Perspective™

by PPM

ADMINISTRATOR'S GUIDE

Perspective by PPM™

Version 4.0

Printed October 2013

Contents

Welcome to Perspective by PPM 2000

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

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

Perspective is available in the following four editions:

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

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

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

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

Default Admin Master vs. Users with Administrator Rights

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

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

Logon Options

1. In order to access Perspective, navigate to your Perspective Services URL: **http://<IISServer>/PerspectiveServices**. <IISServer> refers to the Perspective Web server installed during the Perspective installation process.

2. Click the **Launch Perspective** button.

3. In the Logon window, click the small icon in the top right corner to open the logon options.

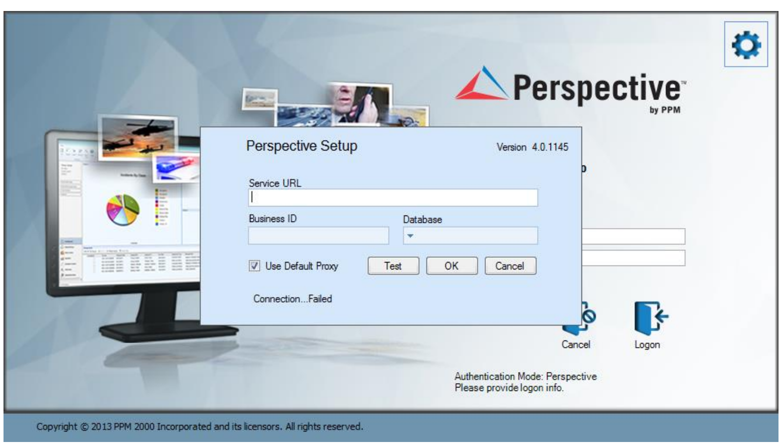
4. Specify the service path by inputting a **Service URL**. Click the **Test** button to test the connection with the URL.

5. Select the appropriate database from the **Database** lookup list.

6. If required, switch from Windows® authentication to Perspective authentication by pressing the **F5** key (only available if Windows authentication is already being used).

7. Enter the **Business Unit** (only available if using Perspective SaaS).

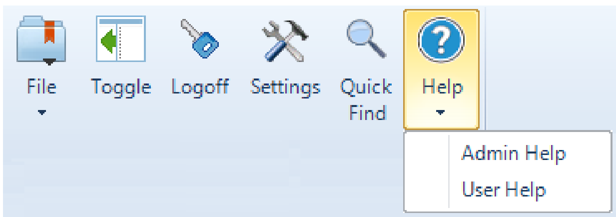
8. Click **OK** to save the changes made and proceed with the standard login.



Help Options

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

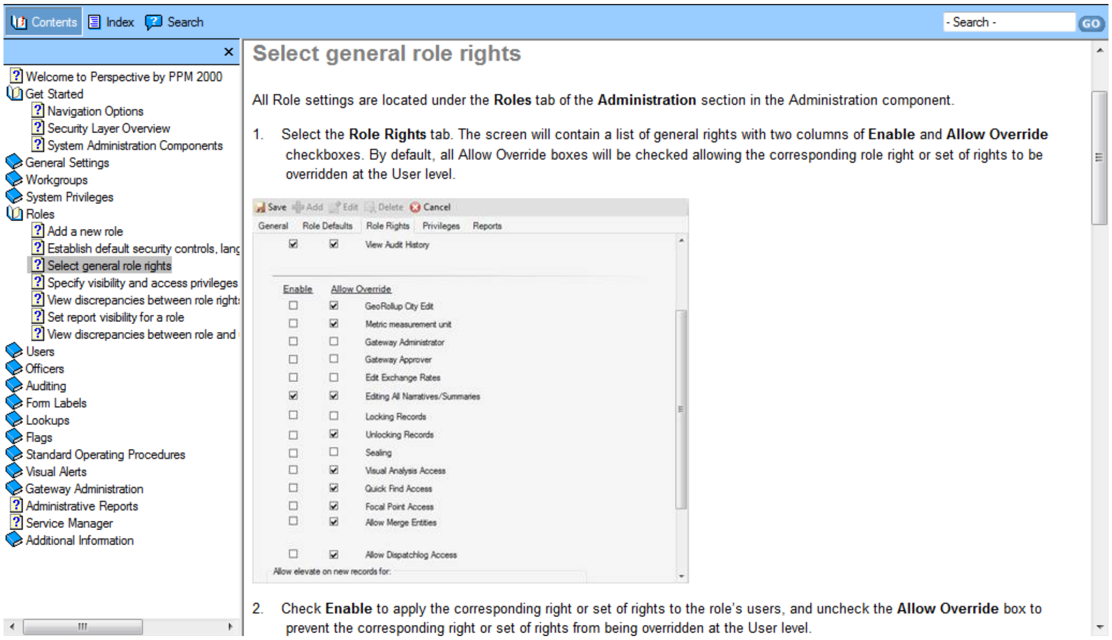
- To open one of the available Help files, click the Help icon located on the Action toolbar. Click on **User Help** to access general Help files. Select **Admin Help** to access Administrator-specific Help files.



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

Contents Tab: Browse Help by topic

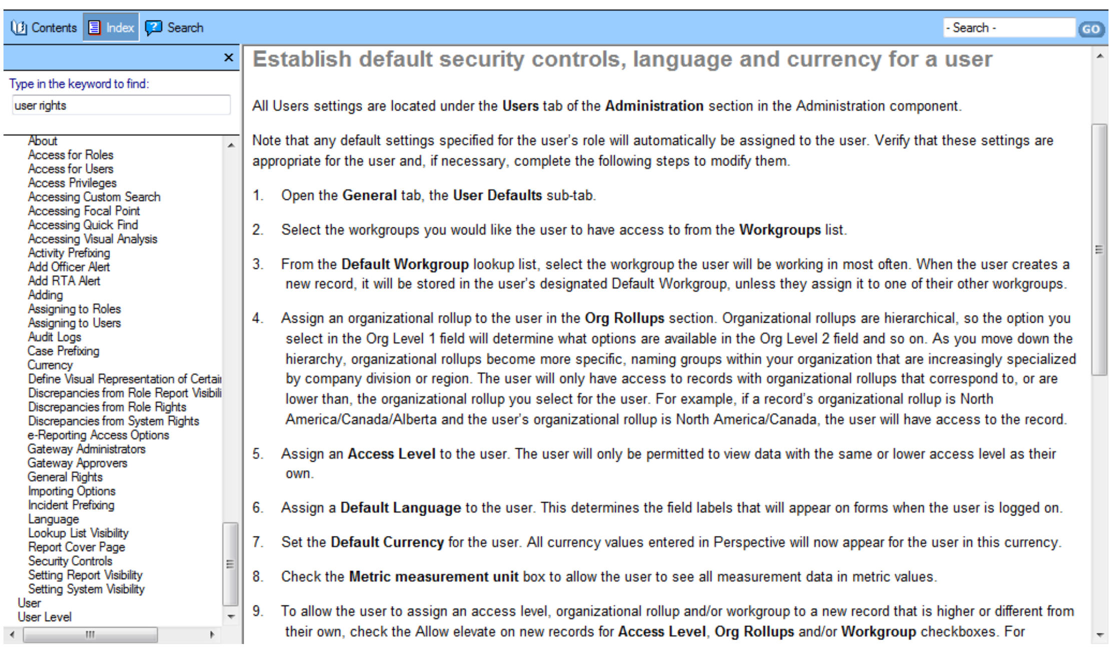
1. Click a **Contents** button to open it and view the chapters and pages contained within.
2. Then click a page icon to fill the Viewing pane with information on the selected subject.



Index Tab: Browse Help by Index

1. Scroll through the listed keywords or type a keyword to reference.

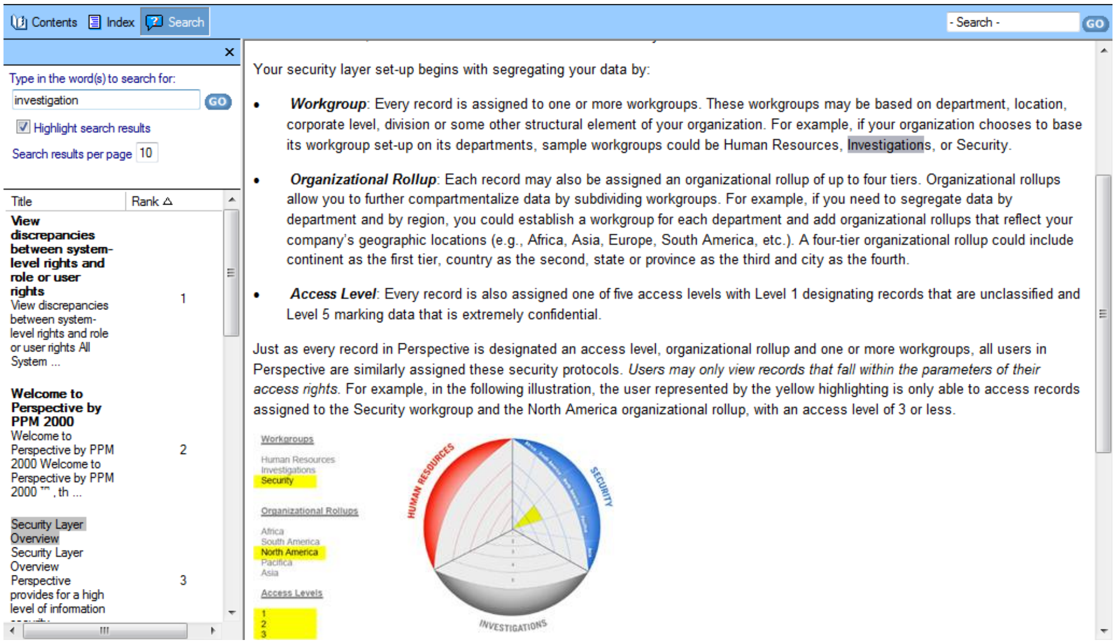
2. Click a keyword from the list to display the associated topic.



Search Tab: Search Help

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

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



Navigation Options

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

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

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

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

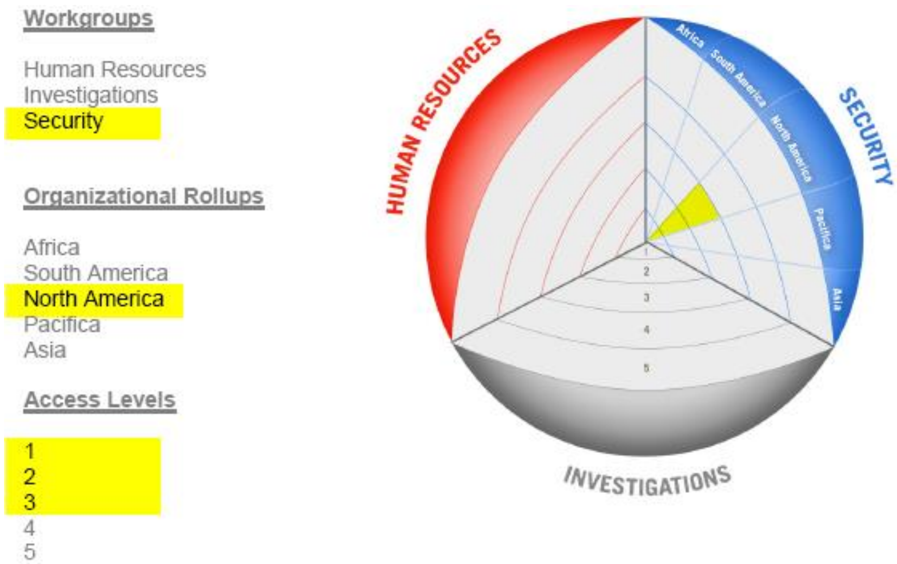
Security Layer Overview

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

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

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

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



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

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

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

System Administration Components

General Settings
General
• Assign Incident, Case (ICM and EIM only) and Activity Number formats/prefixes. • Choose the default measurement system for numeric data. • Set your organization's logo and address to print on report cover pages. • Select the default font for narratives, summaries and interviews. • Set to display your organization's privacy statement or legal notice upon logon. • Hide the All Records View option on data forms and pick lists. • Allow users to send formatted email messages.
Account Usage Policies
• Define user password and logon parameters.
Currencies
• Select the system's default currency, add new currencies and update exchange rates.
Languages
• Enter new custom languages or label sets into the system.
Administration
Workgroups
• Add a new workgroup. • Specify a workgroup's Gateway import parameters and identifier prefixes.
System Privileges
• Assign system-level visibility and access rights. • View discrepancies between system-level rights and role or user rights.
Roles
• Create a new role. • Establish default security controls, language and currency for a role. • Select general role rights. • Specify visibility and access privileges for a role. • Set report visibility for a role. • View discrepancies between role and user rights and report visibility.

Users

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

Officers

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

Auditing

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

Lookups

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

Flags

- Create a new incident or person flag.

Standard Operating Procedures (SOP)

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

Visual Alerts

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

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

Language

Languages

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

Form Labels

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

License Management

Concurrent Licenses

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

Named Licenses

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

General Settings

Set the Basic System Settings

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

Assign Incident, Case, and Activity Number Formats and Prefixes

1. Enter a prefix for all Incident Numbers, Case Numbers and Activity Numbers. If you would prefer not to have a prefix for a specific number type, leave the corresponding fields blank.

2. Choose **Identifier Formats** for Incident, Case, and Activity records from the corresponding lookup lists:

   - **CCYY-MM-#####**: This format identifies the record by the calendar year (CCYY) and month (MM) that it was added to Perspective, followed by a five digit sequential number that re-sets at the beginning of each month. For example, 2011-04-00123 identifies the 123rd incident/case/activity entered in Perspective in April 2011.

   - **CCYY-######**: This format identifies the record by the calendar year (CCYY) that it was added to Perspective, followed by a six digit sequential number that re-sets at the beginning of each year. For example, 2011-004567 identifies the 4567th incident/case/activity entered in Perspective in 2011.

   - **##########**: This is known as *flat file format*. There is no year or month preceding the number. The first record entered in Perspective will be identified by the number 0000000001, and this sequential numbering will continue indefinitely with no re-set.

Choose the Default Measurement System for Numeric Data

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

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

1. Click the Add icon in the **Organization** field. A pop-up Entity List window will open.

2. Select the name of a company whose Organization record contains the logo and address you wish to place on report cover pages. If an Organization record does not already exist for your company, use the Quick Add function at the bottom of the pick list to create one, ensuring that you add your company's logo and address to the new record.

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

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

Select the Default Font for Narratives, Summaries, and Interviews

1. Under **Default Font**, click the Add icon in the **Font Name** field. A pop-up Font window will open.

2. Choose the **Font**, **Font Style** and **Size** that will be the new system default for all narrative, summary and interview text. Note that Arial, Tahoma and Times New Roman are the recommended fonts for optimal visualization.

3. Click **OK** to close the pop-up window and apply your selection to the **Font Preview** window.

Set to Display Organization Privacy Statement or Legal Notice After Logon

1. To automatically display your organization’s privacy statement after user logon, check the **Display Privacy Statement on logon** box. This will prompt users to read the privacy statement and click OK before Perspective loads.

2. To automatically display your organization’s legal notice after user logon, check the **Display Legal Notice on logon** box. This will prompt users to read the legal notice and click OK before Perspective loads.

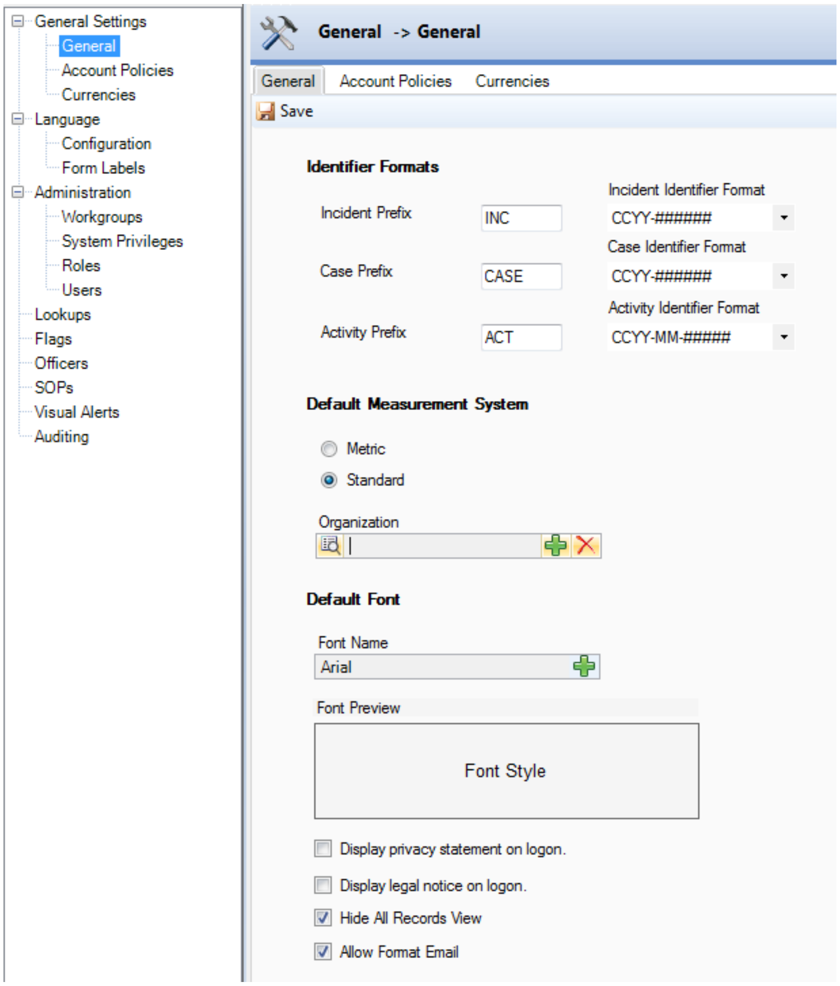
Hide the All Records View Option on Data Forms and Pick Lists

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

Allow Users to Send Formatted Email Messages

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

Click **Save** after each editing action.



Define User Password and Logon Parameters

1. Open the **Account Policies** tab.

2. Under **Password Length**, set the minimum length for user passwords (3 to 35 characters).

3. Under **Password Uniqueness**, specify whether or not Perspective should keep a history of user passwords. If yes, indicate the number of passwords to be kept in the password history from one to 10. For example, choosing 3 would require a user to go through three passwords before Perspective would allow him or her to re-use a former password.

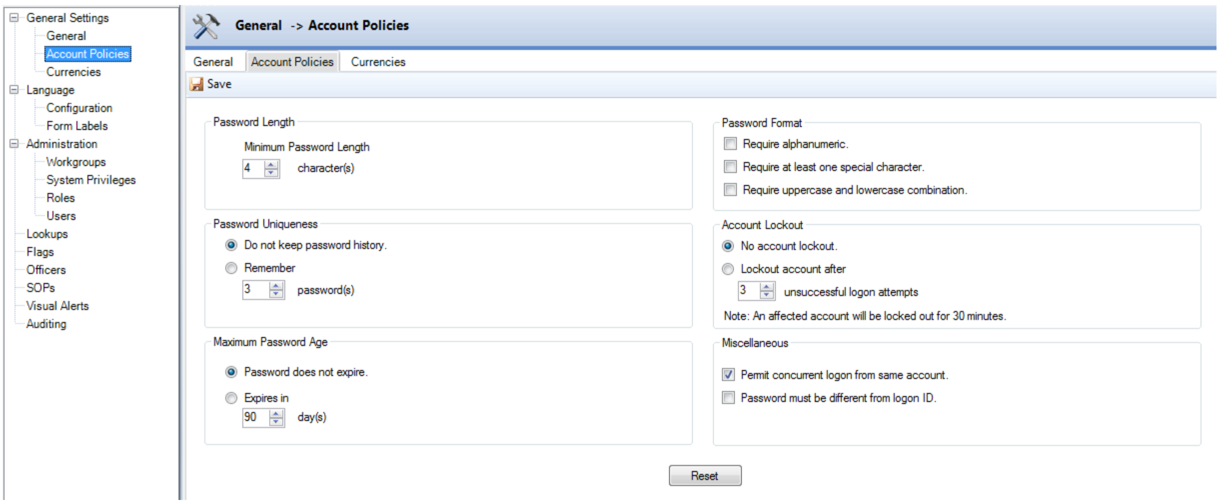
4. Under **Maximum Password Age**, indicate whether or not passwords should expire after a certain number of days (1 to 180 days). Once a user password has expired, Perspective will prompt the user to select a new password.

5. Under **Password Format**, specify if passwords must contain special characters, both letters and numbers, or both uppercase and lowercase text. You can choose all, none or a combination of these options.

6. Under **Account Lockout**, enable or disable the option to lock out users after a specified number of unsuccessful logon attempts (1 to 9 attempts).

7. Under **Miscellaneous**, choose to enable or disable users to log on to Perspective from more than one machine at the same time. Also, indicate whether passwords must be different from user IDs. It is recommended that concurrent logons should not be permitted and that passwords should be distinct from user IDs.

8. To reset the settings modified back to the old values, click **Reset**. In the confirmation window that pops up, click Yes. To save the reset, click **Save**.



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

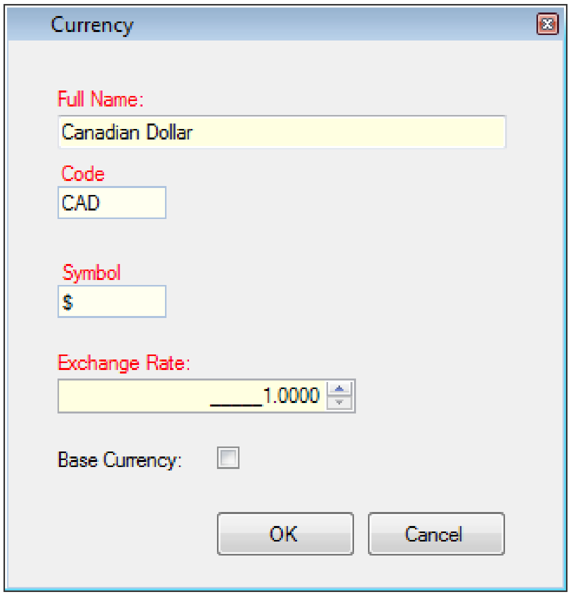
1. Open the **Currencies** tab.

2. To add a new currency to the list, click **Add**.

3. Enter the currency's **Full Name**, **Code** (abbreviated name), **Symbol** and **Exchange Rate** in the pop-up window.

4. Check the **Base Currency** box to identify the new currency as the default currency of your Perspective database. Note that it is **not recommended** that you change your Base Currency once it has been initially set. Doing so creates inconsistency in your data.

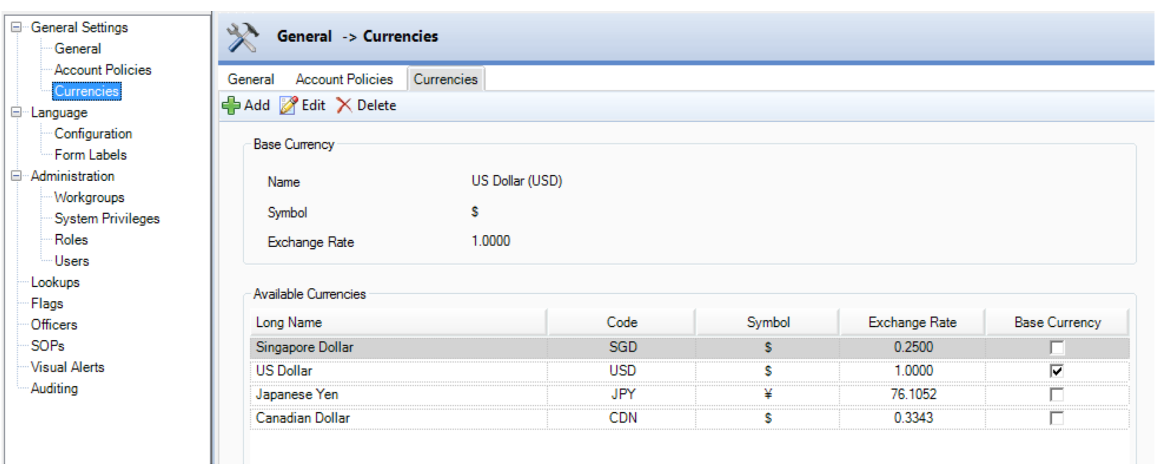
5. Click **OK** in the pop-up window, and then click **Save**.



6. To update the exchange rates of other currencies in relation to the base currency (the base currency is automatically given an exchange rate of 1.0000), select the currency, click **Edit**, modify the **Exchange Rate** in the pop-up window, and click **OK**.

7. To change the default currency listed under Base Currency, select the currency you wish to set as the new default and click **Edit**. Check the **Base Currency** checkbox in the pop-up window. In the confirmation window that pops up, click **Yes**. If you click No, the old Base Currency will be preserved. Click **OK**.

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



Workgroups

Add a New Workgroup

1. Open **Administration**, **Workgroups** in the Navigation pane, then click **Add**.

2. Enter the **Workgroup Name** and a **Workgroup Description**.

3. From the **Organization** pick list, select the organization that applies to the workgroup. If an applicable Organization record does not exist, use the Quick Add function at the bottom of the entity list to create one, ensuring that you add the logo and address of the organization to the new record. The logo and address (specifically the primary address) are recorded in the selected Organization record will appear on the workgroup’s report cover pages.

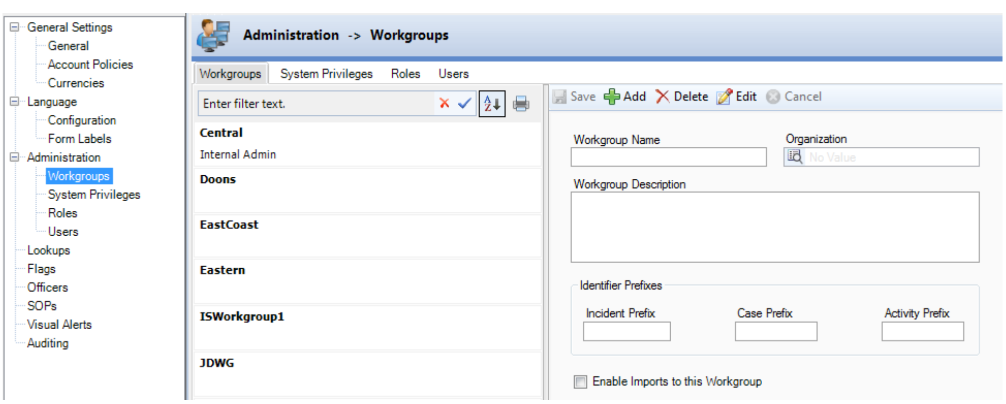
   *Note: If no organization is selected for the workgroup, the organization specified in the **General Settings** form under the **General** tab will be used by default. Organizations can also be assigned at the individual User level, overriding any selections made in General Settings and/or Workgroups.*

4. *Optional*: If you would like incidents associated with this workgroup to be identified with a unique Incident Number, Case Number or Activity Number prefix (that differs from the default prefix assigned under General Settings), enter this in the relevant **Prefix** field.

5. If you would like to allow the workgroup to import reports into the Gateway, check the **Enable Imports to this Workgroup** box. The Gateway tab will open by default. See “Specify Gateway file import options and/or e-Reporting access options for a workgroup” in the “Gateway Administration” section of this guide for further information. Note that checking this box *does not* give the workgroup access to the Gateway; it only gives them rights to submit reports to the Gateway. Only designated Gateway Administrators and Gateway Approvers are permitted to access the Gateway.

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

6. Click **Save**.



System Privileges

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

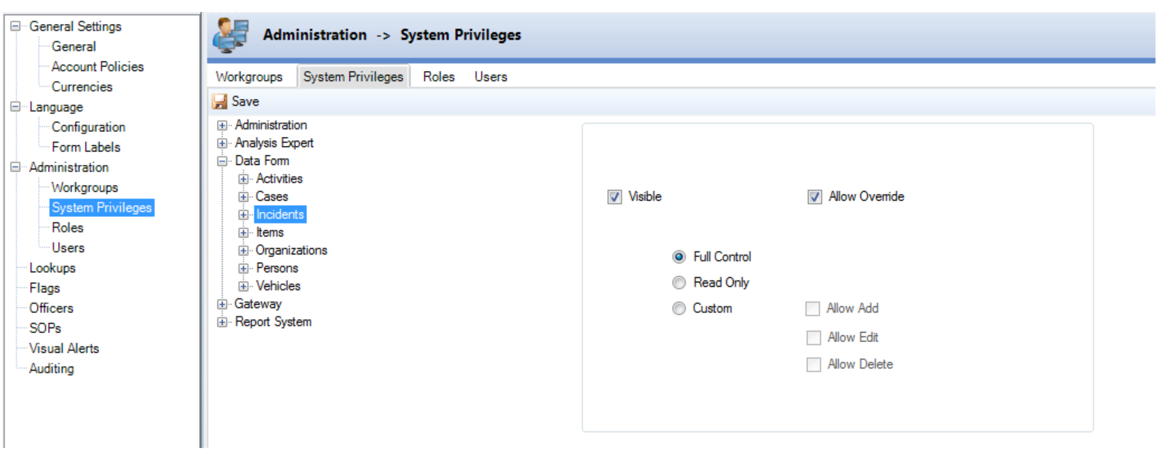
Assign System-Level Visibility and Access Rights

1. Expand the four root nodes of the tree in the left part of the Visualization pane and select a system component, data form or other entity that you wish to work with.

2. Click the checkboxes and radio buttons on the right to define what users can see and how users can manipulate the selected entity:

   - ***Visible***: Allows users to see the entity and its related buttons, icons and records, when they access Perspective.
   - ***Allow Override***: Allows system-level entity rights to be overridden at a lower level (i.e., Role or User).
   - ***Full Control***: Authorizes users to read, create, edit and delete entity records.
   - ***Read Only***: Switches entity records to the read-only mode, so that they could not be edited or deleted by users.
   - ***Custom***: Grants users the ability to create new entity records (Allow Add), read and edit existing entity records (Allow Edit) and/or delete entity records (Allow Delete).

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

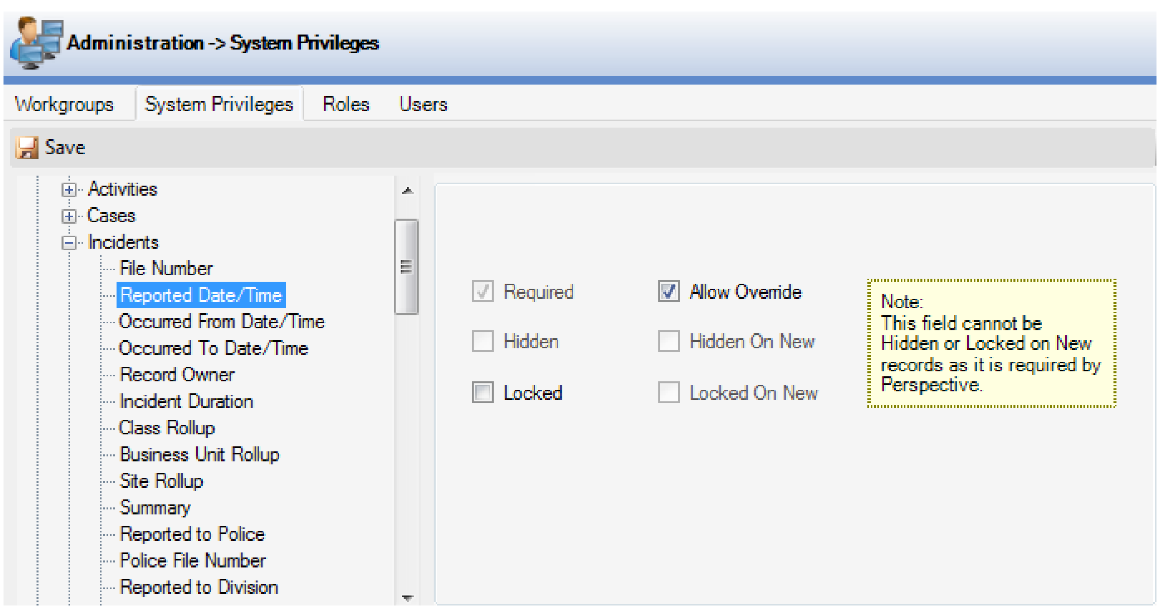


3. Expand the remaining child nodes to display complete list of fields that constitute all the entities. Select a field name in the list.

4. Use the checkboxes on the right to customize users' access rights for the selected field:

   - ***Required***: Designates the field as a required field that must be completed by users.
   - ***Hidden***: Removes the field from the interface (hidden from users).
   - ***Hidden On New*** (active when the Hidden box is checked): Unchecking this box allows users to see the field in the records that are newly created. Checking both Hidden and Hidden On New options hides the field from both new and existing records.
   - ***Locked***: Makes the field visible to the user, but not accessible for data entry or editing. In this case, the field appears greyed out and is locked from use.
   - ***Locked On New*** (active when the Locked box is checked): Unchecking this box allows users to access the field in the records that are newly created. Checking both Locked and Locked on New options locks the field from use in both new and existing records.
   - ***Allow Override***: Allows system-level field rights to be overridden at a lower level (i.e., Role or User).

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



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

6. Click **Save**.

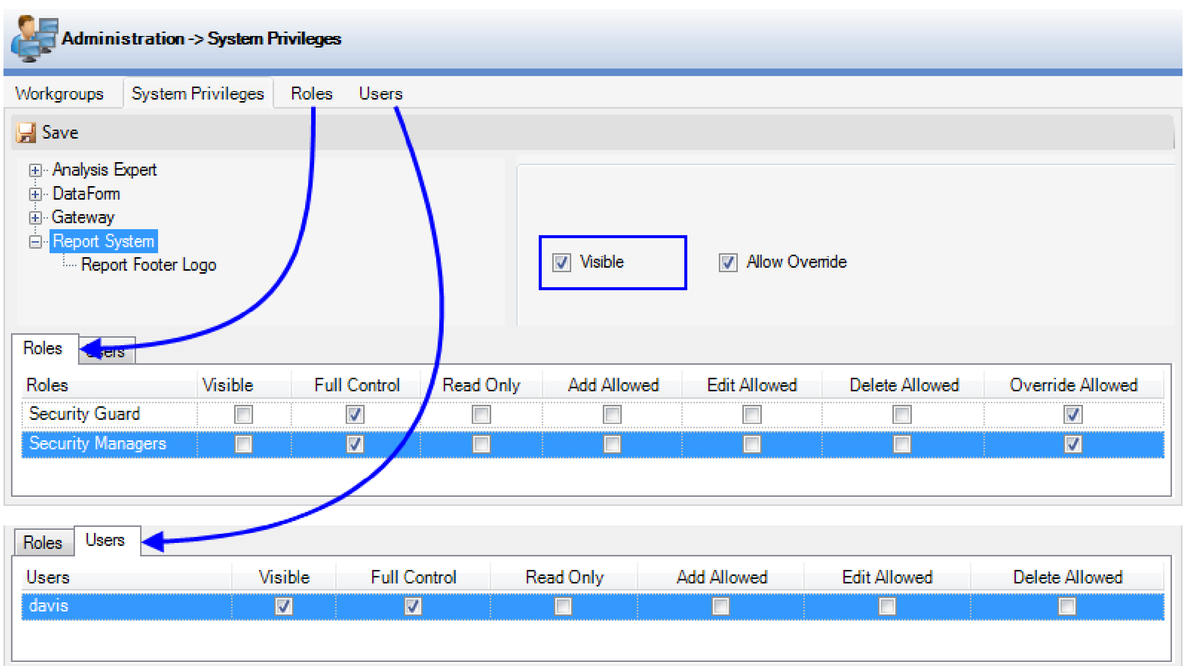
View Discrepancies Between System-Level Rights and Role or User Rights

1. Expand the nodes to see available entities and fields, and make a selection.

2. By default, the **Roles** tab at the bottom of the screen will open. If any discrepancies exist between the system-level rights for the selected entity or field and a role's rights for the same entity or field, the role and its access rights will be displayed at the bottom.

3. To view discrepancies between the role-level rights for the selected entity or field and a particular user's rights to the same entity or field, click the **Users** tab at the bottom of the screen. If any discrepancies exist, the user's ID and their access rights will be displayed below.

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

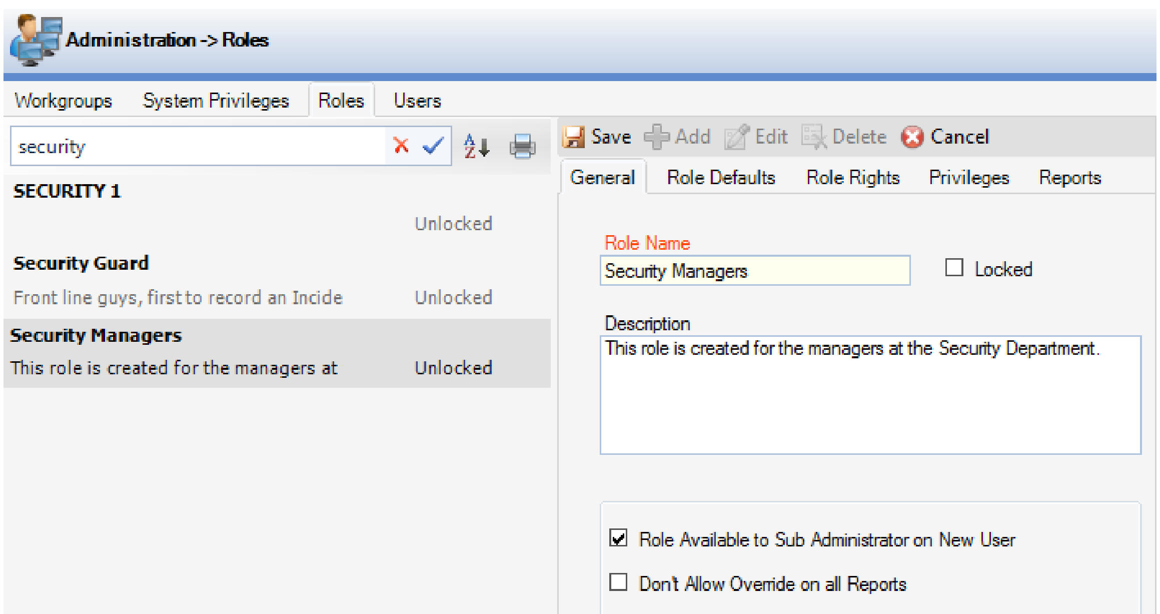


Roles

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

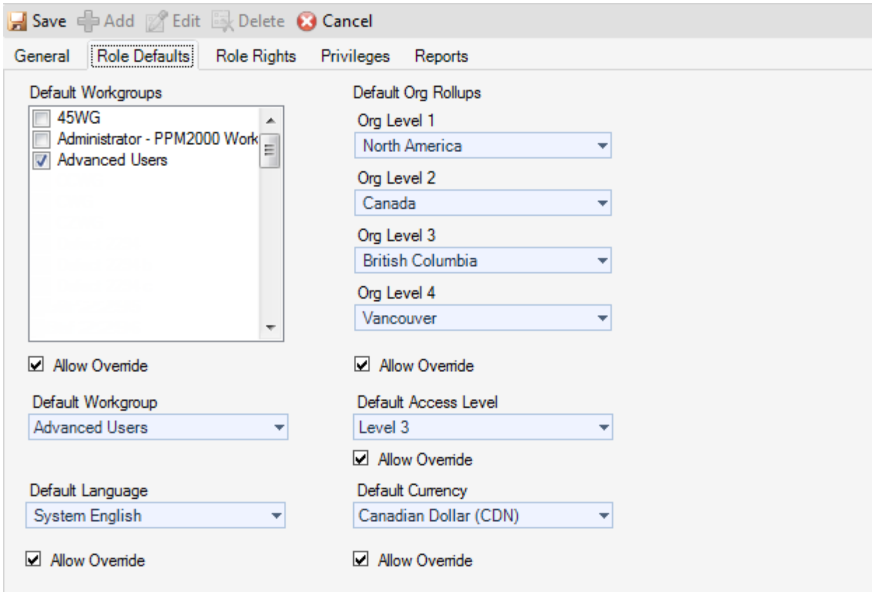
Add a New Role

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



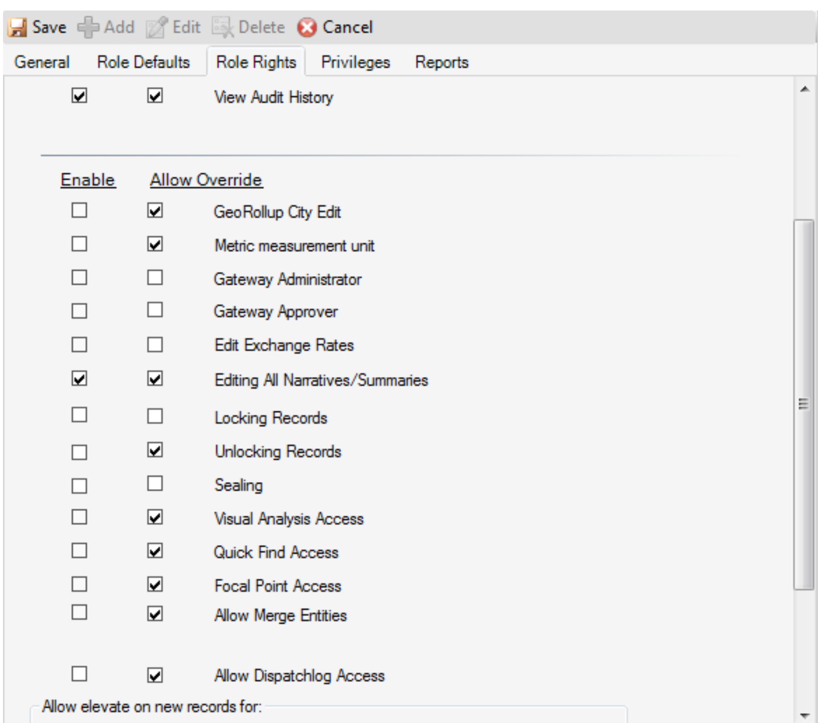
Establish Default Security Controls, Language, and Currency for a Role

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



Select General Role Rights

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



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

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

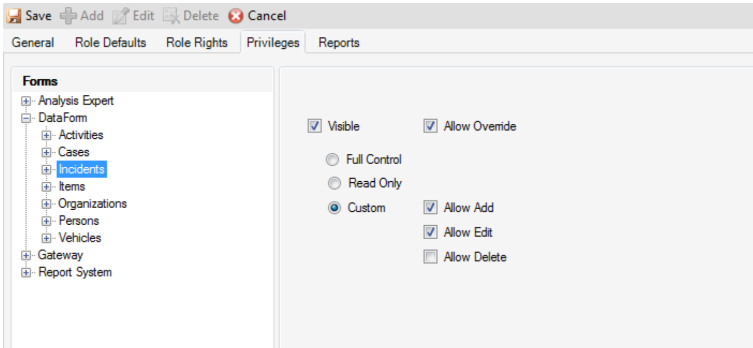
Gateway Approver	Assigns the role's users associated Gateway Approver access privileges. *Note: For more information on these roles and what they entail, see the Perspective User's Guide or Perspective's User Help.*
Edit Exchange Rates	Allows the role's users to update exchange rates under the Currencies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

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

Specify Visibility and Access Privileges for a Role

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

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

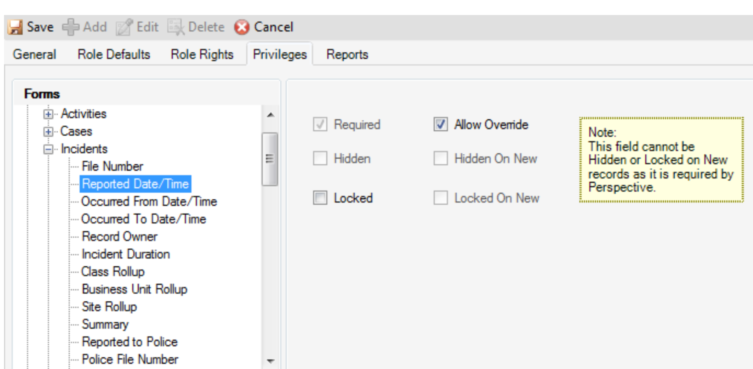


4. Expand the remaining child nodes to display a complete list of fields that constitute all the entities. Select a field name in the list. The field's system rights appear on the right.

5. To override system rights for this particular role, use the checkboxes to define the role's access rights for the selected field:

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

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



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

7. Click **Save**.

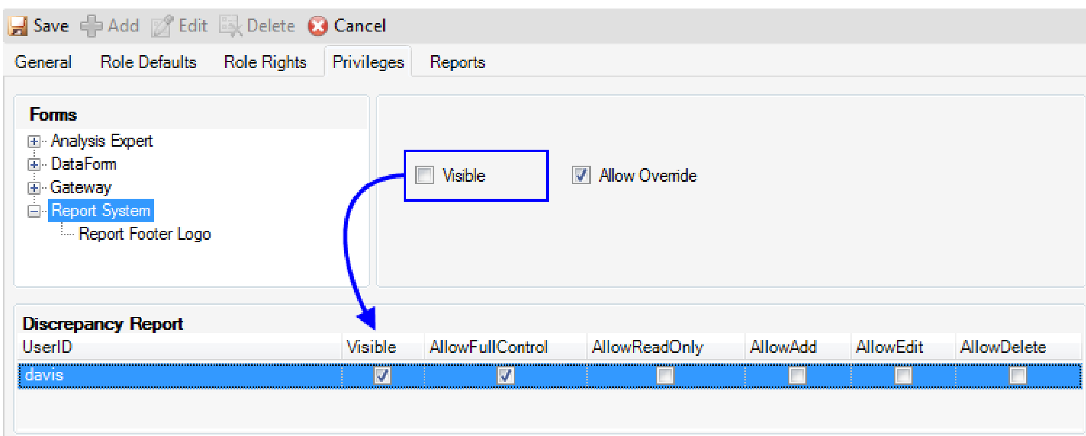
View Discrepancies Between Role Rights and User Rights

1. Open the **Privileges** tab.

2. Expand the nodes to see available entities and fields, and make a selection.

3. If any discrepancies exist between the role-level rights for the selected entity or field and a user's rights for the same entity or field, the user and their access rights will be displayed at the bottom of the screen.

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



Set Report Visibility for a Role

1. Open the **Reports** tab.

2. To allow a role's users to see reports listed under Report Title, check the **Visible** boxes beside the report names.

3. To allow any of these report visibility settings to be overridden at the User level, check the **Allow Override** box for the report, or uncheck the Allow Override box to prevent the role's report visibility from being overridden. By default, Allow Override boxes are checked, unless the **Don't Allow Override on all Reports** box has been checked on the **General** tab of this form.

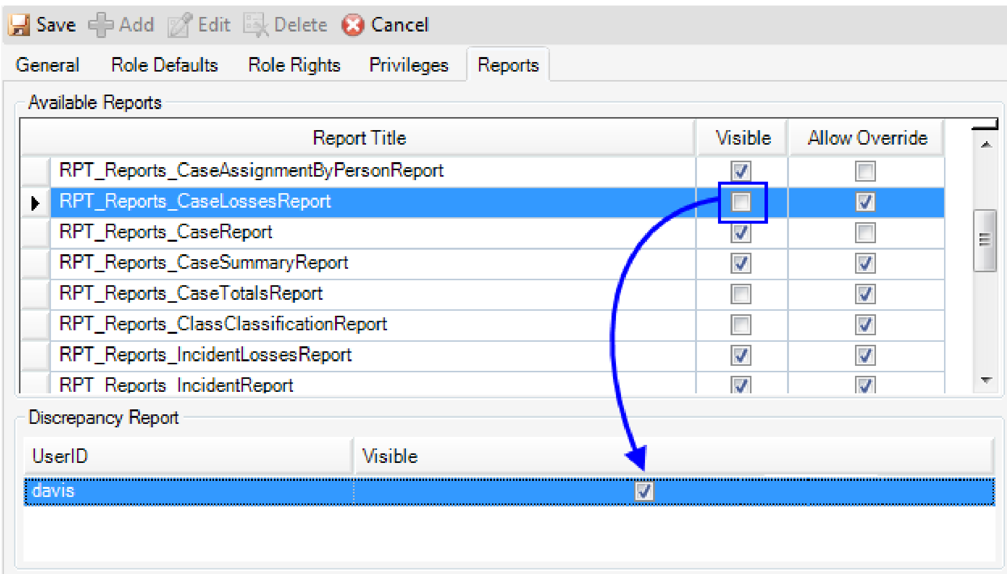
4. Click **Save**.

View Discrepancies Between Role and User Report Visibility

1. Open the **Reports** tab.

2. Select a report listed under Report Title.

3. If any discrepancies exist between the role's visibility for the selected report and a user's visibility for the same report, the user and their visibility setting will be displayed at the **Discrepancy Report** pane.

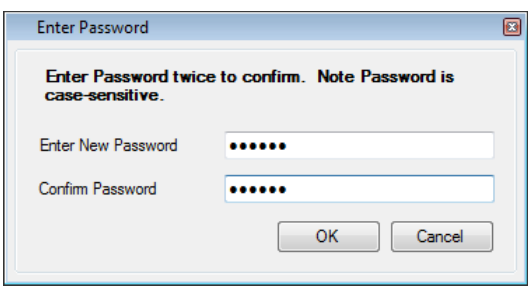


Users

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

Add a New User

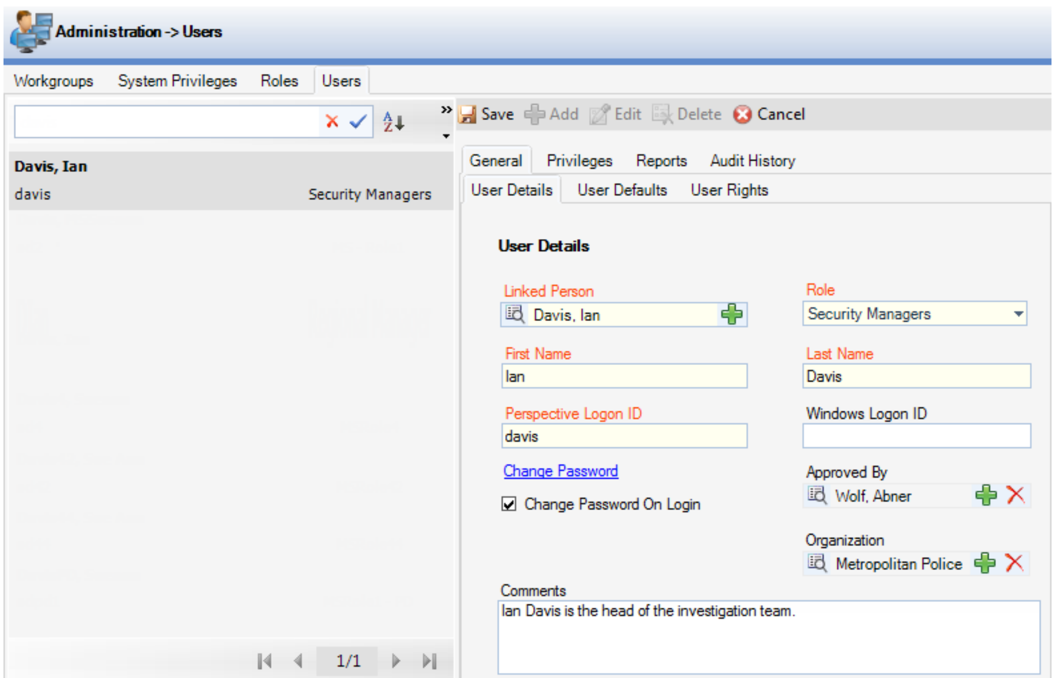
1. Click **Add**.
2. Select the name of the user from the **Linked Person** pick list. If a Person record does not already exist for the user, use the Quick Add function to create one. The **First Name** and **Last Name** fields will now automatically populate with information drawn from the linked person’s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



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

9. Select the organization that the user belongs to from the **Organization** pick list. If an applicable Organization record does not already exist, use the Quick Add function to create one, ensuring that you add the organization's logo and address to the new record. The logo and address appearing in the selected Organization record will now appear on the user's report cover pages. If no organization is selected for the user, the organization specified for the user's workgroup will be used. If none is specified for the user's workgroup, then the organization selected under the General tab of the General Settings form will be used by default.

10. Enter any other notes in the **Comments** box. You have now completed the **User Details** form. Before saving a user's record, you must enter required default settings for the user account under the User Defaults sub-tab.



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

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

1. Open the **General** tab, the **User Defaults** sub-tab.

2. Select the workgroups you would like the user to have access to from the **Workgroups** list.

3. From the **Default Workgroup** lookup list, select the workgroup the user will be working in most often. When the user creates a new record, it will be stored in the user's designated Default Workgroup, unless they assign it to one of their other workgroups.

4. Assign an organizational rollup to the user in the **Org Rollups** section. Organizational rollups are hierarchical, so the option you select in the Org Level 1 field will determine what options are available in the Org Level 2 field and so on. As you move down the hierarchy, organizational rollups become more specific, naming groups within your organization that are increasingly specialized by company division or region. The user will only have access to records with organizational rollups that correspond to, or are lower than, the organizational rollup you select for the user. For example, if a record's organizational rollup is North America/Canada/Alberta and the user's organizational rollup is North America/Canada, the user will have access to the record.

5. Assign an **Access Level** to the user. The user will only be permitted to view data with the same or lower access level as their own.

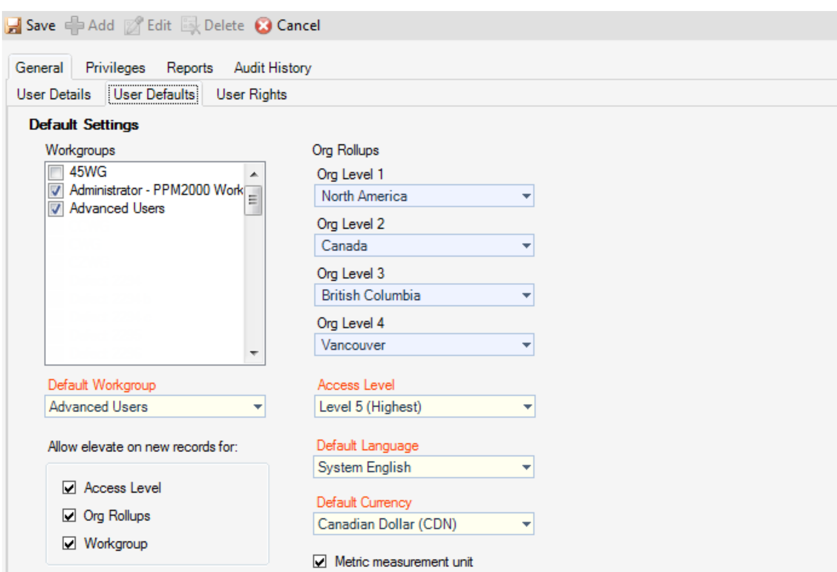
6. Assign a **Default Language** to the user. This determines the field labels that will appear on forms when the user is logged on.

7. Set the **Default Currency** for the user. All currency values entered in Perspective will now appear for the user in this currency.

8. Check the **Metric measurement unit** box to allow the user to see measurements in metric.

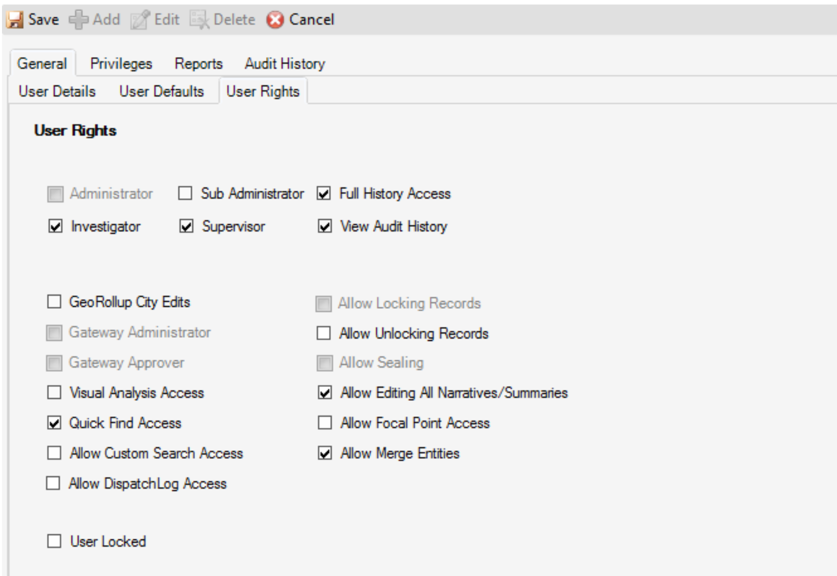
9. To allow the user to assign an access level, organizational rollup and/or workgroup to a new record that is higher or different from their own, check the Allow elevate on new records for **Access Level**, **Org Rollups** and/or **Workgroup** checkboxes. For example, if the Allow elevate on new records for Access Level checkbox is selected for a user with an Access Level of 3, the user will be able to assign Access Levels of 4 or 5 to new records. However, once the user has assigned an elevated access level to a new record, saved the change and exited the record, they will no longer be permitted access to the record, as it falls beyond the scope of their user privileges.

10. Click **Save**.



Set General User Rights

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



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

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

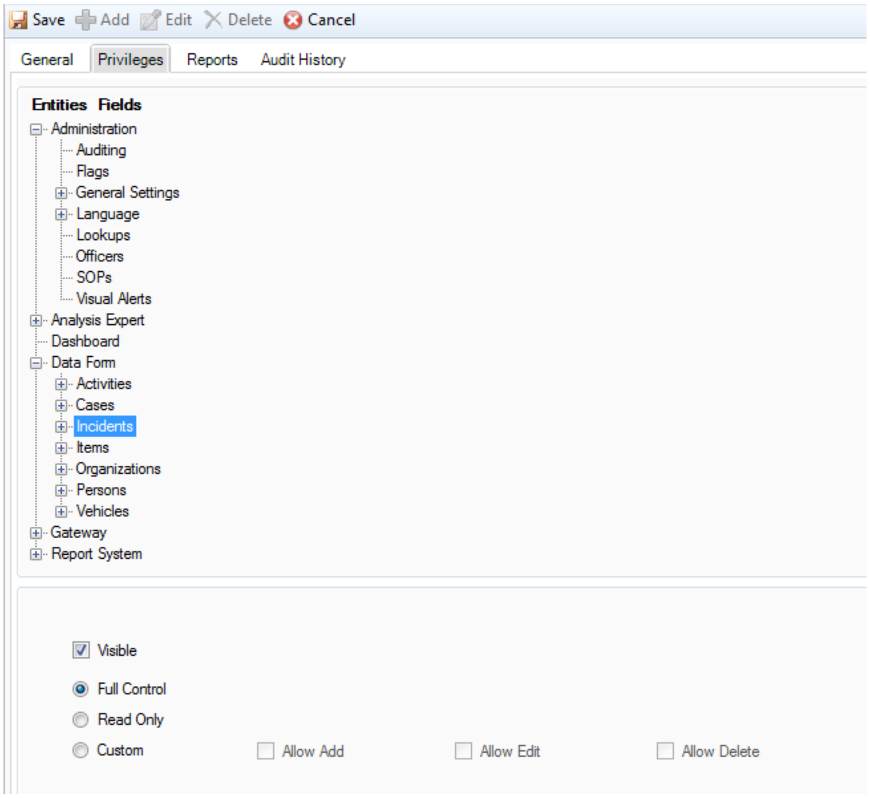
Full History Access	Allows the user to view all incident involvements under the History tabs of Item, Person, Organization and Vehicle records, regardless of the security controls assigned to the records. Checking this box will not allow the user access to the actual Incident records, only the knowledge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

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

Specify Visibility and Access Privileges for a User

1. Open the **Privileges** tab.
2. Expand the four root nodes and select a system component, data form or other entity from the list. The system and/or role rights set for the entity will be displayed below.
3. To override system and/or role rights for this particular user, use the checkboxes and radio buttons to define what the user can see and how the user can manipulate the selected entity:
   - ***Visible***: Allows the user to see the entity and its related buttons, icons and records, when they access Perspective.
   - ***Full Control***: Authorizes the user to read, create, edit and delete entity records.
   - ***Read Only***: Switches entity records to the read-only mode, so that they could not be edited or deleted by the user.
   - ***Custom***: Grants the user the ability to create new entity records (Allow Add), read and edit existing entity records (Allow Edit) and/or delete entity records (Allow Delete).

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

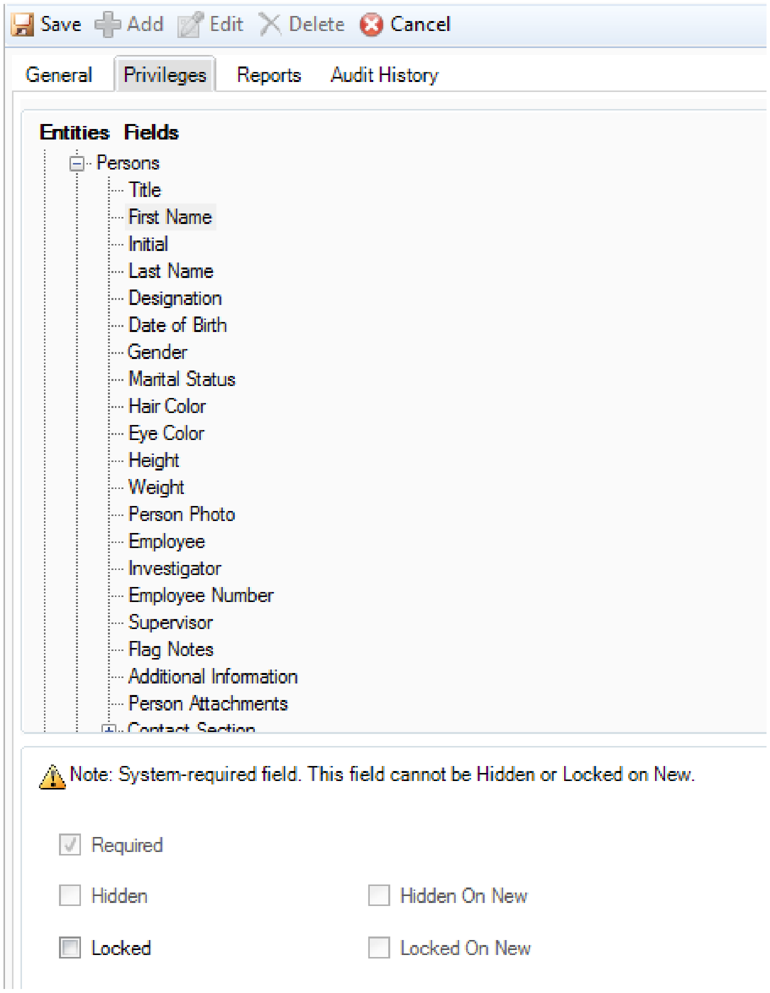


4. Expand the remaining child nodes to display a complete list of fields that constitute all the entities. Select a field name. The system and/or role rights set for the field will be displayed below.

5. To override system and/or role rights for this particular user, use the checkboxes to define the user's access rights to the selected field:

   - ***Required***: Designates the field as a required field that must be completed by users.
   - ***Hidden***: Removes the field from the interface (hidden from the user).
   - ***Hidden On New*** (active when the Hidden box is checked): Unchecking this box allows users to see the field in the records that are newly created. Checking both Hidden and Hidden On New options hides the field from both new and existing records.
   - ***Locked***: Makes the field visible to the user, but not accessible for data entry or editing. In this case, the field appears greyed out and is locked from use.
   - ***Locked On New*** (active when the Locked box is checked): Unchecking this box allows users to access the field in the records that are newly created. Checking both Locked and Locked on New options locks the field from use in both new and existing records.

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



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

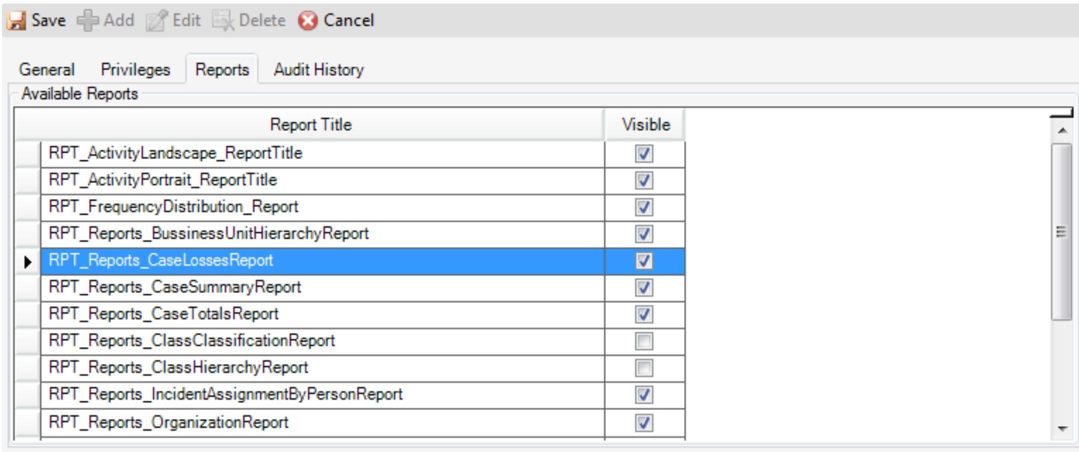
7. Click **Save**.

Set Report Visibility for a User

1. Open the **Reports** tab.

2. To allow a user to see reports listed under Report Title, check the **Visible** boxes beside the report names.

3. Click **Save**.

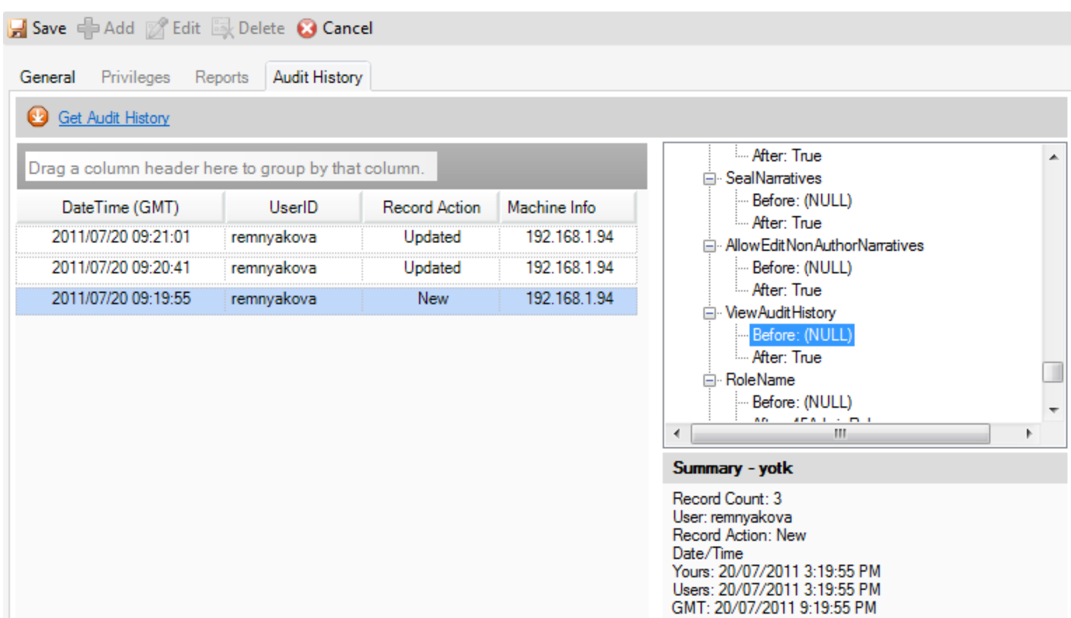


Track All Changes Made to a User Account

1. Open the **Audit History** tab.

2. Click the **Get Audit History** button to view all modifications made to the user account since its creation. The pane on the left contains entries for each change made to the record. **DateTime** indicates when the change was made; **UserID** reveals who made the change; **Record Action** describes what type of change was made; and **Machine Info** specifies which computer was used to make the change.

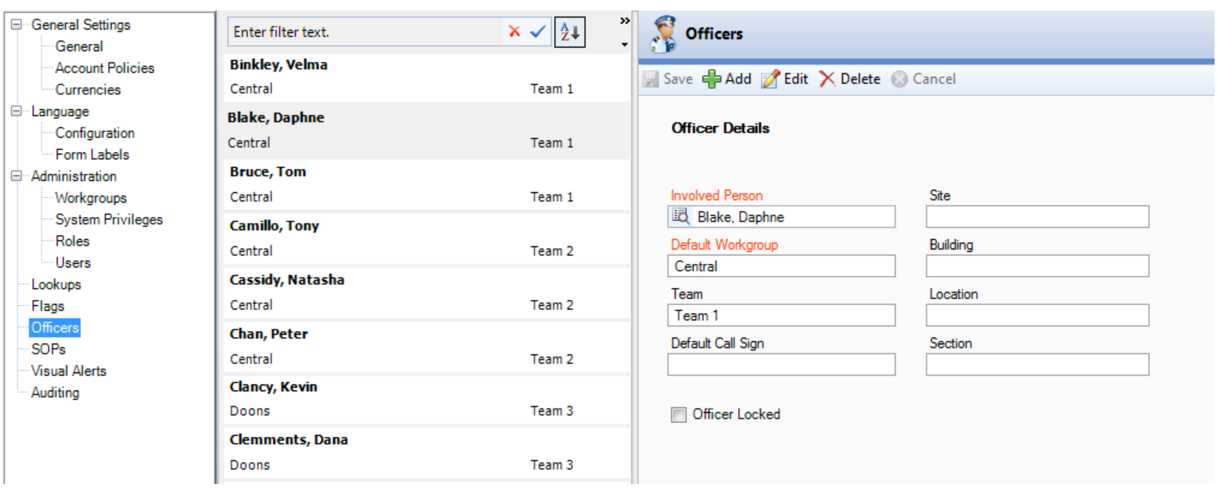
3. Select an entry to view further details of the change made in the pane on the right. Expand the nodes to see exactly what the data value was **Before** and **After** the change was made.



Officers

Add a New Officer for Perspective Dispatching

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



License Management

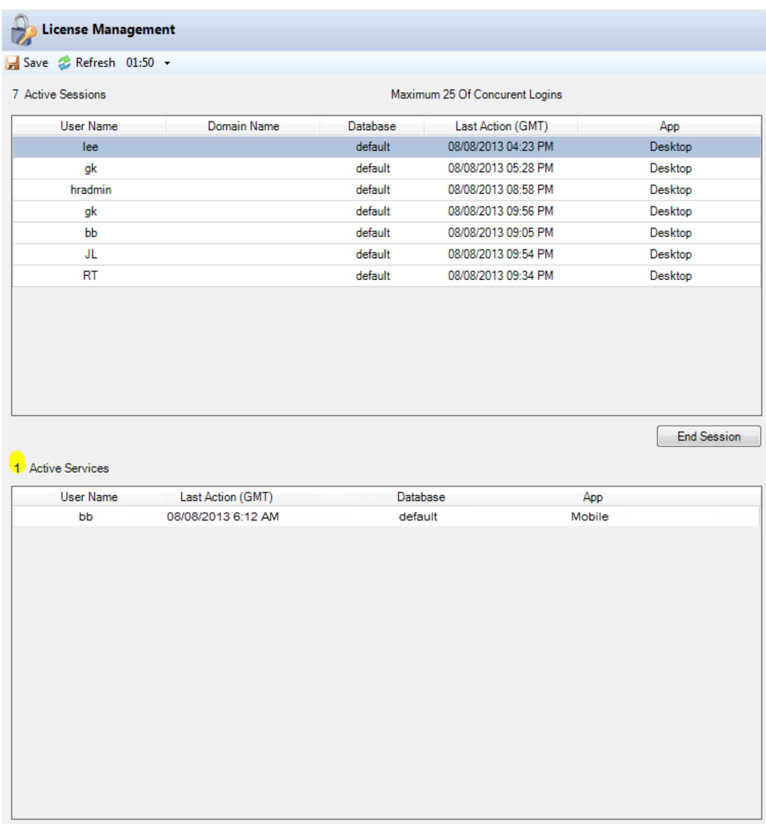
Depending on your licensing, use the License Management tool to access concurrent licenses, or named licenses.

Concurrent Licenses

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

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

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



Named Licenses

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

To access your licensed Perspective users, select **License Management**.

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

Assign a User

To assign users individually, do the following steps:

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

Remove a User

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

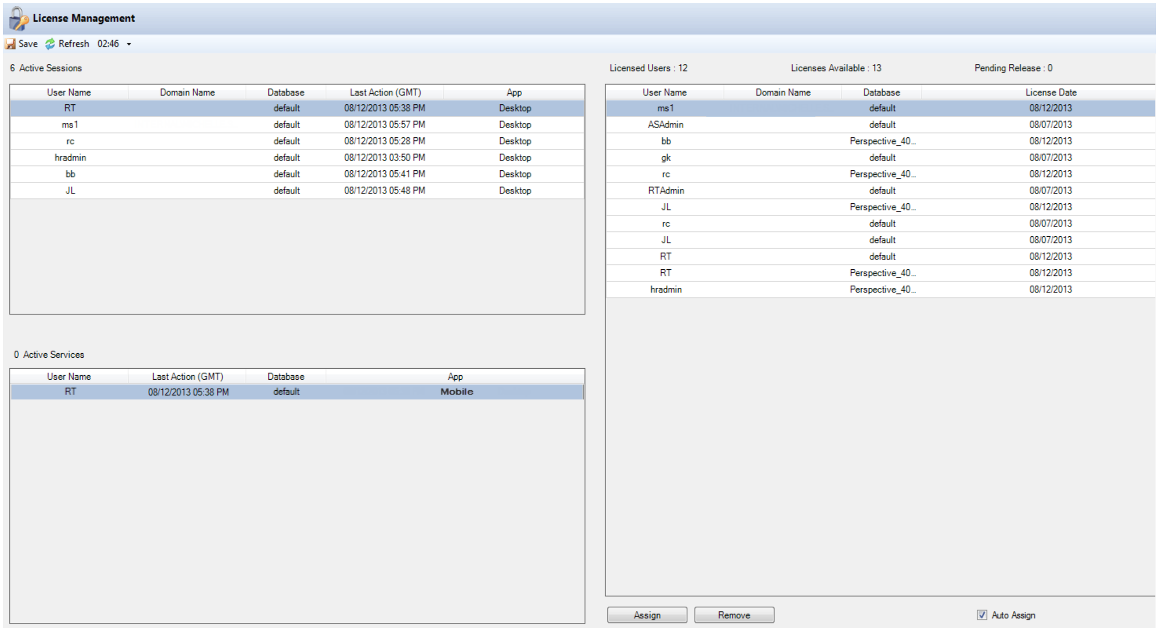
1. Click the name (or corresponding row) of the license you want to remove from either the active session list, or the licensed user's list.
2. Click the **Remove** button on the bottom of the screen. A pop-up window will appear.
3. Click **Yes** if you want to remove the license. Click **No** if you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

Auto Assign Users

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

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

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


License Management
Save
Refresh
02:46
6 Active Sessions
User Name
Domain Name
Database
Last Action (GMT)
App
RT default 08/12/2013 05:38 PM Desktop
ms1 default 08/12/2013 05:57 PM Desktop
rc default 08/12/2013 05:28 PM Desktop
hradmin default 08/12/2013 03:50 PM Desktop
bb default 08/12/2013 05:41 PM Desktop
JL default 08/12/2013 05:48 PM Desktop
0 Active Services
User Name
Last Action (GMT)
Database
App
RT 08/12/2013 05:38 PM default Mobile
Licensed Users : 12
Licenses Available : 13
Pending Release : 0
User Name
Domain Name
Database
License Date
ms1 default 08/12/2013
ASAdmin default 08/07/2013
bb Perspective_40... 08/12/2013
gk default 08/07/2013
rc Perspective_40... 08/12/2013
RTAdmin default 08/07/2013
JL Perspective_40... 08/12/2013
rc default 08/07/2013
JL default 08/07/2013
RT default 08/12/2013
RT Perspective_40... 08/12/2013
hradmin Perspective_40... 08/12/2013
Assign
Remove
Auto Assign

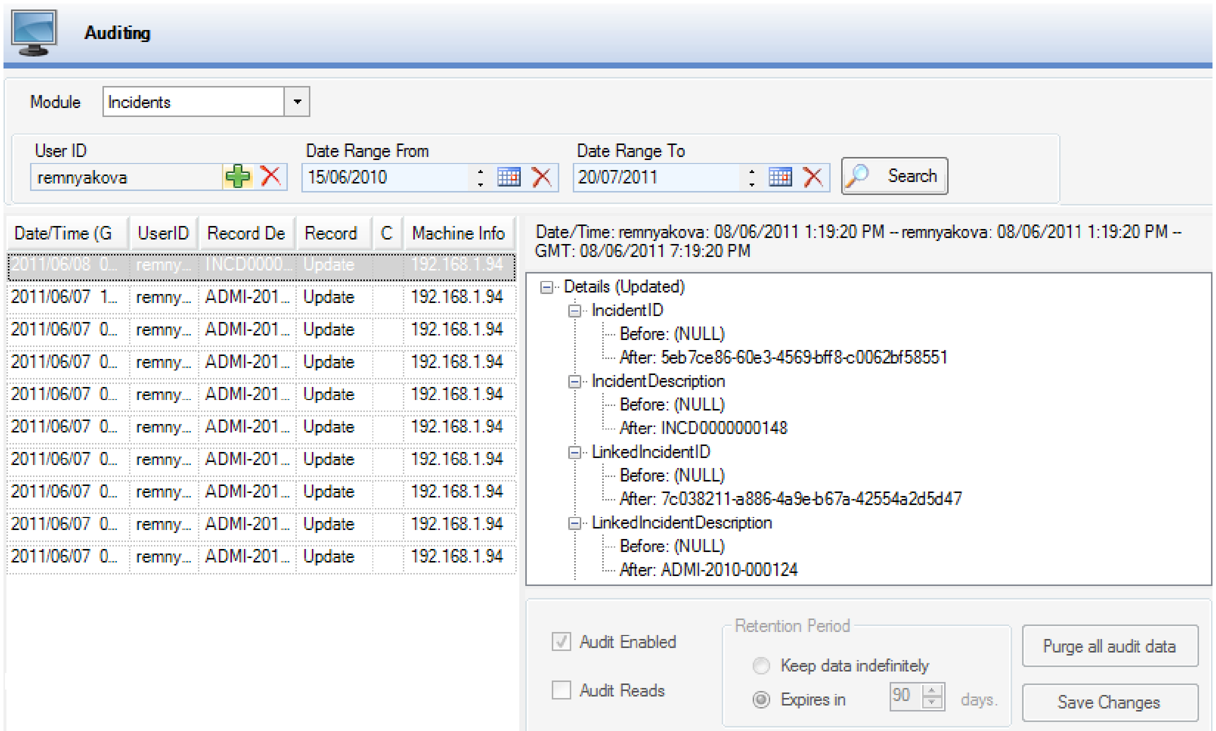
Auditing

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

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

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

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


Auditing
Module
Incidents
User ID
remnyakova
Date Range From
15/06/2010
Date Range To
20/07/2011
Search
Date/Time (G
UserID
Record De
Record
C
Machine Info
2011/06/08 0...
remny...
INCD0000...
Update
192.168.1.94
2011/06/07 1...
remny...
ADMI-201...
Update
192.168.1.94
2011/06/07 0...
remny...
ADMI-201...
Update
192.168.1.94
Date/Time: remnyakova: 08/06/2011 1:19:20 PM -- remnyakova: 08/06/2011 1:19:20 PM -- GMT: 08/06/2011 7:19:20 PM
Details (Updated)
IncidentID
Before: (NULL)
After: 5eb7ce86-60e3-4569-bff8-c0062bf58551
IncidentDescription
Before: (NULL)
After: INCD0000000148
LinkedIncidentID
Before: (NULL)
After: 7c038211-a886-4a9e-b67a-42554a2d5d47
LinkedIncidentDescription
Before: (NULL)
After: ADMI-2010-000124
Audit Enabled
Audit Reads
Retention Period
Keep data indefinitely
Expires in
90
days.
Purge all audit data
Save Changes

Lookups

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

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

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

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

Modify a Single-Tier Lookup List

1. Click once to select one of the lookup categories in the alphabetized list and display its content on the right. Double-click to select a category and see the associated forms at the bottom of the screen with the Language tab open by default.

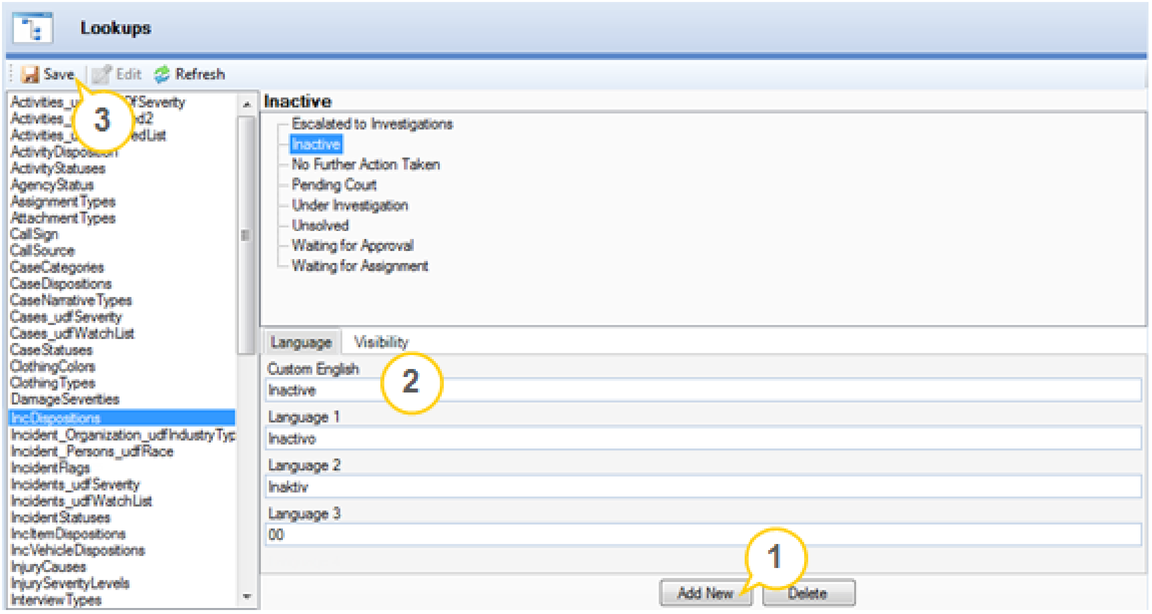
2. Select the type of modification required and follow the procedures below:

- To add a new option to the selected lookup list, click the **Add New** button and type the option in the **Custom English** field. Although Custom English is the default language for all lookups, you can enter language-specific lookup options in the appropriate language/label set text fields. Custom English lookup options still appear for users assigned to other languages, if there are no alternative lookup options specified for their assigned language.

- To edit an option in the selected lookup list, click on the option to highlight it, and edit the text in the **Custom English** field.

- To delete an option from the selected lookup list, highlight the option in the list, and click the **Delete** button. Note that you will not be able to delete any lookup list options that have already been used in existing Perspective records. If this occurs, you can hide the value from visibility so users cannot choose the value from the lookup list when completing a record. See "Specify Workgroup Visibility for a Lookup List Value" on page 51 for further details.

3. Click **Save**.



Modify a Multi-Tier or Hierarchical Lookup List

1. Multi-tier lookup lists (rollups) appear in capital letters at the bottom of the list. Double-click on one rollup name to display the hierarchical list of its options on the right and see the associated forms at the bottom of the screen with the Language tab open by default.

2. Expand the nodes of the rollup. Each rollup has up to four tiers of options for users to select from (e.g., the Class Rollup consists of Class, Category, Subcategory and Type).

- The first tier is the **Root** of the rollup (e.g., Class in the Class Rollup). The option selected in the first tier determines what options are available in the second tier and so forth.

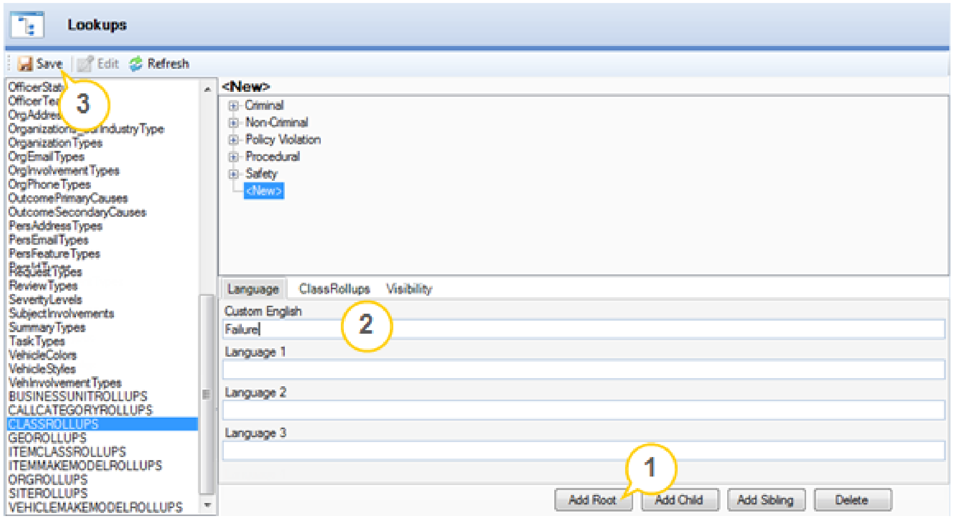
- The higher tier in the hierarchy is the **Parent field**, while the lower tier is the **Child field**. For example, Class is the parent field to the Category child field.

- Any child fields that are on the same tier of the hierarchy are **Sibling fields**. In other words, all Class fields are siblings to each other; all Category fields are siblings to each other, and so on.

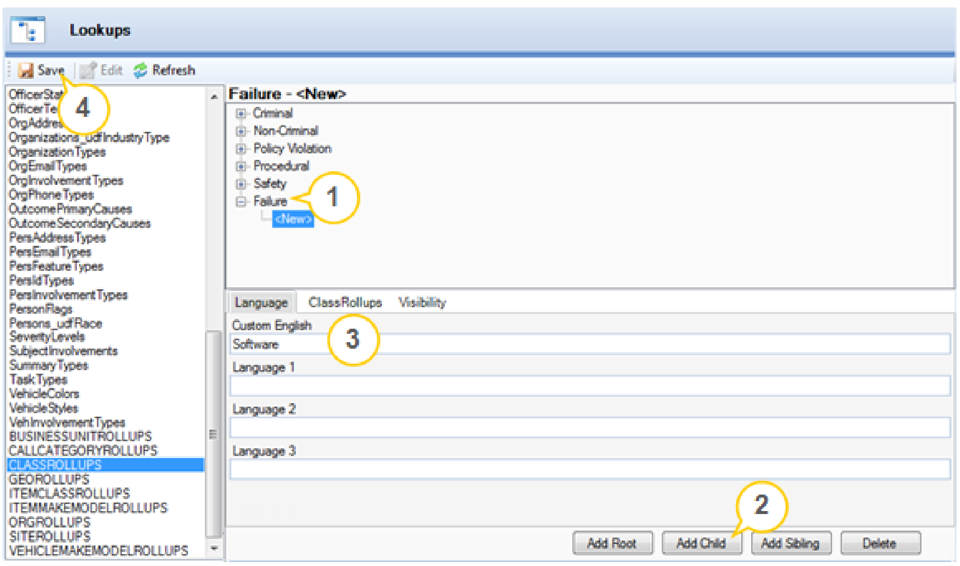
4. Select the type of modification required and follow the procedures below:

- To delete an option from a rollup, select the option and click **Delete**. If the option has child fields, you must first delete all of the option’s child fields before deleting the option itself. Note that you will be unable to delete any rollup options that are already saved in existing records. If this occurs, you can hide the value from visibility so users cannot choose the value from the lookup list when completing a record. See “Specify Workgroup Visibility for a Lookup List Value” on page 51 for further details.

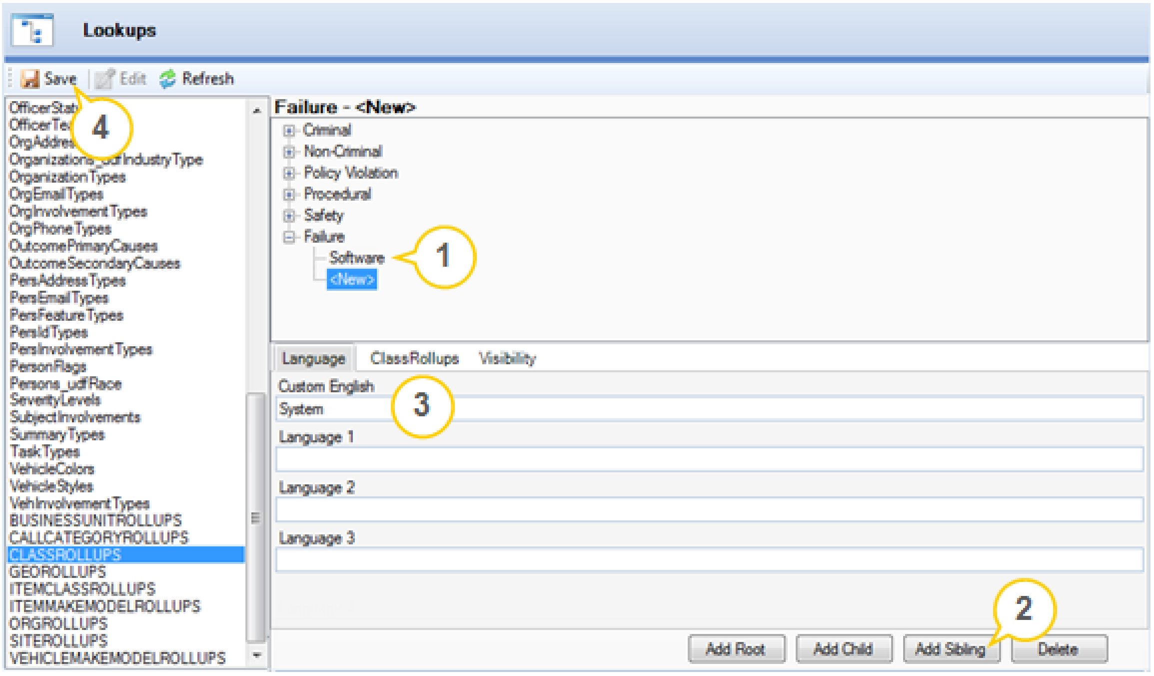
- To add an option to the first tier of a rollup hierarchy, click **Add Root**, or select one of the first-tier options (e.g., Criminal) and click **Add Sibling**.



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



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



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

6. Click **Save**.

Specify Workgroup Visibility for a Lookup List Value

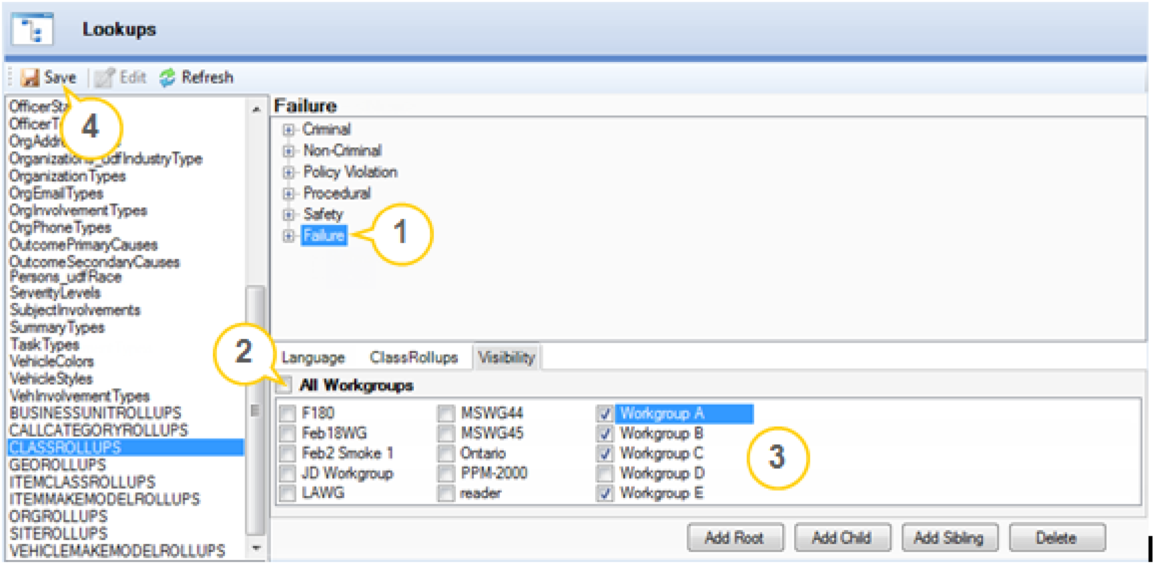
1. Double-click on the correct lookup list to see the associated forms at the bottom of the screen with the Language tab open by default.

2. From the lookup list, select the lookup value you would like to adjust workgroup visibility for. Some hierarchical lookups or rollups allow you to adjust visibility at the second level of the hierarchy as well as the first. In this case, expand the nodes at the root level to view further lookup options and select the option for which you wish to adjust workgroup visibility.

3. Open the **Visibility** tab. Note that this tab will not appear for ORGROLLUPS, because it is not possible to adjust visibility for organizational rollups.

4. By default, all lookup lists and their available options are visible to all workgroups. To permit specific workgroups to use the selected lookup option, first uncheck the **All Workgroups** box, and then click the checkboxes corresponding to the appropriate workgroups.

5. Click **Save**.



Enter Call Codes for the Call Category Lookup List

1. Double-click on **CALLCATEGORYROLLUPS** at the bottom of the Lookups list and see all Call Category options on the right and the associated forms at the bottom of the screen with the Language tab open by default.

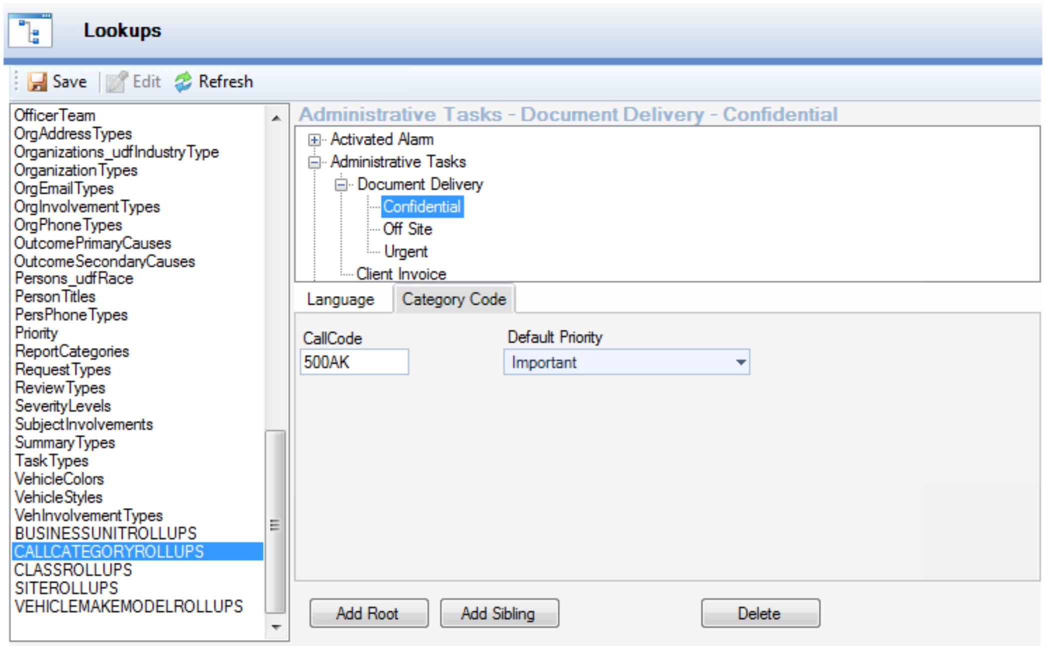
2. Expand the nodes in the Call Category rollup's list of options. Each category has up to three tiers available. Select the call categories (e.g., Administrative Tasks or Activated Alarm) and sub-categories (e.g., Document Delivery or Test Alarm) for which you want to specify the code.

3. Select the **Category Code** tab.

4. Input the appropriate code for the selected option in the **Call Code** field. The code entered will only be saved for the particular category or sub-category selected. To enter a code for a different level of the Call Category rollup, you must select the option and input the appropriate code individually. One way to approach call codes is to build codes for sub-categories (e.g., 500A for Document Delivery and 500AK for Confidential Document Delivery) upon the codes for categories (e.g., 500 for Administrative Tasks).

5. Select the appropriate **Default Priority** for each of the call categories. The priority selected will only be saved for the particular category or sub-category that you chose. To enter a priority for a different level of the Call Category rollup, you must select the option and input the correct priority marker individually.

6. Click **Save**.



Enter Address Information for the Site Lookup List

1. Double-click on **SITEROLLUPS** at the bottom of the Lookups list and see all Site options on the right and the associated forms at the bottom of the screen with the Language tab open by default.

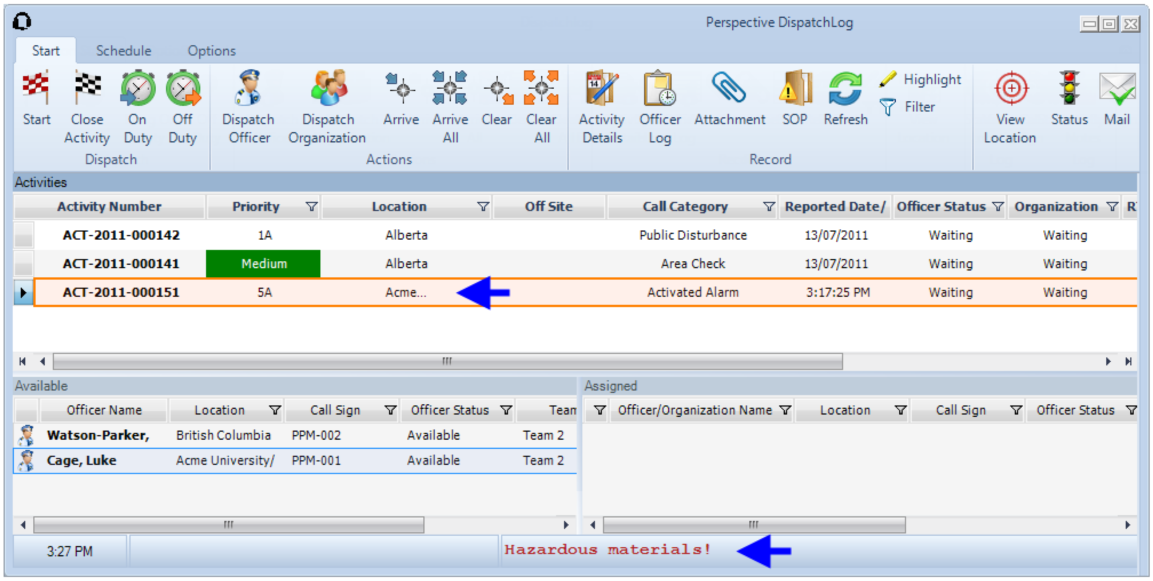
2. Expand the nodes in the Site rollup's list of options. Each Site has up to four tiers available. Select the Site, Building, Location or Section for which you want to specify the address.

3. Select the **SiteRollups** tab.

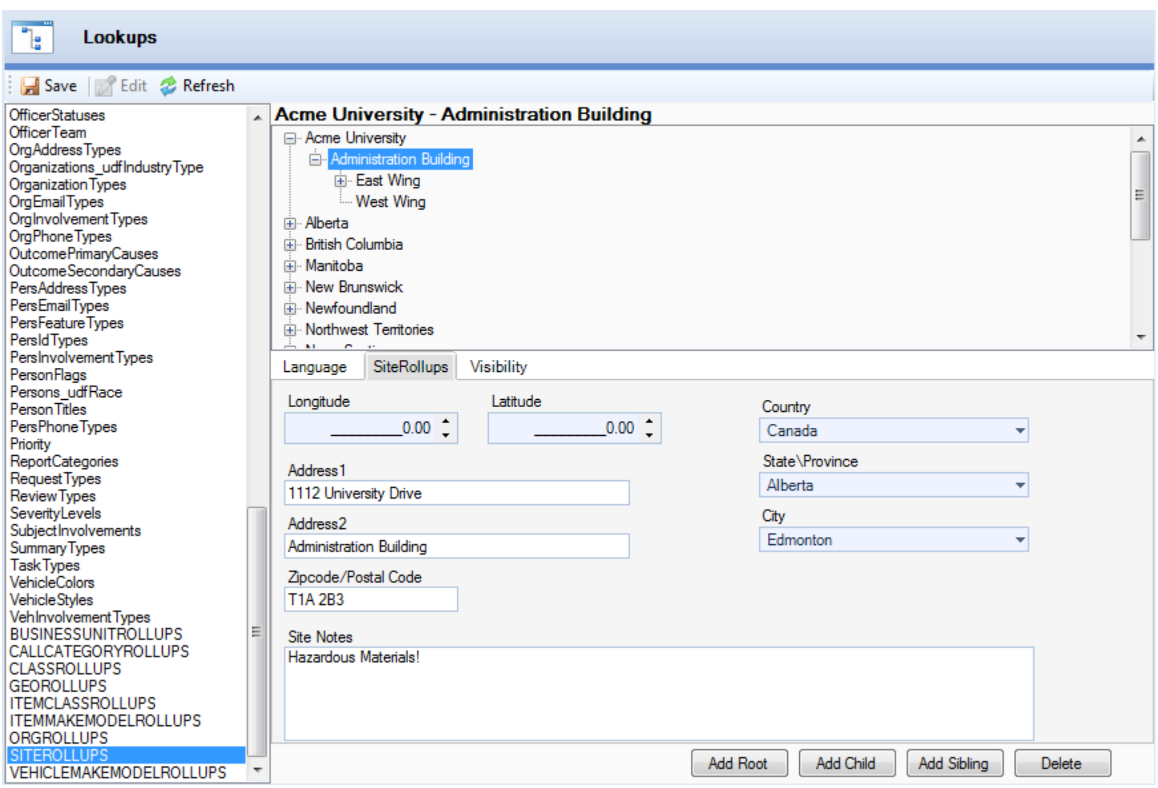
4. Input the appropriate address for the selected option in the **Address**, **Country**, **State/Province**, **City** and **Zipcode/Postal Code** fields. The address entered will only be saved for the particular Site, Building, Location or Section selected. To enter an address for a different level of the Site rollup, you must select the option and input the appropriate address individually.

5. The **Longitude** and **Latitude** fields will display the coordinates set for the Site available for any custom integrations using Integration Services.

6. If required, enter any important **Site Notes** for display in Perspective DispatchLog. Once stored for a specific site in Perspective, this text will be running on the Status bar in Perspective DispatchLog every time you select an Activity record that has its location set to this site.



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



Activity Statuses and Officer Statuses

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

The Relationship Between Activity Statuses and Officer Statuses

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

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

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

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

System Values

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

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

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

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

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

Flags

Add a New Incident or Person Flag

1. Select **Lookups** in the Navigation pane.

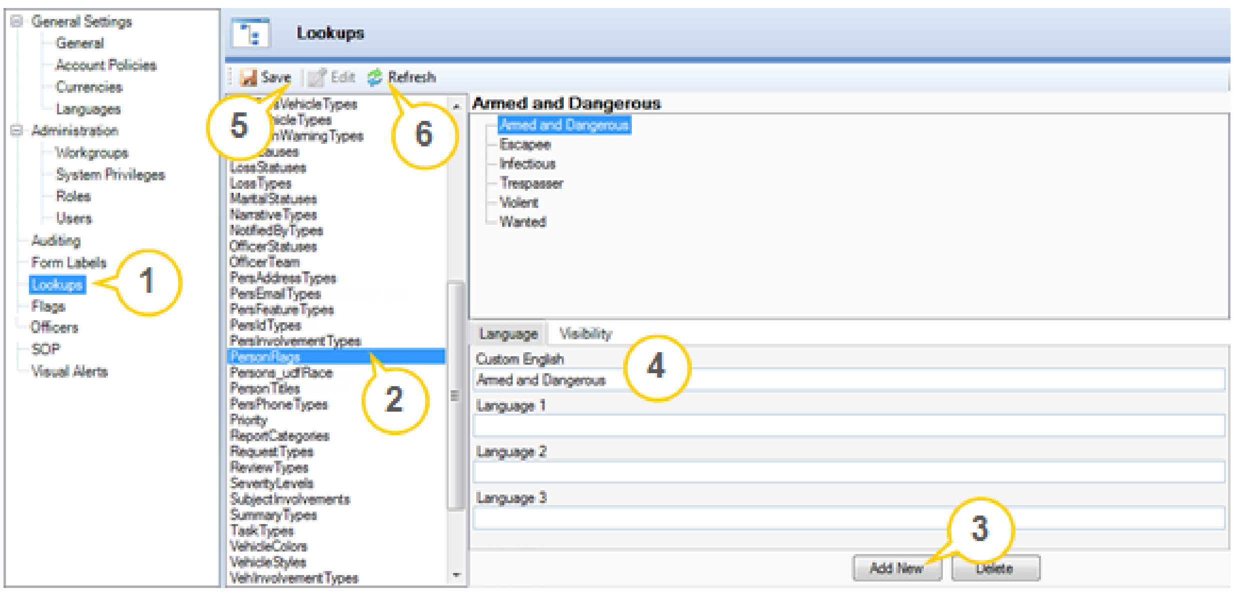
2. In the Lookups list, double-click **IncidentFlags** if you wish to add a flag to the Incident form, or **PersonFlags** if you wish to add a flag to the Person form.

3. Click the **Add New** button at the bottom of the screen.

4. Type the name of the new flag in the **Base Language** field.

5. Click **Save**.

6. Click the **Refresh** button.



7. Select **Flags** in the Navigation pane.

8. Specify the type of flags intended for editing by selecting either **Incidents** or **Persons** from the **View Flags For** lookup list.

9. Click **Add**.

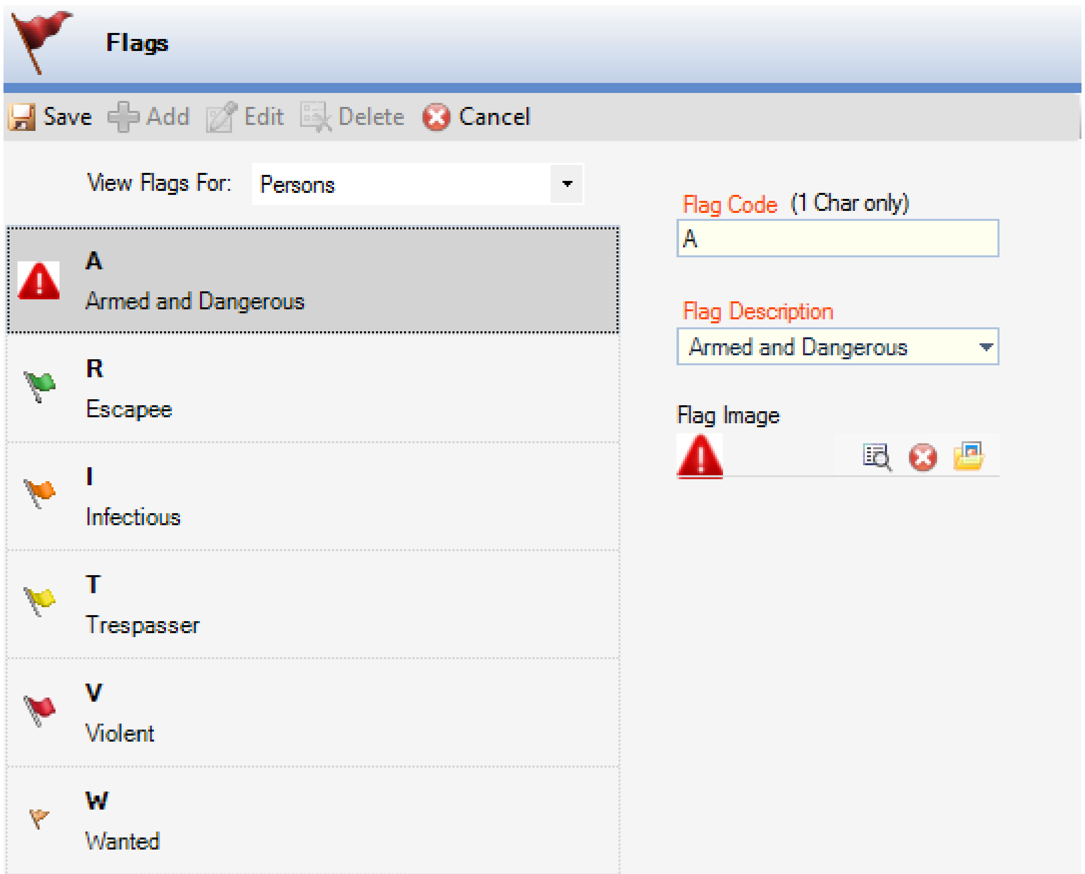
10. In the new flag form on the right, select the flag name you created earlier in the Lookups section on the **Flag Description** lookup list.

11. Enter a unique one-character designation for the flag in the **Flag Code** field.

12. To add an image to the new flag, click the **Add** icon in the **Flag Image** field, select an image from the pop-up browser and click Open.

13. Click **Save**.

14. To edit an existing flag, click **Edit** and proceed as described above. To delete a flag, go to the Lookups section, the IncidentFlags or the PersonFlags lookup, select the relevant flag's node and click **Delete**.



Standard Operating Procedures

Create a New Standard Operating Procedure Rule for an Activity

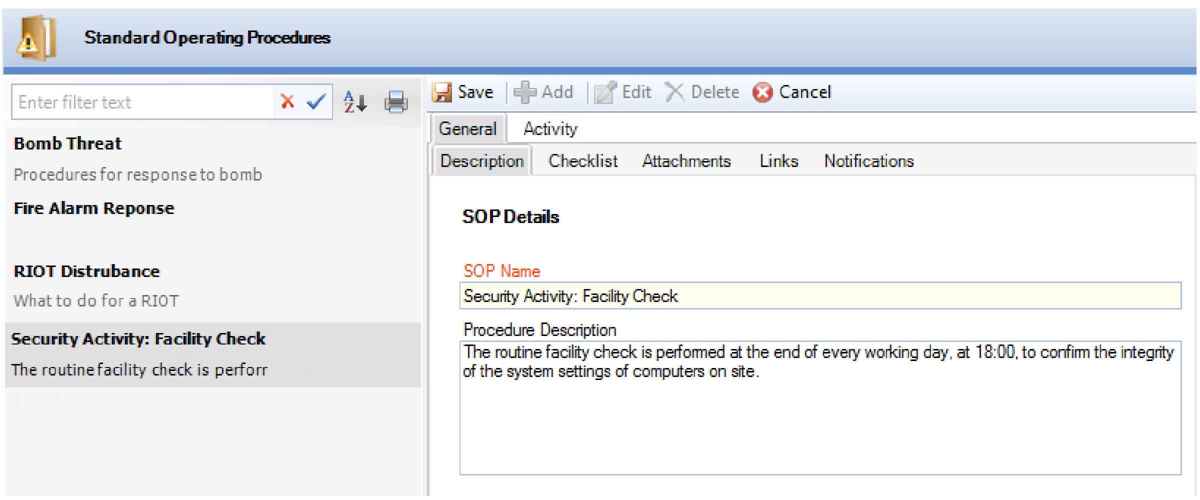
Using the Standard Operating Procedures (SOP) component of Administration, you can create a new SOP rule restricting it to a specific call category, site specifications and/or activity status. The created SOP rule will subsequently feature in Activity records that correspond to the settings specified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

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

1. Click **Add**. A blank SOP form will open with the **General** tab, the **Description** sub-tab open.

2. Start with specifying the official **SOP Name** in the required field.

3. Add a brief **Procedure Description** in the textbox below.



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

5. Click **Add New**.

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

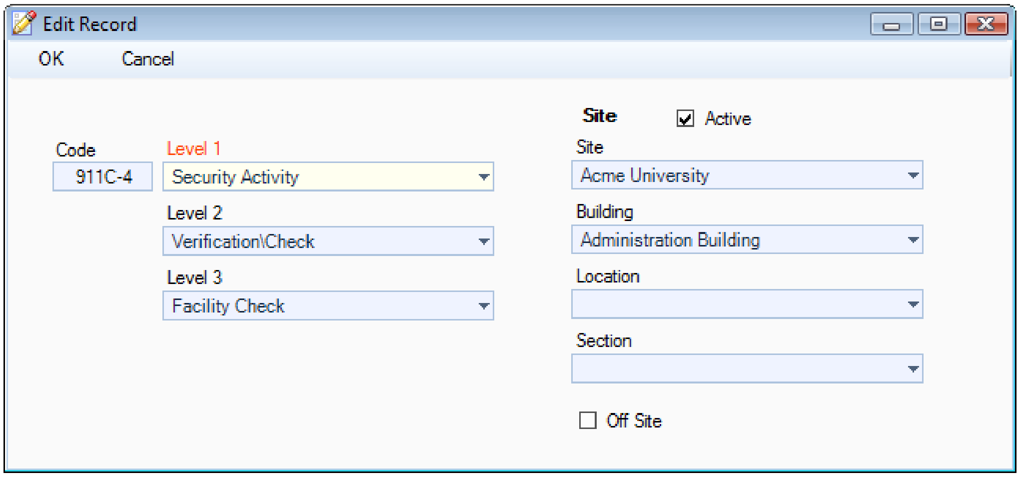
7. Check the **Active** box to restrict the SOP to active activities only.

8. Restrict the location of the SOP-related activities by selecting their common **Site**, **Building**, **Location** and **Section**. Make the parameters as specific as necessary (e.g., Acme University, Acme University/Administration Building, etc.).

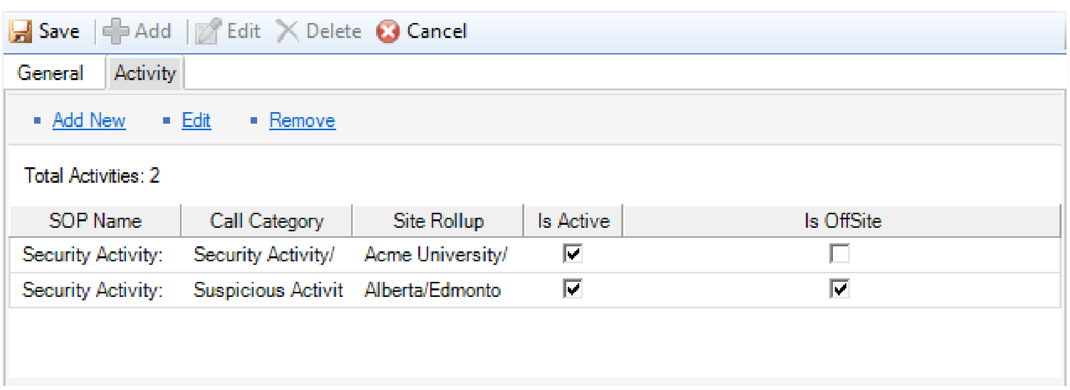
9. Check the **Off Site** box to implement the SOP to the off-site activities only.

10. Click **OK** to save the parameters for immediate activation of the SOP.

11. If required, add relevant SOP Checklist(s), Attachment(s), Link(s), and set up Notification(s).



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

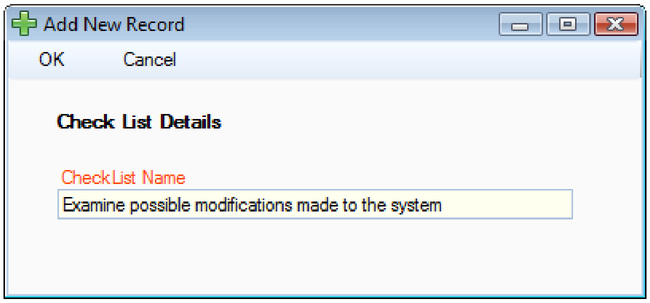


Add a Checklist for the SOP

1. Open the **General** tab, the **Checklist** sub-tab.

2. To specify the first checklist item, click **Add New**.

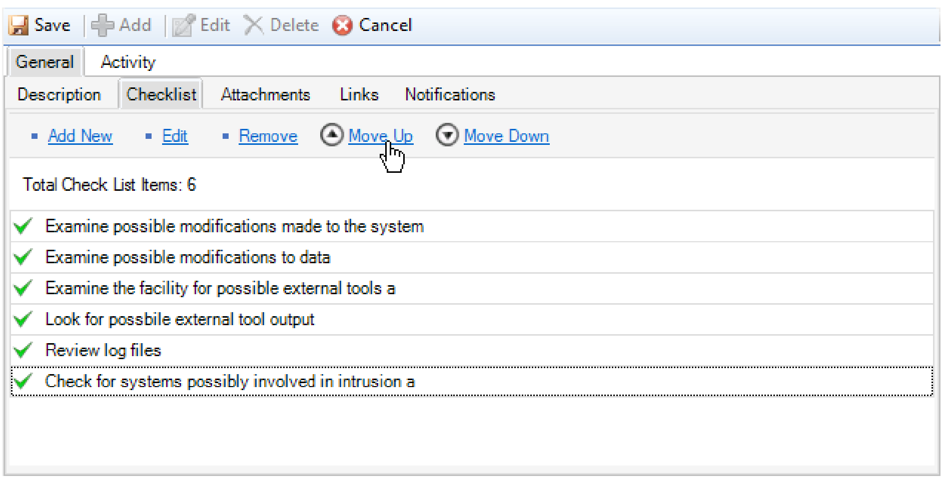
3. Enter the text of the initial recommended procedure, and click **OK**.



4. Add as many procedures that constitute your required SOP as necessary.

5. To re-arrange the position of items in the checklist, select the item of interest and click **Move Up** and **Move Down**, as required.

6. Click **Save**. The next time an activity with the specified parameters is created the system will automatically activate the SOP option in Perspective and Perspective DispatchLog and display the interactive checklist. In the Activity record, you will be able to check the completed actions.



Attach a Relevant SOP File

1. Open the **General** tab, the **Attachments** sub-tab.

2. To attach a file related to the SOP, click **Add New**. A pop-up window will open.

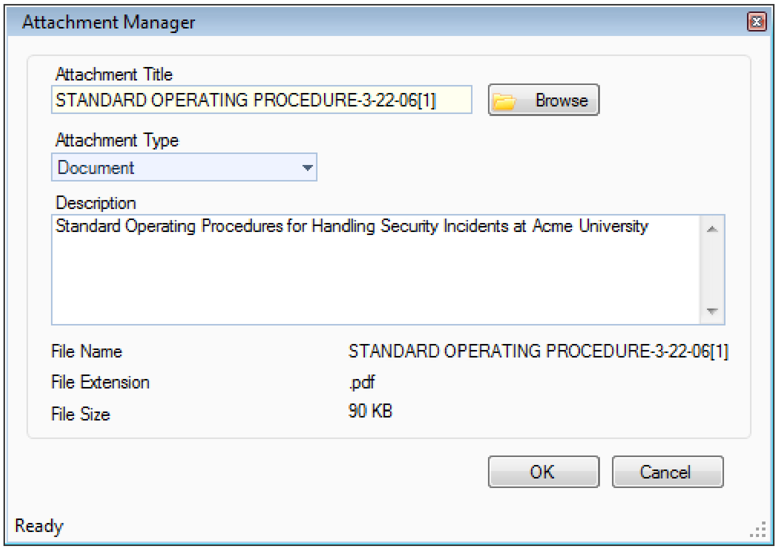
3. Click **Browse** to locate and select the file you wish to attach.

4. The **Attachment Title** field will automatically populate with the name of the attached file. If necessary, modify the name.

5. From the **Attachment Type** lookup list, select the appropriate designator for the attachment (e.g., Document, Picture, Video).

6. Give an overview of the attachment in the **Description** text box.

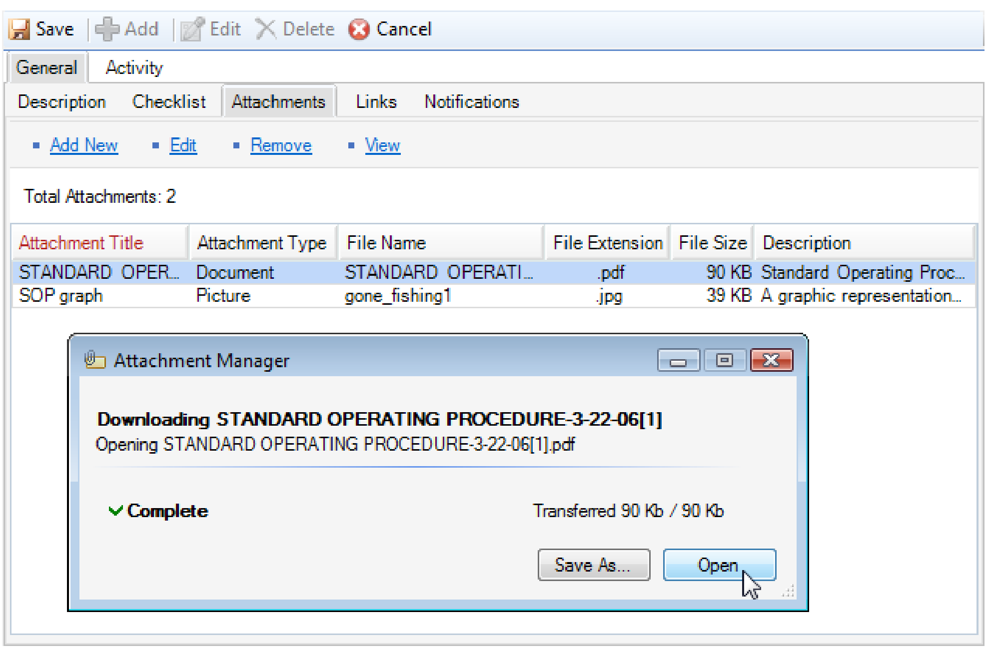
7. Click **OK** to upload the attachment. Once the upload is complete, click OK again to return to the record.



8. Add as many attachments as necessary.

9. Click **Save**. The next time an activity with the specified parameters is created the system will automatically activate the SOP option in Perspective and Perspective DispatchLog and display the list of viewable attachments.

10. To view an attachment that has been added to the list, select it in the grid and click **View**. Then, click **Open** to see it, or **Save As** to save it on your computer.



Add a Relevant SOP Link

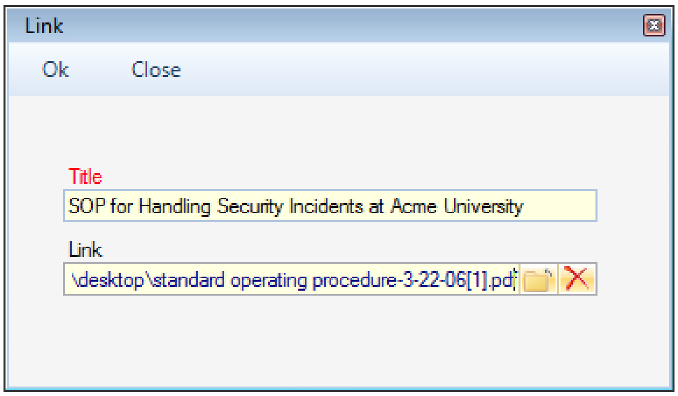
1. Open the **General** tab, the **Links** sub-tab.

2. To add a relevant SOP link to a file on your organization’s commonly accessible local drive or an external Web URL, click **Add New**. A pop-up window will open.

3. In the Title field, enter a descriptor for the link you are creating.

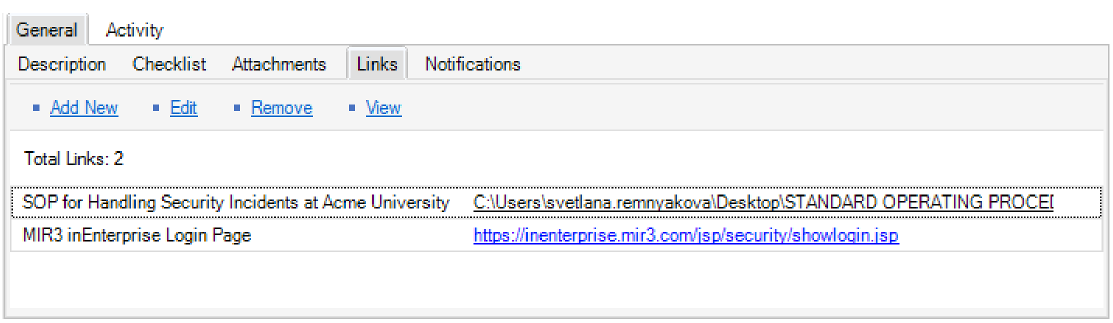
4. If you are linking a local file, click the **Browse** icon, find the corresponding file and click **Open** to confirm the operation. If the link is a Web URL, paste the link into the **Link** field.

5. Click **OK** to add the link to the list.



6. Click **Save**. The next time an activity with the specified parameters is created the system will automatically activate the SOP option in Perspective and Perspective DispatchLog and display the links for reference.

7. To view the created link, select the link in the grid and click **View**. If the link is still valid, the file or URL will open.



Set Up Individual and Mass Notifications for the SOP

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

1. Open the **General** tab, the **Links** sub-tab.

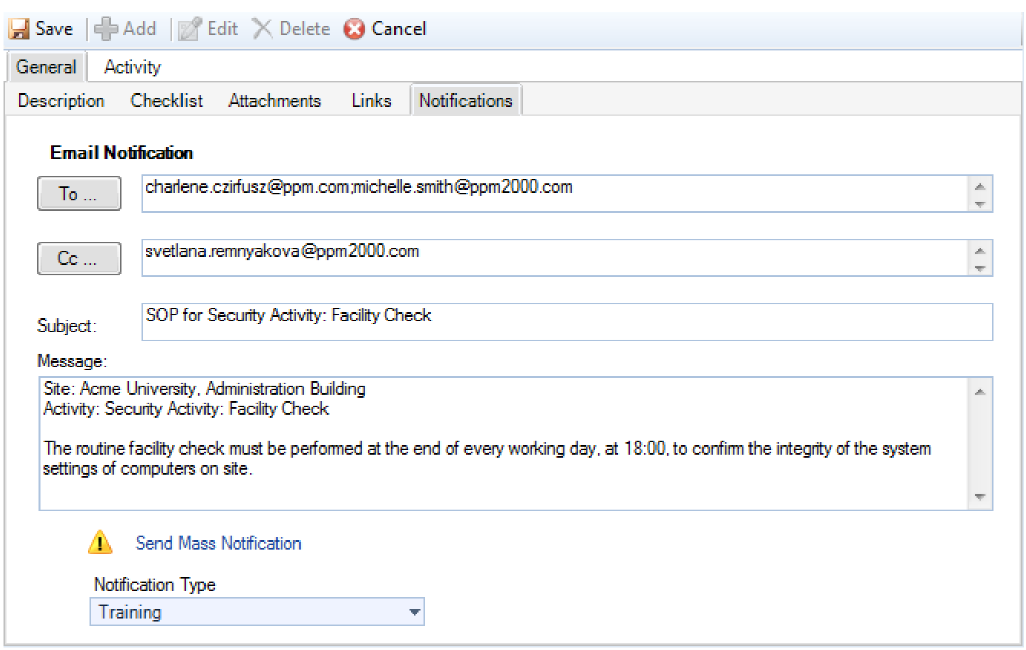
2. Under **To** and **Cc** fields, specify the recipients' direct and the carbon copy email addresses respectively for the delivery of the individual notifications. You may either type the addresses in, or click the relevant buttons and select the user(s) you wish to email the notification to from the list. Note that only the users with specified Primary Email Address will be available for the list selection.

3. Enter the **Subject** of the notification.

4. In the **Message** textbox, enter the SOP notification message.

5. If mass notification feature is enabled in your system and a mass notification is required for the SOP, select the **Notification Type** from the lookup list below. For details about setting up the available Notification Type options, refer to the *Perspective Installation Guide*.

6. Click **Save**. The next time the appropriate activity is created the system will automatically activate the SOP option in Perspective and Perspective DispatchLog and provide a form to send out the relevant notifications. In the Activity record, you will also be able to read the notifications that have previously been sent.



Visual Alerts

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

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

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

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

Define Visual Representation for Certain Data Types

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

Activities

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

1. Open the appropriate tab (e.g., Officer Team, Priority, Location).

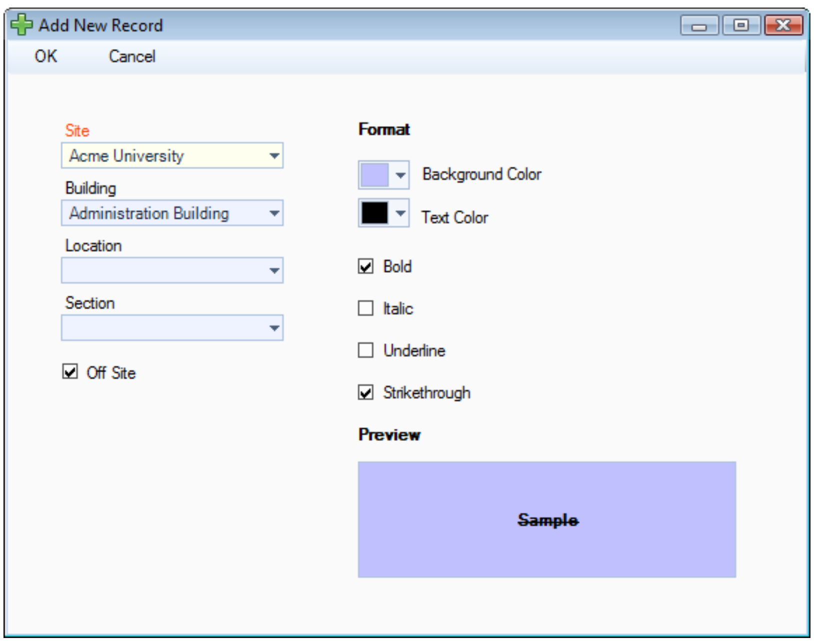
2. Click **Add New**.

3. A blank alert window will pop up. In the lookup, select the descriptor(s) of the category for which you wish to edit the format (e.g., Officer Team, Priority, Site/Building/Location/Section). For Location, check the Off Site box to indicate that the location is off-site.

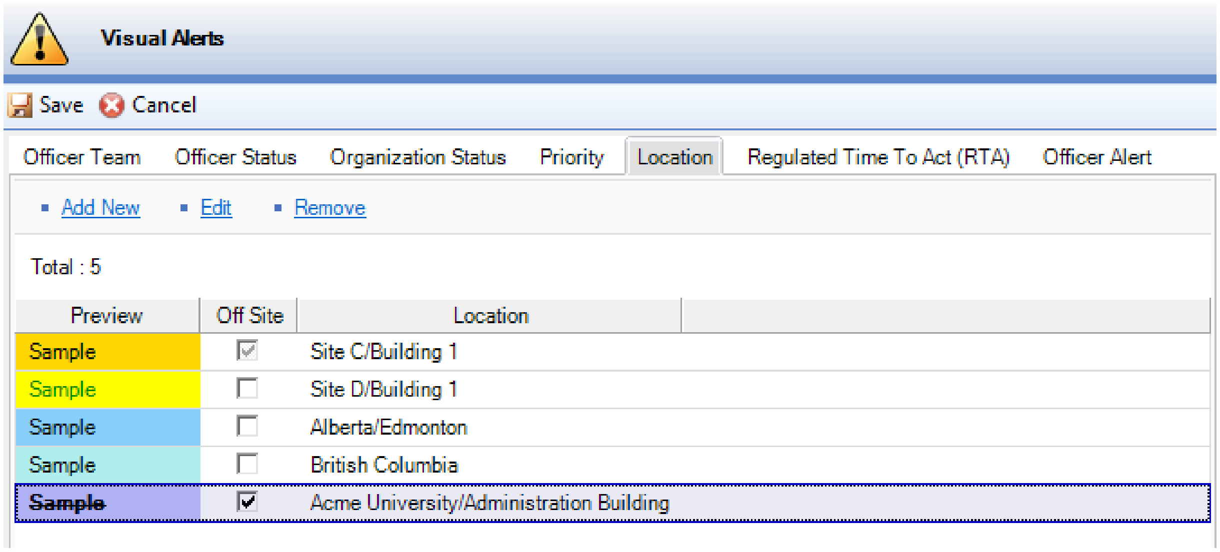
4. Using the color lookups, select the **Background** and the **Text Colors** for the field of the selected category.

5. Check the **Bold**, **Italic**, **Underline** and/or **Strikethrough** boxes to add further font effects.

6. Preview the resulting field view below and click **OK**, if the result corresponds to your expectations.



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



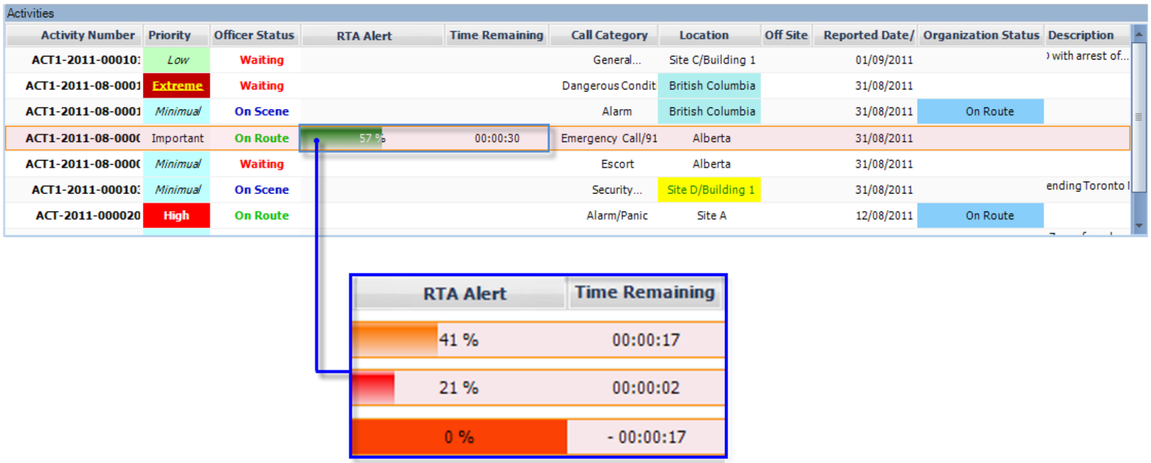
Create a New Regulated Time to Act (RTA) Alert

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

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

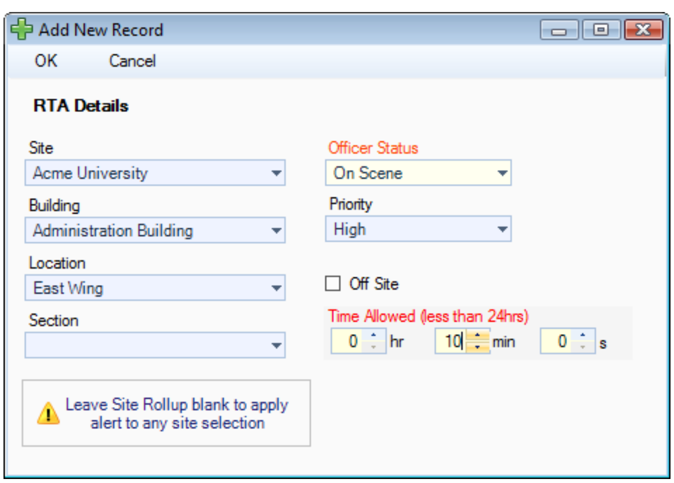
If, for some reason, the officer failed to respond about their status change during the allotted period of time, the timer will start counting the time the officer spends in the set conditions after the RTA expiry, advancing in negative values. The display of the RTA time bar will change to flashing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

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

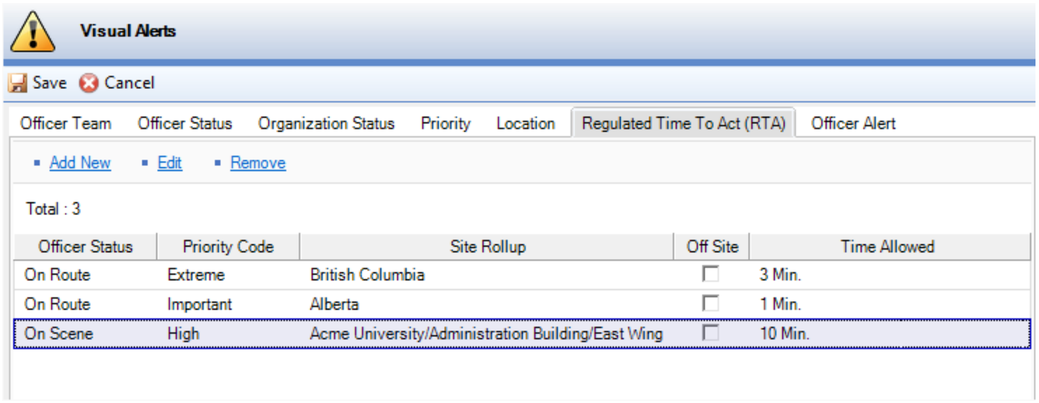


To create a new RTA alert, follow the steps below:

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



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



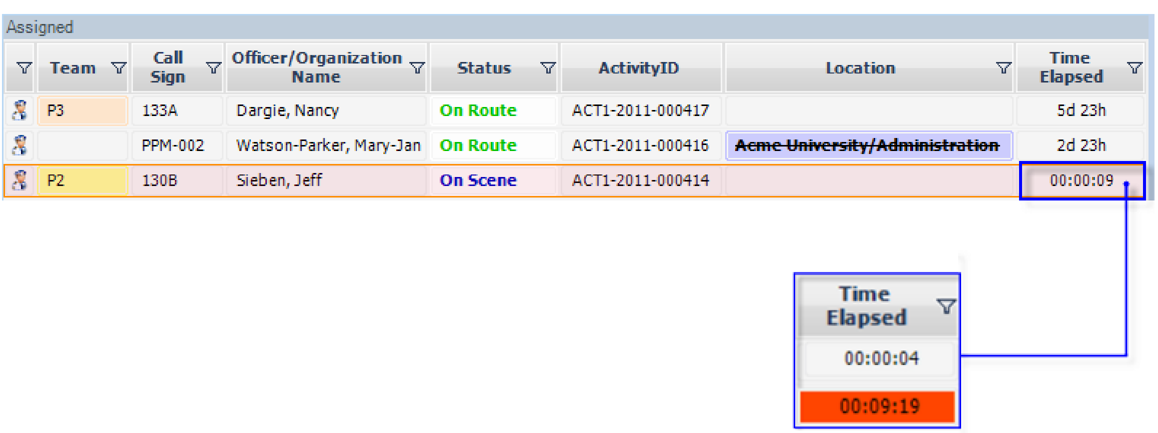
Create a New Officer Alert

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

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

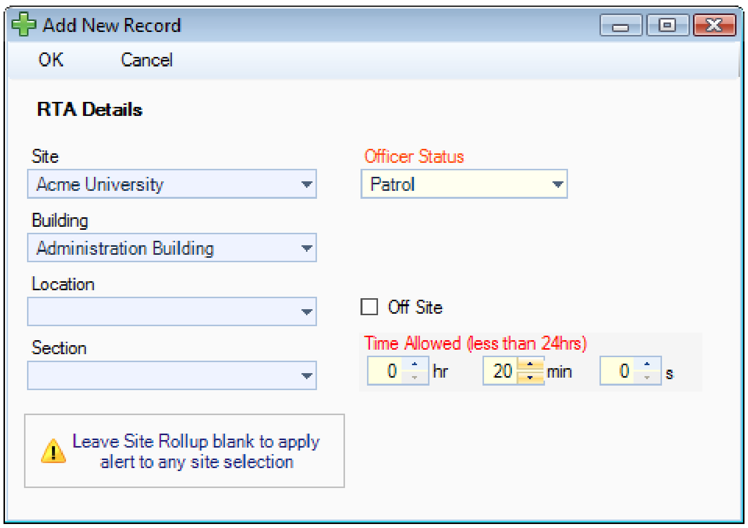
If, for some reason, the officer failed to respond about their status change during the allotted period of time, the timer will start counting the time the officer spends in the set conditions after the time alert expiry, advancing in negative values. The display of the time bar will change to flashing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

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

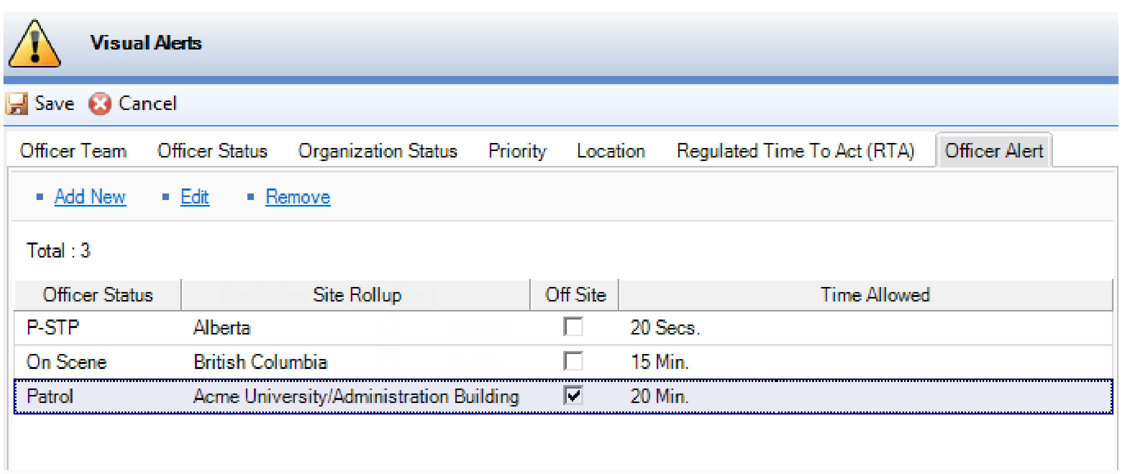


To create a new Officer alert, follow the steps below:

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



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



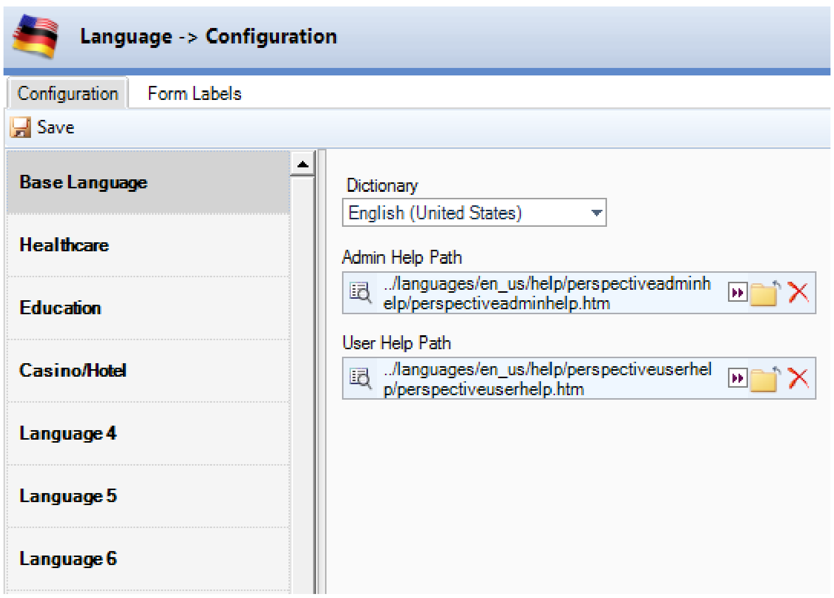
Language

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

Languages

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

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



Set Languages and Help File Paths

1. Select a dictionary to use in the **Dictionary** drop down box.

2. In the **Admin Help Path** and **User Help Path** fields, type the path for the language's associated help files, or click the **Browse** (**...**) button and browse to the appropriate file on your computer or network.

3. Click **Save**.

Form Labels

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

Create a Single Custom Label Set for All Users

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

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

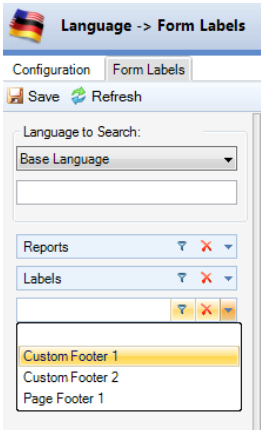
1. Use the **Language to Search** section to bring up the field names you wish to change.
2. Enter your custom field label in the text field that corresponds to the customized language that you created previously.
3. Continue re-labelling fields for your customized language. The column for your customized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

Create Custom Report Footers

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

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

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



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

2. Enter custom footer text in the language label sets required.

The following sample report shows custom footers in effect:

Gateway Administration

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

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

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

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

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

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

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

> The workgroups that will be working with Perspective e-Reporting should have limited visibility to GeoRollups (see the "Specify workgroup visibility for a lookup list" chapter for details). Large lists may cause e-Reporting to hang or crash.

1. Select **Workgroups** in the Navigation pane, choose the correct workgroup from the list, and click **Edit**.

2. Check the **Enable Imports to this Workgroup** checkbox. The Gateway opens by default.

3. Under the **Gateway** tab, start specifying Gateway file import options for the workgroup by providing the workgroup with a unique **Import Key**. This import key will act as an added security measure, restricting imports to the authorized workgroup only.

4. In the **Incident Settings** section below, specify a unique **Incident Prefix** for all of the workgroup's e-Incidents. For example, *WEB* for e-Reports and *EINC* for some other type of electronic reports (e.g., reports from Perspective Web Portal).

5. Choose an **Incident Identifier Format** from the lookup list:

   - **CCYY-MM-#####**: This format identifies the e-Incident by the calendar year (CCYY) and month (MM) that the report was submitted to the Gateway, followed by a five digit sequential number that re-sets at the beginning of each month. For example, 2011-03-00123 identifies the 123rd e-Incident submitted to the Gateway in March 2011.

   - **CCYY-######**: This format identifies the e-Incident by the calendar year (CCYY) that the report was submitted to the Gateway, followed by a six digit sequential number that re-sets at the beginning of each year. For example, 2011-004567 identifies the 4567th e-Incident submitted to the Gateway in 2011.

   - **##########**: This is known as *flat file format*. There is no year or month preceding the number. The first e-Incident submitted to the Gateway will be identified by the number 0000000001, and this sequential numbering will continue indefinitely with no re-set.

6. Specify an **Accepted Retention Period** and a **Deleted Retention Period** for how long imported Item, Person, Organization or Vehicle reports should remain in the Gateway after they have been accepted or deleted by the Gateway Approver or Gateway Administrator.

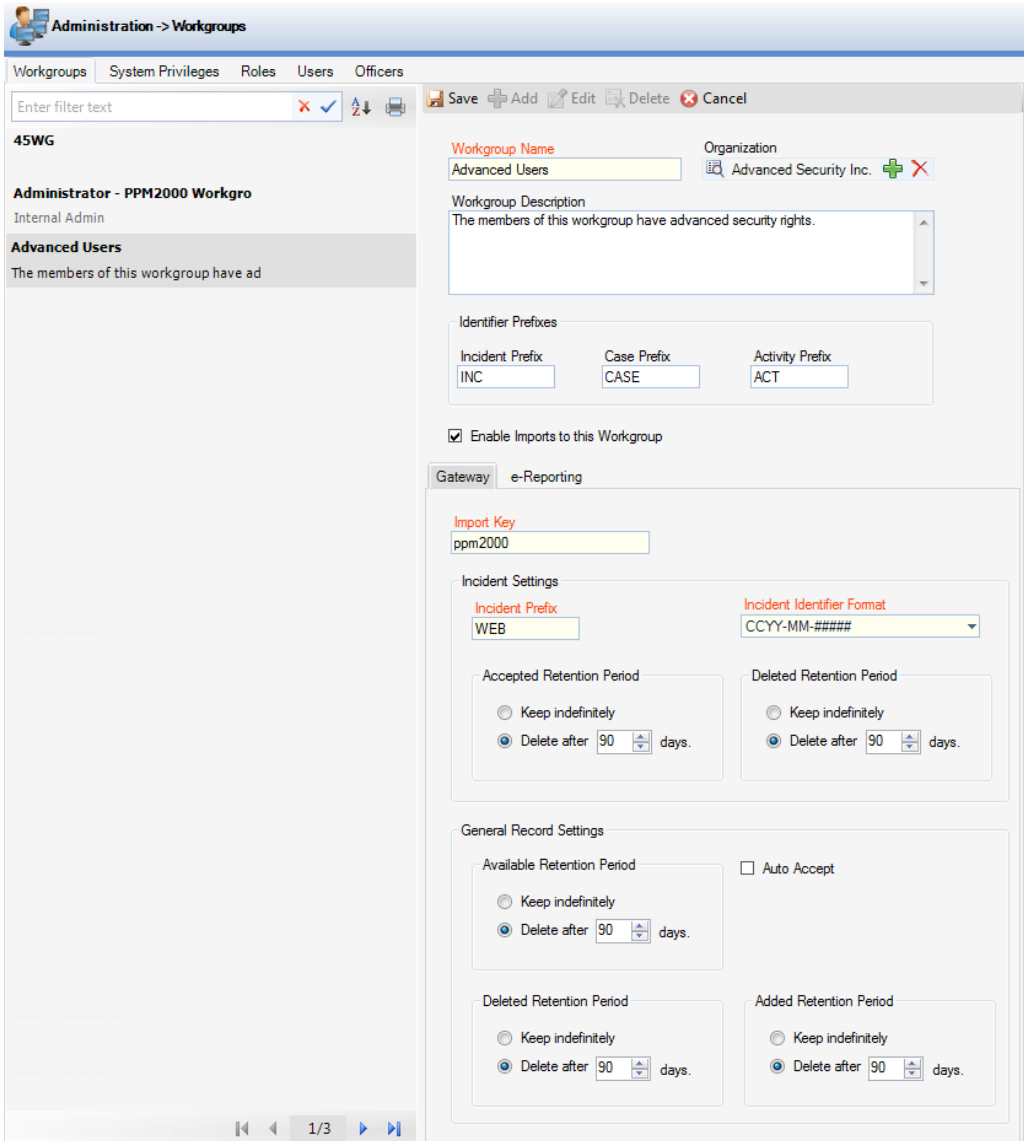
7. Indicate how long imported e-Incidents should remain in the Gateway after they have been made available or deleted by the Gateway Administrator or Gateway Approver under **Available Retention Period** and **Deleted Retention Period**.

8. Under **Added Retention Period**, specify how long imported Item, Person, Organization or Vehicle reports should remain in the Gateway after they have been added to the main Perspective database by authorized users.

9. In the **General Record Settings** section, check the **Auto Accept** box to automatically accept every Item, Person, Organization or Vehicle report that the workgroup imports, making them available for authorized users to add to the Perspective database. If this box is not checked, the workgroup's imported reports will undergo the normal Gateway review process by a designated Gateway Administrator or Gateway Approver prior to being made available or being deleted.

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

10. Click **Save**.



Assign Access Rights to a Gateway Administrator or Gateway Approver

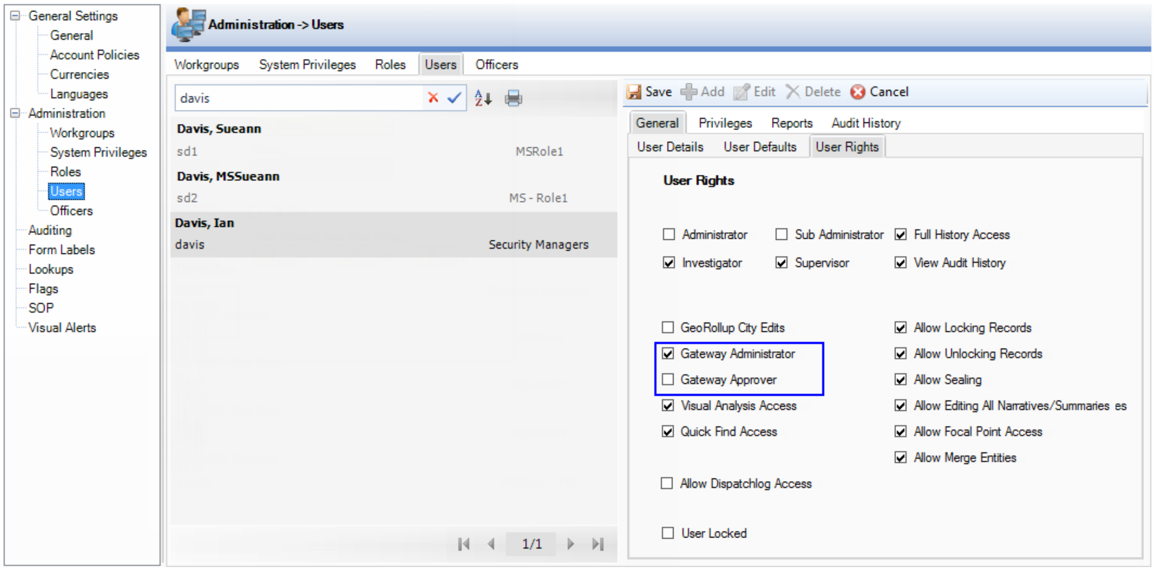
1. Select **Users** in the Navigation pane.

2. Select the correct user from the list, and click **Edit**. By default, the General tab will open.

3. Open the **User Rights** sub-tab.

4. Check the **Gateway Administrator** box or the **Gateway Approver** box to grant the user access to their associated Gateway functions.

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



Administrative Reports

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

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

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

Service Manager

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

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

  Note: Microsoft SQL Server® 2005 Express (supported for the Standard Edition of Perspective only) has a maximum attachment allowance of 50 MB.
- ***Quick Find Indexing***: The Quick Find tool requires regular indexing of your Perspective database for search accuracy.
- ***User Defined Fields***: User defined fields can be added to the Incident, Case (Perspective Premium only), Item, Person, Organization and Vehicle forms under the General tab; to the Incident and Case forms under the Controls tab; and to the Incident form under the Involved Persons, Involved Items, Involved Organizations, Involved Vehicles and Investigation Details tabs.
- ***Custom Search Integration***: With the Custom Search feature, you can launch the Infoglide Identity Resolution Engine™ (IRE) from Perspective to search several data sources at once.
- ***Mass Notification***: With the mass notification feature, you can integrate your MIR3℠ inEnterprise™ solution into Perspective in order to launch notification via Perspective DispatchLog. This will require the Service URL, User Name and Password provided by MIR3
- ***Integration Services URL***: To enable event trigger in Integration Services, enter the URL set up with the Integration Services.

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

Index

Contact Information

Technical Support

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

PPM 2000

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

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