Perspective™

by PPM

GETTING STARTED GUIDE

Printed October 2014

Copyright © 2014 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. Licensed users may print additional copies of this document for internal use only. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any other purpose, without the express written permission of PPM 2000 Inc.

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

Contents

Getting Started with Perspective™ by PPM 2000

Before getting started with your implementation of Perspective by PPM 2000, you must understand what Perspective is, and all that is involved in the implementation process.

Perspective is a highly configurable Consumer Off The Shelf (COTS) program, permitting individual companies the ability to configure the data elements (individual fields), system inputs (various lists), data record security, and form and field level security.

Each of these configuration pieces will be explained in this document.

Below is a list of all the steps/tasks you will need to address as a project team before you can “Go Live” with Perspective. The amount of time spent on each step or task is dependent on each company, as there are some pieces that are required for all companies and others that are dependent on company needs.

Steps/Tasks Required

There are seven steps to implementing Perspective:

1. **PLAN YOUR TEAMS.** Know who is responsible for what task(s) at what stage of the project.
2. **REQUIREMENTS GATHERING.** Know what your needs are, and document them in a clear and easy to understand format. These requirements will drive many portions of the following steps/tasks, and consist of the following processes:
   a. Planning your output/reporting requirements.
   b. Planning your system inputs (various lists that exist within the program).
   c. Adding single level lookups that are tied to the lists.
3. **OUTLINE YOUR USERS AND GROUPS OF USERS.** Understand who your users will be and group them into functional groups. This section will deal with two areas of security:
   a. Data Segregation or Record Level Security—identify who gets to see what incidents.
   b. Form and Field Level Security—identify how they interact with the records that they see.
4. **IDENTIFY YOUR USE OF THE PERSPECTIVE PORTAL.** Determine who will use it, how they will use it, and their purpose for using it.
5. **IDENTIFY YOUR WORKFLOW NEEDS.** Identify from the existing Event Packages how workflow can be configured to automate notifications or tasks within Perspective.
6. **USER ACCEPTANCE TESTING.** Test the application, utilizing your requirements that have been gathered previously, and ensure the application accomplishes what has been identified in those requirements.
7. **“GO LIVE”.** Ensure your user base has the information necessary to move forward with Perspective. Finally, launch your Perspective system.

STEP 1 Plan Your Teams

There are three teams that need to be in place prior to, or identified early on in the implementation process. These teams are the planning committee, the user acceptance team, and the system Administrators. This chapter discusses these three teams in detail.

Planning Committee

The planning committee is comprised of individuals from throughout your company that will have a direct impact on the success of this project:

a. Project Manager or Project Champion: This person will organize the team and ensure various tasks are accomplished in an approved timeframe. This will be the core person who is in communication with the PPM Project Team.
b. Subject Matter Experts (SMEs): One or more people from each impacted team that will be utilizing the program.
c. Decision Maker: One or two individuals who are able to take the input of the group and focus the ideas into a single approach. The decision maker(s) provides answers to the PPM Project Lead’s usability questions.

Once the initial project to launch Perspective has been completed, this team can reconvene at intervals to discuss adjustments and improvements to the product that have been identified throughout the use of the application.

User Acceptance Team

The user acceptance team is comprised of individuals who will take the configured database and test it against the documented requirements, ensuring that the needs identified have been accomplished. It is best that this team have people who were not part of the SMEs from the planning committee but still understand the user’s needs in the reporting process, as the planning committee SMEs have been involved in the decision making. The user acceptance team often comes up with things that the planning committee missed.

Once the initial project to launch Perspective has been completed, this team can disband. Should a subsequent project be created, this team can be reformed with the same, or new, members.

System Administrators

The system Administrators will be responsible for the ongoing configuration needs of your system, including post "Go Live" of the application. There are several sections of Administration in Perspective, most of which can be assigned with separate rights. This permits your Administrator to be a single person (with backups in place) or multiple people with segregated duties. These Administrators will be responsible for the following tasks:

- General system settings.
- Password Policies.
- Currency Exchange Rate adjustment.
- Label set configuration and adjustment of labels throughout the program.
- Data segregation, Role & User adjustment/creation.
- Creating/editing values in your drop-down lists.
- Creation of incident and person record flags.
- Creation of officers for use within the Dispatching component.
- Standard Operating Procedure (SOP) creation and adjustment.
- Visual Alerts for use in Dispatching.
- Auditing.

Please stop here and configure these teams. Once that has occurred, continue reading so you can provide the various groups instructions on what to do next.

Your Teams Have Gathered

Now that you have your teams gathered, your first step is to teach them what Perspective is, and what it is capable of doing.

To assist with this process, we recommend all clients and all members of the above teams sit through some online training sessions to familiarize themselves with Perspective.

Perspective is available in the following 4 editions:

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

There are 5 orientation sessions per Perspective edition. The following link will take you to Perspective's online training site, where you can view a list of upcoming training sessions and register for them:

https://ppm2000.webex.com/mw0307l/mywebex/default.do?siteurl=ppm2000&service=7.

Initially, you will be looking for orientation sessions, which have SSP in front of the name. If you are having difficulty locating the correct sessions, please email our training department: training@ppm2000.com.

Once the orientation sessions have been attended, there are advanced sessions that go into Perspective's specific pieces in greater depth. You can attend as many or as few of these as desired, but they will assist you with preparing your various teams for the tasks ahead of them.

For clients that have purchased a Service Package, this online training does not replace the specific client-focused training that comes later in this guide.

Once your teams are comfortable with Perspective and the core pieces they will be using, move onto the next steps.

STEP 2 Requirements Gathering

Plan Your Output/Reporting Requirements

Once the planning committee has been established, their first step is to identify what the organization requires for outputs from the data that exists within Perspective.

First, review the Sample Reports document included in your documentation.

Once the planning committee has reviewed these reports, the next step is to review organizational-specific reporting requirements. Some examples of these are the following:

- Weekly reports
- Monthly reports
- Quarterly reports
- Annual reports
- Regular notifications

In reviewing these reports, you will need to identify two things: Data Elements and Data Segregation for Reporting Purposes.

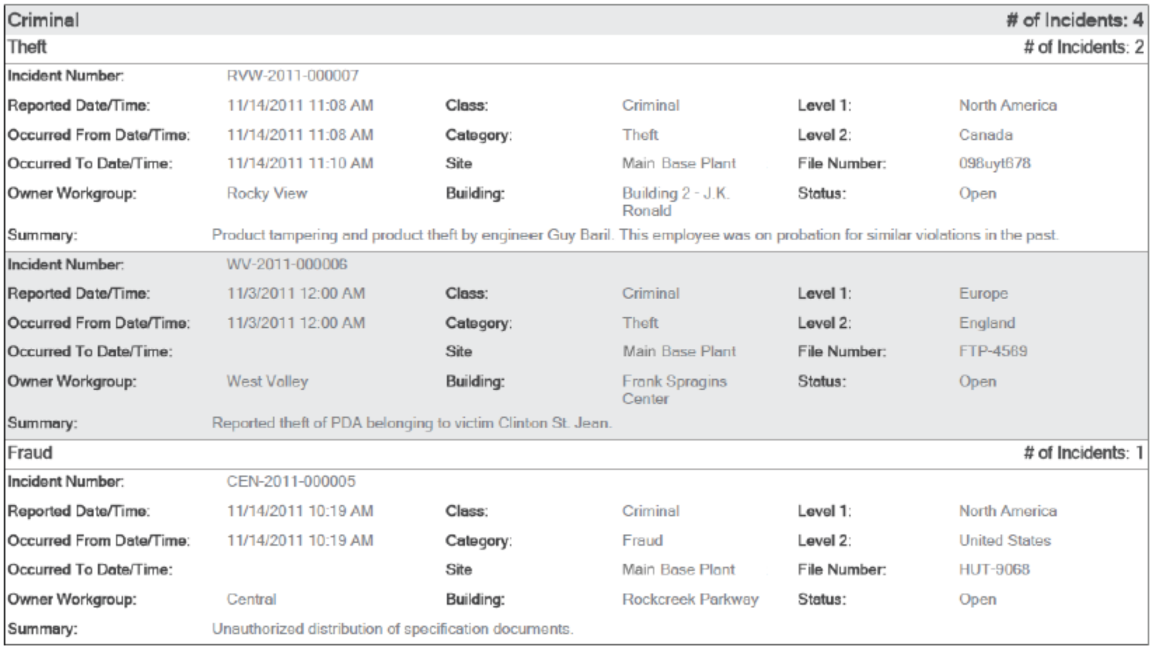
Data Elements

Ask yourself the following questions:

- What metrics are being measured?
- What data pieces are being listed out?
- What data do you need in order to calculate other data elements for these reports?
- What data elements are needed for your investigative process?

Data elements will need to be searched and can be pulled into the embedded Custom Report Designer, or into Microsoft Excel, for the purpose of manipulating that data to provide the report you would like. To provide that report, the data must either exist as individual data fields within Perspective or as a field that could be calculated from within Excel against one or more data fields within Perspective.

For example, if your report requires the age of an incident based on when it was reported to your organization, you would not specifically require a data field that shows the incident age. Minimally, you would need a field that identifies the date an incident was reported, and then we could calculate the age by subtracting that from the current date (a function within Excel).



Criminal					# of Incidents: 4
Theft					# of Incidents: 2
Incident Number:	RVW-2011-000007				
Reported Date/Time:	11/14/2011 11:08 AM	**Class:**	Criminal	**Level 1:**	North America
Occurred From Date/Time:	11/14/2011 11:08 AM	**Category:**	Theft	**Level 2:**	Canada
Occurred To Date/Time:	11/14/2011 11:10 AM	**Site**	Main Base Plant	**File Number:**	098uyt678
Owner Workgroup:	Rocky View	**Building:**	Building 2 - J.K. Ronald	**Status:**	Open
Summary:	Product tampering and product theft by engineer Guy Baril. This employee was on probation for similar violations in the past.				
Incident Number:	WV-2011-000006				
Reported Date/Time:	11/3/2011 12:00 AM	**Class:**	Criminal	**Level 1:**	Europe
Occurred From Date/Time:	11/3/2011 12:00 AM	**Category:**	Theft	**Level 2:**	England
Occurred To Date/Time:		**Site**	Main Base Plant	**File Number:**	FTP-4589
Owner Workgroup:	West Valley	**Building:**	Frank Spragins Center	**Status:**	Open
Summary:	Reported theft of PDA belonging to victim Clinton St. Jean.				
Fraud					# of Incidents: 1
Incident Number:	CEN-2011-000005				
Reported Date/Time:	11/14/2011 10:19 AM	**Class:**	Criminal	**Level 1:**	North America
Occurred From Date/Time:	11/14/2011 10:19 AM	**Category:**	Fraud	**Level 2:**	United States
Occurred To Date/Time:		**Site**	Main Base Plant	**File Number:**	HUT-9068
Owner Workgroup:	Central	**Building:**	Rockcreek Parkway	**Status:**	Open
Summary:	Unauthorized distribution of specification documents.				

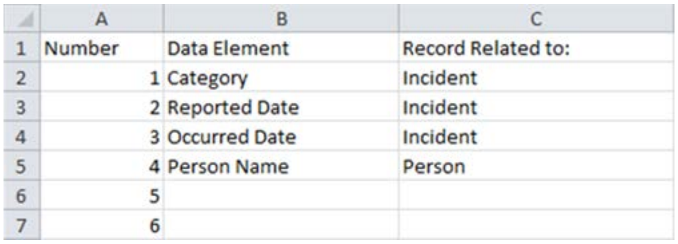
In the above example, there are 14 different data elements represented.

1. Incident Number
2. Reported Date/Time
3. Occurred From Date/Time
4. Occurred To Date/Time
5. Owner Workgroup
6. Class
7. Category
8. Site
9. Building
10. Level 1
11. Level 2
12. File Number
13. Status
14. Summary

If this is a report your organization needs, then we need to ensure the data from this report are individual fields identified within Perspective or could be calculated from individual fields.

This is a key step because without knowing what you need to get out of the system, you will have a difficult time identifying what needs to go into the system.

The initial documentation of this list can be done in the Excel Document, Output-Reporting Planning.xlsx. This document is located in the documents package.



	A	B	C
1	Number	Data Element	Record Related to:
2	1	Category	Incident
3	2	Reported Date	Incident
4	3	Occurred Date	Incident
5	4	Person Name	Person
6	5		
7	6		

In this document, there are 3 columns:

Column A (Number)—An incrementing number allowing us to identify the data element you are referencing. If more numbers are required, feel free to add to the 100 that are included.

Column B (Data Element)—A simplified name of the data you want to enter about something, or someone.

Column C (Record Related to:)—The type of entity the data element relates to.

There are 7 types of entities, and 4 types of sub-entities your data can relate to, and they can relate to multiple entities:

1. Activities
2. Incidents
   a. Involved Persons
   b. Involved Organizations
   c. Involved Items
   d. Involved Vehicles
3. Cases
4. Persons
5. Organizations
6. Items
7. Vehicles

Based on the above example, Person Name would relate to both Persons and Involved Persons. It would be best to list Person Name twice, and show the relationship for each entity.

Data Segregation for Reporting Purposes

Ask yourself the following questions:

- Does the report information get generated and sent to a group of people who all see the same information?
- Or, does the data generated get split into different reports so that one location gets a report, and the other location gets a different report?

Another example could be a report that lists all outstanding investigations and shows the investigator name. You may want each investigator to get a list of outstanding investigations, but only for investigations that he/she is the investigator of.

Required reports need to identify the different individuals or groups that would receive segregated data sets.

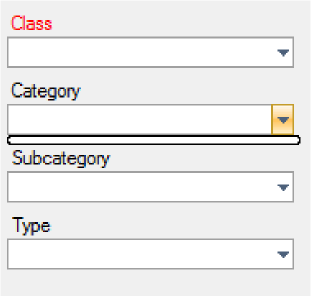
Document those segregations (if any) for future use.

Plan Your System Inputs

There are a number of drop-down lists available to populate with data specific to your needs. Drop-down lists (known as lookups in Perspective) fall into two categories: hierarchy lists and single level lookup lists.

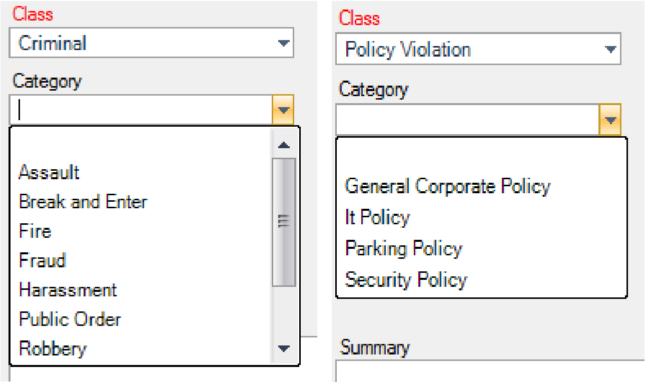
Category 1—Hierarchy Lists

Hierarchy lists consist of multiple breakdowns for your data. The values of one list are directly dependent on the data before it.



The above image appears to show that the Category field has no values in it. However, this is not accurate. It has no values showing because it has no value to filter on in the Class field.

The Class field must have a value in it so that the Category field knows what to filter on.



Class
Criminal

Category

Assault
Break and Enter
Fire
Fraud
Harassment
Public Order
Robbery

Class
Policy Violation

Category

General Corporate Policy
It Policy
Parking Policy
Security Policy

Summary

Above is an example of how the Category field filters based on the value of the Class field above it.

Incident Related Hierarchies

Class Rollups—Identifies what has happened that requires an incident to be documented (4-tier hierarchy).

Site Rollups—Identifies where something happened that requires an incident to be documented (4-tier hierarchy).

Business Unit Rollups—Identifies responsibility or ownership of the incident occurrence (4-tier hierarchy).

Activity Related Hierarchies

Call Category Rollups—Identifies what has happened that requires an activity to be documented (3-tier hierarchy).

Item Related Hierarchies

Item Class Rollups—Identifies groupings of items for reporting purposes (2-tier hierarchy).

Item Make/Model Rollups—Identifies an item's make and model (2-tier hierarchy).

Vehicle Related Hierarchies

Vehicle Make/Model Rollups—Identifies a vehicle's make and model (2-tier hierarchy).

General Use Hierarchies

Geo Rollups—Identifies the country, state/province, or city for use in addresses or vehicle license plate registration information (3-tier hierarchy).

Org Rollups—For use in data security. This is discussed further in the "Resolve the Issues" section (pg. 56) of this document (4-tier hierarchy).

Note: These definitions are PPM's definitions. The hierarchy lists can be renamed for your organization's needs.

Category 2—Single Level Lookup Lists

In addition to the hierarchy lists, there are out-of-the box lookup lists. While many are commonly used lists (Hair Color, Eye Color), others are less obvious (No Impact Methods).

Note: These lists can be renamed to suit your organization's needs.

Understanding the terms below will assist you when defining your lookup lists.

Activity

A single-occurrence action, often by a guard force, that is often a routine action, but can cross into the non-routine type of emergency calls. This is anything a guard force officer can respond to, or a duty they must perform. This type of documentation is minimal, unless the call crosses into an emergency call.

Incident

A single-occurrence event that is not a routine action, and may require significantly more in-depth documentation.

Case

A multiple-occurrence event, consisting of two or more Incident records.

Loss

A monetary loss that occurred in the course of the incident.

Recovery

A loss amount associated with an incident that has been restored or regained.

No Impact

A monetary amount that does not impact the Net Loss amount (Total Loss - Recovery = Net Loss). This can be a prevented loss or an expected recovery.

PPM’s definitions of the lookup lists are as follows:

ActivityDisposition—What step in your process is the activity at?	LinkVehicleTypes—How would two vehicles be linked?
ActivityStatuses—Is the activity open or closed with/without report?	LossCauses—What caused the loss?
AssignmentTypes—Type of assignments given to various people.	LossMethods—What was the technique of the loss occurrence?
AttachmentTypes—What type of file was attached?	LossStatuses—Was the loss a direct or indirect loss to the loss cause?
CallSign—Call signs assigned to each dispatched Officer.	LossTypes—What categorization of loss occurred?
CallSource—Source of the activity/dispatch call.	MaritalStatuses—A person’s marital status.
CaseCategories—Categorization of case records.	NarrativeTypes—Categorization of your incident narrative documents.
CaseDispositions—What step in your process is the case at?	NoImpactCauses—What caused the no impact amount?
CaseNarrativeTypes—Categorization of your case narrative documents.	NoImpactMethods—What was the technique of the no impact amount?
CaseStatuses—Is the case record open or closed?	NoImpactTypes—What categorization of no impact occurred?
ClothingColors—What color was the clothing?	NotifiedByTypes—How was your organization notified of an activity call?
ClothingTypes—What type of clothing was worn?	OfficerTeam—What team does your officer belong on?
DamageSeverities—Severity of the damage a vehicle incurred.	OrgAddressTypes—The type of address for an organization, allowing for distinction between multiple addresses.
Divisions—Departments an incident could be referred to.	OrganizationTypes—The type of organization identified.
EvidenceDispositions—What step in your process is your evidence at?	OrgEmailTypes—The type of email address for an organization, allowing for distinction between multiple email addresses.
EvidenceStatuses—Is the evidence secured in your control or not?	OrgInvolvementTypes—How an organization may be connected to an incident or activity record.
EvidenceTypes—Was the evidence found or seized from someone?	OrgPhoneTypes—The type of phone for an organization, allowing for distinction between multiple phones numbers.
ExpenseTypes—Types of investigative expenses that can be incurred.	OutcomePrimaryCauses—The primary root cause of an incident occurrence.
EyeColors—A person’s eye color.	OutcomeSecondaryCauses—The secondary root cause of an incident occurrence.
GenderTypes—A person’s gender.	PersAddressTypes—The type of address for a person, allowing for distinction between multiple addresses.
HairColors—A person’s hair color.	PersEmailTypes—The type of email address for a person, allowing for distinction between multiple email addresses.
IncDispositions—What step in your process is the incident at?	PersFeatureTypes—Types of distinguishing features for a person.

IncidentFlags—High level classification of an incident record.	PersIdTypes—Types of identification for a person.
IncidentStatuses—Is the incident record open or closed?	PersInvolvementTypes—How a person may be connected to an incident or activity record.
IncItemDispositions—Where is the involved item currently?	PersonFlags—High level classification of a person record.
IncVehicleDispositions—Where is the involved vehicle currently?	PersonTitles—How you address a person.
InjuryCauses—What caused a person's injury?	PersPhoneTypes—The type of phone for a person, allowing for distinction between multiple phone numbers.
InjurySeverityLevels—How severe is the injury?	Priority—The urgency/severity of an activity record.
InterviewTypes—What type of interview was conducted?	RecoveryMethods—What was the technique of the recovery?
InvestigatorTypes—The types of investigators utilized in your incident.	RecoveryTypes—What categorization of recovery occurred?
LinkActivityIncidentTypes—How would an activity and incident be linked?	RequestTypes—The types of requests made of an organization during an incident or activity.
LinkActivityTypes—How would two activities be linked?	ReviewTypes—The types of reviews documented on an incident or case record.
LinkCaseIncidentTypes—How would a case and incident be linked?	SeverityLevels—The level of urgency of a person record flag.
LinkCaseTypes—How would two cases be linked?	SubjectInvolvements—The incident involvement type of an interviewed person.
LinkIncidentTypes—How would two incidents be linked?	SummaryTypes—Categorization of an investigation narrative summary.
LinkOrganizationTypes—How would two organizations be linked?	TaskTypes—Types of tasks accomplished by incident investigators.
LinkOrgVehicleTypes—How would an organization and vehicle be linked?	VehicleColors—The color of a vehicle.
LinkPersonTypes—How would two persons be linked?	VehicleStyles—The style of a vehicle.
LinkPersOrganizationTypes—How would a person and an organization be linked?	VehInvolvementTypes—How a vehicle may be connected to an incident or activity record.
LinkPersVehicleTypes—How would a person and a vehicle be linked?	

To view the default values that Perspective ships with, please review Perspective40ConfigurationWorkbook.xlsx, located within the same package as this guide.

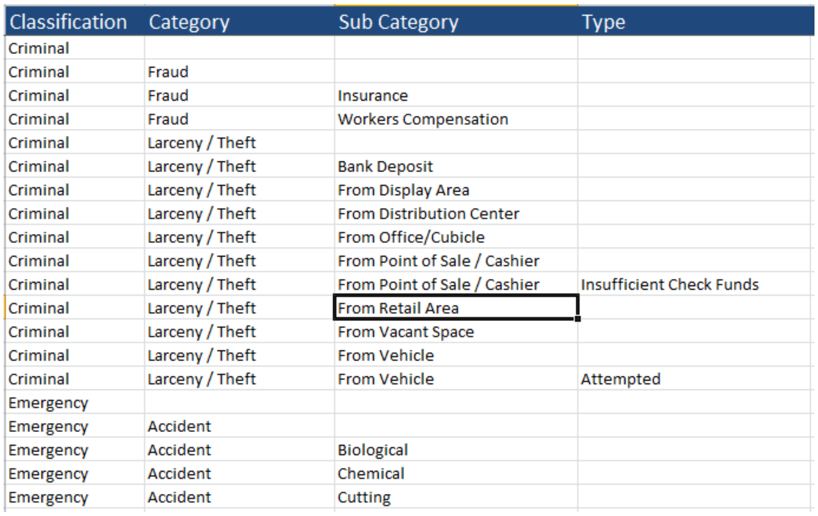
Documentation of Your Hierarchy Lists

Now that you understand what lists you need and what you have available, you can begin documenting this information.

Before entering the information into Perspective, it is best to first document these lists in the Perspective Workbook spreadsheet. This allows you to view, manipulate, and retain the lists for use in training and documentation review. Furthermore, is important to know that by default, all lookup values sort within their lists alphabetically. To force a non-alphabetical sort order, number your values for the order that you want to see them.

If you purchased a Services Package with the PPM Consulting & Training team, this workbook serves as a way for your Project Lead to review your work, and to move your data into a Perspective database, limiting the need for manual data entry.

Verify that the documentation is concise. PPM recommends that you duplicate the information within each column, on each row, as needed.



Classification	Category	Sub Category	Type
Criminal			
Criminal	Fraud		
Criminal	Fraud	Insurance	
Criminal	Fraud	Workers Compensation	
Criminal	Larceny / Theft		
Criminal	Larceny / Theft	Bank Deposit	
Criminal	Larceny / Theft	From Display Area	
Criminal	Larceny / Theft	From Distribution Center	
Criminal	Larceny / Theft	From Office/Cubicle	
Criminal	Larceny / Theft	From Point of Sale / Cashier	
Criminal	Larceny / Theft	From Point of Sale / Cashier	Insufficient Check Funds
Criminal	Larceny / Theft	From Retail Area	
Criminal	Larceny / Theft	From Vacant Space	
Criminal	Larceny / Theft	From Vehicle	
Criminal	Larceny / Theft	From Vehicle	Attempted
Emergency			
Emergency	Accident		
Emergency	Accident	Biological	
Emergency	Accident	Chemical	
Emergency	Accident	Cutting	

In the example above, you'll notice that the classification of Criminal is repeated for each row that represents a criminal act. It is also repeated for the category as each subcategory and type relate. As you can also see, it is not required for each set of values to go down to all four levels (or less, depending on which list you are working on).

You may also notice that Criminal exists in a row on its own. As does Criminal-Fraud, Criminal-Larceny/Theft, etc.

While this is not crucial for the Class Rollup list, this is a crucial note for your Site list and Activity Category list. These two lists have settings that can be utilized at all three or four levels of each list.

Note: The values used in the examples shown below are for illustration and example purposes.

Classification List

As described earlier, the Classification list identifies what happened that caused an Incident to be created. Classification lists should be anything that requires more detailed documentation. The key here is to not give your users so many, or unclear options that identifying what an incident is about is difficult. Creating lists can be difficult, but is the most crucial list to complete correctly, as it drives your organizational metrics.

Confirm that a concise list is available to your users. This means limiting the available options and making sure there is no chance of categorizing an incident as more than one option.

Below is an example of a classification list identifying a fire.

Class	Category	Subcategory	Type
Criminal	Arson		
Emergency	Fire	Smoke/Flame Present	
Emergency	Fire	Alarm Only	

If the scenario is that a fire was set intentionally, which of the above options would your users need to choose? Both the Criminal Arson and the Emergency Fire would work, which makes it difficult for your users to choose the correct option. This also prevents you from getting all of your data metrics appropriately. If some of your metrics are classified as Arson and others as Fire, you would need to merge this data before knowing the total number of incidents. A better solution is the following:

Class	Category	Subcategory	Type
Emergency	Fire	Arson	Smoke/Flame Present
Emergency	Fire	Accidental	Alarm Only
Emergency	Fire	Accidental	Smoke/Flame Present

Before moving forward, document your organization’s overall needs, and then evaluate based on confusion points.

Limit Your Options

The next thing your organization needs to evaluate is the number of options a user should have to choose from.

Your organization needs to identify all of the possible WHATs that could occur, and be able to document them. The degree of identification is what is being discussed here.

One of the more common physical security examples we see is the need to identify Bomb Threats.

Consider the following example:

Classification	Category
Emergency Response	Bomb Threat

This may not be enough of a breakdown of your information. You may require additional levels:

Classification	Category	Subcategory
Emergency Response	Bomb Threat	
Emergency Response	Bomb Threat	By Found Device
Emergency Response	Bomb Threat	By Note
Emergency Response	Bomb Threat	By Phone

Before you break down your categories or subcategories, identify the need for doing so. There may be no need to break down your information, because the data does little to further your metrics measuring.

This is often decided by the number of incidents you anticipate your organization needs to track. Based on the above example, the questions your PPM Project Lead should ask are the following:

- *How many Bomb Threats does your organization anticipate in a one-year period?*
- *Based on that number, what is the likelihood of needing to measure the details of that bomb threat?*

The detail of how the bomb threat was identified will be tracked in the narrative of the incident, through various notes, etc. But at the end of the year, are there enough bomb threat's identified to make it worthwhile to show the count of those details? The goal is to show a report at the end of the year that shows a limited number of zeros.

There is an equation that will assist you in identifying the best number of options, limiting the number of zeros in an annual report. Take the estimated number of incident reports written in one year and have a list length that is approximately 5-10% of that number. An approximate 1000 incidents written in one year would mean that there should be approximately 50-100 ways of segregating that data.

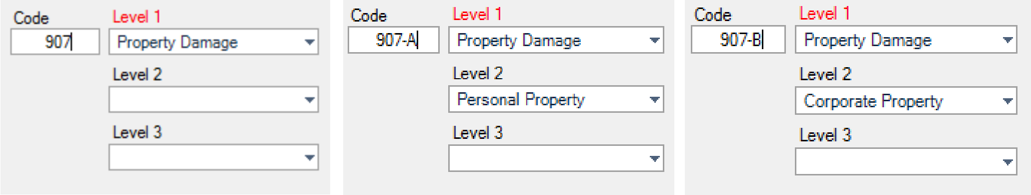
Activity Category List

Your Activity Category list is used to identify what happens with regards to your Activity records. These records will get into everything that occurs and needs to be tracked. This tracking has less to do with the detailed documentation and more to do with metrics for the purpose of the tracking of the duties. The Activity category list, while used directly within Activities, is also the primary list of the Dispatching component used to deal with documentation of an Activity from initiation, to deployment, and finally, response.

The rules of this list match that of the Incident Classification list, but there are two subtle differences that can have a major impact on the Dispatching component: Category Code and Priority.

Category Code

This code is a unique identifier for each potential value of the category list.



Code: 907
Level 1: Property Damage
Level 2:
Level 3:

Code: 907-A
Level 1: Property Damage
Level 2: Personal Property
Level 3:

Code: 907-B
Level 1: Property Damage
Level 2: Corporate Property
Level 3:

The example above shows that code 907 has a value of Property Damage only. On the other hand, code 907-A takes Property Damage and breaks it down a single level to Personal Property. Finally, code 907-B changes Level 2 from Personal Property to Corporate Property. Each value typed into the Code field helps identify the value needed in the Level 3 hierarchies.

Each value that is possible to choose (at any level of the hierarchy) does not require a code. As an example, you would not necessarily require identifying the 907 code for Property Damage in order to have a code for Personal Property or Corporate Property.

There are two restrictions for this field.

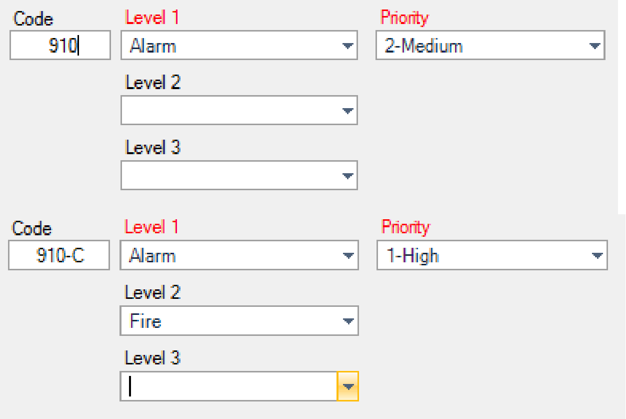
1. The code must be unique for each potential value. If a code is entered, Perspective must know exactly which value will be given.
2. There is a six character limit for the code. This character limit includes all alpha-numeric characters, special characters, and spaces.

Priority

The Priority field allows immediate identification of the urgency of a call. The default values of Perspective for this field are as follows:

1. High
2. Medium
3. Low

This list can be adjusted to show more or less options. The values can also be changed.



Code: 910

Level 1: Alarm

Priority: 2-Medium

Level 2:

Level 3:

Code: 910-C

Level 1: Alarm

Priority: 1-High

Level 2: Fire

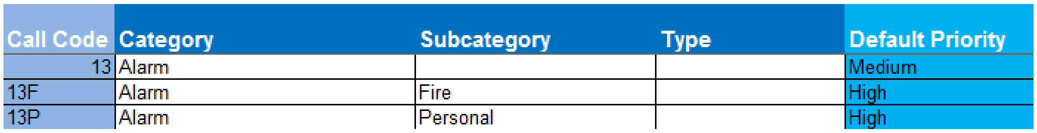
Level 3:

In the above example, an Alarm that has not been identified at Level 2 has a different default Priority than an Alarm for Fire (if chosen, as it is not a requirement to have a default Priority). The default value is only there for initial settings of the call but can be adjusted at any time.

To set what you want for Priorities, please refer to pages 32 and 33 of the Single Level Lookup Values section.

Documentation

The Category Code and Priority need to be considered, because depending on how you document your Activity list, you will allow or limit your options within a data push.



Call Code	Category	Subcategory	Type	Default Priority
13	Alarm			Medium
13F	Alarm	Fire		High
13P	Alarm	Personal		High

In the above example, if Alarm was not on its own line, it would not have been possible in the PPM automated data push to have a unique code, nor could it have had a different Priority.

Site List

Your Site hierarchy list is used to identify where something occurs. This list identifies the location where an event took place.

Site hierarchy is used in Activity data forms and Incident data forms. The WHERE for your records often requires different levels of detail.

Activities can usually be tracked to a room number, whereas incidents don’t require that level of breakdown. When building this list, make sure it will work for both data forms.

First, determine the data needed for a location breakdown. The out-of-the-box field names are as follows:

- Site
- Building
- Location

- Section

There is no requirement for the data to equate to those labels, unless your data points will work with these values. This is the case for some clients. They track a Site, Campus, or Property area. Then the various buildings within each campus are listed, as well as the locations and sections within those buildings.

Other clients, however, may not need to get into that kind of detail. There can be variations of this list, including, but not limited to, the following:

- Region (such as EMEA, North America, APAC)
- Country
- City
- Property

Or

- Region (East, West, Central)
- State
- City
- Property

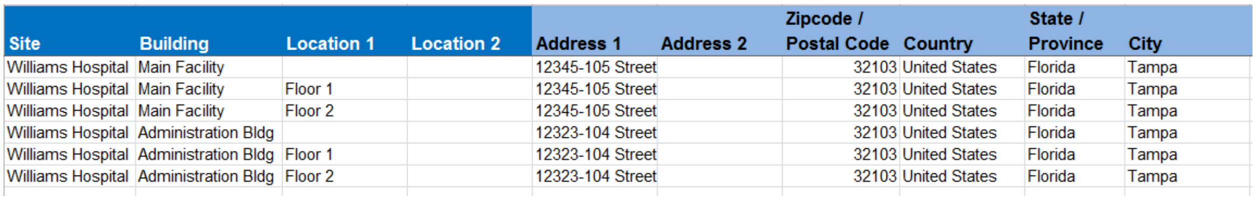
Similar to Classification and Activity Category lists, identifying the data required for reporting is a high priority. It allows for a geographical breakdown of Incident and Activity data. Clients sometimes believe they need to take location information down to a room number in order to use all four levels of the hierarchy. However, unless reporting/metrics breakdown requires down to a room number, or searching would be needed at a room level, breaking the site hierarchy down to a room number is unneeded. The details, down to the room number, can be documented in the Summary/Notes area of the record.

The next consideration for the Site list is to know the data that can be associated with a site value, regardless of the level the list stops at. The Site list tracks the following additional information:

- Address 1
- Address 2
- Postal/Zip code
- Geographic information (Country, State/Province, City)
- Geo Coordinates (Latitude and Longitude)
- Site Notes (used in Dispatching only, as a scrolling message that is a visual alert for your dispatchers—see the “Dispatching” section in the *Perspective Users Guide* for more details)

Documentation

Similar to the Activity Category list, each hierarchy level can track additional information, including the above data elements.



Site	Building	Location 1	Location 2	Address 1	Address 2	Zipcode / Postal Code	Country	State / Province	City
Williams Hospital	Main Facility			12345-105 Street		32103	United States	Florida	Tampa
Williams Hospital	Main Facility	Floor 1		12345-105 Street		32103	United States	Florida	Tampa
Williams Hospital	Main Facility	Floor 2		12345-105 Street		32103	United States	Florida	Tampa
Williams Hospital	Administration Bldg			12323-104 Street		32103	United States	Florida	Tampa
Williams Hospital	Administration Bldg	Floor 1		12323-104 Street		32103	United States	Florida	Tampa
Williams Hospital	Administration Bldg	Floor 2		12323-104 Street		32103	United States	Florida	Tampa

As shown above, the main facility and the Administration building, both part of the main campus (Williams Hospital), have different addresses.

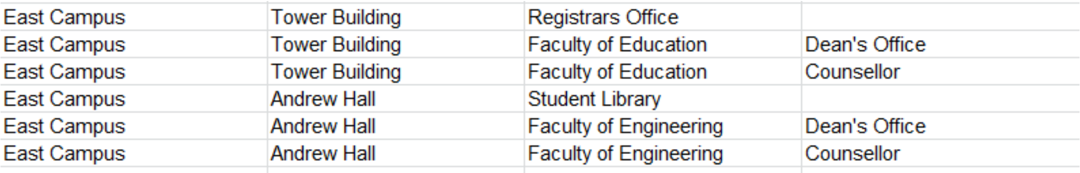
For each value that exists in the first four columns of this sheet that requires its own unique address, or to show an address for that value, you must show it on its own separate line.

As an example, while the Main Facility and the Administration Building have unique lines and thus, unique addresses, Williams Hospital does not have its own line, and therefore does not have an address associated to it.

Business Unit List

The Business Unit list is used in different ways by different clients. You can modify this hierarchy list for your organization's purposes.

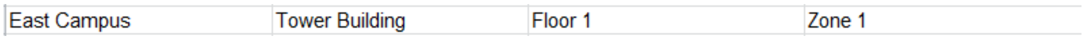
This field is often used to marry the data together with the Site list (pg. 21). Where the Site list identifies where something took place, the Business Unit allows you to identify who occupied that location.



East Campus	Tower Building	Registrars Office	
East Campus	Tower Building	Faculty of Education	Dean's Office
East Campus	Tower Building	Faculty of Education	Counsellor
East Campus	Andrew Hall	Student Library	
East Campus	Andrew Hall	Faculty of Engineering	Dean's Office
East Campus	Andrew Hall	Faculty of Engineering	Counsellor

Consider the Site list example above. If the Faculty of Education ever needed to move to a different building, it would be difficult to maintain old records that occurred in the Tower Building, but then prevent future incidents from using the Faculty of Education within the Tower Building.

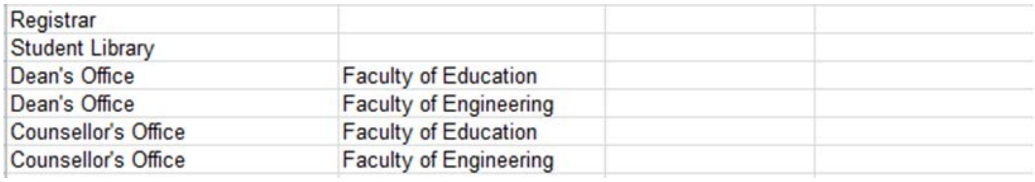
PPM recommends using the Site list to identify a location that never changes:



East Campus	Tower Building	Floor 1	Zone 1

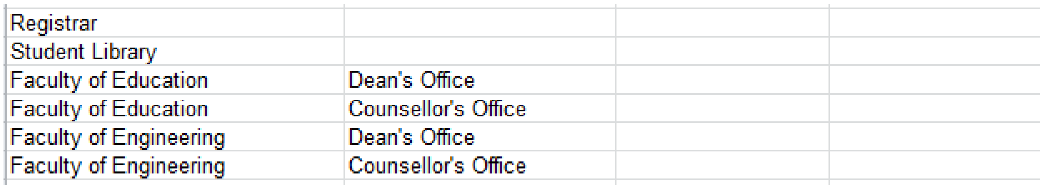
While this isn't enough information for your Incident record, this is information that probably won't change. For as long as the organization has the East Campus and a Tower Building, there will be a Floor 1 and Zone 1.

To identify that this was the Faculty of Education, and occurred in the Dean's Office, you could use the Business Unit list:



Registrar			
Student Library			
Dean's Office	Faculty of Education		
Dean's Office	Faculty of Engineering		
Counsellor's Office	Faculty of Education		
Counsellor's Office	Faculty of Engineering		

Or,



Registrar			
Student Library			
Faculty of Education	Dean's Office		
Faculty of Education	Counsellor's Office		
Faculty of Engineering	Dean's Office		
Faculty of Engineering	Counsellor's Office		

There are two benefits of documenting your record information this way:

1. There is a high likelihood that you will always have an East Campus and a Tower Building, and there is a high likelihood that you will always have a Faculty of Education and a Faculty of Engineering. However, there is no guarantee that they will remain in the same locations throughout their lifespan. By separating the location and the occupancy, you remove the need to maintain an accurate combined list.

   Should the Faculty of Education move from the Tower Building to Andrew Hall, there would be no list maintenance needed because Andrew Hall already exists in the Site list, and the Faculty of Education already exists in the Business Unit list. On the other hand, if you were to combine them in the Site list, then any move would require potentially difficult maintenance of that Site list.

2. You can now track the metrics of the Location and the Occupancy separately. If the Faculty of Education moves from the Tower Building to Andrew Hall, it is simple to run queries and metrics for Incidents that occurred only at Andrew Hall and exclude the Incidents while the Faculty of Education was at the Tower Building. By separating these data pieces, queries can be run individually or in tandem.

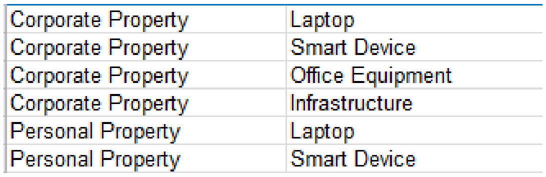
Documentation

The documentation of this list is done in the same way as the Classification list. There is no special documentation for this list.

Item Class List

This list is for Item records of Perspective. The two-tier hierarchy is used to allow classification of any item that is involved in an Incident record.

Identify Corporate Property versus Personal Property. This allows you to run metrics around the losses or recoveries that have a direct impact on business due to it being corporate related, but still track your risk for all losses, corporate or personal.



Corporate Property	Laptop
Corporate Property	Smart Device
Corporate Property	Office Equipment
Corporate Property	Infrastructure
Personal Property	Laptop
Personal Property	Smart Device

In the above example, you would be able to track any loss/recovery around Corporate versus Personal Property, but also losses around laptops or smart devices, regardless of what someone named them (iPhone, Blackberry, Dell, etc.), and regardless of whether it was Corporate Property or not.

Documentation

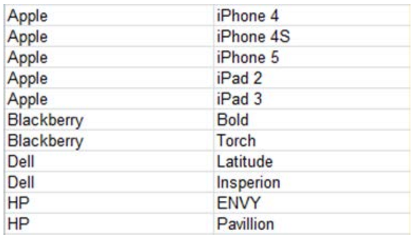
The documentation of this list is done in the same way as the Classification list. There is no special documentation for this list.

Item Make/Model List

This list is generally used as described, but usually tracked limited to Corporate Property.

With this being a hierarchy list, end users do not have the ability to add to this list while documenting their records. Thus, the list must be pre-built by Administrators, or added to by Administrators.

Because this list must be pre-determined before Incidents are documented, organizations usually only track the Makes/Models of items that they know will be involved in Incident records, or items that are high-ticket or high-risk items. This allows organizations to track trending differences.



Apple	iPhone 4
Apple	iPhone 4S
Apple	iPhone 5
Apple	iPad 2
Apple	iPad 3
Blackberry	Bold
Blackberry	Torch
Dell	Latitude
Dell	Insperion
HP	ENVY
HP	Pavillion

Documentation

The documentation of this list is done in the same way as the Classification list. There is no special documentation for this list.

Vehicle Make/Model List

The Vehicle Make/Model list is a pre-determined list of makes/models of vehicles that are involved in various incidents.

This list is usually substantial as the number of different models of vehicles on the road today is broad, and continues to change every year.

To assist with this, Perspective is shipped with a default list of vehicle makes/models that are commonly seen in North America. This is not intended to be a complete or final list, but includes most vehicles.

Addition to this list can be done through the application, or if there is a set list that needs to be added before you “Go Live”, this can be done through the data push process, if included in your Services Package.

Documentation

The documentation of this list is done in the same way as the Classification list. There is no special documentation for this list.

Geographic List

This is a list of Country, State/Province, and City, and is used in the following areas:

1. Address information for your:
    a. Site List
    b. Person Addresses
    c. Organization Addresses
2. Vehicle registration locations (Country and State/Province only)

Perspective is shipped by default with a North American list that includes approximately 27,000 cities and towns. This is not intended to be a complete list, but a good starting point for most North American organizations.

Adding to this list can be done through the application, or if there is a set list that needs to be added before you “Go Live”, this can be done through the data push process, if included in your Services Package. To assist with this, PPM has derived starting lists for various parts of the globe, and they can be provided upon request.

Documentation

The documentation of this list is done in the same way as the Classification list. There is no special documentation for this list.

Organizational Rollups

While this is a hierarchy list, and can be used for the purpose of metrics and measurements, it is specifically built with functionality relating to your data record security. As such, this is discussed further in the “Resolve the Issues” section (pg. 56) of this document.

Documentation

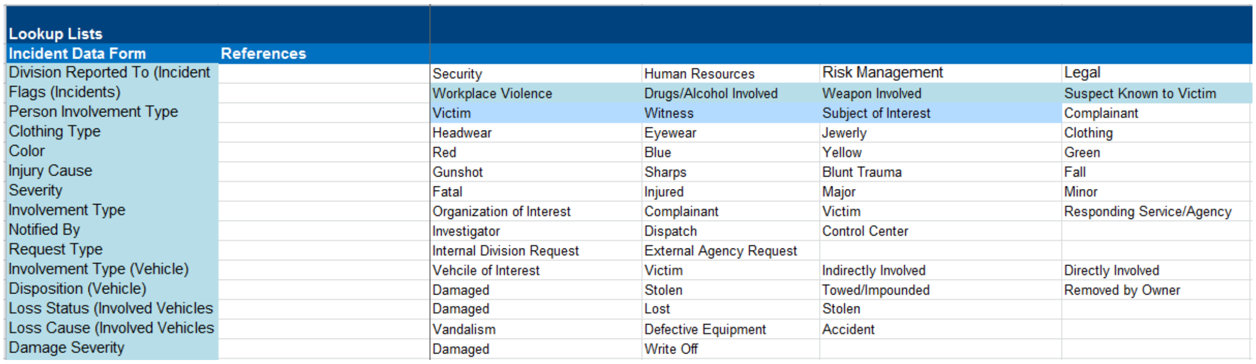
The documentation of this list is done in the same way as the Classification list. There is no special documentation for this list.

Documentation of Your Single Level Lookup Lists

The documentation of your single level lookup values is in your configuration document, in the tab titled Master Lookup Lists.

On this tab, you will see all editable and available lists that you can add to or remove from.

The values listed in this tab are what Perspective ships with. This means that any values that are on this sheet will continue to be in your database unless you choose to remove them.



Lookup Lists					
Incident Data Form	**References**				
Division Reported To (Incident		Security	Human Resources	Risk Management	Legal
Flags (Incidents)		Workplace Violence	Drugs/Alcohol Involved	Weapon Involved	Suspect Known to Victim
Person Involvement Type		Victim	Witness	Subject of Interest	Complainant
Clothing Type		Headwear	Eyewear	Jewerly	Clothing
Color		Red	Blue	Yellow	Green
Injury Cause		Gunshot	Sharps	Blunt Trauma	Fall
Severity		Fatal	Injured	Major	Minor
Involvement Type		Organization of Interest	Complainant	Victim	Responding Service/Agency
Notified By		Investigator	Dispatch	Control Center	
Request Type		Internal Division Request	External Agency Request		
Involvement Type (Vehicle)		Vehcile of Interest	Victim	Indirectly Involved	Directly Involved
Disposition (Vehicle)		Damaged	Stolen	Towed/Impounded	Removed by Owner
Loss Status (Involved Vehicles		Damaged	Lost	Stolen	
Loss Cause (Involved Vehicles		Vandalism	Defective Equipment	Accident	
Damage Severity		Damaged	Write Off		

In the image above, the single level lookup values are oriented horizontally. The list name exists in the first column. The second column references the location of this field in relation to the form shown in the document Perspective40ConfigurationWorkbook.xlsx.

In the third column, the lists begin. When any row encounters a blank column, the tool used by PPM to take this data and move it into a database will stop entry on this list and move on to the next list. Therefore, lists must be documented in consecutive columns, or values will be missed.

During this documentation, you will also come across values where cells are highlighted in blue. These values are system required values in the program and cannot be deleted. However, your organization does not have to use them. If this is the case, leave these values in place and they can be manipulated in the application.

Additional List Descriptions

While these are default lists, they can be adjusted to meet your organization's needs. Additionally, most of them can be hidden, locked, or made required.

The values in this list work in two different areas of the application, and are filtered in up to four different ways.

Activity Status – Activity Data Form

Available Officer Status – DispatchLog

Dispatched Officer/Organization Status – DispatchLog

Dispatch Call Status – DispatchLog

The default values (all of which have functionality around them) are the following:

Activity Statuses

Open – Report Required

Closed – No Report

Closed – Report Completed

Available Officer Statuses

Available

Busy

Out of Service

Dispatched Officer/Organization Statuses

On Hold

On Route

On Scene

Suspended

Dispatch Call Statuses

Cleared

Waiting

While the single list of Activity Statuses is used for all four of these areas, adding to the list of Activity Statuses will only add to the Available Officer Status section. All other values are locked into the areas they used. All default values have specific functionality behind them, so while the wording can be adjusted, this must be done with extreme caution as the functionality will not change, regardless of what word is used.

As an example, the status of On Route means that an officer or organization has been dispatched to a call and they are on route. Regardless of what this value is changed to, the moment an officer or organization is dispatched to a call, this value will be used. A different value cannot be chosen, and this value cannot be removed because the program has coded functionality to act in this specific way.

In addressing the Available Officer Status section, common value adjustments may include the following:

Break – 15 minutes

Break – 30 minutes

Patrol

Person Stop

Vehicle Stop

The intent of these additions is for two reasons:

1. Officer Logs—Being able to track where an officer is and what they are doing but not having to document an Activity for each action. Often, Activity actions can be so routine that documentation in any way other than acknowledgement that they have occurred is required. By having a status of this action, organizations can change an officer status to this action by logging it. But it often is an action that the officer can be prematurely pulled from at any time and make the choice at a later time, to continue, if necessary.

2. Officer Alerts—Within DispatchLog, there are visual alerts (having some data highlighted in different colors, bolded, flashing, etc.) used to alert dispatchers to something that needs their attention. An officer alert is always tied to an individual officer status. When a particular status is given to an officer, and a particular amount of time has passed, a visual alert begins, bringing this officer to the attention of the dispatcher.

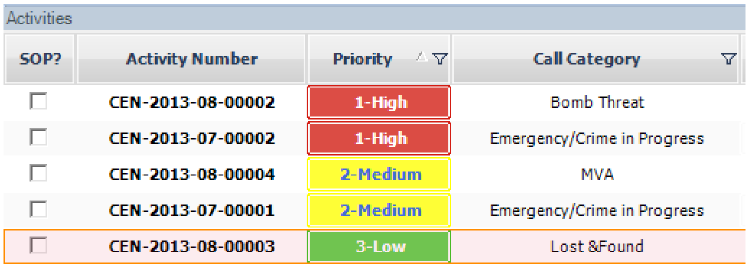
   For example, a status of Break – 15 minutes may have a visual alert set at 14 minutes so the dispatcher can remember to verify if that officer is available for duties again. Or, for officer safety needs, a status of On Scene may require a check-in every 30 minutes, or every 10 minutes, etc.

Priority

1. Order—All Perspective lookup lists sort alphabetically. If a particular order is desired, the only way to force an order to these lists is to number them. By default, Perspective ships with three values in this list: High, Medium, Low.

Without Numbers	With Numbers
High	1. Low
Low	2. Medium
Medium	3. High

   This is important because you may want your active dispatch screen to be sorted based on priority, with the more severe at the top and the least severe at the bottom.



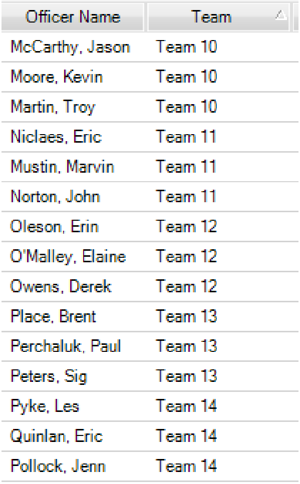
Activities

SOP?	Activity Number	Priority	Call Category
☐	CEN-2013-08-00002	1-High	Bomb Threat
☐	CEN-2013-07-00002	1-High	Emergency/Crime in Progress
☐	CEN-2013-08-00004	2-Medium	MVA
☐	CEN-2013-07-00001	2-Medium	Emergency/Crime in Progress
☐	CEN-2013-08-00003	3-Low	Lost &Found

2. Although High, Medium, and Low are the most commonly used values in this list, there is no limit or requirement (except the need to have at least one priority type as it is a system required field) to the number of values you can use in this list.

Officer Team

The main purpose of this list is metrics; however, there is some functionality that will assist in bringing officers on duty if the teams are identified properly.



Officer Name	Team
McCarthy, Jason	Team 10
Moore, Kevin	Team 10
Martin, Troy	Team 10
Niclaes, Eric	Team 11
Mustin, Marvin	Team 11
Norton, John	Team 11
Oleson, Erin	Team 12
O'Malley, Elaine	Team 12
Owens, Derek	Team 12
Place, Brent	Team 13
Perchaluk, Paul	Team 13
Peters, Sig	Team 13
Pyke, Les	Team 14
Quinlan, Eric	Team 14
Pollock, Jenn	Team 14

If the officers are assigned to set teams during setup, then when bringing officers on duty, it makes it easier to sort by officer team and bring a whole team on shift at one time. This is not a requirement, but will make the task of bringing officers on shift simpler.

STEP 3 Outline Your Users and Groups of Users

Data Segregation or Record Level Security

In Perspective, data is segregated by workgroups, organizational rollups, and access levels. Each user is classified by these criteria, and the Administrator controls his or her visibility. Every time a user accesses the system, Perspective looks for key components in order to set the segregation. Perspective determines the workgroup or workgroups you have received visibility of; it then determines the organizational rollups (if used) and the access level given to the role or user.

This section will illustrate specific areas of Perspective.

A Workgroup is the first layer of segregation. It can represent a department within your organization, a specific location such as a building, or a region such as Asia, Europe, or North America. However, in some cases, Region is used for organizational segregation, which will be covered below.

HUMAN RESOURCES
SECURITY
INVESTIGATIONS

Every time a user accesses Perspective, his or her visibility of records is directly linked to the workgroup(s) assigned to him or her. As an example, if User 1 is assigned visibility of Workgroup “Security”, User 1 cannot see nor have access to records within workgroup “Investigations” or “Human Resources”. However, users can have access to multiple workgroups.

The key is to identify, from the groups of users you have, how data should or should not be shared across groups. Each group of users that cannot share data should be their own workgroup.

Although it is best practice to not have exceedingly large amounts of workgroups, there is no limit to the number of workgroups that can be created in Perspective.

To create a Workgroup, click the Administration component, select Workgroups in the Navigation pane, then click Add.

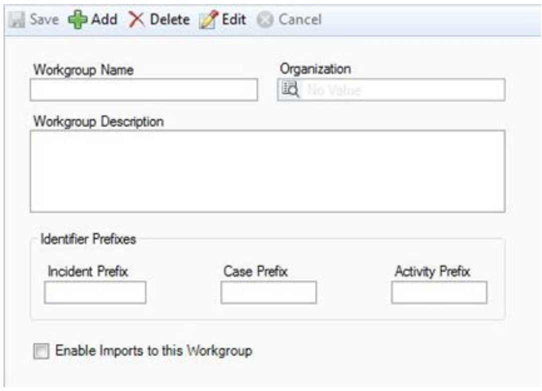
Enter the Workgroup Name and a Workgroup Description.

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) will appear on the workgroup's report cover pages.

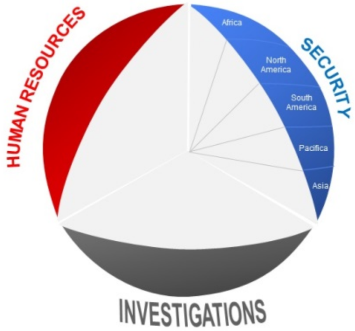
Note: If no organization is selected for the workgroup, the organization specified in the General Settings form under the General tab will be used by default. Organizations can also be assigned at the individual user level, overriding any selections made in General Settings and/or Workgroups.

Optional: If you want Incidents associated with a particular 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), specify this in the relevant prefix field.

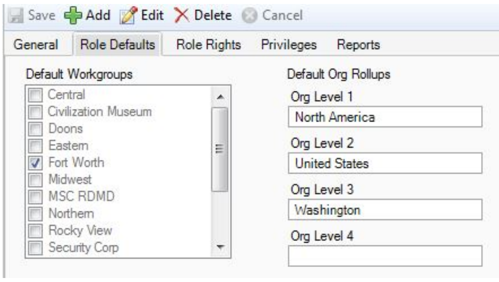
If you would like to allow the workgroup to import reports into the Gateway, check the Enable Imports to this Workgroup box.



An Organizational Rollup is the second layer of segregation that can be used in your segregation plan. Though not mandatory, it can further segregate data by sub-department or sub-region level, as shown in the image below.



Organizational Rollups are set at the Role level and/or at the User level, not within the Workgroup module. Unlike workgroups, a user can only be assigned one Organizational Rollups setting. 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. In the example below, the Role used here will only have access to the workgroup Fort Worth and will be further segregated all the way down to the city of Washington. This means that a user with this specific setting will only have visibility of records from the workgroup Fort Worth/North America/United States/Washington.



Default Workgroups

- □ Central
- □ Civilization Museum
- □ Doons
- □ Eastern
- ☑ Fort Worth
- □ Midwest
- □ MSC RDMD
- □ Northern
- □ Rocky View
- □ Security Corp

Default Org Rollups

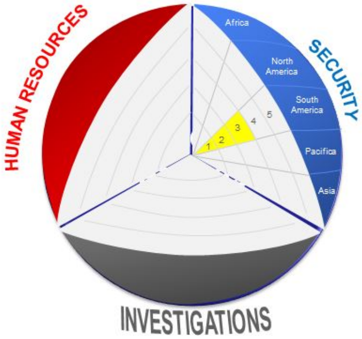
Org Level 1: North America

Org Level 2: United States

Org Level 3: Washington

Org Level 4:

The Access Level is the third layer of segregation. There are 5 Access Levels in Perspective, where Level 1 is the lowest and Level 5 is the highest. If a role is assigned Default Access, the role will only be permitted to view data with the same or lower access level as its own. As shown below, the user only has access to the workgroup Security, Organizational Rollups South America, and granted Access Level 3. Therefore, this user is limited to seeing records at Access Level 3 within South America inside Security Workgroup.

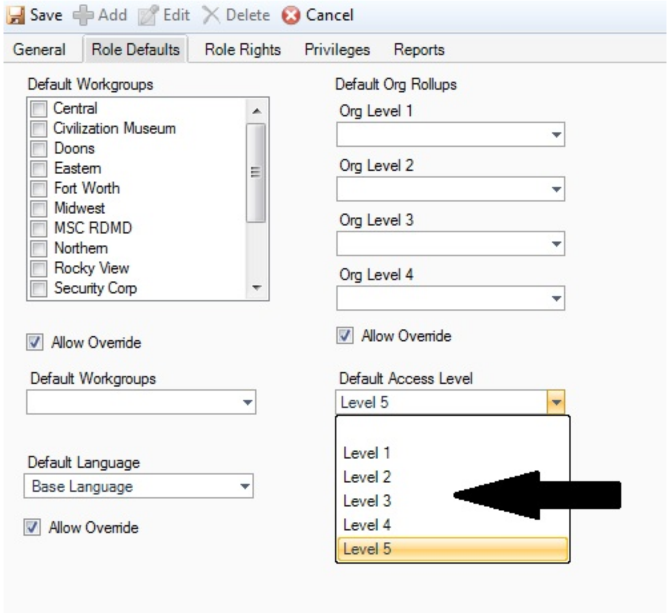


Another way to apply this concept is to look at Access Level as your classification of information, where Access Level 1 can be categorized as your unclassified information and Access Level 5 your top secret or sensitive information. The table below describe this concept:

Access Level	Classification
Access Level 1	Unclassified
Access Level 2	Restricted
Access Level 3	Confidential
Access Level 4	Secret

Access Level 5	Top secret

To assign an Access Level to a role and/or individual user, from the Role screen, go to the Role Defaults tab, set the Default Access between 1 and 5. If a Role is set at Level 3 but within the users assigned to that role, one of them needs to have Access Level 4, you can always check the Allow Override box to assign another Access Level to that particular user.



Default Workgroups
☐ Central
☐ Civilization Museum
☐ Doons
☐ Eastern
☐ Fort Worth
☐ Midwest
☐ MSC RDMD
☐ Northern
☐ Rocky View
☐ Security Corp

☑ Allow Override

Default Workgroups:

Default Language: Base Language

☑ Allow Override

Default Org Rollups
Org Level 1:
Org Level 2:
Org Level 3:
Org Level 4:

☑ Allow Override

Default Access Level: Level 5
Level 1
Level 2
Level 3
Level 4
Level 5

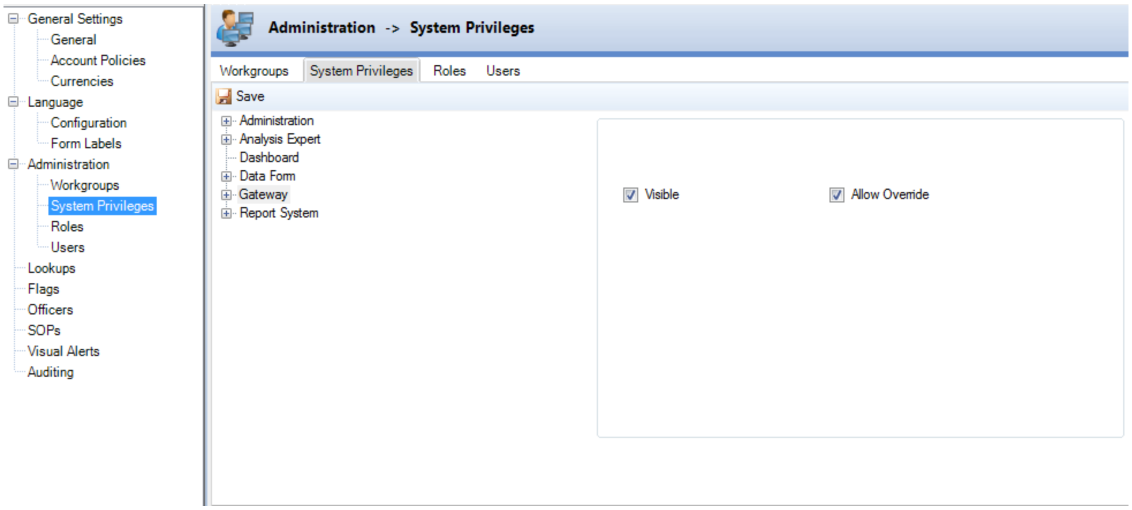
When a record is created, the Workgroup, the Organizational Rollups (if used), and the Access Level is placed on the control tab of that record, based on the user Workgroup, Organizational Rollup, and Access Level assigned to him or her.

In the next section, you will see Form and Field Level Security interact with records.

Form and Field Level Security

Form and Field Level Security directly affects who can see what fields/data within your Perspective System. In the previous section, Record Level Security, you identified who gets to see what record. Now you can begin to identify who can see various fields within the individual records, or see the data forms themselves. You can also make fields required or omit certain areas. Further, these rights and privileges can be set at three system levels—The System Level, the Role level, and the User Level. The rights and privileges set at the highest level will migrate to each lower level, unless you decide to make exceptions. It is good practice to configure these settings to the rule, rather than the exception, while at the highest level. An example of this would be that you have an individual within the system who will never need access to the Activities module, however, most of his/her colleagues will. In this case, you would set Activities as visible to your largest group of users, and then override this visibility at the Role or User level.

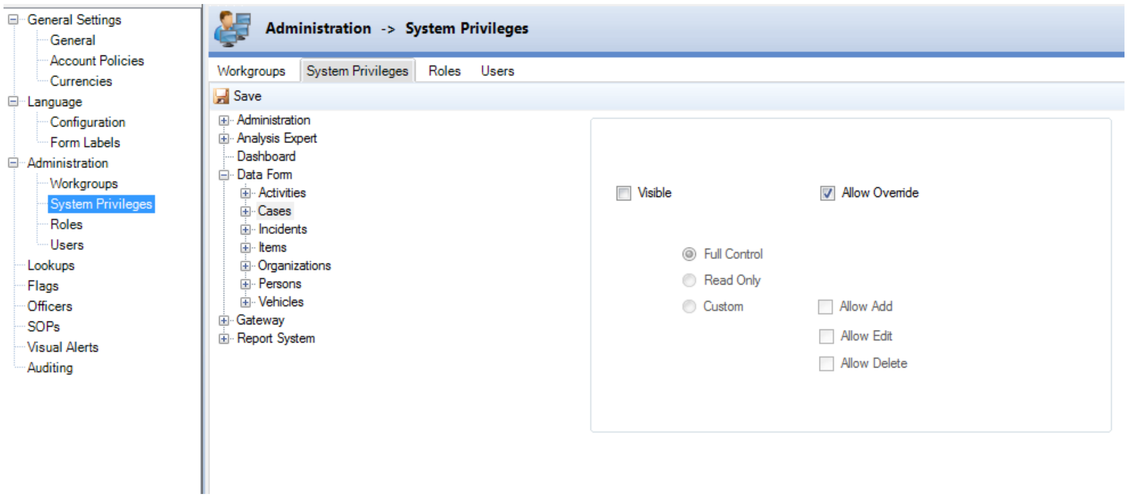
Form Level Security—This area allows you to decide who can see what forms and/or modules. Beginning at the system level, you can determine which forms and modules are visible to the majority of your users. These forms include the individual data forms: Activities, Incidents, Persons, Vehicles, Organizations, and Items, as well as on-board Perspective modules, Administration, Analyze and Report and its components: Analysis Expert, Reports, and Custom Reports. Additional privileges here allow you to specify which roles/users can do the following: only execute existing queries, manage (add, edit, and clone) queries, or share their queries with others.



☑ Visible ☑ Allow Override

By highlighting a module and selecting or deselecting Visible, you can control whether or not the module is seen at this level. The privileges set at this level will migrate down to the Role and User level, but can be overridden at these levels if the Allow Override button is checked.

Expanding the nodes beside any module will take you deeper into that module, where you can determine the visibility of specific pieces of a module.



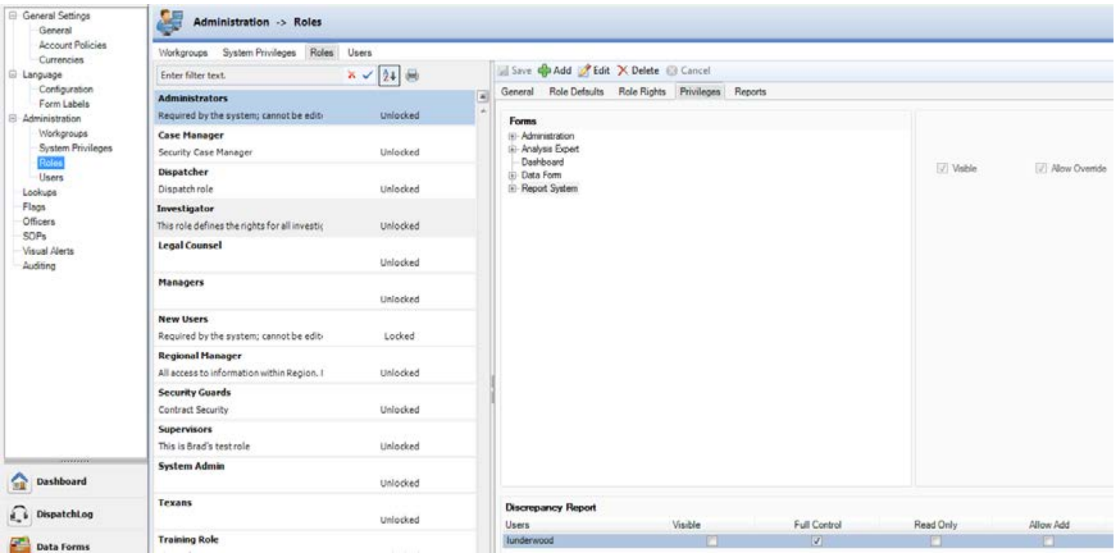
□ Visible ☑ Allow Override

● Full Control
○ Read Only
○ Custom □ Allow Add
□ Allow Edit
□ Allow Delete

In the above image, Cases has been removed from view at the System Level, meaning that the majority of users will not be able to see the Cases data form. With the Allow Override button checked, this can be modified at the Role or User level, thereby granting access to Cases to some users.

In the Data Forms module, you are able to control not only visibility of each specific form, but also what can be done to that form. There are three options, Full Control, Read Only, and Custom. Full Control allows a user to add, edit, and delete any of the selected form they want to. Read Only allows users to view records but not make changes. Custom allows you, as the Administrator, to determine the privileges pertaining to each form. Populating the checkboxes next to Allow Add, Allow Edit, and Allow Delete will enable these functions. The Allow Override button, if checked, will allow for these privileges to be changed at a later instance.

Once you have set your desired privileges at the system level, you will move next to the role level. As you can see, the set system privileges have migrated to the role level, and each role should be respecting the permissions set. You can now make any exceptions to your System Privileges, and these will migrate to the individual user level. The privileges are now found under a separate tab—Role Privileges. The role displayed below—Investigators—has Gateway rights removed, as they were rendered invisible at the system level, with the Allow Override button remaining unchecked. This role also displays an exception to the visibility that has been set for the Reporting System. As you can see below, the user lunderwood is not able to see reports, while all members of the role are. This is known as the discrepancy report, and is Perspective’s way of letting you know that there are exceptions to the rules you set.



Administrators Required by the system; cannot be edit	Unlocked
Case Manager Security Case Manager	Unlocked
Dispatcher Dispatch role	Unlocked
Investigator This role defines the rights for all investi	Unlocked
Legal Counsel	Unlocked
Managers	Unlocked
New Users Required by the system; cannot be edit	Locked
Regional Manager All access to information within Region. I	Unlocked
Security Guards Contract Security	Unlocked
Supervisors This is Brad's test role	Unlocked
System Admin	Unlocked
Texans	Unlocked
Training Role	

☑ Visible ☑ Allow Override

Discrepancy Report

Users	Visible	Full Control	Read Only	Allow Add
lunderwood	☐	☑	☐	☐

Finally, you can access the Users’ area and make changes to the privileges you set at the Role or System level. Following the same principles as described above, you can effectively create many different sets of privileges with your user group.

To make a change at a superior level that will migrate down to all subsequent levels, make the change, and uncheck the Allow Override button. Click Save, log out and then log back in, and the changes will have passed to each lower level. You can then re-check Allow Override if you want.

Field Level Security

Field level Security can be set in all three areas: System Privileges, Role Privileges, and User Privileges. If the Allow Override button is checked, privileges set at a higher level can be overruled at a lower level. If the Allow Override button is not checked, the privileges will transfer to the lowest level without opportunity for reversal. Fields within forms can be made Required, Hidden, or Locked.

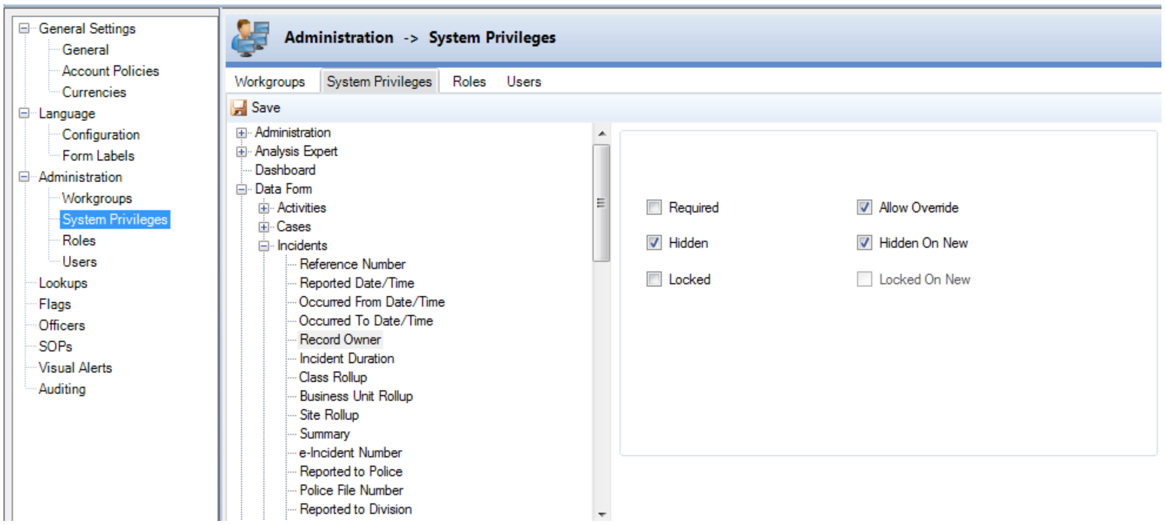
Required fields—Select a data form and expand the node beside it. A list of all fields within that form will appear. Highlight the field you want to make required and a number of options will appear on the right-hand side of the screen. Checking the Required box will make that field required for this user or group of users.

Some fields within Perspective are system-required and cannot be unrequired, or Locked on New.

Making a field required means that data must be populated within that field in order for Perspective to allow a Save to be generated. Fields should only be required if there will be consistent data to populate them. An Incident will always have a Classification, but may not always have a file number. Planning is necessary to ensure you are not making a field required that may not be filled in on all occasions.

Hidden fields—There are two methods of Hiding a field, Hidden and Hidden on New. If the Hidden box is checked, the field will be visible when a new report is created, but invisible afterwards. This allows for one-time data entry into the field before it is hidden. If both the Hidden and Hidden on New checkboxes are checked, the field will be hidden even when a new report is created.

Locked fields—Following the same principles as Hidden fields, there are two options, Locked and Locked on New. Checking the Locked box will make the field available for population on creation of a new report, and lock it thereafter. Checking both the Locked and Locked on New boxes will prevent the field from being accessed at any time. You may lock a system-required field.



☐ Required ☑ Allow Override

☑ Hidden ☑ Hidden On New

☐ Locked ☐ Locked On New

In the example above, the Incident Record Owner field is Hidden and Hidden on New, meaning it will not be visible at any point in the reporting process to anyone who has this privilege applied.

Role Defaults and Rights

As discussed above, Perspective offers privilege layering beginning at the System level. The privileges set at the System level then cascade to the Role level, where they may be changed. A role is basically a group of users who have a relatively similar position or access rights within Perspective. In order to make use of a Role, you must first create that Role, taking advantage of the default settings and rights that can be applied.

To add a role, click the Add button. Give the Role a name and description. There are three check boxes on the Roles general page:

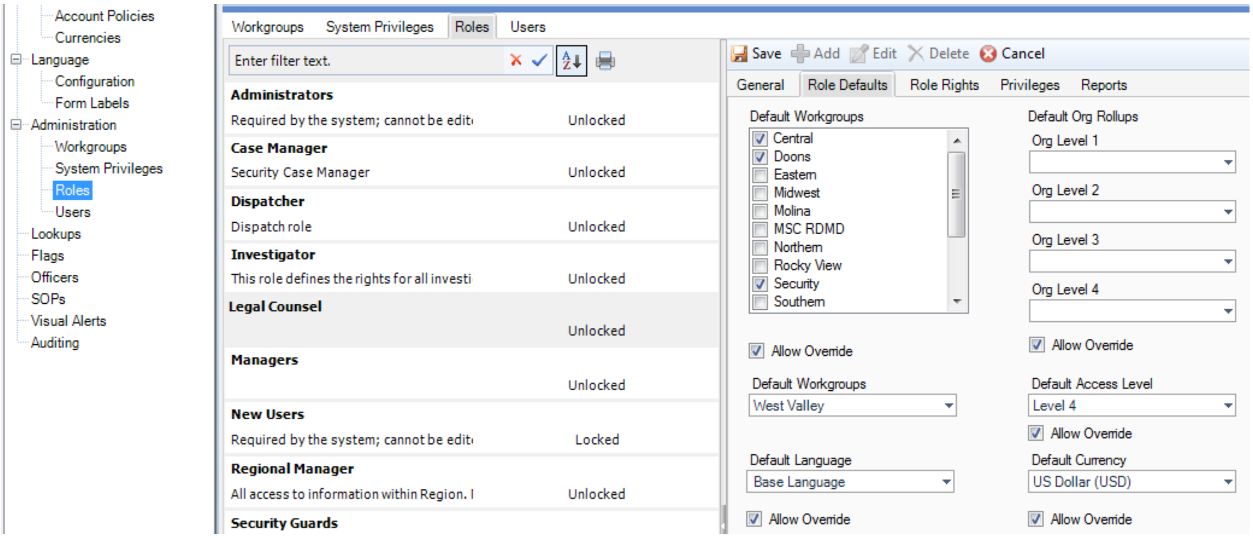
Role Locked—This locks all members of the Role out of the Perspective system.

Role Available to Sub-Admin on New User—If checked, this allows a sub-Administrative user to add a new member to this Role.

Do not Allow Override on All Reports—This removes the Allow Override option from the Reports Section, meaning that report visibility is set at this level and cannot be altered at the user level.

Role defaults allow you to set common elements for the role. The Workgroups area allows you to determine which workgroups within your system structure the role will have access to, and also allows you to set a primary workgroup for the role. The primary workgroup can be thought of as the area where the members of this role will be most responsible, and is the area where any of their filed reports will land. You can also determine a default language for the role, default access level, and default currency. If you are making use of the Organizational Rollups Security Layer, you can set up a default organizational rollup here, as well. Settings will be alterable at the user level if the Allow Override button is checked. If you want the settings to remain set at the role level, deselect the Allow Override box.

The role defaults screen is shown below.



Administrators
Required by the system; cannot be edit — Unlocked

Case Manager
Security Case Manager — Unlocked

Dispatcher
Dispatch role — Unlocked

Investigator
This role defines the rights for all investi — Unlocked

Legal Counsel
Unlocked

Managers
Unlocked

New Users
Required by the system; cannot be edit — Locked

Regional Manager
All access to information within Region. I — Unlocked

Security Guards

Default Workgroups
☑ Central
☑ Doons
□ Eastern
□ Midwest
□ Molina
□ MSC RDMD
□ Northern
□ Rocky View
☑ Security
□ Southern

☑ Allow Override

Default Org Rollups
Org Level 1:
Org Level 2:
Org Level 3:
Org Level 4:

☑ Allow Override

Default Workgroups: West Valley

Default Access Level: Level 4

☑ Allow Override

Default Language: Base Language

☑ Allow Override

Default Currency: US Dollar (USD)

☑ Allow Override

Each role also has a number of rights that can leveraged to further determine what members of the role can do within the Perspective system.

Administrator—Grants the user Administrative privileges. Unlike the Master Administration account, individual permissions for each Administrator can be set, determining what areas of the Administration module they can see, and what areas of the system they can work in/make changes to.

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 in Perspective, 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—Identifies the role's users as Investigators in Perspective, 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. 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—*Please disregard. This feature will become functional in a future Perspective release.*

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.

Gateway Approver—Assigns the role's users associated Gateway Approver access privileges.

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.

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.

Custom Search Access—Allows the role's users access to the Custom Search feature. 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 component.

Allow Elevate on New Records - 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.

Allow Elevate on New Records – Workgroup—Allows the role's users to assign a workgroup to a new record that is higher or different from their own.

Allow Elevate on New Records - Org Rollups—Allows the role's users to assign an organizational rollup to a new record that is higher or different from their own.

Role Privileges cascade from the System Level and are discussed in greater detail in the "Form and Field Security" (pg. 35) section. You can change the privileges for each role from the System Settings provided the Allow Override box is checked at the System Level, and allow for changes at the user level by leaving the Allow Override box checked at the role level.

The Reports component allows you to determine what reports the role is able to access/print.

User Defaults and Rights

Each Perspective user must be a member of a Role. Rights and Privileges set at the role level migrate down to the user level. Each user will absorb the rights of the role they are in when added to that role. However, these Rights and Privileges can be altered if the Allow Override box remains checked at the role level.

To add a user, click the Add button and begin typing your user's name. An area below the field should auto-populate with text suggestions matching the text you are typing. (If this does not occur, your user may not yet exist in your Perspective system and must be created as a Persons Record first.) Select the role the user will be a member of from the drop-down list. Give your user a login name and a password. If you are pre-determining the user's password for them, uncheck the Change Password on Login box; otherwise, he or she will be prompted to change his or her password when first logging into Perspective. The Windows Login ID feature will allow the user to access Perspective using their Windows Login. The Approved By and Organization lookups allow you to specify who approved the user, and what organization they are responsible to or a member of.

Once you have filled out the General tab, you will then set your user defaults. These default areas will have migrated from the role level, and can be changed if the Allow Override box was left checked at the role level. If you are not able to make changes but want to, you will have to return to the role level and grant override permissions. Set the default workgroup and workgroup permissions, organizational rollup, language, access level, and currency for your user, or leave them set at the role level.

Moving to the User Rights tab, you now have the opportunity to determine the individual rights each user will have. Again, these rights have migrated from the role level, so changes can only be made if the Allow Override box was left checked at the role level. Select/deselect the individual's rights as you deem necessary.

Note: The User Locked button will lock this user out of Perspective.

User Privileges cascade from the role level and are discussed in greater detail above in the "Form and Field Security" (pg. 35) section.

The Reports component allows you to make changes to the Report Visibilities set at the role level.

STEP 4 Identify Your Use of Perspective’s Web Portal

What the Web Portal Provides

Perspective’s Web Portal is a web-based tool that allows you to request an officer or report an incident without being a traditional Perspective user. The Portal also allows you to post BOLOs (Be on the Lookout), announcements, and links. Like the Perspective Desktop Client, you have the ability to control features and functions by turning them on or off.

The Request an Officer function allows a user to request an officer through an online submission directly through DispatchLog. Your dispatchers will receive the request and can dispatch the officer to the location specified in the request. While this function will remain visible for all Perspective platforms, it will only interact with DispatchLog if you have a Perspective edition that supports Dispatching (SOC and EIM). If your Perspective edition does not support Dispatching, the Request an Officer function can be turned off.

The Report an Incident function is a web version of the Incident form that includes everything you need to quickly capture incident details such as location, occurred dates, times, and summary. The form also gives you the ability to add more details like a narrative, Persons, Items, Vehicles, and Organizations. You can also upload photos. Once entered, the report goes through the Perspective Gateway for review and, if accepted, is added to your Perspective Incident records.

The Home page is a great communication tool. Post BOLOs, announcements, and links, all of which have an expiration date to keep the information current and relevant.

Plan Your Use of the Web Portal

Just like the Perspective Desktop Client, you need to determine what you want to get out of the Portal. What is the goal? Are there certain objectives that the Portal can help you achieve? Some things to consider for your Portal include the following:

- The current programs and services your organization provides.
  - Do you have a lost and found program?
  - Do you have an access control program to request new/replacement keys and ID cards?
- Planned programs and services you would like to provide in the future.

The next step is to decide who gets to use the Portal. Some possible examples of these groups are the following:

- Front Line Security Personnel
  - Many organizations have front line employees that do not have access to Perspective. This option allows for your officers to enter all the necessary information without needing access to Perspective. It also allows a supervisor to vet the information before it goes into Perspective as an Incident report.

- Company Employees
  - The ease of reporting an incident and/or the convenience of submitting a report anonymously may appeal to employees who would rather not have to meet with an officer to report an incident.
- Visitors, Vendors, or Contractors
  - Many options are available to meet the needs of everyone that visits your organization. Even with limited personal interaction, easy reporting and a central location of announcements allows for the transfer of essential knowledge.

Your Web Portal Configuration

Now that you have decided how you want to use the Portal and who should use it, it’s time to configure it. Web Portal can be configured to accommodate different languages, label/field name changes, hide fields and sections, add your logo and color themes, upload attachments, and make certain fields required. Portal can be a simple single page where everyone across the organization can see everything, or you can have a more complex Portal where each type of report/service goes to a different department. In either case, you’ll need to carefully consider your configuration options.

Think long term. If you only think about what your current system provides, you may be limiting yourself and not taking advantage of everything your Portal has to offer. This does not mean that you have to implement new changes all at once, but planning for future growth can make your overall implementation more efficient.

Portal requires Internet Explorer 10 or Google Chrome.

Web Portal Configuration Requirements

Your Portal Configuration can be broken down into the following requirements:

Portal Pages managed through URLs: Your Portal is based off of a URL. This URL is set up by an Administrator.

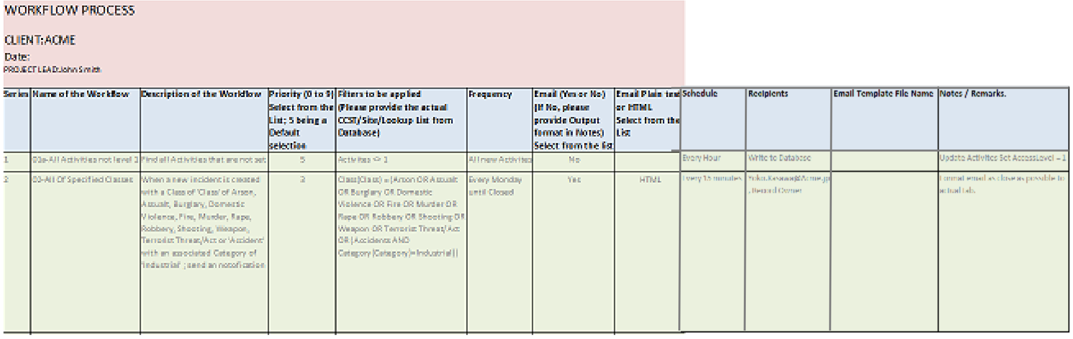
- Single URL that spans all departments/divisions and workgroups.
  - If you want all users to see all announcements across the organization and a single point of contact for any type of submission, a single URL may fit your needs.
- Multiple URLs that are specific for each department, division, or workgroup.
  - If you have multiple locations, sites, and/or workgroups, your Web Portal can be set up to handle different URLs. This means that you can have multiple URLs for specific purposes, or for different departments/divisions. This allows you to have a key or access card request form go specifically to the department that handles your physical security, a form to handle complaints against an employee that would go to Internal Investigations or Human Resources, or a Lost and Found Form that goes straight to the Client Service Department.
- Portal Elements that need to be configured:
  - Service Functions:

- Report an Incident
- Request an Officer
- Announcements
  - Data Form Sections: Consider the type(s) of information you want to get out of the Portal. Are there fields or sections on the form that you don't need? Decide which fields and sections on the forms you want visible.
    - You can turn off full sections within the Portal. You choose whether or not to display the following sections:
      - Report an Incident Function
      - Request an Officer Function
      - Incident Report Sections such as:
        - Persons
        - Organizations
        - Items
        - Vehicles
        - Narrative
- Data Form Fields: You can also hide individual fields. If the full section provides most of what you want to capture, but don't need a particular field, you can hide it.
    - You can also decide if you need the field hidden from all workgroups or just a few.
    - Is there a field that is critical for you to capture? Make these fields required.
        - Making a field required means that the user must fill out that field before the form can be saved and submitted.
        - Keep in mind that not all field types are an appropriate choice to make required. An example of this is a checkbox. If a checkbox is required, the answer must always be yes.
- Languages:
    - Web Portal can handle up to 20 different languages. Languages are usually used when you need new English terminology or non-English languages.
- Labels:
    - When using different Label sets for different workgroups, your Portal will utilize the same data field, but display a different label name for each associated workgroup that you have set.
- Logo and Color Theme:
    - Your Portal can be further configured to display your organization or department logo and color theme. If you use multiple workgroups and URLs, each of your pages can display the logo or image for that particular workgroup or department/division.

STEP 5 Identify Your Workflow Needs

To get started with Perspective Workflow, you first need to document your requirements. In order to assist with this documentation process, PPM has provided a Workflow Process Template. This Workflow Process Template will assist in the documentation of your Workflow requirements and make the process for building Workflow Event Paks much easier. Please see our *Workflow User's Guide* for detailed instructions on configuring your Workflow Event Paks.

Workflow Process Template



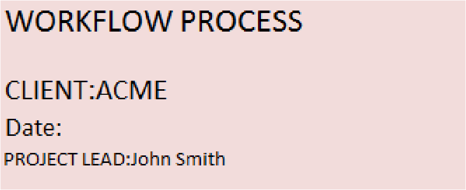
WORKFLOW PROCESS

CLIENT:ACME
Date:
PROJECT LEAD:John Smith

Series	Name of the Workflow	Description of the Workflow	Priority (0 to 5) Select from the List; 5 being a Default selection	Filters to be applied (Please provide the actual CCST/Site/Lookup List from Database)	Frequency	Email (Yes or No) (If No, please provide Output format in Notes) Select from the list	Email Plain tex or HTML Select from the List	Schedule	Recipients	Email Template File Name	Notes / Remarks.
1	03a-All Activities not level 1	Find all Activities that are not set	5	Activities <> 1	All new Activities	No		Every Hour	Write to Database		Update Activities Set AccessLevel = 1
2	03-All Of Specified Classes	When a new incident is created with a Class of 'Class' of Arson, Assault, Burglary, Domestic Violence, Fire, Murder, Rape, Robbery, Shooting, Weapon, Terrorist Threat/Act or 'Accident' with an associated Category of 'Industrial' ; send an notification	3	Class(Class) = (Arson OR Assault OR Burglary OR Domestic Violence OR Fire OR Murder OR Rape OR Robbery OR Shooting OR Weapon OR Terrorist Threat/Act OR (Accident AND Category (Category)=Industrial))	Every Monday until Closed	Yes	HTML	Every 15 minutes	Yoko.Kawasa@Acme.jp, Record Owner		Format email as close as possible to actual tab.

The Workflow Process Template can be broken down into three parts.

Part I—Allows you to document your organization's name, the date of your document, and the name of your Project Lead.



WORKFLOW PROCESS

CLIENT:ACME
Date:
PROJECT LEAD:John Smith

Part II—Allows you to define your Workflow query, apply filters, and decide its priority amongst other Workflows, the frequency of the query, and whether or not the notification will be via email.

The following columns make up Part II:

Series—Allows you to track the query (ie. Workflow for Activities, Workflow for Incidents), or you may want to number each query separately.

Name of the Workflow—Allows you to name the Workflow (ie. All Incidents Open 7 Days), or you can copy and paste from one of our standard Workflows.

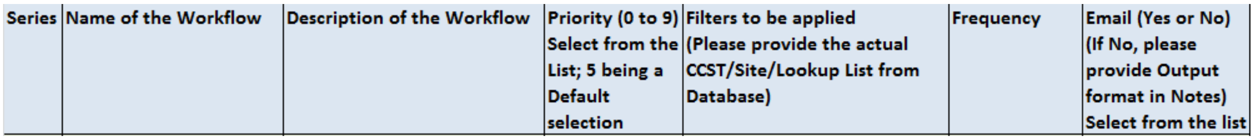
Description of the Workflow—Allows you to give a broader description of the requirement, or you can copy and paste the details from one of our standard Workflows.

Priority—You choose the importance of each Workflow in comparison to your other Workflows. If you have a time-sensitive Workflow running every few minutes, you may want to have it be a higher priority in case it happens to run at the same time as a monthly, less time-sensitive report.

Filters to be applied—This is where you document what fields are to be included in the query.

Frequency—Do you want to be notified of the results of your query every time or only when there are new results? This is where you document if the query results are repeated in future notifications.

Email (Yes or No)—The majority of our clients prefer to be notified of Workflow queries via email which is why we choose to have this as the standard. Please let us know if you require the notification to be via something other than email (i.e., fax, page, webcast).



Series	Name of the Workflow	Description of the Workflow	Priority (0 to 9) Select from the List; 5 being a Default selection	Filters to be applied (Please provide the actual CCST/Site/Lookup List from Database)	Frequency	Email (Yes or No) (If No, please provide Output format in Notes) Select from the list

Part III—Allows you to document how the notification will be sent, including plain text or HTML. You can also document how the notification will be received: schedule and recipients.

There are 6 columns for your use which make up Part III:

Email Plain Text or HTML—Choose to receive the email notification in email plain text or HTML (Hint: HTML which will allow for nicer formatting).

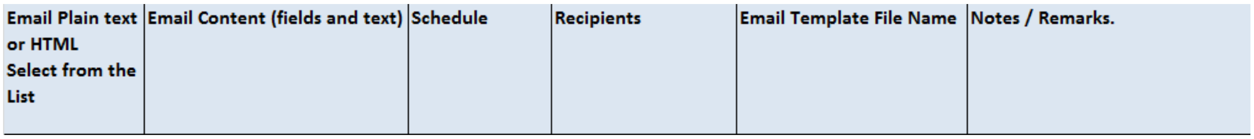
Email Content (fields and text) —Document which Perspective fields you want displayed and the accompanying text you want in the email notification.

Schedule—Want the query to run against your Perspective database hourly, daily, or weekly? This is where you can document when Workflow will conduct the query (starting with every five minutes for important, time-sensitive notifications)

Recipients—Who should receive the Workflow notification? List the email addresses and/or Perspective user names to have them receive this particular notification.

Email Template File Name—Document how you would like your email to look, create an example or template, and add the File Name here for reference.

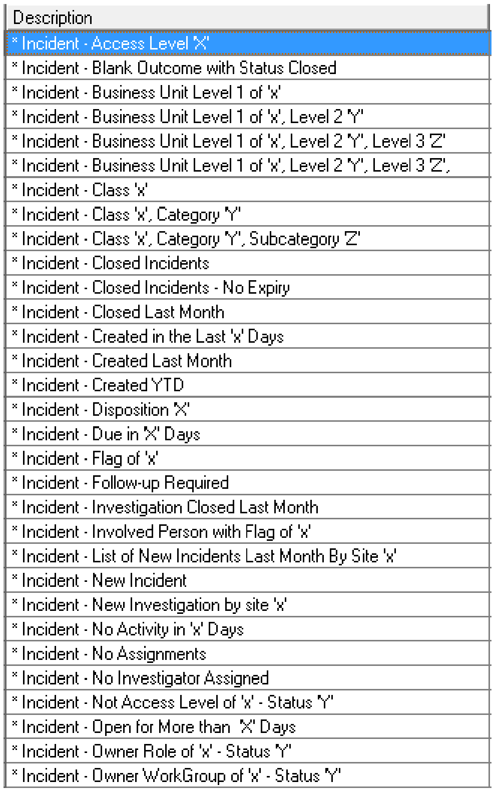
Notes: Document any other pertinent details related to this query.



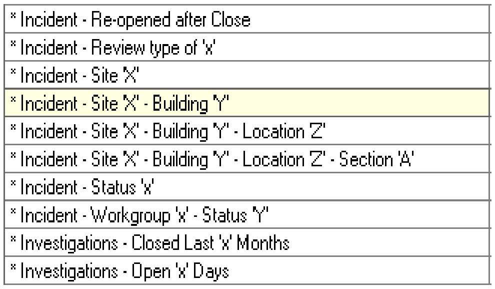
Email Plain text or HTML Select from the List	Email Content (fields and text)	Schedule	Recipients	Email Template File Name	Notes / Remarks.

To assist with your Perspective Workflow queries, PPM has developed 100 standard queries which allow you to easily pick which ones you would like. If you choose to build your own Workflow Event Pak, these included standard Workflows can be easily copied, pasted, and modified to fit your organization's needs.

INCIDENTS

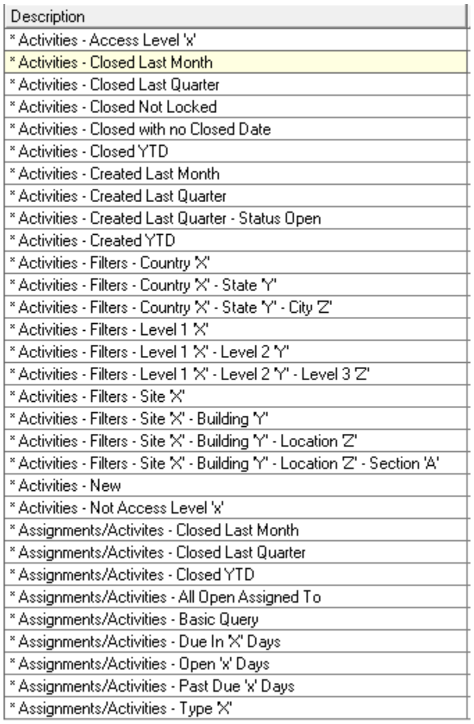


Description
* Incident - Access Level 'X'
* Incident - Blank Outcome with Status Closed
* Incident - Business Unit Level 1 of 'x'
* Incident - Business Unit Level 1 of 'x', Level 2 'Y'
* Incident - Business Unit Level 1 of 'x', Level 2 'Y', Level 3 'Z'
* Incident - Business Unit Level 1 of 'x', Level 2 'Y', Level 3 'Z',
* Incident - Class 'x'
* Incident - Class 'x', Category 'Y'
* Incident - Class 'x', Category 'Y', Subcategory 'Z'
* Incident - Closed Incidents
* Incident - Closed Incidents - No Expiry
* Incident - Closed Last Month
* Incident - Created in the Last 'x' Days
* Incident - Created Last Month
* Incident - Created YTD
* Incident - Disposition 'X'
* Incident - Due in 'X' Days
* Incident - Flag of 'x'
* Incident - Follow-up Required
* Incident - Investigation Closed Last Month
* Incident - Involved Person with Flag of 'x'
* Incident - List of New Incidents Last Month By Site 'x'
* Incident - New Incident
* Incident - New Investigation by site 'x'
* Incident - No Activity in 'x' Days
* Incident - No Assignments
* Incident - No Investigator Assigned
* Incident - Not Access Level of 'x' - Status 'Y'
* Incident - Open for More than 'X' Days
* Incident - Owner Role of 'x' - Status 'Y'
* Incident - Owner WorkGroup of 'x' - Status 'Y'



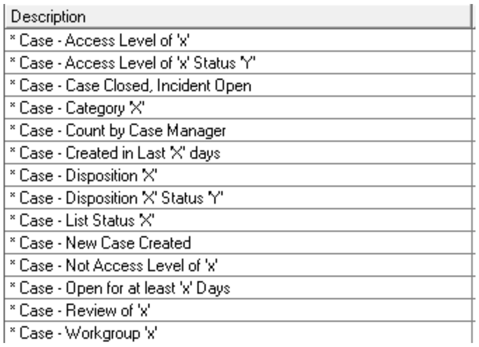
* Incident - Re-opened after Close
* Incident - Review type of 'x'
* Incident - Site 'X'
* Incident - Site 'X' - Building 'Y'
* Incident - Site 'X' - Building 'Y' - Location 'Z'
* Incident - Site 'X' - Building 'Y' - Location 'Z' - Section 'A'
* Incident - Status 'x'
* Incident - Workgroup 'x' - Status 'Y'
* Investigations - Closed Last 'x' Months
* Investigations - Open 'x' Days

ACTIVITIES



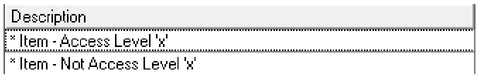
Description
* Activities - Access Level 'x'
* Activities - Closed Last Month
* Activities - Closed Last Quarter
* Activities - Closed Not Locked
* Activities - Closed with no Closed Date
* Activities - Closed YTD
* Activities - Created Last Month
* Activities - Created Last Quarter
* Activities - Created Last Quarter - Status Open
* Activities - Created YTD
* Activities - Filters - Country 'X'
* Activities - Filters - Country 'X' - State 'Y'
* Activities - Filters - Country 'X' - State 'Y' - City 'Z'
* Activities - Filters - Level 1 'X'
* Activities - Filters - Level 1 'X' - Level 2 'Y'
* Activities - Filters - Level 1 'X' - Level 2 'Y' - Level 3 'Z'
* Activities - Filters - Site 'X'
* Activities - Filters - Site 'X' - Building 'Y'
* Activities - Filters - Site 'X' - Building 'Y' - Location 'Z'
* Activities - Filters - Site 'X' - Building 'Y' - Location 'Z' - Section 'A'
* Activities - New
* Activities - Not Access Level 'x'
* Assignments/Activites - Closed Last Month
* Assignments/Activites - Closed Last Quarter
* Assignments/Activites - Closed YTD
* Assignments/Activities - All Open Assigned To
* Assignments/Activities - Basic Query
* Assignments/Activities - Due In 'X' Days
* Assignments/Activities - Open 'x' Days
* Assignments/Activities - Past Due 'x' Days
* Assignments/Activities - Type 'X'

CASES



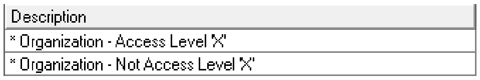
Description
* Case - Access Level of 'x'
* Case - Access Level of 'x' Status 'Y'
* Case - Case Closed, Incident Open
* Case - Category 'X'
* Case - Count by Case Manager
* Case - Created in Last 'X' days
* Case - Disposition 'X'
* Case - Disposition 'X' Status 'Y'
* Case - List Status 'X'
* Case - New Case Created
* Case - Not Access Level of 'x'
* Case - Open for at least 'x' Days
* Case - Review of 'x'
* Case - Workgroup 'x'

ITEMS



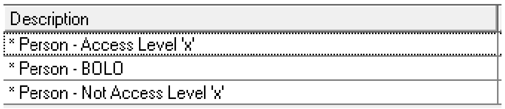
Description
* Item - Access Level 'x'
* Item - Not Access Level 'x'

ORGANIZATIONS



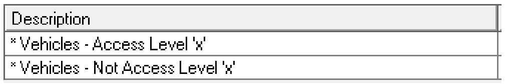
Description
* Organization - Access Level 'X'
* Organization - Not Access Level 'X'

PERSONS



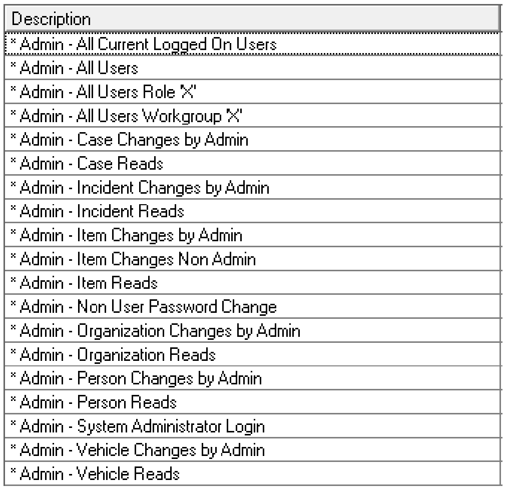
Description
* Person - Access Level 'x'
* Person - BOLO
* Person - Not Access Level 'x'

VEHICLES



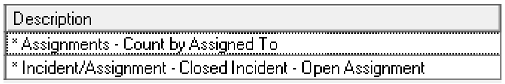
Description
* Vehicles - Access Level 'x'
* Vehicles - Not Access Level 'x'

ADMIN



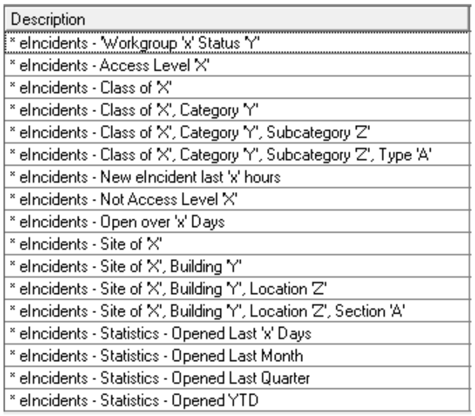
Description
* Admin - All Current Logged On Users
* Admin - All Users
* Admin - All Users Role 'X'
* Admin - All Users Workgroup 'X'
* Admin - Case Changes by Admin
* Admin - Case Reads
* Admin - Incident Changes by Admin
* Admin - Incident Reads
* Admin - Item Changes by Admin
* Admin - Item Changes Non Admin
* Admin - Item Reads
* Admin - Non User Password Change
* Admin - Organization Changes by Admin
* Admin - Organization Reads
* Admin - Person Changes by Admin
* Admin - Person Reads
* Admin - System Administrator Login
* Admin - Vehicle Changes by Admin
* Admin - Vehicle Reads

ASSIGNMENTS



Description
* Assignments - Count by Assigned To
* Incident/Assignment - Closed Incident - Open Assignment

E-INCIDENTS



Description
* eIncidents - 'Workgroup 'x' Status 'Y'
* eIncidents - Access Level 'X'
* eIncidents - Class of 'X'
* eIncidents - Class of 'X', Category 'Y'
* eIncidents - Class of 'X', Category 'Y', Subcategory 'Z'
* eIncidents - Class of 'X', Category 'Y', Subcategory 'Z', Type 'A'
* eIncidents - New eIncident last 'x' hours
* eIncidents - Not Access Level 'X'
* eIncidents - Open over 'x' Days
* eIncidents - Site of 'X'
* eIncidents - Site of 'X', Building 'Y'
* eIncidents - Site of 'X', Building 'Y', Location 'Z'
* eIncidents - Site of 'X', Building 'Y', Location 'Z', Section 'A'
* eIncidents - Statistics - Opened Last 'x' Days
* eIncidents - Statistics - Opened Last Month
* eIncidents - Statistics - Opened Last Quarter
* eIncidents - Statistics - Opened YTD

Once you have completed the Workflow Process Template, you are ready to have your Workflow Event Pak built.

Perspective Workflow Standard Event Pak

Event Pak Installation

1. Ensure the Event Pak provided is on the Workflow server.

2. Open the Workflow Event Manager.

3. Select File > EventPak > Install.

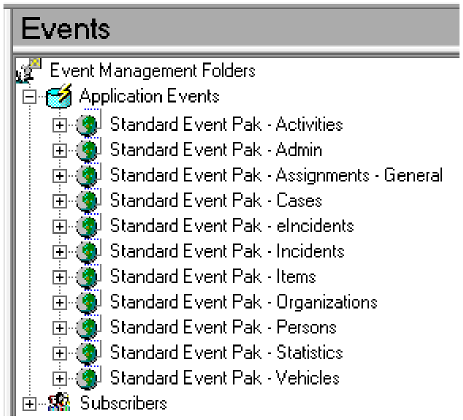
4. Navigate to the Event Pak (StandardEventPak.kse) file, and open it.

5. Click the Install button.

   - As long as it states Finished after the installation is complete, disregard any error messages.

6. Event Manager should close and reload automatically.

   - Eleven application events have been installed.



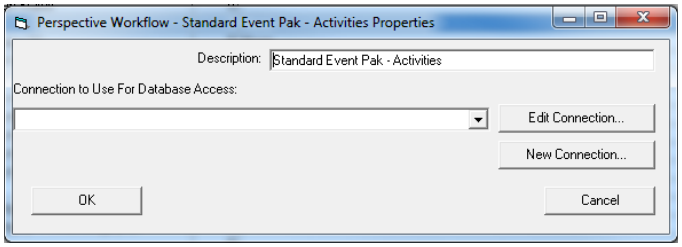
Events

Event Management Folders
Application Events
Standard Event Pak - Activities
Standard Event Pak - Admin
Standard Event Pak - Assignments - General
Standard Event Pak - Cases
Standard Event Pak - eIncidents
Standard Event Pak - Incidents
Standard Event Pak - Items
Standard Event Pak - Organizations
Standard Event Pak - Persons
Standard Event Pak - Statistics
Standard Event Pak - Vehicles
Subscribers

7. Click the Standard Event Pak applications.

8. Select Properties.

9. If there is no value in the drop-down list, skip to step 16, otherwise, select Edit Connection.



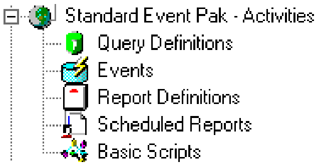
Perspective Workflow - Standard Event Pak - Activities Properties

Description: Standard Event Pak - Activities

Connection to Use For Database Access:

10. Click the Delete button, as this is likely the connection from our machine, not yours.
11. If there are additional connections, repeat steps 13 and 14 until there are no more connections in the list.
12. Click New Connection.
13. On the screen that appears, add data to the following fields (all other fields can be left as is):
    a. Connection Description—Change this value to your company name.
    b. ODBC Data Source Name—If there was a previously created ODBC data connection, select it and skip to step f. If not, select NONE (Specify Driver Information).
    c. Server Name—the SQL Server location including an instance, if applicable.
    d. Database Name—The name of the database on the SQL Server.
    e. Database Driver Description—Must be SQL Server.
    f. Username—Use the same SQL user that is used to connect Perspective to the database (can be found in the config file). You can create a new SQL user, if desired, specifically for Workflow. This user must have database owner rights though.
    g. Password—The password for the SQL user above.

14. Click Save and Close.
15. Click OK.
16. Test this connection by opening the node beside one of the applications and selecting Query Definitions.



17. Double-click on any of the queries in the list on the right. If the window opens without an error, stay in this open query, and move to the next step. If there is an error that pops up, click on the Event Pak node, return to the properties, and choose Edit Connection, then verify the data in step 14.
18. Once the connection has been verified, select each of the Event Paks.
19. Click Properties.

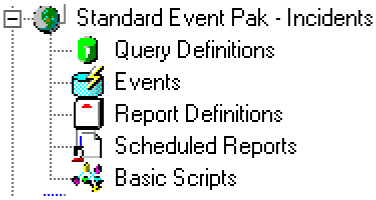
20. Select the database connection that has just been made.

21. Regardless of which query you opened, move to the Tables tab, and scroll down the Available Tables window until you see dbo._Activities. (There will be numerous tables that show dbo._ starting their name, but as long as you see one, the rest will be there.) If you do not see dbo._, return to the installation instructions to install the views package supplied with the Workflow install zip file.

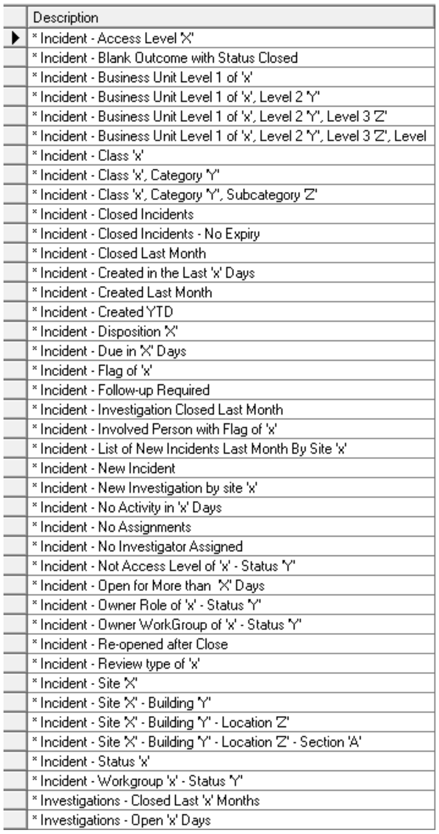
22. Click Cancel.

Understanding the Queries

Select Standard Event Pak – Incidents and click on Query Definitions.



You will see a list of premade queries. The name of the query is a brief description of what it does.

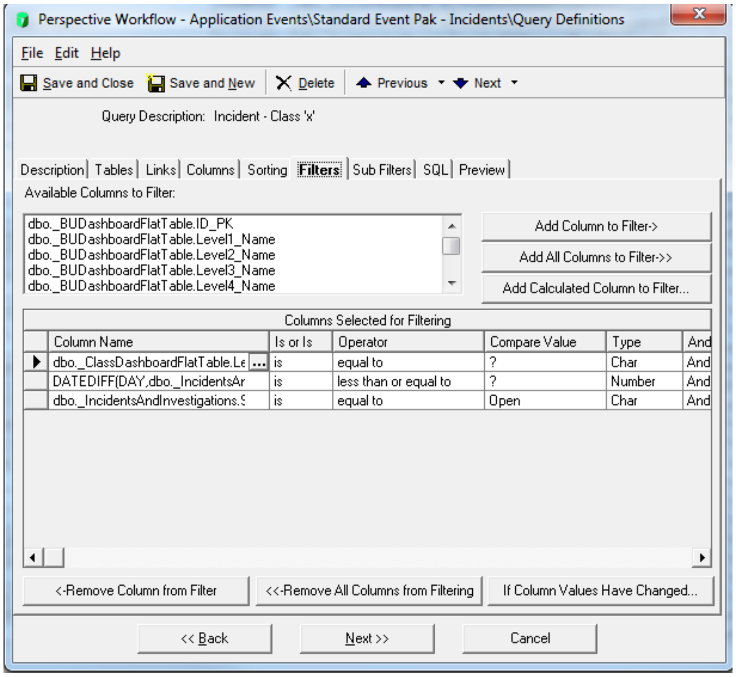


Description
* Incident - Access Level 'X'
* Incident - Blank Outcome with Status Closed
* Incident - Business Unit Level 1 of 'x'
* Incident - Business Unit Level 1 of 'x', Level 2 'Y'
* Incident - Business Unit Level 1 of 'x', Level 2 'Y', Level 3 'Z'
* Incident - Business Unit Level 1 of 'x', Level 2 'Y', Level 3 'Z', Level
* Incident - Class 'x'
* Incident - Class 'x', Category 'Y'
* Incident - Class 'x', Category 'Y', Subcategory 'Z'
* Incident - Closed Incidents
* Incident - Closed Incidents - No Expiry
* Incident - Closed Last Month
* Incident - Created in the Last 'x' Days
* Incident - Created Last Month
* Incident - Created YTD
* Incident - Disposition 'X'
* Incident - Due in 'X' Days
* Incident - Flag of 'x'
* Incident - Follow-up Required
* Incident - Investigation Closed Last Month
* Incident - Involved Person with Flag of 'x'
* Incident - List of New Incidents Last Month By Site 'x'
* Incident - New Incident
* Incident - New Investigation by site 'x'
* Incident - No Activity in 'x' Days
* Incident - No Assignments
* Incident - No Investigator Assigned
* Incident - Not Access Level of 'x' - Status 'Y'
* Incident - Open for More than 'X' Days
* Incident - Owner Role of 'x' - Status 'Y'
* Incident - Owner WorkGroup of 'x' - Status 'Y'
* Incident - Re-opened after Close
* Incident - Review type of 'x'
* Incident - Site 'X'
* Incident - Site 'X' - Building 'Y'
* Incident - Site 'X' - Building 'Y' - Location 'Z'
* Incident - Site 'X' - Building 'Y' - Location 'Z' - Section 'A'
* Incident - Status 'x'
* Incident - Workgroup 'x' - Status 'Y'
* Investigations - Closed Last 'x' Months
* Investigations - Open 'x' Days

Some queries are configurable others are useable out of the box. An example of a non-configurable query is ‘Incident – Closed Last Month’. This one will find all incidents closed the previous calendar month.

A configurable query would be one like ‘Incident – Class ‘x’’. This means that it will find all incidents that have a Class rollup level 1 of whatever you specify. To see how it works double click on the query and Navigate to the Filters tab.

Under compare values you can see two question (?) marks. This means the compare value can be entered on the event level instead of the query level. The top mark is the Class to search for such as Criminal, Internal etc. and the second mark is how many days back you want to check. To test the query click Preview and you will be prompted:


Perspective Workflow - Application Events\Standard Event Pak - Incidents\Query Definitions
File Edit Help
Save and Close
Save and New
Delete
Previous
Next
Description
Tables
Links
Columns
Sorting
Filters
Sub Filters
SQL
Preview
Add Column to Filter->
Add All Columns to Filter->>
Add Calculated Column to Filter...
<-Remove Column from Filter
<<-Remove All Columns from Filtering
If Column Values Have Changed...
<< Back
Next >>
Cancel

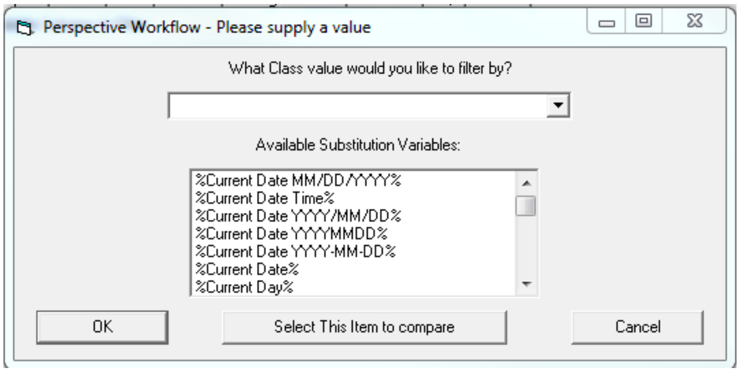
Query Description: Incident - Class 'x'

Available Columns to Filter:

dbo._BUDashboardFlatTable.ID_PK
dbo._BUDashboardFlatTable.Level1_Name
dbo._BUDashboardFlatTable.Level2_Name
dbo._BUDashboardFlatTable.Level3_Name
dbo._BUDashboardFlatTable.Level4_Name

Columns Selected for Filtering

Column Name	Is or Is	Operator	Compare Value	Type	And
dbo._ClassDashboardFlatTable.Le	is	equal to	?	Char	And
DATEDIFF(DAY,dbo._IncidentsAr	is	less than or equal to	?	Number	And
dbo._IncidentsAndInvestigations.S	is	equal to	Open	Char	And

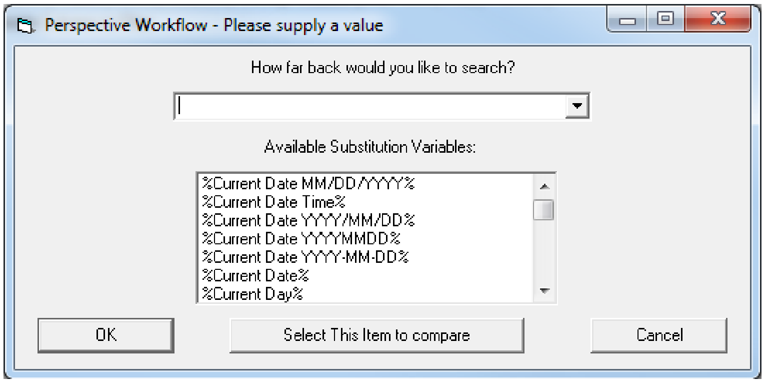

Perspective Workflow - Please supply a value
OK
Select This Item to compare
Cancel

What Class value would you like to filter by?

Available Substitution Variables:

%Current Date MM/DD/YYYY%
%Current Date Time%
%Current Date YYYY/MM/DD%
%Current Date YYYYMMDD%
%Current Date YYYY-MM-DD%
%Current Date%
%Current Day%

Type in a top level class or select one from the drop-down list and click ok. There will be a second prompt:



Perspective Workflow - Please supply a value

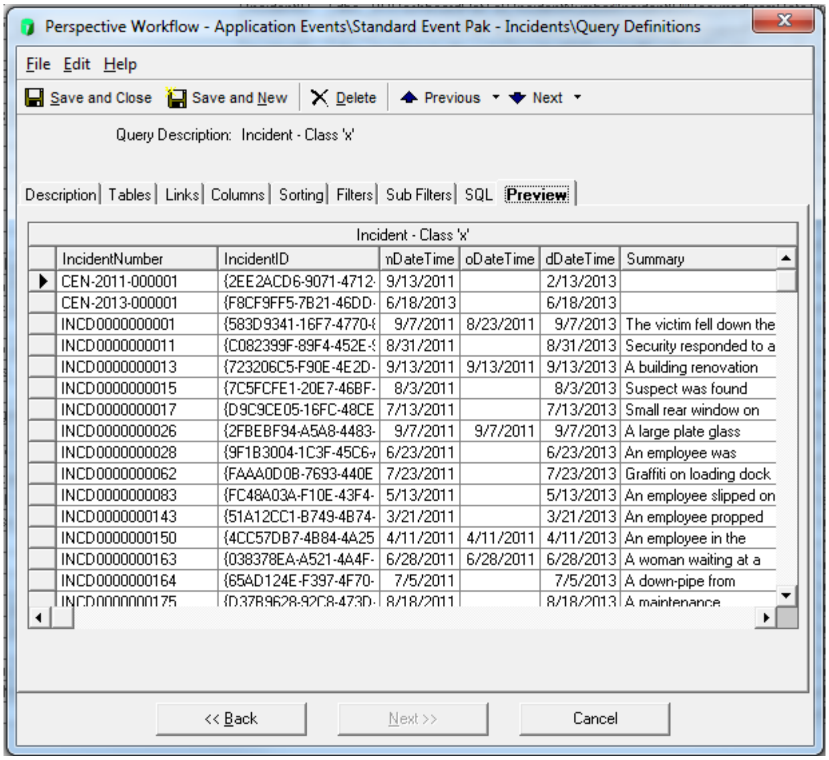
How far back would you like to search?

Available Substitution Variables:

%Current Date MM/DD/YYYY%
%Current Date Time%
%Current Date YYYY/MM/DD%
%Current Date YYYYMMDD%
%Current Date YYYY-MM-DD%
%Current Date%
%Current Day%

Type in how many days ago you want to start your search.

For example: if you want a weekly report of all Incidents of the specified class created in the last week type 7, if it a daily email, type 1.



Perspective Workflow - Application Events\Standard Event Pak - Incidents\Query Definitions

Query Description: Incident - Class 'x'

Incident - Class 'x'

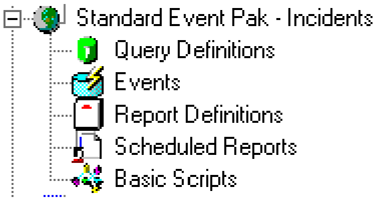
IncidentNumber	IncidentID	nDateTime	oDateTime	dDateTime	Summary
CEN-2011-000001	{2EE2ACD6-9071-4712-	9/13/2011		2/13/2013	
CEN-2013-000001	{F8CF9FF5-7B21-46DD-	6/18/2013		6/18/2013	
INCD0000000001	{583D9341-16F7-4770-	9/7/2011	8/23/2011	9/7/2013	The victim fell down the
INCD0000000011	{C082399F-89F4-452E-	8/31/2011		8/31/2013	Security responded to a
INCD0000000013	{723206C5-F90E-4E2D-	9/13/2011	9/13/2011	9/13/2013	A building renovation
INCD0000000015	{7C5FCFE1-20E7-46BF-	8/3/2011		8/3/2013	Suspect was found
INCD0000000017	{D9C9CE05-16FC-48CE	7/13/2011		7/13/2013	Small rear window on
INCD0000000026	{2FBEBF94-A5A8-4483-	9/7/2011	9/7/2011	9/7/2013	A large plate glass
INCD0000000028	{9F1B3004-1C3F-45C6-	6/23/2011		6/23/2013	An employee was
INCD0000000062	{FAAA0D0B-7693-440E	7/23/2011		7/23/2013	Graffiti on loading dock
INCD0000000083	{FC48A03A-F10E-43F4-	5/13/2011		5/13/2013	An employee slipped on
INCD0000000143	{51A12CC1-B749-4B74-	3/21/2011		3/21/2013	An employee propped
INCD0000000150	{4CC57DB7-4B84-4A25	4/11/2011	4/11/2011	4/11/2013	An employee in the
INCD0000000163	{038378EA-A521-4A4F-	6/28/2011	6/28/2011	6/28/2013	A woman waiting at a
INCD0000000164	{65AD124E-F397-4F70-	7/5/2011		7/5/2013	A down-pipe from
INCD0000000175	{D37B9628-92C8-473D-	8/18/2011		8/18/2013	A maintenance

The preview window will give you all the Incidents in your Perspective data base that matches your query parameters.

For more information on customizing queries please refer to the *Perspective Workflow User's Guide*.

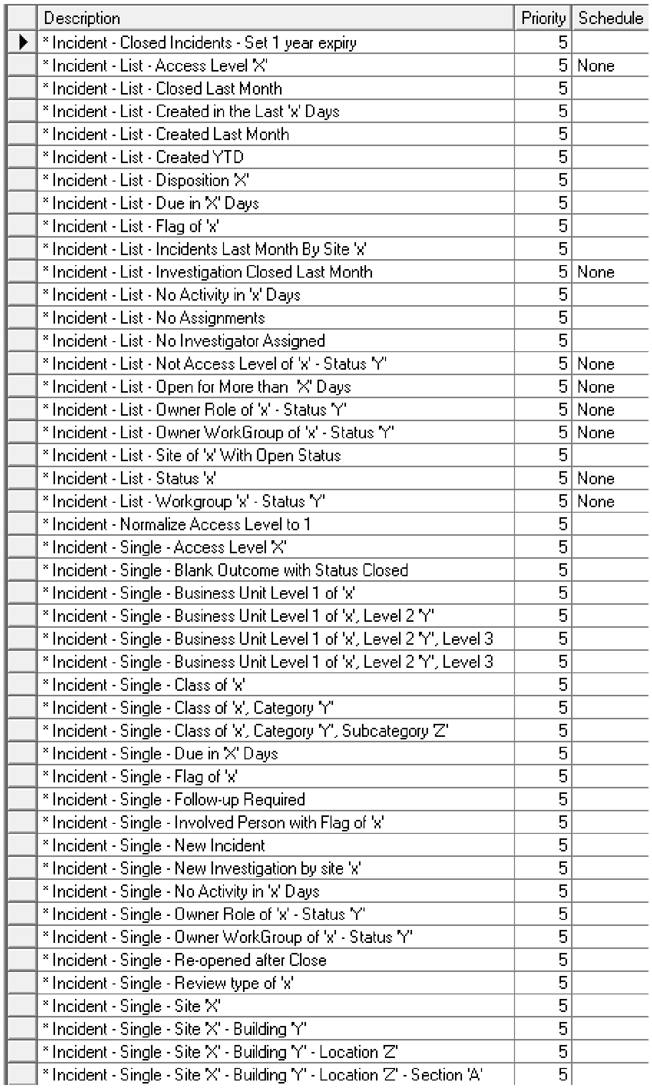
Understanding the Events

Select Standard Event Pak > Incidents and click on Events.



Standard Event Pak - Incidents
- Query Definitions
- Events
- Report Definitions
- Scheduled Reports
- Basic Scripts

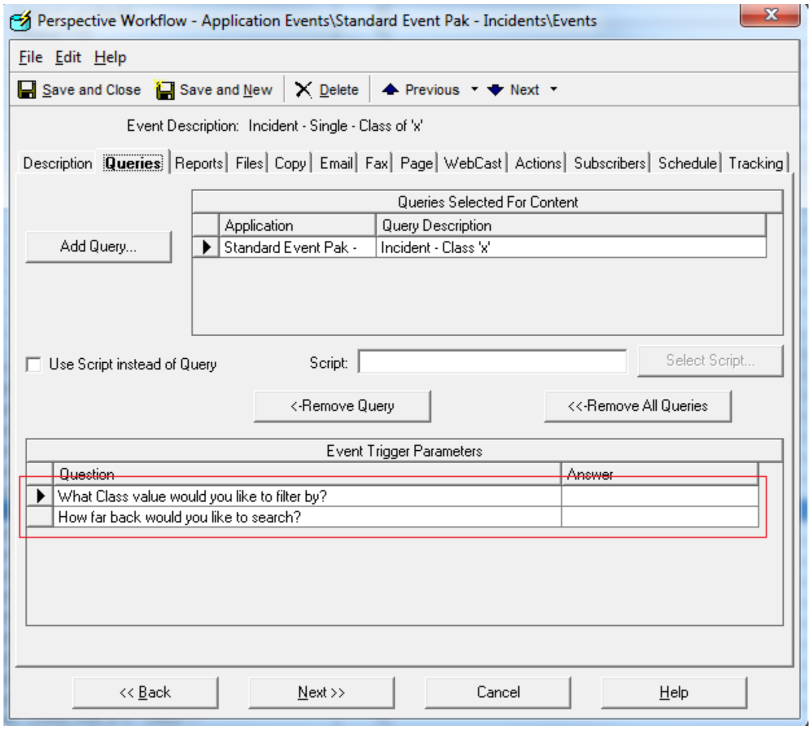
You will see a list of pre-made events. The name of the event is a brief description of what it does.



	Description	Priority	Schedule
▶	* Incident - Closed Incidents - Set 1 year expiry	5	
	* Incident - List - Access Level 'X'	5	None
	* Incident - List - Closed Last Month	5	
	* Incident - List - Created in the Last 'x' Days	5	
	* Incident - List - Created Last Month	5	
	* Incident - List - Created YTD	5	
	* Incident - List - Disposition 'X'	5	
	* Incident - List - Due in 'X' Days	5	
	* Incident - List - Flag of 'x'	5	
	* Incident - List - Incidents Last Month By Site 'x'	5	
	* Incident - List - Investigation Closed Last Month	5	None
	* Incident - List - No Activity in 'x' Days	5	
	* Incident - List - No Assignments	5	
	* Incident - List - No Investigator Assigned	5	
	* Incident - List - Not Access Level of 'x' - Status 'Y'	5	None
	* Incident - List - Open for More than 'X' Days	5	None
	* Incident - List - Owner Role of 'x' - Status 'Y'	5	None
	* Incident - List - Owner WorkGroup of 'x' - Status 'Y'	5	None
	* Incident - List - Site of 'x' With Open Status	5	
	* Incident - List - Status 'x'	5	None
	* Incident - List - Workgroup 'x' - Status 'Y'	5	None
	* Incident - Normalize Access Level to 1	5	
	* Incident - Single - Access Level 'X'	5	
	* Incident - Single - Blank Outcome with Status Closed	5	
	* Incident - Single - Business Unit Level 1 of 'x'	5	
	* Incident - Single - Business Unit Level 1 of 'x', Level 2 'Y'	5	
	* Incident - Single - Business Unit Level 1 of 'x', Level 2 'Y', Level 3	5	
	* Incident - Single - Business Unit Level 1 of 'x', Level 2 'Y', Level 3	5	
	* Incident - Single - Class of 'x'	5	
	* Incident - Single - Class of 'x', Category 'Y'	5	
	* Incident - Single - Class of 'x', Category 'Y', Subcategory 'Z'	5	
	* Incident - Single - Due in 'X' Days	5	
	* Incident - Single - Flag of 'x'	5	
	* Incident - Single - Follow-up Required	5	
	* Incident - Single - Involved Person with Flag of 'x'	5	
	* Incident - Single - New Incident	5	
	* Incident - Single - New Investigation by site 'x'	5	
	* Incident - Single - No Activity in 'x' Days	5	
	* Incident - Single - Owner Role of 'x' - Status 'Y'	5	
	* Incident - Single - Owner WorkGroup of 'x' - Status 'Y'	5	
	* Incident - Single - Re-opened after Close	5	
	* Incident - Single - Review type of 'x'	5	
	* Incident - Single - Site 'X'	5	
	* Incident - Single - Site 'X' - Building 'Y'	5	
	* Incident - Single - Site 'X' - Building 'Y' - Location 'Z'	5	
	* Incident - Single - Site 'X' - Building 'Y' - Location 'Z' - Section 'A'	5	

Every event ties to a query of a similar name.

When you find the premade queries that fit your needs you can start building an application. For this example we will be using Incident – Single – Class of X. Double-click on the event and navigate to the Queries Tab.



Event Description: Incident - Single - Class of 'x'

Queries Selected For Content

Application	Query Description
Standard Event Pak -	Incident - Class 'x'

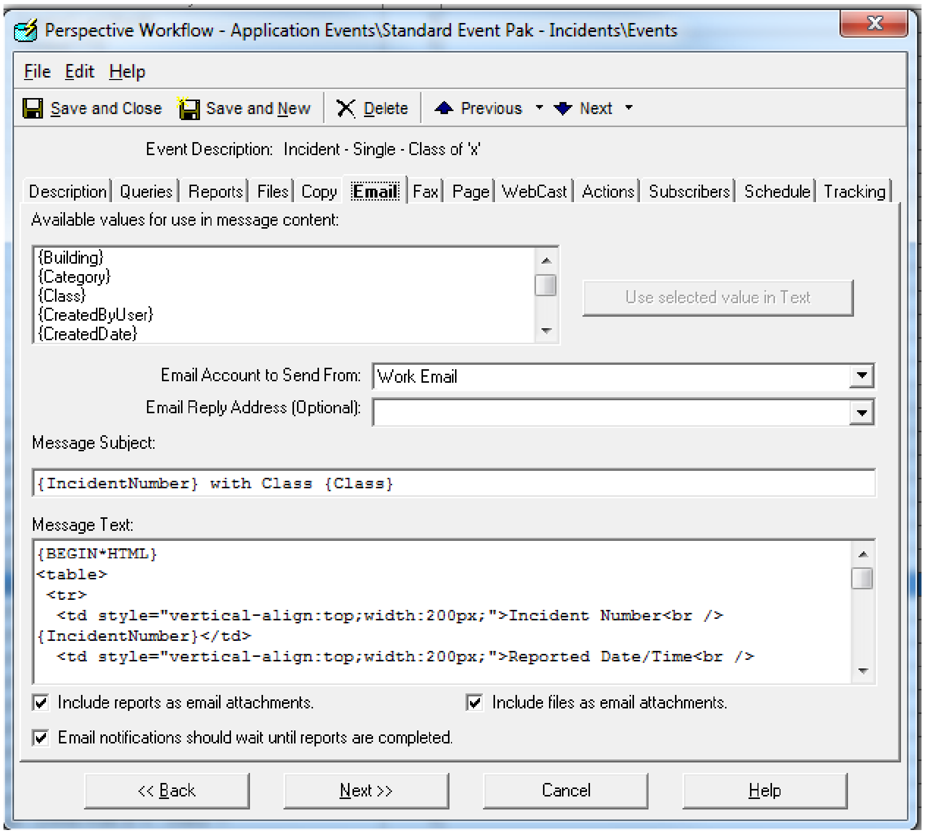
Event Trigger Parameters

Question	Answer
What Class value would you like to filter by?	
How far back would you like to search?	

Check that the query being referenced is in the same application as the event you are currently working on. This is shown under Queries Selected for Content.

In the Event Trigger Parameters you will see the two parameters you can specify. Enter a Class value, such as Criminal, for the top and how many days you wish to include in the search. Because this event is only returning a single record you should only want one day to be checked so enter 1.

Navigate to the Email tab.



Event Description: Incident - Single - Class of 'x'

Available values for use in message content:

{Building}
{Category}
{Class}
{CreatedByUser}
{CreatedDate}

Email Account to Send From: Work Email

Email Reply Address (Optional):

Message Subject:

```
{IncidentNumber} with Class {Class}
```

Message Text:

```
{BEGIN*HTML}
<table>
 <tr>
  <td style="vertical-align:top;width:200px;">Incident Number<br />
{IncidentNumber}</td>
  <td style="vertical-align:top;width:200px;">Reported Date/Time<br />
```

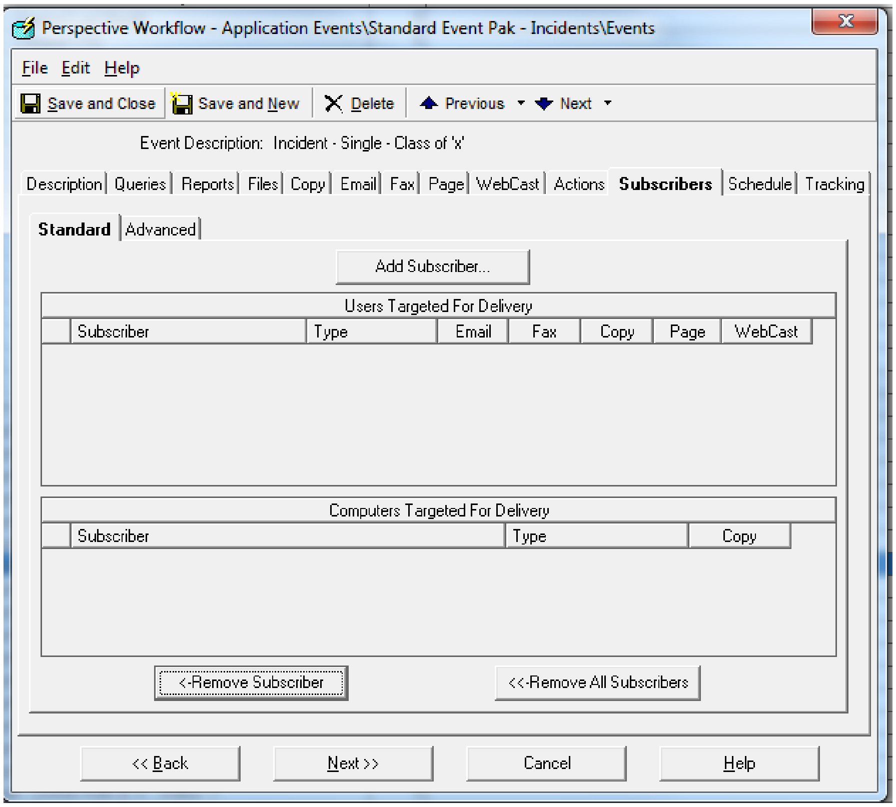
☑ Include reports as email attachments. ☑ Include files as email attachments.

☑ Email notifications should wait until reports are completed.

In the Email Account to Send From be sure to select your specified email account from the drop down.

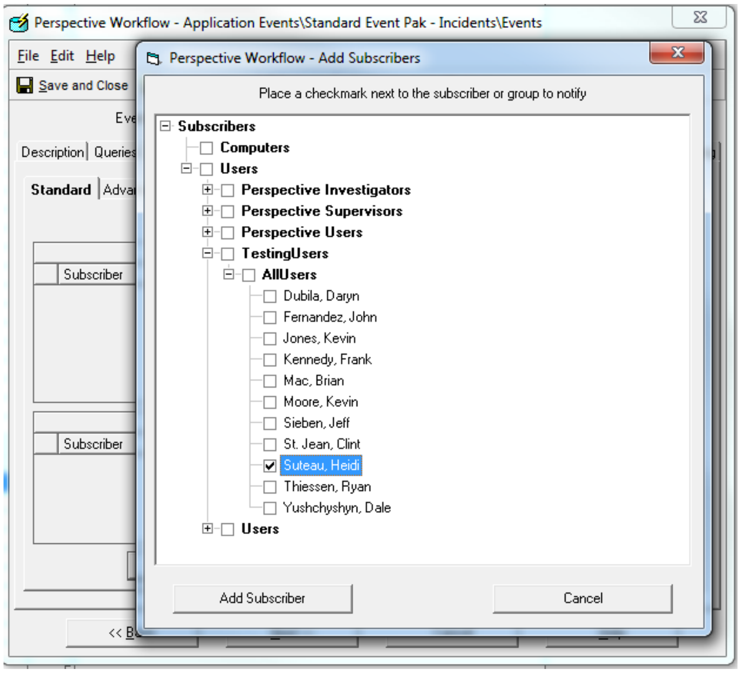
If you are comfortable editing HTML feel free to edit the message text otherwise the email will contain general information about the record returned.

Navigate to the Subscribers tab



Event Description: Incident - Single - Class of 'x'

Click Add Subscriber.

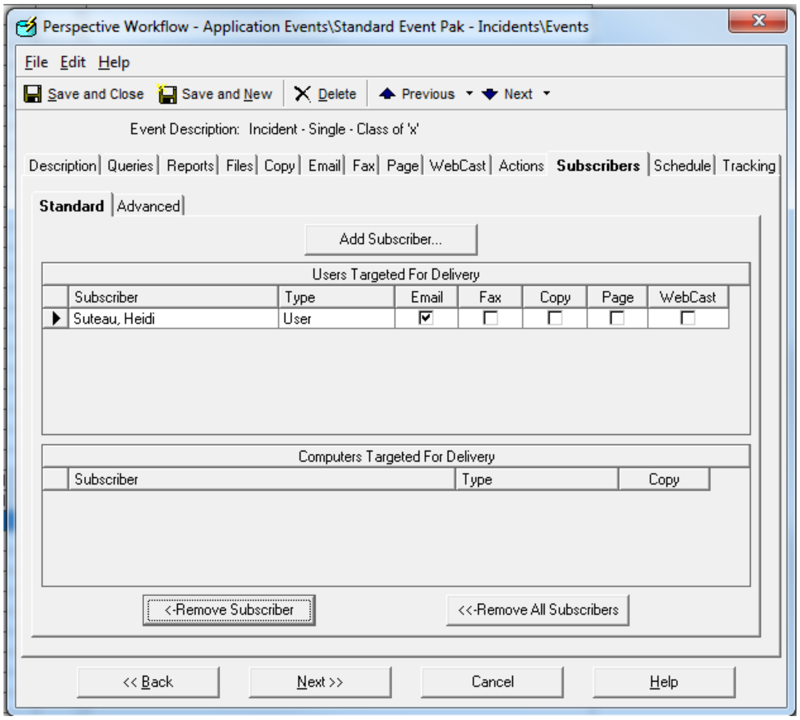


Place a checkmark next to the subscriber or group to notify

☑ Suteau, Heidi

Select the user you want the email to go to.

Click Add Subscriber



Event Description: Incident - Single - Class of 'x'

Users Targeted For Delivery

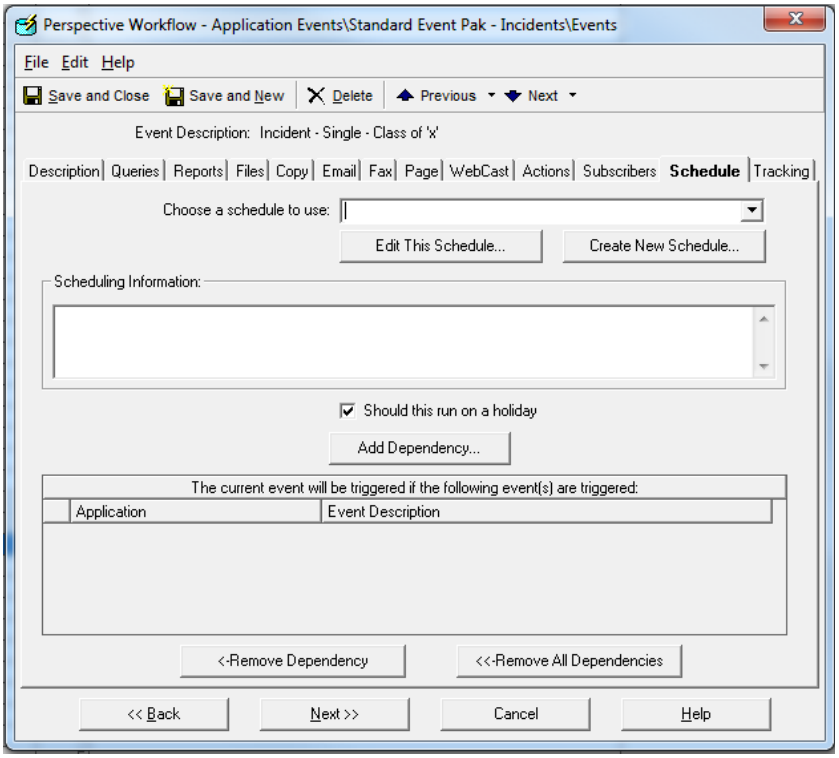
Subscriber	Type	Email	Fax	Copy	Page	WebCast
Suteau, Heidi	User	☑	☐	☐	☐	☐

Computers Targeted For Delivery

Subscriber	Type	Copy

Double check that Email is checked off beside the subscriber name.

Navigate to the Schedule Tab.



Event Description: Incident - Single - Class of 'x'

Choose a schedule to use:

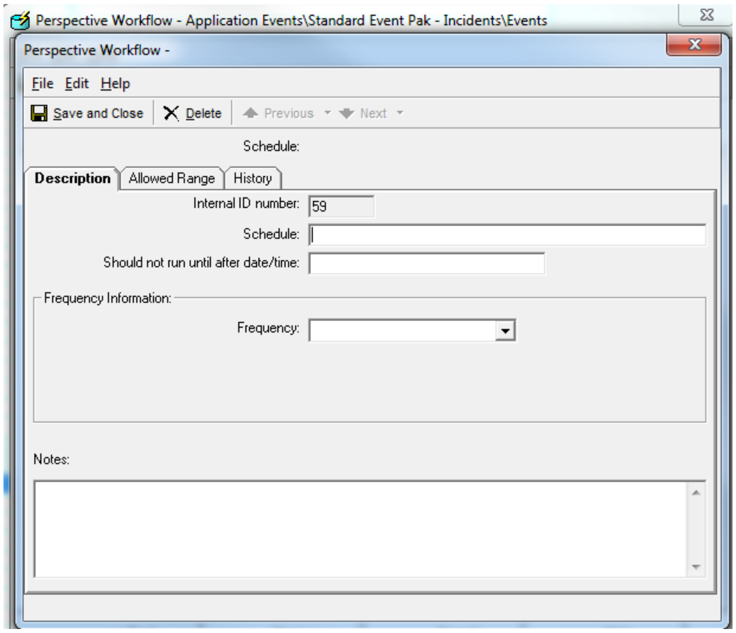
Scheduling Information:

☑ Should this run on a holiday

The current event will be triggered if the following event(s) are triggered:

Application	Event Description

You can either select a premade schedule from the drop down or Click Create New Schedule. For this example click Create New Schedule.



Schedule:

Internal ID number: 59

Schedule:

Should not run until after date/time:

Frequency Information:

Frequency:

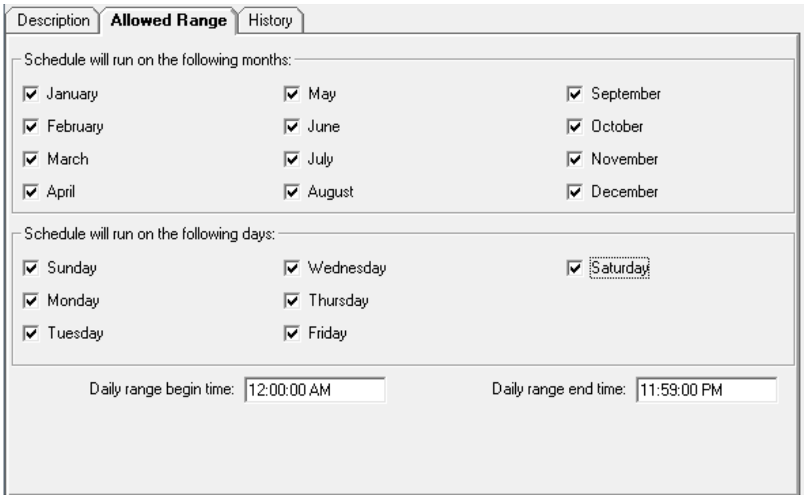
Notes:

We will create a schedule that runs daily at 07:00 h (7:00 AM) local server time.

On the ‘Description’ tab, enter the following in the fields (enter exact – if there is no value after the colon, leave field blank:

1. Schedule: Daily @ 7:00 AM
2. Should not run until after date/time:
3. Frequency: Daily
4. Daily Time to Run: 07:00 AM

On the ‘Allowed Range’ tab, ensure there are checks all months and all days are checked. Leave values in ‘Daily Range’



Schedule will run on the following months:

☑ January
☑ February
☑ March
☑ April
☑ May
☑ June
☑ July
☑ August
☑ September
☑ October
☑ November
☑ December

Schedule will run on the following days:

☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Daily range begin time: 12:00:00 AM

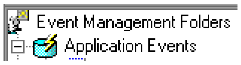
Daily range end time: 11:59:00 PM

Click Save and Close.

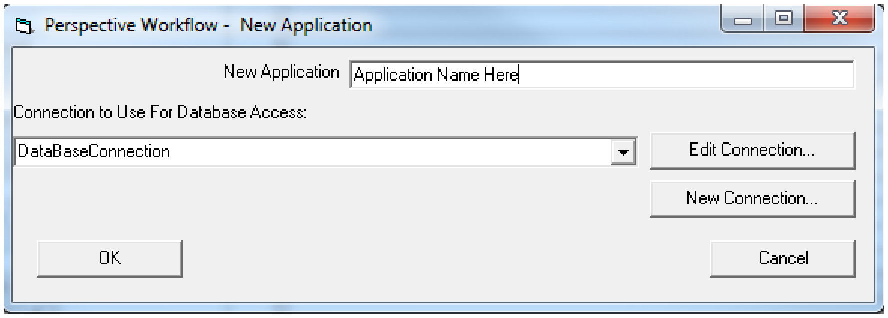
You have now customized and event.

Building a Custom Event Pak

Select Application Events



Click New Application.



New Application: Application Name Here

Connection to Use For Database Access: DataBaseConnection

Name your application and select your database connection from the drop down.

Go through all the premade queries that fit your needs. Select them one at a time and either use Edit>Copy or ctrl-C. Now select your new Event Pak and open Query Definitions. Use Edit>Paste or ctrl-v to paste the query in. You can copy and paste a query to be used multiple times. Just be sure to rename it in the Description tab.

Now go through the premade events and copy and paste them like you did the queries. For each one open and Navigate to the Queries tab. Make a note of the name of the query it is referencing. Click Remove All Queries. Now Click Add Query and find the one it was referencing before. You must do this for the events that are moved otherwise they will be referencing the wrong application query and will not work.

Feel free to rename queries and events to better distinguish what they do. For example you can rename Incident – Single – Class of ‘X’ to be Incident - Single – Class Criminal if it is Criminal you are searching for.

Fill in the blanks for what you wish to search, set up a schedule and select a subscriber and you should be ready to go.

STEP 6 User Acceptance Testing

Every implementation of a new Information System should be tested before passing the system into a production (“Go Live”) state. The degree to which you test the application can range from casual to formal.

Determine If Your Company Has Testing Standards

Find out if your Company has testing standards that must be met. There are three possible sources for this information:

- Project Management Department
- Information Technology Department
- Quality Assurance Department

Other departments may also have test standards that you need to check, so researching this fully is recommended.

Once you have completed your research, determine if the standards apply to the Implementation of Perspective or its related products.

Test Cases

The next step is to define which component applications will be tested. Perspective, Workflow, and Perspective Portal are highly configurable. Other component applications such as Focal Point and Visual Analysis have fewer options for setup and likely require less testing.

Examples of the most common are the following:

- Confirm Role X has its form and field privileges configured correctly.
- Confirm Role Y has its special functions configured correctly.
- Determine if there are enough fields to fully qualify an incident of category Z.

Design Your Test Cases

Each test case should have three elements:

- A description and or title for the the test case.
- A list of steps to complete the test.
- What results are expected during the test.

Example Test Case

Test Number	**#1**	
Description/Title	**Log In and Exit Application**	
Steps	1	Click on the Perspective Shortcut
	2	Type “Dale” in the User field
	3	Type “Security” in the Password field
	4	Click the Logon button
	5	Wait until the Perspective Dashboard displays
	6	Click on File and select Exit
Expected Results	Perspective should launch and exit error free	

The degree of definition for each step can be specific, as in the above example, or can be vague, dependent on the degree of formality required for your testing process. As a general rule, a test should be written for each requirement that there is for the system, but occasionally one test may suffice to cover multiple requirements.

Test the Application(s)

Running through the tests should be completed at least once prior to deployment of the product. A second round of testing is only recommended if significant changes to the configuration were needed after completing the first round.

While the amount of time required to complete your testing is highly dependent on the number of test cases and steps within each test case, it is generally recommended that a one to two week period be set aside to complete this.

Document Your Findings

During the testing process, the testers should maintain an Issue Log. The issue log should be used to document each time a test did not obtain the “Expected Result”. It can also be used to document any unexpected behavior of the product being tested.

An issue log should, at a minimum, contain the following:

- An Issue Number.
- A description of the issue.
- Date that the issue was found.

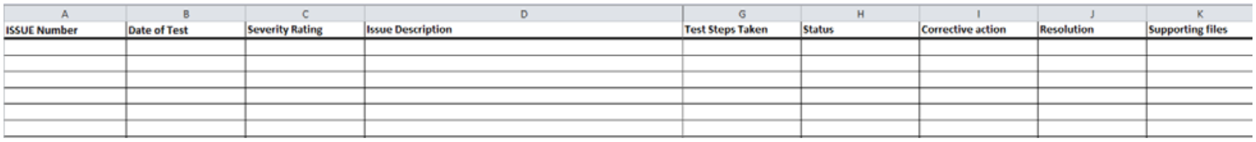
- A Severity Rating for the issue.
- A status field.
- Steps taken to correct the issue.

<u>Use of Severity Ratings:</u>

Severity ratings are used in order to triage the importance of the issues. A list of acceptable values, as well as the criteria necessary to assign the rating to an issue, should be provided to the testers prior to the beginning of testing.

A number of products exist for documenting issues discovered during testing, which your organization may have access to. If your organization doesn't have a formal tool, a simple spreadsheet like the following example works.

Example Issue Log



A	B	C	D	G	H	I	J	K
ISSUE Number	Date of Test	Severity Rating	Issue Description	Test Steps Taken	Status	Corrective action	Resolution	Supporting files

Resolve the Issues

Issues can be categorized in a number of ways:

1. Product Education/Functionality Issues—These issues are caused by a misunderstanding of how the product operates.
2. Visibility Issues—These issues can be related to either fields or forms that a specific user group should not have access to. These are generally caused by a misconfiguration of the product.
3. Data Security Issues—These issues are related to the ability of a user to view a group of records. This issue could be the ability or the inability to see restricted records. This could indicate a misconfiguration or a design problem with the data security model.
4. Label Issues—These issues are associated with any field or form label which should be modified for a better understanding of what information is placed into the field or the message that is displayed to the user.
5. Error message Issues—These issues are present when a user follows a specific list of steps and consistently receives an error message.

Each issue will then need to be resolved, by a number of ways:

- Formal Product Training.
- Configuration of a label.
- Configuration of a field.
- Correction of the data security element.
- Escalation of issue to PPM support.
- Request of a product functionality enhancement.

Most issues that are encountered will probably be resolved by the correct configuration of the component, but occasionally a “Go” or “No Go” decision will be required in order to proceed.

STEP 7 “Go Live”–Launch your Perspective System

Develop your Support Plan(s)

Prior to “Go Live”, a support plan should be in place to determine the escalation path for resolving issues that are encountered during day-to-day use.

There are two plans that are needed:

1. “Go Live” support Plan—Generally during the first two weeks of using a program, an above average number of issues will be encountered. Quite often these are simple, “How do I do that again?” questions, but occasionally more serious issues are encountered.
2. Maintenance Support Plan—Once the product has been utilized for a couple of weeks, the number of support questions should begin to dwindle. A maintenance support plan may be necessary in cases where the escalation path will differ from the “Go Live” Support Plan.

   In cases where simple issues are encountered, a plan to use your product champions to assist in the triaging of the issue could help streamline the resolution process.

   In cases where more serious issues are encountered, it may be necessary to contact PPM Support Services for assistance.

   Issues that are investigated with PPM Support should also be communicated to the user community, so that these issues are not repeatedly investigated.

Develop a Training Plan

Introduction

It is imperative that your staff has the necessary working knowledge of the data entry process for Perspective. With adequate training, the qualitative data inputted into Perspective will greatly increase, providing accurate reports and meaningful statistics.

It is not necessary for all staff members to have a full working knowledge of every aspect of Perspective; however, users must be competent in the fields and forms they are expected to use. In addition, supervisors must have a working knowledge of Perspective to provide suitable advice and expertise to subordinates.

After any formal training, it is important that users have the opportunity to practice what they have learned. The sample database is an excellent resource, as users can have hands-on practice without any concern of corrupting the “live” data.

Planning a Training Program

The training offered should be relevant to the user’s role and function in Perspective. There is no advantage in training an officer on different aspects of the program (i.e.: Analysis Expert) when he or she will not have access to it. After determining the training needs for each role, prepare a syllabus of the topics to be covered. This will not only keep you on track during the training, but also ensure your staff is getting the correct information. All training should be conducted on the sample database.

A sample database is typically installed with your program. It allows for practice without the concern of corrupting a “live” database. However, sample databases are not an exact duplicate of your live database and could be confusing to some users. To avoid this and to enhance training, it is recommended that the default database be cloned, and the cloned database be used in place of the sample database. All sensitive information can be removed to ensure privacy and security. The cloned database allows users to practice on a database that mirrors their live one, with the same privileges and rights they would normally have.

Training Offered by PPM

PPM 2000 offers a variety of training options ranging from on-site to online training. Each session can be tailored to meet your individual needs.

A sample of sessions PPM offers

- User Basic – Part 1
- User Basic – Part 2
- Analysis Expert - Basic
- Analysis Expert - Advanced
- Administration - Form and Interface
- Administration - Roles & User Accounts
- DispatchLog User Basic – Part 1
- DispatchLog User Basic – Part 2
- Investigation and Case Management
- Visual Analysis
- E-Reporting

PPM posts all upcoming training sessions on its website (excluding on-site client training) at www.ppm2000.com/home_services.asp. Registration for on-line training is available at www.ppm2000.com/services/services_Training.asp.

On-Site Training

A qualified PPM Consultant will travel to your site and provide Administration & User Training, in addition to providing individualized consulting on all aspects of the program. The training is customized to meet your organization’s needs and ensures that all additional program options are covered. This is a hands-on training session; therefore, all users are required to access to a computer and the Perspective program.

A “Not to Exceed” quote including travel costs, accommodations, and meals can be provided through your PPM Sales Representative.

Edmonton Regional Training

Throughout the year, PPM provides several three-day training workshops at their head office in Edmonton, Alberta, Canada. The first two days include Basic User & Administrator Training Operations, and on the third day Advanced Techniques are covered. Training is hands-on with PPM training lab and includes computers equipped with the most recent version of Perspective.

PPM’s website provides a calendar with all upcoming training workshops, locations, and topics. Registration can be completed online at www.ppm2000.com/events/events_hands-on_training.asp.

Online Training

The online training workshops allow users to gain valuable knowledge of Perspective without having to leave their office. The training is conducted through WebEx Training Center and is one hour in length.

PPM's website provides a calendar with all upcoming training workshops, locations, and topics. Registration can be completed online at www.ppm2000.com/events/events_online.asp.

PPM also offers custom online training. These training workshops are up to four hours each and cover a topic, or topics, of your choice. Most online workshops can be recorded and used for repeated training for you and your staff. Arrangements can be provided through your PPM 200 Sales Representative

Annual User Conference

PPM hosts an annual users' conference that provides users with the following:

- Hands-on training on a variety of topics (basic and advanced).
- Workshops on best practices with Perspective.
- Networking lunches.

PPM's management, developers, trainers, and consultants are available during the conference for one-on-one meetings to discuss how Perspective can meet your incident reporting/case management needs.

Details about the Annual User Conference and location are available on the PPM website: http://www.ppm2000.com/events/events_psv_users_conference.asp.

Develop a Product Update Plan

PPM releases updates to Perspective and other components at least once per year. Each new release comes with potential functionality improvements that could be useful to the user community. Advanced planning for updating the software can assist in streamlining the effort required to get the product operational with the minimum amount of downtime.

SaaS clients are always early adopters of the new version, as it is deployed almost immediately after release. Keeping up to date on the "What's New in Perspective" online session will help an organization prepare for the new changes. Update training and communication of the changes to the user community are critical for SaaS clients.

For clients who host their own system, a plan should be in place so that the process of updating Perspective to the newer versions exists and can be planned for. Generally this plan will need to include your IT department, but in some cases will also require a project manager.

Review and Update Procedures

The implementation of Information Systems products often result in the need for process changes. Any process or procedure that is related to the use of Perspective or its components should be reviewed and updated so that they are relevant.

Suggestions of Procedures or documentation that may currently be in place and need modification are:

- Incident response procedures.
- Incident documentation procedures.
- Investigation procedures.
- Activity response procedures.
- Emergency response procedures.
- Yearly reporting standards.

A review and update should be completed prior to “Go Live” and then revisited again post “Go Live” to ensure that no further enhancements to the documentation is required.

Setup Remaining User Accounts

During the initial build of Perspective, most likely, not every user of the Perspective will have taken part in the development of the database. It is also possible that new hires or terminations of existing employees took place. An evaluation of current users versus “Go Live” users should be completed just prior to training the users.

Communication to each user as to their login credentials should follow the setup.

Deletion of any test accounts that were utilized for development should be completed during this stage.

As a general rule the user accounts should remain locked in the production database until the date of “Go Live” to ensure that no early use of the database can occur.

Train Your Users

When training users, there are some specific points that PPM recommends:

- **Do not** train in your production database—PPM can help you set up a Training Database.
    - Once you are done your system customization, and before you go into production use, we recommend taking a back-up and using this for setting up your training environment. If it’s too late, we do recommend using a database as similar as possible to your production database.
- Train a single user group at a time (one functional group per session).

- Limit the size of the training class to 10-12 people at a time. Larger groups are more difficult to control and keep on track due to questions, issues, etc.
- Allow one computer per trainee in a sufficient training lab, so each user gets hands-on experience.
- Project the trainer's computer on a screen for all trainees to see.
- We recommend a full day of training if possible, so that the following can be accomplished:
  - Provide a walkthrough of the data entry for a standard Incident Report, based on your organization.
  - Provide all users a "scenario" or hard copy Incident Report that your user enters just as you did in the walkthrough.
  - Don't just "demo" the functionality, allow the trainees to go into the program and play.

Set a Date and "Go Live"

The final step in the implementation is to "Go Live" with the products. Setting the appropriate date is an important step in the process. Often clients will set a date which corresponds to the first day of the month, financial quarter, or fiscal year. This is often set to ensure that a full period of reporting can take place. It is strongly recommended that special consideration be given to the date, as the first week of launch can be hectic.

For example, going live with the product on a Friday, Saturday, or Sunday may not be a good idea if the support resources/product champions are not available to work through "Go Live" issues. Weekends are also generally not a good day of the week as PPM Support Services are not available in most cases to support you through critical issues that may be encountered.

A "Go Live" checklist can also be used to ensure that no step is missed during initiation.

Example "Go Live" Checklist

1. Set the date.
2. Communicate the date to the users.
3. Send the User credentials to all users.
4. Complete last minute training.
5. Provide instructions as to Login procedures as well as expected behavior that the users should expect.
6. Update Procedure Manual.
7. Communicate procedure changes to the users.
8. Notify PPM Client Service/Support of your intent to "Go Live".
9. Unlock any locked user accounts.
10. Communicate to users that the product is active.

11. Schedule a successful launch party (you earned it).

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
Web Site:	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.

PPM