
17. Click OK, a message box will appear, click Yes.



18. Now you are finish on the CCure machine

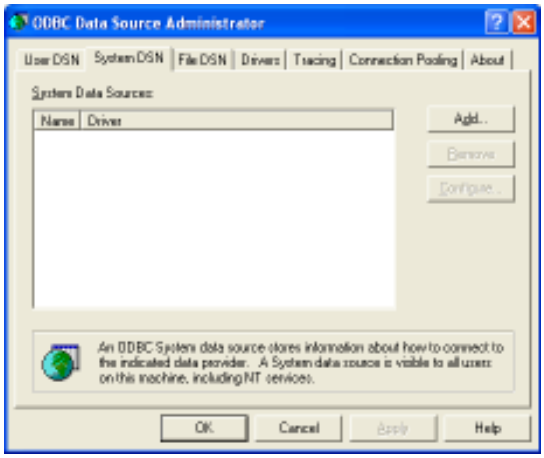
On the PassagePoint Server machine:

1. Map a drive to the directory containing the CCure.mdb file on the CCure Server (e.g. X: drive).

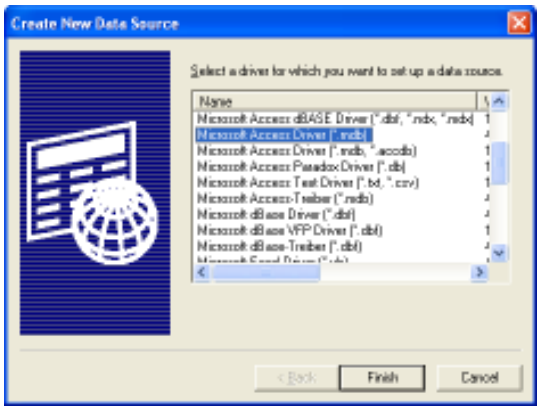


2. Go to control panel > administrator tools

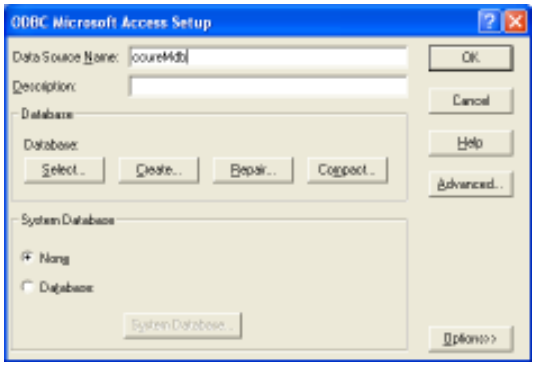
3. Click on Data source ODBC, go to the System DSN tab then click on add.



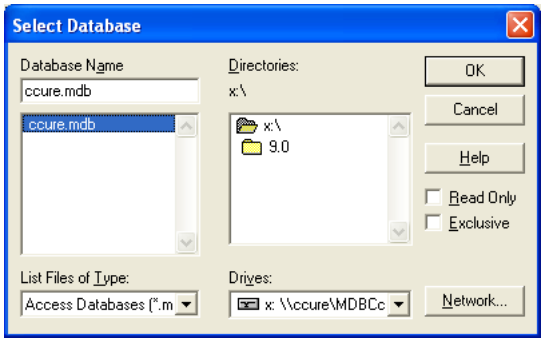
4. Click on Microsoft Access Driver, and Finish.



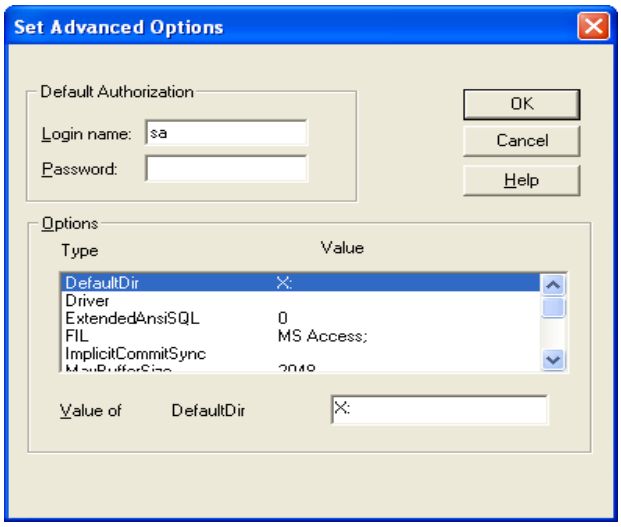
5. Enter an ODBC name (e.g. ccureMdb.)



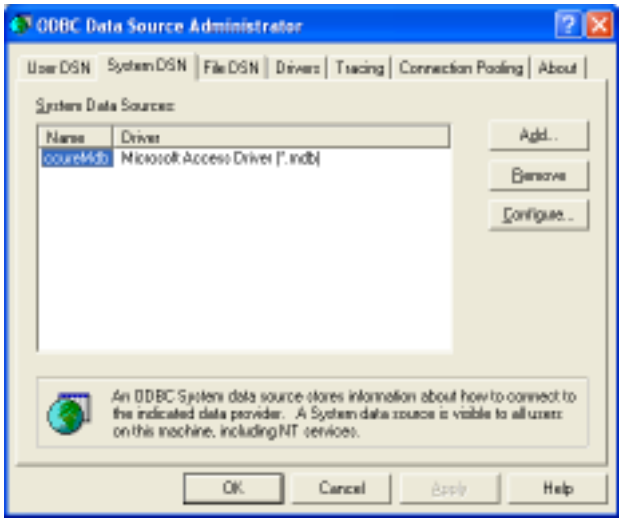
6. Click on select, select the drive to the MDB file (e.g. x: drive) and select the ccure.mdb file.



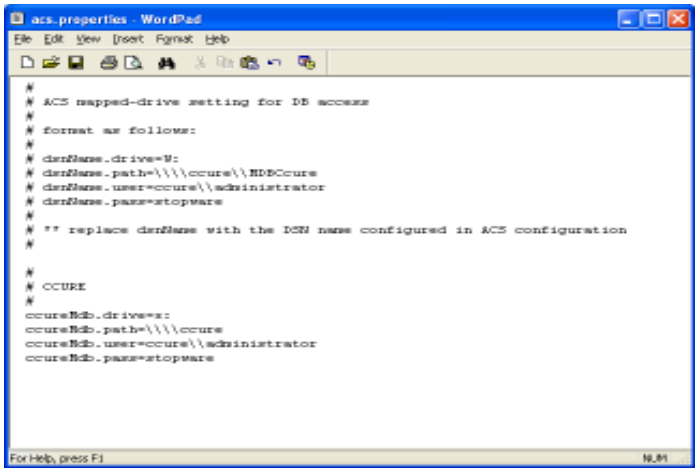
7. Click on the Advance button, enter a user name (e.g. sa), and click on OK.



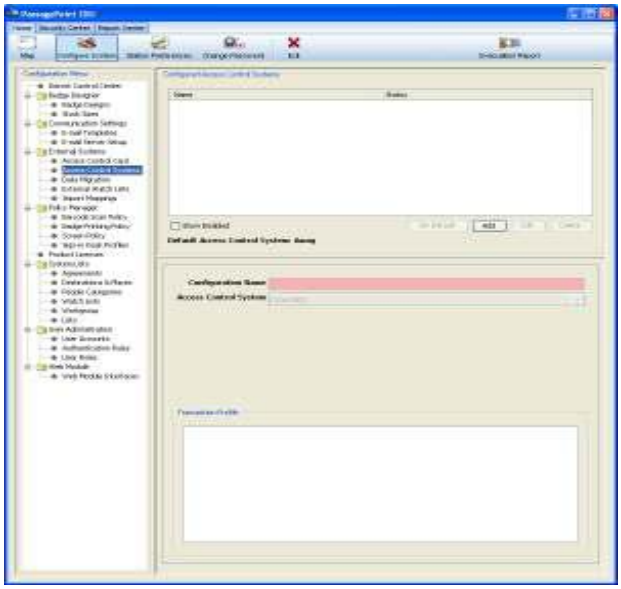
8. Click on OK again, the ODBC should now be created.



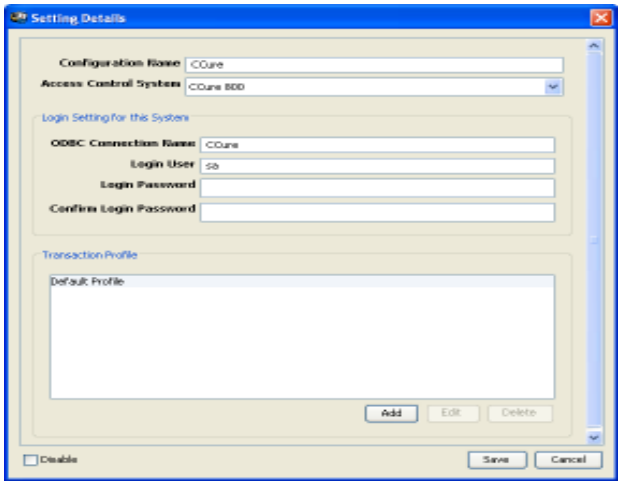
9. Go to your PassagePoint\tomcat\webapps\pp\web-inf\classes folder and edit the acs.propties file with Notepad or Wordpad.



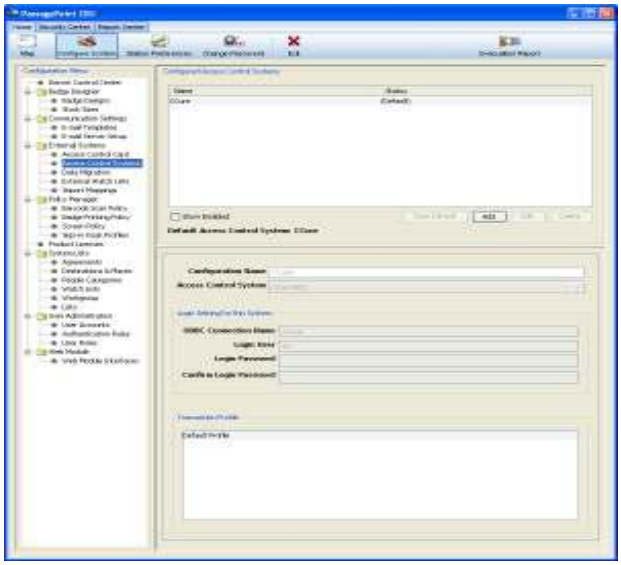
10. Change the dsnName (ODBC name also cap sensitive), the drive letter, the path, user name, and password. The example is provided above with the document marked with the # sign.
11. Restart the PassagePoint services.
12. Log into your PassagePoint client, and go to home>configure system>external system>access control system. Click Add.



13. Enter the configuration name, select the Ccure 800, enter the ODBC connection name (cap sensitive), enter the login user (required), and password (if available). Click on save.



14. Select the CCure name and click on set default.



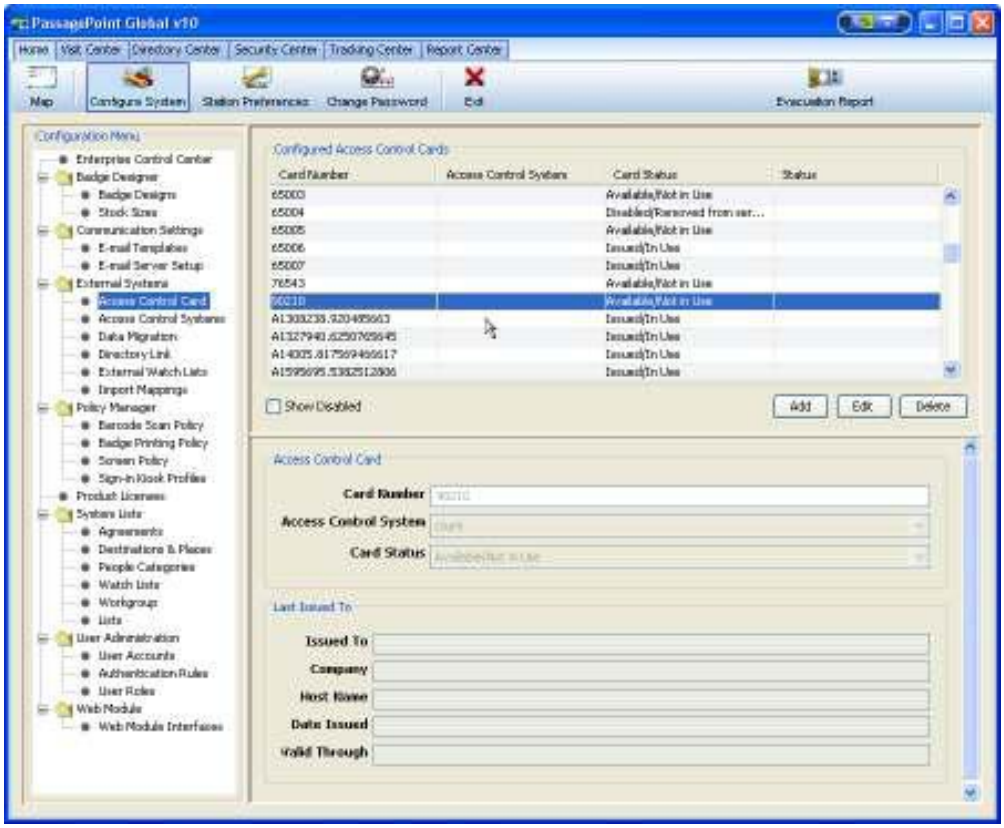
15. Restart the PassagePoint Client.

Access Control Card

Cards to be used with Access Control Systems can be tracked within PassagePoint. The status of the card is shown within the card listing. Cards may also be deactivated if lost.

From the Home | Configure System | External Systems |Access Control Card screen, card numbers can be tracked, as well as numbers added, edited or deleted. Card numbers can then be assigned to a visitor through the Access Control panel on the Rapid Registration screen when visitors are signed in. Signing a visitor out will automatically release the card for reuse.

Figure 31 – Configure Access Control Card Numbers



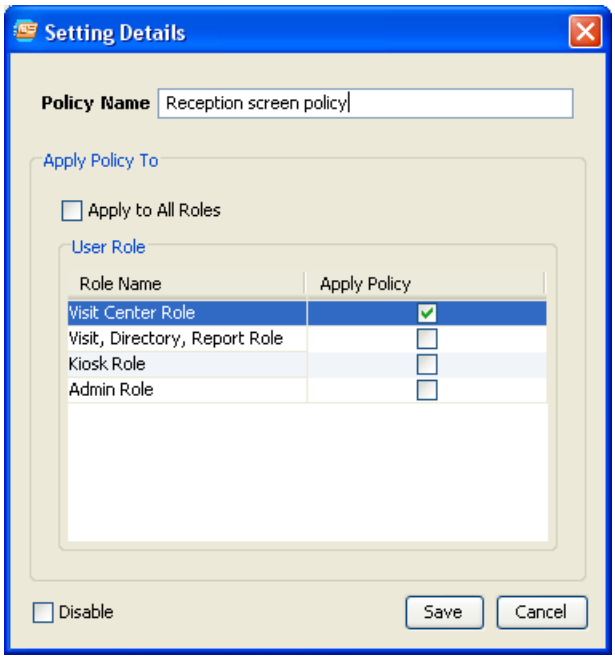
Chapter 8 – Policy Manager

PassagePoint provides you with the capability of modifying the fields on a screen. Field properties which may be altered include enabling users to change data and control the visibility of fields. Additionally, labels for fields can be modified to suit your needs, which is critical for renaming custom fields. Screens can be customized based on a user's role and category of people.

Screen Policy

To create a Screen Policy, access *Home | Configure System | Policy Manager | Screen Policy*. From within Configured Policies, you can click "Add" or "Edit" to manage a Screen Policy. Either buttons will open a Setting Details window that allows you to name the policy, modify a screen setting, and apply the policy to multiple User Roles.

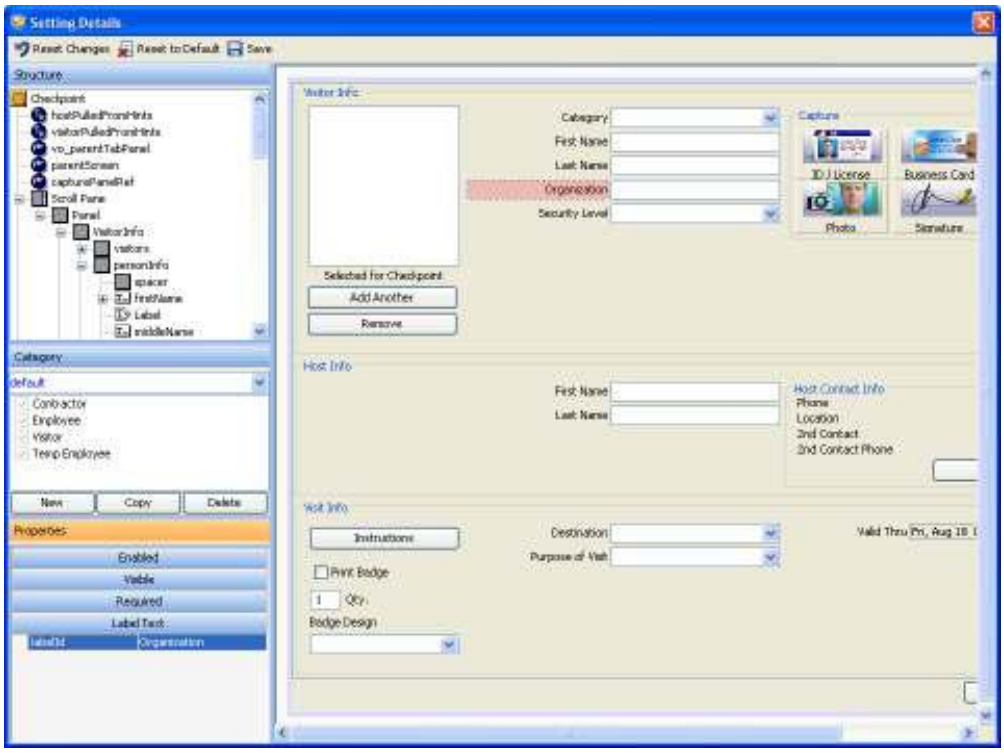
Figure 32 - Screen Policy Settings



Edit Screen Settings

Multiple screens may be modified under a single policy. To edit elements on a screen, select the Center and Screen Name from the dropdowns and click "Edit Screen Settings". The Screen Policy Editor opens and displays a mock of the screen to be edited with panels for modifying screen elements.

Figure 33 - Screen Policy Editor



The modifier panels shown on the left side of the Screen Policy Editor allows you to navigate to the various screen elements and change their properties. Additionally, you can create a category group that will be affected by this screen edit. A third panel controls the properties of elements on the screen and is used to set enable / disable editing, visible / invisible and field label text.

Setting Enabled Fields As Non-editable

Fields and elements on screens can be made to not be non-editable by setting their Enable property to False. Before setting the property, create a Category Group that this field enabling / disabling will be applied to. See the *Applying Screen Policies* section for more details on defining Category Groups.

To change the Enabled property, first select the field that you want to modify by clicking the field in the mock screen or selecting it from the structure panel. Next, select the Category Group that this property will affect. Then in the Properties panel, select the Enabled pane and set it to False. Switching between Category Groups will show elements that have been altered highlighted in pink.

Setting Visibility of Fields

Fields and elements on the screen can be hidden from users by setting their Visible property to False. Select a field, label or element that you want hidden by clicking on the item in the mock screen or by selecting it from the structure panel. Next choose the Category Group that this visibility setting affects. In the Properties panel, click Visibility and set the value to False for hidden. Switch between Category Groups to display the screen elements that have been modified.

Re-labeling Fields

Labels for fields can be renamed. This is handy if you are using custom fields to manage additional data that is not typically maintained by PassagePoint. As with Enabled and Visible, first select the label to modify and choose a Category Group. In the Properties panel, choose the Label Text pane and enter the new label value. If you want to reset the label to its default, delete the value for Label. Selecting between different Category Groups will show the labels that are applied for each. Modified labels display with pink highlights.

Business Logic Variables

Within each entry screen, you will find variable which can be set to specify you organization's business logic. By changing the values within these variables, you can specify policies such as whether data from a license is captured or not, host must be from the Directory, etc. For specific settings of each business logic variable, please contact Technical Support.

Applying Screen Policies

Screen Policies are applied to a group of Categories and to selected User Roles.

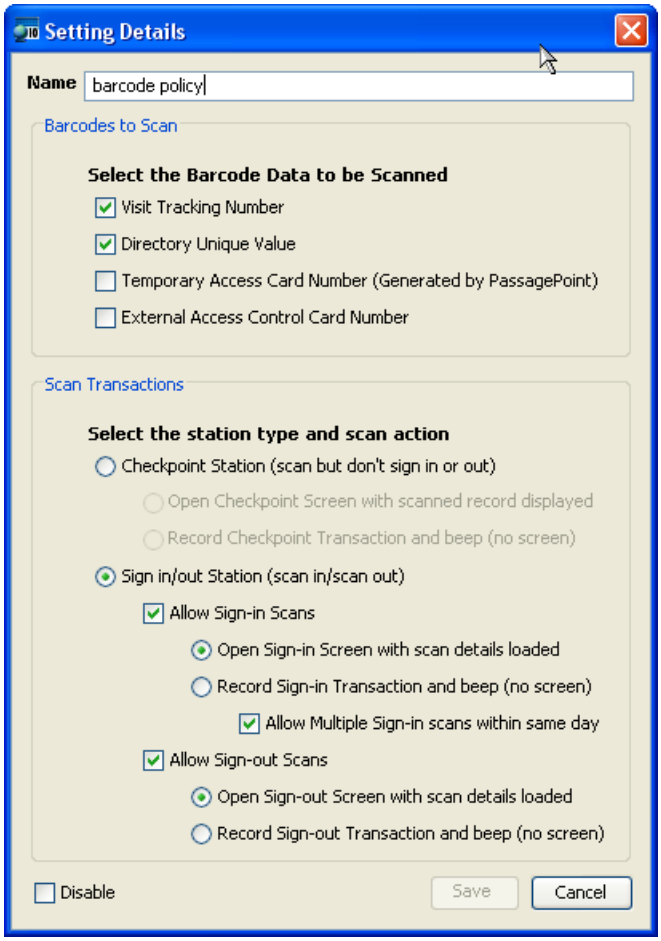
When creating a policy, you can define a Category group that the screen policy applies to. To create a Category group, click the "New" button in the Category panel in the Screen Policy Editor. Select the category of people that you want this policy to be applied to. Any categories not selected in a Category Group will remain in the Default Category Group. To apply the setting to all categories, use the Default Category Group without creating any new groups. At runtime when a user selects a category for the visitor, the screen will be modified automatically if their user login has a User Role that has a policy.

After making screen policy edits, save your changes by closing the editor with the "X" windows icon. On the policy screen, make sure that the policy is given a name. In the Apply To panel, choose the User Roles that this policy applies to. At runtime, user logins which use these User Role will see modified screens.

Barcode Scan Policy

Barcodes can be used to quickly sign in/out and Checkpoint a person. A Barcode Scan Policy defines what data the barcode is to be matched against. Also, it specifies how a barcode is to be treated when scanned depending on the station type.

Figure 34 – Barcode Scan Policy



Configuring Barcode Policy

Barcode to Scan

Specify the data that the barcode represents. Barcodes will be search against all of the data types which are checked.

- Visitor Tracking Number – a number that represent each unique visit
- Directory Unique Value – Unique ID number that is specified for each directory person
- Temporary Access Control Number – a unique number generated by PassagePoint that is also being activated against the Access Control System

- Extended Access Control Number – an Access Control card number

Scan Transactions

Specify whether the configuration will be used by a Checkpoint station or a Sign In/Out station. A scan can either display the full visitor record that is found or process the scan with no screen interaction. For sign-in transactions, you can specify if people are allowed multiple visits in a single day. Multiple sign-ins allow people to sign back in after having signed out.

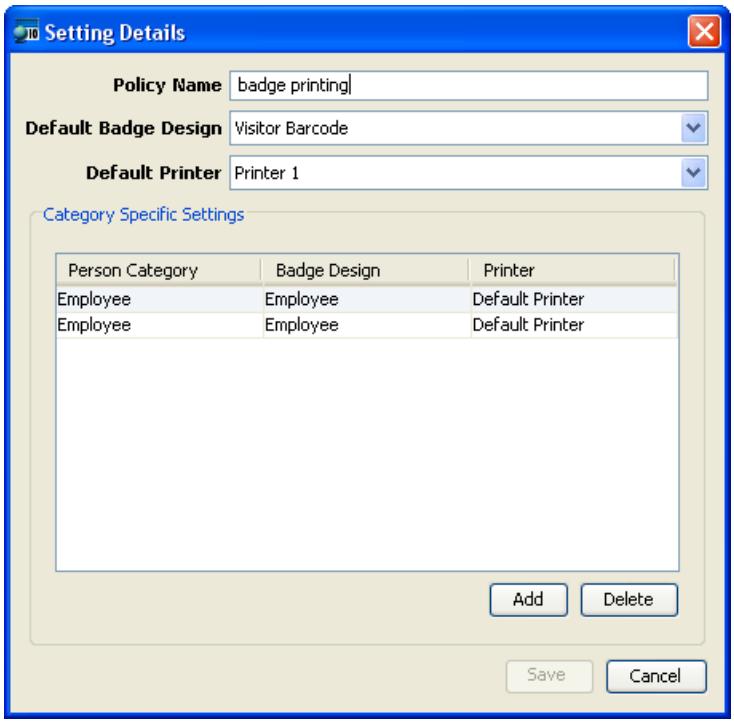
BADGE PRINTING POLICY

Badge designs and printers can be associated to a category of people through Badge Printing Policy. When a visitor category is selected on the Visitor Center screen, the badge design selector is automatically updated with the design specified in Badge Printing Policy. If multiple printers have been added to PassagePoint, the specified printer for the selected category will used to print the badge.

Configuring Printing Policy

The Default Badge Design and Default Printer fields specify which design and printer to use if a category has not been specifically defined. In the "Catgory Specific Settings", click "Add" and choose the category which you want a design or printer associated against. Select the associated badge design and/or printer for this category. Selecting default from the list will use the design or printer that was specified above.

Figure 35 – Badge Printing Policy



SIGN-IN KIOSK PROFILES

A Sign-in Kiosk is a self-help sign-in stations that can be used in a lobby with heavy traffic or and unattended lobby. A kiosk allows a user to sign-in with successive screens that ask user to enter data about themselves. Additionally, kiosks have support for taking a photo, watching an orientation video, signing an agreement, and using ID scanners to capture visitor information. The Sign-In Kiosk Profile specifies the screens displayed and the order which they appear.

Configuring Kiosk Profiles

When configuring kiosk, specify the kiosk user account that will be used to startup the kiosk. Only user accounts with a Kiosk Role assigned will be listed in Linked User Accounts dropdown. The account specified when logging into PassagePoint Client will determine which Kiosk policy is loaded.

Category – Specify to show all categories on the kiosk or select categories. To only see specified categories, choose Specific Categories and check the Display boxes of each category you want displayed.

Screen Policy – As with PassagePoint Client Screen Policy, screens for the Kiosk can be modified to suite your specific implementation. Settings are based on category of people. Fields on the screen can be made to be visible/hidden or required/not required, graphics can be substituted, policies can be set through variable settings. For more details on capabilities of Screen Policy, refer to Chapter 8.

To set Screen Policy for a screen, click the Screen Policy dropdown, navigate down the screen listing, and select the screen you want to edit. Click "Edit" to launch the Screen Policy Editor. To save your settings, click the "Save" icon on the Setting Details toolbar. If you want to reset the screen the installed default, click the "Reset to Default" button on the toolbar. Clicking the "X" in the upper right corner will close the window and return you to the Kiosk configuration screen.

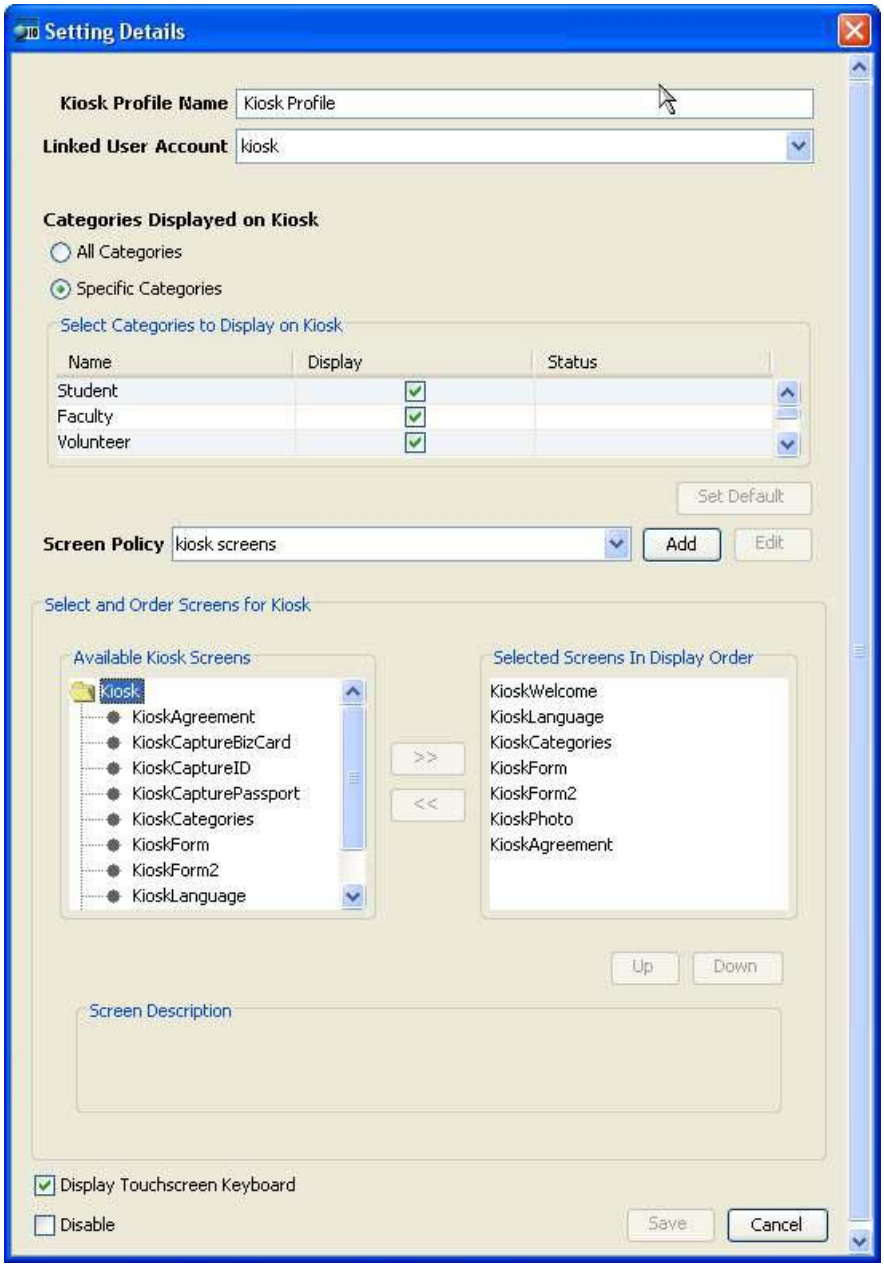
Select and Order Screens – The available Kiosk screens are listed on the left panel. Select the screen that you would like to include on the kiosk and click the ">>" button to add that screen to your set of screens. To remove the screen from your order, highlight the screen on the right panel and click the "<<" button.

Screen may be ordered by selecting the screen you want moved and clicking the "Up" and "Down" buttons. The list order will be the order in which screens will sequentially appear on the Sign-in Kiosk.

Display On Screen Keyboard – For Kiosk systems equipped with a touch screen, you can add an on-screen keyboard to the data entry screens. Having "Display On Screen Keyboard" check will display the keyboard on the kiosk screens.

The On Screen Keyboard can also be used without a touch screen by using a mouse to click each letter on the screen.

Figure 36 – Sign-in Kiosk Profile

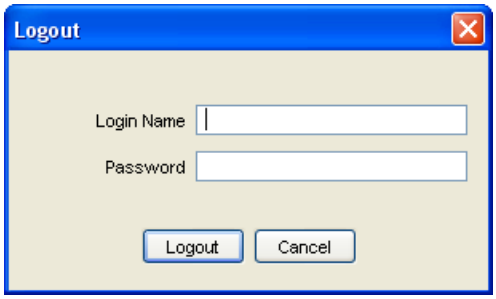


Running Sign-in Kiosk

To startup the Sign-in Kiosk, launch PassagePoint Client and log in as the kiosk user that was specified in the Sign-in Kiosk Policy. Kiosk mode is activated based on the User Account Role of Kiosk. The default User Account "kiosk" with no password will load the kiosk policy and screens.

To exit out of Kiosk mode, use a physical keyboard to type Alt-F4. This key combination will open a user-password dialog window. Enter any valid PassagePoint User Account login name and password to exit.

Figure 37 – Exit Kiosk



Chapter 9 – Web Module

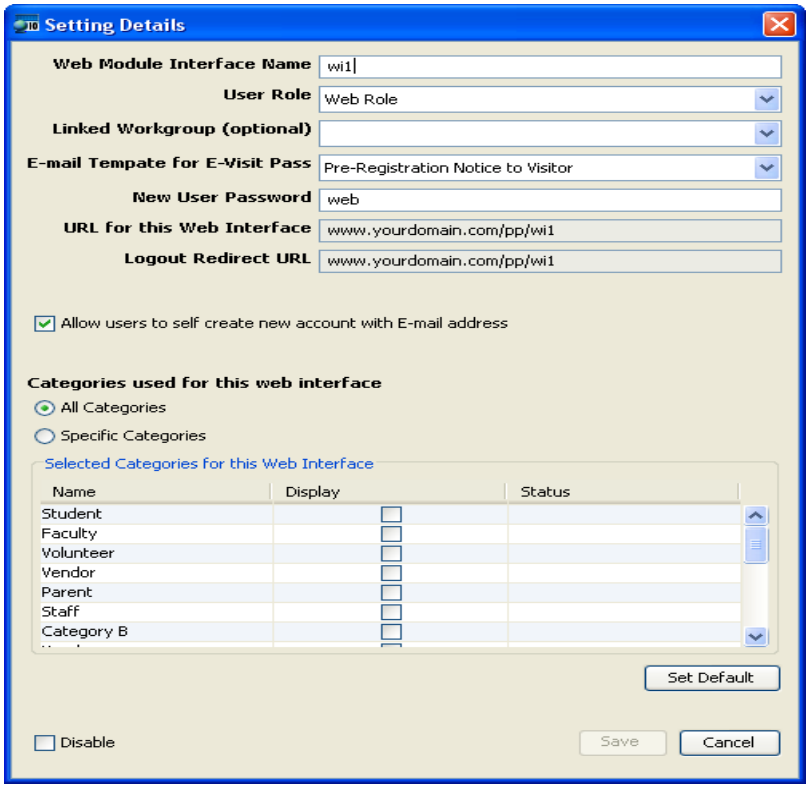
The Web Interface Module allows users to pre-register visitors using a web browser. Users will be able to enter information about upcoming visits for both visits they will host or create pre-registrations hosted by others. This module requires that a Web Module License be installed before it can be accessed from a browser. Web user login do not count against Client Licenses.

Currently, only one Web Pre-Registration interface is supported. If multiple definitions are created, only the default setting will be active.

Configuring a Web Module Interface

From the Configure System screen, choose Web Module Interfaces under the Web Module header. To configure a Web Module, select the "wi1" web interface from the table of interfaces and click the "Edit" button.

Figure 38 – Configure Web Module



On the Setting Details screen for Web Module Interface, specify the name of the module interface. This name will determine the URL that users will need to access the Web Pre-Registration site.

User Role – This indicates which role will be used for new user accounts using this interface.

Linked Workgroup – The user accounts which are created from the Web Pre-Registration site will be assigned to the Workgroup specified here.

E-mail Template for E-Visit Pass – When a pre-registration visit is saved, each visitor can be sent an E-mail notifying them of the upcoming visit. The E-Visit Pass E-mail can contain information such as who they will be seeing, location, directions and a Visit Tracking Barcode. The E-Visit Pass E-mail template can be created under E-mail templates and specified here.

If you have PassagePoint Control Center enabled to manage multiple sites, the E-Visit Pass template used for the E-mail will depend on the Destination that is selected for the visit. The first E-mail template

that is found looking up the Location Tree starting from the Destination will be the template that will be used. This enable you to customize the E-mail for each location based on Destination. If an E-mail Template is not found in the Destination path, then the default E-Visit Pass Template that is specified in the Web Module Interface will be used.

New User Password – This password is used when users self-create their accounts using the Web Pre-Registration site. You will need to give this password to your users who you would like to be able to create their own web access accounts.

URL for Web Interface and Logout Redirect URL – These are only informative strings that specify the http link for the Web Pre-Registration web site.

Allow Users to Self Create New Accounts – By checking this box, you are enabling the feature for users to create their own accounts. Users will need to provide the New User Password, their first and last names, and their E-mail address. The User Account they specify will be their user login name. If all of these fields match their record within the local Directory or in Directory Link, they will receive an E-mail giving them their new account login password.

Figure 39 – Create New Web User Account

Categories for Web Interface – Specify either all categories or select categories to display on Web Pre-Registration entry screen.

Accessing Web Pre-Registration with a Browser

User will use their web browser to access the Web Pre-Registration site. Use either of the following links to access the default "wi1" web interface:

- http://ppserver.yourdomain.com:2080/pp/wi1
- http://<ip_address>:2080/pp/wi1

The Welcome screen for Web PreRegistration site will display which users can either sign-in with an exisiting Web User Account or create a new account. Creating new accounts requires that the user be already defined in the local Directory or found via Directory Link. Users will need to know the New User Password for the Web Interface.

If users from outside of your domain need access to the Web Pre-Registration site, you can create a tunnel in your firewall that points to the PassagePoint Server via ports 2080 and 2443. Consult with your Information Services team to best handle this within your network infrastructure.

Single Sign-On with IIS

Key Benefits

1. Security – Managed by Windows security
2. Authentication – Possible to use Active Directory to authenticate users through IIS through Single-Sign on and pass this information to PassagePoint

File STOPware Distributes

1. default.htm – Proxy file which calls redirect. Proxies browser to /bin/isapi_redirect.dll
2. isapi_redirect.dll – IIS ISAPI Redirector library
3. isapi_redirect.properties – Configuration file for IIS Redirector.
4. workers.properties – Configuration file for host address for PassagePoint Server, port number of PassagePoint web server, etc.
5. uriworkermap.properties – Configuration file for Web Pre-Registration module address.

Configuring Single Sign-On

PassagePoint Settings

No configuration on the PassagePoint side is necessary. By default, PassagePoint's web server Tomcat, runs on port 2080.

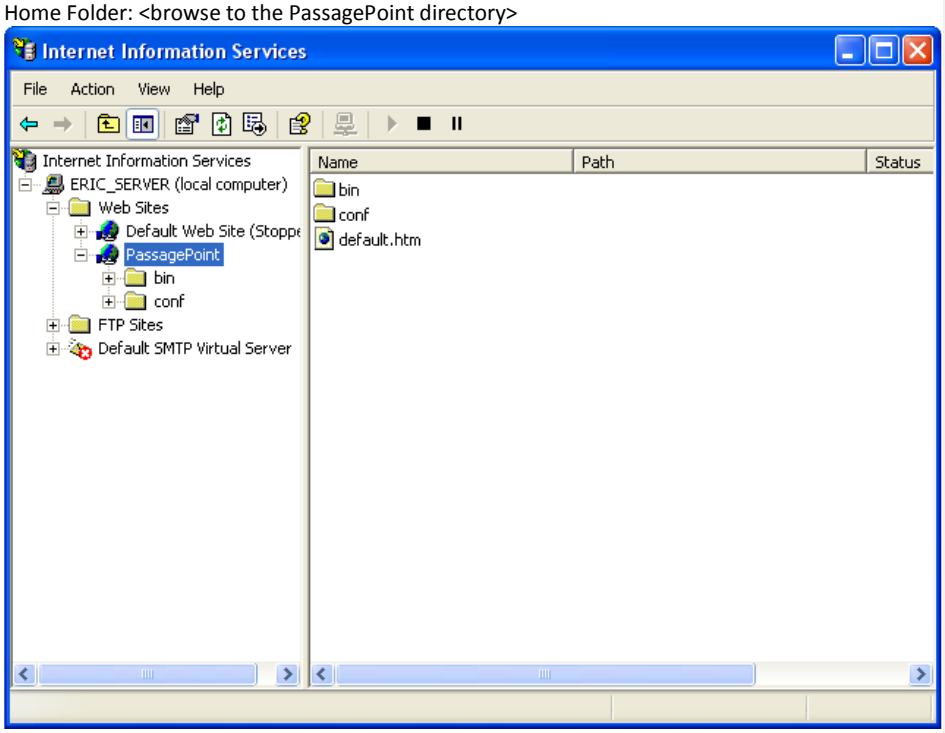
IIS Settings

1. Create PassagePoint directory under C:\Inetpub, with the following directory structure and files:

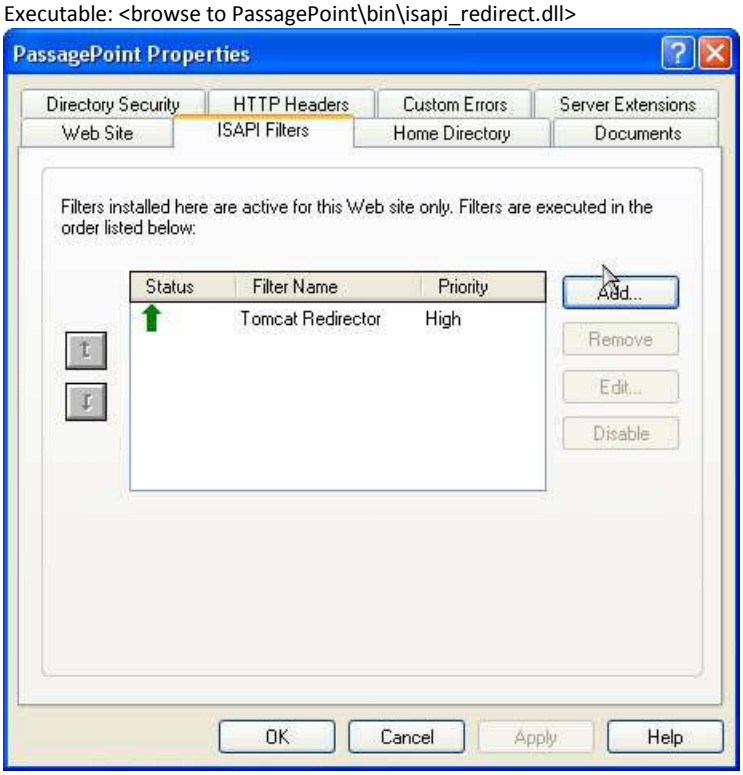
   PassagePoint
   default.htm

bin (folder)
isapi_redirect.dll
isapi_redirect.properties
conf (folder)
workers.properties
uriworkermap.properties

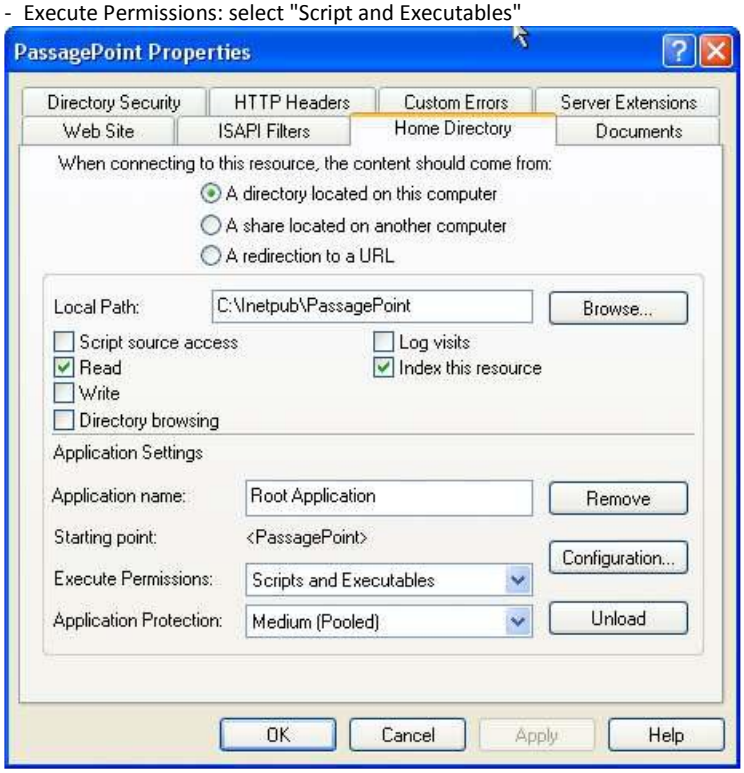
2. Create a new website in IIS named PassagePoint.
   Host Name: localhost
   Description: PassagePoint
   Home Folder: <browse to the PassagePoint directory>



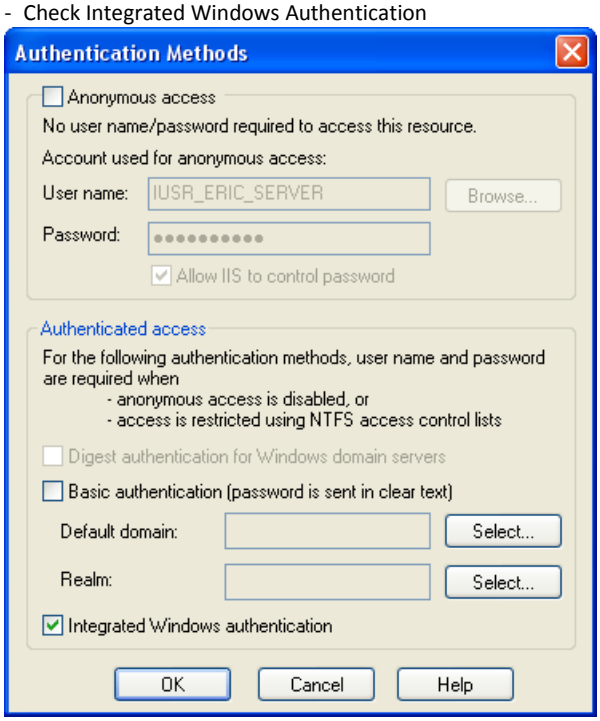
3. Right-click PassagePoint web site and do "Properties" and click on "Home Directory" Tab
   The Execute permissions should be set to Scripts and Executables. (This allows the isapi_redirect.dll to work properly)
   a. ISAPI Filters tab and add:
      Filter Name: Tomcat Redirector
      Executable: <browse to PassagePoint\bin\isapi_redirect.dll>



b. Home Directory tab:
   - Uncheck Directory browsing
   - Execute Permissions: select "Script and Executables"



c. Directory Security tab
Edit Anonymous access and authentication control
- Uncheck Anonymous access. IIS is not used for authentication and is used for rerouting request to PassagePoint. PassagePoint would do the authentication. In this setup, you would have to set up users/passwords in PassagePoint.
- Check Integrated Windows Authentication



Configuration of PassagePoint\conf\workers.properties file

If the PassagePoint Server is runs on a system other than the IIS server, you need to assign the server to *worker.ajp13.host* property in PassagePoint\conf\workers.properties file. Replace 'localhost' with the hostname or IP address of the machine PassagePoint Server resides on.

Leave everything else at its defaults and save the file.

Sample File

```
# workers.properties
#
# This file provides jk derived plugins with with the needed
# information to connect to the different tomcat workers.
```

```
#
# You should configure your environment slash... ps=\ on NT and / on UNIX
# and maybe something different elsewhere.
#
ps=\

#------ ADVANCED MODE ----------------------------------------------
#
#------ DEFAULT worket list ----------------------------------------
# The workers that your plugins should create and work with
#
worker.list=ajp13

#------ DEFAULT ajp13 WORKER DEFINITION ----------------------------
# Defining a worker named ajp13 and of type ajp13
# Note that the name and the type do not have to match.
#
worker.ajp13.host=localhost
worker.ajp13.port=8009
worker.ajp13.type=ajp13

# Specifies the load balance factor when used with
# a load balancing worker.
# Note:
#  ----> lbfactor must be > 0
#  ----> Low lbfactor means less work done by the worker.
worker.ajp13.lbfactor=1

# Specify the size of the open connection cache.
#worker.ajp13.cachesize

#------ DEFAULT LOAD BALANCER WORKER DEFINITION ----------------------
# The loadbalancer (type lb) workers perform wighted round-robin
# load balancing with sticky sessions.
# Note:
#  ----> If a worker dies, the load balancer will check its state
#       once in a while. Until then all work is redirected to peer
#       workers.
worker.loadbalancer.type=lb
worker.loadbalancer.balanced_workers=ajp13
```

Restart IIS and You are Done!

To test, you will enter in the IP or hostname of the IIS machine. For example:

http://iis_server/

Windows user name will be matched against PassagePoint's Directory People Unique ID. These people can be either saved locally in PassagePoint Directory or accessible via Directory Link (LDAP or ODBC/JDBC).

Chapter 10 – Control Center

The Control Center is a hierarchical representation of your organization's locations. It is an advanced security feature that will allow an administrator to tailor the visibility of data and Custom settings can be placed into locations within the tree that affect the visibility of data and the access to secure data. For instance, a receptionist of one campus may only be allowed to view data for their local campus, while another receptionist in a remote campus may be allowed to view data for all locations. Allocation Tree allows for diverse settings as such.

If your facility has multiple buildings or sites, Control Center can help manage logistics with the ability to isolate and view only information that is pertinent to each specific location. With a centralized tool, you can configure special policies and settings to be applied for each location; designate users to only login at certain stations; create custom screens specific to a site; and design badges and print policies for specific locations. A single logical site map lets you conveniently track destination and locations for easy operation.

Enabling Control Center

To access the Control Center, open *Home| Configure System | Control Center*. The first time that you try to access the Control Center, you will see the following message:

> *This option enables the Control Center option which allows you to place settings into different location in a virtual tree. The tree represents the physical locations of where you use the PassagePoint Client application.*

Click "Enable Control Center" to active the tree. The Allocation Editor is divided into two panels. The top panel manages the location hierarchy, while the lower panel is settings and resources that are assigned to the selected location.

Disabling Control Center

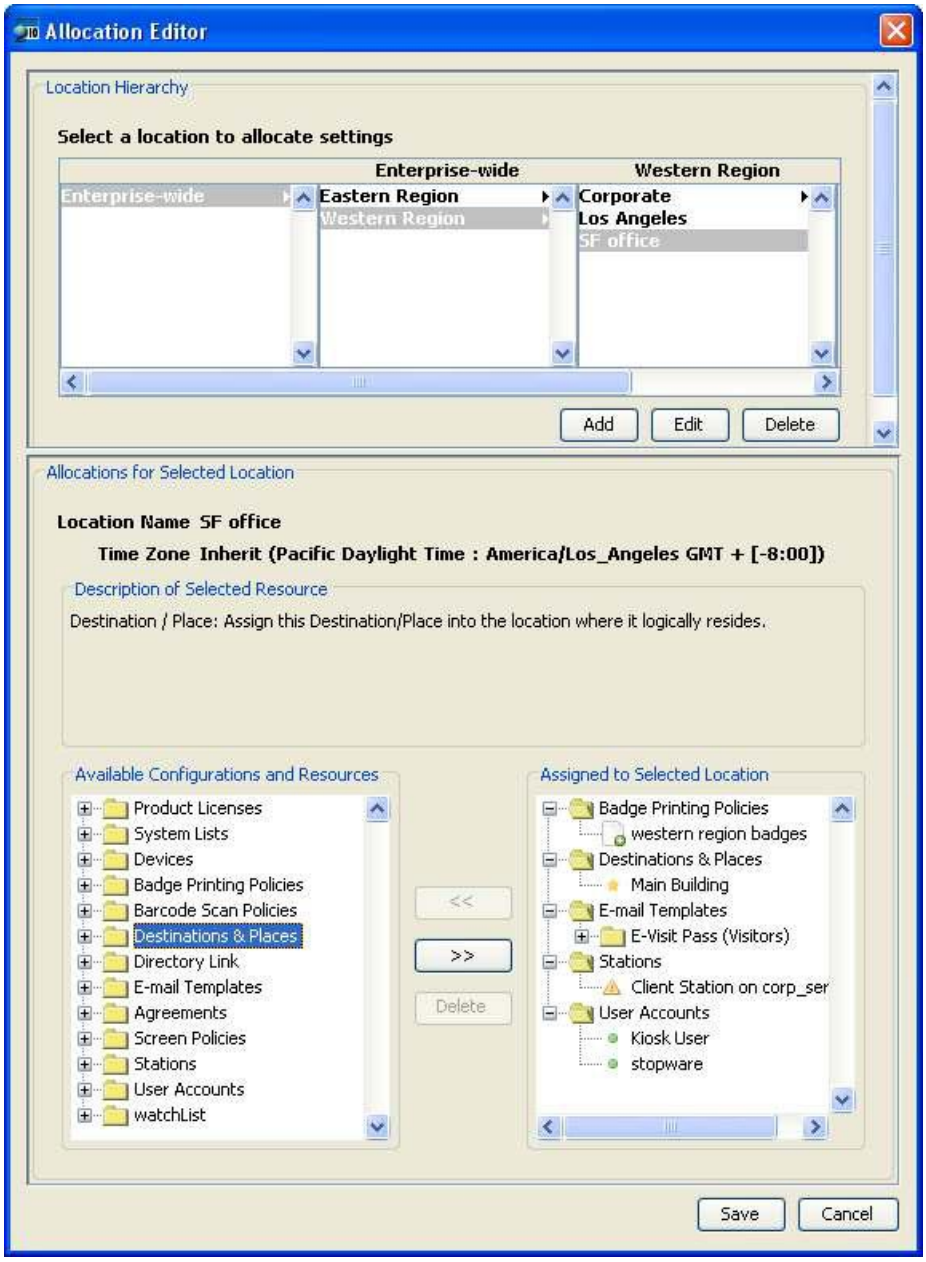
After the Control Center has been activated, disabling the tree means that all settings which were assigned to locations will no longer be in effect. The system will use settings that have been designated as default. For instance, if you have multiple lists of Arrival Instructions, the list that you have set as default will be the Arrival Instructions that will appear in Instruction dropdowns.

A disabled tree can be re-enabled by clicking "Enable Control Center".

Allocation Editor

To add a location and assign custom settings, click the "Edit Locations & Allocations" button on the main Control Center configuration tree to bring up the Allocation Editor. As with the main screen, the editor is sectioned into a mange locations panel and an assign resources panel. The bottom panel is used to assign resources to the location selected in the top panel.

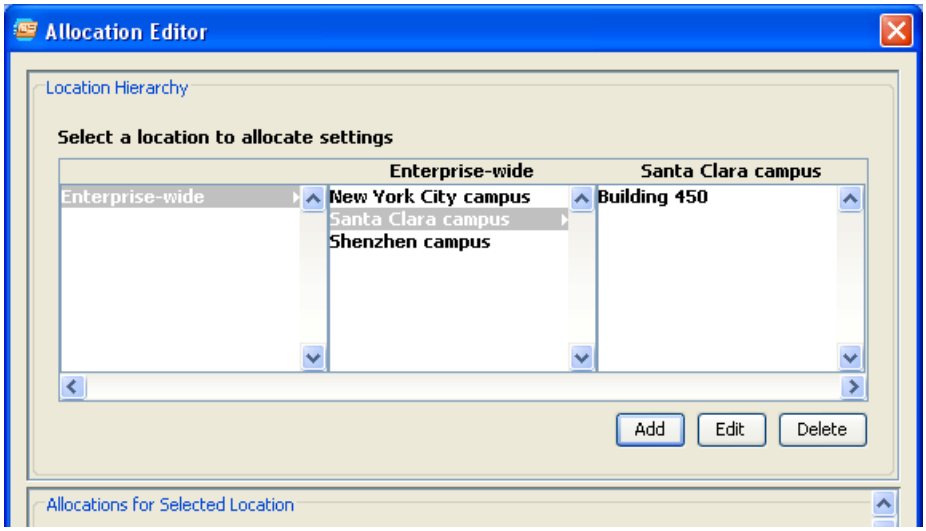
Figure 40 - Allocation Editor



Managing Locations in Location Hierarchy

Locations are created from the Location Hierarchy panel in the Allocation Editor screen. The location hierarchy is sometimes referred to an Allocation Tree. We recommend that you group your physical locations into logical groupings. For example, an enterprise at the top level may have groupings below it such as campus sites. Within each campus location grouping would be sub-categories, such as buildings. Buildings can then be subdivided according to their own grouping, such as lobbies or departments within a campus. These groupings can be represented in the tree structure within Control Center's Allocation Tree. Sublevels are graphically represented with an arrowhead symbol next to a location name.

Figure 41 - Location Hierarchy



Enterprise-wide is a special location which cannot be deleted. It is the top-most location is the Control Center's Allocation Tree. In a hierarchical structure, this is usually referred to as the root of the tree. There can only be one top-most location. To rename Enterprise-wide or specify a default time zone for the enterprise, select it and click "Edit".

To add a location to the Allocation Tree, select the location grouping for the item you would like added and click "Add". For example, to add "Santa Clara Campus" as a location under Enterprise-wide, select Enterprise-wide. Clicking "Add" will open a configuration screen that lets you specify the name of the location and a time zone for this location. Selecting a time zone is important if you are dealing with locations in different time zones as transaction will be displayed in their local time.

To edit a location, select the location and click "Edit". Similarly, delete a location by selecting it and clicking "Delete".

Assigning Configurations to Locations

From within the Allocation Editor, you can assign resources and configurations to a selected location. The process to assign a configuration to a location is accomplished by following these steps:

- Select the location from the Location Hierarchy
- Select a configuration from the list of Available Configurations and Resources
- Click ">>" to assign the selected configuration to this location

The "Allocations for Selected Location" panel shows two panes. The left pane shows the configurations and resources that are available to be assigned to this location. The right pane shows those that have been assigned to this location.

To assign a setting or resource, select the item from the Available Configurations pane and click the ">>" button. Most configurations can be reused in multiple locations. In some cases when a resource of setting is only assignable to one location, a warning message will appear and the configuration will move automatically from its assigned location in the tree to this new location.

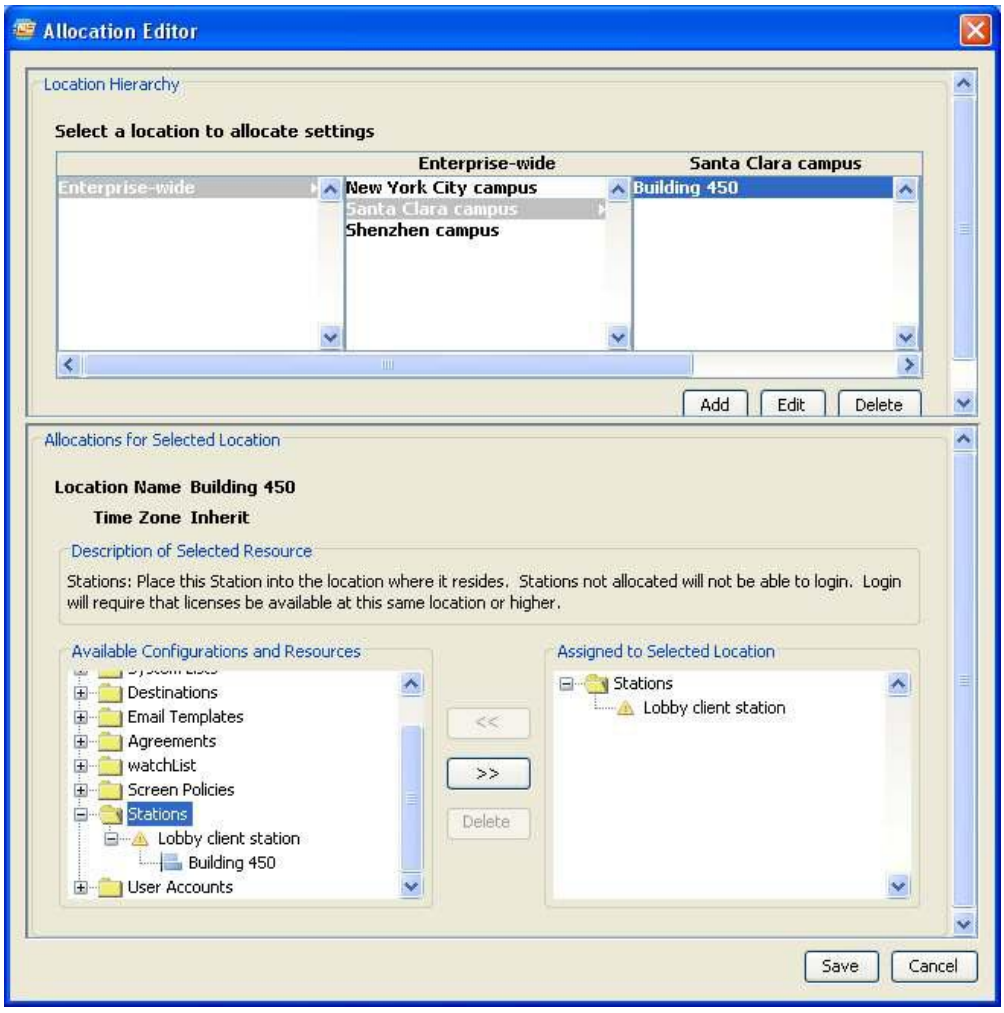
To unassign a configuration from this location, select the configuration and click the "<<" button to move the configuration back into the Available Configurations list.

Assigning Stations

Note:	*If Control Center is activated, Stations must be placed in the tree for allocated settings and resources to be applied properly.*

Settings and resources are accessible based on Station locations. When a setting or resource is needed at run-time, it looks for the settings and/or resources up the tree from where the Client Station resides. The exception to this is Destinations, where the list of destination locations is obtained based on station location on down the tree.

Figure 42 - Assigning Stations to Location



Assigning Product Licenses

Client Stations will be allowed to log into the PassagePoint Server if an available client license is found in that station's location tree path. When a Client Station logs in, it looks for a license starting at its Station location on up the tree to find an available license. Client licenses are based on concurrent usage.

Assigning User Accounts

A user can log into PassagePoint only if the Client Station is at the same location as his/her User Account or below. Users are not allowed to log into stations above their location in the tree. Power users should be placed higher up in the tree. Accounts place lower in the tree will have more limited login capabilities than those placed higher.

Assigning System Lists

Lists typically are used in dropdowns on entry screens. At run-time, user will see the first List that is found starting at the Stations location in the tree on upward. This is helpful to limit the number of items in a dropdown list that a user will need to choose from.

Assigning Destinations

Destinations should be assigned to their logical location in the Allocation Tree. A user will be able to see destinations which are based on their Station location in the tree on downward.

Index