



# Administration Manual



Contents

**Introduction..... 3**

**Overview ..... 3**

Administration User Interface .....3

    Managing Print Agents.....4

    Managing Search Indexers.....4

    Managing Email Services .....4

    Managing Data Integration Agents.....4

Browser Validation.....5

License Management .....5

Configuration Properties.....6

Deployment Properties.....7

Languages.....7



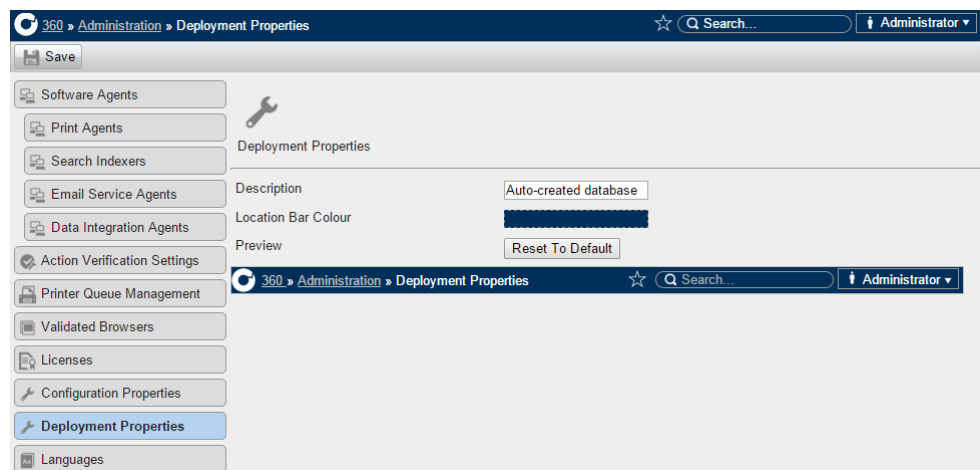
## Introduction

PID provides extensive support for user and password administration, group management and security tags. User name and password policies can be configured to align with organizational requirements or integrated with LDAP or Active Directory for user and group management.

## Overview

### Administration User Interface

Key Administrative functions are performed from the Administration UI (below)  
From the **Home page** select **Administration** to open the **Administration Screen**



Administration Screen showing Deployment Properties

The **Administration** menu (left) allows day to day administration to be performed.

The following functions can be managed:

1. *Software Agent Management*
2. *Action Verification Management*
3. *Printer Queue Management*
4. *Browser Validation Management*
5. *License Management*
6. *Configuration Properties*
7. *Deployment Properties (highlighted)*
8. *Languages*



## **1. Software Agent Management**

### **Managing Print Agents**

Print Agents are locally installed software applications that manage printing at a local site.

### **Managing Search Indexers**

Search Indexers are required to support the general search facility.

### **Managing Email Services**

Email Services are required to manage the notification of users via email.

### **Managing Data Integration Agents**

Data Integration Agents may be required to process and transfer data to or from PID.

## **2. Action Verification Management**

PID prompts users to verify their identity and to provide a reason and/or comment for certain audited actions.

## **3. Printer Queue Management**

PID allows the use of Print Agents. Print Agents are locally installed software applications that manage printing at a local site.

## **4. Browser Validation Management**

PID supports restrictions on which browsers can access the application. This capability may be disabled via a system configuration if there are no regulatory compliance requirements.

## **5. License Management**

PID includes the ability to limit features and modules via the application of licenses.

## **6. Configuration Properties**

Configuration Properties allow the changing or addition of a function.

## **7. Deployment Properties**

Deployment Properties allow a system administrator to change the description of the deployed server.

## **8. Languages**

Language management allows the definition or removal of a set of languages and/or cultural variations.



## Browser Validation

To view validated browsers do the following:

1. From the **Administration screen** select **Validated Browsers**.

The screen displays the relevant capabilities of the detected browser, the list of validated browsers, and options to allow management of the browsers.

The screenshot shows the 'Validated Browsers' screen. The sidebar on the left contains the following options: Software Agents, Print Agents, Search Indexers, Email Service Agents, Data Integration Agents, Action Verification Settings, Printer Queue Management, **Validated Browsers** (selected), Licenses, and Configuration Properties. The main area displays two tables. The 'Validated Browsers' table has columns: Name, Version, Platform, Cookies, and Canvas. It lists three entries for Chrome with versions 39.0.71, 38.0.111, and 28.0.95, all on Windows 7 / Server 2008 R2 (64-bit), with both Cookies and Canvas checked. A 'Delete' button is below this table. The 'Current Browser' table has the same columns and lists one entry for Chrome version 39.0.71 on Windows 7 / Server 2008 R2 (64-bit), with both Cookies and Canvas checked. Below this table are three buttons: 'Exit and Log off', 'Validate Permanently', and 'Validate for this Session'.

### Browser Validation

2. Select **Validate for this Session** to temporarily validate the browser for this session only.
3. Select **Validate Permanently** to allow unrestricted validation for this browser

Any decisions made on this page by users are recorded within the Audit Log.

The application compares the details provided by the User Agent String to the list of validated browsers. If the browser is validated, the user is passed to their normal home page within the site.

If the browser is not on the validated list, the system checks the permissions of the logged in user. If the user has appropriate permission they are directed to validate the browser.

## License Management

PID includes the ability to limit features and modules through the application of licenses.

A new installation of the PID system is initially unlicensed.

An unlicensed **PID** system only allows the Administrator to log in and only for one active session. The session timeout duration for unlicensed sessions is 3 minutes. The system must be adequately licensed before being used.

From the License Management page an Authenticated User can add and remove **PID** Software Licenses.

Licensing Instructions are displayed and License files can be uploaded or the corresponding license text pasted.



**PID** uses a License Chain model where:

- Each added license (except the initial one) is linked (or chained) to the previous one
- Multiple licenses can be added to the system in a very specific order (defined by the way they are linked)
- Any license can be removed from the system in reverse order (last from the current chain)
- Each license has a start date and certain types of licenses may also have an end date (these time limits can be referred to as the licensed period)
- Only the latest license where the current date/time is in the licensed period is the active one
- A License where the licensed period is in the future can be added to the system and automatically becomes active when the current time falls within the licensed period

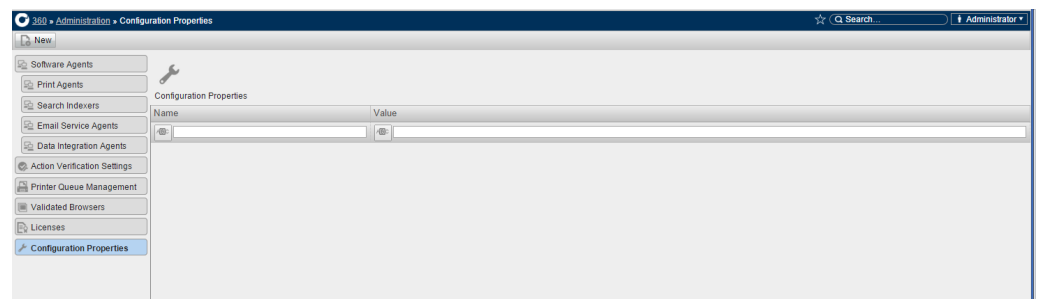
It is recommended that only the built-in Administrator user adds or removes licenses from the system.

When all licenses are removed from the system, all user sessions are terminated and all users logged out. After this, only the built-in Administrator user is able to log in.

## Configuration Properties

**PID** supports the creation of Configuration Properties required to store and manage system wide configuration settings. Access to this area is controlled by the System Level Permission, Manage **Configuration Properties**.

**Configuration Properties** allow the changing or addition of a function. The name of the property and the actions it performs are already defined within **PID**.



Configuration Properties

From the **Configuration Properties** page, the following can be set:

- *CleanupTransientEntitiesDays* – Specifies the number of days an Approval Request or Change Request has been completed before it is



made unavailable. If no value is specified, then a default of 30 days is used.

## Deployment Properties

**PID** allows a system administrator to change the description of the deployed server.

Click in the *Description* field to enter the new description.

To change the Location Bar color:

1. Click on the color box to display a color picker
2. Select the desired color
3. A preview is displayed. Location Bar text and link colors are set automatically based on the location bar color
4. Click Save

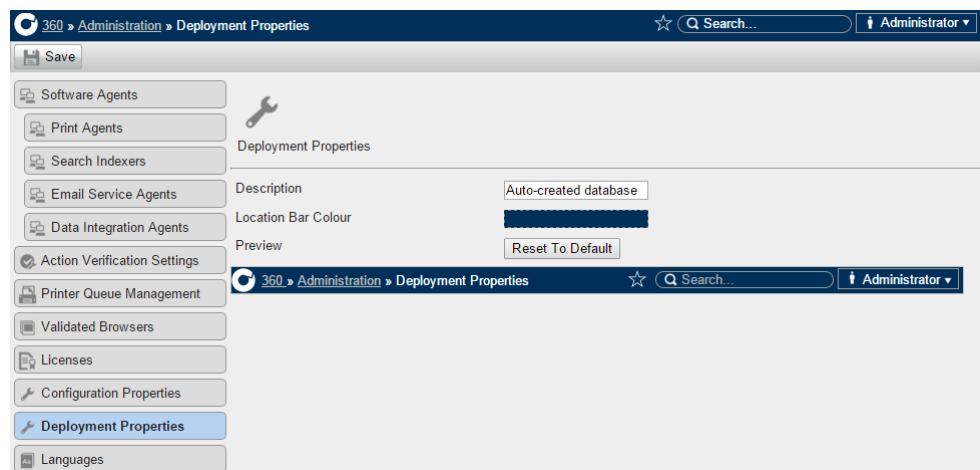


Figure 1 - Deployment Properties

## Languages

### Defining Languages

To define a set of languages and/or cultural variations of a language use **Language Administration**.

1. From the **Administration** page, Select **Languages** to open the *Language Page*.
2. Select which languages are available when new Phrase Tables are created within the Entity Store.
3. Select any or all variants of a language.
4. To restrict each language to a single regional variant, only select the required variant.

It is not possible to save changes that contradict this selection.



Selection of Languages does not impact the operation of **Dictionaries** and **Translations** in any way.

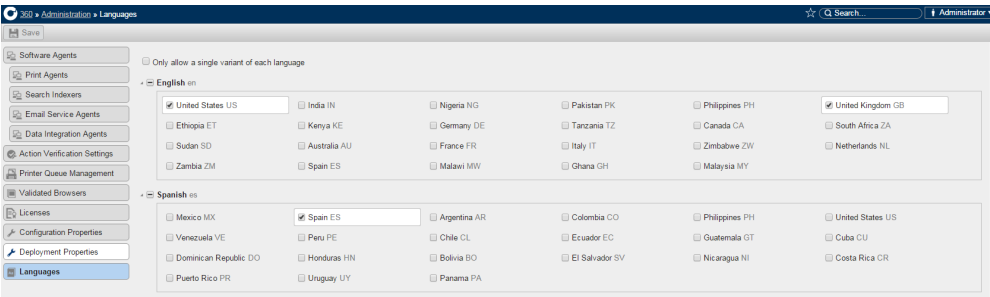
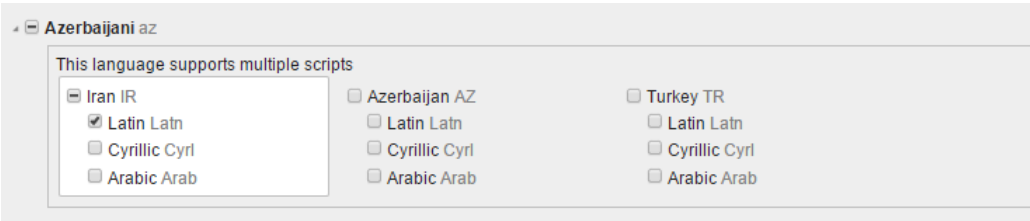


Figure 2 - Language Administration

Setting Regional Variations

Regional variations of a language are implemented using the RFC 564RFC6/BCP47 (ISO639 & ISO3166-1) region name (e.g. en-GB, en-US, en-AU).

- 1. Select from a list of scripts for **Languages** which support alternate scripts as well as regional variations. See Multiple Scripts.



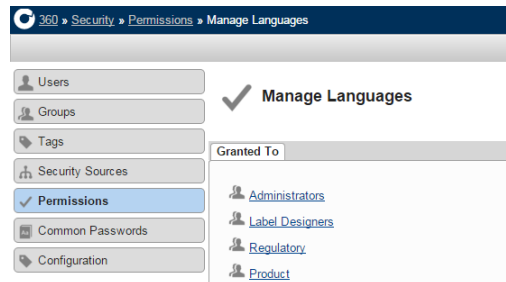
Multiple Scripts





## Controlling Access to Languages

Access to the *Languages* page is controlled by the **Manage Languages** permission.



Manage Languages Permission

## Security Groups

Selecting a specific language from the *Administration > Languages* page causes a **Security Group** for that language to be created. This is named using the convention "Language Specialists [Country and Language Code]".

A Security Group called "*All Language Specialists*" is also created to support Language Specific Voting activities.

## Granting Membership

Membership of a Group is granted by assigning the user to a **Specific Language Specialist Group**.

The user can add or remove supported Languages.

NOTE: Phrase Tables are unaffected by removal or addition.