

ADMINISTRATOR'S GUIDE

Perspective by PPM[™]

Version 4.0

Printed October 2013

Copyright © 2013 PPM 2000 Inc. and its licensors. All rights reserved.

PPM 2000, the PPM 2000 logo, Perspective by PPM 2000, the Perspective by PPM 2000 logo, Perspective by PPM, the Perspective by PPM logo, Perspective Focal Point, and the Incident management from every angle logo are trademarks or registered trademarks of PPM 2000 Inc.

Information in this document is subject to change without notice.

Companies, names, and data used in the examples herein are fictitious unless otherwise noted.

Although every precaution has been taken in preparation of this document, PPM 2000 Inc. assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Permission to modify and distribute this document strictly for the purpose of internal user training is hereby granted, provided that it is made evident the document has been modified, and that all copies contain all proprietary notices set forth in or on the original version. PPM 2000 Inc. assumes no responsibility for errors or omissions resulting from the modification of this document. PPM 2000 Inc. expressly waives all liability assumed for damages resulting from the modification of the information contained herein. Notwithstanding the permission granted herein, no part of this document may otherwise be reproduced, transmitted, disseminated or distributed, in any form or by any means, electronic or mechanical, for any other purpose, without the express written permission of PPM 2000 Inc.

Adobe, the Adobe logo, Acrobat, and Reader are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and other countries.

Apple, the Apple logo, iPad, iPhone, iPod, iPod touch, and iTunes are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc.

BlackBerry, SureType, SurePress, and related trademarks, names, and logos are the property of Blackberry Limited and are registered and/or used in the U.S. and countries around the world.

Brivo ACS WebService is a registered trademark of Brivo Systems LLC.

dtSearch is a registered trademark of dtSearch Corp.

Google, Google Chrome, and Android are trademarks or registered trademarks of Google Inc.

i2, the i2 logo, and i2 Analyst's Notebook are registered trademarks of IBM Corporation.

Identity Resolution Engine (IRE) is a trademark of Infoglide Software Corporation.

IDV Solutions and Visual Command Center are trademarks or registered trademarks of IDV Solutions, LLC.

Lenel, the Lenel logo, OnGuard, and the Lenel OpenAccess Alliance Program (OAAP) are trademarks or registered trademarks of Lenel Systems International Inc.

Microsoft, Windows, Windows Vista, Windows Server, SQL Server, Access, Internet Explorer, Excel, PowerPoint, Outlook, Active Directory, Visual Studio, Visual Basic, the Office logo, .NET logo, and Microsoft Gold Independent Software Vendor (ISV) Partner logo are trademarks or registered trademarks of Microsoft Corporation in the U.S. and other countries.

MIR3 is a service mark of MIR3, Inc. inAccountPortal, inTechCenter, inAlertCenter, inEnterprise, and Intelligent Notification are trademarks or registered trademarks of MIR3, Inc.

Mozilla, the Mozilla logo, Firefox, and the Firefox logo are trademarks or registered trademarks of the Mozilla Foundation.

QlikTech, the QlikTech logo, and QlikView are trademarks of QlikTech International AB.

Samsung, Galaxy S, and Galaxy Note are trademarks of Samsung Electronics Co., Ltd.

Wi-Fi is a registered trademark of the Wi-Fi Alliance.

All other products, brands, names, or trademarks mentioned in this document may be trademarks or registered trademarks of their respective owners.

Contents

Welcome to Perspective by PPM 2000	5
Default Admin Master vs. Users with Administrator Rights	5
Logon Options	6
Help Options	7
Contents Tab: Browse Help by topic	7
Index Tab: Browse Help by Index	8
Search Tab: Search Help	8
Navigation Options	9
Security Layer Overview	10
System Administration Components	12
General Settings	15
Set the Basic System Settings	15
Assign Incident, Case, and Activity Number Formats and Prefixes	15
Choose the Default Measurement System for Numeric Data	15
Set your organization's logo and address to print on report cover pages	15
Select the Default Font for Narratives, Summaries, and Interviews	16
Set to Display Organization Privacy Statement or Legal Notice After Logon	16
Hide the All Records View Option on Data Forms and Pick Lists	16
Allow Users to Send Formatted Email Messages	16
Define User Password and Logon Parameters	17
Select Default Currency, Add New Currencies, and Update Exchange Rates	18
Workgroups	20
Add a New Workgroup	20
System Privileges	21
Assign System-Level Visibility and Access Rights	21
View Discrepancies Between System-Level Rights and Role or User Rights	23
Roles	24
Add a New Role	
Establish Default Security Controls, Language, and Currency for a Role	25
Select General Role Rights	
Specify Visibility and Access Privileges for a Role	
View Discrepancies Between Role Rights and User Rights	31

Set Report Visibility for a Role	
View Discrepancies Between Role and User Report Visibility	32
Users	33
Add a New User	
Establish Default Security Controls, Language, and Currency for a User	
Set General User Rights	
Specify Visibility and Access Privileges for a User	
Set Report Visibility for a User	40
Track All Changes Made to a User Account	41
Officers	42
Add a New Officer for Perspective Dispatching	42
License Management	43
Concurrent Licenses	43
Named Licenses	44
Auditing	46
View When, Where, and Who Accessed or Modified a Record	46
Lookups	48
Modify a Single-Tier Lookup List	48
Modify a Multi-Tier or Hierarchical Lookup List	49
Specify Workgroup Visibility for a Lookup List Value	51
Enter Call Codes for the Call Category Lookup List	52
Enter Address Information for the Site Lookup List	53
Activity Statuses and Officer Statuses	55
The Relationship Between Activity Statuses and Officer Statuses	55
System Values	55
Flags	57
Add a New Incident or Person Flag	57
Standard Operating Procedures	59
Create a New Standard Operating Procedure Rule for an Activity	59
Add a Checklist for the SOP	60
Attach a Relevant SOP File	61
Add a Relevant SOP Link	63
Set Up Individual and Mass Notifications for the SOP	64
Visual Alerts	

Define Visual Representation for Certain Data Types	65
Create a New Regulated Time to Act (RTA) Alert	67
Create a New Officer Alert	69
Language	71
Languages	71
Set Languages and Help File Paths	71
Form Labels	72
Create a Single Custom Label Set for All Users	72
Create a Custom Label Set for Each User Group in Your Organization	72
Create Custom Report Footers	72
Gateway Administration	74
Gateway Administration Specify Gateway File Import and/or e-Reporting Access Options for a Workgroup	
	74
Specify Gateway File Import and/or e-Reporting Access Options for a Workgroup	74 76
Specify Gateway File Import and/or e-Reporting Access Options for a Workgroup Assign Access Rights to a Gateway Administrator or Gateway Approver	74 76 78
Specify Gateway File Import and/or e-Reporting Access Options for a Workgroup Assign Access Rights to a Gateway Administrator or Gateway Approver Administrative Reports	74 76 78 79
Specify Gateway File Import and/or e-Reporting Access Options for a Workgroup Assign Access Rights to a Gateway Administrator or Gateway Approver Administrative Reports Service Manager	74 76 78 79 80
Specify Gateway File Import and/or e-Reporting Access Options for a Workgroup Assign Access Rights to a Gateway Administrator or Gateway Approver Administrative Reports Service Manager	74 76 78 79 80 84

Welcome to Perspective by PPM 2000

Welcome to Perspective by PPM 2000[™], the industry leader in Incident Reporting and Investigation Management software.

Perspective not only records and tracks incident data, but also assesses and analyzes it to chart trends and report statistics. With the recent incorporation of the centralized dispatching tool Perspective DispatchLog[™], Perspective now also offers an extensive range of dispatching capabilities.

Perspective is available in the following four editions:

- AIR: Activity & Incident Reporting Software
- **SOC**: Security Operations Center Software
- ICM: Investigation & Case Management Software
- EIM: Enterprise Incident Management Software

These four Perspective editions offer just the right level of functionality for your specific incident management needs. Throughout this guide, variances in feature and functionality between the four editions are specifically identified. All screenshots reflect the EIM edition of Perspective. Note that your Perspective system may not look identical to the sample system described in this guide; your system may be customized with field labels, lookup list options, and user defined fields that are unique to your organization.

This guide outlines the options and settings available in the **Administration** component of Perspective only, and is developed primarily for designated Perspective Administrators. For information about other components of Perspective, see *Perspective User's Guide*, *Perspective DispatchLog Guide*, and *Perspective Visual Analysis Guide*. For additional server-side configuration options, refer to the *Perspective Installation Guide*.

Note: Investigation Management is only available in the ICM and EIM editions of Perspective.

Default Admin Master vs. Users with Administrator Rights

There are differences between the default Admin Master account and a Perspective User with Administrator rights. Specifically, the Admin Master has select features available that other Users, even with Administrator rights, do not.

However, the default Admin Master **can only access the Administration** and **Dashboard panels of Perspective**. Other components are unavailable to the Admin Master.

Logon Options

- In order to access Perspective, navigate to your Perspective Services URL: http://<IISServer>/PerspectiveServices. <IISServer> refers to the Perspective Web server installed during the Perspective installation process.
- 2. Click the Launch Perspective button.

Perspective
Perspective Version 4.0
Launch Perspective
.Net Framework 4.0 needs to be installed to launch this application.
If you do not have the .NET Framework: <u>Click here to download .NET Framework 4.0 from Microsoft</u>

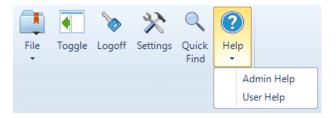
- 3. In the Logon window, click the small icon 🍄 in the top right corner to open the logon options.
- 4. Specify the service path by inputting a **Service URL**. Click the **Test** button to test the connection with the URL.
- 5. Select the appropriate database from the **Database** lookup list.
- 6. If required, switch from Windows[®] authentication to Perspective authentication by pressing the **F5** key (only available if Windows authentication is already being used).
- 7. Enter the **Business Unit** (only available if using Perspective SaaS).
- 8. Click **OK** to save the changes made and proceed with the standard login.



Help Options

Whether you are learning how to use Perspective or looking for information on a specific topic, Perspective Help will explain how to use program features, identify windows and fields, and answer common questions. Finding the specific information you are looking for is easy.

• To open one of the available Help files, click the Help icon *located* on the Action toolbar. Click on **User Help** to access general Help files. Select **Admin Help** to access Administrator-specific Help files.



- To navigate directly to the pages in the Help file that correspond to a specific keyword (e.g., Users), click **Search** in the top left corner, type in the keyword to look for and click **Go**. The Help file will list all topics relevant to your query.
- To navigate through the Help file, click the **Contents** button on the upper left corner or the links on the top right corner.
- In the Help screens, look for words that are Hyperlink Blue; these link to other topics with related information.

Contents Tab: Browse Help by topic

- 1. Click a **Contents** button to open it and view the chapters and pages contained within.
- 2. Then click a page icon 1 to fill the Viewing pane with information on the selected subject.

Contents 🗐 Index 🔽 Search				- Search -				
×	Sele	ct ae	neral role rights		_			
Velcome to Perspective by PPM 2000		<u>9</u> -						
Set Started								
Navigation Options	All Role	le settings are located under the Roles tab of the Administration section in the Administration component.						
Security Laver Overview		Select the Role Rights tab. The screen will contain a list of general rights with two columns of Enable and Allow Override						
System Administration Components								
General Settings				es will be checked allowing the corresponding role right or set of rights to be				
Vorkgroups	OVE	erridden	at the User level.					
ystem Privileges								
loles			t 🗐 Delete 😧 Cancel					
Add a new role		Role Defaults						
Establish default security controls, lanc	8	×	Vew Audt History					
Select general role rights								
Specify visibility and access privileges	Enal	ble Allow	Override					
View discrepancies between role right:			GeoRollup City Edit					
Set report visibility for a role			Metric measurement unit					
? View discrepancies between role and			Gateway Administrator					
lsers			Gateway Approver					
Afficers			Edit Exchange Rates					
uditing om Labels			Editing All Narratives/Summaries					
om Labeis ookuos			Locking Records	E				
lags		8	Unlocking Records					
tandard Operating Procedures			Sealing					
Asual Alerts			Visual Analysis Access					
ateway Administration			Quick Find Access					
Administrative Reports			Focal Point Access					
Service Manager		8	Allow Merge Entities					
dditional Information								
		2	Allow Dispatchlog Access					
	Allow ele	evate on new r	ecords for:	· ·				
	2. Che	eck Enal	le to apply the corresponding right	or set of rights to the role's users, and uncheck the Allow Override box to				
4 111	nre	went the	corresponding right or set of rights f	rom being overridden at the Lleer level				

Index Tab: Browse Help by Index

- 1. Scroll through the listed keywords or type a keyword to reference.
- 2. Click a keyword from the list to display the associated topic.

🔰 Contents 📃 Index 😰 Search	- Search -	60
×	Establish default security controls, language and currency for a user	
Type in the keyword to find:		
user rights	All Users settings are located under the Users tab of the Administration section in the Administration component.	
About Access for Roles Access for Users	Note that any default settings specified for the user's role will automatically be assigned to the user. Verify that these settings are appropriate for the user and, if necessary, complete the following steps to modify them.	
Access Privileges Accessing Custom Search Accessing Focal Point	1. Open the General tab, the User Defaults sub-tab.	
Accessing Quick Find Accessing Visual Analysis	2. Select the workgroups you would like the user to have access to from the Workgroups list.	
Activity Prefixing Add Officer Alert Add RTA Alert Adding	 From the Default Workgroup lookup list, select the workgroup the user will be working in most often. When the user creates a new record, it will be stored in the user's designated Default Workgroup, unless they assign it to one of their other workgroups. 	
Assigning to Roles Assigning to Users Audt Logs Case Prefixing Currency Define Visual Representation of Certain Discrepancies from Role Report Visibili Discrepancies from Role Rights Discrepancies from System Rights e-Reporting Access Ottoms	4. Assign an organizational rollup to the user in the Org Rollups section. Organizational rollups are hierarchical, so the option you select in the Org Level 1 field will determine what options are available in the Org Level 2 field and so on. As you move down th hierarchy, organizational rollups become more specific, naming groups within your organization that are increasingly specialize by company division or region. The user will only have access to records with organizational rollups that correspond to, or are lower than, the organizational rollup you select for the user. For example, if a record's organizational rollup is North America/Canada/Alberta and the user's organizational rollup is North America/Canada, the user will have access to the record.	e ed
e-reporting Access Options Gateway Administrators Gateway Approvers General Rights Importing Options	 Assign an Access Level to the user. The user will only be permitted to view data with the same or lower access level as their own. 	
Incident Prefixing Language	6. Assign a Default Language to the user. This determines the field labels that will appear on forms when the user is logged on.	
Lookup List Visibility Report Cover Page Security Controls =	7. Set the Default Currency for the user. All currency values entered in Perspective will now appear for the user in this currency.	
Security Controls Setting Report Visibility Setting System Visibility	8. Check the Metric measurement unit box to allow the user to see all measurement data in metric values.	
User User Level TII	 To allow the user to assign an access level, organizational rollup and/or workgroup to a new record that is higher or different fror their own, check the Allow elevate on new records for Access Level, Org Rollups and/or Workgroup checkboxes. For 	n

Search Tab: Search Help

1. Type a word or phrase and click the **Go** button. Perspective Help will list topics containing the word or phrase below.

2. Click the topic you want to display. The topic will appear in the Viewing pane.

🕑 Contents 🗐 Index 🔀 Search	- Search -	G
xype in the word(s) to search for: nvestigation GO I Highlight search results Search results pr page 10	 Your security layer set-up begins with segregating your data by: Workgroup: Every record is assigned to one or more workgroups. These workgroups may be based on department, location, corporate level, division or some other structural element of your organization. For example, if your organization chooses to base its workgroup set-up on its departments, sample workgroups could be Human Resources, Investigations, or Security. Organizational Rollup: Each record may also be assigned an organizational rollup of up to four tiers. Organizational rollups 	9
le Rank △ ▲ ew screpancies streen system- vel rights and le or user phts mits 1 w discrepancies 1 tween system-	 Organizational Kondp. Each record may also be assigned an organizational routes. Organizationes. Organizationes. Organizatio	1
el nghts and role user rights All stern elcome to srspective by 2000 alcome to D Welcome to	Just as every record in Perspective is designated an access level, organizational rollup and one or more workgroups, all users in Perspective are similarly assigned these security protocols. Users may only view records that fall within the parameters of their access rights. For example, in the following illustration, the user represented by the yellow highlighting is only able to access records assigned to the Security workgroup and the North America organizational rollup, with an access level of 3 or less.	
erspective by PPM J000 ^m , th scurity Layer verview scurity Layer verview erspective 3 ovides for a high vides for a high vel of information -	Human Resources meeting tools Security Organicational Rollings South America Anic	

Navigation Options

To start modifying administrative settings, you must first open the **Administration** module on the Navigation pane. By default, the General Settings form will be displayed with the General tab open. Then, select a **component** (e.g., Administration) or a **sub-component** (e.g., Roles) of the program administration that you would like to modify from the menu on the left hand side. The relevant settings and/or fields available for viewing or editing will be displayed in the Visualization pane on the right.

Most of the interface components of the Administration module are equipped with a toolbar that enables the convenient navigation and modification of the administrative settings. Each administrative toolbar includes a number of functions from the list below.

🛃 Save	Preserves your changes to the entity. Complete every editing action with saving the changes applied to the record by clicking Save on the toolbar.
📝 Edit	Modifies the entity. After clicking Edit, select the entity you wish to edit and make the necessary change.
🐈 Add	Creates a new entity from scratch.
X Delete	Deletes an entire entity. In the confirmation window that pops up, click Yes.

8	Cancel	Cancels the changes made to an edited setting.
2	Refresh	Displays the saved changes made to an administrative setting.

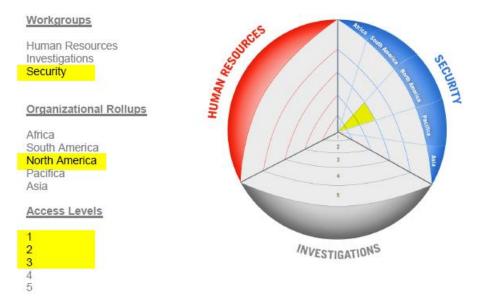
Security Layer Overview

Perspective provides for a high level of information security. Its unique security layers give you the flexibility to segregate and consolidate vast amounts of data while controlling data visibility through a sophisticated system of *workgroups*, *organizational rollups* and *access levels*, combined with *field* and *function* level security.

Your security layer set-up begins with segregating your data by:

- *Workgroup*: Every record is assigned to one or more workgroups. These workgroups may be based on department, location, corporate level, division or some other structural element of your organization. For example, if your organization chooses to base its workgroup set-up on its departments, sample workgroups could be Human Resources, Investigations, or Security.
- **Organizational Rollup**: Each record may also be assigned an organizational rollup of up to four tiers. Organizational rollups allow you to further compartmentalize data by subdividing workgroups. For example, if you need to segregate data by department and by region, you could establish a workgroup for each department and add organizational rollups that reflect your company's geographic locations (e.g., Africa, Asia, Europe, South America). A four-tier organizational rollup could include continent as the first tier, country as the second, state or province as the third and city as the fourth.
- **Access Level**: Every record is also assigned one of five access levels with Level 1 designating records that are unclassified and Level 5 marking data that is extremely confidential.

Just as every record in Perspective is designated an access level, organizational rollup and one or more workgroups, all users in Perspective are similarly assigned these security protocols. *Users may only view records that fall within the parameters of their access rights.* For example, in the following illustration, the user represented by the yellow highlighting is only able to access records assigned to the Security workgroup and the North America organizational rollup, with an access level of 3 or less.



User visibility may be even further refined with *field* and *function* level security. While workgroups, organizational rollups and access levels specify which records a user is able to access, field and function level security options go a step further to specify precisely which sections of a record a user can see (forms, sub-forms and fields), as well as what they are permitted to do with this data (read, add, edit and/or delete).

Within Perspective, user visibility and access rights are assigned at the:

- **System Level**: Default access rights (or privileges) are first applied to all users across the system.
- **Role Level**: Default access rights (or privileges) are inherited from the System level and can then be modified for each role.
- **User level**: Access rights (or privileges) are inherited from the Role level and can then be customized for each user.

System Administration Components

General Settings

General

- Assign Incident, Case (ICM and EIM only) and Activity Number formats/prefixes.
- Choose the default measurement system for numeric data.
- Set your organization's logo and address to print on report cover pages.
- Select the default font for narratives, summaries and interviews.
- Set to display your organization's privacy statement or legal notice upon logon.
- Hide the All Records View option on data forms and pick lists.
- Allow users to send formatted email messages.

Account Usage Policies

• Define user password and logon parameters.

Currencies

• Select the system's default currency, add new currencies and update exchange rates.

Languages

• Enter new custom languages or label sets into the system.

Administration

Workgroups

- Add a new workgroup.
- Specify a workgroup's Gateway import parameters and identifier prefixes.

System Privileges

- Assign system-level visibility and access rights.
- View discrepancies between system-level rights and role or user rights.

Roles

- Create a new role.
- Establish default security controls, language and currency for a role.
- Select general role rights.
- Specify visibility and access privileges for a role.
- Set report visibility for a role.
- View discrepancies between role and user rights and report visibility.

Users

- Create a new user.
- Establish default security controls, language and currency for a user.
- Set general user rights.
- Specify visibility and access privileges for a user.
- Set report visibility for a user.
- Track all changes made to a user account.

Officers

- Create a new officer for Perspective DispatchLog[™].
- Lock an officer from displaying in Perspective or Perspective DispatchLog.

Auditing

- View when, where and who accessed or modified a record.
- Enable or disable general and read auditing (Admin Master authority).
- Specify retention period for audit data (Admin Master authority).
- Choose to purge all audit data (Admin Master authority).

Lookups

- Modify a single-tier, multi-tier or hierarchical lookup list.
- Specify workgroup visibility for a lookup list.
- Enter call codes for the Call Category lookup list.
- Enter address information to the Site lookup list.
- Add running text to the Site lookup list for display in Perspective DispatchLog.

Flags

• Create a new incident or person flag.

Standard Operating Procedures (SOP)

- Create a new Standard Operating Procedure rule restricting it to specific call category, site specifications and/or activity status.
- Include the necessary description, checklist, attachments and links.
- Create the relevant notification message and specify the email addresses for their delivery.
- Specify the notification type for mass notifications sent via MIR3[™] inEnterprise[™].

Visual Alerts

- Define the visual representation (i.e., the font and the background color) for the fields that differentiate various Officer Teams, Officer Statuses, Organization Statuses, Priorities and Locations.
- Create Regulated Time to Act (RTA) alerts for activities in Perspective DispatchLog.

• Create Officer Alerts for officers in Perspective DispatchLog whose Status or Site change.

Language

Languages

- Set custom languages.
- Define custom web help paths.
- Assign dictionaries.

Form Labels

- Create a default label set for all users.
- Create a custom label set for each custom language.
- Create a custom report footer.
- Edit default report titles and labels.

License Management

Concurrent Licenses

- Displays a list of all users currently logged in to Perspective.
- Lets you know the maximum number of concurrent logins available to you.
- You can end sessions.
- Displays active services.

Named Licenses

- Assign licenses or use the Auto Assign option.
- Displays a list of all users currently logged in to Perspective.
- Displays active services.

General Settings

Set the Basic System Settings

All basic administration settings are located under the **General** tab of the General Settings section that opens by default as you open the Administration component.

Assign Incident, Case, and Activity Number Formats and Prefixes

- 1. Enter a prefix for all Incident Numbers, Case Numbers and Activity Numbers. If you would prefer not to have a prefix for a specific number type, leave the corresponding fields blank.
- 2. Choose **Identifier Formats** for Incident, Case, and Activity records from the corresponding lookup lists:
 - CCYY-MM-#####: This format identifies the record by the calendar year (CCYY) and month (MM) that it was added to Perspective, followed by a five digit sequential number that re-sets at the beginning of each month. For example, 2011-04-00123 identifies the 123rd incident/case/activity entered in Perspective in April 2011.
 - CCYY-######: This format identifies the record by the calendar year (CCYY) that it was added to Perspective, followed by a six digit sequential number that re-sets at the beginning of each year. For example, 2011-004567 identifies the 4567th incident/case/activity entered in Perspective in 2011.
 - ##########: This is known as *flat file format*. There is no year or month preceding the number. The first record entered in Perspective will be identified by the number 0000000001, and this sequential numbering will continue indefinitely with no re-set.

Choose the Default Measurement System for Numeric Data

Under **Default Measurement System**, choose **Metric** or **Standard** as the default system for entering numeric data, such as a person's Height, Weight, etc. Note that this setting can be overridden in individual user accounts.

Set your organization's logo and address to print on report cover pages

- 1. Click the Add icon 🖶 in the **Organization** field. A pop-up Entity List window will open.
- 2. Select the name of a company whose Organization record contains the logo and address you wish to place on report cover pages. If an Organization record does not already exist for your company, use the Quick Add function at the bottom of the pick list to create one, ensuring that you add your company's logo and address to the new record.

Note: Only the primary address will be displayed on the report cover pages, so ensure that the address that you want displayed is set to primary.

Note: This selection may be overridden by choosing a different organization at the workgroup and/or User levels.

Select the Default Font for Narratives, Summaries, and Interviews

- 1. Under **Default Font**, click the Add icon 🖶 in the **Font Name** field. A pop-up Font window will open.
- 2. Choose the **Font**, **Font Style** and **Size** that will be the new system default for all narrative, summary and interview text. Note that Arial, Tahoma and Times New Roman are the recommended fonts for optimal visualization.
- 3. Click **OK** to close the pop-up window and apply your selection to the **Font Preview** window.

Set to Display Organization Privacy Statement or Legal Notice After Logon

- To automatically display your organization's privacy statement after user logon, check the Display Privacy Statement on logon box. This will prompt users to read the privacy statement and click OK before Perspective loads.
- To automatically display your organization's legal notice after user logon, check the Display Legal Notice on logon box. This will prompt users to read the legal notice and click OK before Perspective loads.

Hide the All Records View Option on Data Forms and Pick Lists

To hide the All Records View option on data forms and pick lists, check the **Hide All Records View** box. Only the Quick View and Saved View options will now be available for all data forms in the Navigation pane, and only saved views will be available in pick lists.

Allow Users to Send Formatted Email Messages

To allow users to send formatted email messages, check the **Allow Format Email** box. Users will now have the option of sending email messages in plain text or in a formatted HTML table.

Click **Save** after each editing action.

General Settings	*	General -> Gener	al			
Account Policies	General	Account Policies	Currencies			
E Language	🚽 Save					
Configuration Form Labels		entifier Formats			Incident Identifier Format	
Workgroups		Incident Prefix	INC		CCYY-######	-
System Privileges					Case Identifier Format	
Roles Users		Case Prefix	CASE		CCYY-######	•
Lookups					Activity Identifier Format	
Flags		Activity Prefix	ACT		CCYY-MM-#####	•
Officers						
SOPs Visual Alerts Auditing	C De F	efault Measurement Metric Standard Organization Companization Company Standard Company Stan	-	×		
			on logon.			

Define User Password and Logon Parameters

- 1. Open the Account Policies tab.
- 2. Under **Password Length**, set the minimum length for user passwords (3 to 35 characters).
- 3. Under **Password Uniqueness**, specify whether or not Perspective should keep a history of user passwords. If yes, indicate the number of passwords to be kept in the password history from one to 10. For example, choosing 3 would require a user to go through three passwords before Perspective would allow him or her to re-use a former password.
- 4. Under Maximum Password Age, indicate whether or not passwords should expire after a certain number of days (1 to 180 days). Once a user password has expired, Perspective will prompt the user to select a new password.
- 5. Under **Password Format**, specify if passwords must contain special characters, both letters and numbers, or both uppercase and lowercase text. You can choose all, none or a combination of these options.

- 6. Under **Account Lockout**, enable or disable the option to lock out users after a specified number of unsuccessful logon attempts (1 to 9 attempts).
- 7. Under **Miscellaneous**, choose to enable or disable users to log on to Perspective from more than one machine at the same time. Also, indicate whether passwords must be different from user IDs. It is recommended that concurrent logons should not be permitted and that passwords should be distinct from user IDs.
- 8. To reset the settings modified back to the old values, click **Reset**. In the confirmation window that pops up, click Yes. To save the reset, click **Save**.

General Settings	Seneral -> Account Policies	
Account Policies Currencies Currencies Configuration Form Labels Administration Workgroups System Privileges Roles Users Lookups Flags Officers SOPs Visual Alerts Auditing	General Account Policies Currencies	
	Password Length Minimum Password Length 4 👳 character(s)	Password Format Require alphanumeric. Require at least one special character. Require uppercase and lowercase combination.
	Password Uniqueness Do not keep password history. Remember a mathefailing password(s)	Account Lockout No account lockout. Lockout account after Solution Soluti
	Maximum Password Age Password does not expire. Expires in 90 day(s) Reference	Miscellaneous Image: Permit concurrent logon from same account. Image: Password must be different from logon ID. set

Select Default Currency, Add New Currencies, and Update Exchange Rates

- 1. Open the **Currencies** tab.
- 2. To add a new currency to the list, click Add.
- 3. Enter the currency's **Full Name**, **Code** (abbreviated name), **Symbol** and **Exchange Rate** in the pop-up window.
- 4. Check the **Base Currency** box to identify the new currency as the default currency of your Perspective database. Note that it is **not recommended** that you change your Base Currency once it has been initially set. Doing so creates inconsistency in your data.
- 5. Click **OK** in the pop-up window, and then click **Save**.

Currency		×
Full Name: Canadian Dollar		
Code CAD		
Symbol \$		
Exchange Rate:	1.0000 🚔	
Base Currency:		
	OK Cancel	

- 6. To update the exchange rates of other currencies in relation to the base currency (the base currency is automatically given an exchange rate of 1.0000), select the currency, click **Edit**, modify the **Exchange Rate** in the pop-up window, and click **OK**.
- 7. To change the default currency listed under Base Currency, select the currency you wish to set as the new default and click Edit. Check the Base Currency checkbox in the pop-up window. In the confirmation window that pops up, click Yes. If you click No, the old Base Currency will be preserved. Click OK.

Note: The Base Currency cannot be deleted. If you wish to delete the current Base Currency, nominate a new Base Currency first, and then delete the unwanted currency entry.

General Settings General	🔆 General -> Curren	ncies				
Account Policies Currencies	General Account Policies I → Add 2 Edit X Delete	Currencies				
Configuration Form Labels	Base Currency					
Administration Workgroups	Name	US Dollar (USD)				
System Privileges	Symbol	\$				
Roles	Exchange Rate	1.0000				
Lookups Flags	Available Currencies					
Officers	Long Name		Code	Symbol	Exchange Rate	Base Currency
60Ps	Singapore Dollar		SGD	\$	0.2500	
/isual Alerts	US Dollar		USD	S	1.0000	•
Auditing	Japanese Yen		JPY	¥	76.1052	
	Canadian Dollar		CDN	S	0.3343	Π

Workgroups

Add a New Workgroup

- 1. Open Administration, Workgroups in the Navigation pane, then click Add.
- 2. Enter the **Workgroup Name** and a **Workgroup Description**.
- 3. From the **Organization** pick list, select the organization that applies to the workgroup. If an applicable Organization record does not exist, use the Quick Add function at the bottom of the entity list to create one, ensuring that you add the logo and address of the organization to the new record. The logo and address (specifically the primary address) are recorded in the selected Organization record will appear on the workgroup's report cover pages.

Note: If no organization is selected for the workgroup, the organization specified in the **General Settings** form under the **General** tab will be used by default. Organizations can also be assigned at the individual User level, overriding any selections made in General Settings and/or Workgroups.

- 4. *Optional*: If you would like incidents associated with this workgroup to be identified with a unique Incident Number, Case Number or Activity Number prefix (that differs from the default prefix assigned under General Settings), enter this in the relevant **Prefix** field.
- 5. If you would like to allow the workgroup to import reports into the Gateway, check the Enable Imports to this Workgroup box. The Gateway tab will open by default. See "Specify Gateway file import options and/or e-Reporting access options for a workgroup" in the "Gateway Administration" section of this guide for further information. Note that checking this box *does not* give the workgroup access to the Gateway; it only gives them rights to submit reports to the Gateway. Only designated Gateway Administrators and Gateway Approvers are permitted to access the Gateway.

Note: Incident, Item, Person, Organization and Vehicle reports can be imported through the Import Manager.

General Settings General	Administration -> Workgroups
Currencies	Workgroups System Privileges Roles Users Enter filter text. X 21 Image: Save Image: Sav
Configuration Form Labels	Central Workgroup Name Organization
Workgroups System Privileges Roles	Doons Workgroup Description
Users	EastCoast
- Flags Officers - SOPs	Eastern Identifier Prefixes
- Visual Alerts - Auditing	15Workgroup1 Incident Prefix Case Prefix Activity Prefix
	JDWG Enable Imports to this Workgroup

6. Click Save.

System Privileges

All System Privileges settings are located under the **System Privileges** tab of the **Administration** section in the Administration component.

Assign System-Level Visibility and Access Rights

- 1. Expand the four root nodes of the tree in the left part of the Visualization pane and select a system component, data form or other entity that you wish to work with.
- 2. Click the checkboxes and radio buttons on the right to define what users can see and how users can manipulate the selected entity:
 - Visible: Allows users to see the entity and its related buttons, icons and records, when they access Perspective.
 - Allow Override: Allows system-level entity rights to be overridden at a lower level (i.e., Role or User).
 - Full Control: Authorizes users to read, create, edit and delete entity records.
 - Read Only: Switches entity records to the read-only mode, so that they could not be edited or deleted by users.
 - Custom: Grants users the ability to create new entity records (Allow Add), read and edit existing entity records (Allow Edit) and/or delete entity records (Allow Delete).

It is highly recommended that users not be allowed to delete any records. A record deletion could compromise the integrity of your system and should be avoided in all but extraordinary circumstances.

General Settings General	Administration -> System Privileges		
Account Policies	Workgroups System Privileges Roles Users		
Currencies	Save		
Language			
Configuration			
Form Labels	Analysis Expert Data Form		
Administration	- Activities		
Workgroups		Visible	Allow Override
System Privileges			Line
Roles	+- Items		
Users	Organizations	Full Control	
Lookups	Persons	Read Only	
Flags	· Vehicles		
Officers	er-Gateway er-Report System	Custom	Allow Add
SOPs	Im Report System		Allow Edit
Visual Alerts			
Auditing			Allow Delete

- 3. Expand the remaining child nodes to display complete list of fields that constitute all the entities. Select a field name in the list.
- 4. Use the checkboxes on the right to customize users' access rights for the selected field:
 - **Required**: Designates the field as a required field that must be completed by users.
 - *Hidden*: Removes the field from the interface (hidden from users).
 - Hidden On New (active when the Hidden box is checked): Unchecking this box allows
 users to see the field in the records that are newly created. Checking both Hidden and
 Hidden On New options hides the field from both new and existing records.
 - **Locked**: Makes the field visible to the user, but not accessible for data entry or editing. In this case, the field appears greyed out and is locked from use.
 - Locked On New (active when the Locked box is checked): Unchecking this box allows
 users to access the field in the records that are newly created. Checking both Locked
 and Locked on New options locks the field from use in both new and existing records.
 - Allow Override: Allows system-level field rights to be overridden at a lower level (i.e., Role or User).

Note: Some system entities and fields are required by Perspective, and cannot be Overridden, Hidden or Locked. Whenever you encounter these entities, they will be marked with yellow explanatory Notes, while the unauthorized functions will be greyed out.

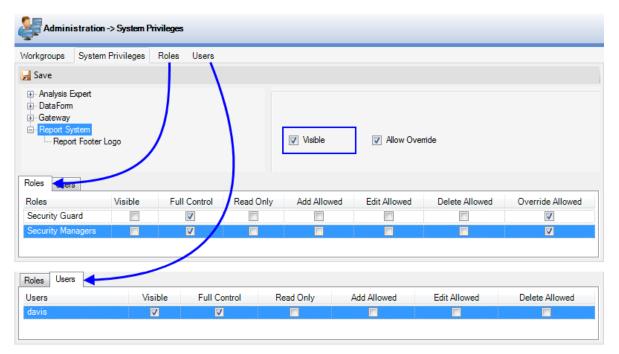
Admini	stration -> System F	rivileges				
Workgroups	System Privileges	Roles	Users			
Save	lies	ne	Lisers	Required Hidden Locked	Allow Override Hidden On New Locked On New	Note: This field cannot be Hidden or Locked on New records as it is required by Perspective.
S R P	ummary eported to Police olice File Number eported to Division		Ŧ			

- 5. Expand the child nodes contained within the field nodes to continue to assign system-level visibility and access rights for as many entities and fields as you wish.
- 6. Click Save.

View Discrepancies Between System-Level Rights and Role or User Rights

- 1. Expand the nodes to see available entities and fields, and make a selection.
- 2. By default, the **Roles** tab at the bottom of the screen will open. If any discrepancies exist between the system-level rights for the selected entity or field and a role's rights for the same entity or field, the role and its access rights will be displayed at the bottom.
- 3. To view discrepancies between the role-level rights for the selected entity or field and a particular user's rights to the same entity or field, click the Users tab at the bottom of the screen. If any discrepancies exist, the user's ID and their access rights will be displayed below.

In the illustration below, *davis* is a user whose role is *Security Managers*. On the system level, reports are generally visible for new roles. However, the reports' visibility is disabled for all the users whose role is set to *Security Managers*, except for the user *davis*. The bottom Roles and Users tabs are cross-populated from the grids stored under **Privileges** of the corresponding roles (i.e., under Privileges tab of the *Security Managers* role) and users (i.e., under Privileges tab of the user *davis*) that are accessible from the top Roles and Users tabs in Administration.



Roles

All Role settings are located under the **Roles** tab of the **Administration** section in the Administration component.

Add a New Role

- 1. Click Add.
- 2. Enter the **Role Name** and add a **Description**.
- 3. Check **Locked** to lock users belonging to the role out of Perspective (e.g., employees on leave, seasonal workers, etc.).
- 4. Check the **Role Available to Sub-Administrator on New User** box to allow Sub-Administrators to assign this particular role, and its associated rights and privileges, to new user accounts.
- Check Don't Allow Override on all Reports to prevent any of the role's visibility rights for reports from being altered at the User level. This checkbox is only activated once Save is clicked.

Administration -> Roles		
Workgroups System Privileges Roles	Users	
security	🗙 🖌 👌 🖶	🛃 Save 🖶 Add 📝 Edit 🖳 Delete 区 Cancel
SECURITY 1		General Role Defaults Role Rights Privileges Reports
	Unlocked	Role Name
Security Guard		Security Managers Locked
Front line guys, first to record an Incide	Unlocked	
Security Managers		Description This role is created for the managers at the Security Department.
This role is created for the managers at	Unlocked	
		Role Available to Sub Administrator on New User
		Don't Allow Override on all Reports

6. Click Save.

Establish Default Security Controls, Language, and Currency for a Role

- 1. Open the **Role Defaults** tab.
- Select the workgroups you would like the role to have access to from the Default Workgroups list.
- 3. From the **Default Workgroup** lookup list, select the workgroup the role's users will be working in most often. When a user belonging to this role creates a new record, it will be stored in the role's designated Default Workgroup.
- 4. Assign a **Default Language** to the role. This determines the field labels that will appear on forms when the role's users are logged on.
- 5. Assign an organizational rollup to the role in the **Default Org Rollups** section. Organizational rollups are hierarchical, so the option you select in the Org Level 1 field will determine what options are available in the Org Level 2 field and so on. As you move down the hierarchy, organizational rollups become more specific, naming groups within your organization that are increasingly specialized by company division or region. The role will only have access to records with organizational rollups that correspond to, or are lower than, the organizational rollup you select for the role. For example, if a record's organizational rollup is North America/Canada/Alberta and the role's organizational rollup is North America/Canada, the role will have access to the record.
- 6. Assign a **Default Access Level** to the role. The role will only be permitted to view data with the same or lower access level as its own.
- 7. Set the **Default Currency** for the role. All currency values entered in Perspective will now appear for the role in this currency.
- To allow any of the Role Defaults to be overridden at the User level, check the Allow Override box directly beneath the relevant default setting, or uncheck the Allow Override box to prevent the setting from being overridden. By default, Allow Override boxes are checked.

🛃 Save 📲 Add 📝 Edit 🖳 Delete 🌘	Cancel	
General Role Defaults Role Rights	Privileges Reports	
Default Workgroups	Default Org Rollups Org Level 1 North America Org Level 2 Canada Org Level 3 British Columbia Org Level 4 Vancouver	▼ ▼ ▼
Allow Override	Allow Override	
Default Workgroup	Default Access Level	
Advanced Users 👻	Level 3	~
	Allow Override	
Default Language	Default Currency	
System English 💌	Canadian Dollar (CDN)	~
Allow Override	Allow Override	

Select General Role Rights

1. Select the **Role Rights** tab. The screen will contain a list of general rights with two columns of **Enable** and **Allow Override** checkboxes. By default, all Allow Override boxes will be checked allowing the corresponding role right or set of rights to be overridden at the User level.

🚽 Sa	ve 🛑 Add	🖉 Edit	🔄 Delete 🔞 Cancel	
Gene	eral Role	Defaults	Role Rights Privileges Reports	
	¥	¥	View Audit History	٨
_				
	Enable	Allow C	Werride	
		✓	GeoRollup City Edit	_
		✓	Metric measurement unit	
			Gateway Administrator	
			Gateway Approver	
			Edit Exchange Rates	
		✓	Editing All Narratives/Summaries	
			Locking Records	E
		✓	Unlocking Records	
			Sealing	
		✓	Visual Analysis Access	
		✓	Quick Find Access	
		✓	Focal Point Access	
		✓	Allow Merge Entities	
	_			
		✓	Allow Dispatchlog Access	
^	Now elevate	on new rec	pords for:	Ŧ

2. Check **Enable** to apply the corresponding right or set of rights to the role's users, and uncheck the **Allow Override** box to prevent the corresponding right or set of rights from being overridden at the User level.

 Administrator	Grants the user administrative privileges. Note: There are differences between the default Admin Master account and a Perspective User with Administrator rights. See the section Default Admin Master vs. Users with Administrator Rights for more information.
Sub-administrator	Allows the role's users to create user accounts and modify User Details and User Defaults, but only for users who are within their default workgroup and who have the same (or lower) access level and organizational rollup as their own.
Supervisor	Identifies the role's users as Supervisors within the system, giving them access to the Controls tab on all records. Among other things, this allows the role's users to change workgroups, organizational rollups and access levels of records.
Investigator (Perspective Premium)	Identifies the role's users as Investigators within the system, giving them access to Investigation forms, tabs and functions.
Full History Access	Allows the role's users to view all incident involvements under the History tabs of Item, Person, Organization and Vehicle records, regardless of the security controls assigned to the records. Note that checking this box will not allow the role's users access to the actual Incident records, only the knowledge that the person, organization, item or vehicle was involved.
View Audit History	Permits the role's users to view all record modifications (including the information as to when and where they were made and who made them) tracked under the Audit History tab of each record.
GeoRollup City Edit	This feature will become functional in a future Perspective release. Please, disregard it for now.
Metric Measurement Unit	Allows the role's users to see all measurement data in metric values. Currently, only the Height and Weight fields contain measurement data in Perspective.
Gateway Administrator	Assigns the role's users associated Gateway Administrator access privileges. <i>Note: For more information on these roles and what they entail, see the Perspective User's Guide or Perspective's User Help.</i>

Gateway Approver	Assigns the role's users associated Gateway Approver access privileges. Note: For more information on these roles and what they entail, see the Perspective User's Guide or Perspective's User Help.
Edit Exchange Rates	Allows the role's users to update exchange rates under the Currencies tab of General Settings.
Editing All Narratives/Summaries	Allows the role's users to edit any unsealed narratives or summaries, even if they are not the original author.
Locking Records	Allows the role's users to lock records while barring all users from making any changes or additions to the selected records.
Unlocking Records	Allows the role's users to re-instate editing rights to previously locked records.
Sealing	Allows the role's users to seal narratives, summaries and interviews from future editing by any user.
Visual Analysis Access	If your system includes Perspective Visual Analysis, grants the role's users access to the application. Note: Visual Analysis is an optional module for Perspective. If you are not certain whether your Perspective system includes this module, please contact Customer Service for verification.
Quick Find Access	Grants the role's users access to the Quick Find tool.
Focal Point Access	If your system includes Perspective Focal Point, [†] grants the role's users access to the application. Note: Focal Point is an optional module for Perspective. If you are not certain whether your Perspective system includes this module, please contact Customer Service for verification.
Custom Search Access	Allows the role's users access to the Custom Search feature. Note: This option will only be visible if the Custom Search feature has been configured in the Perspective Service Manager.
Allow Merge Entities	Allows the role's users to merge Item, Organization, Person and Vehicle records in the Data Forms component of Perspective.
Allow DispatchLog Access	Grants the role's users access to the Perspective DispatchLog module.

Access Level	Allows the role's users to assign an access level to a new record that is higher or different from their own. For example, if the Enable box for the Allow elevate on new records for Access Level right is selected for a role with an Access Level of 3, the role's users will be able to assign Access Levels of 4 or 5 to new records. However, once one of the role's users has assigned an elevated access level to a new record, saved the change and exited the record, the role's users will no longer be permitted access to the record, as it falls beyond the scope of their role privileges.
Workgroup	Allows the role's users to assign a workgroup to a new record that is higher or different from their own.
Org Rollups	Allows the role's users to assign an organizational rollup to a new record that is higher or different from their own.

Specify Visibility and Access Privileges for a Role

1. Open the **Privileges** tab.

- 2. Expand the four root nodes and select a system component, data form or other entity from the list. The system rights set for the entity will be displayed on the right.
- 3. To override system rights for this particular role, use the checkboxes and the radio buttons on the right to define what the role's users can see and how users can manipulate the selected entity:
 - *Visible*: Allows users to see the entity and its related buttons, icons and records, when they access Perspective.
 - Full Control: Authorizes users to read, create, edit and delete entity records.
 - Read Only: Switches entity records to the read-only mode, so that they could not be edited or deleted by users.
 - Custom: Grants users the ability to create new entity records (Allow Add), read and edit existing entity records (Allow Edit) and/or delete entity records (Allow Delete).
 - Allow Override: Allows role-level entity rights to be overridden at a lower level (i.e., User). By default, Allow Override boxes are checked, unless the Don't Allow Override on all Forms/Fields box has been checked on the General tab of this form.

It is highly recommended that users not be allowed to delete any records. A record deletion could compromise the integrity of your system and should be avoided in all but extraordinary circumstances.

🚽 Save 🖶 Add 📝 Edit 🖳 Delete 🐼 Cano General Role Defaults Role Rights Privil	eges Reports		
Forms Analysis Expert DataForm Activities Cases Instatents Organizations Persons Persons Vehicles Gateway Report System	Visble Full Control Read Only Custom	 Allow Override Allow Add Allow Edt Allow Delete 	

- 4. Expand the remaining child nodes to display a complete list of fields that constitute all the entities. Select a field name in the list. The field's system rights appear on the right.
- 5. To override system rights for this particular role, use the checkboxes to define the role's access rights for the selected field:
 - **Required**: Designates the field as a required field that must be completed by users.
 - Hidden: Removes the field from the interface (hidden from the user).
 - Hidden On New (active when the Hidden box is checked): Unchecking this box allows
 users to see the field in the records that are newly created. Checking both Hidden and
 Hidden On New options hides the field from both new and existing records.
 - Locked: Makes the field visible to the user, but not accessible for data entry or editing. In this case, the field appears greyed out and is locked from use.
 - Locked On New (active when the Locked box is checked): Unchecking this box allows
 users to access the field in the records that are newly created. Checking both Locked
 and Locked on New options locks the field from use in both new and existing records.
 - Allow Override: Allows role-level field rights to be overridden at a lower level (i.e., User). By default, Allow Override boxes are checked, unless the Don't Allow Override on all Forms/Fields box has been checked on the General tab of this form.

Note: Some system entities and fields are required by Perspective, and cannot be Overridden, Hidden or Locked. Whenever you encounter these entities, they will be marked with yellow explanatory Notes, while unauthorized functions will be greyed out.

ieneral Role Defaults Role Rights	Privileges	Reports		
Forms				
ie- Activities ie- Cases ie- Incidents	^ _	Required	Allow Override	Note: This field cannot be
File Number Reported Date/Time Occurred From Date/Time	=	 Hidden Locked 	 Hidden On New Locked On New 	Hidden or Locked on New records as it is required by Perspective.
Occurred To Date/Time Record Owner				
Incident Duration Class Rollup Business Unit Rollup				
Site Rollup Summary				
 Reported to Police Police File Number 	-			

- 6. Expand the child nodes contained within the field nodes to continue to specify visibility and access rights of the role for as many entities and fields as you wish.
- 7. Click Save.

View Discrepancies Between Role Rights and User Rights

- 1. Open the **Privileges** tab.
- 2. Expand the nodes to see available entities and fields, and make a selection.
- 3. If any discrepancies exist between the role-level rights for the selected entity or field and a user's rights for the same entity or field, the user and their access rights will be displayed at the bottom of the screen.

In the illustration below, the role's report visibility is disabled for all the constituent users, except for the user *davis*.

General Role Defaults Role Rights	D 1 1					
	s Privileges	Reports				
Forms Analysis Expert DataForm Gateway Report System Report Footer Logo	(🕅 Visible	✓ Allow Override			
Discrepancy Report	Visible	AllowFullControl	AllowReadOnly	AllowAdd	AllowEdit	AllowDelete
davis	V	V				

Set Report Visibility for a Role

- 1. Open the **Reports** tab.
- 2. To allow a role's users to see reports listed under Report Title, check the **Visible** boxes beside the report names.
- 3. To allow any of these report visibility settings to be overridden at the User level, check the Allow Override box for the report, or uncheck the Allow Override box to prevent the role's report visibility from being overridden. By default, Allow Override boxes are checked, unless the Don't Allow Override on all Reports box has been checked on the General tab of this form.
- 4. Click Save.

View Discrepancies Between Role and User Report Visibility

- 1. Open the **Reports** tab.
- 2. Select a report listed under Report Title.
- 3. If any discrepancies exist between the role's visibility for the selected report and a user's visibility for the same report, the user and their visibility setting will be displayed at the **Discrepancy Report** pane.

neral Role Defaults Ro	le Rights	Privileges	Reports				
vailable Reports							
	Repo	rt Title			Visible	Allow Override	1
RPT_Reports_CaseAssign	nmentByPe	rsonReport			V		
RPT_Reports_CaseLosse	sReport			_		V	
RPT_Reports_CaseReport			1				
RPT_Reports_CaseSummaryReport			V	V			
RPT_Reports_CaseTotals	Report					V	
RPT_Reports_ClassClass	ificationRe	port				v	
RPT_Reports_IncidentLossesReport			V	V			
RPT Reports IncidentRep	oort				V	V	
)iscrepancy Report				<u> </u>			
UserID		Visible		4			
davis				V			

Users

All Users settings are located under the **Users** tab of the **Administration** section in the Administration component.

Add a New User

- 1. Click Add.
- Select the name of the user from the Linked Person pick list. If a Person record does not already exist for the user, use the Quick Add function to create one. The First Name and Last Name fields will now automatically populate with information drawn from the linked person's record.
- 3. Assign a **Role** to the user. All rights and privileges assigned to the role will automatically cascade down to the user.
- 4. Choose a **Perspective Logon ID** for the person.
- If your Perspective system uses Windows authentication, enter the user's Windows Logon ID for logging onto their computer.
- 6. Click **Set Password** to assign a password to the user account. An Enter Password pop-up window will appear. Enter the password twice and click OK. (Note that once this record has been saved, the Set Password link will be labelled **Change Password**.)

Enter Password	X
Enter Password twic case-sensitive.	e to confirm. Note Password is
Enter New Password	•••••
Confirm Password	•••••
	OK Cancel

- 7. Check the **Change Password On Logon** checkbox to force the user to choose a new password the next time they logon to the system.
- 8. Select the name of the person who approved the creation of this user account from the **Approved By** pick list. If a Person record does not already exist for the user, use the Quick Add function to create one.

- 9. Select the organization that the user belongs to from the Organization pick list. If an applicable Organization record does not already exist, use the Quick Add function to create one, ensuring that you add the organization's logo and address to the new record. The logo and address appearing in the selected Organization record will now appear on the user's report cover pages. If no organization is selected for the user, the organization specified for the user's workgroup will be used. If none is specified for the user's workgroup, then the organization selected under the General tab of the General Settings form will be used by default.
- 10. Enter any other notes in the **Comments** box. You have now completed the **User Details** form. Before saving a user's record, you must enter required default settings for the user account under the User Defaults sub-tab.

Administration ->	Users		
Workgroups System Pr	rivileges Roles Users		
	× ✓ Å	📙 Save 👘 Add 📝 Edit 🖳 Delete 😣 Ca	ncel
Davis, Ian		General Privileges Reports Audit Hist	ory
davis	Security Managers	User Details User Defaults User Rights	
		User Details	
		Linked Person	Role Security Managers
		First Name Ian	Last Name Davis
		Perspective Logon ID davis	Windows Logon ID
		Change Password	Approved By
		Change Password On Login	🖾 Wolf, Abner 🛛 🖶 🗙
			Organization
			🖾 Metropolitan Police 🖶 🗙
		Comments Ian Davis is the head of the investigation tea	am.

Establish Default Security Controls, Language, and Currency for a User

Note: Any default settings specified for the user's role will automatically be assigned to the user. Verify that these settings are appropriate for the user and, if necessary, complete the following steps to modify them.

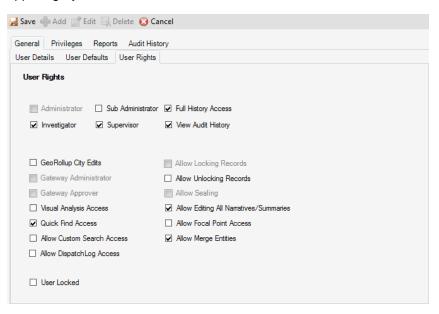
- 1. Open the **General** tab, the **User Defaults** sub-tab.
- 2. Select the workgroups you would like the user to have access to from the **Workgroups** list.
- 3. From the **Default Workgroup** lookup list, select the workgroup the user will be working in most often. When the user creates a new record, it will be stored in the user's designated Default Workgroup, unless they assign it to one of their other workgroups.

- 4. Assign an organizational rollup to the user in the Org Rollups section. Organizational rollups are hierarchical, so the option you select in the Org Level 1 field will determine what options are available in the Org Level 2 field and so on. As you move down the hierarchy, organizational rollups become more specific, naming groups within your organization that are increasingly specialized by company division or region. The user will only have access to records with organizational rollups that correspond to, or are lower than, the organizational rollup you select for the user. For example, if a record's organizational rollup is North America/Canada/Alberta and the user's organizational rollup is North America/Canada, the user will have access to the record.
- 5. Assign an **Access Level** to the user. The user will only be permitted to view data with the same or lower access level as their own.
- 6. Assign a **Default Language** to the user. This determines the field labels that will appear on forms when the user is logged on.
- 7. Set the **Default Currency** for the user. All currency values entered in Perspective will now appear for the user in this currency.
- 8. Check the Metric measurement unit box to allow the user to see measurements in metric.
- 9. To allow the user to assign an access level, organizational rollup and/or workgroup to a new record that is higher or different from their own, check the Allow elevate on new records for Access Level, Org Rollups and/or Workgroup checkboxes. For example, if the Allow elevate on new records for Access Level checkbox is selected for a user with an Access Level of 3, the user will be able to assign Access Levels of 4 or 5 to new records. However, once the user has assigned an elevated access level to a new record, saved the change and exited the record, they will no longer be permitted access to the record, as it falls beyond the scope of their user privileges.
- 10. Click Save.

e 🖶 Add 📝 Edit 🖳 Delete 🔞 C	ancel	
al Privileges Reports Audit His	story	
Details User Defaults User Rights		
ault Settings	, 	
Vorkgroups	Org Rollups	
45WG	Org Level 1	
Administrator - PPM2000 Work	North America	•
Advanced Users	Org Level 2	
	Canada	-
	Org Level 3	
	British Columbia	-
	Org Level 4	
	Vancouver	•
T	Vancouver	
Default Workgroup	Access Level	
Advanced Users 👻	Level 5 (Highest)	~
	Defection and the second	
Allow elevate on new records for:	Default Language System English	*
Access level	System English	Ť
	Default Currency	
Org Rollups	Canadian Dollar (CDN)	~
✓ Workgroup	Metric measurement unit	

Set General User Rights

1. Open the **General** tab, the **User Rights** sub-tab. The screen will contain groups of general rights with checkboxes. The rights that are disabled for the user on their role level will appear greyed out.



2. Check the rights that you would like to apply to the user.

Administrator	Grants the user administrative privileges. Note: There are differences between the default Admin Master account and a Perspective User with Administrator rights. See the section Default Admin Master vs. Users with Administrator Rights for more information.
Sub-administrator	Allows the user to create user accounts and modify User Details and User Defaults, but only for users who are within their default workgroup and who have the same (or lower) access level and organizational rollup as their own.
Supervisor	Identifies the users as Supervisors within the system, giving them access to the Controls tab on all records. Among other things, this allows the user to change workgroups, organizational rollups and access levels of records.
Investigator (ICM and EIM)	Identifies the user as an Investigator within the system, giving them access to Investigation forms, tabs and functions.

Full History Access	Allows the user to view all incident involvements under the History tabs of Item, Person, Organization and Vehicle records, regardless of the security controls assigned to the records. Checking this box will not allow the user access to the actual Incident records, only the knowledge that the person, organization, item or vehicle was involved.
View Audit History	Permits the user to view all record modifications (including when and where they were made and who made them) tracked under the Audit History tab.
GeoRollup City Edits	This feature will become functional in a future Perspective release. Please, disregard it for now.
Gateway Administrator	Assigns user associated Gateway Administrator access privileges. Note: For more information on these roles and what they entail, see the Perspective User's Guide or Perspective's User Help.
Gateway Approver	Assigns user associated Gateway Approver access privileges. Note: For more information on these roles and what they entail, see the Perspective User's Guide or Perspective's User Help.
Visual Analysis Access	If your system includes Perspective Visual Analysis, grants the user access to the application.
Allow Focal Point Access	If your system includes Perspective Focal Point, grants the user access to the application. <i>Note: Focal Point is an optional module for Perspective. If you are not</i> <i>certain whether your Perspective system includes this module, please</i> <i>contact Customer Service for verification.</i>
Quick Find Access	Grants the user access to the Quick Find tool.
Allow DispatchLog Access	Grants the role's users access to the Perspective DispatchLog module.
Allow Custom Search Access	Allows the role's users access to the Custom Search feature. Note: This option will only be visible if the Custom Search feature has been configured in the Perspective Service Manager.
Allow Locking Records	Allows the user to lock records while barring all other users from making any changes or additions to the selected records.
Allow Unlocking Records	Allows the user to re-instate editing rights to previously locked records.

Allow Sealing	Allows the user to seal narratives, summaries and interviews from future editing by any user.
Allow Editing All Narratives/Summaries	Allows the user to edit any unsealed narratives or summaries, even if they are not the original author.
Allow Merge Entities	Allows the role's users to merge Item, Organization, Person and Vehicle records in the Data Forms component of Perspective.
User Locked	Locks the user out of the system (e.g., employees who have been terminated, employees on leave, seasonal employees, etc.).

Specify Visibility and Access Privileges for a User

1. Open the **Privileges** tab.

- 2. Expand the four root nodes and select a system component, data form or other entity from the list. The system and/or role rights set for the entity will be displayed below.
- To override system and/or role rights for this particular user, use the checkboxes and radio buttons to define what the user can see and how the user can manipulate the selected entity:
 - **Visible**: Allows the user to see the entity and its related buttons, icons and records, when they access Perspective.
 - *Full Control*: Authorizes the user to read, create, edit and delete entity records.
 - Read Only: Switches entity records to the read-only mode, so that they could not be edited or deleted by the user.
 - **Custom**: Grants the user the ability to create new entity records (Allow Add), read and edit existing entity records (Allow Edit) and/or delete entity records (Allow Delete).
- It is highly recommended that users not be allowed to delete any records. A record deletion could compromise the integrity of your system and should be avoided in all but extraordinary circumstances.

🛃 Save 🛑 Add 📝 Edit 📏	< Delete 🔞 Cancel		
General Privileges Rep	orts Audit History		
Entities Fields Administration Auditing Flags Ceneral Settings Concentration Officers Office			
 Visible Full Control Read Only Custom 	Allow Add	Allow Edit	Allow Delete

- 4. Expand the remaining child nodes to display a complete list of fields that constitute all the entities. Select a field name. The system and/or role rights set for the field will be displayed below.
- 5. To override system and/or role rights for this particular user, use the checkboxes to define the user's access rights to the selected field:
 - **Required**: Designates the field as a required field that must be completed by users.
 - *Hidden*: Removes the field from the interface (hidden from the user).
 - Hidden On New (active when the Hidden box is checked): Unchecking this box allows
 users to see the field in the records that are newly created. Checking both Hidden and
 Hidden On New options hides the field from both new and existing records.
 - Locked: Makes the field visible to the user, but not accessible for data entry or editing. In this case, the field appears greyed out and is locked from use.
 - Locked On New (active when the Locked box is checked): Unchecking this box allows
 users to access the field in the records that are newly created. Checking both Locked
 and Locked on New options locks the field from use in both new and existing records.

Note: Some system entities and fields are required by Perspective, and cannot be Hidden or Locked. Whenever you encounter these entities, they will be marked with yellow explanatory Notes, while the unauthorized functions will be greyed out.

Save 🖶 Add 📝 Edit 🗙 Delet	e 😢 Cancel
General Privileges Reports	Audit History
Entities Fields	
- Persons	
Title	
···· First Name	
Initial	
··· Last Name	
···· Designation	
··· Date of Birth	
Gender	
···· Marital Status	
Hair Color Eve Color	
Height	
···· Weight	
Person Photo	
Employee	
···· Investigator	
Employee Number	
···· Supervisor	
Flag Notes	
Additional Information	
Person Attachments Contact Section	
A Note: System-required field. Thi	s field cannot be Hidden or Locked on New.
✓ Required	
Hidden	Hidden On New
Locked	Locked On New

- 6. Expand the child nodes contained within the field nodes to continue to specify visibility and access rights for the user for as many entities and fields as you wish.
- 7. Click Save.

Set Report Visibility for a User

- 1. Open the **Reports** tab.
- 2. To allow a user to see reports listed under Report Title, check the **Visible** boxes beside the report names.
- 3. Click Save.

Seneral Privileges Reports Audit History Available Reports		
Report Title	Visible	-
RPT_ActivityLandscape_ReportTitle		1
RPT_ActivityPortrait_ReportTitle		
RPT_FrequencyDistribution_Report		
RPT_Reports_BussinessUnitHierarchyReport		
RPT_Reports_CaseLossesReport		
RPT_Reports_CaseSummaryReport		
RPT_Reports_CaseTotalsReport		
RPT_Reports_ClassClassificationReport		
RPT_Reports_ClassHierarchyReport		
RPT_Reports_IncidentAssignmentByPersonReport		
RPT_Reports_OrganizationReport		

Track All Changes Made to a User Account

- 1. Open the Audit History tab.
- Click the Get Audit History button to view all modifications made to the user account since its creation. The pane on the left contains entries for each change made to the record. DateTime indicates when the change was made; UserID reveals who made the change; Record Action describes what type of change was made; and Machine Info specifies which computer was used to make the change.
- 3. Select an entry to view further details of the change made in the pane on the right. Expand the nodes to see exactly what the data value was **Before** and **After** the change was made.

🛃 Save 🖶 Add 📝 Edit General Privileges Re	🚉 Delete 🔞 Can				
😢 Get Audit History					
Drag a column header h	nere to group by tha	at column.		After: True ⊡∵ SealNarratives	*
DateTime (GMT) 2011/07/20 09:21:01	UserID	Record Action	Machine Info 192.168.1.94	Before: (NULL) After: True	
2011/07/20 09:21:01	remnyakova remnyakova	Updated Updated	192.168.1.94	 Allow Edit Non Author Narratives Before: (NULL) 	
2011/07/20 09:19:55	remnyakova	New	192.168.1.94	After: True View Audit History Before: (NULL) After: True RoleName Before: (NULL) After: True True RoleName Before: (NULL)	
				Summary - yotk	
				Record Count: 3 User: remnyakova Record Action: New Date/Time Yours: 20/07/2011 3:19:55 PM Users: 20/07/2011 3:19:55 PM GMT: 20/07/2011 9:19:55 PM	

Officers

Add a New Officer for Perspective Dispatching

- 1. In the Navigation pane, select **Officers**.
- 2. Click Add.
- 3. Select the name of the officer from the **Involved Person** pick list. If a Person record does not already exist for the user, use the Quick Add function to create one.
- 4. From the **Default Workgroup** lookup list, select the workgroup to which the officer will normally be administered.
- 5. Place the officer into a **Team** selecting it from the lookup.
- 6. In the **Default Call Sign** lookup, select a call sign that will be attributed to the officer once they are brought on duty in Perspective DispatchLog.
- 7. Under the **Default Location** lookups, select the initial location specifications that will be attached to the officer once they are brought on duty in Perspective DispatchLog.
- 8. Check the **Officer Locked** box to hide the officer in Perspective DispatchLog.
- 9. Click Save.

■ General Settings General	Enter filter text.	× ✓ 🛓 🕺	officers	
Account Policies Currencies	Binkley, Velma Central	Team 1	🔄 Save 🖶 Add 📝 Edit 🗙 Delete 📀) Cancel
Configuration Form Labels	Blake, Daphne Central	Team 1	Officer Details	
 Administration Workgroups System Privileges 	Bruce, Tom Central Camillo, Tony	Team 1	Involved Person	Site
Roles	Central	Team 2	Default Workgroup Central	Building
- Lookups Flags	Cassidy, Natasha Central	Team 2	Team Team 1	Location
<mark>Officers</mark> SOPs Visual Alerts	Chan, Peter Central	Team 2	Default Call Sign	Section
Auditing	Clancy, Kevin Doons	Team 3	Officer Locked	
	Clemments, Dana Doons	Team 3		

License Management

Depending on your licensing, use the License Management tool to access concurrent licenses, or named licenses.

Concurrent Licenses

If you have concurrent licenses, the License Management tool displays a list of all users currently logged in to Perspective, and the maximum number of concurrent logins available to you. You have the ability to end these sessions. The Active Services grid displays a list of any service running on a service account; this takes up a license, and these sessions cannot be ended.

To end a user's session, do the following steps:

- 1. In the Navigation pane, select License Management.
- 2. Select a user from the User Name list.
- 3. Click End Session.
- 4. Click Yes.

License Manageme	int			
ave <i>参</i> Refresh 01:50	•			
ctive Sessions		Maxim	um 25 Of Concurent Logins	i
User Name	Domain Name	Database	Last Action (GMT)	Арр
lee		default	08/08/2013 04:23 PM	Desktop
gk		default	08/08/2013 05:28 PM	Desktop
hradmin		default	08/08/2013 08:58 PM	Desktop
gk		default	08/08/2013 09:56 PM	Desktop
bb		default	08/08/2013 09:05 PM	Desktop
JL		default	08/08/2013 09:54 PM	Desktop
RT		default	08/08/2013 09:34 PM	Desktop
Active Services				End Session
User Name	Last Action (GMT)	Datab	ase	Арр
bb	08/08/2013 6:12 AM	defa	ult	Mobile

Named Licenses

If you have named licenses, the License Management tool allows you to assign user licenses, or use the Auto Assign option.

To access your licensed Perspective users, select License Management.

The left grid displays a list of all active sessions. The right grid displays a list of all licensed users (the number of licensed users is above this grid, as well as the number of licenses available, and the number of pending releases). The bottom grid displays a list of all active services.

Assign a User

To assign users individually, do the following steps:

- 1. Click the **Assign** button on the bottom of the screen.
- 2. Find the user from the entity list that you want to assign a license to.
- 3. Click Select.

Remove a User

You may want to remove a user to free up a license:

- 1. Click the name (or corresponding row) of the license you want to remove from either the active session list, or the licensed user's list.
- 2. Click the **Remove** button on the bottom of the screen. A pop-up window will appear.
- 3. Click **Yes** if you want to remove the license. Click **No** if you do not want to remove the license.
 - It will take 24 hours for the license to become available again.

Auto Assign Users

If you have a large number of users and want to automatically assign each of them a license, do the following steps:

- 1. Check the Auto Assign box.
 - All users will be assigned licenses.

Note: More than one of the same User Account cannot be used on the same application at the same time. For example, a user cannot be logged into Perspective Desktop Client more than once at the same time, but the same user can be logged into Perspective Desktop Client and Mobile at the same time.

	•							
Sessions					Licensed Users : 12	Licenses A	Available : 13	Pending Release : 0
User Name	Domain Name	Database	Last Action (GMT)	Арр	User Name	Domain Name	Database	License Date
RT		default	08/12/2013 05:38 PM	Desktop	ms1		default	08/12/2013
ms1		default	08/12/2013 05:57 PM	Desktop	ASAdmin		default	08/07/2013
rc		default	08/12/2013 05:28 PM	Desktop	bb		Perspective_40	08/12/2013
hradmin		default	08/12/2013 03:50 PM	Desktop	gk		default	08/07/2013
bb		default	08/12/2013 05:41 PM	Desktop	rc		Perspective_40	08/12/2013
JL		default	08/12/2013 05:48 PM	Desktop	RTAdmin		default	08/07/2013
					JL		Perspective_40	08/12/2013
					rc		default	08/07/2013
					JL		default	08/07/2013
					RT		default	08/12/2013
					RT		Perspective_40	08/12/2013
					hradmin		Perspective_40	08/12/2013
Canviana								
Services								
Services User Name	Last Action (GMT)	Database	Ap	p				
	Last Action (GMT) 08/12/2013 05:38 PM	Database default	Ар					
User Name								
User Name								
User Name								
User Name								
Jser Name								
Jser Name								
Jser Name								
User Name								
Jser Name								
Jser Name								
User Name								

Auditing

View When, Where, and Who Accessed or Modified a Record

- 1. Select **Auditing** in the Navigation pane.
- 2. From the **Module** lookup list, choose the system component for which you would like to view audit information (e.g., Administration, Incidents, Persons, etc.).
- 3. If you would like to view record modifications made by a particular user, select the name of the user from the **User ID** pick list.
- 4. Specify a **Date Range** to narrow your search results temporally.
- 5. Click Search. Results will be displayed in the panes below. The pane on the left contains entries for each change made to the record. The details reflected in the list of entries (i.e., column headings) vary depending on the module selected. Generally, the entries indicate the date and time the change was made (Date/Time), who made the change (UserID), where the change was applied (Record Description), what type of change was made (Record Action), which computer was used to make the change (Machine Info), as well as other module-specific information.
- 6. Select an entry to view further details of the change made in the pane on the right. Expand the nodes to see what the data value was **Before** and **After** the change was made.

Note: Functions 7-11 are only available when logged in as the default Admin Master user.

- 7. To ensure the system continues to track the creation and modification of records in the selected module, leave the **Audit Enabled** box checked. Unchecking this box will disable audit functionality.
- 8. To allow the system to track when records are accessed and read in the selected module, check the **Audit Reads** box. Perspective will only keep track of this information once this box is checked; the system cannot audit retroactively.
- To specify how long the system should store audit information for the selected module, click Keep data indefinitely or choose the number of days (1-180) in Retention Period.
- 10. Click **Purge all audit data** to clear the system of the module's stored audit information.
- 11. Once you have altered the Retention Period of audit data, or clicked the Audit Reads or Audit Enabled box, click **Save Changes**.

User ID remnyakova	3	<mark>₽</mark> ×	Date Rar 15/06/20	-	Date Range To 20/07/2011 : III X Search
Date/Time (G	UserID	Record De	Record	C Machine Info	Date/Time: remnyakova: 08/06/2011 1:19:20 PM remnyakova: 08/06/2011 1:19:20 PM GMT: 08/06/2011 7:19:20 PM
2011/06/07 1	remny	ADMI-201	Update	192.168.1.94	Details (Updated)
2011/06/07 0		ADMI-201	•	192.168.1.94	⊡- IncidentID — Before: (NULL)
011/06/07 0		ADMI-201	•	192.168.1.94	
011/06/07 0	remny	ADMI-201	Update	192.168.1.94	⊡ · IncidentDescription
2011/06/07 0	remny	ADMI-201	Update	192.168.1.94	
2011/06/07 0	remny	ADMI-201	Update	192.168.1.94	⊡ LinkedIncidentID
2011/06/07 0	remny	ADMI-201	Update	192.168.1.94	Before: (NULL) After: 7c038211-a886-4a9e-b67a-42554a2d5d47
2011/06/07 0	remny	ADMI-201	Update	192.168.1.94	
2011/06/07 0	remny	ADMI-201	Update	192.168.1.94	Before: (NULL) After: ADMI-2010-000124
					Image: Audit Enabled Retention Period Purge all audit data Image: Audit Reads Image: Audit Reads Purge all audit data

Lookups

A "lookup" is a controlled part of Perspective's interface which is represented by a single-string field with an attached list of options to choose from (e.g., the Vehicle Color drop-down list or Site Rollup). There are two types of lookups in Perspective—single-tier lookups and multi-tier lookups.

A **single-tier lookup** is an independent lookup that does not imply any subordinate lookups. For example, the *Vehicle Color* drop-down list may provide a choice of such values as "Silver", "Black" or "Blue", which does not pre-define the choices that are available for lookups that describe other vehicle properties, like *Vehicle Style* or *Vehicle Model*.

In contrast, a **multi-tier lookup**—also known as "rollup"—is a complex architecture of hierarchically dependent lookups, where the value selected for the first lookup in the sequence pre-defines the values available for the following lookup. For example, the *Vehicle Make Model Rollup* consists of the embedded lookups *Vehicle Make* (e.g., Audi, BMW, etc.) and *Vehicle Model* (e.g., A3, Q7, etc. for Audi; 630csi, M6, etc. for BMW).

To edit the content of lookups that are available in Perspective, use the **Lookups** section in the Administration component.

Modify a Single-Tier Lookup List

- 1. Click once to select one of the lookup categories in the alphabetized list and display its content on the right. Double-click to select a category and see the associated forms at the bottom of the screen with the Language tab open by default.
- 2. Select the type of modification required and follow the procedures below:
- To add a new option to the selected lookup list, click the **Add New** button and type the option in the **Custom English** field. Although Custom English is the default language for all lookups, you can enter language-specific lookup options in the appropriate language/label set text fields. Custom English lookup options still appear for users assigned to other languages, if there are no alternative lookup options specified for their assigned language.
- To edit an option in the selected lookup list, click on the option to highlight it, and edit the text in the **Custom English** field.
- To delete an option from the selected lookup list, highlight the option in the list, and click the **Delete** button. Note that you will not be able to delete any lookup list options that have already been used in existing Perspective records. If this occurs, you can hide the value from visibility so users cannot choose the value from the lookup list when completing a record. See "Specify Workgroup Visibility for a Lookup List Value" on page 51 for further details.
- 3. Click Save.

Lookups	
Activities dedist Activities dedist ActivityStatuses AgencyStatus Assignment Types Attachment Types CallSon CallSon CalSource CaseOlepostons	Inactive Escalated to Investigations Inactive No Further Action Taken Pending Cout Under Investigation Unsolved Wating for Approval Wating for Assignment
CaseNarativeTypes Cases_udTSeverty Cases_udWatchList CaseStatuses OptingColors OptingTypes DamageSeverties	Language Visibility Custom English Inactive 2
Inclent_Organization_udfIndustryTyp Incident_Persons_udfRace IncidentRags Incidents_udfSeverty Incidents_udfSeverty Incidents_udfWatchList	Language 1 Inactivo Language 2 Inaktiv
Incident Statuses Incitem Dispositions Incivehicle Dispositions Injury Causes Injury Severity Levels Interview Types	Add New Delete

Modify a Multi-Tier or Hierarchical Lookup List

- 1. Multi-tier lookup lists (rollups) appear in capital letters at the bottom of the list. Double-click on one rollup name to display the hierarchical list of its options on the right and see the associated forms at the bottom of the screen with the Language tab open by default.
- 2. Expand the nodes of the rollup. Each rollup has up to four tiers of options for users to select from (e.g., the Class Rollup consists of Class, Category, Subcategory and Type).
- The first tier is the **Root** of the rollup (e.g., Class in the Class Rollup). The option selected in the first tier determines what options are available in the second tier and so forth.
- The higher tier in the hierarchy is the **Parent field**, while the lower tier is the **Child field**. For example, Class is the parent field to the Category child field.
- Any child fields that are on the same tier of the hierarchy are **Sibling fields**. In other words, all Class fields are siblings to each other; all Category fields are siblings to each other, and so on.
- 4. Select the type of modification required and follow the procedures below:
- To delete an option from a rollup, select the option and click **Delete**. If the option has child fields, you must first delete all of the option's child fields before deleting the option itself. Note that you will be unable to delete any rollup options that are already saved in existing records. If this occurs, you can hide the value from visibility so users cannot choose the value from the lookup list when completing a record. See "Specify Workgroup Visibility for a Lookup List Value" on page 51 for further details.

• To add an option to the first tier of a rollup hierarchy, click **Add Root**, or select one of the first-tier options (e.g., Criminal) and click **Add Sibling**.

Lookups		
🛛 🛃 Save 🛛 📝 Edit 🛭 👙 Refresh		
OfficerStat OfficerTet Organizations-unindustryType OrganizationTypes Orgimulypes Orgimulypes Orgimulypes Orgimulypes Orgimulypes Orgimulypes PesiSmaiTypes PesiSmaiTypes PesiSmaiTypes PesiSmaiTypes PesiSmaiTypes	*	<new> ⊕ Criminal ⊕ Policy Volation ⊕ Procedural ⊕ Safety Glavo</new>
ReviewTypes SevertyLevels SummayTypes SummayTypes VehicleColors VehicleSyles VehicleSyles VehivolvementTypes BUSINESSUMTROLLUPS CALLCATEGORYROLLUPS	E	Language ClassRollups Visibility Custom English Failurel Language 1 Language 2
GEOROLLUPS ITEMCLASSROLLUPS ITEMMAKEMODELROLLUPS ORGROLLUPS SITEROLLUPS VEHICLEMAKEMODELROLLUPS	Ţ	Language 3 Add Root Add Child Add Sibling Delete

• To add an option to the second (or lower) tier of a rollup hierarchy, select one of the first-tier (or higher-tier) options (e.g., Failure) and click **Add Child** (e.g., Software).

Lookups		
🛃 Save 📝 Edit 👙 Refresh		
Officer Star Organizations and Industry Type Organization Types Organization Types Orghron Types Orghrone Types Orghrone Types Outcome Premary Causes Dutcome Press Outcome Press Outcome Press Pers Start Types Pers Start Types Pers Start Types Pers Start Types	•	Failure - <new> Cminal Non-Cminal Policy Volation Pocodural Safety Failure I I I I I I I I I I I I I I I I I I I</new>
Persinvolvement Types Person Flags		Language ClassRollups Visibility
Persons_udfRace SeverityLevels SubjectInvolvements	h	Custom English Software 3
Summary Types Task Types		Language 1
VehicleColors VehicleStyles		Language 2
Vehinvolvement Types BUSINESSUNITROLLUPS	E	
CALLCATEGORYROLLUPS CLASSROLLUPS	d	Language 3
GEOROLLUPS ITEMCLASSROLLUPS ITEMMAKEMODELROLLUPS ORGROLLUPS		2
SITEROLLUPS VEHICLEMAKEMODELROLLUPS	+	Add Root Add Child Add Sibling Delete

• To add a new option to a tier that already contains other options, select an item in the tier (e.g., Software), and click **Add Sibling** (e.g., System).

1: Lookups		
🛃 Save 🛛 📝 Edit 👙 Refresh		
OfficerStat		Failure - <new></new>
OfficerTe 4 Organizations out industry Type Organization Types OrgEmailTypes OrgPhone Types OutcomePrimary Causes OutcomePrimary Causes PersAddress Types PersFeature Types PersFeature Types		Criminal Policy Violation Procedural Softy Software Software Software Software
PersidTypes		
PersInvolvement Types Person Flags		Language ClassRollups Visibility
Persons_udfRace SeventyLevels		Custom English System 3
SubjectInvolvements		System (J)
Summary Types		Language 1
TaskTypes VehicleColors		
Vehicle Styles		Language 2
Vehinvolvement Types		
BUSINESSUNITROLLUPS	E	
CALLCATEGORYROLLUPS CLASSROLLUPS		Language 3
GEOROLLUPS ITEMCLASSROLLUPS ITEMAKEMODELROLLUPS ORGROLLUPS SITEROLLUPS		2
VEHICLEMAKEMODELROLLUPS	٠	Add Root Add Child Add Sibling Delete

- 5. Type the new option in the **Custom English** field (the default language for all lookup lists), or another language's corresponding text field to make the option exclusive to users of a particular language/label set.
- 6. Click Save.

Specify Workgroup Visibility for a Lookup List Value

- 1. Double-click on the correct lookup list to see the associated forms at the bottom of the screen with the Language tab open by default.
- 2. From the lookup list, select the lookup value you would like to adjust workgroup visibility for. Some hierarchical lookups or rollups allow you to adjust visibility at the second level of the hierarchy as well as the first. In this case, expand the nodes at the root level to view further lookup options and select the option for which you wish to adjust workgroup visibility.
- 3. Open the **Visibility** tab. Note that this tab will not appear for ORGROLLUPS, because it is not possible to adjust visibility for organizational rollups.
- 4. By default, all lookup lists and their available options are visible to all workgroups. To permit specific workgroups to use the selected lookup option, first uncheck the **All Workgroups** box, and then click the checkboxes corresponding to the appropriate workgroups.
- 5. Click Save.

Lookups			
GflicerSt OfficerSt OfficerCa OrgAddi	Failure		
OrganizationOffIndustryType OrganizationTypes OrgEmaiTypes OrgPhoneTypes OrgPhoneTypes OutcomePrimaryCauses	Policy Volation Procedural Safety Folure	1	
OutcomeSecondaryCauses Persons_udFRace SevertyLevels SubjectInvolvements SummaryTypes TaskTypes	Language Clas	ssRollups Visibility	
VehicleColors VehicleStyles VehinvolvementTypes	All Workgrou		
BUSINESSUNITROLLUPS CALLCATEGORYROLLUPS GEOROLLUPS ITEMCLASSROLLUPS ITEMCLASSROLLUPS ITEMMAKEMODELROLLUPS	F180 Feb18WG Feb2 Smoke 1 JD Workgroup LAWG	MSWG44 MSWG45 Ontario PPM-2000 reader	V Workgroup A V Workgroup C Workgroup D V Workgroup E
ORGROLLUPS SITEROLLUPS VEHICLEMAKEMODELROLLUPS			Add Root Add Child Add Sibling Delete

Enter Call Codes for the Call Category Lookup List

- Double-click on CALLCATEGORYROLLUPS at the bottom of the Lookups list and see all Call Category options on the right and the associated forms at the bottom of the screen with the Language tab open by default.
- 2. Expand the nodes in the Call Category rollup's list of options. Each category has up to three tiers available. Select the call categories (e.g., Administrative Tasks or Activated Alarm) and sub-categories (e.g., Document Delivery or Test Alarm) for which you want to specify the code.
- 3. Select the **Category Code** tab.
- 4. Input the appropriate code for the selected option in the **Call Code** field. The code entered will only be saved for the particular category or sub-category selected. To enter a code for a different level of the Call Category rollup, you must select the option and input the appropriate code individually. One way to approach call codes is to build codes for sub-categories (e.g., 500A for Document Delivery and 500AK for Confidential Document Delivery) upon the codes for categories (e.g., 500 for Administrative Tasks).
- 5. Select the appropriate **Default Priority** for each of the call categories. The priority selected will only be saved for the particular category or sub-category that you chose. To enter a priority for a different level of the Call Category rollup, you must select the option and input the correct priority marker individually.
- 6. Click Save.

Lookups						
🗄 🛃 Save 🛛 📝 Edit 🛭 😂 Refresh						
OfficerTeam OrgAddressTypes Organizations_udfIndustryType Organization Types OrgEmailTypes OrgInvolvementTypes OutcomePrimaryCauses OutcomePrimaryCauses OutcomeSecondaryCauses Persons_udfRace PersonTitles PersonTitles PersoPhoneTypes PersoPhoneTypes PersoPhoneTypes RequestTypes ReviewTypes ReviewTypes SeventyLevels SubjectInvolvements SummarTypes TaskTypes VehicleColors VehicleStyles VehicleStyles VehicleStyles USINESSUNITROLLUPS CALLCATEGORYROLLUPS SITEROLLUPS	E	Activated Administra Administra Ocu O	Alarm ative Tasks ment Delivery onfidential ff Site rgent Invoice Category Code	- Document Delive	ery - Confiden	tial
VEHICLEMAKEMODELROLLUPS	-	Add Roo	t Add Sil	bling	Delete	

Enter Address Information for the Site Lookup List

- 1. Double-click on **SITEROLLUPS** at the bottom of the Lookups list and see all Site options on the right and the associated forms at the bottom of the screen with the Language tab open by default.
- 2. Expand the nodes in the Site rollup's list of options. Each Site has up to four tiers available. Select the Site, Building, Location or Section for which you want to specify the address.
- 3. Select the **SiteRollups** tab.
- 4. Input the appropriate address for the selected option in the Address, Country, State/Province, City and Zipcode/Postal Code fields. The address entered will only be saved for the particular Site, Building, Location or Section selected. To enter an address for a different level of the Site rollup, you must select the option and input the appropriate address individually.
- 5. The **Longitude** and **Latitude** fields will display the coordinates set for the Site available for any custom integrations using Integration Services.
- If required, enter any important Site Notes for display in Perspective DispatchLog. Once stored for a specific site in Perspective, this text will be running on the Status bar in Perspective DispatchLog every time you select an Activity record that has its location set to this site.

O Start	Schedu		Ontinge							Perspecti	ve Dispatch	log				1 🖂
Start	Close Or Activity Dur Dispatch					Arrive Cle All	ar Clear All	Activity Details	Officer Log	Attachmen Re	t SOP R		/ Highlight	View St Location	atus N	V Aail
Activitie	-												1			
1	Activity Num	ber	Priori	ty 🗸	Location	7	Off Site		Call Ca	tegory		ed Date/	Officer Status	S 🖓 Organiz	ation 5	7 P
	ACT-2011-0	0 0142	1	4	Alberta				Public D	isturbance	13/07	/2011	Waiting	Wa	iting	
	ACT-2011-0	00141	Med	ium	Alberta				Area	Check	13/07	/2011	Waiting	Wa	iting	
•	ACT-2011-0	00151	5	4	Acme		-		Activat	ed Alarm	3:17	25 PM	Waiting	Wa	iting	
H 4															Þ	•
wailabl	le							Assign	ed							
	Officer Name		Location	∽ Call Sig	n ⊽ Offic	er Status	Tea	ס ער ו	fficer/Orga	anization Nan	ne 🗸 🛛 Lo	cation		n 🛛 Offic	er Statu	s '
🦹 w	atson-Parke	г, В	ritish Columbi	a PPM-002	Avail	able	Team 2									
🤻 Ca	ige, Luke	А	cme University	/ PPM-001	Avail	able	Team 2									
•	10		111				Þ	•		111						
3:2	27 PM						Hazardo	ous ma	terial	ls! <						

7. Click **Save**. The Site rollup address will now cross-populate for any Site/Location entered on any of the forms in the system and print on Incident and Activity reports. The particular address that appears on the forms and reports will be that of the *lowest* level in the record's Site rollup with an address entered in Perspective. For example, if a particular Site, Building and Location have been selected in a record and only the Site and Building have addresses entered in Perspective, the latter's address will appear on a form or a report.

Lookups		
🗄 🛃 Save 🛛 📝 Edit 🛭 🧔 Refresh		
OfficerStatuses	Acme University - Administration Building	
OfficerTeam		
OrgAddressTypes		Â
Organizations_udfIndustryType	E-Administration Building	
OrganizationTypes	East Wing	-
OrgEmailTypes	West Wing	Ξ
OrgInvolvementTypes	- Alberta	
OrgPhoneTypes	British Columbia	
OutcomePrimaryCauses		
OutcomeSecondaryCauses		
PersAddressTypes	⊕ New Brunswick	
PersEmailTypes	. Newfoundland	
PersFeatureTypes	. Northwest Territories	
PersIdTypes		*
PersInvolvementTypes	Language SiteRollups Visibility	
Person Flags		
Persons_udfRace PersonTitles	Longitude Latitude Country	
PersPhone Types		
Priority	0.000.00 - Canada -	
ReportCategories	State\Province	
RequestTypes	Address 1	
ReviewTypes	1112 University Drive Alberta 👻	
SeverityLevels	City City	
SubjectInvolvements	AddressZ	
SummaryTypes	Administration Building Edmonton	
TaskTypes		
VehicleColors	Zipcode/Postal Code	
VehicleStyles	T1A 2B3	
VehInvolvement Types		
DODINEDODININOEEDIO	E Site Notes	
CALLCATEGORYROLLUPS	Hazardous Materials!	
CLASSROLLUPS		
GEOROLLUPS		
ITEMCLASSROLLUPS		
ITEMMAKEMODELROLLUPS		
ORGROLLUPS		
VEHICLEMAKEMODELROLLUPS	Add Root Add Child Add Sibling Delete	
VERICLEWAREMODELROLLUPS		

Activity Statuses and Officer Statuses

The **Activity Statuses** Lookup, used in Activity and DispatchLog tasks, warrants special mention, as it behaves differently than its name may suggest. In effect, these statuses apply to both activities and officers, as in DispatchLog an Activity's status is usually determine by the status of the Officer(s) currently assigned to it.

The Relationship Between Activity Statuses and Officer Statuses

Adding new values to the Activity Statuses Lookup list doesn't strictly add statuses to activities as the name may suggest; these statuses are also tied directly to Officer Statuses.

Refer to **System values** below for a list of Activity Statuses already in the Perspective system.

Note: System Values cannot be deleted, though they can be renamed on a per-language basis.

Additional values added to this Lookup, due to the nature of how Activity and Officer Statuses relate, become new <u>Officer</u> Statuses. For example, if the custom value "On Lunch Break" is added, this status applies only to Officers and <u>not</u> Activities.

System Values

The following Activity Statuses are considered System values (i.e., they cannot be deleted):

- Available: Applies to Officers and denotes the associated Officer is available for assignment.
- **Busy**: Applies to Officers and denotes the associated Officer is on duty, but currently "busy" and cannot be assigned at this time.
- **Cleared**: Applies to Activities and denotes the assigned Officer(s) have been cleared and the associated Activity may be marked as Closed.
- **Closed No Report**: Applies to Activities and denotes the associated Activity is closed with no report required.
- **Closed Report Completed**: Applies to Activities and denotes the associated Activity was open, then had a report completed, causing it to close.
- **On Hold**: Applies to both Officers and Activities; denotes the assigned Officer considers the Activity "on hold" while the Officer completes his or her current assignment. This is considered a "temporary" status.
- **On Route**: Applies to both Officers and Activities; denotes the associated Officer is on route to the site of an assigned Activity.
- **On Scene**: Applies to both Officers and Activities; denotes the associated Officer is at the site of an assigned Activity.

Open - Report Required: Applies to Activities and denotes the associated Activity requires a report to be completed. The Activity status can only be move to Closed either once a report is complete (i.e., Closed – Report Completed) or a report is no longer required (i.e., Closed – No Report).

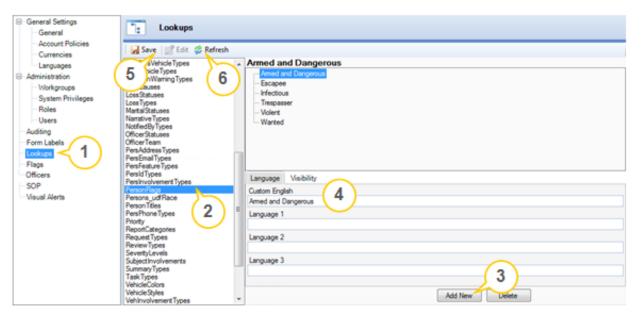
Note: To note an Activity's state further than Open or Closed, use **Activity Disposition** Lookup values.

- **Out of Service**: Applies to Officers and denotes the associated Officer is considered "out of service" an unavailable in the field for any assignment.
- **Suspended**: Applies to both Officers and Activities; denotes the assigned Officer was either On Route or On Scene and was reassigned before the former Activity was cleared. The response is considered "suspended" until the officer is assigned; once that happens, the suspended response is then cleared. This is considered a "temporary" status.
- Waiting: Applies to Activities and denotes a new Activity awaiting an Officer assignment.

Flags

Add a New Incident or Person Flag

- 1. Select **Lookups** in the Navigation pane.
- 2. In the Lookups list, double-click **IncidentFlags** if you wish to add a flag to the Incident form, or **PersonFlags** if you wish to add a flag to the Person form.
- 3. Click the Add New button at the bottom of the screen.
- 4. Type the name of the new flag in the **Base Language** field.
- 5. Click Save.
- 6. Click the **Refresh** button.



- 7. Select **Flags** in the Navigation pane.
- 8. Specify the type of flags intended for editing by selecting either **Incidents** or **Persons** from the **View Flags For** lookup list.
- 9. Click Add.
- 10. In the new flag form on the right, select the flag name you created earlier in the Lookups section on the **Flag Description** lookup list.
- 11. Enter a unique one-character designation for the flag in the Flag Code field.

- 12. To add an image to the new flag, click the **Add** icon **G** in the **Flag Image** field, select an image from the pop-up browser and click Open.
- 13. Click Save.
- 14. To edit an existing flag, click **Edit** and proceed as described above. To delete a flag, go to the Lookups section, the IncidentFlags or the PersonFlags lookup, select the relevant flag's node and click **Delete**.

۲	Flags			
🚽 Sav	ve 🛑 Add 📝 Edit 🖳 Delete 😣 Cancel			
	View Flags For: Persons -		code (1 Char only)	_
	Α	A		
4	Armed and Dangerous	Flag D	Description	_
-	R	Arme	ed and Dangerous 🔻	
6	Escapee	Flag Im	nage	
1	1		ট্ 😢 🖆	
	Infectious			
*	T Trespasser			
۵	V Violent			
۴	W Wanted			

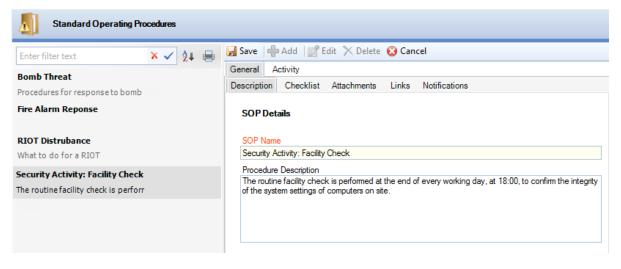
Standard Operating Procedures

Create a New Standard Operating Procedure Rule for an Activity

Using the Standard Operating Procedures (SOP) component of Administration, you can create a new SOP rule restricting it to a specific call category, site specifications and/or activity status. The created SOP rule will subsequently feature in Activity records that correspond to the settings specified in both Perspective's Activity data forms and the SOP component in Perspective DispatchLog.

In order to complete this operation, select **SOP** on the Navigation pane and follow the steps below:

- 1. Click Add. A blank SOP form will open with the General tub, the Description sub-tab open.
- 2. Start with specifying the official **SOP Name** in the required field.
- 3. Add a brief **Procedure Description** in the textbox below.



4. To start defining the activity parameters that would trigger the SOP, open the **Activity** tab.

5. Click Add New.

- 6. In the new record window, specify the restrictive parameters for the activities that would trigger the SOP by entering the activity type's **Code** and/or the **Levels**. Make the parameters as specific as necessary (e.g., Security Activity, Security Activity/Verification\Check, etc.).
- 7. Check the Active box to restrict the SOP to active activities only.

- Restrict the location of the SOP-related activities by selecting their common Site, Building, Location and Section. Make the parameters as specific as necessary (e.g., Acme University, Acme University/Administration Building, etc.).
- 9. Check the Off Site box to implement the SOP to the off-site activities only.
- 10. Click **OK** to save the parameters for immediate activation of the SOP.
- 11. If required, add relevant SOP Checklist(s), Attachment(s), Link(s), and set up Notification(s).

📝 Edit Record				- • •
OK Car	ncel			
Code 911C-4	Level 1 Security Activity Level 2 Verification\Check	•	Site ✓ Active Site Acme University Building Administration Building	•
	Level 3 Facility Check	-	Location	-
			Section	-
			☐ Off Site	

 Add as many activity parameters that match the SOP requirements as necessary, and click Save. The next time an activity with the specified parameters is created the system will automatically activate the SOP option in Perspective and Perspective DispatchLog.

General Activity				
Add New	Edit Remove			
Total Activities: 2				
SOP Name	Call Category	Site Rollup	Is Active	Is OffSite
Security Activity:	Security Activity/	Acme University/	V	
Security Activity:	Suspicious Activit	Alberta/Edmonto	V	V

Add a Checklist for the SOP

- 1. Open the **General** tab, the **Checklist** sub-tab.
- 2. To specify the first checklist item, click Add New.
- 3. Enter the text of the initial recommended procedure, and click **OK**.

🖶 Add N	lew Record	
ок	Cancel	
	ck List Details ckList Name	
Exa	mine possible modifications made to the system	

- 4. Add as many procedures that constitute your required SOP as necessary.
- 5. To re-arrange the position of items in the checklist, select the item of interest and click **Move Up** and **Move Down**, as required.
- Click Save. The next time an activity with the specified parameters is created the system will automatically activate the SOP option in Perspective and Perspective DispatchLog and display the interactive checklist. In the Activity record, you will be able to check the completed actions.

🛃 Save 🖶 Add 📝 Edit 📉 Delete 😣 Cancel	
General Activity	
Description Checklist Attachments Links Notifications	
Add New Edit Edit Remove Omove Up Omove Down	
Total Check List Items: 6	
 Examine possible modifications made to the system 	
 Examine possible modifications to data 	
 Examine the facility for possible external tools a 	
✓ Look for possbile external tool output	
✓ Review log files	
Check for systems possibly involved in intrusion a	

Attach a Relevant SOP File

- 1. Open the **General** tab, the **Attachments** sub-tab.
- 2. To attach a file related to the SOP, click **Add New**. A pop-up window will open.
- 3. Click **Browse** to locate and select the file you wish to attach.
- 4. The **Attachment Title** field will automatically populate with the name of the attached file. If necessary, modify the name.
- 5. From the **Attachment Type** lookup list, select the appropriate designator for the attachment (e.g., Document, Picture, Video).
- 6. Give an overview of the attachment in the **Description** text box.

7. Click **OK** to upload the attachment. Once the upload is complete, click OK again to return to the record.

Attachment Title	
STANDARD OPERATING	PROCEDURE-3-22-06[1] Erowse
Attachment Type	
Document	•
Description	
	dures for Handling Security Incidents at Acme University
	dures for Handling Security Incidents at Acme University
	dures for Handling Security Incidents at Acme University
	dures for Handling Security Incidents at Acme University
Standard Operating Proce	dures for Handling Security Incidents at Acme University
Standard Operating Procee	STANDARD OPERATING PROCEDURE-3-22-06

- 8. Add as many attachments as necessary.
- 9. Click **Save**. The next time an activity with the specified parameters is created the system will automatically activate the SOP option in Perspective and Perspective DispatchLog and display the list of viewable attachments.
- 10. To view an attachment that has been added to the list, select it in the grid and click **View**. Then, click **Open** to see it, or **Save As** to save it on your computer.

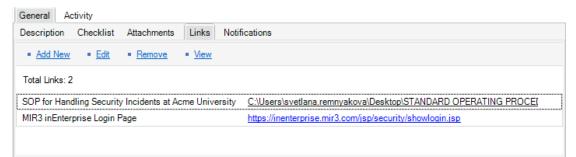
🛃 Save 🖶 Add	🖉 Edit 🗙 Delete	🔞 Cancel			
General Activity					
Description Check	list Attachments	Links Notifications			
• Add New • Ed	<u>dit</u> • <u>Remove</u>	• <u>View</u>			
Total Attachments: 2					
Attachment Title	Attachment Type	File Name	File Extension	File Size	Description
STANDARD OPER	Document	STANDARD OPERATI	.pdf	90 KB	Standard Operating Proc
SOP graph	Picture	gone_fishing1	jpg	39 KB	A graphic representation
Download	-	DPERATING PROCEDU NG PROCEDURE-3-22-06[1	RE-3-22-06[1]		X
✓ Completion	ete	ד 	ransferred 90 Kb	/ 90 Kb Open	

Add a Relevant SOP Link

- 1. Open the **General** tab, the **Links** sub-tab.
- 2. To add a relevant SOP link to a file on your organization's commonly accessible local drive or an external Web URL, click **Add New**. A pop-up window will open.
- 3. In the Title field, enter a descriptor for the link you are creating.
- If you are linking a local file, click the Browse icon, find the corresponding file and click
 Open to confirm the operation. If the link is a Web URL, paste the link into the Link field.
- 5. Click **OK** to add the link to the list.

	×
Close	
Title	
SOP for Handling Security Incidents at Acme University	
Link	
\desktop\standard operating procedure-3-22-06[1].pd 📄 🗙	
	Title SOP for Handling Security Incidents at Acme University

- 6. Click **Save**. The next time an activity with the specified parameters is created the system will automatically activate the SOP option in Perspective and Perspective DispatchLog and display the links for reference.
- 7. To view the created link, select the link in the grid and click **View**. If the link is still valid, the file or URL will open.



Set Up Individual and Mass Notifications for the SOP

Using the Notification feature of Administration, you may set up multiple individual, as well as mass notifications that will be sent out once an activity with the previously specified parameters is created. The mass notifications are being sent in conjunction with the third-party notification tool, the MIR3[™] inEnterprise[™].

- 1. Open the **General** tab, the **Links** sub-tab.
- 2. Under **To** and **Cc** fields, specify the recipients' direct and the carbon copy email addresses respectively for the delivery of the individual notifications. You may either type the addresses in, or click the relevant buttons and select the user(s) you wish to email the notification to from the list. Note that only the users with specified Primary Email Address will be available for the list selection.
- 3. Enter the **Subject** of the notification.
- 4. In the **Message** textbox, enter the SOP notification message.
- 5. If mass notification feature is enabled in your system and a mass notification is required for the SOP, select the **Notification Type** from the lookup list below. For details about setting up the available Notification Type options, refer to the *Perspective Installation Guide*.
- 6. Click Save. The next time the appropriate activity is created the system will automatically activate the SOP option in Perspective and Perspective DispatchLog and provide a form to send out the relevant notifications. In the Activity record, you will also be able to read the notifications that have previously been sent.

🚽 Save	🖶 Add 🛛 📝 Edit 🔀 Delete 🔞 Cancel	
General	Activity	
Descripti	on Checklist Attachments Links Notifications	
Ema	il Notification	
To .	charlene.czirfusz@ppm.com,michelle.smith@ppm2000.com	<u>^</u>
Cc .	svetlana.remnyakova@ppm2000.com	-
Subjec	t: SOP for Security Activity: Facility Check	
Messa	ge:	
	Acme University, Administration Building	*
Activit	y: Security Activity: Facility Check	
	putine facility check must be performed at the end of every working day, at 18:00, to confirm the integrity of the system as of computers on site.	
setting	s of computers on site.	-
	A Send Mass Notification	
	Notification Type	
	Training 💌	

Visual Alerts

Using the Visual Alerts section in the Administration module of Perspective, you can easily manipulate the display of specific types of information in Perspective DispatchLog[™]. For instance, you may highlight important or urgent data to easily prioritize information for the dispatcher.

Creating visualization settings contained in the Visual Alerts component of Administration you can customize the visual representation (i.e., set background color, text font and color, flashing, or time bars) of the following types of data:

- Officer Team: Fields with names of specific Officer Teams (e.g., Front Entrance, Lobby).
- Officer Status: Fields with specific Officers' Statuses (e.g., On Route, On Scene).
- **Organization Status**: Fields with specific Organizations' Statuses (e.g., Waiting, On Route, Cleared).
- **Priority:** Fields with specific activity Priority values (e.g., High, Medium, Low, Caution).
- **Location**: Fields with specific activity location (i.e., Site, Building, Location, Section) values (e.g., Site C/Building 1, Alberta/Edmonton/Downtown)

Moreover, using the **Regulated Time to Act** feature, you may set amounts of time to act for officers that have been assigned a specific officer status, have been placed to a specific location and/or dispatched for an activity with a specific priority. With an equivalent **Officer Alerts** feature, you may also specify the set amounts of time for officers' Status changes.

Define Visual Representation for Certain Data Types

In order to set up visual alerts for the future use in Perspective DispatchLog, click **Visual Alerts** on the Navigation pane. Using the first five tabs of the component, you may define the visual representation (i.e., the font and the background color) for the fields that differentiate various **Officer Teams**, **Officer Statuses**, **Organization Statuses**, **Priorities** and **Locations**.

Activities										
Activity Number	Priority 7	7 Officer Status 🗸	RTA Start Dal	Time Rer	Call Category	Location	Off Site	Reported Date/	Organization Status	Description
ACT1-2011-000105	Low	Waiting			Security	Site B/Building 1		2:47 PM		Officer working at CapE
ACT1-2011-000101	Low	Waiting			General	Site C/Building 1		2:10 PM		Assist SPD with arrest of
ACT1-2011-08-00013	Extreme	Waiting			Dangerous Conditi	British Columbia		31/08/2011		
ACT1-2011-08-00012	Minimual	Waiting			Alarm	British Columbia		31/08/2011	On Route	
ACT1-2011-08-00010	Important	Waiting			Dangerous Conditi	British Columbia		31/08/2011		
ACT1-2011-000103	Minimual	On Scene			Security	Site D/Building 1		31/08/2011		Officer attending Toront
ACT1-2011-000005	High	Waiting			Bomb Threat			31/08/2011		
ACT-2011-000022	High	On Scene			Bomb Threat			15/08/2011	On Route	
ACT-2011-000020	High	On Route			Alarm/Panic	Site A		12/08/2011	On Route	

- 1. Open the appropriate tab (e.g., Officer Team, Priority, Location).
- 2. Click Add New.
- A blank alert window will pop up. In the lookup, select the descriptor(s) of the category for which you wish to edit the format (e.g., Officer Team, Priority, Site/Building/Location/Section). For Location, check the Off Site box to indicate that the location is off-site.
- 4. Using the color lookups, select the **Background** and the **Text Colors** for the field of the selected category.
- 5. Check the Bold, Italic, Underline and/or Strikethrough boxes to add further font effects.
- 6. Preview the resulting field view below and click **OK**, if the result corresponds to your expectations.

🕂 🔶	ld New Record			- • •
ОК	Cancel			
	Site Acme University Building Administration Building Location Section	•	Format Format Background Color Text Color Bold Italic Underline Strikethrough Preview	
			Sample	

7. Add as many visual specifications to as many of the available categories as necessary. Click **Save**.

Visua	I Alerts					
🚽 Save 🔞 Ca	ncel					
Officer Team Officer Status Organization Status Priority Location Regulated Time To Act (RTA) Officer Alert						
= <u>Add New</u> = <u>Edit</u> = <u>Remove</u>						
Total : 5						
Preview	Off Site	Location	n			
Sample		Site C/Building 1				
Sample		Site D/Building 1				
Sample		Alberta/Edmonton				
Sample		British Columbia				

Create a New Regulated Time to Act (RTA) Alert

To create a new RTA alert for a dispatched activity in Perspective DispatchLog, open the **Regulated Time to Act (RTA)** tab and define the settings of the alert (Officer Status, Location and activity's Priority). Once activated in DispatchLog, the settings defined for the alert will cause the RTA timer to start counting the time the dispatcher is left to check and modify the status of the dispatched officer.

For example, you may set a specific regulated time to act (e.g., 10 minutes) for a "High Priority" activity for which an officer has been dispatched with the status "On Scene" who has now reached the location "Acme University/Administration Building". Then, as soon as the officer under all these conditions is dispatched for a matching activity in DispatchLog, the dispatcher will see the timer on their screen counting the time during which the officer is supposed to respond to the current combination of conditions.

If, for some reason, the officer failed to respond about their status change during the allotted period of time, the timer will start counting the time the officer spends in the set conditions after the RTA expiry, advancing in negative values. The display of the RTA time bar will change to flashing red to alert the dispatcher on the absence of an adequate response to the activity.

Note: The only obligatory condition for the timer to set on is the allocation of an RTA alert to a particular **Officer Status**. The officer's location and priority of the activity the officer is involved can be optionally added to restrict the set of activities to the particular combination of settings.

ivities										
Activity Number	Priority	Officer Status	RTA Alert	Time Remaining	Call Category	Location	Off Site	Reported Date/	Organization Status	
ACT1-2011-00010	Low	Waiting			General	Site C/Building 1		01/09/2011) with arrest of
ACT1-2011-08-0001	Extreme	Waiting			Dangerous Condit	British Columbia		31/08/2011		
ACT1-2011-08-0001	Minimual	On Scene			Alarm	British Columbia		31/08/2011	On Route	
ACT1-2011-08-0000	Important	On Route	57 %	00:00:30	Emergency Call/91	Alberta		31/08/2011		
ACT1-2011-08-0000	Minimual	Waiting			Escort	Alberta		31/08/2011		
ACT1-2011-000103	Minimual	On Scene			Security	Site D/Building 1		31/08/2011		ending Toront
ACT-2011-000020	High	On Route			Alarm/Panic	Site A		12/08/2011	On Route	
				RTA Alert	Time Rem	aining				
				41 %	00:00:	17				
				21 %	00:00:	02				

To create a new RTA alert, follow the steps below:

- 1. Click Add New. A new entity form will pop up.
- Specify the Site, Building, Location and/or Section for which you are setting the alert, selecting as many restrictive location options as necessary from the lookups. Check the Off Site box, if necessary.
- 3. Set the **Officer Status** that is intended to initiate the timer of the alert.
- 4. Make the timer respond to a particular activity priority by specifying the **Priority** setting for the alert.
- 5. Define the amount of time during which the dispatcher is supposed to respond to the activity with the set combination of conditions under the **Time Allowed** fields.
- 6. Click **OK**. The RTA table will populate with the new activity alert.

🕂 Add New Record	
OK Cancel	
RTA Details	
Site	Officer Status
Acme University 👻	On Scene 👻
Building	Priority
Administration Building 👻	High 👻
Location	
East Wing 👻	Off Site
Section 🗸	Time Allowed (less than 24hrs)
Leave Site Rollup blank to apply alert to any site selection	

7. To edit an RTA alert, select it in the grid and click **Edit**. To delete an alert, select it in the grid and click **Remove**.

Save 🔞 Cance	1						
Officer Team Officer Status Organization Status Priority Location Regulated Time To Act (RTA) Officer Alert							
Add New Edit Remove Total : 3							
Total : 3							
Total : 3 Officer Status	Priority Code	Site Rollup	Off Site		Time Allowed		
	Priority Code Extreme	Site Rollup British Columbia	Off Site	3 Min.	Time Allowed		
Officer Status			_	3 Min. 1 Min.	Time Allowed		

Create a New Officer Alert

To create a new time alert for an officer in Perspective DispatchLog, open the **Officer Alert** tab and define the settings of the alert (Officer Status and Location). Once activated in DispatchLog, the settings defined for the officer alert will cause the available or assigned officer's RTA timer to start counting the time the officer is left to act in the set status and/or at the set location.

For example, you may set a specific regulated time to act (e.g., 20 minutes) for an officer whose status has switched to "On Scene" and who has now reached the location "British Columbia". Then, as soon as these conditions activate in DispatchLog for this officer, the dispatcher will see the timer on their screen that will count the time for the officer to respond to the current combination of conditions before their status must be modified.

If, for some reason, the officer failed to respond about their status change during the allotted period of time, the timer will start counting the time the officer spends in the set conditions after the time alert expiry, advancing in negative values. The display of the time bar will change to flashing red to alert the dispatcher on the absence of an adequate response from the officer.

As with the RTA alerts for activities, the only obligatory condition for the officer's timer to set on is the allocation of a time alert to a particular **Officer Status**. The officer's location can be optionally added to restrict the population of officers to the particular location.

Assi	gned						
V	Team ▽	Call ⊽ Sign ▽	Officer/Organization Name ∀	Status 7	ActivityID	Location V	Time Elapsed ♡
8	P3	133A	Dargie, Nancy	On Route	ACT1-2011-000417		5d 23h
8		PPM-002	Watson-Parker, Mary-Jan	On Route	ACT1-2011-000416	Acme University/Administration	2d 23h
8	P2	130B	Sieben, Jeff	On Scene	ACT1-2011-000414		00:00:09
						Time Elapsed ⊽ 00:00:04 00:09:19	

To create a new Officer alert, follow the steps below:

- 1. Click **Add New**. A new entity form will pop up.
- Specify the Site, Building, Location and/or Section for which you are setting the alert, selecting as many restrictive location options as necessary from the lookups. Check the Off Site box, if necessary.
- 3. Set the **Officer Status** that is intended to initiate the timer of the alert.
- 4. Define the amount of time during which the officer is supposed to respond to the activity with the set combination of conditions under the **Time Allowed** fields.
- 5. Click **OK**. The Officer Alert table will populate with the new officer alert.

🖶 Add New Record	
OK Cancel	
RTA Details	
Site	Officer Status
Acme University 👻	Patrol 👻
Building	
Administration Building 🔹	
Location	
	Off Site
Section	Time Allowed (less than 24hrs)
Leave Site Rollup blank to apply alert to any site selection	

6. To edit an officer alert, select it in the grid and click **Edit**. To delete an alert, select it in the grid and click **Remove**.

Save 🔞 Cance							
Officer Team O	fficer Status	Organization Statu	s Priorit	ty Locati	on Regulat	ed Time To Act (RT	A) Officer Alert
Add New	Edit Rei	move					
Total : 3							
Total : 3 Officer Status	500100	Site Rollup		Off Site		Time Allo	owed
Officer Status	Alberta	Site Rollup		Off Site	20 Secs.	Time Allo	wed
	Alberta British Colu			Off Site	20 Secs. 15 Min.	Time Allo	wed

Language

The Language section allows you to set Perspective's operating language and, if desired, custom help files.

Languages

The Languages section—not to be confused with "Language" above it—allows you to set language names and associated help paths.

Note that Perspective comes pre-installed with a default language (**System English**) and associated help files. Only set additional languages if you need either new English terminology or non-English languages.

Eanguage -> Configuration							
Configuration Form Labels							
Save							
Base Language	Dictionary English (United States) Admin Help Path /languages/en_us/help/perspectiveadminh elp/perspectiveadminhelp.htm						
Healthcare							
Education							
Casino/Hotel	User Help Path Image: User Help Path						
Language 4							
Language 5							
Language 6							

Set Languages and Help File Paths

- 1. Select a dictionary to use in the **Dictionary** drop down box.
- 2. In the Admin Help Path and User Help Path fields, type the path for the language's associated help files, or click the Browse (...) button and browse to the appropriate file on your computer or network.
- 3. Click Save.

Form Labels

The Form Labels section provides lists of text fields that display throughout the Perspective interface, and are tied to the selected Perspective language. In order to set new or modify existing labels, open the **Form Labels** component, under **Language**, in the Navigation pane. On the right pane, a list of text fields will be displayed that specifies the selected entity. The first two columns of the list provide the string **ID** and the default **System English** label for each text field.

Create a Single Custom Label Set for All Users

- 1. Use the Language to Search section to bring up the field names you wish to change.
- 2. Enter your custom field label in the Base Language text field. The Custom English column will automatically populate with the new field label. As soon as a new label name is added to the Custom English column, Perspective defaults to this name rather than the original System English label. If you would prefer to have different users see different field labels, refer to the "Create a Custom Label Set for Each User Group in Your Organization" chapter for more information.
- 3. Continue assigning custom field labels.
- 4. Click **Save**. The next time any user without an assigned custom language logs on, they will see the new Custom English labels rather than the original System English labels.

Create a Custom Label Set for Each User Group in Your Organization

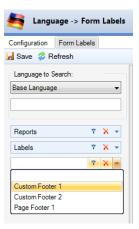
- 1. Use the **Language to Search** section to bring up the field names you wish to change.
- 2. Enter your custom field label in the text field that corresponds to the customized language that you created previously.
- 3. Continue re-labelling fields for your customized language. The column for your customized language will automatically populate with the new field labels you create.
- 4. Click **Save**. If you have already assigned your customized language to some users, your custom field labels will appear the next time they log on.

Create Custom Report Footers

Custom report footer labels are normally hidden from view, as the labels themselves are blank, and therefore not searchable.

Report footers are added to the end of a report and are listed in Perspective as **Custom Footer 1** and **Custom Footer 2**. **Page Footer 1** is added to the bottom of each report page.

1. Under the **Language to Search** section, drill-down to **Reports**, then **Labels**. The third drilldown contains the custom report footers.



- Custom Footer 1 appears in bold at the end of a report.
- **Custom Footer 2** appears as a sub-heading to Custom Footer 1. Custom Footer 2 is not bolded.
- **Page Footer 1** appears in small text at the bottom left of every page.
- 2. Enter custom footer text in the language label sets required.

The following sample report shows custom footers in effect:



Incident Record Created By PPM2000, 9/18/2011 4:18 PM GMT Last Modified By FKennedy, 12/14/2011 7:14 PM GMT

Owner Work	group
Doons	6
This is Page Footer 1.	

Access Level: Level 1 (Lowest) Local Print Date/Time: 2/5/2013 2:13 PM Page 1 of 1

Gateway Administration

Once a member of your organization has submitted an electronic report to the Gateway or imported a file into the Gateway, the Gateway Administrator and/or Gateway Approver are responsible for the assessment of the report.

Note: Incident, Item, Person, Organization and Vehicle reports can be imported through the Import Manager.

Before any of the steps in this reporting process take place, the Perspective Administrator must first permit workgroups to import files into the Gateway and/or grant Perspective e-Reporting and/or Web Portal access to workgroups, as well as authorize Gateway Administrators and Gateway Approvers to perform their associated Gateway functions.

Note: For more information on these roles and what they entail, consult the Perspective User's Guide or Perspective's online User Help.

In this guide, the term *e-Incident* refers to the electronic reports submitted both via Perspective e-Reporting (the so-called *e-Reports*), and via the rest of the possible Perspective's electronic submission methods, such as Perspective's Web Portal.

Specify Gateway File Import and/or e-Reporting Access Options for a Workgroup

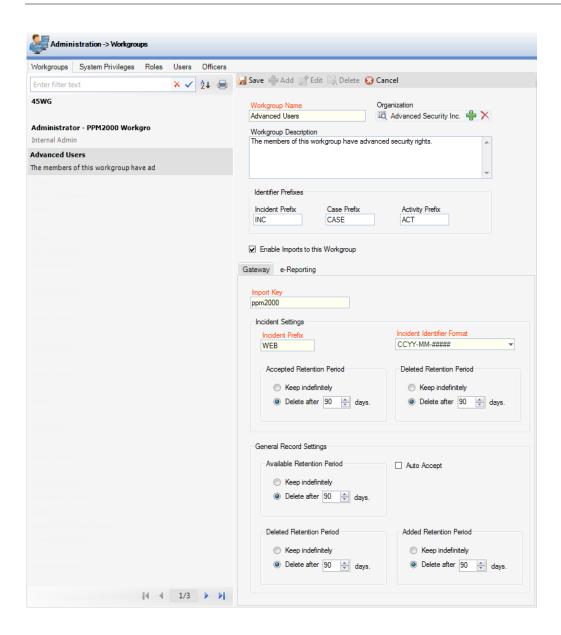
In order to enable smooth data communication between Perspective's electronic submission devices and Perspective Gateway, the Perspective's Administrator must permit workgroups to import files into the Gateway and/or grant e-Reporting and/or Web Portal access to appropriate workgroups.

- (w) The workgroups that will be working with Perspective e-Reporting should have limited visibility to GeoRollups (see the "Specify workgroup visibility for a lookup list" chapter for details). Large lists may cause e-Reporting to hang or crash.
- 1. Select **Workgroups** in the Navigation pane, choose the correct workgroup from the list, and click **Edit**.
- 2. Check the **Enable Imports to this Workgroup** checkbox. The Gateway opens by default.
- 3. Under the **Gateway** tab, start specifying Gateway file import options for the workgroup by providing the workgroup with a unique **Import Key**. This import key will act as an added security measure, restricting imports to the authorized workgroup only.

- 4. In the **Incident Settings** section below, specify a unique **Incident Prefix** for all of the workgroup's e-Incidents. For example, *WEB* for e-Reports and *EINC* for some other type of electronic reports (e.g., reports from Perspective Web Portal).
- 5. Choose an **Incident Identifier Format** from the lookup list:
 - CCYY-MM-#####: This format identifies the e-Incident by the calendar year (CCYY) and month (MM) that the report was submitted to the Gateway, followed by a five digit sequential number that re-sets at the beginning of each month. For example, 2011-03-00123 identifies the 123rd e-Incident submitted to the Gateway in March 2011.
 - CCYY-######: This format identifies the e-Incident by the calendar year (CCYY) that the report was submitted to the Gateway, followed by a six digit sequential number that re-sets at the beginning of each year. For example, 2011-004567 identifies the 4567th e-Incident submitted to the Gateway in 2011.
 - ##########: This is known as flat file format. There is no year or month preceding the number. The first e-Incident submitted to the Gateway will be identified by the number 0000000001, and this sequential numbering will continue indefinitely with no re-set.
- 6. Specify an **Accepted Retention Period** and a **Deleted Retention Period** for how long imported Item, Person, Organization or Vehicle reports should remain in the Gateway after they have been accepted or deleted by the Gateway Approver or Gateway Administrator.
- Indicate how long imported e-Incidents should remain in the Gateway after they have been made available or deleted by the Gateway Administrator or Gateway Approver under Available Retention Period and Deleted Retention Period.
- 8. Under **Added Retention Period**, specify how long imported Item, Person, Organization or Vehicle reports should remain in the Gateway after they have been added to the main Perspective database by authorized users.
- 9. In the **General Record Settings** section, check the **Auto Accept** box to automatically accept every Item, Person, Organization or Vehicle report that the workgroup imports, making them available for authorized users to add to the Perspective database. If this box is not checked, the workgroup's imported reports will undergo the normal Gateway review process by a designated Gateway Administrator or Gateway Approver prior to being made available or being deleted.

This box does not apply to imported Incident reports. Incident reports must always undergo Gateway assessment and review before being accepted into the Perspective database.

10. Click Save.



Assign Access Rights to a Gateway Administrator or Gateway Approver

- 1. Select **Users** in the Navigation pane.
- 2. Select the correct user from the list, and click Edit. By default, the General tab will open.
- 3. Open the User Rights sub-tab.
- Check the Gateway Administrator box or the Gateway Approver box to grant the user access to their associated Gateway functions.

5. Click **Save**. The next time the designated Gateway Administrator or Gateway Approver logs on to Perspective, they will be able to access the Gateway component from the Navigation pane.

 General Settings General 	Administration -> Users			
Account Policies Currencies Languages Administration Workgroups	Workgroups System Privileges Roles	Users Officers		
	davis	X 🗸 👌 🖶	🛃 Save 🖷 Add 📝 Edit 🔀 Delete 🔞 Can	cel
	Davis, Sueann		General Privileges Reports Audit Histor	ry
System Privileges	sd1	MSRole1	User Details User Defaults User Rights	
Roles Users Officers Auditing Form Labels	Davis, MSSueann sd2	MS - Role1	User Rights	
	Davis, Ian davis	Security Managers	Administrator Sub Administrator	Full History Access
Lookups Flags SOP			Investigator Supervisor	View Audit History
Visual Alerts			GeoRollup City Edits	Allow Locking Records
			Gateway Administrator	Allow Unlocking Records
			Gateway Approver	Allow Sealing
			Visual Analysis Access	Allow Editing All Narratives/Summaries es
			Quick Find Access	Allow Focal Point Access
				Allow Merge Entities
			Allow Dispatchlog Access	
			User Locked	

Administrative Reports

Perspective contains a number of pre-set reports that you may use to generate statistics and analyze trends in your data, and many of them have been designed specifically for Administrators.

For information on the types of reports available in Perspective, including administrative reports, and on how to generate reports, please, refer to the "Reports" section of the *Perspective User's Guide* or online User Help.

To read more about administering report access for roles and users, see "Set Report Visibility for a Role" and "Set Report Visibility for a User" in the "Roles" and "Users" sections of this guide.

Service Manager

The Service Manager is an external application available only on the Web server hosting Perspective services. It is used to manage configuration files, databases, licenses and keys, as well as to set up the following features:

- *Email Notifications*: Perspective's default email settings can be configured for either Microsoft[®] Outlook[®] or SMTP integration.
- **Attachment Sizes**: The maximum attachment size allowable in Perspective (up to 2 GB) can be tailored to your organization's needs.

Note: Microsoft SQL Server[®] 2005 Express (supported for the Standard Edition of Perspective only) has a maximum attachment allowance of 50 MB.

- **Quick Find Indexing**: The Quick Find tool requires regular indexing of your Perspective database for search accuracy.
- **User Defined Fields**: User defined fields can be added to the Incident, Case (Perspective Premium only), Item, Person, Organization and Vehicle forms under the General tab; to the Incident and Case forms under the Controls tab; and to the Incident form under the Involved Persons, Involved Items, Involved Organizations, Involved Vehicles and Investigation Details tabs.
- **Custom Search Integration**: With the Custom Search feature, you can launch the Infoglide Identity Resolution Engine[™] (IRE) from Perspective to search several data sources at once.
- Mass Notification: With the mass notification feature, you can integrate your MIR3[™] inEnterprise[™] solution into Perspective in order to launch notification via Perspective DispatchLog. This will require the Service URL, User Name and Password provided by MIR3
- **Integration Services URL**: To enable event trigger in Integration Services, enter the URL set up with the Integration Services.

For further information on any of the features listed above, including detailed setup instructions, please, refer to the *Perspective Installation Guide*.

Index

Α

Access Levels	
About	11
Role	26
System	22
User	35
Administration	
Gateway Se	e also Gateway
Administration	
Navigation	10
All Records View	17
Audit Logs	
System Level	47
User Level	42
Authentication	7

С

Child Field	50
Contact Information	
PPM 2000	85
Technical Support	85
Currencies	
Role Level	26
System Level	19
User Level	35
Custom English	.49, 73
Custom Search	
Access for Roles	27
Access for Users	37
Setting Up	80

D

Discrepancies	
Role vs. User Report Visibility	33
Role vs. User Rights	32
System vs. Role and User Rights	24

Е

Emails
LIIIdiis
Formatting17
Setting Up Notifications80

F

Flags	
Adding	58
Focal Point	
Access for Roles	27
Access for Users	37
Fonts	17
Form Labels	
Creating a Single Label Set	73
Creating Multiple Label Sets	73

G

Gateway Administration	
Designating Administrators and	
Approvers7	78
e-Reporting Access Options7	75
Importing Options21, 7	75
Gateway Administrator	
Access for Roles2	28
Access for Users	38
Designating7	78
Gateway Approver	
Access for Roles2	29
Access for Users	38
Designating7	78

Н

Help	
Contents	8
Help files	7
Index	9
Search	9

I

Integration	Services		80
-------------	----------	--	----

L

Languages	
Role Level	
System Level	73

User Level Legal Notices	
Logon Options	
Displaying Legal Notices	17
Displaying Privacy Statements	17
Password Parameters	18
Perspective Authentication	7
Setting for User	
Windows Authentication	34, 43
Lookups	
Adding Flags	58
Addresses for Site Rollups	54
Call Codes for Call Category Ro	llups
	53
Multi-Tier	49
Multi-Tier/Hierarchical Lists	50
Setting Workgroup Visibility	52
Single-Tier	49
Single-Tier Lists	49

Μ

Mass Notifications80	С
Measurement System	
System Level10	6
User Level	6

0

Officers	
Adding	43
Organizational Rollups	
About	11
Role Level	26
Setting Workgroup Visibility	52
User Level	35

Ρ

Parent Field	50
Password Parameters	18
Perspective Services URL	7
Privacy Statements	17
Privileges	
Assigning to Roles	30
Assigning to Users	39

Q

Quick Find	
Access for Roles.	27
Access for Users.	37
Indexing	80

R

Regulated Time to Act (RTA)	68
Reports	
About	79
Incident Site Addresses	55
Setting Visibility for Roles	32
Setting Visibility for Users	
System Level Cover Page	16
User Level Cover Page	
Workgroup Level Cover Page	21
Rights	
Assigning to Roles	27
Assigning to Users	37
Roles	
About	12
Access Privileges	
Accessing Custom Search	
Accessing Focal Point	
Accessing Quick Find	
Accessing Visual Analysis	
Adding	
Currency	
Discrepancies from System Rights	
Discrepancies from User Report	
Visibility	33
Discrepancies from User Rights	
General Rights	
Language	
Security Controls	
Setting Report Visibility	
Setting System Visibility	
Rollups	
Entering Addresses for Site Rollup	s 54
Entering Call Codes for Call Catego	
Rollups	
GeoRollups Visibility for e-Reportir	
	•
Modifying	
, ,	

OrganizationalSee also Organizational Rollups

Root	 	 50

S

Security Layers11
Service Manager80
Settings
Creating10
Deleting10
Editing10
Saving10
Sibling Field50
SOP
Add a Checklist61
Add a Link64
Attach a File62
Create a New Rule60
Set Up Notifications65
System Administration
Audit Logs See also Audit Logs
Components13
Flags
Form Labels See also Form Labels
General Settings See also System
Settings
LookupsSee also Lookups
OfficersSee also Officers
RolesSee also Roles
Security Layers11
Standard Operating Procedures See
also SOP
System Privileges See also System
Privileges
UsersSee also Users
Visual Alerts See also Visual Alerts
Workgroups See also Workgroups
System Privileges
Access Rights22
System vs. Role and User
Discrepancies24
Visibility22
System Settings
About12
Activity Numbering16
Activity Prefixing16

Attachment Sizes	80
Case Numbering	16
Case Prefixing	16
Currencies	19
e-Incident Numbering	76
e-Incident Prefixing	75
Fonts	17
Formatting Emails	
Hiding All Records View	17
Incident Numbering	16
Incident Prefixing	16
Measurement System	16
Notes upon Logon	17
Password Parameters	18
Report Cover Page	16
User Defined Fields	80

т

Technical	Support			.85
-----------	---------	--	--	-----

U

Users	
About	.12
Access Privileges	.39
Accessing Custom Search	
Accessing Focal Point	.37
Accessing Quick Find	.37
Accessing Visual Analysis	.37
Adding	.34
Audit Logs	.42
Currency	.35
Discrepancies from Role Report	
Visibility	.33
Discrepancies from Role Rights	.32
Discrepancies from System Rights.	.24
Gateway Administrators	.78
Gateway Approvers	.78
General Rights	78
Language	.35
Report Cover Page	.35
Security Controls	.35
Setting Report Visibility	.41
Setting System Visibility	. 39

۷

Visual Alerts	
Add Officer Alert	70
Add RTA Alert	68
Define Visual Representation of	
Certain Data Types	66
Visual Analysis	
Access for Roles	27
Access for Users	37

W

Workgroups

About	11
Activity Prefixing	21
Adding	21
Assigning to Roles	26
Assigning to Users	35
Case Prefixing	21
e-Reporting Access Options	75
Importing Options	.21, 75
Incident Prefixing	21
Lookup List Visibility	52
Report Cover Page	21

Contact Information

Technical Support

Toll Free:	1-877-776-2995
Phone:	(780) 448-0616
Email:	support@ppm2000.com

PPM 2000

Toll Free:	1-888-PPM-9PPM (1-888-776-9776)
Phone:	(780) 448-0616
Fax:	(780) 448-0618
Email:	information@ppm2000.com
Website:	http://www.ppm2000.com

WHEN YOU THINK 'INCIDENT MANAGEMENT' — THINK PPM. www.ppm2000.com

Copyright © PPM 2000 Inc. All rights reserved. PPM 2000, the PPM 2000 logo, Perspective by PPM 2000, the Perspective by PPM 2000 logo, Perspective by PPM, the Perspective by PPM logo and Perspective Focal Point are trademarks or registered trademarks of PPM 2000 Inc. Printed in Canada 09/13.

