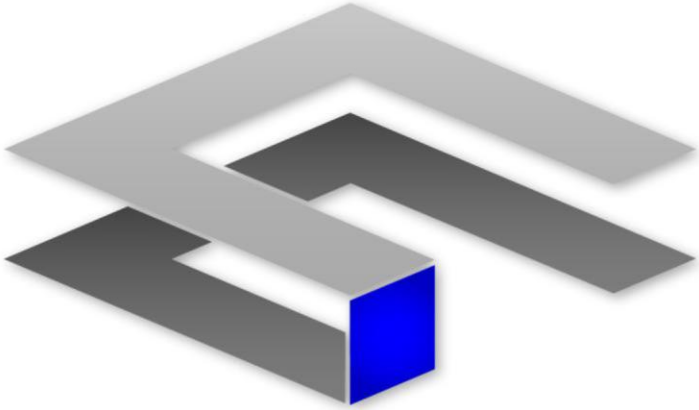


REPORT EXEC ENTERPRISE | ADMIN MANUAL

Table of Contents

Overview

At a Glance

The Report Exec Enterprise Admin program is the control center for all the various features and modules contained within the software. This piece of the program is very powerful and should be used with care. Administrators will have the power to setup the software with the organization's locations, incident types, report dispositions, etc, but they will also have the power to completely re-arrange pre-existing data. If these tasks are performed in an improper manner, or done without backing up the current database beforehand, data loss can occur as a result.

There are 4 main sections of Report Exec Enterprise Admin: System Wide Setup, User Setup, Group Setup, and Auditing. Each area of the Admin program will be covered in great detail in order to provide a supplement to the training that is available for users and Administrators of the software.

System Wide Setup

All of the main settings of the Report Exec Enterprise software are configured within System Wide Setup. In order to be able to track statistics for an organization properly, the dictionaries in the system need to be defined with information pertinent to the organization.

All dictionaries, Tree View and Dropdown, for your organization are defined here and will copy themselves down to the Group dictionaries within the software. System Wide Setup also contains other configurations that will affect the entire program. An Administrator with "System Wide Settings Access" has complete access to all sections of the Administrative part of the program.

User Setup

Administrators will create users and edit their corresponding settings within the User Setup section. A user must be assigned to a Group, or Groups, and given a Role for that Group, in order to access the system. A basic user may be granted "Add/Edit User Access Only" on their user account which will give them the ability to create and manage users of their Group.

Group Setup

Groups are essentially locations or logical divisions within your organization. They are meant to create a separation of workflow within the organization and, as such, certain users can be members of multiple Groups depending on the situation. Once the System Wide Setup is completed, the Group Setup allows specific Groups to have certain features configured differently for them only. For example, different incident types for one or two Groups, or, if the enterprise spans international borders, differing formats for their dates on reports. Administrative access to the software can also be given on a Group-by-Group basis. In other words, a user can be a basic Officer in one Group, yet still have Administrative access for another Group where he has been given more responsibility.

Auditing

Report Exec Enterprise has a built in Auditing function that can give Administrators a basic idea of some of the changes that were made in the program. The system can be audited based on several different criteria: User, Error Messages, Reference Number, Date Range, Sent E-mails, and Messages.

Controlling Access

When giving an individual system wide administrative access to Report Exec Enterprise, it is important to know that these individuals have the power to create, delete, and merge important data within the system. It is recommended to be very selective on the users that are given full admin rights. Group Administrators can be used to control the level of access given to individuals within the program. This includes granting permissions on a user-by-user basis for the Group.

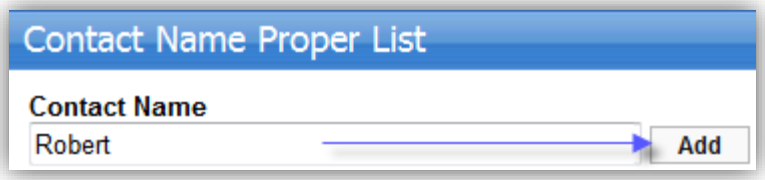
Report Exec Admin

System Wide Setup

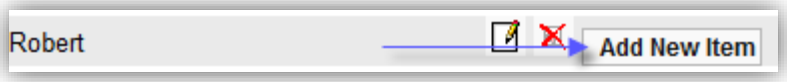
Contact Name Proper List

There are many common proper first names that people have in the world. Many of these names have commonly used shortened variations of them. In order to make tracking and searching for names with multiple variations work with any variation of the name, those variations will need to be added to the Contact Name Proper List. This list will allow your organization to easily search for contacts within the system by any variation of their proper name. For instance, the proper name "William" can be searched and will return results that also match "Will," "Bill," "Billy," "Willy," and any other name added to the list for "William." Many common names are already in the system by default.

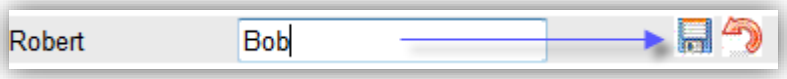
1. Type the proper first name to be added into the **Contact Name** field and click **Add**. This example will use the name Robert although Robert is one of the many names already entered into the listing.



2. Click **Add New Item** to begin entering variations of Robert's name.



3. Enter the variation of the name that needs to be included in the search and click the disk icon to save.



4. "Bob" is now a valid variation for the proper name of "Robert."

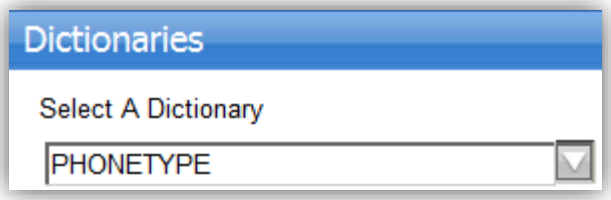
Database Server Configuration

Agencies that use Report Exec Enterprise can choose to share their contact and vehicle information with other organizations with whom they may work with closely. For example, if a University wants to share their vehicle and contact information with a local law enforcement agency that also uses the Report Exec software. Database Server Configuration allows those agencies that use the application, but have a separate database of information, to be able to run searches for those contacts and vehicles from the other system.

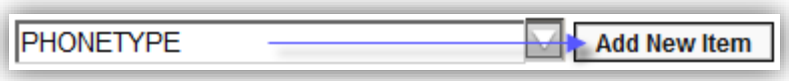
Dropdown Dictionaries

Throughout the Report Exec system there are many dropdown menus that are used to ease the process of filling out reports. These dropdown menus are all configured within the Dropdown Dictionaries section in either System Wide Setup or Group Setup. For example: genders, hair colors, and report dispositions are a few of the various dropdown menu items that can have values both added and removed via the Dropdown Dictionaries section. Dropdown Dictionaries are configured in System Wide Setup, but can additionally be edited on a Group-by-Group basis in Group Setup.

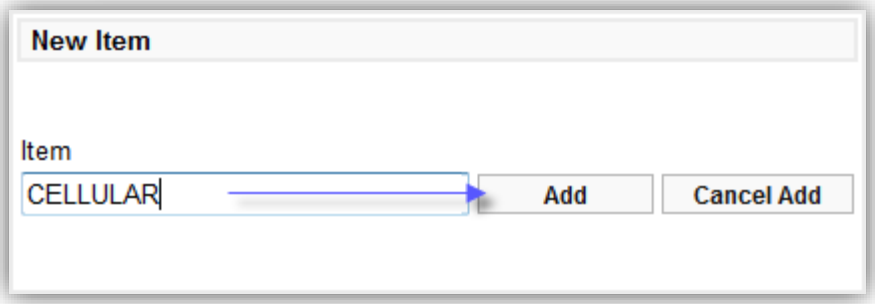
1. Select a dictionary to add new items to from the list. A description of where each dropdown dictionary is located can be found in the table below. For this example we will use the **PHONETYPE** dictionary.



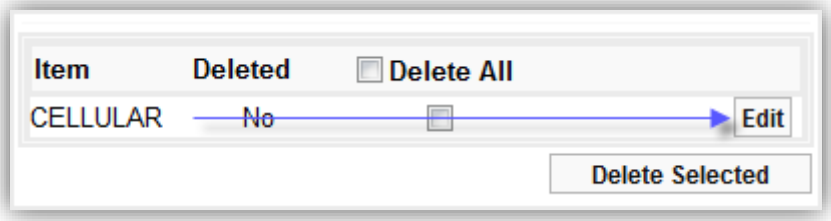
2. To add a new dropdown item to the dictionary click **Add New Item**.



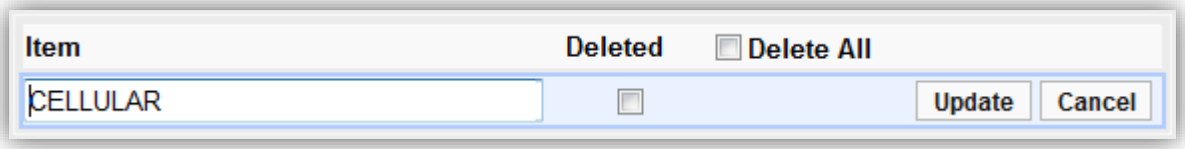
3. Enter the new value into the text field and click **Add**.



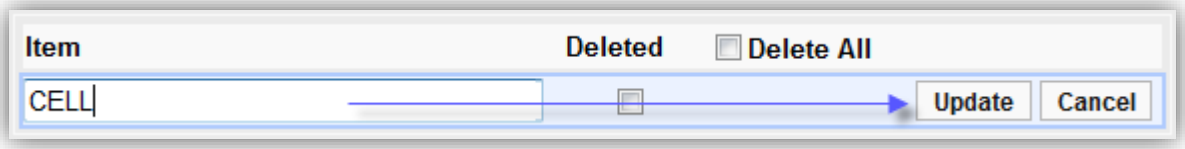
4. To edit an existing item click **Edit**.



5. The item will now be in a free text field and able to be modified.



6. When done, click **Update** to apply the change.



Items can be deleted by checking the corresponding box in the column under **Delete All** and clicking **Delete Selected** to delete a single item. Multiple items may be removed in this manner as well by selecting each item you want to delete and, again, pressing **Delete Selected**. It is important to note that deleting an item will remove it from all reports it was ever used in. Recreating the item will not put it back into the reports because the program will see it as a completely new item, even though the name may be the same.

Dropdown menus in the program are used for a wide array of modules in Report Exec. The following table briefly outlines where each dropdown dictionary is used and whether it is only in System Wide Setup or also in Group Setup. The **S/G** column identifies whether the dropdown dictionary is a System Wide Setup **(S)** or both System Wide and Group Setup as well **(S/G)**.

Dictionary	Location	Description	S/G
Access Level	Visitor Tracking	Visitor's access to a site	**S/G**
ActivityType*	Daily Event Log & Field Interview Report	Daily Event Log – What officer is doing Field Interview Report – Type of report	**S/G**
AddressType	Contact – Person/Business	Type of address (i.e. Home, Work)	**S**
Age	Contact – Person	Approximate age of person	**S/G**
AlarmType*	Case Report	Description of alarm (i.e. Burglar, Motion, Panic)	**S/G**
AnimalBreed	Contact – Animal	Breed of animal	**S**
AnimalHairColor	Contact – Animal	Hair color of animal	**S**
AnimalType	Contact – Animal	Type of animal	**S**
Attire	Contact – Person – Use of Force	Clothing officer was wearing (i.e. Plain Clothes, Uniform)	**S/G**
BodyPart	Contact – Person – Injury	Injured body part (i.e. ankle, neck)	**S/G**
BOLOType	BOLO Report	Type of BOLO being issued	**S/G**
Breathing	Contact – Person – Injury	Located in "Medical Officer" area of Case Report. Description of contacts' breathing (i.e. rapid, shallow)	**S**
Build	Contact – Person	Description of person's general body type. (i.e. muscular, skinny)	**S/G**
CautionType	Contact – Person	Category of Caution	**S/G**
CellPhoneProvider	Online Permit Registration (OPR)	Cell Phone Provider (i.e. AT&T)	**S/G**
CheckOutPurpose	Property Manager	Reason property was removed (i.e. Court, Lab)	**S/G**
CitationType	Citation Report	Category of Citation (i.e. Parking, Moving)	**S/G**
Company	Admin – User Setup	Company a Report Exec user works for	**S**
ConsciousnessLevel	Contact – Person – Injury	Located in "Medical Officer" area, description of contacts' consciousness	**S**
ContactType	Contact – Person/Business	Contact's relationship to case (i.e. Victim, Witness, Suspect)	**S/G**
ContrabandDiscoveredType	Profiling	Any contraband discovered during stop	**S/G**
CorrectiveAction	Risk Management	Corrective action taken during risk assessment	**S/G**
Court	Arrest/Booking	Court contact is being seen in	**S/G**

CourtLocation	Arrest/Booking	Location of Court (i.e. County, Municipal)	**S/G**
CrimeAlleged	Profiling	Purpose for stop	**S/G**
CrimeClass	Case Report	Ties directly to incident type. Degree of incident (i.e. Felony)	**S/G**
Demeanor	Contact – Person	Description of person's demeanor	**S/G**
Department	Visitor Tracking	Department person works for who is being visited	**S/G**
Direction	Contact – Person/Business	Street direction	**S**
Disposition	Reports	Dispositions for all of the various report types in Report Exec	**S/G**
Distance	Contact – Person – Use of Force	Distance officer standing from offender when using OC, Taser or Firearm	**S/G**
DistinguishingFeature	Contact – Person	Any distinguishing features of an individual	**S/G**
EmergencyAlarmSounded	Emergency Response	Type of alarm sounded	**S/G**
EmergencyNotificationType	Emergency Response	How department notified of emergency	**S/G**
EmergencyResponseLevel	Emergency Response	Agency level of response	**S/G**
EmergencyType	Emergency Response	Type of emergency	**S/G**
EyeColor*	Contact – Person	Person's eye color	**S**
FireAlarmMethod*	Case Report	How a fire alarm sounded	**S/G**
FireAlarmNature*	Case Report	Purpose or reason for fire alarm	**S/G**
FireExtinguisherType*	Case Report	Type of fire extinguisher used	**S/G**
Gender*	Contact – Person	Person's gender	**S**
HairColor*	Contact – Person	Person's hair color	**S**
HairLength	Contact – Animal	Length of animals fur	**S**
Hospital*	Contact – Person – Injury	Hospital contact was transported to	**S/G**
IDNumberType	Contact – Person – Additional Info	Other ID types contacts can have (i.e. Passport, State)	**S/G**
IncidentCostItem	Case Report	Item used that incurred a cost	**S/G**
IncidentDisposition	Case Report	Disposition field for Incident Type	**S/G**
IncidentStatus	Risk Management		**S/G**
Indoors	Contact – Person – Use of Force	Type of indoor environment force was used in	**S/G**
InjuryStatus*	Contact – Person – Injury	Severity of injury	**S/G**
InjuryType*	Contact – Person – Injury	Type of injury	**S/G**
InvestigationEvent	Investigations	Task investigator is doing – used for tracking time spent on investigation	**S/G**
InvestigationStatus	Investigations	Current status of investigation (i.e. Open, Closed)	**S/G**
InvestigationType	Investigations	Type of investigation being conducted	**S/G**

JailActivityType	Arrest/Booking Module	Action being taken with person being held (i.e. Meal, Check)	**S/G**
KeyboardLocation	Key Tracking	Location keys are being kept	**S**
KnownAssociateType	Contact Screen	The type of person a known associate is being listed (i.e. Parent, Friend)	**S/G**
Lighting	Case Report – Injury	Lighting of area injury occurred	**S/G**
LikelihoodofReoccurrence	Risk Management		**S/G**
LocationOfSubjectWeapon	Contact – Person – Use of Force	Where a weapon was a subject had access to	**S/G**
MaxientLocation	Maxient Integration	Location for Maxient report.	**S/G**
MaxientNature	Maxient Integration	Nature of Maxient report.	**S/G**
MaxientUrgency	Maxient Integration	Urgency of Maxient report.	**S/G**
MethodofReporting	Case Report	Way a report was made/discovered	**S/G**
MissingResources			**S/G**
OffenderForce	Contact – Person – Use of Force	Offender's use of force	**S/G**
OffenseLocation	Profiling	Location type stop occurred (i.e. Highway, Country Road)	**S/G**
OfficerPresenceAtTimeOfIncident	Use of Force	Officers present at use of force event (i.e. Alone, other officers present)	**S/G**
OriginofThreat	Online Reporting (OLR)		**S/G**
OSHAInjuryType	Contact – Person – Injury – Employee Injury	OSHA defined Injury Types	**S/G**
OTEvent	Scheduling Module	Type of overtime being scheduled	**S/G**
OtherNameType	Contact Screen	Types of other names that can be used	**S/G**
Outdoors	Contact – Person – Use of Force	Type of outdoor environment force was used in	**S/G**
Ownership	Property	Ownership of property (i.e. Personal, Company)	**S/G**
PermitLotStructure	Permit Module	Location permit is assigned to	**S/G**
PermitPeriod	Permit Module	Permit period (i.e. Fall, Annual)	**S/G**
PermitRegistrationType	Online Permit Registration	Affiliation of person registering	**S/G**
PermitRestriction	Permit Module	Any restrictions on a permit type	**S/G**
PermitType	Permit Module	Type of permit being assigned/requested	**S/G**
PersonType	Key Tracking Module	Type of person checking out key	**S/G**
PhoneType	Contact Screen	Type of phone number (i.e. Home, Cell)	**S**
PhysicalDevice*	Contact – Person – Injury	Any devices that help a person physically move (i.e. cane)	**S/G**
PlateType*	Vehicle Screen	Type of plate on vehicle	**S**
ProbableCause	Profiling	Type of probable cause leading to	**S/G**

		search	
PropertyCategory*	Property Screen	Classification of property being entered (i.e. Stolen, Evidence)	**S/G**
PropertyColor	Property Screen	Color of property item	**S/G**
PropertyLocation*	Property Screen	Location property taken into custody was placed	**S/G**
PropertyReleaseMethod	Property Manager	How property was released	**S/G**
PropertyType*	Property Screen	Type of property being entered (i.e. Cash, Clothing, iPod)	**S/G**
PublicProperty	Contact – Person – Use of Force	Type of public property environment a use of force incident occurred	**S/G**
QuickNotes	Daily Event Log	Common notes used in log entries	**S/G**
Race*	Contact – Person	Race of a contact	**S**
Reason	Reports	Reason a report was returned	**S/G**
ReasonForForce	Contact – Person – Use of Force	Why a level of force was used	**S/G**
RootCause	Risk Management		**S/G**
Skin	Contact – Person – Injury	Located in "Medical Officer" area, description of contacts' skin	**S**
SprayType	Contact – Person – Use of Force	Type of OC spray used	**S/G**
State	Dispatch – Vehicle	State a vehicle registration belongs to	**S/G**
StatsCanAgeCategory	Statscan – CANADA ONLY		**S/G**
StatsCanHandlingType	Statscan – CANADA ONLY		**S/G**
StatsCanOffense	Statscan – CANADA ONLY		**S/G**
StatsCanStatus	Statscan – CANADA ONLY		**S/G**
StreetType	Contact – Person/Business	Type of street (i.e. Street, Road)	**S**
StructureType	Case Report – Fire	Type of structure fire was in	**S/G**
SurfaceType	Case Report – Injury	Surface type injury occurred	**S/G**
TaskStatus	Task	Status of assigned task	**S**
TrafficStopType	Profiling	Why a stop was done	**S/G**
Training*[1]	Training Module	Type of training	**S/G**
TransportingAgency*	Contact – Person – Injury	Agency that transported person to hospital	**S/G**
TypeOfAssignment	Contact – Person – Use of Force	What officer was doing when use of force incident occurred (i.e. general patrol, undercover)	**S/G**
TypeOfFirearmUsed	Contact – Person – Use of Force	Type of firearm used by officer	**S/G**
TypeOfTeam	Contact – Person – Use of Force	If officer was part of a team (i.e. SWAT), type of team	**S/G**

[1] **Note**: When setting up training drop down options there is a column for "Notification Days." This allows users to define the number of days prior to a training certification expiring to automatically notify the officer about the upcoming expiration.

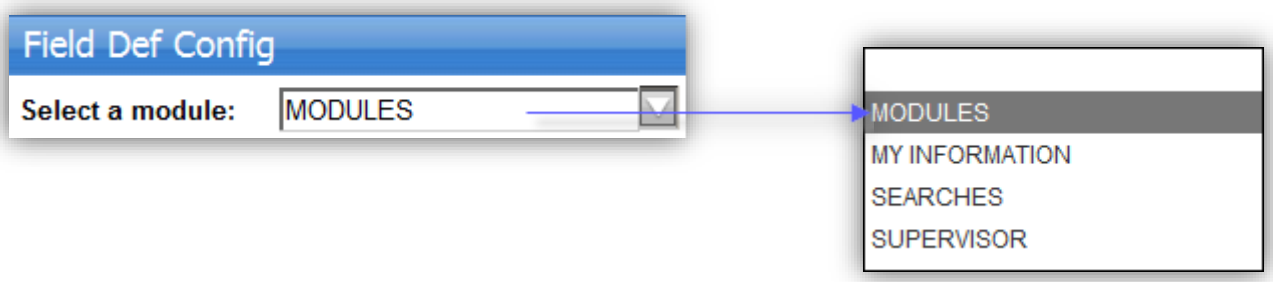
VehicleColor*	Vehicles	Color of vehicle	**S**
VehicleMake*	Vehicles	Make of vehicle	**S**
VehicleStyle*	Vehicles	Style of vehicle (i.e. sedan)	**S**
ViolationDescription	Profiling	Description of violation person was stopped for	**S/G**
ViolationType	Citation Report	Type of violation for Citations	**S/G**
VisitorIDType	Visitor Tracking	Type of ID visitor used when checking in	**S/G**
VisitorTrackingPriority	Visitor Tracking	Priority of visitor checking in (i.e. VIP)	**S/G**
VisitorType	Visitor Tracking	Type of visitor (i.e. contractor)	**S/G**
WarningMethod	Clery	How a timely warning was made	**S/G**
WarrantStatus	Arrest/Booking	Status of warrant	**S/G**
WarrantType	Arrest/Booking	Type of warrant issued	**S/G**
Weather	Case Report – Injury	Weather at time of injury	**S/G**

Field Definition Configuration

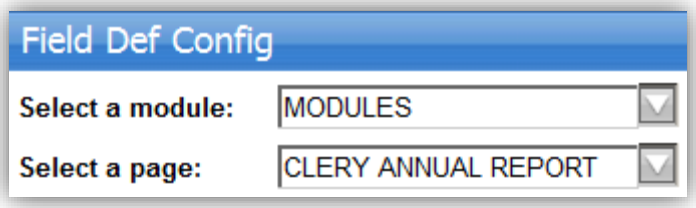
Administrators of Report Exec Enterprise have the ability to customize nearly every area of the system with Field Definition Configuration. The Enterprise software is a very robust package that provides the ability to be tailored to the needs of each organization that uses it. As a result, some agencies find that there are fields that are not, and will never be, required or used by their organization. On the other hand, there may also be some fields that absolutely must be filled in by a user for the requirements of the agency.

The three main purposes of this configuration tool within the system are: to hide or unhide fields, to make specified fields be required fields, and to change the text of nearly any field throughout the program. The following example will customize the **Cancel Button** from the **Clery Annual Report** page within **Modules**.

1. Select a module from the dropdown. This example will use **Modules**.

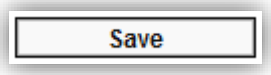


2. Select a page that corresponds with the module selected in Step One.



3. To hide a field, uncheck the box in the **Visible** column (3a). To make a field required, check the box in the **Validation** column (3b). To change the title of the field, type the new name in the **Custom Label** field (3c).

4. Click **Save** to apply changes when complete.



Import Contacts

A Microsoft Excel Spreadsheet may be populated with large numbers of contacts to be imported into the system through Import Contacts. This import is designed to bring contacts into the system without having to first enter them into a report. It can also be used to update existing contacts without having to change them within a report.

Importing updated information of a pre-existing name will update the existing Master Name record. This only affects the contacts' Master Name in the system and will not affect all other entries of the contact in reports, also known as "entities." This function cannot be used to delete a Master Name.

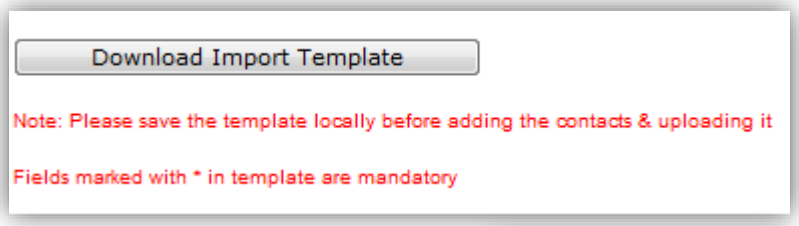
The Contact Import reads the specifically formatted Excel spreadsheet that contains one line per contact. All of the fields seen in the table below are available, but only First Name and Last Name are truly required. The format of the spreadsheet cannot be changed.

Import Spreadsheet Fields

First Name (required)	Eye Color	Street Number	Zip
Middle Name	Height	Street Name	Home Number
Last Name (required)	Weight	Street Type	Cell Number
Date of Birth	Driver's License Number	Direction	Work Number
Gender	Driver's License State	Apartment	Notes
Race	Title	City	Department
Hair Color	Social Security Number	State	E-mail

Preparing to import:

1. Click **Download Import Template** and save the file to an easy to find location on your local computer.



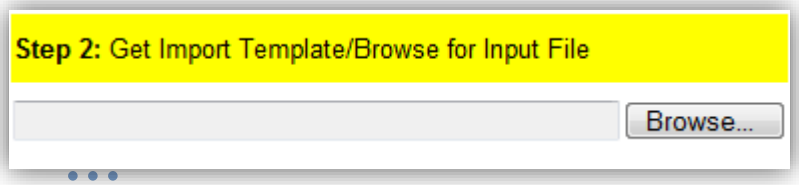
2. Open the spreadsheet in Microsoft Excel and fill in the needed information but do not alter the formatting of the template. The program needs it to be as-is.

3. Save the template.

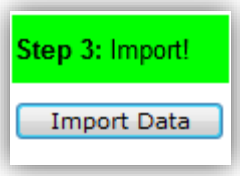
To import contacts:

1. Under the red box labeled **Step 1**, select the fields that Report Exec will use to determine if a person is already in the system. For example, selecting First Name, Last Name, Date of Birth, and SSN/Other ID means if an imported contact matches all of the selected fields for an existing person in the system, they are considered the same person and the imported information will update the existing information for this person.

2. Click **Browse** and locate the template file in the directory it was saved in.



3. Click **Import Data**.



If a contact is determined to be new, it will be added as a "Person" Contact Type into the system. If the contact is already in the system, their information will be updated based on the information imported into the program. Note that only a contact's master record will be updated. Any information for a contact already added to a report will not be affected. If a contact that is in the Report Exec system is not in the imported contact list, it will NOT be deleted since the contact may be referenced in a report.

Additionally, a log file is available after the import if you click **View Log**. All import log files are stored in the **CESIReportExecAdmin** folder on the IIS server, in the folder **…\CESIReportExecAdmin\Templates\Contact Import Logs**.

License Setup

Administrators can see which users are logged into the program and using licenses, and from what IP address the connection is coming from. Users can be forced out of the program by clicking on their corresponding IP Address next to their user name under the System Licenses area at the bottom of the page.

Session IP	User	Type	Time Logged In
192.168.0.1	USER, TEST	Web Module	2011/12/28 01:20 PM

If requested, Report Exec Technical Support will use this area to increase/decrease an organization's concurrent licenses and also to change the name of the company that is displayed, if it is ever needed. Any changes to this area must be done by a Technical Support Representative of Report Exec. Technical Support can be reached by emailing support@reportexec.com or calling 414-423-9800, option two.

Mass Change Dictionaries

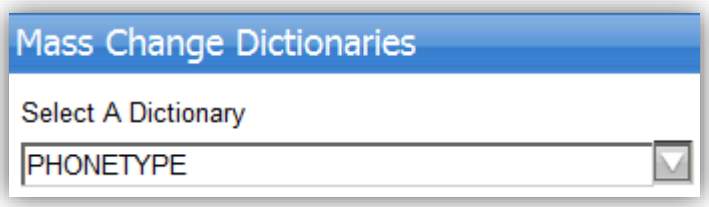
It is recommended to backup the database before making any large changes to the dictionaries in the system.

Administrators have the ability to merge or change the dropdown dictionary items throughout the system using the Mass Change Dictionaries tool. The ability to change these items is only available to an Administrator with **System Wide Settings Access** enabled on their user account and can be used as an alternative to deleting.

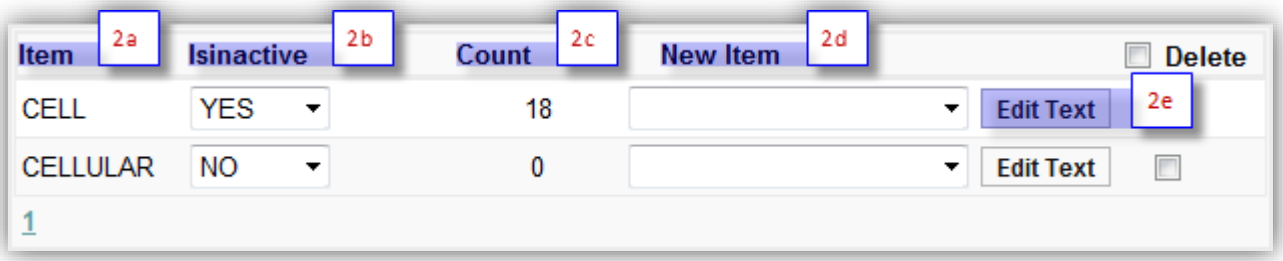
Changing dictionary items, typically, is not something that needs to be done, but the feature is there when needed and should be used with caution. This tool is meant to aid in the restructuring of the dictionaries for the organization to allow for future changes within the agency. Changing an item here and pressing **Mass Change Items** tells the program to overwrite all entries for that item throughout the entire system.

As an example, an organization has used the abbreviation "CELL" to define the cell phones for years. A change in the regulations for the agency now requires that they spell out the words, such as "Cellular," on all of their reports. An Administrator can make the change to the **PHONETYPE** dictionary here, which will then mass change that item through all reports it was ever used in. The following illustration will use the **PHONETYPE** dictionary.

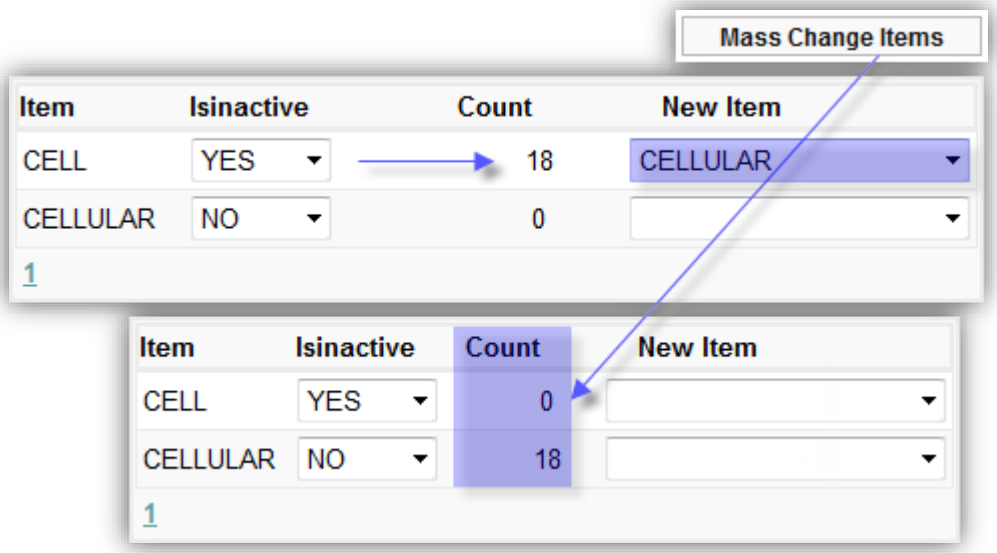
1. Select the dictionary to change.



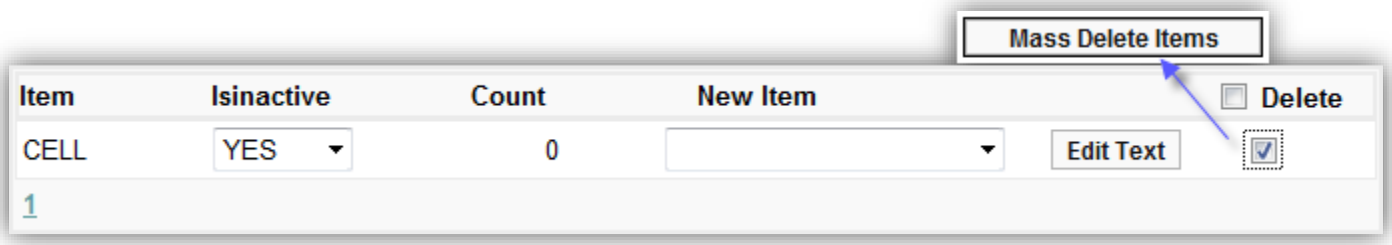
2. Find the item to change in the **Item** column (2a). In the **New Item** column (2d), select the item name to change from the dropdown field, or click **Edit Text** (2e) and type in a new name for the dictionary. The **Count** column (2c) will tell indicate how many times the item is used throughout the system. **Isinactive** (2b) means the item is deleted.



3. Click **Mass Change Items**. Multiple dropdown dictionary items may be renamed at a single time. Once the change is completed, the **Count** column should read "0" next to the old items that were changed, and the new item should now have a value for that column.



4. After the change has been completed a check box will show under the **Delete** column if the item has a count of zero. Dictionaries with a count of zero are safe to be deleted, if necessary.



Menu Items Configuration

As of Enterprise version 11.08.15112.3, this section only provides the option to hide or rename the "Court Schedule" section of My Information.

Module Authentication

The online modules are designed as a portal for people, outside of the normal Report Exec Enterprise program users, to have a way to submit information to be entered into the system. Anyone who's Role includes Online Reports, Online Permits, or Visitor Tracking has permission to view the information submitted by the corresponding online module.

There are three online reporting modules: **Online Reports (OLR)**, **Online Permit Registration (OPR)**, or **Online Visitor Tracking (VT)**. These modules may be disabled system wide or for specific Groups if they are not needed.

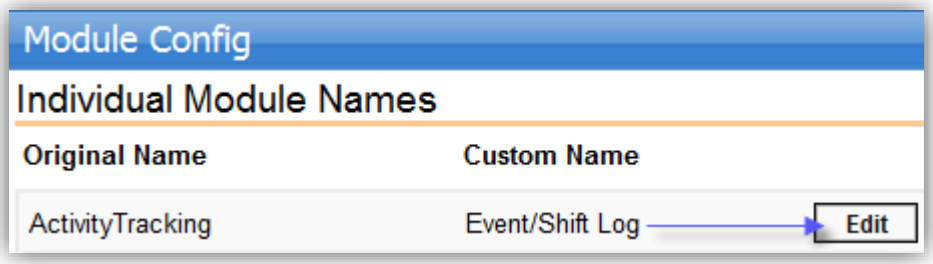
If the online modules are enabled then the online information can be submitted by anyone with internet access, unless authentication is required. Requiring authentication is a way to only allow Report Exec users to use the online modules as it requires them to login first.

Module Configuration

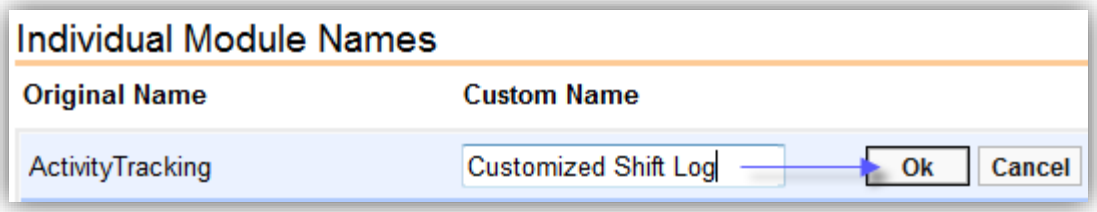
Report Exec Enterprise is designed to be adapted to meet the needs of the individual company that uses the software. What might be called an "Event Log" in one place may be a "Shift Log" in another. Module Configuration allows the Administrators to change the names of the various modules in the software to better match the workflow of the company utilizing it.

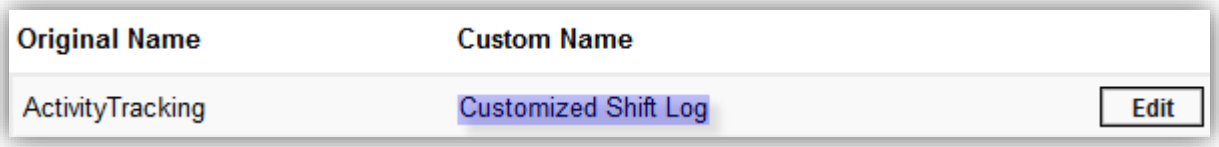
The only drawback to changing the default names is if the Report Exec Technical Support or Training Teams ever needs to be contacted with a question or problem, they would not know the customized module names right away which may cause some confusion. An example would be an agency that renames the "Follow Up Report" to "Supplemental". Technically speaking any report type can be a supplement to another report so Report Exec Technical Support and training might not know exactly what is being asked at first. The original name of the module can be also be found here in Module Configuration as well for future reference, if needed.

1. Click the **Edit** button next to the module name to be changed.



2. Type the new name into the **Custom Name** column and click **Ok** to apply the changes.





3. Click **Update Changes** at the bottom of the page to finish saving any changes made to the page.

ODBC External Data Configuration

Any agency with a pre-existing database may find it useful to integrate their current data into the Report Exec system using the Outside Database Connection module. There are no setup options that can be configured here by an Administrator, as this module must be customized depending on the specifications of the pre-existing database.

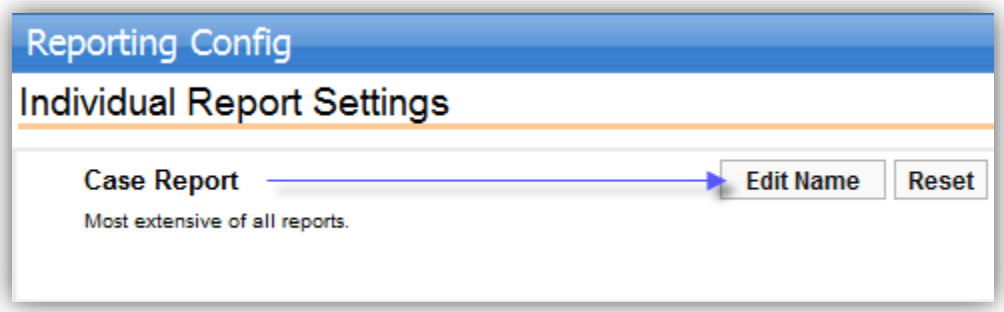
To learn more about integrating an external data source into the Report Exec Enterprise system email the Sales Team at sales@reportexec.com or call (414) 423-9800 option one for more information about the ODBC Module.

Reporting Configuration

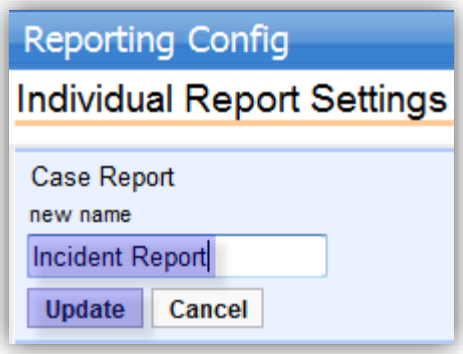
As stated in the previous section about Module Configuration, Report Exec Enterprise is designed to adapt to meet the individual needs of the company using the software. Reports in the system can have their default titles changed to whatever the organization needs them to be. For example, a "Case Report" for one agency might be the same as an "Incident Report" for another agency. Reporting Configuration is where an Administrator can go to make those changes to the software.

It is also possible that an organization may need reports named with different titles, depending on the Group that writes the report. Report titles can be further configured Group-by-Group in the Reporting Configuration section found under Group Setup.

1. Click **Edit Name** next to the report name to be changed.



2. Click **Update** once the new name has been entered.



3. Click **Update Changes** at the bottom of the page once all changes have been made.

Roles

The Roles in Report Exec Enterprise define what permissions/access a user has available to them when they log in. A Role must be assigned to a user in order for them to gain access to the program. For example, the default settings of the Administrator Role allow access to all modules with privileges to delete information and run Admin Reports. Individual users that belong to multiple Groups in the company may have a different Role in each of those Groups.

Report Exec Enterprise has 16 commonly used Roles, with corresponding permissions, pre-configured in the software by default. The following table lists those Roles in no particular order.

Default Roles			
Administrator	Head Reviewing Officer	Officer	Schedule Administrator
Clery Officer	Investigator	Property Manager	Schedule Officer
Dispatch Supervisor	Investigator Supervisor	Report Reader	Schedule Supervisor
Dispatcher	No Access	Reviewing Supervisor	Supervisor

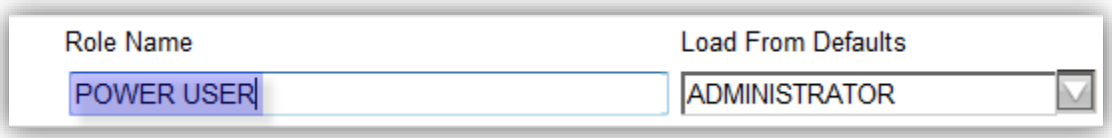
The default Roles each have their settings configured in a way that coincides with the name the Role has been given. It is recommended to leave the default Roles the way they are, however each may be configured to give more or less permission depending on the needs. Also, a new custom Role may be created if your needs require.

In the next example a custom Administrator Role is created that allows access to the Admin program, using the Module and Role permission tabs some of the access that a default Administrator would have can be removed.

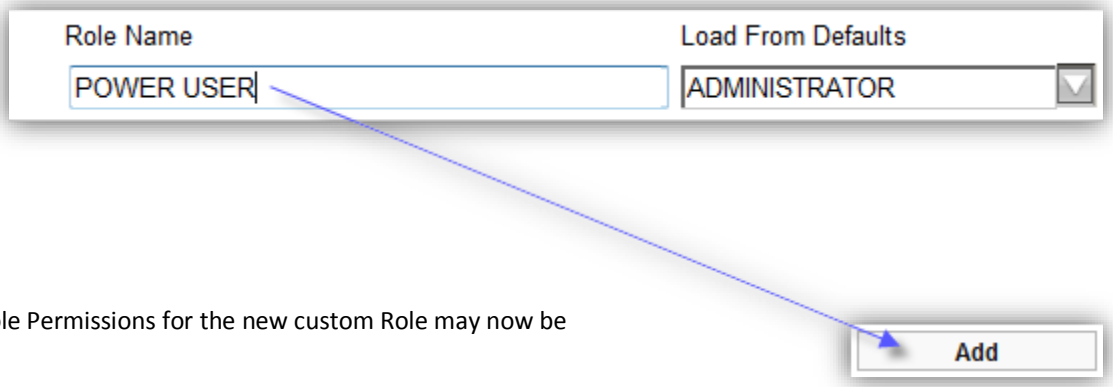
Creating a custom Role:

1. Click **Add New Role**.

2. Enter a name for the new Role then select a default set of permissions to load from the dropdown menu **Load From Defaults**. The Role Name "Power User" has no significance, it is simply for illustration. This Power User Role will be able to access the Admin program to change settings, but not be able to create reports like a full Administrator would.



3. Click **Add** at the bottom of the page to add the new Role to the system.



4. The Module and Role Permissions for the new custom Role may now be configured.

The access for the Role is controlled through the Module Permission and Role Permission tabs. Both the Module Permission and Role Permission tabs will be covered in the following sections.

Module Permission Tab

Module Permissions define what a Role is allowed to do once it has been given access to the Module on the "Role Permission" tab. The following table will illustrate the modules in Report Exec that permissions can be set for.

Modules				
BOLO	Citations	Clery Reports	Dispatch	Emergency Response
Event/Shift Log	Investigation	Key Tracking	Online Permit Registration	Online Reporting
Parking Permit	Pass Down Log	Profiling	Property	Report: Case Report
Report: Field Interview	Report: Follow Up	Report: Found Item Report	Report: Lost Item Report	Report: Towed Vehicle
Scheduling	Traffic Stop	Training	Trespass	Visitor Tracking
Work Place Violence				

The module names in the above table are the default module names. Individual names can be changed with Module Configuration within System Wide Setup. Each Role may be allowed a different Module Permission for any number of different modules. When defining a Role, the Administrator has the option to give any of the following five permissions to a module:

- ***Create*** – Users with create access can create a new record in the associated module.
- ***Read*** – Users with read access can view records associated with that module.
- ***Edit*** – Users with edit access can edit records in the associated module. Only an Administrator may edit another user's records. A Dispatcher, by default, can edit other user's Daily Events.
- ***Print*** – Users with print access can print records from the associated module.
- ***Delete*** – Users with delete access can delete a record in the associated module.

Role Permission Tab

Role Permission determines the modules that a Role is permitted to access. Once a Role has been given access to a module it will also need permissions specified in the Module Permission tab to define what they can do once in the module. There are 17 Role Permissions that determine the type of access a user or Administrator will have in Report Exec Enterprise.

Role Permissions	Description
Role Permissions	Description
Clery Access	Ability to enter Clery information into reports.
CodeRed Mass Notification Access	Ability send and configure CodeRed mass notifications.
Dispatch Mobile User	Access to log into Dispatch Mobile.
E-mail Notifications	E-mails are sent to the users when they are assigned a report, task, or investigation.[2]
Group Admin	Administrative rights within the report-writing part of the program (i.e. ability to delete and re-open reports).
Group Dispatch Supervisor	Access to the Setup menus within Report Exec Dispatch.
Group Dispatcher	Access to Report Exec Dispatch.
Group Supervisor	Access to the Supervisor menu within the report-writing part of the program.
Investigations Supervisor	Allows a user edit access to Investigations the user was not assigned to.

[2] *A user must have an e-mail address associated with their user account within User Setup in order to be able to receive the e-mail notifications generated by this Role Permission.*

Lost & Found Property Editor	Gives the ability to edit the Found Item Reports and Lost Item Reports that were created by other users
Medical Officer	Adds an additional tab of information to fill in on the Contact Injury screen.
Preview Access	Ability to view reports that are in progress.
Property Manager	Access to Property Manager.
Review All Reports	Gives a listing of reports, under the Investigations module, that have been completed without the user needing to be listed as a reviewer.
Risk Manager	Provides access to the Risk Management module components.
Schedule Administrator	Final level approval for scheduling requests.
Schedule Officer	Ability to view and make requests for days off, overtime, and swaps.
Schedule Supervisor	First level of approval for schedule requests.
Statscan Officer	Ability to enter statscan information. (Canada only)
UCR Officer	Ability to enter UCR information.

Once done giving Role Permissions, make sure to click **Update** at the bottom of the screen to apply any changes.

Customize permissions by checking or un-checking what module access and permission the Role should have. Separate access can be given for various types of reports. For example, there is a front desk person that may write lost and found reports, but no other type of report, the Administrator can create a custom Role and just give permission to Lost Item and Found Item Reports. Once that Role is assigned to the desired user(s) within the desired Groups then they will only be able to write/access those Lost and Found Reports.

System Settings

System Settings is where most of the finer details of the Report Exec Enterprise/Direct application are configured. System settings can be further defined by Group within Group System Settings. The following list contains all of the options found in System Settings, and their purpose, in the order in which they are found in the program.

- **Client Web Time Out** – Number of minutes of inactivity before the program automatically logs a user out and releases the license.
- **Dashboard Refresh Timer** – Number of minutes for the Dashboard to refresh with current information.
- **Dashboard Bolo Refresh Timer** – Number of minutes for the Bolo section of the Dashboard to refresh with current information.
- **Dashboard Task Refresh Timer** – Number of minutes for the Task section of the Dashboard to refresh with current information.
- **Dashboard Messages Refresh Timer** – Number of minutes for the Messages section of the Dashboard to refresh with current information.
- **Keep Clients Logged In Ping Timer** – Number of minutes for the system to ping the server for a response – if the ping timer is set to a number lower than the Client Web Time Out the system will not log a person out for inactivity.
- **Auditing Level** – The level of auditing that occurs in the system – auditing records are accessed through the administrative page.
- **Past Shift Event Hours** – The number of hours a user has to make a modification to a daily log entry.
- **Enable Multiple Field Specific Report Address** – If set to **NO** the Specific Location field is a single free text field. If set to **YES** the Specific Location field changes to an address format with five fields.
- **Enable Single Field Contact Address** – If set to **NO** the contact address is a five field address format. If set to **YES** the contact address is a single free text field.
- **Time Mode** – Select **AMPM** for 12-hour time or **Military** for 24-hour time formatting.

- **Server Time Zone Offset** – The difference in time between where the server is located and where the program is being used.
- **Date Format** – The default setting is **ISO** (*International Standard Time*)[3].
- **Date Format Override** – Allows the agency to change the date format to what is used locally.
- **Use Daylight Savings** -
- **Culture** – If **en-US** is selected certain terminology, such as "Miranda Warning," will be the U.S. based standards. If **en-CA** is selected then the program will use Canadian-English terminology.
- **Hide Juvenile Record** – If **YES** is selected the program will always hide juvenile information from printing, if **NO** is selected the system will not automatically hide juvenile information but will provide the user with the option to hide juvenile information upon printing.
- **Enable UCR Codes** – If a department reports UCR this field needs to be marked **YES** which will enable the UCR Module.
- **Enable ODBC Module** – This should only be marked "Yes" if the ODBC Module has been purchased.
- **Enable Review Messages** – Sends messages to reviewers through the messages area of the dashboard when cases have been submitted.
- **Measurement System** – Defines whether Height and Weight fields use **METRIC** or **IMPERIAL** measurements.
- **Concurrent Logins** – If this setting is unchecked then a user can only login to one computer at a time with the same user ID. Once the user logs out from that computer then can then login to a different computer.
- **Required Password Length** – Checking this option and defining a value for the length forces this setting on passwords. For example, "8" requires passwords to be at least 8 characters long.
- **Required Number of Alphabetical Characters –** Defines the number of letters required in a password.
- **Required Number of Numeric Characters** – Checking this option and defining a value for the number of numeric characters requires passwords to have that many numbers in them. For example, "2" requires that passwords have at least 2 numbers in them.
- **Required Number of Non-Alphanumeric Characters** – Defines the number of symbols required in a password.
- **Password Attempts** – Checking this option and defining a value will lock out the user if they unsuccessfully login that many times. For example, "3" will lockout a user if they enter the wrong password 3 times.
- **Password Expiration Interval** – Checking this option will force users to change their passwords after the defined number of days has passed.
- **Password Change on Next Logon Interval** – Number of days before a user must change their password.
- **Active Directory Setups** – The following fields are required for AD/LDAP authentication into the program: Password Authentication Mode, Active Directory Server Name, Active Directory Server Base Domain, and LDAP Domain Controller.
  - ***Password authentication*** is how the program authenticates for logging in. There are 2 settings for this field. The first way and most widely used is **DB**. **DB** authenticates directly to the Report Exec database and needs no additional set up other than setting up a user in the "Add User" section. The second way is through Lightweight Directory Access Protocol or **LDAP**. **LDAP** authenticates directly against an agency's Active Directory (AD) server. What this mean is that as long as the user has an AD account the user will be able to log into the system. Users still need to have an account built in Report Exec Admin for **Role** and **Module** permissions. This user name must be exactly identical to the user name in AD otherwise they will be denied access. If a user logs in that does not have an AD account, or they do not have an account in Admin to match, they will be denied access and asked to log in again with a valid account.
  - ***Active Directory Sever Name*** is the name of the server that the Active Directory resides on. This server will need to be accessed by the Report Exec Admin in order to verify if the user has an account or not.
  - ***Active Directory Server Base Domain*** is the domain name that the Active Directory users reside in.
  - ***LDAP Domain Controller*** set to local simply means that it is the local domain.

[3] *The purpose of this standard is to provide an unambiguous and well-defined method of representing dates and times, so as to avoid misinterpretation of numeric representations of dates and times, particularly when data is transferred between countries with different conventions for writing numeric dates and times.*

- **Mail Server** – Name or IP address of the mail server that will generate the e-mails generated by Report Exec.
- **Mail User Name** – User name for the program to use when accessing the mail server.
- **Mail Password** – Password for the user that accesses the e-mail server. Once saved, the password will hide itself from view for security.
- **Enable Mail PDF Password** – Reports e-mailed as a .pdf document may be secured with a password.
- **Mail PDF Password** – If "Enable Mail PDF Password" is checked, enter the password to be used for opening reports in this field.
- **Mail From** – The e-mail address that all e-mails generated from the Report Exec Enterprise will be from. Typically, an Information Technology contact is the best option to use here.
- **Mail Port** – The port your network uses for e-mailing.
- **Enable Review Sets** – Enables or disables the Review Level Sets feature.
- **E-mail Reports After Written** – Turns on ability to automatically e-mail reports after a user has clicked **Submit**.
- **E-mail Reports After Review** – Turns on ability to automatically e-mail reports after final approval is given.
- **Enable Property Bar Code Generation** – Automatically generates a number in the "Bar Code Number" field for property.
- **Enable Permit Bar Code Generation** – Automatically generates a Bar Code Number for permits.
- **Email Outlook Meeting For Assigned Tasks** – Users can be sent an Outlook Meeting Invite for their calendar when they are assigned a task through Report Exec if this feature is enabled.
- **Training Notification E-mail** – E-mail address or addresses of those individuals that should receive notifications of training certification expiration. If entering multiple e-mail addresses must use a semi-colon ";" between addresses.
- **Error Notification E-mail** – If an error message is generated by Report Exec Enterprise, an error report can be sent directly to Report Exec Technical Support. This field is always set to support@reportexec.com.
- **Error Notification Email Copy to** – Copies of error reports submitted to Report Exec will be sent to all e-mail addresses entered here.
- **Current Property Bar Code Number** – The last number used in the Bar Code field in property.
- **Current Permit Bar Code Number** – The last number used in the Bar Code field in permits.
- **Enable Single Group Selection** – This setting enables agencies with users that are part of multiple Groups to allow them to login under a single group and have all activities/reports fall under the group logged into. For example, if this setting is not on, and users are part of multiple Groups, then they have to select which Group they are writing a report for.
- **Enable Editing in Submitted Report** – This gives users the ability to reopen one of their reports that was sent for approval to make modifications. If the report has already been reviewed, they cannot make changes.
- **Use Narrative Versions**[4] – Narrative versioning may be enabled or disabled here.
- **Force Password Login on Online Reporting** – Requires a user name and password to create an online report.
- **Force Password Login on Online Permit** – Require a user name and password to create an online permit registration.
- **Force Password Login on Online Visitor Tracking** – Require a user name and password to create an online visitor registration.
- **Hide Start Page on OPR** – If checked, a person accessing the Online Permit Registration will start on the Contacts page
- **Property Gets Case Number** – If checked, Lost and Found Property Reports will get the next available case number instead of its own tracking number.
- **Show Dashboard Unread Bolos for how many days back?** – The number of days a BOLO will remain on the Dashboard if it is unread.
- **Only show unread Bolos on the dashboard –** When enabled, only Bolo Reports that haven't been read will be visible in the Bolo section of the Dashboard.

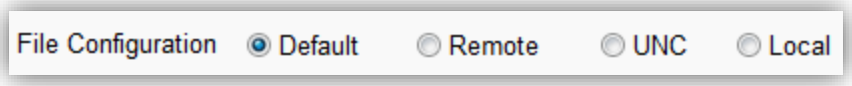
---

[4] ***Narrative Versions*** *are used solely for the purposes of auditing changes made to the narrative section of a report, so that the individuals that have access to make changes are held accountable for those changes that they may make to reports in the system. It is recommended to leave this function enabled and should only be disabled if there is a need for it.*

- **Enable Horizontal Menu on Dashboard –** When enabled, the menu items will be displayed at the top of the screen instead of on the left-hand side.
- **Delete Visitor Image on Check Out? –** In the Visitor Tracking Module you can use a webcam to capture a picture of someone for an identification badge. Keeping the images can speed up the process of checking in visitors, however over time the space used by pictures can add up. If disk space is a concern then the images can be set to delete themselves once the visitor is checked out.
- **Show error details when error occurs in the application –** When enabled, detailed error messages will appear if, and only if, an error occurs. When disabled errors will not provide good details.
- **Maximum Size of Report Email Attachments –** Size of file, in Megabytes (MB), that a file is allowed to be for uploading into reports.
- **Compress Report Email Attachments –** When automatically emailed reports include attachments, this setting dictates whether the attachments are compressed or not.
- **File Configuration** – Digital media in Report Exec Enterprise is typically stored on the application (IIS) server within the 'data' folder but can be configured to save to another location using File Configuration. Digital media can be any file that is attached to a report, from text documents to video files. These files can start to use a lot of space over time, so it is possible to move the directory if space in the default directory is a concern. There are four radio buttons with different options to choose from; Default, Remote, UNC, and Local. The "Test File Configuration" button will tell you if the current settings will work or not.

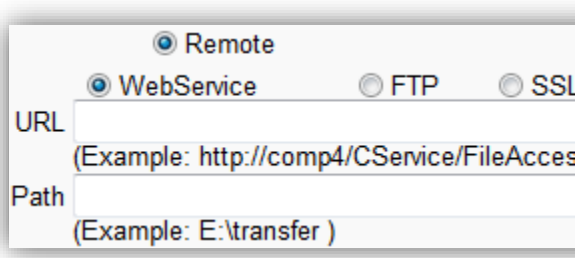
System Settings File Configuration

Default – The default location for digital media is in the **…CESIReportExec\Data** folder on the application (IIS) server.

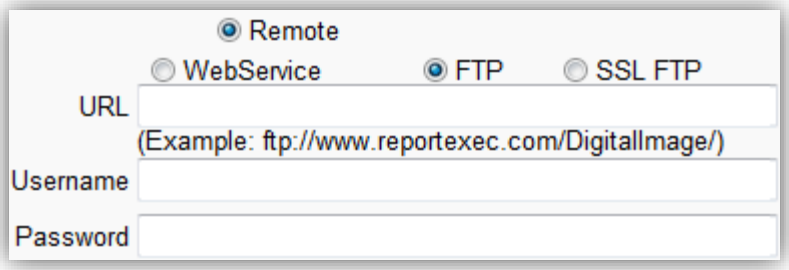


Remote – The digital media can be saved across the internet to a designated location with one of three different options: Web Service, FTP, and SSL FTP.

i. Web Service -

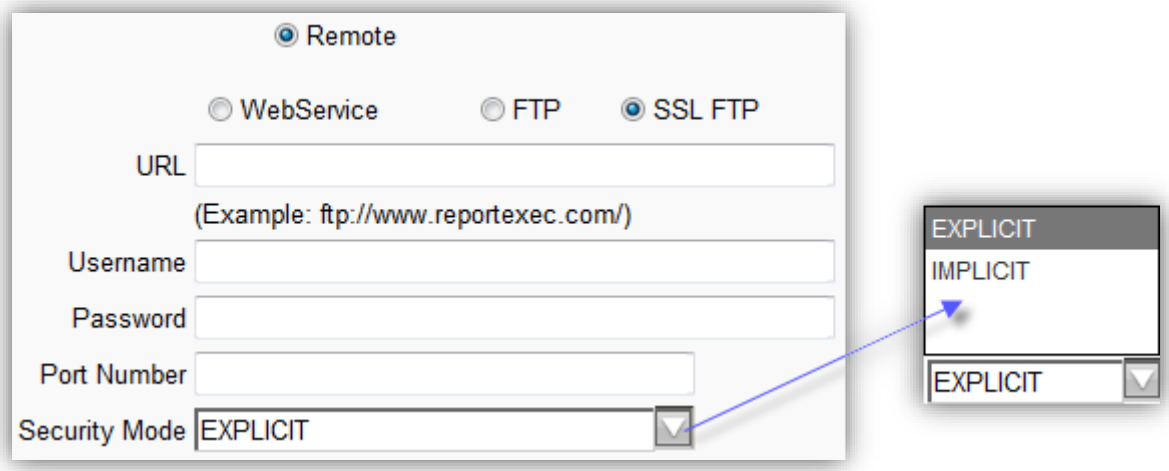


ii. FTP (File Transfer Protocol) – A site for receiving the digital media files that are attached to reports, passed through File Transfer Protocol, must be created by your organization's I.T. Department. Once this is done, the credentials for that site are

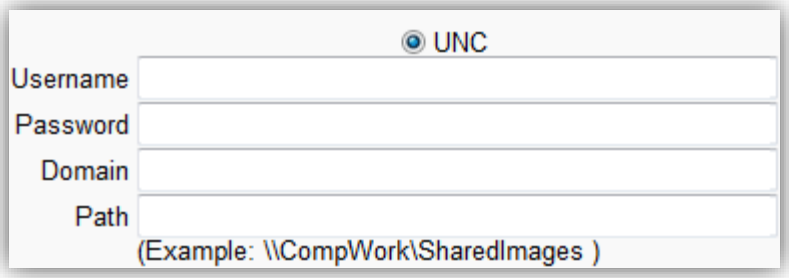


entered into this menu. Click **Test File Configuration** when ready to verify if the settings are correct. File Transfer Protocol is inherently slow so it is recommended not to use this configuration unless certain it is absolutely necessary.

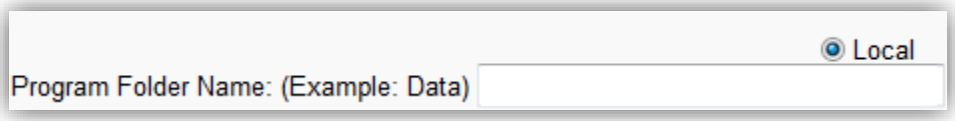
iii. SSL FTP (Secure Socket Layer File Transfer Protocol) – SSLFTP is a more secure way to use the File Transfer Protocol. As with normal FTP, a site must be created by your I.T. for receiving the digital media across the internet. Enter in the proper credentials into this menu when the site is created and click **Test File Configuration** to verify the settings. FTP is an inherently slow protocol and should only be used if necessary.



UNC – A directory on the network can be designated as a dump spot for the digital media with a UNC path provided the proper credentials for that directory are supplied in this menu. Click **Test File Configuration** to verify if your settings are correct.



Local – Digital media can be saved to a directory on the application (IIS) server that is different than the default directory.



Tree View Dictionaries

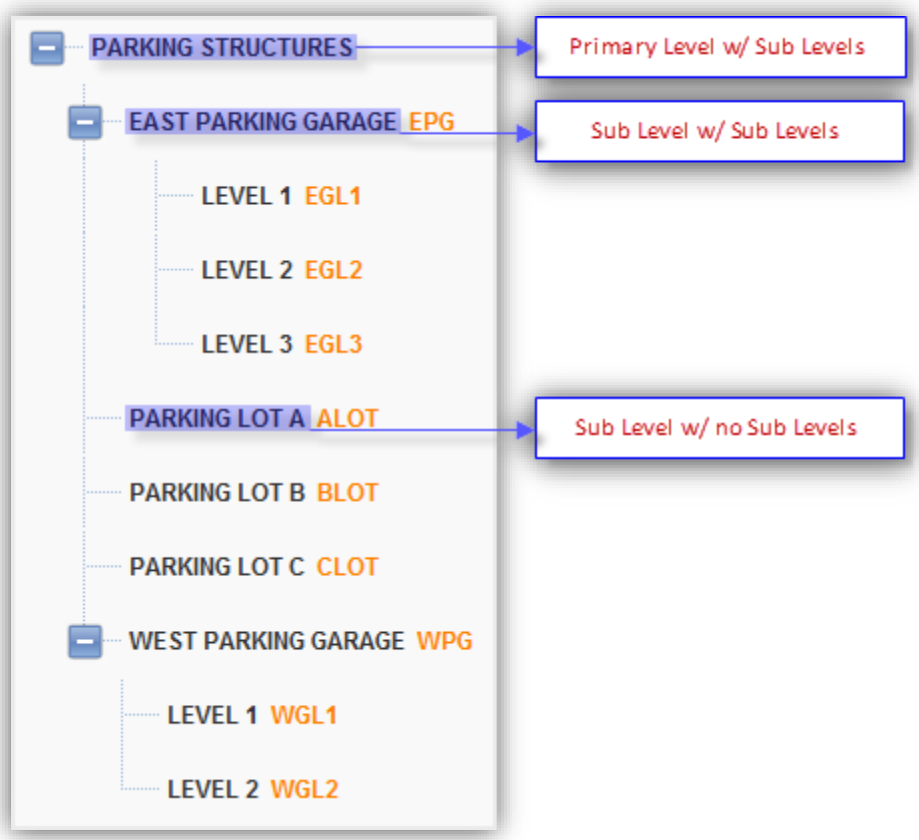
A hierarchical table is used to organize the five Tree View Dictionaries in Report Exec Enterprise. Dictionary items with a "+" next to them indicate there are sub-levels for that item, while items with no symbol have no sub-levels below them. The following table briefly describes each dictionary.

Tree View Dictionaries

Dictionary	Description
Agency	Used to define outside agencies/departments that the organization may need to add to reports using the External Agency sub-module.
Force	Denotes the level or type of force that an officer used in an incident for the Officer's Force sub-module of a Case Report.
Incident	Used only for Case Reports.
Location	Used throughout the program to define locations, including the Dispatch program.
Violation	Used in the Citation and Arrest/Booking Modules.

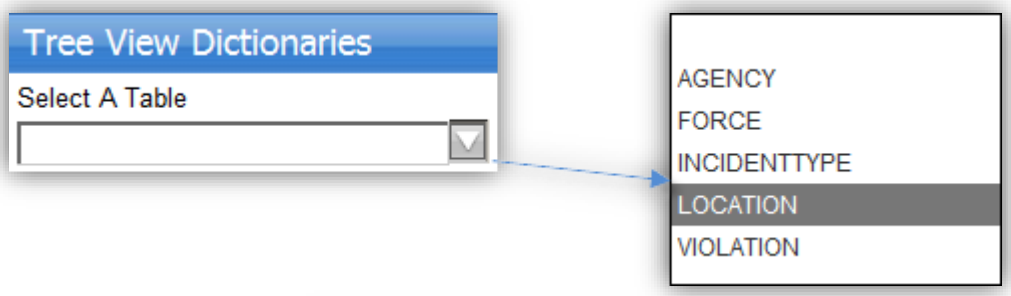
The Tree View Dictionaries in Report Exec will likely be different for each organization depending on any number of different variables that differ between agencies. The dictionaries are setup with Primary Levels and Sub Levels that will further breakdown a Primary Level.

Primary Levels are the broadest level of a dictionary and Sub Levels are the more specific levels within the tree view. Not only will primary levels have sub levels, but within a sub level could be numerous other sub levels. Below is a +sample of what a location dictionary may look like for the user setting up the tree.



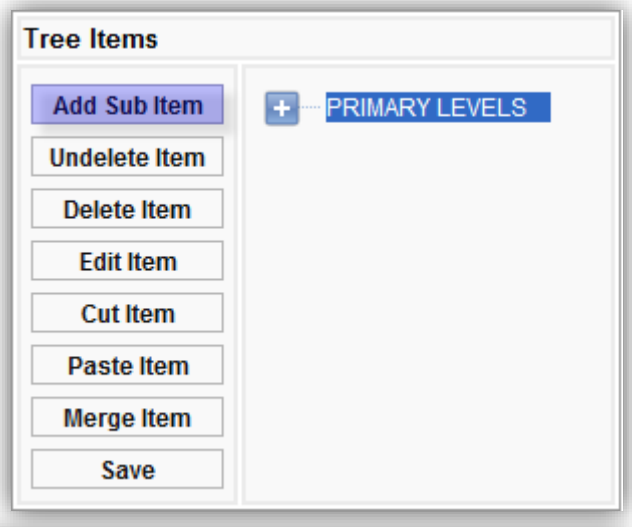
Setting up the Tree View Dictionaries

1. Select the dictionary to configure. The **Location** dictionary is used for this example.

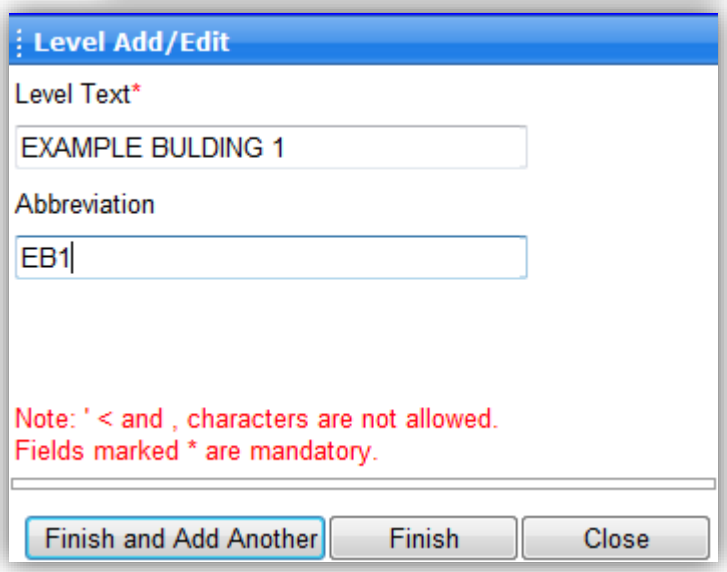


2. Select the highest level of the tree to work on. This example is working on the **Primary Levels**[5] of the tree.

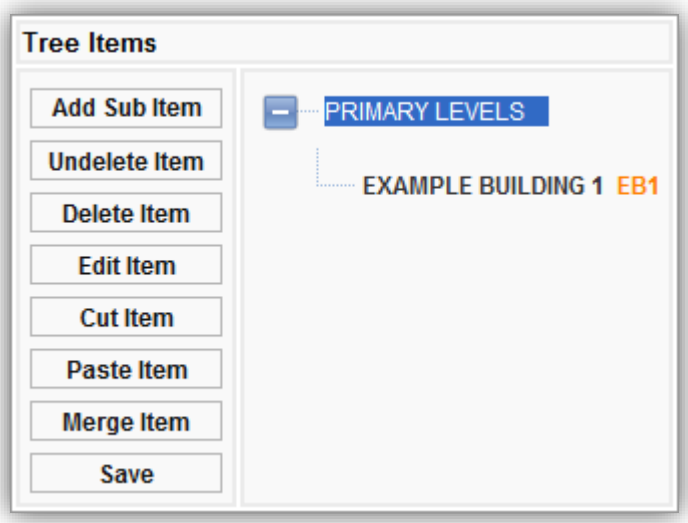
3. To add a Primary Level, select the **Primary Level** wording and click **Add Sub Item**.



4. In the **Level Text** field, enter the new item. In the **Abbreviation** field, a quick code can be entered that will make more common locations easier to add to reports. If you have additional items to enter that are on the same level you are currently working in, click **Finish and Add Another**, otherwise just click **Finish**.



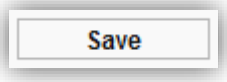
[5] *In the **Select Primary Level** drop down menu, only primary levels that have sub levels added to them will appear in the list. If the item that is being looked for is not being found, select **Primary Levels** from the dropdown.*



5. Here, the example adds "Example Building 1" to the Primary Levels for the location tree.

6. To continue adding sub levels, select the tree item to put the sub level under and click **Add Sub Item**.

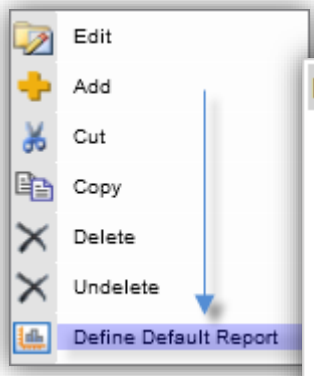
7. Click **Save** when done to apply the changes (the system will automatically prompt to save after 10 minutes).

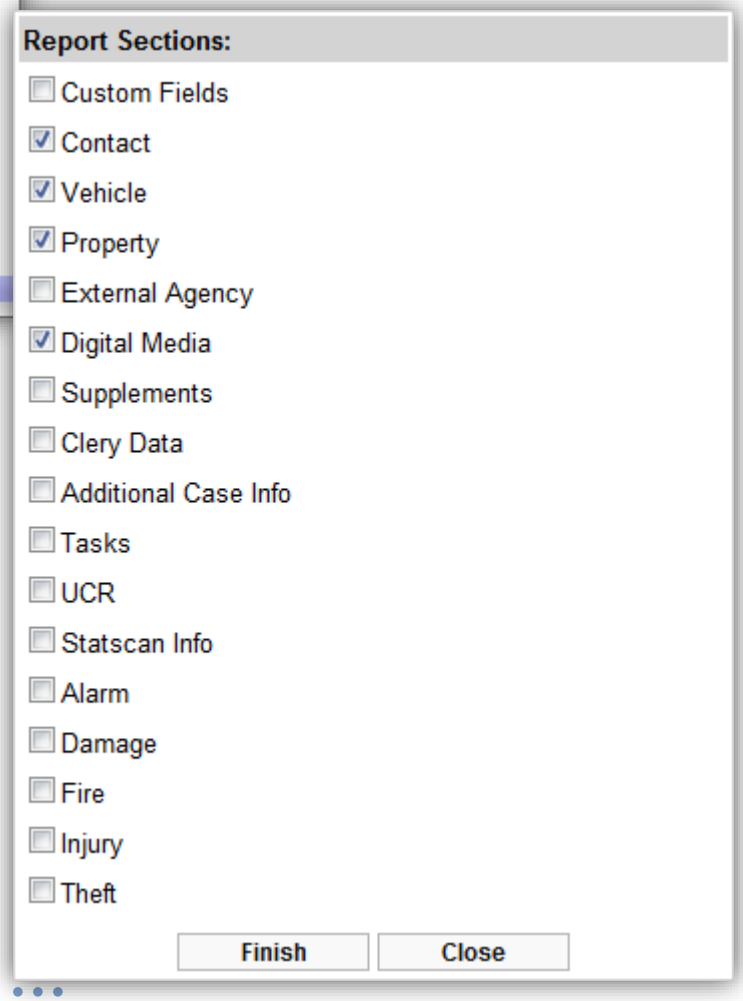


Special notes on dictionaries

Incident Type Dictionary

The additional sub-modules of reports can be set to be active by default for specific Incident Types. A report for a "Door Unlock" will likely require less information that a report for "Murder." When an Incident Type is selected in a report, the program will then turn on the sub-modules that are enabled here in the Tree View Dictionary setup.

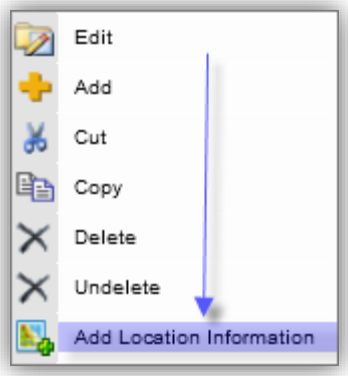




Default reports may be assigned when adding new Incident Types simply by clicking **Define Default Reports** in the **Level Add/Edit** window. If changes need to be made to an Incident Type that already exists, right-click the Incident Type and then select **Define Default Report**. The window pictured below is where the default sections of a report for a specific Incident Type are enabled. Click **Finish** when done to apply the changes.

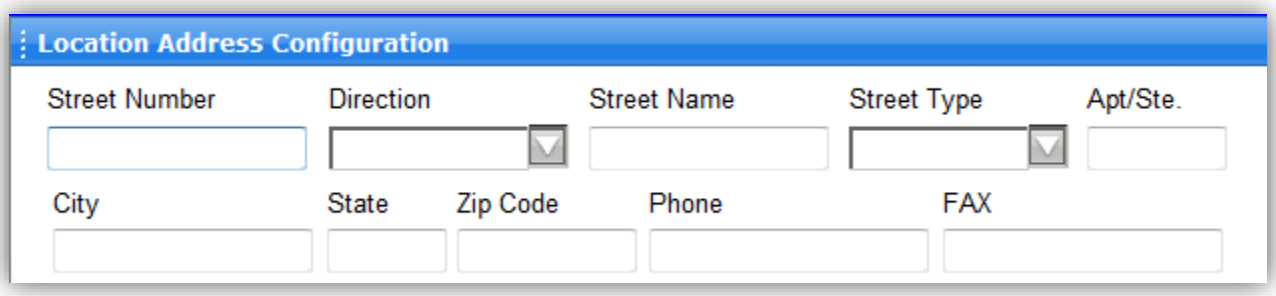
Location Dictionary

The Location Dictionary has additional configuration options available for each location if it is necessary. Each location entered into Report Exec Enterprise can have specific information assigned to it for tracking purposes, including address and phone number. The address information can be used to auto-populate the address fields within reports and Dispatch calls, if the location configuration has been entered. Digital Media for floor plans, Emergency Contact information, and Hazardous Materials related to that location can be uploaded for use by Dispatchers in the Report Exec Enterprise Dispatch program and calls Dispatched for this location can also be set to be automatically e-mailed to people that need to be notified of activity for the location.

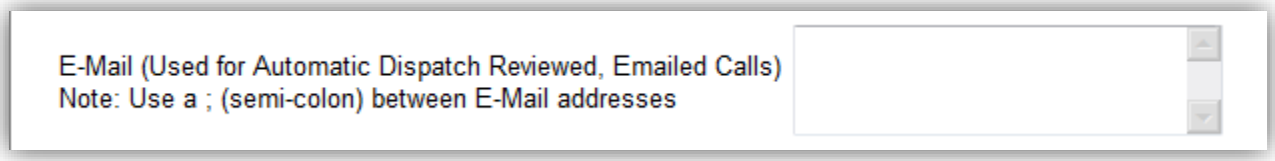


1. Right click on a location and select **Add Location Information**.

2. Enter the address information for the location. Address information is available in Dispatch when clicking the L button within a call and will also auto fill the "Specific Location" field, if Specific Location is set in the 5-field address, law enforcement format [6]as seen in the picture below.



3. If certain people need to be notified by e-mail when a Dispatch call is reviewed you can designate those people's e-mail addresses here. In order for this to work, Dispatch Review needs to be enabled and the call must be marked as "Reviewed" by a Group Dispatch Supervisor. When a call from this location is marked as reviewed, all individuals in the listing will receive a notification. Multiple e-mail addresses must be separated with a semi-colon (;).



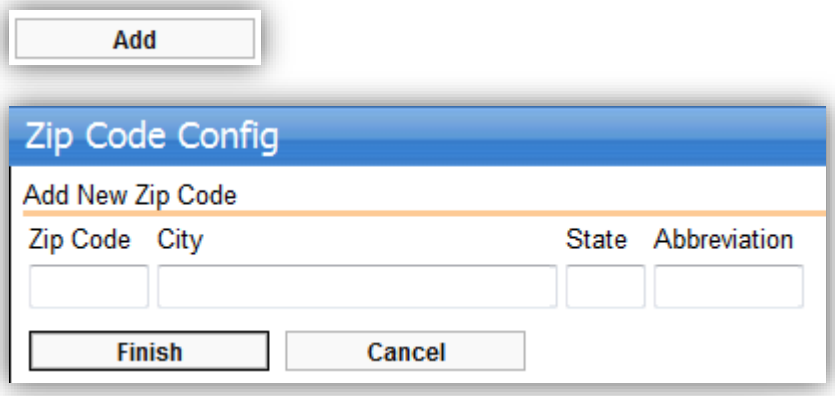
[6] *Addresses can be set to be one large field, or five individual fields each individually pertaining to Street Name, Direction, etc.*

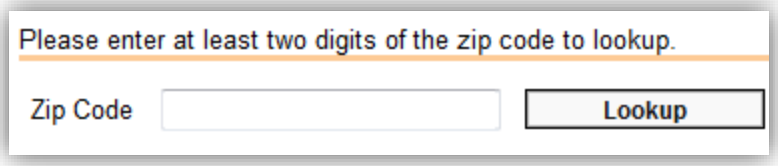
4. Click **Add/Edit Media** under the corresponding section to add or edit the Floor Plans, Emergency Contact Information, and Hazardous Materials Information. Any pertinent documentation can be uploaded to be used with the Dispatch program when Dispatching calls to this location. The [L] button within a Dispatch call will give Dispatchers access to this information[7].

Zip Code Setup

A pre-defined list of Zip Codes for the United States, included City and State, is included in the program by default. When a Zip/Postal Code is typed into the contact information screen on the user side of the program, it will automatically populate the city and state if that information has been entered into the Zip Code Setup. Zip or Postal Codes can be added here by clicking **Add** and then typing in the pertinent information.

Zip/Postal Codes can be searched by typing in at least the first 2 digits of the code to bring back a list of results. If any of the city/state information needs to be altered, click **Edit**.





[7] *This feature is a forthcoming addition to the Report Exec Enterprise software to allow viewing of the Digital Media that was added to Location Address Configuration. For now it is only viewable in the Admin program.*

User Setup

Create New User

For someone to be able to access the system they must have a user account created for them and that account must be assigned to a Group and given a Role permission that designates the access they have. The **Role** defines what permissions that user will have within the Group they have been assigned. All users in Report Exec are created and edited through the User Setup section. Adding and editing users must be done by an Administrator or by someone who has been given either **Group Setup Access** or **Add/Edit User Access Only** for their user account. A user that has **Give System Wide Settings Access** will not need the additional permission to add/edit users. With the system wide access a user will have full permission to access all sections of the Admin program.

User Information Tab

1. To create a user a First Name, Last Name, User Name, and Password must be specified. All four fields are required for any user account in the program. The **Username** is what will be used as the login ID and the password can be set to change upon the next logon by the user when they log in. The user can also manually change their password later from the user side of the program in the "My Information" tab. The **ReportName / AKA** field is for controlling what the user's name prints out as on a printed report.

2. The next several fields are not required information but can be filled in as desired and used for employee tracking purposes. It is good to have an e-mail address entered if one is available. This will give Report Exec Technical Support a direct means of communication to a user when errors are reported. An e-mail address is also needed if using the "E-mail Notifications" Role Permission for assigning tasks, reports, and/or investigations as-well-as the "Assign Outlook Meeting on Assigned Task" feature. Finally, the **Lock Out Expiration** is designed to allow users of the system to be locked out until the specified date. Organizations that rotate shifts every few months will find this feature useful.

3. Each of the following checkboxes pictured below will be explained in detail below:

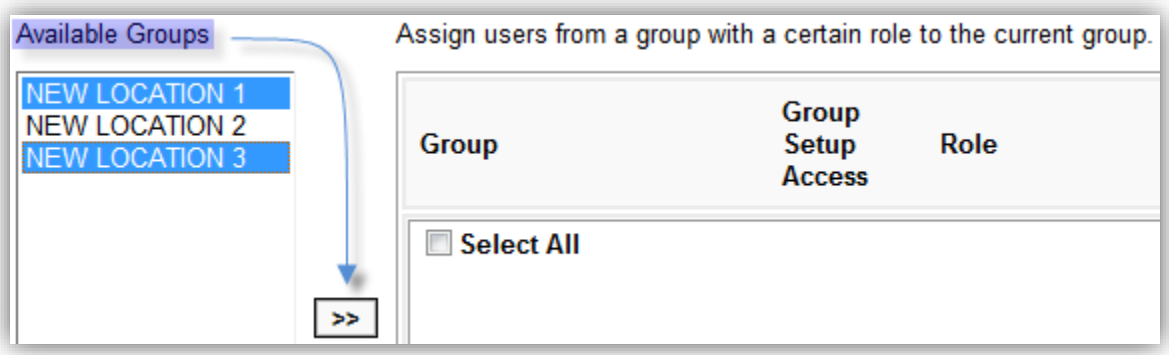
   - **Admin - System Wide Settings Access** – Provides full access to the administrative program.
   - **Admin - Add/Edit User Access Only** – Allows a user to log into the administrative program for the sole purpose of configuring new and existing user accounts.
   - **User - Confidential Report Access** – Allows the user to search for and open reports marked as *Confidential*.
   - **User - Enable Group Search Only** – Only allows viewing of report histories tied to contacts and vehicles that have been entered in the current Group(s) the user belong(s) to.
   - **Deactivate User** – Removes the user name from dropdown menus that show users.

- **Lock Out User** – Prevents the user from being able to log into the program. This will automatically turn on if "Password Attempts" are enabled in System Settings and a user enters their password in incorrectly enough times to trigger a lockout. This also ties to the "Lock Out Expiration" date field on the Add User screen. If an expiration date is entered for a locked out user, the user will automatically be unlocked when the expiration date has been reached.
- **User - Hide Release Version Update Notification** – Stops a user from being notified when updates are available.

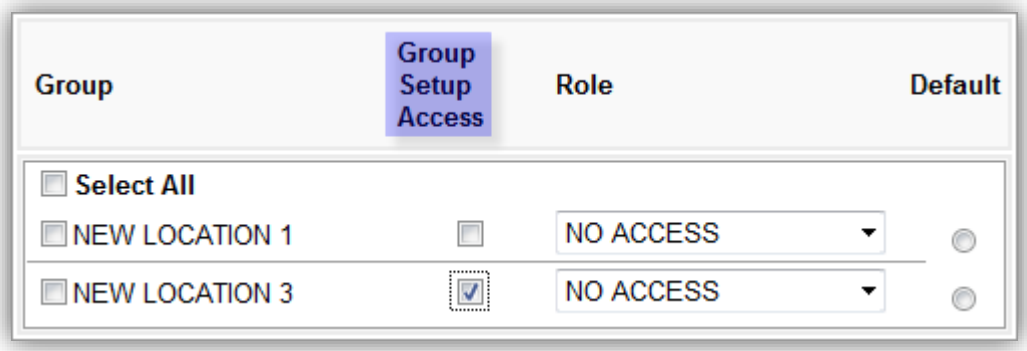
4. Once the User Information tab is completed, click the "Assign Groups and Roles" tab to provide the user access to the program. A Group will need to be created in the Group Setup section before access to the system will be able to be granted.

Assign Groups and Roles tab

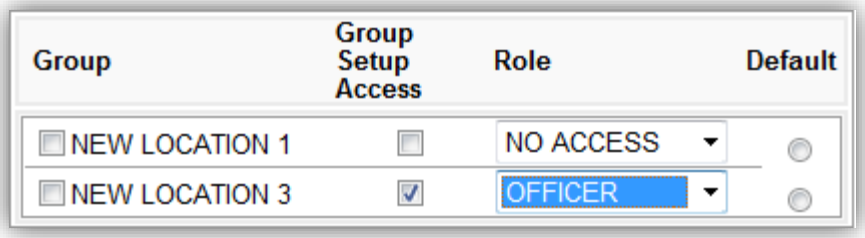
1. From the **Available Groups** list, select the Group(s) the user needs to belong to and click the >> button. Multiple groups can be selected by holding down the **CTRL** key while selecting.



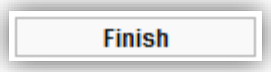
2. A user can be given administrative access to the Group with the **Group Setup Access** checkbox. Group Setup Access allows a user access to **Group Setup** within the Admin program. This access can be granted without providing a user with the Administrator Role which will prevent them from having more power than is needed to affect settings in the system.



3. Click on the drop down menu next to a Group the user has been assigned to and select a Role. A user can have a different Role in each Group they are in. For example, a Supervisor of one location within the company may only be allowed the access of a normal employee at any other physical location he goes to that uses Report Exec Enterprise. The user in the example has been given the Officer Role, but has access to make changes to Group Setup for the "New Location 3" Group but still has no access to "New Location 1."



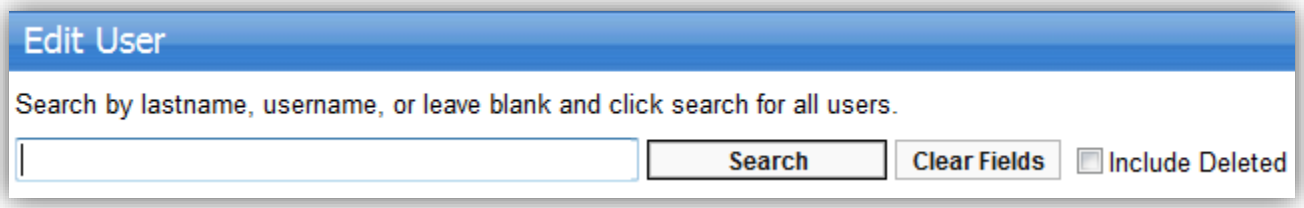
4. Click **Finish** at the bottom of the page when done to save all additions/changes made. Leaving the Add User section before clicking **Finish** will not allow the changes to be applied.



Edit Existing User

User accounts can be edited at any time by a user given the access to do so. Permission to edit a user's information is granted to the Administrator Role by default but can also be given to individual users with the **Admin – Add/Edit User Access Only** checkbox that is located within a user's account settings.

1. If a specific user is the desired, enter in a last name or user name if it is known. A general search can be done by leaving the field blank and clicking **Search**. Deleted users may also be searched for in this manner if the checkbox to **Include Deleted** is checked.



2. A list of user accounts will come back that match the specified search criteria. Leaving the field blank and pressing **Search** brings back a list of all the users currently entered into the system.

3. Selecting a user will bring you into the account information page where you can edit the **User Information** and **Assign Groups and Roles** tabs. **See section: Create New User**.

Permissions Report by User

The Permissions Report by User is a quick way to get a printout of all users of the program to find out what permissions they have in each Group they have access to. Simply click the link for the Permissions Report and it will generate itself in a separate window. The example below shows the user Officer Tutorial's access within the "New Location 1" Group.

OFFICER, TUTORIAL

Group Name	User	Module	Reader	Writer	Printer
NEW LOCATION 1	OFFICER, TUTORIAL	ActivityTracking	True	True	True
NEW LOCATION 1	OFFICER, TUTORIAL	Bolo	True	True	True
NEW LOCATION 1	OFFICER, TUTORIAL	Citation	True	True	True
NEW LOCATION 1	OFFICER, TUTORIAL	Dispatch	False	False	False
NEW LOCATION 1	OFFICER, TUTORIAL	KeyTracking	False	False	False
NEW LOCATION 1	OFFICER, TUTORIAL	Property	False	False	False
NEW LOCATION 1	OFFICER, TUTORIAL	Training	False	False	False
NEW LOCATION 1	OFFICER, TUTORIAL	Trespass	True	True	True
NEW LOCATION 1	OFFICER, TUTORIAL	VisitorCheckIn	True	True	True
NEW LOCATION 1	OFFICER, TUTORIAL	Reporting	True	True	True
NEW LOCATION 1	OFFICER, TUTORIAL	Clery	False	False	False
NEW LOCATION 1	OFFICER, TUTORIAL	KeyTracking	True	True	True
NEW LOCATION 1	OFFICER, TUTORIAL	ProfilingIncludeInSupplement	True	True	True

Roles Report by User

The Roles Report by User is a quick way to get a printout of all users of the program that shows the Groups they belong to and the Role within each Group they have been assigned. In the example below, Tutorial Officer has been assigned to two Groups. He/she has the Officer Role in the "New Location 1" Group but has not been assigned access to the "New Location 2" Group.

OFFICER, TUTORIAL (to1)

Group Name	User	Role
NEW LOCATION 1	OFFICER, TUTORIAL (to1)	OFFICER
NEW LOCATION 2	OFFICER, TUTORIAL (to1)	NO ACCESS

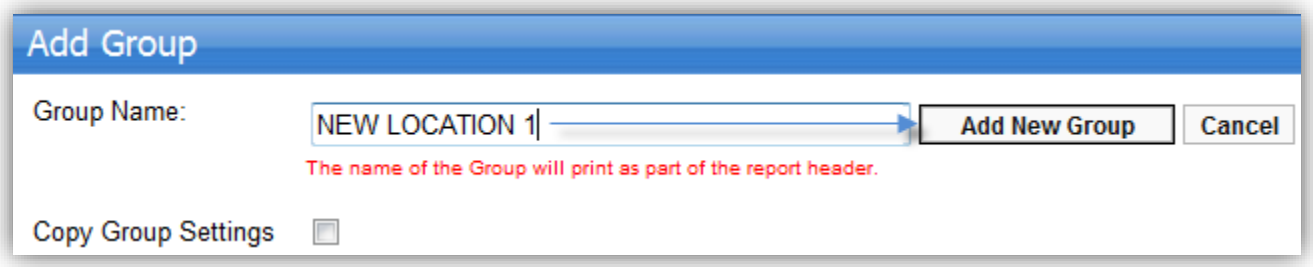
Total Roles for (OFFICER, TUTORIAL (to1)): 2

Group Setup

Add Group

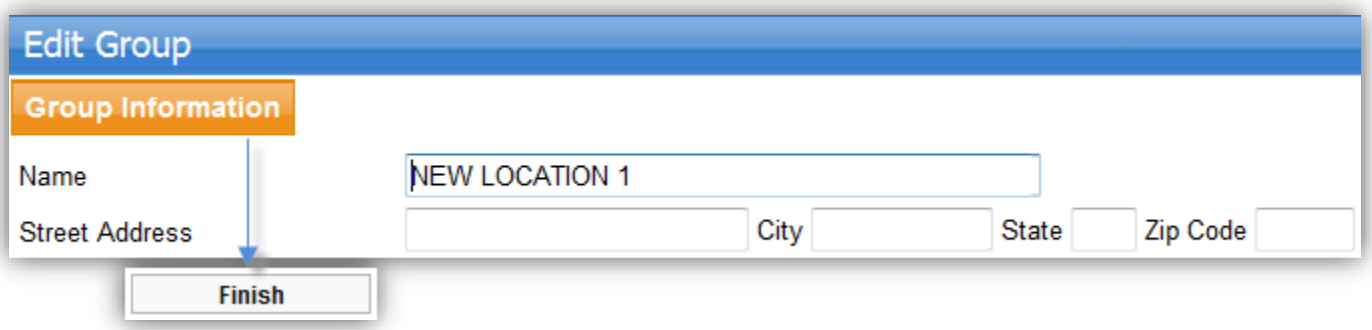
Groups are used as a separation of workflow within the organization. Sometimes this is done by site location and sometimes the workflow is separated by department, or both. At times it may be necessary for one, or multiple Groups within the organization to have settings that differ from those defined in the System Wide Setup section of Report Exec Admin program.

Quite often the Groups in Report Exec Enterprise are used to divide different physical locations, or workgroups, of the greater Enterprise. For example, a Group in Dallas, Texas is likely going to need a few different settings than a Group in Ontario, Canada, or an East Campus Group may have settings that differ from a West Campus Group, etc. Changes in Group Setup can only be made by a user with System Wide Settings Access or they must have Group Setup Access checked on their user account for the Group they need to edit. System Wide Settings Access and Group Setup Access are explained in the previous section on User Setup.



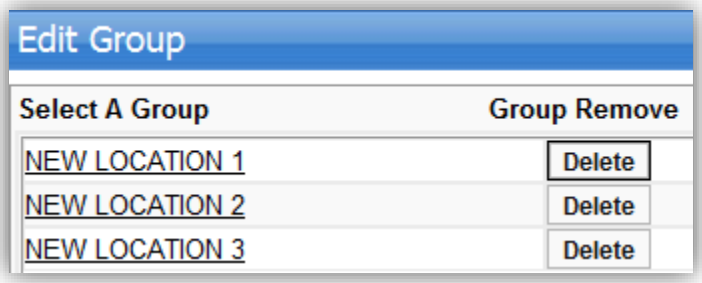
In order for a user to be able to access the program, they must be added to a Group and given a Role within that Group. As stated in previous sections, the Role defines the access level a user has within a Group and the users can be given a different Role for each Group he/she is assigned to, if necessary. Some of the settings that can be changed for different Groups are: report numbering systems, Group logos, review levels, and various options in System Settings.

Enter in a Group Name and click **Add New Group**. The Group Name will display at the top of reports as part of the header. Once you click **Add New Group** you will be taken to the "Edit Group" section, "Group Information" tab. Be sure to click **Finish** at the bottom of the page to apply all changes made to the Group. To finish configuring a new Group, follow the steps in the proceeding section that describes the Edit Group area.



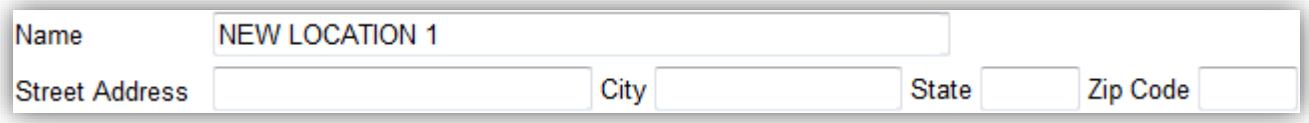
Edit Group

When creating a Group within Report Exec Enterprise, you will automatically be redirected to "Edit Group" within the Admin program. Once a Group is created and successfully saved to the program, future changes can then be made by going to the Edit Group section. When the **Edit Group** link is clicked you are provided with a list of all Groups in the system that you have permission to edit. Once a Group is selected, you are then redirected to the "Group Information" tab.

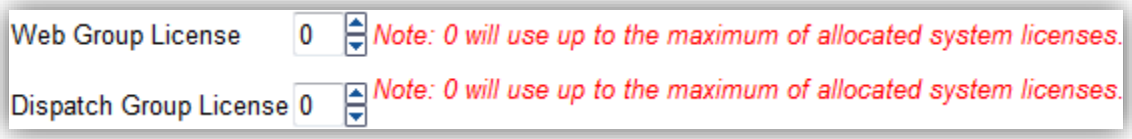


Group Information Tab

1. The name of the Group is the only piece of the Group Information tab that is required in order to create a new Group. All settings beyond the name field in this tab are purely optional. If address information for the Group is entered here, it will print in the header of a report.

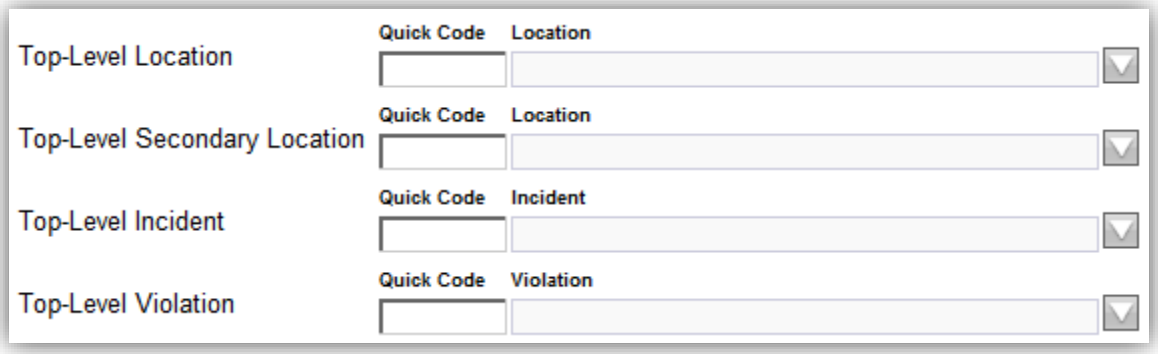


2. The Group Licenses only need to be defined in instances where multiple agencies have collaborated on a purchase of the software and each has purchased a specified number of licenses for use. Otherwise, the Group Licenses should be left at 0 to allow the maximum to be allocated.



3. Select the Bar Code Type used by the Group, if needed. 3 of 9 is a longer bar code that 2 of 5.

4. Top-Level Locations are used in situation where an Organization has multiple sites, or divisions, that each use a different tree dictionary than that the others. The organization can 'lock' a Group in a specific part of the tree by defining where their top level starts at. This is a not required setup and will only need to be enabled if deemed necessary.

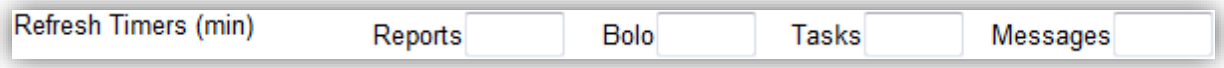


5. Enter a description for the Group if necessary.

6. In the Visitor Tracking Module when creating a badge ID for users, the program can either automatically number the temporary badges that are created, or the user can enter in the number manually when checking in the visitor.

7. File Configuration is discussed in the System Wide Setup, System Settings section. Digital Media attached to reports can be saved in a different directory on the server than the default. **See section: System Wide Setup > System Settings**.

8. The Refresh Timers define how frequently the sections of the Dashboard refresh by default. If the Group needs the refresh timers to be different than the setting in System Wide Setup, System Settings, those changes are applied here.



9. OLR and OPR Group Messages are displayed on the final page after an Online Report or Online Permit has been submitted. The message is typically used to convey additional steps to the user that submitted the report. For example, "PLEASE WAIT 24 HOURS FOR YOUR REPORT TO BE PROCESSED." The message can be anything deemed necessary including company procedures for what to do next after submitting such a report or permit.

Modules Tab

Group Access to the various modules in Report Exec Enterprise is assigned by checking the checkbox next to the corresponding module that needs to be accessed by the Group. A user's individual Role will then ultimately decide if that particular user has access to the module or not. Certain modules have an additional checkbox for **Include in Supplement** which will allow that report type to be added as a supplemental report to another report if it is necessary.

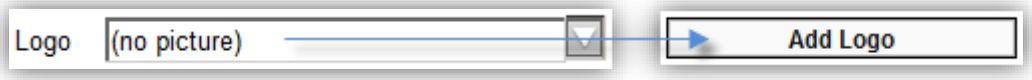
Module	Description
Event Shift Log	Track the daily events of officers with a daily log generated by the officer and the program.
BOLO	Post and receive "Be on the lookout" alerts to users' dashboards.
Citations	Track the status of citations issued by officers.
Clery Report	Used by colleges and universities in compliance with The Jeanne Clery Act.
Dispatch	Track officer and call activity in real time and create reports for officers' dashboards.
Emergency Response	Define departmental procedures for managing responses to emergencies.
Investigation	Special module used to manage and track investigations.
Key Tracking	Track the use of company equipment and run reports on the usage of the equipment.
Online Citation Payments	Integration that allows for Citations to be paid via Credit Card online.
Online Reporting	Enable a website for people outside Report Exec to submit reports for review by an officer.
Online Reporting Search	Allow people that submit online reports to search for those reports.
Online Permit Registation	Enable a website for people outside Report Exec to submit their permit requests.
Online Visitor Registration	Enable a website for visitors to pre-register their information for a visitor badge.
Parking Permit	Track any type of permit information.
Profiling	A report that supplements the citation reporting, used for tracking traffic stop profiling.
Property	Track any type of property entered into the system.
Reports	Enables report-writing.
Risk Management	Enables the Risk Management Module.
Scheduling	Post, manage, and track shifts, day off requests, over time, etc.
Traffic Stop	A real-time traffic stop tracking, including integration with a dashboard camera.
Training	Track officer training and certifications and set notifications for training renewals.
Trespass	Special report for tracking trespass information.
Visitor Tracking	Track visitors and print visitor badges.
Work Place Violence	Special report for tracking violence in the workplace.

Report Setup Tab

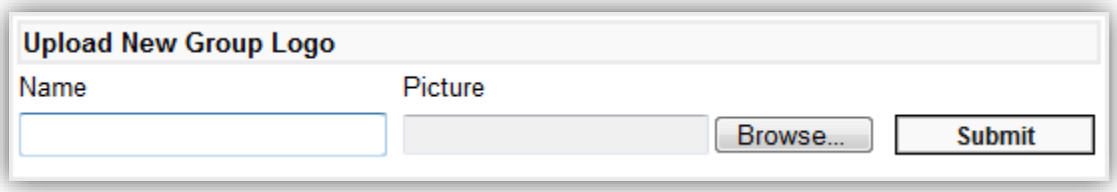
The Report Setup tab is another optional, however useful, setup tool in the Edit Group section. Each Group can be given its own logo for their printed reports and a custom numbering system for each report type in the system if necessary. A writable Portable Document Format (.pdf) file can also be associated with the Group that will attach itself to the narratives of Case Reports.

Printed Report Logo

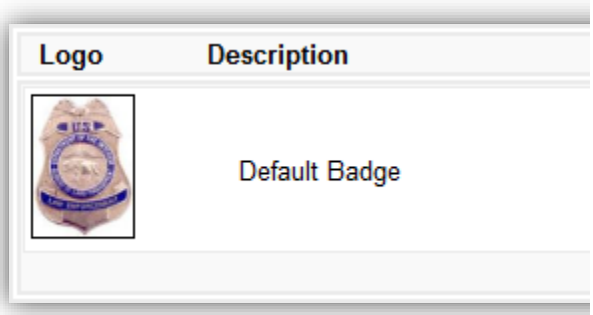
1. Click **Add Logo** and you are given a window that allows you to browse to a picture on your computer.



2. Click **Browse…** and select a picture from your computer to upload. The file size of the picture must be less than 800kb and its dimensions cannot exceed 1000 x 1000 pixels. Once the file is selected it can be titled with the **Name** field before clicking **Submit**.



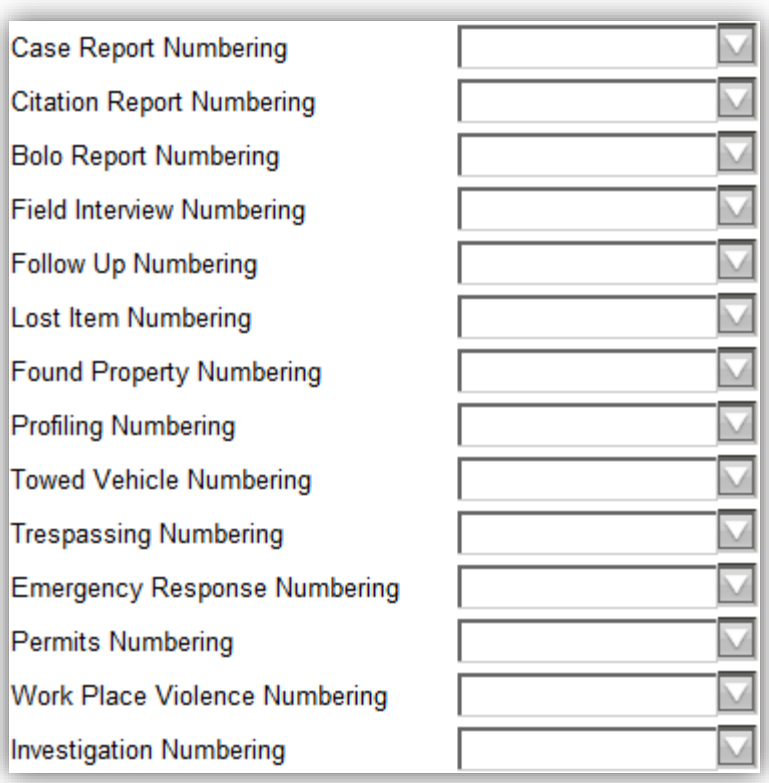
3. To edit the name of an existing logo, click edit and make the corresponding changes. To delete, simply click **Delete** and it will be removed instantly.



4. Select the desired logo from the **Logo** dropdown menu on the main section of the **Report Setup** tab.

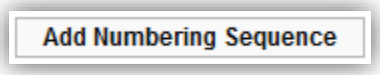
Custom Report Numbering Systems

Report Exec Enterprise, by default, generates a 6 digit reference number for reports in the system. This number can be edited by the report writer if necessary. Agencies that require their own numbering sequence for certain report types have been given the ability to customize those numbering formats for each Group in the system.



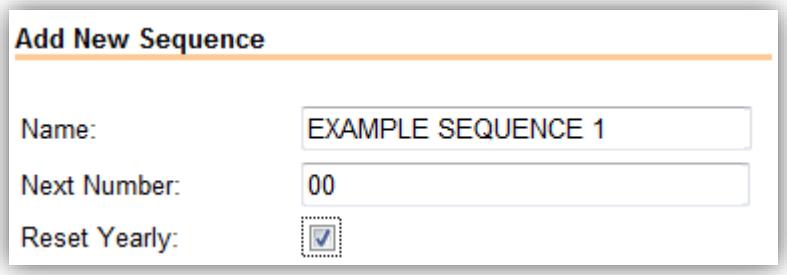
Create Numbering Sequence:

1. Click **Add Numbering Sequence** next to the corresponding report type that needs custom numbering.

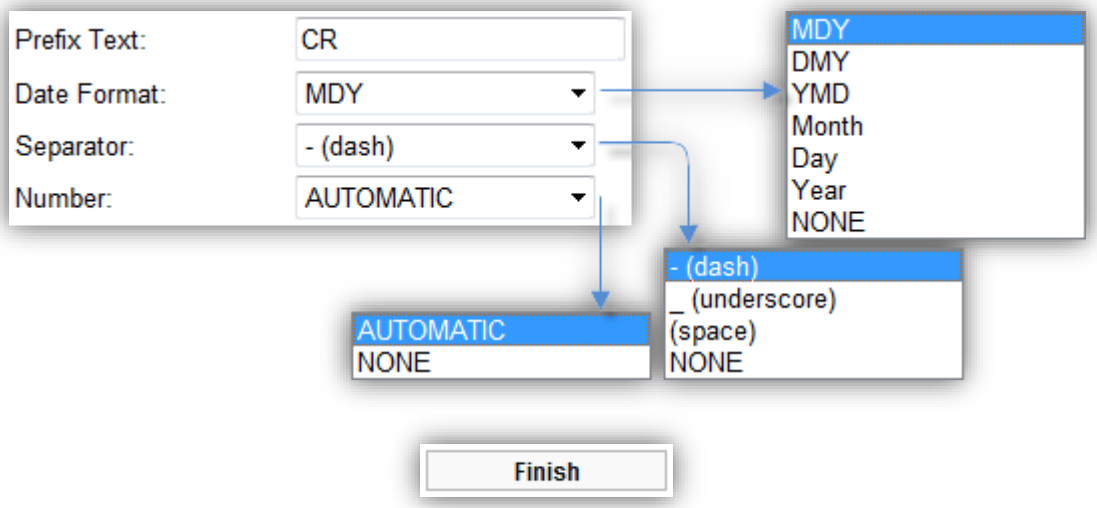


2. Click **Add New Item** in the bottom right of the window.

3. Give the new sequence a name. The sequence can be reused for other Groups, or for other report types if desired. The **Next Number** field can be adjusted to reflect what number the next report created needs to be at. The example sequence below will start at "00." The sequence can also be set to reset at the New Year with the **Reset Yearly** checkbox.

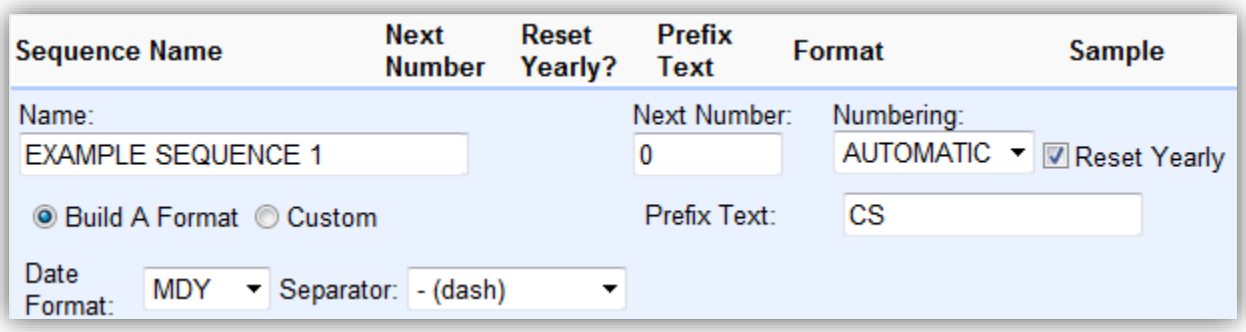


4. The prefix text will be at the beginning of the report number, the date format will follow the prefix, followed by a separator, and then the number itself. In this example, "00" will be the first number used and will be assigned automatically. Instead of letting the system assign the **Number** portion of the sequence, **None** can be selected to assign the report number manually. The program will then only assign the prefix numbering sequence and allow the officer to manually assign the actual number of the report. Click **Finish** to add the numbering sequence to the system.

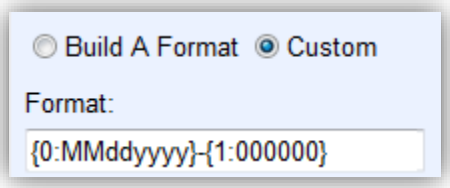


Sequence Name	Next Number	Reset Yearly?	Prefix Text	Format	Sample	Actions
EXAMPLE SEQUENCE 1	0	yes	CS	MDY-AUTOMATIC	02152012-000000	Edit

5. The sequence can be further customized or edited by clicking **Edit** next to the corresponding sequence.



6. Select the **Custom** radio button to edit the date format string for the sequence if necessary. Format Strings should only be edited by an Administrator that possesses a knowledge of how to do so. Microsoft has documentation on standard and custom date strings on their website.
   - Standard Date and Time Format Strings - http://msdn.microsoft.com/en-us/library/az4se3k1.aspx
   - Custom Date and Time Format Strings - http://msdn.microsoft.com/en-us/library/8kb3ddd4.aspx



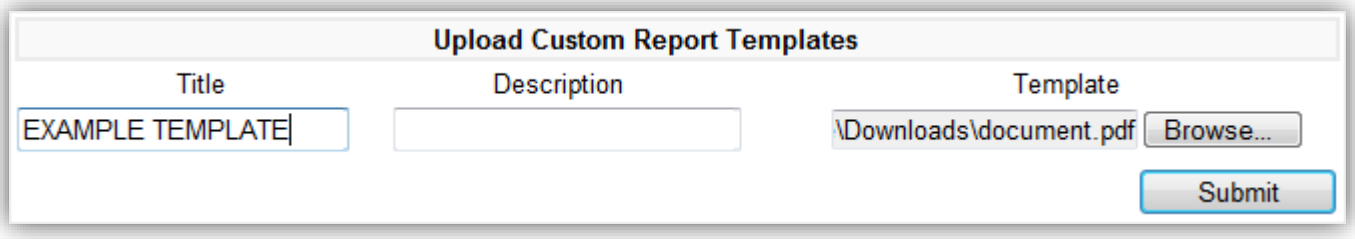
7. Click the drop down next to the report type to define the numbering for, and select the desired numbering sequence.

Attach Custom Report Template to Narrative Page

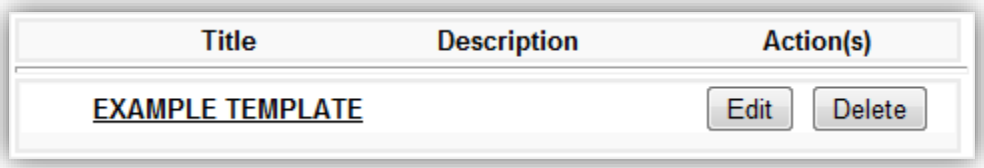
A Custom Report Template can be added if it is in a writable Portable Document File (.pdf) format and can be attached as a digital media item for the Group to have access to. While on the narrative entry page on the user side then can download the template, fill in the information required by the organization, then attach the finished document as Digital Media to the report. The custom template does not create a template for the Narrative in Report Exec, but instead gives an additional writable document for organizations that may require additional procedures to be carried out. The following steps will demonstrate adding a Narrative Template for a Group.

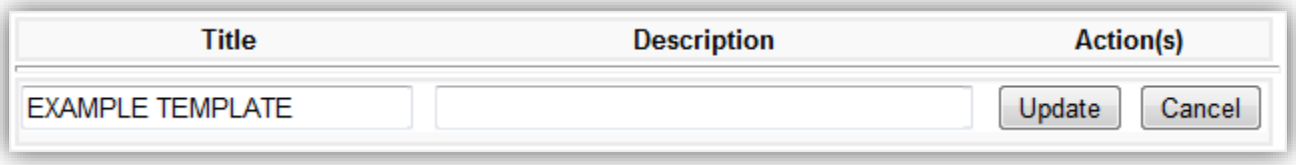
1. Click **Add Custom Template**.

2. Click **Browse…** and select the writable Portable Document File (.pdf) from the directory where it is saved on your computer. Name the template in the "Title" field and enter a description if needed. Click **Submit** when ready to attach the document.



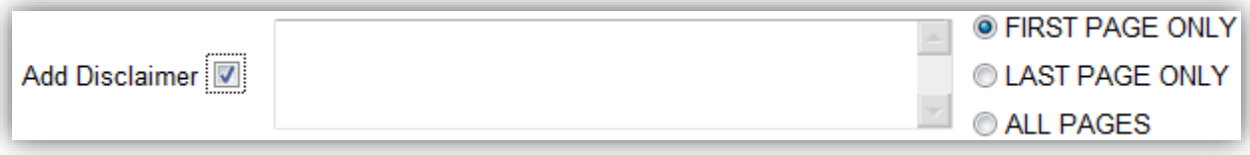
3. Once the document is attached it is ready to be used by the users writing their narratives on the report writing side. If the title or description ever needs to be changed, click **Edit**. Once the changes are made, click **Update**.



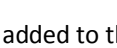


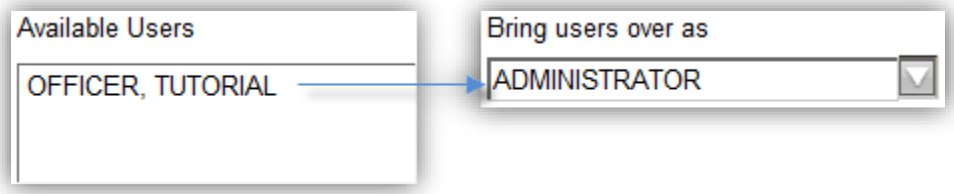
Printed Report Disclaimer

A paragraph can be added to the bottom of reports that are printed from Report Exec Enterprise. Three disclaimer print options are provided. It can print off on the bottom of the first page of the report, the last page of the report, or at the bottom of all pages of the report. The disclaimer was designed for a custom confidentiality notice but can be used to fit the needs of the organization. Each Group in the system can have its own separate disclaimer on reports, if needed.

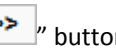


Assign Users Tab

Users available to be added to the Group will appear in a list on the left side of the screen of the Assign Users tab. To include a user in the Group, select a Role from the **Bring users over as** dropdown, then select the user(s) from the **Available Users** list and click the "  " button to bring them over into the Group. Multiple user names can be selected by using the **CTRL** key on the keyboard.



Assigning users to a Group:

1. Select what role the user(s) should get from the **Bring users over as** drop down.
2. Click on the user from the **Available Users** list to assign to the group. Multiple users being assigned to a group with the same role by using the **CTRL** key on the keyboard when highlighting their names.
3. Click the "  " button to move the users into the Assigned Users list. The role selected in the step 1 will be located next to each individual user and can be changed to another Role later if necessary.
4. Repeat steps 1-3 until all desired users are assigned to the Group.

Assign Groups Tab

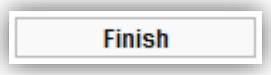
It is possible to assign an entire Group to have a specific Role within another separate Group. The most common reason for doing this is if Group A and Group B need to see the reports that are written by the other Group. Group A can be added to Group B with a "read-only" Role, thus allowing them to see the other Group's reports but not allowing them to make any changes to them. This section does not have to be used if your organization has no use for it.

Assigning Groups to a Group:

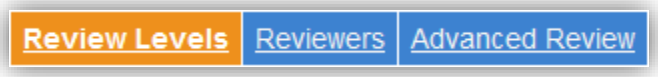
1. Click on the Group from the **Available Groups** list.
2. Click the "  " button to move the Group into the Assigned Groups list on the right.
3. Select a Role from the dropdown menu to assign for the Group.

Review Tab

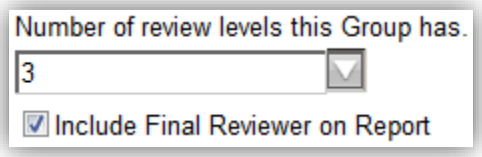
A review process for reports created in the system for the Group can be established on the Review Tab of Group Setup. Within the Review Tab there are 3 additional sections: Review Levels, Reviewers, and Advanced Review. It is a good idea to visualize the workflow of reports to decide if a review process is necessary and how it should be configured if it is. Without a review process, submitted reports will simply become completed reports entered into the system. A review process allows Supervisors to decide if changes need to be made to the report before it is submitted as a "completed" report into the system. When all necessary changes are made to the Review tab, click **Finish** at the bottom of the page to save the settings.

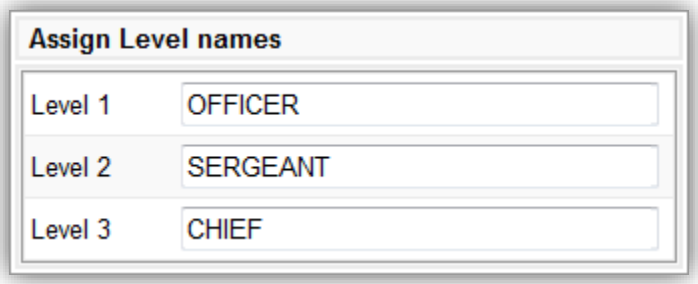


Review Levels:



There can be up to 10 levels of review in Report Exec Enterprise. That number is set here once it has been decided how many levels of review the Group needs. The checkbox to **Include Final Reviewer on Report** will print the name of the final reviewer on the printout of the report. Our example below will have 3 levels of review. That means that once a basic user submits a report, the first level will be able to look it over. Once they look it over, then can pass it up to the next level of review, or send it back to the creator. The person on the final level, in this example the Chief, has the option to send it back to the previous level, send it back to the owner to be re-submitted up through the process, or they can submit it as a valid report into the system. Once it is submitted, the report becomes "completed."





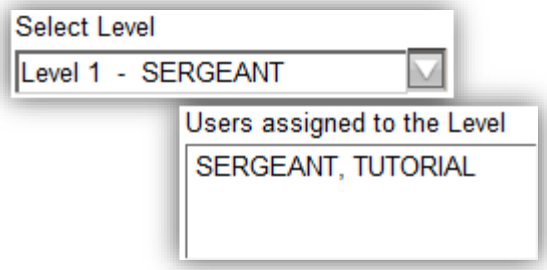
Reviewers:

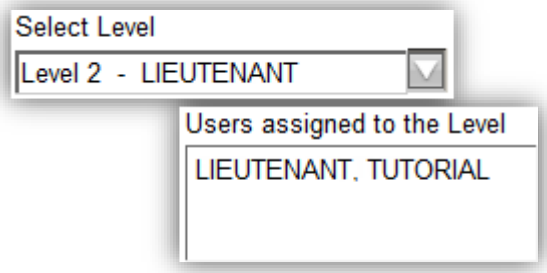
The Reviewers tab is used to create a basic review process. Once the levels of review have been established the users that will be reviewing officers will be added to their corresponding level of review. If one user is added to a level, that person will be responsible for reviewing all reports that come to that level of review. If more than one user is added to a level then it is a "first-come, first-serve" for reviewing reports. Users are chosen from the **Users in Group** list. Multiple users can be pulled over simultaneously with the **CTRL** key on the keyboard. The first user to review the report becomes the reviewing officer for that report until it is sent forward or sent back.

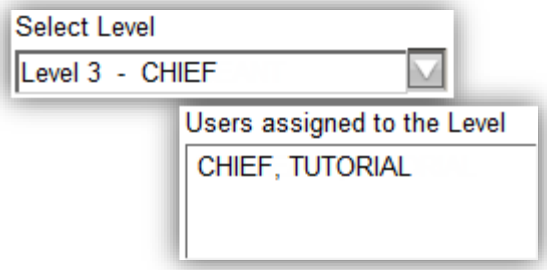
An example of a basic review process:

Officer
↓
Sergeant (Level 1)
↓
Lieutenant (Level 2)
↓
Chief (Level 3)

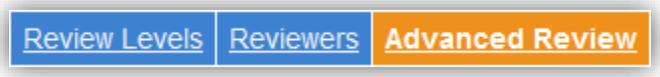
In the above example the Group has 3 levels of review. When the Officer finishes a report it goes to the Sergeant level where it can then be forwarded the report to the Lieutenant level if the reviewing officer felt it was ready to go. The reviewing officer at the Lieutenant level has the option to send it back a level to the Sergeant level, send it straight to the report creator if necessary, or submit it to the next level. The Chief level is the final level of review and reviewing officers there will review all reports in the in the program. If a user of the Sergeant level writes a report it will go to Level 2 first, then Level 3. If a user of the Level 2 writes a report it will go to Level 3 first. If Level 3 writes a report there will be no review.





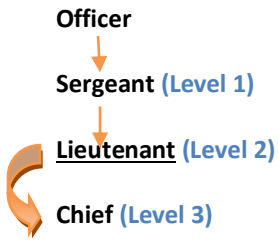


Advanced Review:



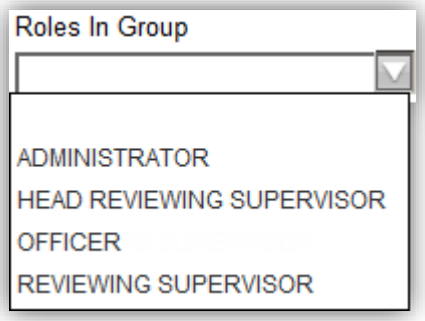
Organizations with a larger volume of reports to be reviewed may find it necessary to change the workflow of their review process. In the following example when a user of the Officer or Sergeant Level submits a report, the final reviewer will be a user of the Lieutenant Level. The Chief Level in this example will only review reports submitted by those users at the Lieutenant Level.

An example of an advanced review process:



In the above example we use the same 3 levels of review for the Group. The final level of review for most users will be Level 2. If users of Level 2 need to generate a report and if that report also has to be subject to a review process then Advanced Review will allow their reports to be submitted through a separate review process within the Group. If the user(s) of Level 3 have to write a report, that report will not be reviewed.

Advanced Review is defined by the user's Role within the Group. For our example the users are each given one of the default Roles in Report Exec. Each Role can have its reports go through a different review process. Select a Role to define a review process for from the "Roles in Group" dropdown. Our example Group has a total of 4 different Roles for all of its users. Choose the starting and ending level for the Role from the Levels that were created on the Review Levels Tab. Do this as many time as needed to fully define the Group's review process.



Role	Starting Review Level	Ending Review Level	
OFFICER	Level 1 - SERGEANT	Level 2 - LIEUTENANT	Delete
HEAD REVIEWING SUPERVISOR	Level 3 - CHIEF	Level 3 - CHIEF	Delete

Check Setups

Report Exec Enterprise has a lot that needs to be configured within the program and keeping track of everything can sometimes be tough. Check setups is a quick way to see which settings have not been setup for each Group in the program. Settings that still need to be configured will appear under the expanded container object in orange.

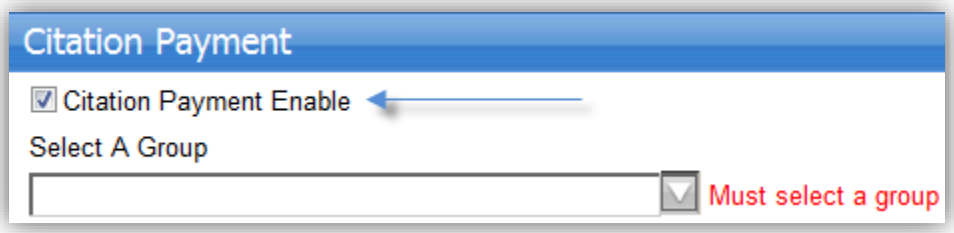
Citation Payment Configuration

The Citation Payment Configuration section of Report Exec Enterprise is used in relation to unpaid Citations that are overdue for a payment. The program can automatically adjust the fine amounts of violations attached to citations based on a specified trigger. An initial fine adjustment and a final fine adjustment can be defined or each Violation. There is also an area to include a letter for the initial and final adjustment that can be printed and mailed out to the contact that is overdue.

In order to configure Citation Payment the Citation Types used by the organization must be added to the Drop Down Dictionaries and the Violations must be added to the Tree View Dictionaries.

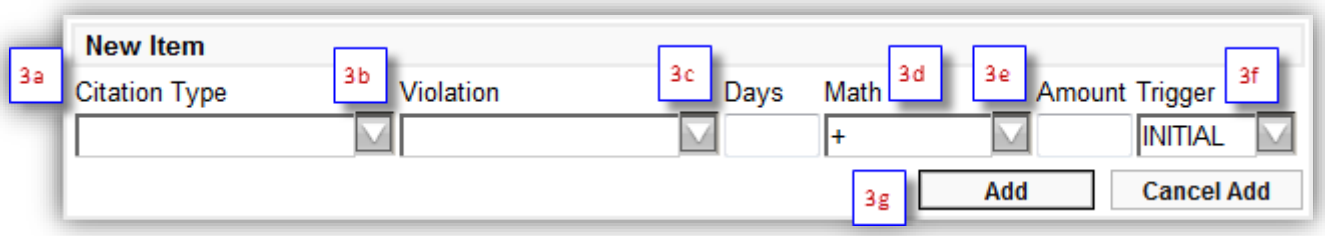
Fine Formula Tab

1. Check **Citation Payment Enable** if not already checked and select a Group to configure from the **Select A Group** dropdown. Once you select a Group you are automatically taken to the **Fine Formula** tab.

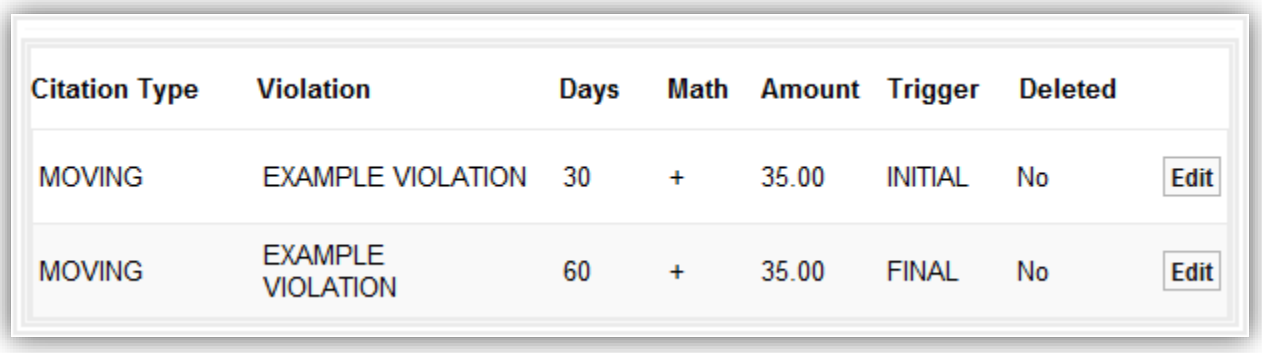


2. Click **Add** to start a new payment trigger.

3. All of the fields in the **New Item** section are required. Click **Cancel Add** to begin again if needed.
    a. Choose a **Citation Type** from the Citation Types defined in the Drop Down Dictionaries.
    b. Choose a **Violation** from the Violations defined in the Tree View Dictionaries.
    c. The **Days** field denotes the number of days before the fine adjustment is applied to the total fine amount.
    d. Select a **Math** function for the adjustment. (Addition, subtraction, multiplication, or division)
    e. Enter the whole dollar **Amount** of the adjustment.
    f. Select **Initial** or **Final** from the drop down for the adjustment **Trigger**.
    g. Click **Add** to create the adjustment trigger.

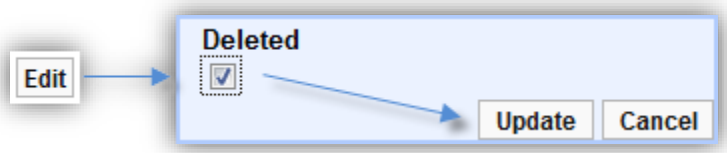


In the example below there is one violation that has had its initial and final adjustment trigger set. If the "Example Violation" is not paid within 30 days then the fine amount defined for the violation will increase by 35 dollars. If the "Example Violation" is not paid within 60 days, 30 days beyond the first trigger, then it will go up an additional 35 dollars.



Citation Type	Violation	Days	Math	Amount	Trigger	Deleted	
MOVING	EXAMPLE VIOLATION	30	+	35.00	INITIAL	No	Edit
MOVING	EXAMPLE VIOLATION	60	+	35.00	FINAL	No	Edit

To change an adjustment trigger, or to remove a trigger that is no longer needed, click **Edit**. Make the changes needed by reviewing the directions previously outlined. To delete the item, mark the checkbox for **Deleted**. Once the desired changes are made, click **Update** to save the changes.



Letter Text Tab

The text for the Initial and Final Citation Letters can be configured here.

Clery Report and Incident Configuration

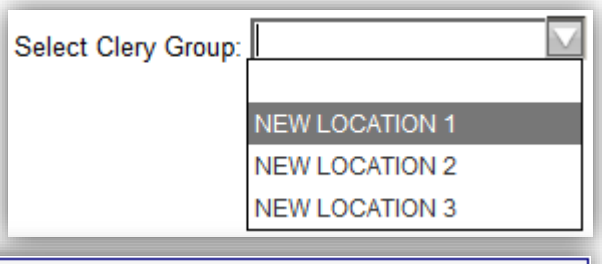
Any Group in Report Exec Enterprise that requires the reporting of Clery statistics under the Student Right to Know Act will use the setups in the following section to configure their annual Clery Report. The Clery Act is a federal requirement of colleges and universities across the United States to disclose information about crime on and around their campuses. The Clery Report that is printed out of Report Exec has a standard format that is universal for all organizations, but there are four sections that can be customized to fit the individual needs of each. Samples are provided to get the user started.

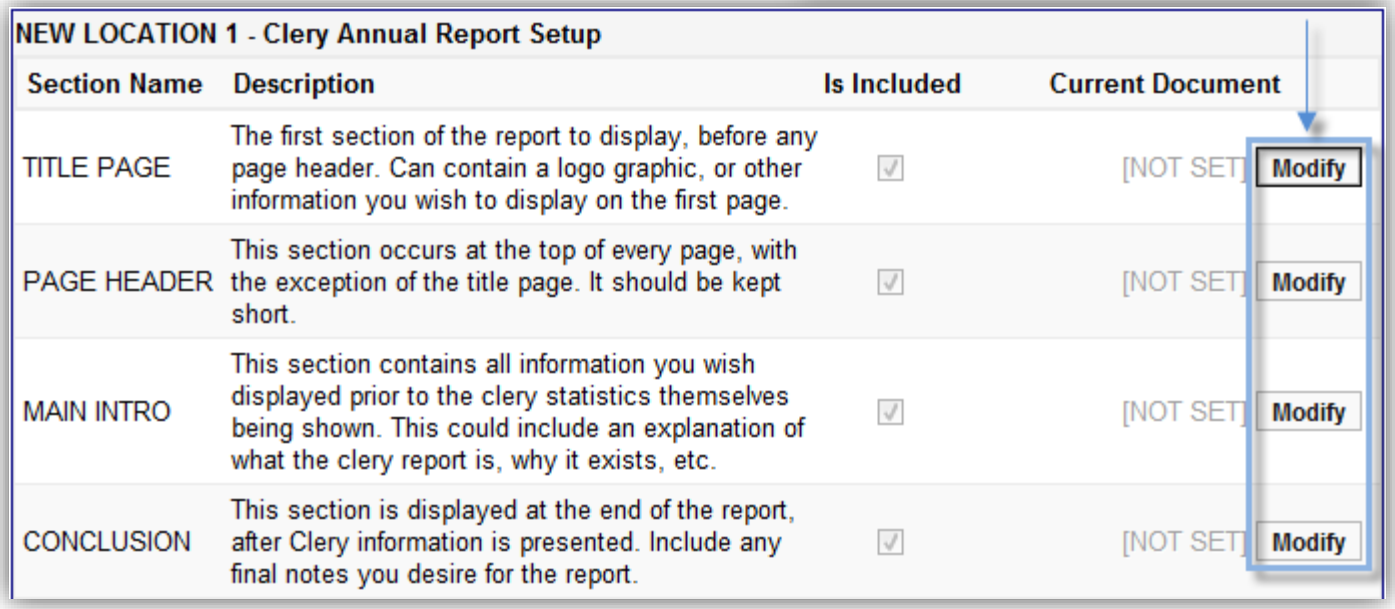
Files uploaded here must be in Rich Text Format (.rtf) in order to work with the program. Most word processing programs provide an option to change the file type when saving. Microsoft Word documents can be saved in Rich Text Format by taking the following path: **File** > **Save As** > in the **Save as Type** dropdown select **Rich Text Format (*.rtf)**.

The incident types that need to be included in the Clery Report are also configured on this page. Once the incident types have been added to the Tree View Dictionaries, the ones that need to be reported on can be checked or unchecked here.

1. Select the Group that needs to have Clery Reporting configured. If an organization has multiple campuses, each campus should be their own Group in Report Exec.

2. Click **Modify** in the section that is being setup.

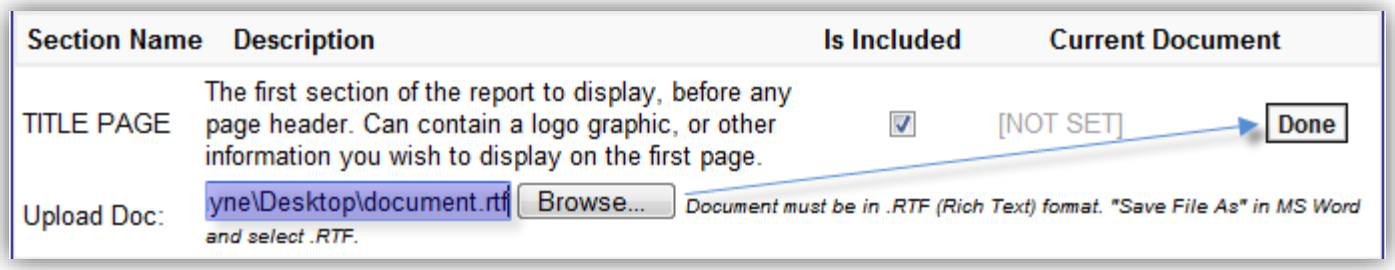




NEW LOCATION 1 - Clery Annual Report Setup

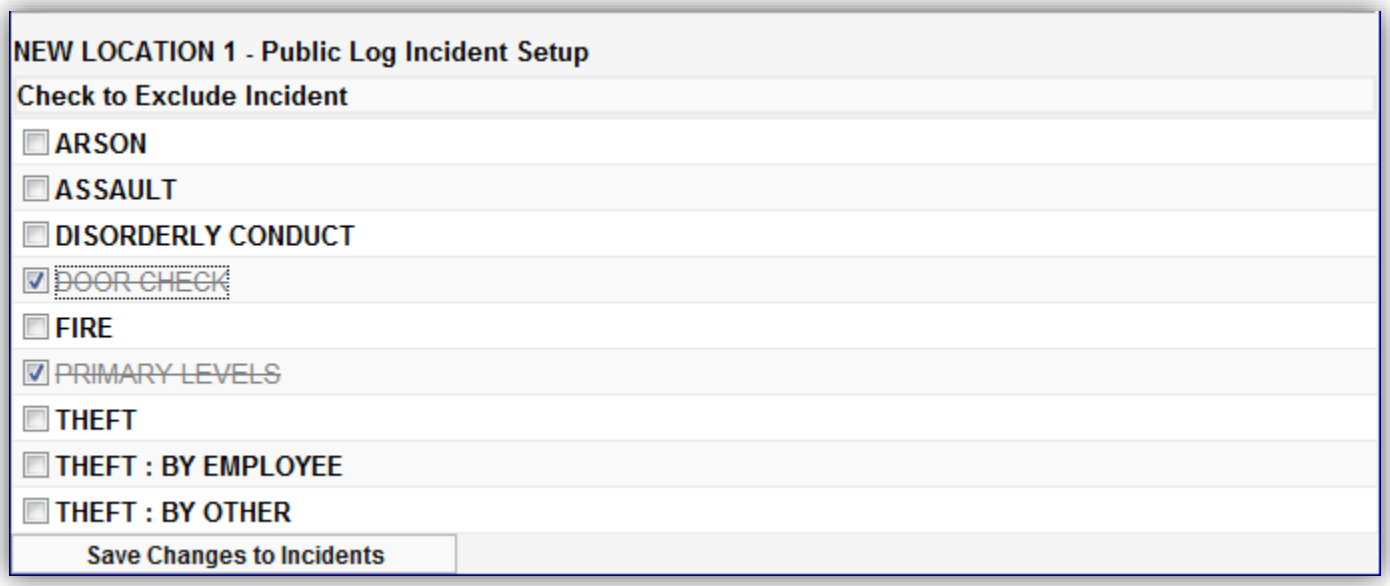
Section Name	Description	Is Included	Current Document	
TITLE PAGE	The first section of the report to display, before any page header. Can contain a logo graphic, or other information you wish to display on the first page.	☑	[NOT SET]	Modify
PAGE HEADER	This section occurs at the top of every page, with the exception of the title page. It should be kept short.	☑	[NOT SET]	Modify
MAIN INTRO	This section contains all information you wish displayed prior to the clery statistics themselves being shown. This could include an explanation of what the clery report is, why it exists, etc.	☑	[NOT SET]	Modify
CONCLUSION	This section is displayed at the end of the report, after Clery information is presented. Include any final notes you desire for the report.	☑	[NOT SET]	Modify

3. Click **Browse** and select the Rich Text Format (.rtf) document from the directory where it is saved on the computer. Click **Done** once the document has been selected.



4. A link to an example document is provided in the **Sample Clery Report Documents** subsection.

5. The Public Crime Log that is typically printed on a daily basis will use data from three different places in the program. Report Exec Dispatch (if used), Daily Event Log, and Incident Reports. To setup what prints out on the Daily Crime Log, put a check box next to the incidents to not include. By default all incidents will be included. In the below example the "Door Check" reports are not necessary to be reported on for the Clery Daily Crime Log and have been removed from being printed.



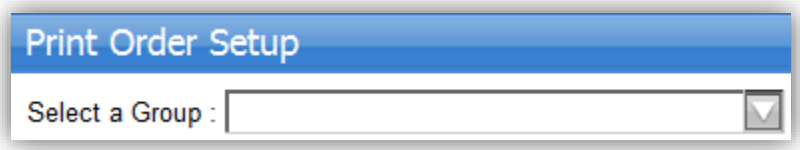
6. Click **Save Changes to Incidents** when done to apply the changes.

Contact Print Order Setup

When a report is printed from the program that contains multiple contacts, by default, Report Exec will print those contacts in alphabetic order by Contact Type. Contact Types are configured in the Drop Down Dictionaries of System Wide Setup.

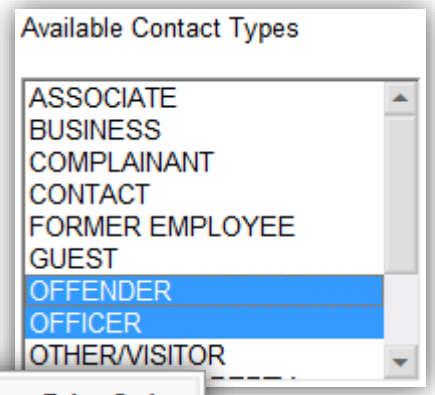
An example would be to use the three contact types: Officer, Offender, and Complainant. By default, the program will print them in the order Complainant, Offender, Officer. In the following example the organization requires that all reports created from this Group need to have an Officer, and an Offender associated to the report. They want the Officer's contact information to always print before the Offender's information on a printed report.

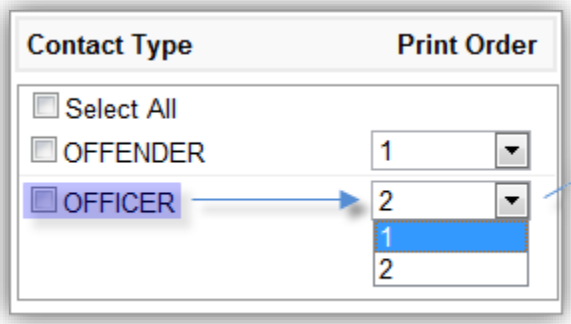
1. Select the Group to configure the contact print order for.

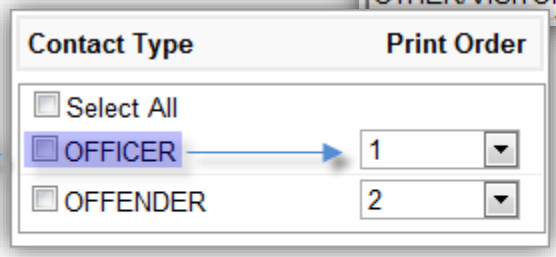


2. From the **Available Contact Types** list on the left, select the Contact Types that will need to print in a certain order and click "  " to bring them into the list on the right. Multiple Contact Types can be selected with the **CTRL** key on the keyboard.

3. Change the print order to reflect the needs of the Group being configured. Click **Finish** when done making the needed changes.



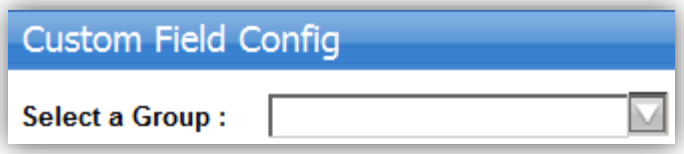




Custom Field Configuration per Group

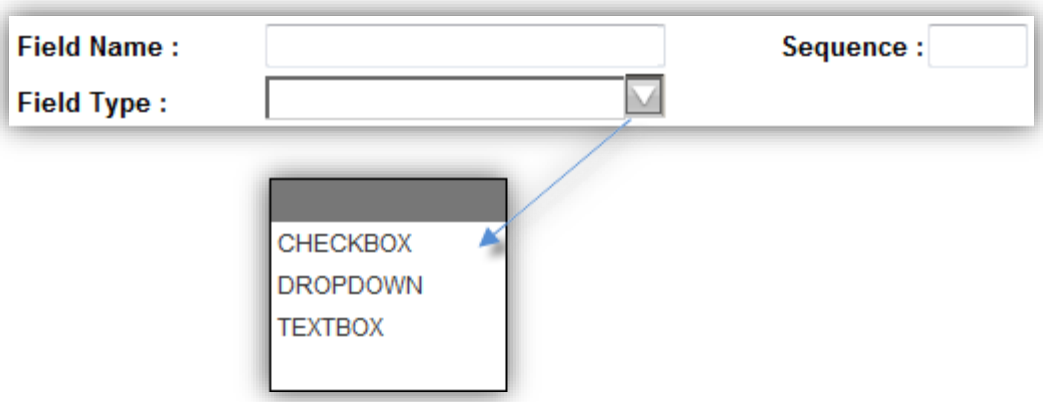
Custom Fields can be added to reports in Report Exec Enterprise depending on the needs of the organization and/or specific Groups within the organization. Enabling custom fields for a Group will add a **Custom Fields** tab to the report type selected to add fields to. The custom fields appear as an additional sub-module (tab) in a report and because they are "custom" they can be anything that is desired by the organization. Custom fields can have a checkbox, dropdown, or free text field. The checkbox option is typically for "yes or no" answers. The dropdown option links a dropdown menu from Report Exec to this custom field dropdown. The textbox option allows for a small free text field for manually inputting the information requested by the custom field.

1. Select the Group to add custom fields to.



2. Select the type of report that needs custom fields.

3. Enter a name for the custom field in **Field Name** and select the type of field from the 3 choices in the **Field Type** dropdown: Checkbox, Dropdown, or Textbox. The **Sequence** is the order that the custom fields will appear.



4. Click **Add** to create the new custom field.

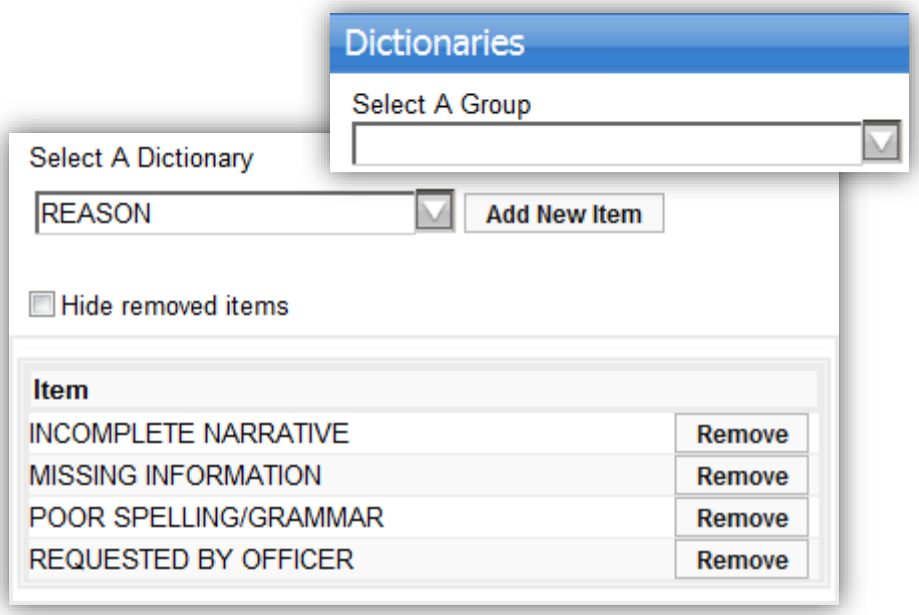
Drop Down Dictionary Configuration

Dropdown Dictionaries in Report Exec Enterprise are first configured in the System Wide Setup section of the program. Those dictionary items can be further defined on a Group-by-Group basis as needed, if needed. Dropdown menus are used throughout the program to ease the process of creating and editing reports. For example, when a Supervisor reviews a report they have the option to send that report back to the creator for some additional changes to be made. When sending the report back the Supervisor is given a dropdown menu that contains reasons why the report was sent back. Those reasons are defined in System Wide Setup but can then be further configured in Group Dropdown Dictionary Configuration.

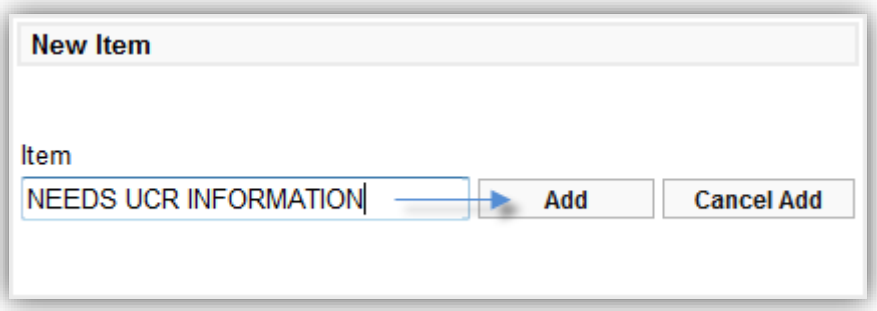
1. Select the Group to define drop down dictionaries for.

2. Select a dictionary from the list. A description where each dropdown dictionary is located can be found in the table on pages 7 – 11. This example will use the **REASON** dictionary.

3. To add a new dropdown item click **Add New Item**.



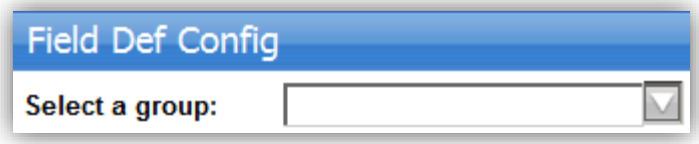
4. Enter the new value into the text field and click **Add**.



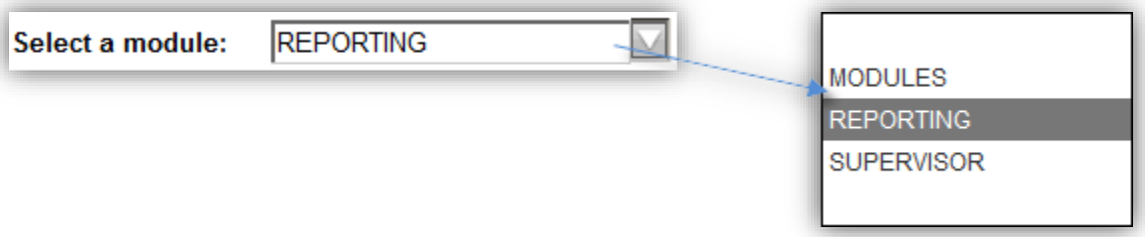
Field Definition Configuration per Group

Many fields in Report Exec are customized in System Wide Setup Field Definition Configuration. Further customizations of fields in the Report Exec application are done in Field Definition Configuration per Group. All of the pages within a report are also customized here and must be done for each Group in the program. Changes to the report pages can only be applied here in Group Setup.

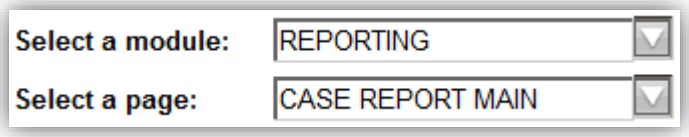
1. Select a Group to define fields for.



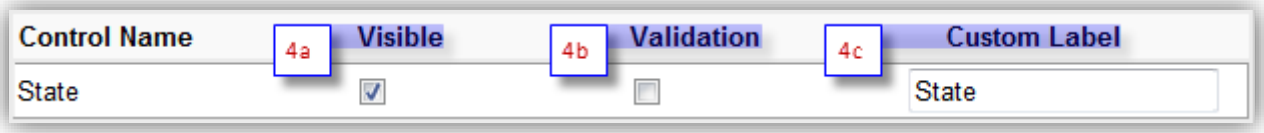
2. Select a module from the drop down. This example will use **Reporting**.



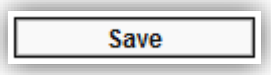
3. Select a page that corresponds with the module selected in Step 2. For example, Groups outside of the United States may need that change **State** to **Province**. This example demonstrates the **CASE REPORT MAIN** page.



4. To hide a field, uncheck the box in the **Visible** column (4a). To make a field required, check the box in the **Validation** column (4b). To change the title of the field, type the new name in the **Custom Label** field (4c).



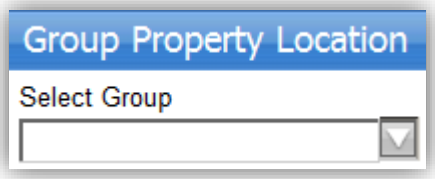
5. Click **Save** to apply changes when complete.



Group Property Location Configuration

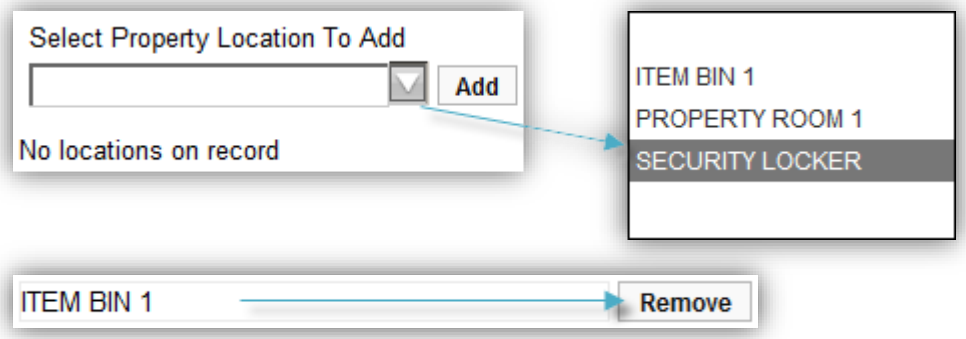
When property is taken into custody, whether it is confiscated, lost, or found, it will be placed somewhere within the organization until it is "released." **PROPERTYLOCATION** is a drop down dictionary that must first be populated in System Wide Setup and/or Group Setup Dropdown Dictionary Configuration. Property locations are assigned per Group and reflect where that Group deposits recovered pieces of property. For example, Group A may have a locker and a small bin for keeping items that have been found, while Group B has an entire room dedicated to storage.

1. Select the **Group** to add Property Locations to.



2. From the **Select Property Location to Add** drop down select a property location and click **Add**.

3. If a property location is added to a Group in error, click the **Remove** button next to that location to remove it.



Move Reports

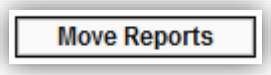
Moving reports cannot be undone. It is recommended to backup the database before doing any restructuring.

Report Exec Enterprise is a scalable application meant to grow with the needs of the organization. There may be a time when the Groups in Report Exec need to be changed or consolidated. The Move Reports section allows reports from one Group to be moved to another Group. This action can be done for the reports of specific users or for all reports in the entire Group.

For example, a security company has one location that they work from which has three work shifts. The company has each of their work shifts setup as a Group in Report Exec. They have now expanded to three locations and want each location to be its own Group in Report Exec. They are now able to combine the reports from all three shifts into the new Group created for their location.

1. Select the **Source Group** to remove reports from and the **Destination Group** to move reports to.

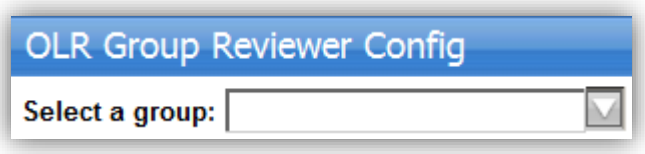
2. Select the user(s) to move the reports for from the **Report Creator List**. Multiple users may be selected by holding the **CTRL** key on the keyboard while selecting users. If all reports of this Group, from all users, need to be moved then click the **Select All** checkbox.

3. Click **Move Reports** when ready. 

Online Reporting – Group Reviewer Setup

Reports submitted through the Online Reporting Module will have to be reviewed by specifically designated users of the program. The users specified in this section are those that will choose which online reports will be brought into the system as a real report. The Online Report Reviewers will have a tab on their Dashboard called **Online Reports** where they will select the reports to be entered into the system.

1. Select the Group to add Online Reviewers to.



2. From the **Users in Group** list on the left, select the user(s) who will be Online Report Reviewers. Multiple users may be selected by holding the **CTRL** key on the keyboard while selecting users.

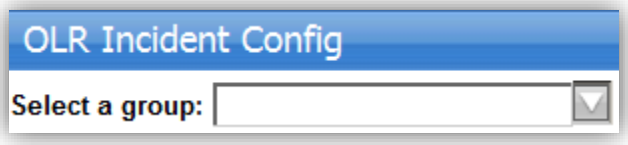
3. Click the " 

" button to move the selected users on the left to the **Users assigned for Review** list on the right.

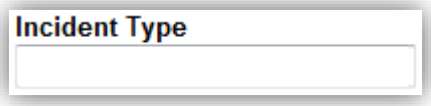
Online Reporting – Incident Type Setup

Incident Types specific to the Online Reporting Module are setup here. These incident types are for the people that are creating an online report and will not necessarily be the same as the Incident Types in the Incident Type Dictionary. Each Incident Type has a free text field for a definition and an example.

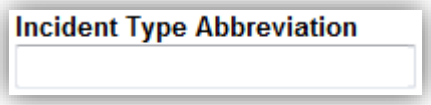
1. Select the Group to define the incident types for.



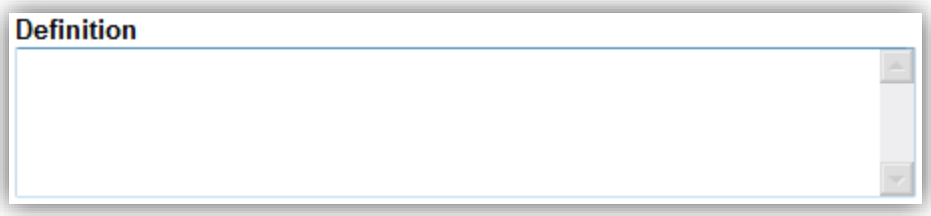
2. Enter the **Incident Type** to be added.



3. The **Incident Type Abbreviation** is not a required field.

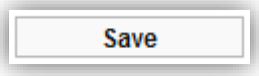


4. A **Definition** for the Incident Type will display for the people using the Online Reporting Module to explain what the Incident Type means. A Definition is not required.



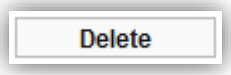
5. **Examples** of the Incident Type can supplement the definition if needed. Examples are not required.

6. Click **Save** when done to apply the changes.



7. To add another Incident Type for the same Group, click **Add New** and repeat steps 2-6.

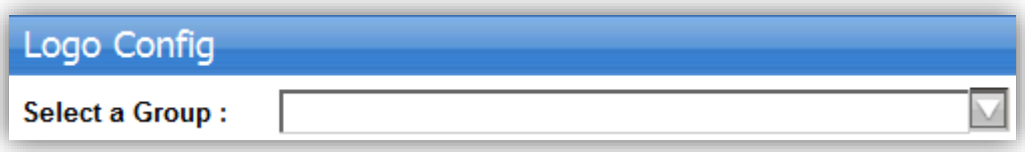
8. To delete an Incident Type highlight it and click **Delete**.



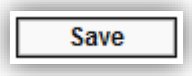
Online Reporting – Logo Configuration

A company wide, and/or Group specific, logo can be added to the upper corners of the Online Reporting page. The **Company Logo** appears on the upper left, the **Module Logo** appears on the upper right.

1. Select a Group to add a logo to or choose to add the logo system wide. A Group logo will override a system wide logo for the Online Reporting page for that Group.



2. For the **Company Logo** click **Browse…** and navigate to the directory on the computer where the picture to be added is saved. Double-click the picture file to select it and be sure to click **Save** to apply the logo.

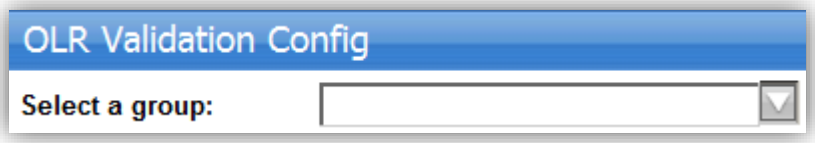


3. In the **Select Module** section click **Browse…** and navigate to the logo to use on the right side of the screen. Double-click the desired image and click **Save** to apply the logo.

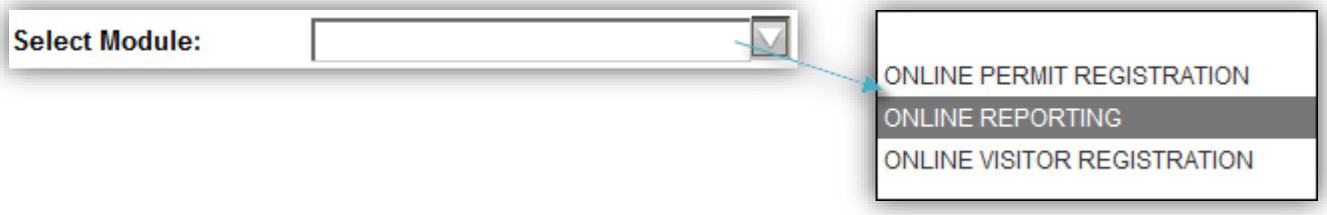
Online Reporting – Validation Configuration per Group

To make sure enough information is received from people creating online reports, certain fields can be set to be required, while others can be hidden if needed. Field titles can also be changed in OLR - Validation Configuration if desired. The following example will edit the **YOUR INFO** page of the **Online Reporting** module which is the page where a person would fill out their personal contact information.

1. Select the Group to apply settings for.

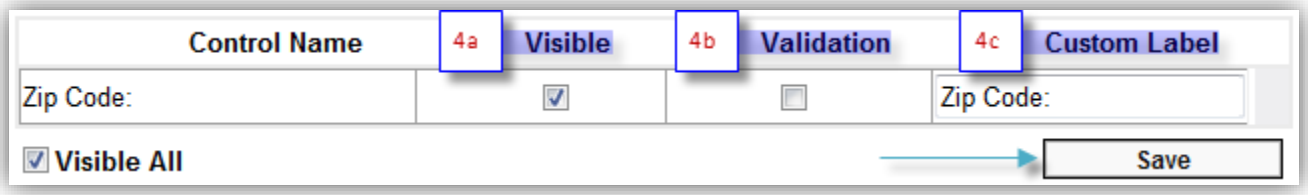


2. Select the module.



3. Select the page to define. The **YOUR INFO** page is a common area to require and/or hide fields.

4. To hide a field, uncheck the box under the **Visible** column (4a). To make a field required, check the box in the **Validation** column (4b). To change the title of the field, type the new name in the **Custom Label** field (4c).



5. Click **Save** to apply changes when complete.

Permissions Report by Group

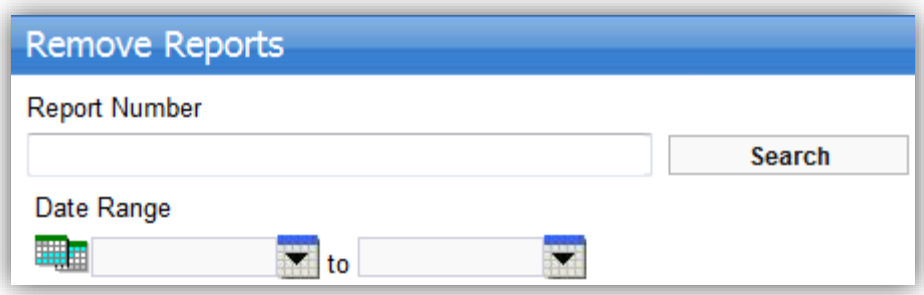
The Permissions Report by Group is a quick way to get a printout of the access that each user in a Group has been given, for all Groups in the program. Simply click the link for the Permissions Report and it will generate itself in a separate window. The example below shows one user's access, Tutorial Chief, for the Group named "New Location 3**."**

NEW LOCATION 3

Group Name	User	Module	Reader	Writer	Printer
NEW LOCATION 3	CHIEF, TUTORIAL	ActivityTracking	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	Bolo	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	Citation	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	Dispatch	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	KeyTracking	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	Property	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	Training	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	Trespass	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	VisitorCheckIn	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	Reporting	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	Clery	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	KeyTracking	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	ProfilingIncludeInSupplement	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	Investigation	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	ParkingPermit	True	True	True
NEW LOCATION 3	CHIEF, TUTORIAL	WPV	True	True	True

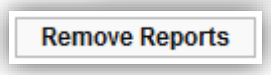
Remove or Restore Reports

The Remove or Restore Reports section of Report Exec Admin allows an Administrator to remove or restore a large number of reports at one time. Reports may need to be removed if there were a series of reports issued in error that need to be made inactive. Conversely, if a series of reports were removed in error, they can be restored from here. This is helpful if new users are being trained and creating test reports to train on or if mistakes are made. Reports can be searched by individual numbers, or by a date range. If there are over 500 results from the defined search criteria then only the top 500 results will be shown.



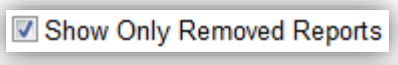
Removing reports

1. Define a search by an individual report number, a date range, or search all reports by leaving the fields blank.
2. Check the checkbox next to reports needing to be deleted in the list that appears below. If it is known for certain that all reports in the search need to be removed then the **Select All Reports Below** checkbox can be used to easily select everything in the search.
3. Click **Remove Reports** when ready.

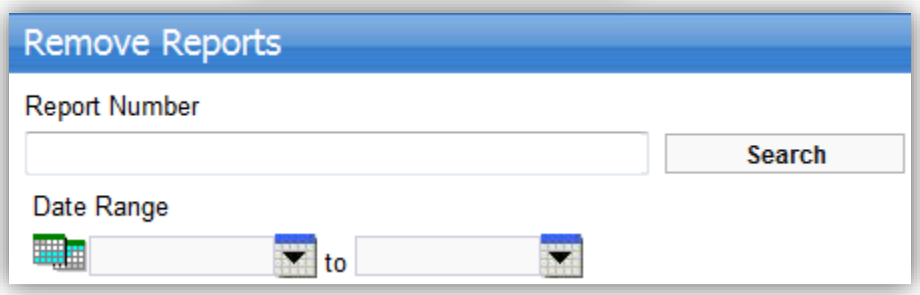


Restoring reports

1. Check the **Show Only Removed Reports** checkbox.



2. Define a search by an individual report number, a date range, or search all reports by leaving the fields blank.



3. Check the checkbox next to reports needing to be deleted in the list that appears below. If it is known for certain that all reports in the search need to be removed then the **Select All Reports Below** checkbox can be used to easily select everything in the search.

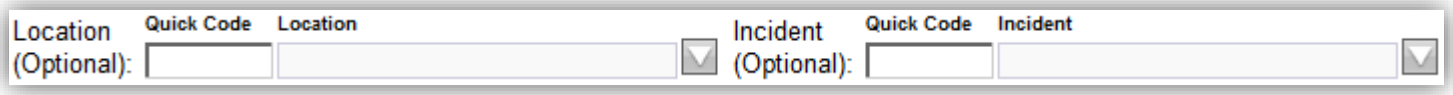
4. Click **Restore Reports** when ready.

Report Message Setup

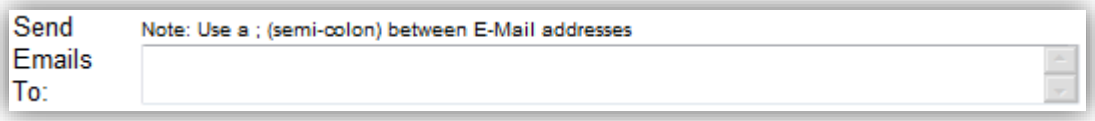
Incident Reports in Report Exec Enterprise can be set to automatically e-mail a copy of the report in Portable Document Format (.pdf) to specified e-mail addresses based on the location of occurrence, the Incident Type, or both. Each Incident Type and/or Location that is defined can be assigned to e-mail upon a user clicking **Submit** or the Final Reviewer clicking **Complete** within a report.

Setting up automatic e-mailing

1. Select a **Location** and/or **Incident Type** that requires an automatic e-mail to generate. At least one is required.



2. Enter the e-mail address or addresses that need the report e-mailed to them. Multiple e-mail addresses must be separated with a semi-colon (;).

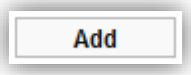


3. A password for the e-mailed **.pdf** files can be required for certain reports if needed by checking the **Use Passwords on e-mailed PDF Reports** checkbox.

4. Select the Group that the reports are being e-mailed from.

5. Select **Submitted** if the report should e-mail when the Submit button is pressed by an Officer. Select **Completed** if the report should e-mail when the Final Reviewer clicks Complete.

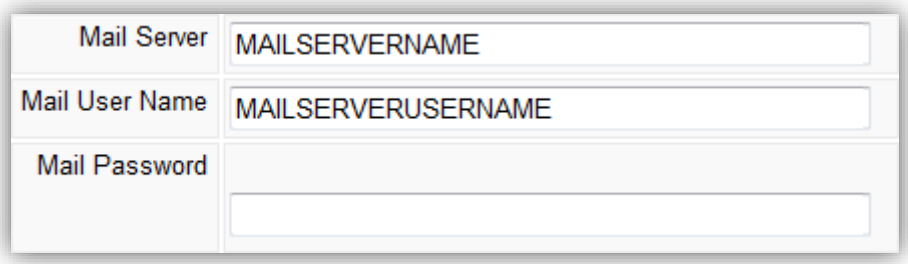
6. Click **Add** to add the new mailing procedure.



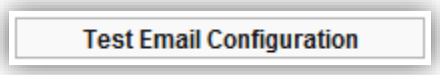
7. Repeat Steps One through Six as many times as needed.

Testing automatic-e-mailing

Automatic e-mailing of reports for a **Direct** customer should work with no additional configuration needed because the mail server information for the relay server is inherent in the program by default. Report Exec **Enterprise** customers, meaning customers that host their own server, will have to enter in their mail server information in **System Wide Setup**, **System Settings**. The **Mail Server** can be entered as the server name (if on the same network), Fully Qualified Domain Name (FQDN), or IP Address. The **Mail User Name** is the name of an account created by I.T. on the mail server. This account allows the Report Exec application to access the mail server so that it can relay e-mails from it. The **Mail Password** is the password for the account created on the mail server.



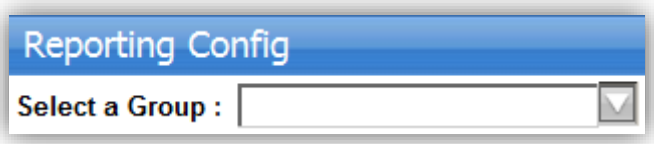
On the **Report Message Setup** screen type in an e-mail address to use to test the functionality of the automatic e-mailing. Click **Test Email Configuration** which will provide a success or fail message.



Reporting Configuration

The Reporting Configuration section of Report Exec Enterprise is where Administrators go to setup which reports are used for a particular Group. Each report type that is in use by a Group can also be set to do one of the following: automatically generate a Daily Event Log entry when a user opens a report of that type, require the report type to be part of the Group's review process, allow the report type to be available to be created as a Supplemental Report.

1. Select a Group to configure reports for.

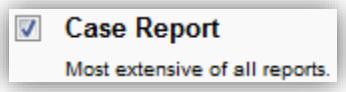


2. If juvenile information should be hidden when reports for this Group print, check the **Hide juvenile contact information on reports** check box. This only needs to be checked if reports for this Group should never have that

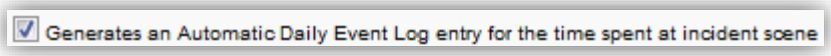
information printed. Users are still given the option to hide juvenile information when printing individual reports from the user side of the program.

3. Check the **Utilize UCR Codes for Reporting** if the Group needs to report UCR information.

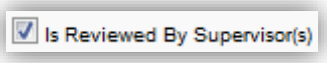
4. By default, all report types are enabled for a Group. Any report that is not being used by the Group may be disabled by clicking the check box to the left of the report title. The example below shows that Case Reports are enabled for the Group.



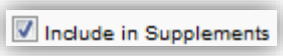
5. Daily Log entries that indicate when an Officer is writing a report can be set to be automatically create themselves by checking the **Generates an Automatic Daily Event Log entry for the time spent at incident scene** checkbox.



6. If a report type needs to go through the review process for the Group, check the **Is Reviewed by Supervisor(s)** checkbox.



7. Report types that are okay to be created as a Supplemental Report to another report need to have the **Include in Supplements** checkbox checked.

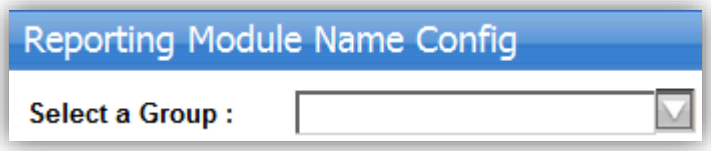


8. Click **Update Changes** to save any changes made to the page.

Reporting Submodule Configuration

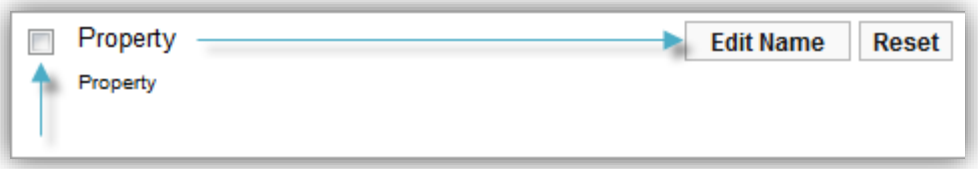
Each report type in Report Exec Enterprise may or may not have various sections of the report that can be activated if needed for further information regarding the incident. These sections are referred to as "Submodules." The Reporting Submodule Configuration area of the Admin application is where an Administrator can define what sections appear as available to be activated (if needed) for a report. The names of each section can also be changed. For example, if an agency doesn't want to use the title "Contacts" but instead want to use "Involved Parties," then that change would be made in this area. If the agency wants to remove "Property" from being able to be entered on Citation Reports, that change would also be made in this area. The following example will illustrate a Group that does not want their Officers to have the option to add Property to a Citation.

1. Select the Group to configure sub-modules for.



2. Select the report type to configure.

3. Uncheck the box next to the corresponding sub-module to remove it from being selectable on a report. If the sub-module needs its name changed, click **Edit Name**.



4. Click **Update** to apply a name change to the sub-module. Click **Cancel** to exit editing without applying a change.

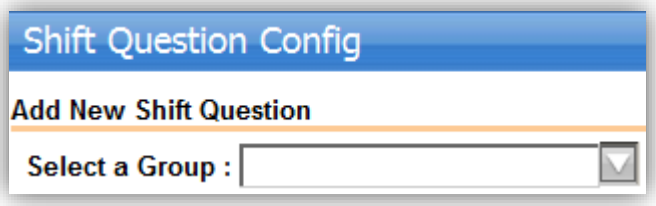
5. When all changes are finished being made click **Update Changes** at the bottom of the page.

6. If a mistake was made when editing a sub-module name the **Reset** button may be clicked before **Update Changes** to revert back to the last saved sub-module name. Alternatively, if multiple sub-module names were edited in error the **Reset All** button at the bottom of the page will change all edited sub-module names back to the previously saved names.

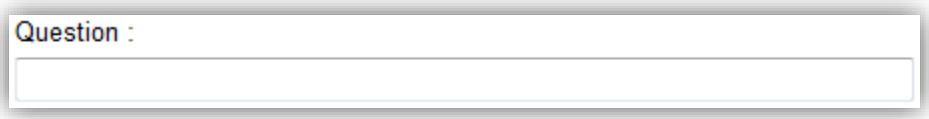
Shift Questions Configuration

The Shift Questions Configuration setup allows an administrator to define additional fields to get populated by a user in the Daily Log when going to Modules > Daily Log > Add New Shift. Administrators can define whether a field is numeric (numbers only), free text (alpha numeric), or true/false (check box). To define additional fields:

1. Select the Group to add or edit Shift Questions for.



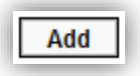
2. Type a field title or question into the free text **Question** field provided.



3. The **Question Type** decides how the user will answer the predefined Shift Question. There are three choices to choose from: **True/False**, **Free text**, and **Numeric**.

- **True/False** provides a checkbox next to the question on the Officer's shift information in Daily Event Log. This is good for yes-or-no answers.
- **Free text** provides a field that will allow letters, numbers, and symbols. This is good for a specific answer.
- **Numeric** provides a field that will only accept numbers.

4. Click **Add** to apply the new question.



5. Shift Questions may be edited by clicking **Edit** next to the corresponding question. Click **Update** to apply any changes or click **Cancel** to stop editing without making changes.

System Settings

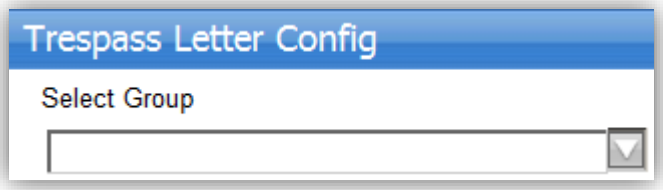
The System Settings area is where certain settings can be defined for a particular Group. Most System Settings are System Wide and defined by an administrator with System Wide Access, but once a Group is selected a Group Administrator can define the following settings:

- **Past Shift Event Hours** – The number of hours a user has to make a modification to a daily log entry.
- **Time Mode** – Select **AMPM** for 12-hour time or **Military** for 24-hour time formatting.
- **Server Time Zone Offset** – The difference in time between where the server is located and where the program is being used by the Group.
- **Date Format** – The default setting is **ISO** (*International Standard Time*).
- **Date Format Override** – Allows the agency to change the date format to what is used locally for the Group.
- **Use Daylight Savings** -
- **Culture** – If **en-US** is selected, certain terminology, such as "Miranda Warning," will be the U.S. based standards. If **en-CA** is selected then the program will use Canadian-English terminology.
- **Hide Juvenile Record** – If **YES** is selected the program will always hide juvenile information from printing, if **NO** is selected the system will not automatically hide juvenile information but will provide the user with the option to hide juvenile information upon printing.
- **Enable UCR Codes** – If a department reports UCR this field needs to be marked **YES** which will enable the UCR Module.
- **Measurement System** – Defines whether Height and Weight fields use **METRIC** or **IMPERIAL** measurements.
- **Concurrent Logins** – If this setting is unchecked then a user can only login to one computer at a time with the same user ID. Once the user logs out from that computer then can then login to a different computer.
- **E-mail Reports After Written** – Turns on ability to automatically e-mail reports after a user has clicked **Submit**.
- **E-mail Reports After Review** – Turns on ability to automatically e-mail reports after final approval is given.
- **Enable Bar Code Generation** – Automatically generates a number in the "Bar Code Number" field for property.
- **Enable Permit Bar Code Generation** – Automatically generates a Bar Code Number for permits.
- **Training Notification E-mail** – E-mail address or addresses of those individuals that should receive notifications of training certification expiration. If entering multiple e-mail addresses must use a semi-colon (;) between addresses.
- **Enable Editing in Submitted Report** – This gives users the ability to reopen one of their reports that was sent for approval to make modifications. If the report has already been reviewed, they cannot make changes.
- **Use Narrative Versions** – Narrative versioning may be enabled or disabled here.
- **Property Gets Case Number** – If checked, Lost and Found Property Reports will get the next available case number instead of its own tracking number.
- **Delete Visitor Image on Check Out?** – In the Visitor Tracking Module you can use a webcam to capture a picture of someone for an identification badge. Keeping the images can speed up the process of checking in visitors, however over time the space used by pictures can add up. If disk space is a concern then the images can be set to delete themselves once the visitor is checked out.

Trespass Letter Configuration

The Trespass Letter Configuration is where an administrator can go to define the wording that prints on the trespass letter. To set this up:

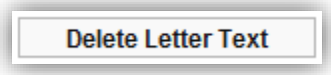
1. Select the Group to configure a Trespass letter for.



2. Fill in the wording in the space provided or copy and paste the wording from another document.

3. Click **Update** to save the changes.

4. Click **Delete Letter Text** to remove the wording and start over.



Auditing

The Auditing section of the administrative side of Report Exec allows administrators to audit activity within the program. Audit functions are as follows:

- Audit a Report – Search a report by number or officer and view any activity within the report
- Audit a User – Search a user by last name, user name or ID and view activity over a date range
- Audit a Dispatch User – Search a dispatch user and audit their login/logout of dispatch
- Audit Emails – Search e-mails sent out from system over a specified date range
- Audit Messages – View whether a user has created or deleted messages on the Dashboard
- View All Auditing for a Date Range – View activity occurring with the Report Exec program over a specified date range
- View Disk Space Used – View how much space is being used by the database and digital media