System Administration

Application User Training

Version 25.x

Last Modified 25.0 | February 2025

Contents

Section 1. Technical Support

AssetWorks provides several ways to connect with the Customer Care team. Be prepared to provide detailed information to the representative. If you are reporting an issue by email, include screen images of the problem. This information provides the Customer Care representative with the necessary information to quickly and effectively respond to you.

Customer Care is available 7AM – 7PM EST Monday through Friday.

Telephone: 800.900.8152

Email: M5Support@AssetWorks.com

Website: Community.AssetWorks.com

You can use this website to open issues, review the status of past submitted issues, review and download documentation, review additional training materials, and access the latest AssetWorks news. For secure access to the website, contact Customer Care by calling the listed telephone number.

Section 2. M5 Configuration and Setup Overview

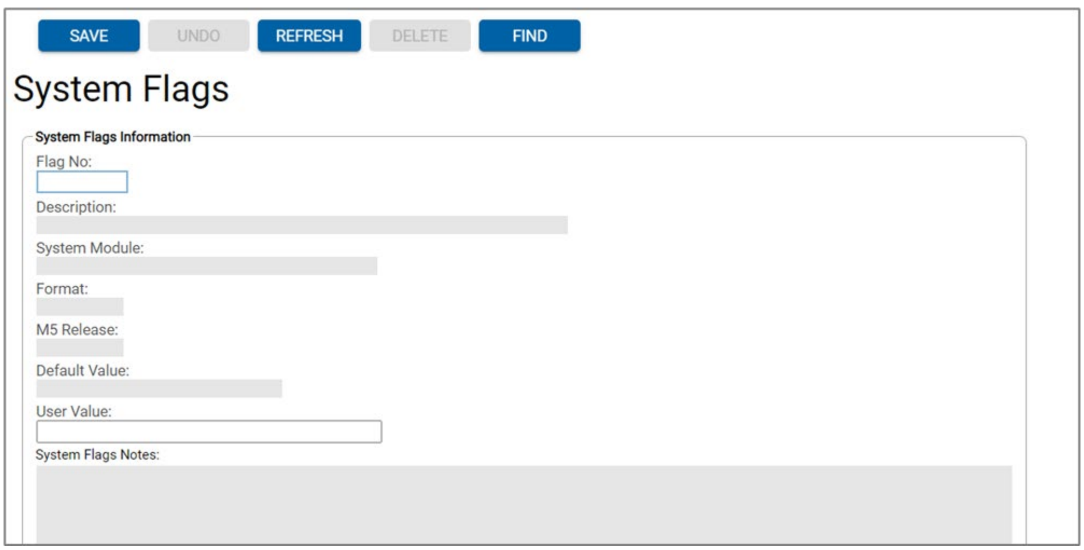
The System Administrator is responsible for the configuration and setup of the M5 System. The configuration and setup steps were defined during the project start up and detail how your M5 system operates in terms of coding, organizational structure, workflow, and inventory.

All these steps must be completed and verified before moving the M5 System into a live production status. After your site has gone into live production these codes should be reviewed and maintained on a regular basis.

As you become familiar with the M5 System you will discover items that can be improved and enhanced to further customize your M5 System. This *System Administrator* document is offered as an ongoing support tool for performing this critical maintenance. However, it is not intended to replace formal AssetWorks training. Your System Administrator should receive the comprehensive AssetWorks training available through your Project Manager. They will use this and other documents during that training.

Appendix C is a Glossary of Terms that you might want to review now as well. You may not be familiar yet with how some of the terms are used in the M5 System.

Setting and Maintaining System Flags



The architecture of your new M5 System is designed to be highly configurable to the specific needs of the working environment in your fleet organization. A key component of this flexible structure are the *System Flags*.

System Flags serve as switches to activate or deactivate various features and functionality. Typically, they are *Yes* or *No* settings, but you will also see numeric choices as well.

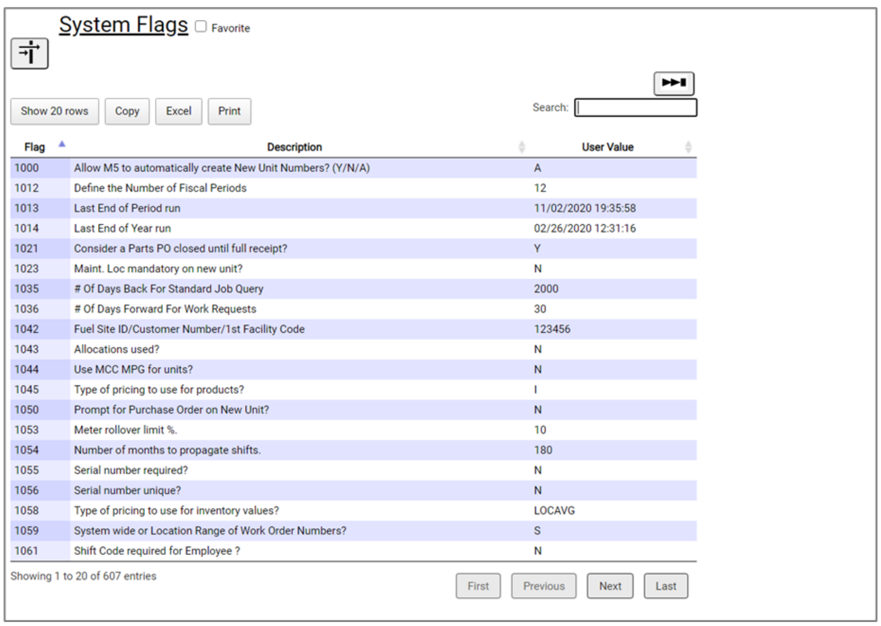
See the *System Flags Table* for a complete listing of system flags.

You should review it and become familiar with the different settings of the system flags that impact the configuration of your system. They must be set according to the current business practices implemented in each of the M5 modules.

These need to be reviewed periodically as your business procedures can change and new system flags can become available in a new release of the software.

To set and maintain the system flags, use the following steps.

1. Open the *System Flags* frame. The quickest way to find any frame in the M5 System is to use the **MENU** at the top of the frame. Enter *System Flags* in the search field, the *System Flags* frame displays.
2. Double-click in the **Flag No** field to view the System Flags list, or enter a system flag number.
3. Select a system flag to see the description and make a change to its setting.
4. Review the **Description** and change the **User Value** field, as applicable. Acceptable values are *Y/N/A* (Yes, No, Always). Numeric values are occasionally included as a selection choice. **User Value** is the only field you can modify on this frame. Select **SAVE** to update the setting.


System Flags Favorite

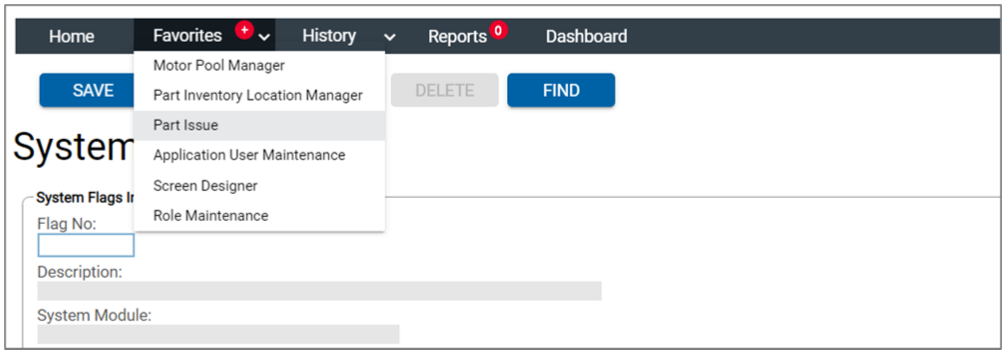
Show 20 rows Copy Excel Print Search:

Flag	Description	User Value
1000	Allow M5 to automatically create New Unit Numbers? (Y/N/A)	A
1012	Define the Number of Fiscal Periods	12
1013	Last End of Period run	11/02/2020 19:35:58
1014	Last End of Year run	02/26/2020 12:31:16
1021	Consider a Parts PO closed until full receipt?	Y
1023	Maint. Loc mandatory on new unit?	N
1035	# Of Days Back For Standard Job Query	2000
1036	# Of Days Forward For Work Requests	30
1042	Fuel Site ID/Customer Number/1st Facility Code	123456
1043	Allocations used?	N
1044	Use MCC MPG for units?	N
1045	Type of pricing to use for products?	I
1050	Prompt for Purchase Order on New Unit?	N
1053	Meter rollover limit %.	10
1054	Number of months to propagate shifts.	180
1055	Serial number required?	N
1056	Serial number unique?	N
1058	Type of pricing to use for inventory values?	LOCAVG
1059	System wide or Location Range of Work Order Numbers?	S
1061	Shift Code required for Employee ?	N

Showing 1 to 20 of 607 entries

First Previous Next Last

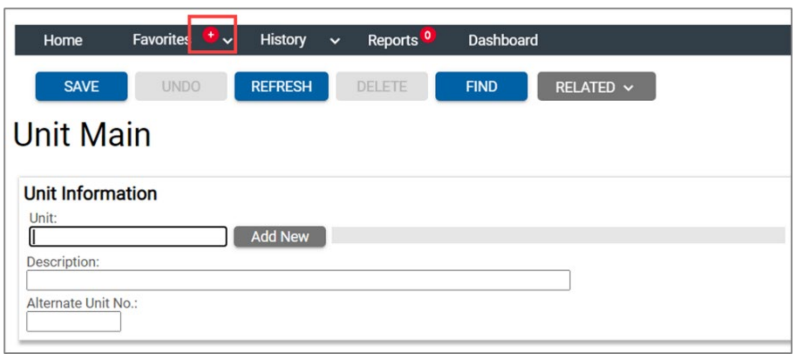
Favorites Menu



The first frame that appears after a user logs into M5 is the *Homepage*. The M5 System Administrator can customize this Homepage by using the *Screen Designer* module and by adding **Favorites** to the user's Favorites Menu.

Screen Designer allows additional elements like dashboard KPI's, notifications and corporate wide messages. However, it is not part of the standard system package. It does require an additional license. Favorites are located on the Static Menu Bar.

When you are viewing a system frame a **Plus** icon appears in the upper right-hand corner if the frame is not currently in the favorites (for example, the Unit Main frame).



Select the **Plus** (+) icon to add it. When the frame is added it appears on the user's homepage in the My Favorites area. To remove a page from the favorites, the user can select that page and select the **Remove** (-) icon by the Favorites Menu. You can also maintain the My Favorites area list from the homepage by using the add or remove icons next to the My Favorites area title.

Creating New Users Overview

Controlling users who access the M5 System is one of the primary functions of the M5 System Administrator.

This is an overview of the basic steps for creating a new user in the M5 system.

1. The role for the user must be created. One role can be assigned to many individual application users. The role designates the locations, menus, privileges, Crystal Reports and Department, or Chats within the M5 system. It can also have restrictions placed by the database administrator (DBA) to better secure the M5 database.
2. If you are using Oracle for your database, you need to create the database user for each role. The database user further identifies the different roles within the M5 system. The Database User ID can be a maximum of 8 characters. The password can be up to 30 characters and cannot start with blanks or a number. If you are using SqlServer for your database then database users are not necessary.
3. You can create an application user and assign a role. The application user identifies each individual user within the M5 system. Multiple Application Users can be assigned the same role. For implementation purposes M5 is delivered with an application username of CSI already created. Do not delete or remove the CSI username. Changing the CSI user in will cause problems during the implementation.
4. If you are using Oracle, there must be at least one role with one database user before an application user can be created. The requirements for the number of application users will be dependent on whether you are implementing a virtual private database (VPD). Application user IDs must be unique for each database. So if you implement VPD to create a database for multiple companies each company will require its own unique CSI application user. Therefore, it’s recommended that you implement the following structure: CSI is used for company 1, CSI_02 is used for company 2, CSI_03 is used for company 3, and so on. This also applies for any other application user who will be allowed to access multiple companies.

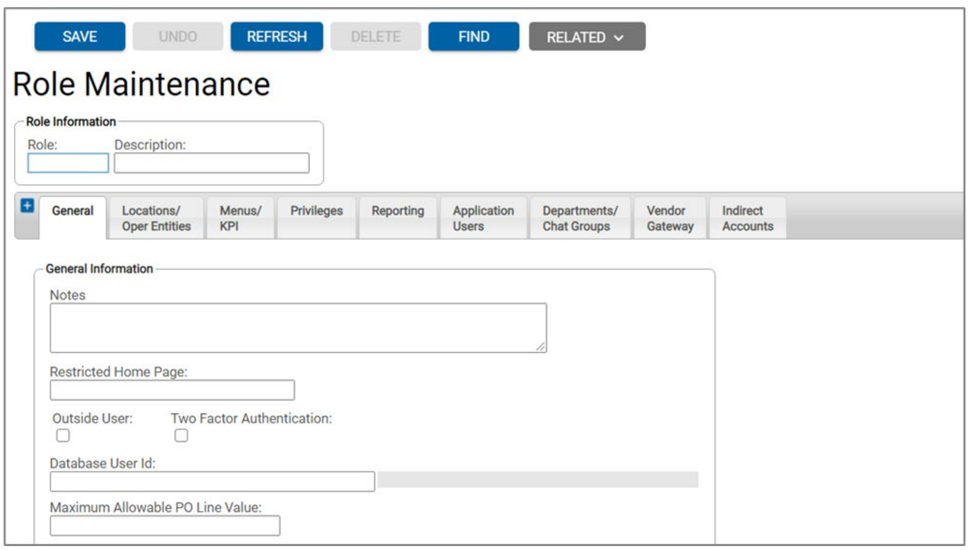
Section 3. Role Creation and Maintenance

As we discussed in the Creating New Users Overview, roles play a central part in defining users of the M5 system. They are the foundation records that Users are built on. The next sections address the details of Role creation and maintenance and illustrate how critical it is to understand the steps required and the sequences to follow when creating and maintaining them.

Before creating a role some preparation steps are necessary. Primarily these involve the creation of groups for locations, operational entities and customized menus with field restrictions. These groups and their dependencies were discussed during your Jump Start Training sessions.

General tab

Open the *Role Maintenance* frame. From this frame you can create a new role or modify one already in the system. The **General** tab information displays.



Create a New Role

To create a new role, select the **Role** field and enter a new role id. It's helpful to style the id in a way that is easily associated with the employees you anticipate assigning to this role such as mech for mechanics.

Your company may already have common abbreviations for various groups that could also be used in this situation. Press tab to move to the Description field, the *Action Required* window opens.

Select **Create** to create the new role. Next enter the data for any of the remaining fields on the **General** tab, as applicable (for example, **Description)**.

The **Restricted Home Page** field allows you to enter a specific home page for Application Users assigned to the role. If a value is entered here it overrides any value set at the App User level and does not allow them to change their individual home page.

Two Factor Authentication can be activated by using the *M5 Parameters* frame. If the **Email_By_Role** value is chosen and the checkbox is selected, as users attempt to log in, the system sends the appropriate email address an authorization number.

Users only have one chance to enter the code. If it is incorrect, it will have to be re-entered. Dashes must be included.

Users will also only have 10 minutes to enter the code in the frame that is presented (unable to use the same code in a different one, should you try to log on again, a new code is generated).

If the user does not enter the correct code in the allotted time, they will receive a code expired notification on-screen and will be required to attempt to log in again (subsequently will be given a new code).

Part Request Approval Amount field:

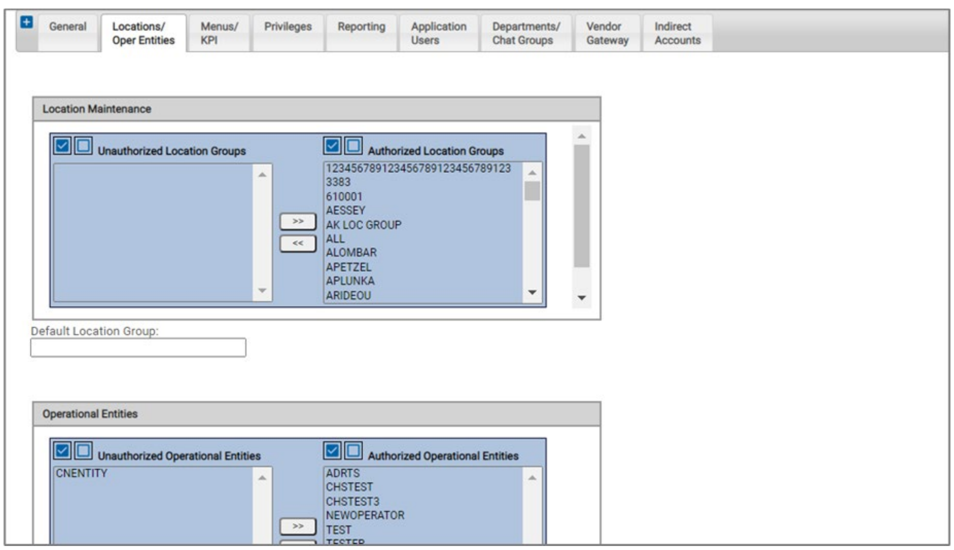
- If the Part Request Approval Amount is left blank - No restrictions will be needed to approve part requests.
- If the Part Request Approval Amount is entered as 0 (Zero) - All part requests will require an approval for this role.
- If the Part Request Approval Amount is entered as a dollar value - Any part requests total exceeding this value would require an approval.
- Works in conjunction with the APPROVE PART REQUEST and APP OWN PART REQUEST privileges.

Commercial Request for Service Approval Amount field:

- If the Commercial Request for Service Approval Amount is left blank - No restrictions will be needed to approve commercial requests for service.
- If the Commercial Request for Service Approval Amount is entered as 0 (Zero) - All commercial requests for service will require an approval for this role.
- If the Commercial Request for Service Approval Amount is entered as a dollar value - Any commercial requests for service total exceeding this value would require an approval.
- Works in conjunction with the APPROVE SVC REQUEST and APP OWN SVC REQUEST privileges.

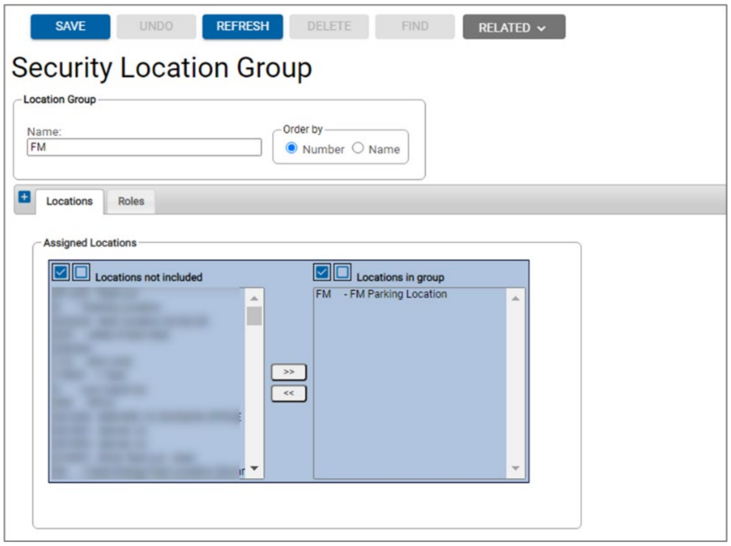
Locations/Operational Entities tab

On this tab, you can assign any **Location Groups** or **Operational Entities** that apply to the specific role. These are generally used as additional system security measures to ensure users are only accessing locations and parts of the system that pertain to their job function.



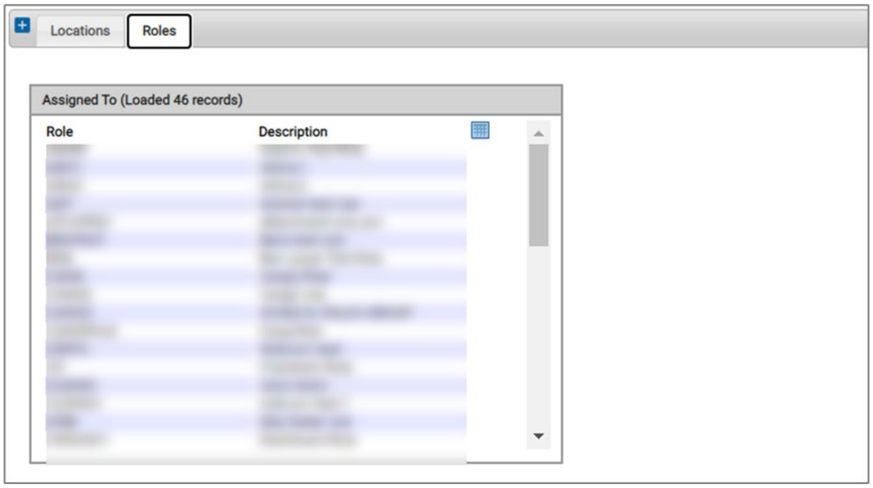
Location Groups

The *Security Location Groups* frame defines a group of locations or a cost center. The security **Location Group** is assigned to the role. If a location is added or deleted from the group, it becomes effective for all users within that group. The location group should be created keeping in mind what functions the users will be allowed to do within each location (for example, Shop Managers can only be allowed access to certain locations).

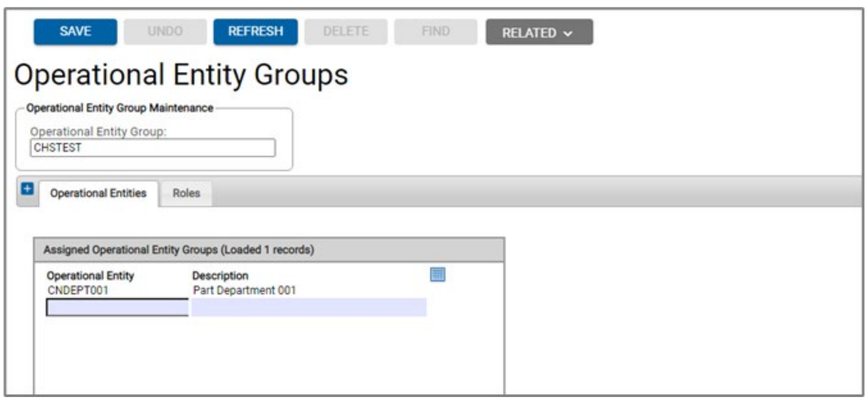


Complete the steps to create a **Location Group**.

1. Open the *Location Groups* frame.
2. Enter the location group **Name** and press tab. An *Action Required* confirmation window opens. Select **Create** to create the new group.
3. The column on the left shows locations that are not included in the group. The column on the right lists locations that are in the group.
4. The column for locations not included will show all locations. Double-click on the location or select the location and then select the **>>** button. You can hold down the *CTRL* key and select multiple locations then select the **>>** button. To select all locations, select the check mark box hen select the **>>** button.
5. To remove a location from the group, highlight the location to be removed and select the **<<** button or just double-click on the group name.
6. Users can be added to the Location Group by selecting the **Roles** tab.
7. Select the roles that belong to the locations you want to include in this group. When you have placed all the locations in the group, select **SAVE**.



Operational Entity Groups



Operational Entity Groups define a group of operational entities or locations. An operational entity is a separate and distinct work group.

The grouping can be done by job functions at the same location or by separate physical locations.

It is used in the *Unit Availability* module.

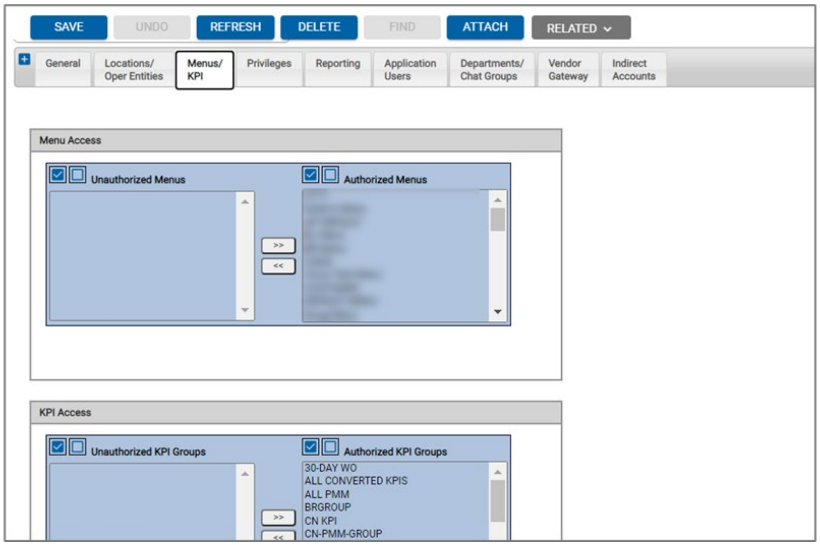
The operational entity group is assigned to the database user. The database user is different from the application user and performs a specialized function that we will discuss later in this manual.

If an operational entity is added or deleted from the group, it becomes effective for all users within that group. The operational entity group should be created keeping in mind what functions the users will be allowed to do within each operational entity.

The selections for **Location Groups** and **Operational Entities** can be added and deleted on this frame by selecting the choices and using the appropriate arrow buttons or double-clicking the selection to move it onto the desired list.

Menus/KPIs tab

On the **Menus/KPI** tab you can assign any custom menus from *Menu Maintenance* as well as KPI Groups that the role should have access to. See the *KPI Groups* frame for more information about setting up these groups



Menu Maintenance

Customizing menus in the M5 System allows the System Administrator to control which menu functions the end user can access. They can be limited to very specific fields within certain frames. This approach also helps the end user to navigate efficiently through the M5 System. The **Menus/KPI** tab on *Role Maintenance* is where you add and remove menus for your roles.

Use the Current Node hyperlinks to add new menus, folders, frames, links, manage security templates, rename folders, or delete items.

Creating Menus

When you first implement your M5 System you will need to create your own menus. M5 is delivered with a *Sample Menu* for your reference.

Do not modify the *Sample Menu*. It is there for your reference and it is a great resource. If you modify it, you will lose the references it contains. As a System Administrator in the *Menu Maintenance* frame you will have the rights to modify it. As you begin your work creating menus double check your updates before saving.

Menu Maintenance contains some additional elements in the columns to the right of the folder names and at the right edge of the frame.

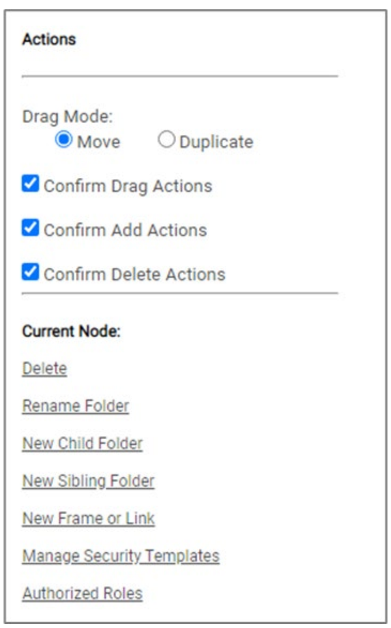
In the **Authorization Group** column, select the checkbox so that the menu appears in the list of menu items on *Role Maintenance*. This allows you to control access to the menu according to role.

Custom if selected, allows the entire menu structure under the folder to be assigned to another menu.

The Security levels can be set as *Read-only*, *Update*, or *Full*.

Security Templates can be assigned that further restrict field access rights.

Reauthenticate on Save requires the user to enter their password again prior to updating the record on that frame.



The **Actions** section controls what happens when you add or delete folders by selecting an action or by dragging a folder from one menu to another with your mouse.

Current Node indicates what actions are available to you based on your current location on the menu folder tree.

To begin creating a menu, select the **ROOT** folder at the top of the tree. Notice that the **Current Node** indicates **ROOT** and the *New Child Folder* is the only option highlighted.

Complete the steps.

1. Select *New Child Folder*. In the *Create Folder* window, name your new menu folder. Select **OK**.
2. Your new menu folder appears at the bottom of the tree. Select it and notice that the **Current Node** options change.
3. Select *New Child Folder* again under the **Current Node** options. The *Create Folder* window opens where you name your new folder and select **OK**.
4. The **Plus** (+) mark now appears by your menu folder, select it to open the folder and see the new *Menu One* folder.
5. If you anticipate assigning the entire menu to a user, select the **Authorization Group** button to check that selection.
6. Now you can add some frames to the new *Menu One*. Select it and select *New Frame* or *Link in the Current Node* choices.
7. The *Add New Item* window opens and you can see the list of every frame that is available in the system. There are currently over 1200. The name, description and type is shown as well as the presence of any Security Templates available on the frame. On this page Dashboard Duplicator has a Security Template available. There is also a **Search** field where can look for a specific frame by name.
8. Select the Dashboard Duplicator and you will see the confirmation notice that it is added to the *Menu One* folder. Select **OK** to close the pop-up and stay on the list to select another frame. When you are through choosing frames select the **X** to close the window.
9. Notice the attributes that have been assigned to the frame by default. There is a roll-over tool on this window that will tell you what each button is for. In this frame it shows.
10. Full access rights to the new frame. Roll your cursor arrow over each of the buttons and you will see the descriptions appear. Notice also that the **Current Node** options now have **Manage Security Templates** highlighted since one is available for this frame.
11. Select the **Manage Security Templates** link. Select *New Template*, enter the **Name** of your choice, and select **OK**.
12. The new template frame opens showing the frames that it controls. By default all the frames are added as Updatable but the ones below are set to illustrate how you might want to customize them. In this case the option Radio screen is hidden, **ReplaceDash** is read-only and **VenNumberDesc** can be updated. Notice also that the **Delete** action is not highlighted. These template items cannot be deleted. Marking them as **Hidden** effectively deletes them from the user’s view. If the field is a required field, do not mark it as hidden.

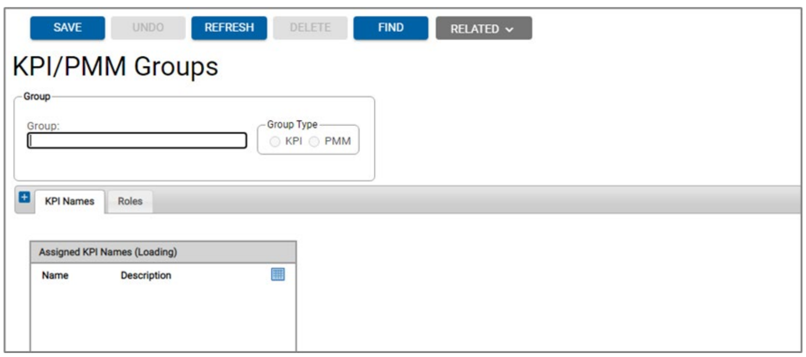
13. Select *Menu Maintenance* to return to the main frame and view your menu folders.
14. If you decide that you need to delete a folder from the menu tree select the folder and select *Delete* in the Current Node choices.

KPI/PMM Groups

KPI's are Key Performance Indicators and PMMs are Performance Measure Monitors. KPIs are indicators of current activities in M5. PMMs are trend indicators. The Performance Measure Monitor is an optional module and it does require an additional licensed.

KPI and PMM groups are added and maintained on the **Menus/KPI** tab. PMMs are listed alphabetically with the KPI Group names.

Before the KPI/PMM's can appear on this assignment group list, they need to be created in the *KPI/PMM Groups* frame. Careful planning prior to completing the creation of these groups will save you considerable maintenance in the future. After you are ready, open the KPI/PMM Group frame.

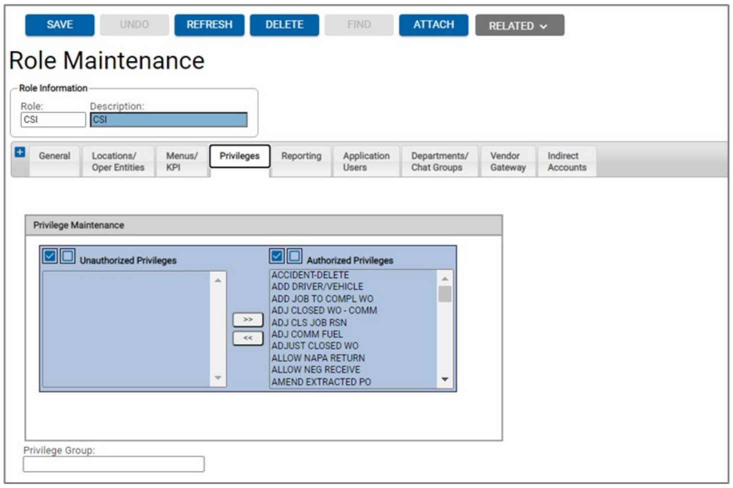


1. To create a new group, enter the KPI **Group** name you are creating and press tab.
2. Select **Create** to create the new group. Select the **Group Type**, *KPI* or *PMM*.
3. Select the **Name** field to select the KPI/PMM to add to this new group.
4. From the KPI List of Values, select the KPIs you want in this group.
5. Select the **SAVE** icon.

Privileges tab

The **Privileges** tab is perhaps the most important aspect of *Role Maintenance*. M5 uses role privileges to determine much of what users with the role can and cannot do within the system.

For more information on specific role privileges and what they do, see the *Role Privileges Table* guide.



Reporting tab

The **Reporting** tab allows you to assign any **Printer Groups** or **Report Groups** that the role needs for use with Crystal Reports.

The **Reporting** tab is used to manage the process of producing reports from the Crystal Enterprise reporting system. Crystal Enterprise is covered in full detail later in this manual. In the *Role Maintenance* section, there are three group components to be familiar with, **Printer Groups**, **Report Groups**, and **Adhoc Groups**. Select the **Reporting** tab in *Role Maintenance*. Here you see three of the familiar *Authorized/Unauthorized Group* frames: **Printer Groups**, **Report Groups,** and **Adhoc Groups**.

From this frame you can add or remove any of the existing group types from authorization on the role you have selected.

Printer Groups

Each role must have a printer group assigned in order to be used in Crystal Enterprise.

To create a new printer group, complete the steps.

1. In the **Name** field enter your new group name and press tab. Select **Create** to make the group.

2. Select the **Role** field to see a list of available roles. Select the desired role to select it, and then select **SAVE** to update the new Printer Group record.
3. Select the **Printer** tab to designate a printer for this group. Select the **Printer** field and a list of available printers appears. Select the desired printer to select it and then select **SAVE** to update the Printer Group record.

Now you have a new printer group with an assigned role and a designated printer.

To delete a printer group, complete the steps.

1. Enter the printer group to delete or select find.
2. Select the **DELETE** button on the toolbar. A confirmation window appears.
3. Select **Delete** in the confirmation window.
4. Select the **SAVE** icon.

Report Group

Report Groups are used with Crystal Enterprise for any scheduled report that is produced for more than one user. Instead of each user running the report a Report Group is created.

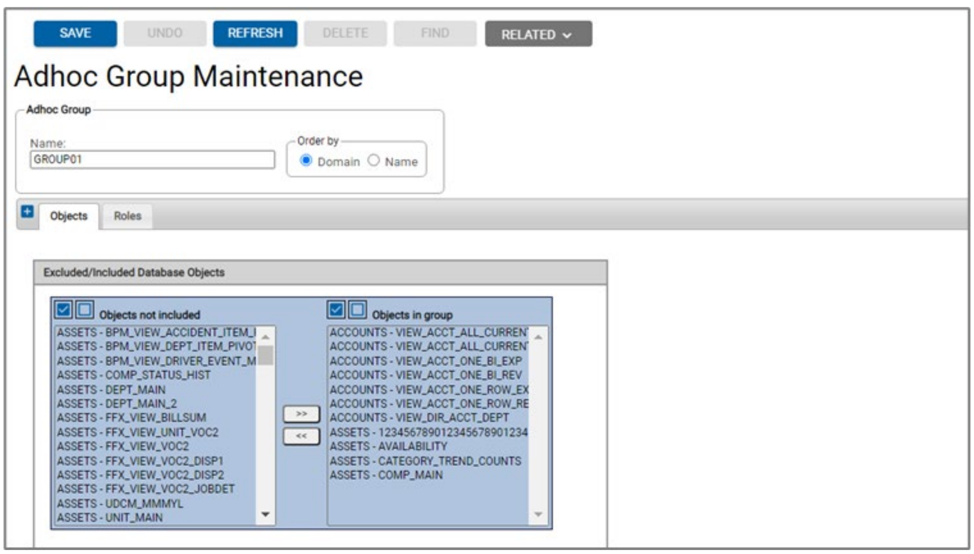
When the report is produced it is stored in each user's bin on their *Home Page*. However, the user running the report also retains the option to keep the report private or send it to the other users.

The report group is assigned to the Role. To create a Report Group, open the *Report Group* frame and scroll to the bottom of the list. Select the empty field and enter your new **Report Group** name. Select **SAVE**.

The new group will be added to the list and a new empty field is added at the bottom. If any changes need to be made to the **Report Group** name, it must be deleted and re-created.

To delete a report group, select the report group name on the list to select it. Select the **DELETE** button on the toolbar. Then select **SAVE** to update the report group list.

Adhoc Groups



Adhoc Groups define a group of data views. Your database contains many tables. A view of the data may be thought of as a picture of certain portions of the tables in your database. The view can be designed to include or exclude portions of the tables depending on the purpose of the users who will be viewing it.

The Adhoc Groups consist of database Objects and database Domains. In the database structure Objects are organized into Domains. A full discussion of Objects and Domains comes later in this manual but for the purpose of Role Maintenance, objects and domains are used to define the views and the views make up the Adhoc Group.

These groups are used in the *Adhoc Reporting* module. The data sources for the Adhoc reports are views of the M5 data. The *Adhoc Group Maintenance* frame defines which views the users can view and report on.

Complete the steps.

1. When you first open the frame it is empty. In the **Name** field you can enter the Name of a new Group if you want to create one or you can double-click to open the list of existing Groups.
2. Enter new **Name** and tab to create it, select **Create**, and then **SAVE** to update it.
3. Double-click **Name** to display the list of existing Adhoc Groups and then double-click the **Group** name to display the objects it contains.
4. After the list of objects is displayed you can exclude or include the objects for the group you are working on. When the list is complete, select **SAVE** to update it.

Application Users tab

The **Application Users** tab gives you the ability to view the Application Users currently assigned a specific role. Each record displays in read-only format and contains the **Application User** id, their **Name**, **Division**, **Phone** number, **Disabled**, and **Expires** information.

Department/Chat Groups tab

The **Department/Chat Groups** tab allows you to manage and assign any **Department** groups or **Chat Groups** to the role. To assign a group, select the group to highlight it, and then select **>>** to move the group into the **Assigned** column.

The **Disable DAF for Reports** checkbox allows users to run any reports regardless of DAF settings.

Select the **Department/Chat Groups** tab on your *Role Maintenance* frame to view the assigned groups for the role you have selected. The **Department Groups** are used for an additional level of security called *Department Access Function (DAF)*.

They are also used for *Customer Data View Users*. The Department Access Function (DAF) provides an additional layer of security at the department level. Similar to Field Security Templates, it controls the user's ability to view or update data on their department's frames.

Security Codes use Department Groups to establish this control and are integrated into the *Frame Maintenance* URL of the corresponding frames to regulate the user's access. As discussed earlier in this section, Departments are created under *Department Main* and detailed in the *Jump Start Guide-M5 System Management Overview* document.

The **Chat Groups** are used for creating message groups that can send messages under the **Message Menu** on the top Menu bar.

These groups may be assigned or authorized by double-clicking the group name or selecting it and by using the **>>** or **<<** buttons.

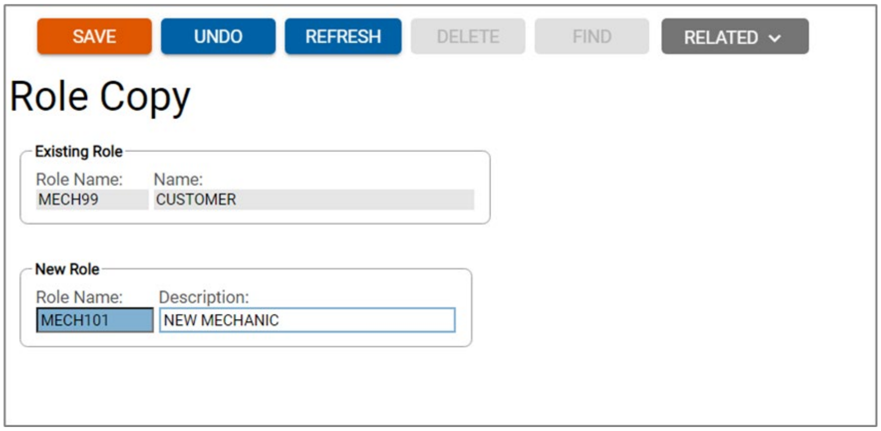
Indirect Accounts tab

The **Indirect Accounts** tab allows you to authorize or unauthorize **Indirect Account Groups** for a specific user role. Use the **>>** or << buttons to move groups between the two columns.

Role Copy

A useful way to create a new role is to use the *Role Copy* frame to create a new role from an existing role.

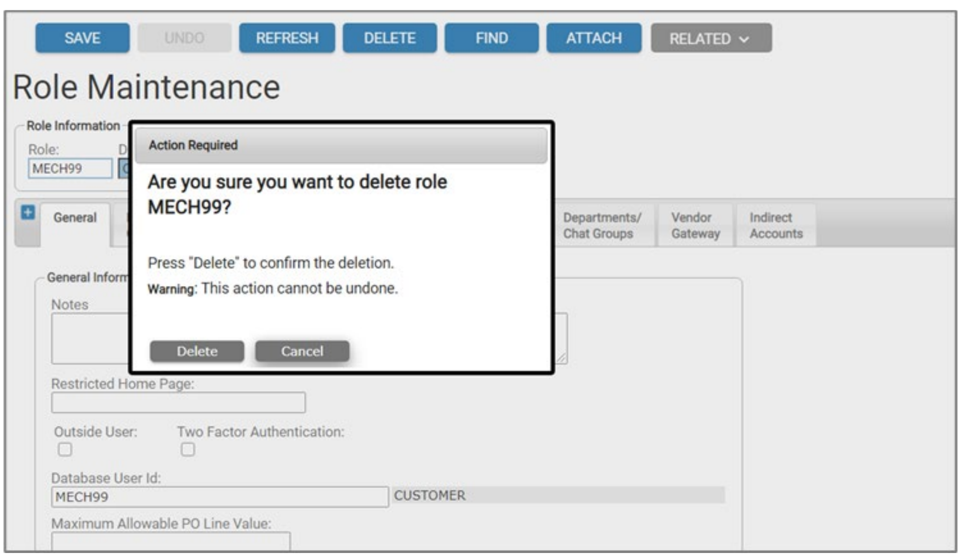
Use the **FIND** button to select the existing role you want to copy. Then input the **Role Name** for the new role and the **Description**. Select **SAVE** to create the role. This is a useful tool for creating new roles but be sure to review all the fields on each tab of the new role to ensure that you have all the new details correct.



Delete a Role

From the *Role Maintenance* frame select the **Role** you want to delete or select **FIND**. Select **DELETE** on the tool bar. You will receive an *Action Required* message to confirm deletion.

Select the **Delete** button to confirm. You will not be able to delete a role if it is in use elsewhere in the system.



Customer Data View Users

Complete the steps to use customer views.

1. In the *Role Maintenance* frame create the **Role**, include a **Description**, and make sure the **Outside User** checkbox is selected.
2. Under the **Departments/Chat Groups** tab you also need to add the *Authorized Departments* this outside customer is allowed to use.
3. If you have not already created the **Department Group** you need to do that before creating the role.

Departments are created on the *Department Main* frame and that process is reviewed in detail in the *Jump Start Guide-M5 System Management Overview* document you received during the implementation of your system.

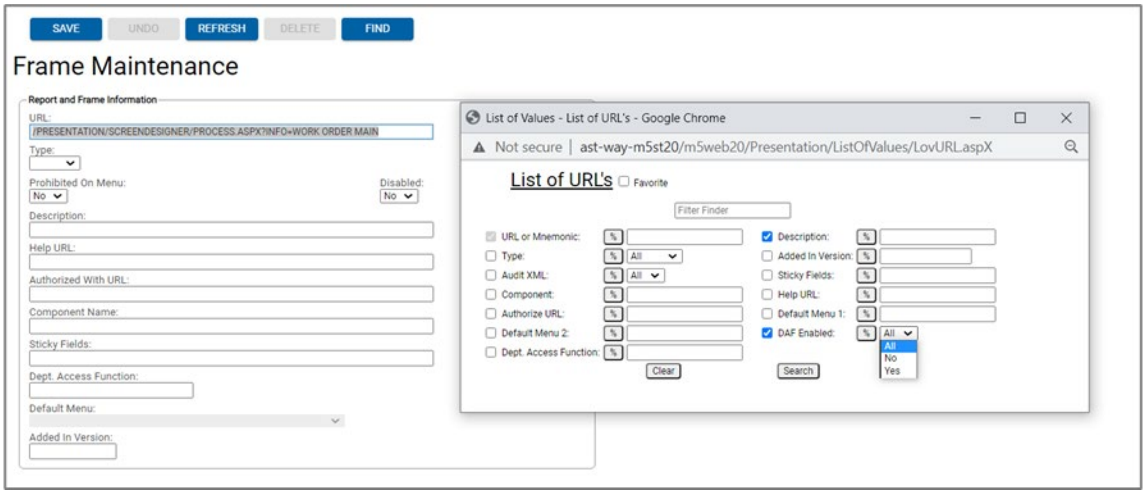
DAF Code Maintenance

The *DAF Code Maintenance* frame is used to manage and create DAF codes. To add a new code scroll to the bottom of the list and enter the new **Code** name and **Description** in the empty row. Select **SAVE** to update the record.

Note: There is a **Disabled** checkbox for each code. This can be used to block usage of the code since it cannot be deleted after they are used in a data record.

Frame Maintenance for the DAF Code

After the new DAF Code is created the next step is to assign it to a specific URL in the *Frame Maintenance* frame. The URL must be designated as **DAF Enabled** in order to do this. Open the *Frame Maintenance* frame and double-click in the **URL** field to open a search window. In the *List of URL's* window, select the **DAF Enabled** checkbox and set its value to *Yes*. Select the **Search** button.



From the list that is produced, double-click to select the **URL** for the new DAF code.

Note: The list displays **Y** in the **DAF Enabled** column on the *List of URL's*.

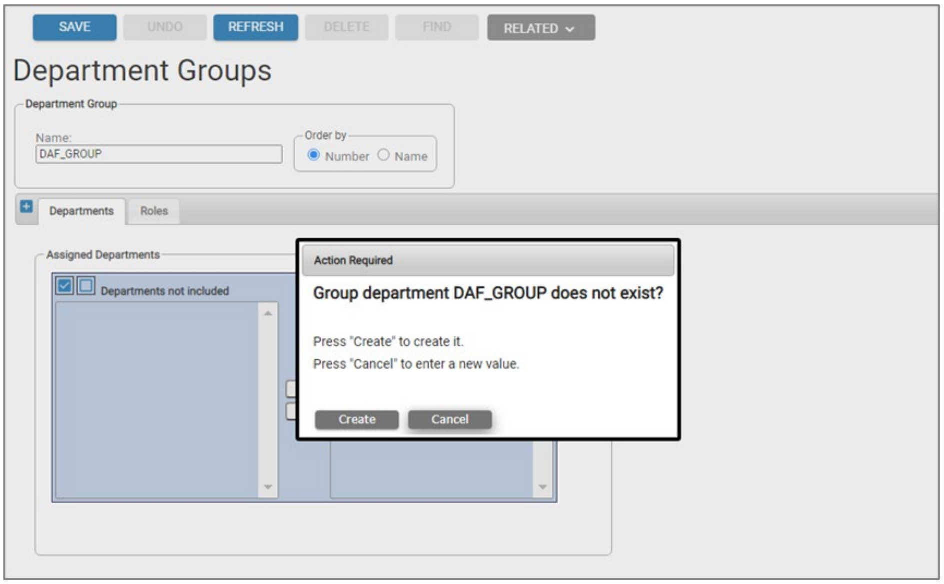
Now with the URL loaded into Frame Maintenance, double-click in the **Dept Access Function** field and to open the list of available DAF Codes that can be applied. Double-click on the code you want to use.

The new code name will be added to the **DAF** field. Select **SAVE** to update the record. Now with the new **DAF Code** created and assigned to URL the next step is to add it to a new Department Group.

Create New DAF Department Group

Open the *Department Groups* frame and enter the department group name. Select **Create** to create the new department group. Select **SAVE** to update the record.

Double-click on the department name on either side of the window to include or exclude them from *Department Group*.



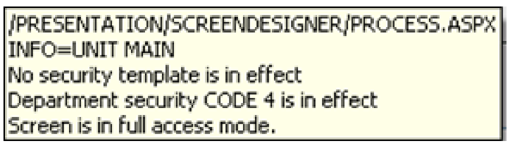
Department Group Level Security

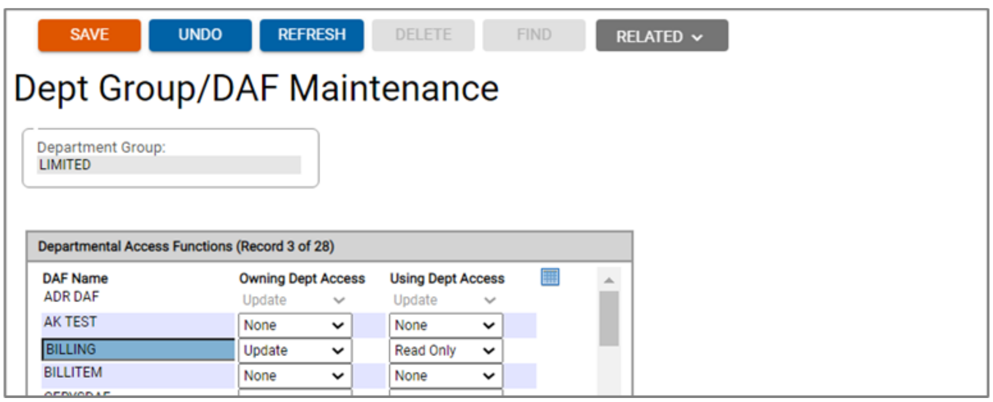
The *Department Group/DAF Maintenance* frame allows the Department Level Security codes to be configured according to each department group. Double-click in the **Department Group** field and select your group. Each Department Level Security code created will be listed and the choices for **Using Dept Access** or **Owning Dept Access** departments are *Update*, *Read Only*, or *None*. In this example for LIMITED, BILLING is set to update for the owning department and read-only for the using department.

Now, the last step is to return to the *Role Maintenance* frame and on the **Departments/Chat Groups** tab find the correct **Role** and add the new **Department Group** to its assigned groups. Select **SAVE** to update the record.

After a frame is enabled with DAF Security, the user receives a message if they try to access a frame that is blocked by the department security code level.

For troubleshooting purposes on frames that have DAF implemented, a message window appears when you move your cursor over the protected field. It will look similar to the one below.





Database Users

If you are using Oracle for the database in your M5 System you will need to create database usernames. SQLServer does not require them. The database user is assigned to the Role and multiple roles can use the same database user id. This reduces the number of distinct database users you have to create and manage.

As part of your implementation planning you should consult with your Oracle DBA and create database users that are consistent in style with the current database username structure. M5 is delivered with a database username of CSI already created.

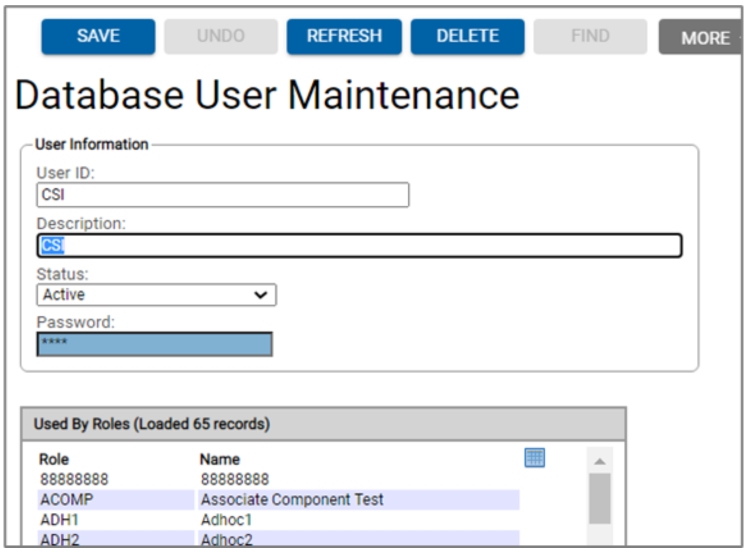
DO NOT MODIFY THE CSI DATABASE USER. It is used for installing and configuring your M5 system.

Open the *Database User Maintenance* frame to create and maintain the User ID. To create a new id enter the new name in the **User ID** field and press tab. Select **Create** in the *Action Required* window and then enter a **Description** and a **Password** for the id.

If the password you select does not meet the system security requirements you will see an error message.

The password must use at least two lower case letters, no upper case, no numbers and may contain # $ + = _ . Select back in the password field and enter a valid password and SAVE to update the record.

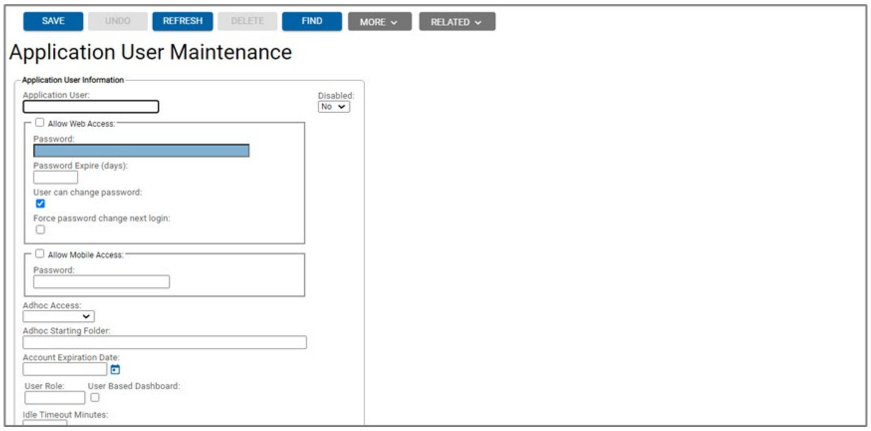
After being created, the database user can be assigned to the **Role** on the **General** tab of the *Role Maintenance* frame.



Section 4. Application User

Application users are the individuals who sign in to the M5 System as part of their job function. Everything they can do in the M5 System must be well defined and assigned to them specifically.

The majority of the application user's capabilities are controlled through application user roles they are assigned in *Role Maintenance*. However, there are some additional items that can be customized after the user id is created. Creating and maintaining the **Application User** id is done on the *Application User Maintenance* frame.



The *Application User Maintenance* frame allows you to create and manage the user accounts for the individuals who use the M5 System as a part of their job function within the fleet organization. It is important that system administrators take the time to carefully define user capabilities and assign them accordingly.

Proper management and configuration of **Application User** ids means controlling user access to the parts of the system they need to perform their jobs while preventing access to parts of the system that are not within the scope of their position. Through the *Application User Maintenance* frame, you can accomplish this by properly defining their roles and security rights.

The majority of the application user's capabilities are role-based. You can create and configure application user roles and edit privileges on the *Role Maintenance* frame. However, there are some additional items that you can customize at the user level after you create the **Application User** id.

Application User Information

Application User - The user name that the assigned user uses to sign in to the M5 System. This field has a limit of 60 alphanumeric characters.

Allow Web Access

M5 is a web application that runs in a browser, select the checkbox to allow the user web access to the system.

Note: When SAML Authentication is in use, the following values are ignored and should not be set on this frame:

- **Password** - Password criteria depends on the system flag settings.
- **Password Expire (days)** - If passwords expire, enter the number of days for which they are valid.
- **User can change password** – Select the checkbox to allow the user to change their own password.
- **Force password change next login** – Select the checkbox to force the user to change their password the next time they sign in.

Allow Mobile Access

To allow mobile access through a handheld device for MobileFocus, select the checkbox and enter a **Password**.

Adhoc Access

Select the level of **Adhoc Access** for the user:

- **None** – No access.
- **Run Reports** – The user is allowed to only run reports, not create them.
- **Create Reports** – The user is allowed to create and run reports.
- **Report Admin** – The user is allowed to create and run reports as well as have certain administrative rights on the *Adhoc Query* frame.
- **Adhoc Starting Folder** - Allows each user to have a distinct starting point in the Adhoc report directory. The value specified will be appended to the value of the M5 Param for **ADHOC_REPORT_PATH**. The path must exist in order to specify this value this frame.
- **Account Expiration Date** - You can set an expiration date for the user account in this field. You can manually enter an expiration date or select from the **Calendar** icon.
- **User Role** - Enter a valid role from *Role Maintenance* that corresponds to the users position or double-click in the field to select one from the List of Values.
- **Idle Timeout Minutes** - The system will sign out the user after the number of entered idle minutes.
- **Pooled** – Select the checkbox to pool a Crystal Enterprise User.
- **Crystal Enterprise User** - Enter the *Crystal Reports User ID*, if applicable. See *Report User Pool* if pooling crystal users.
- **Crystal Enterprise User Password** - Enter the user password.
- **Crystal Enterprise Output Path** - Enter the output path for the user when they run Crystal Reports.

- **Stylesheet Directory** – You can assign a custom stylesheet directory for the user.
- **HomePage** - You can assign a custom home page for the user.
- **Logon Failures** - Read-only field. Displays the number of failed sign in attempts for the user.
- **Last Logon** - Read-only field. Displays the date and time of the last sign in for the user.
- **Starting PMM Location Hierarchy** - If using PMMs and the user has access, enter the beginning location hierarchy.

Application User Identity

Name - This is a required field. Enter a name to identify the application user.

Unique ID – This is a required field. Each application user must have a **Unique ID**.

Employee No - Associates an application user with an employee from *Employee Main*. Certain functionality in M5 will look to see if there is an employee id associated with the application user as a way of defaulting in that employee id in certain frames, such as *Part Issue Request*. The **Name** field automatically populates and is read-only.

Division - If the application user is associated with certain division within the organization.

Phone – Enter a contact number for the application user, if applicable.

E-mail – Application user email address. If entered, M5 automatically sends emails to the address if this runs any batch processes.

Department – Application user's department. Must be a valid department in M5. For use with the *Screen Designer Unit* control option on *Work Request Query* to search departments or department groups. Depending on the setting, the search functionality will look for the value entered.

Department Group – Application user's department group. Must be a valid department group in M5. For use with the *Screen Designer Unit* control option on *Work Request Query* to search departments or department groups. Depending on the setting, the search functionality will look for the value entered.

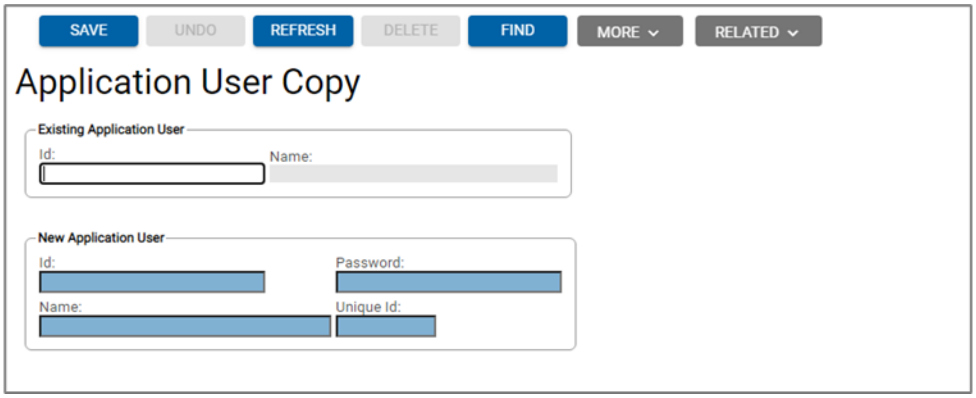
Override Locale – Allows the user to override the user's locale language that is normally set by their browser or query string.

Vendor List

This section only displays if System Flag 5504 is set to **Y**. This functionality pertains to Commercial Work Order security and allows you to limit application users to only see data related to their assigned vendors from this i-frame. When the user enters or otherwise enters a vendor number that is not assigned to them on *Commercial Work Order*, they will receive an error if the entered vendor record is not assigned to them.

Application User Copy

You can use the *Application User Copy* frame to create a new application user from an existing application user. When you use this feature the frame applies the **Existing Application User** information to the **New Application User**. Enter the user **Id** to copy, then the new **Id**, **Password**, **Name**, and **Unique Id** information.



Delete an Application User

To delete an application user, enter the user Id you want to delete, select **DELETE** and confirm the **Delete** action. Keep in mind you have the option of disabling the user Id. There may be an administrative reason to disable it and stop the user's access without fully deleting the account.

Section 5. Crystal Enterprise

There are several programs within M5 that are tailored to those users using Crystal Enterprise. Each of these frames and how to use them are listed below.

Printer Definition

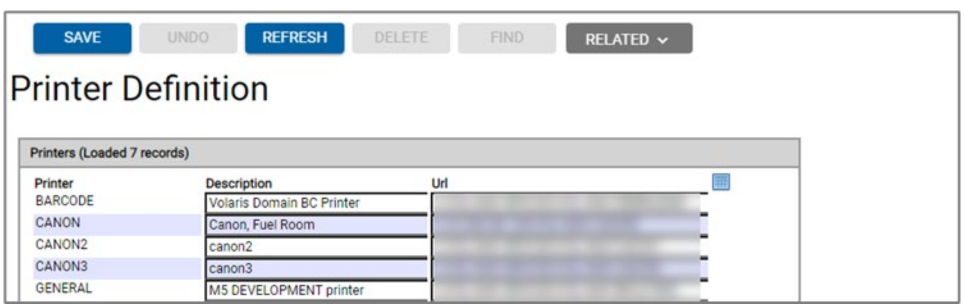
The printer definition is used to create each printer that will be used within M5 and where it is located (by the URL).

Complete the steps to create a new printer on the *Printer Definition* frame.

1. Select the blank row and enter the new printer name in the **Printer** column.
2. Enter the printer **Description**.
3. Enter the **Url** for the printer. You can continue to add more printers, as applicable.
4. Select the **SAVE** button.

Complete the steps to delete a printer definition.

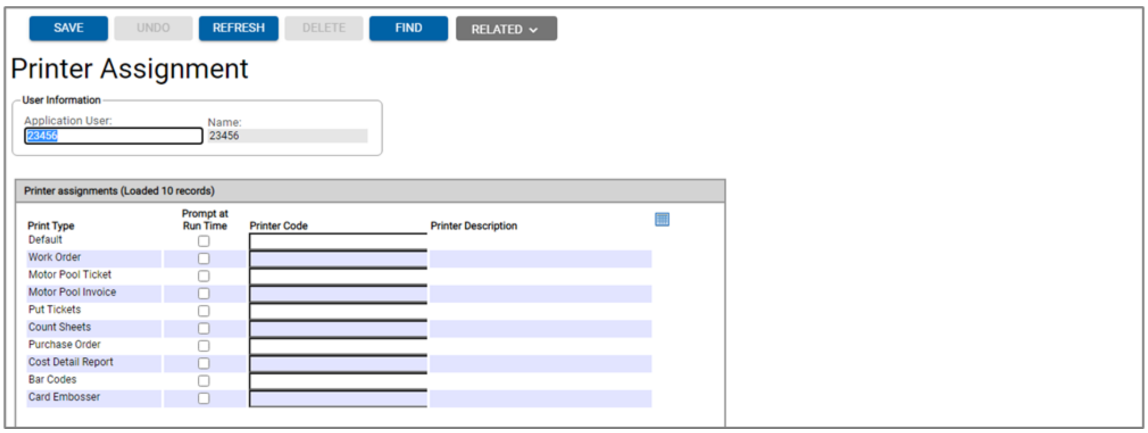
1. In the Printers i-frame, select the **Printer** to delete.
2. Select the **DELETE** button and the printer highlights in red.
3. Select the **SAVE** button.



Printer Assignment

The *Printer Assignment* frame is used to identify each application user, the printer used to print certain report types such as work orders, motor pool tickets, put tickets, and count sheets (parts physical inventory) for direct printing. After you define your printers, complete the steps to create the printer assignment.

1. Open the *Printer Assignment* frame.
2. M5 automatically enters the current **Application User** or you can enter one manually or double-click and select from the List of Values.
3. Double-click in the **Printer Code** field and the list of available printers opens. Select the printer you want to add. The first printer type is the user's default printer. Assign a print code for each printer type on the user's list as needed. The **Print Type** listed are system assigned based on the applications the user has access to.
4. Select the **SAVE** button.



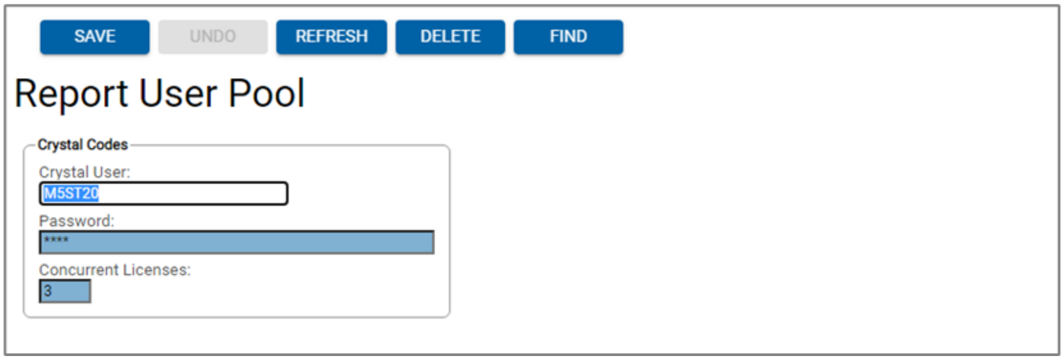
Report User Pool

The *Report User Pool* stores the Crystal Enterprise usernames and passwords to be used if the client has a Crystal Enterprise license that is shared. The *Application User Maintenance* frame includes a checkbox that indicates the pooling of Crystal Enterprise licenses. If the checkbox is selected, pooling is in use. Complete the steps to set up the Crystal User and licenses in the Report User Pool.

1. Open the *Report User Pool* frame.
2. Enter the **Crystal User** name.
3. Enter the **Password**.
4. Enter the number of **Concurrent Licenses**.
5. Select the **SAVE** button.

Complete the steps to delete a **Report User Pool**.

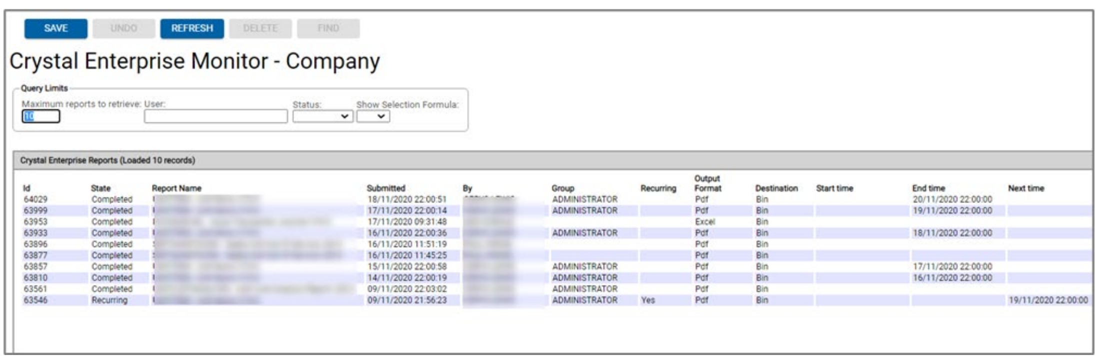
1. Select the **Crystal User** to delete.
2. Select the **DELETE** button.
3. Select the **SAVE** button.



There are two frames that can be used to monitor the status of reports that are scheduled to run automatically. If the report failed to run for any reason it will display on both frames with the cause of the failure listed. Both reports allow the user to enter the maximum reports to retrieve. You can select a specific user and status. The default is for all users and all status types.

Crystal Enterprise Monitor Company

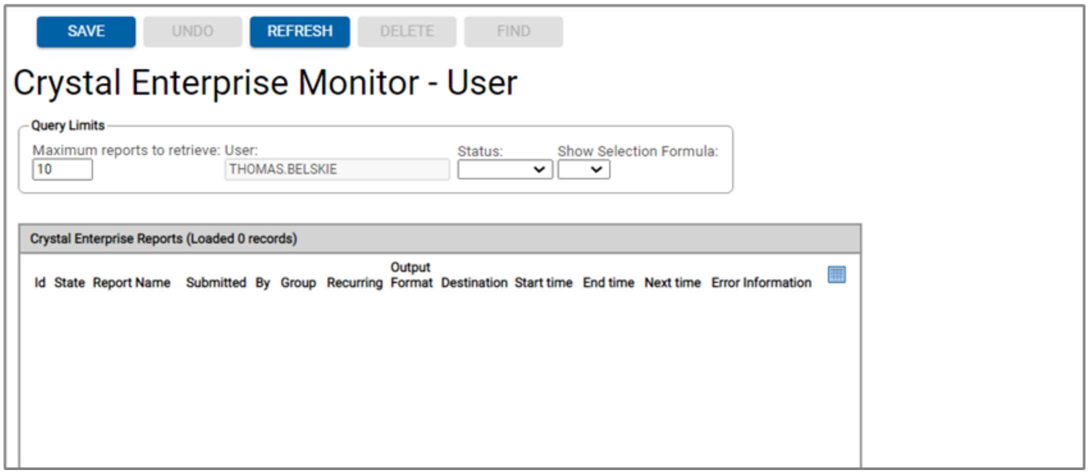
Company displays the reports by company.



Crystal Enterprise Monitor User

User displays reports by the current Application User. The user in this example does not have any reports.

To change the **Maximum reports to retrieve** to retrieve, select the field and enter the new number and press tab. To change the status of the reports shown, select the status dropdown to select *All*, *Executing*, *Completed*, *Pending*, *Recurring*, or *Failed*. Press tab.



Report Log Administration

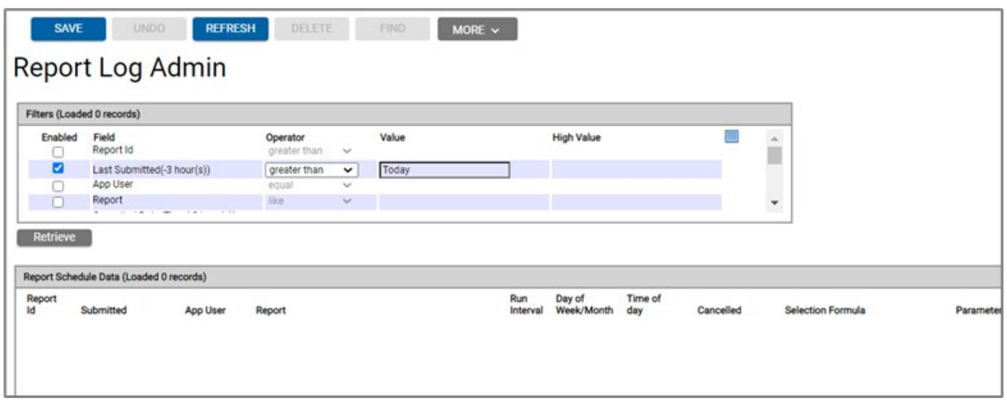
Saved Reports

When AssetWorks delivers updated Crystal Reports they need to be republished in Business Objects XI. This process involves deleting the previous version of the report in order to replace it. If this report has a scheduled run set to execute automatically it is lost in this replacement process. The *Report Log Admin* frame was developed for this process.

This frame allows the user to view all the parameter information for all reports submitted to Crystal Enterprise, not just recurring ones. This frame only queries the captured information and does not reflect the state of the report inside Crystal Enterprise. A link is provided to the *Crystal Enterprise Monitor* frame.

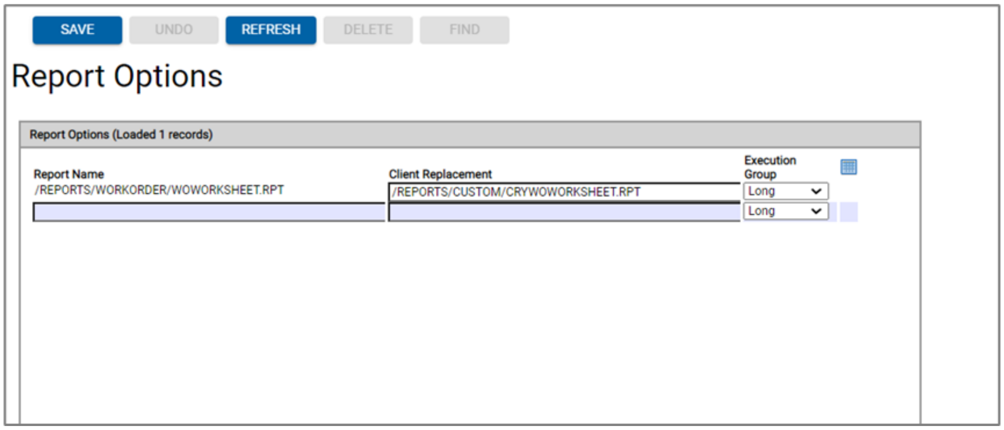
This frame provides the ability to re-establish the recurring reports. After a patch or upgrade is applied the administrator queries the recurring reports in the report log and then selects the **Resubmit all recurring reports to Crystal Enterprise** icon on the toolbar that requests that the reports be rescheduled.

The *Report Log Admin* frame is an M5 administrator frame and access must be restricted to the System Administrator only.



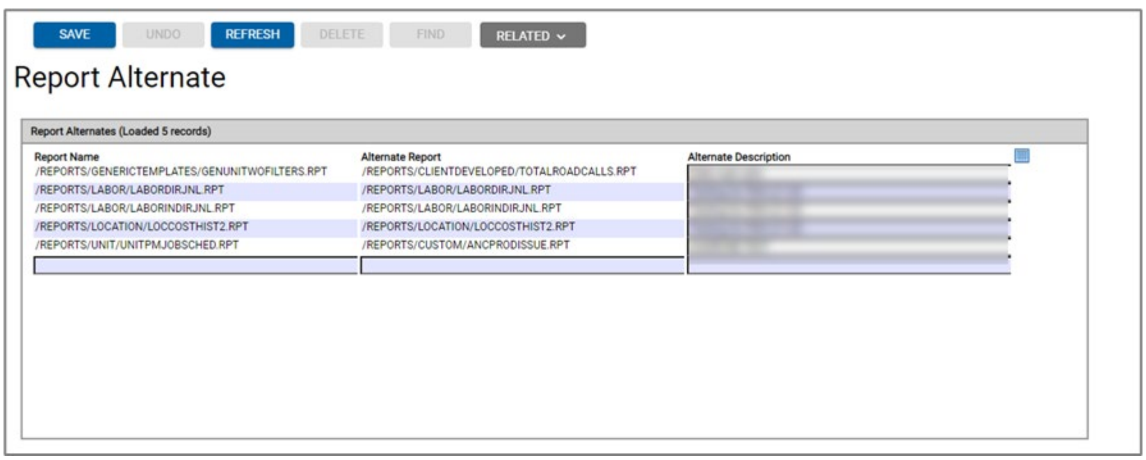
Report Options

Report Options allows the user to replace a standard report with a custom report or an alternative. The M5 report is listed in the report name area on the left side of the frame. The client replacement is listed on the right side of the frame. It can also be used to change the execution group for a report. The choices for the **Execution Group** is *Long*, *Medium*, or *Immediate*.



Report Alternate

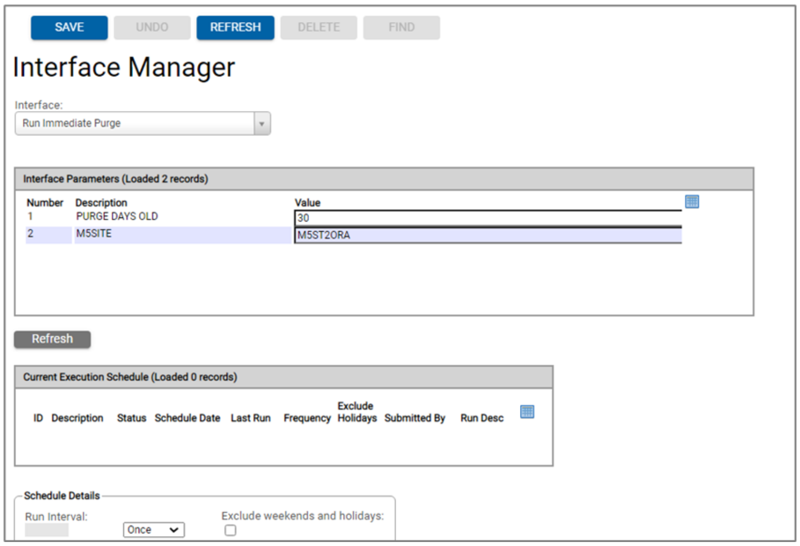
This frame allows the user to change the report name of a custom report. *Report Options* is still needed to say which custom report is replacing the M5 report.



Run Immediate Purge

For customers that print and create reports in run immediate mode, this program helps manage the report in-bin by purging run immediate jobs. To run this program open the *Interface Manager* frame. Enter or select *Run Immediate Purge* from the *Interface* dropdown.

The user determines how often to purge the run immediate jobs from the in-bin using the interface parameters.



System Version

This frame displays the **Current TMS Version** date and time and the **Current Release** version of the updated database tables.

Section 6. M5 Parameters

M5 Parameter Maintenance Frame

For a complete list of M5 Parameters, see Appendix C.

The *M5 Parameter Maintenance* frame is an important frame that displays parameter settings that were made during the installation of your system. It can be very helpful when troubleshooting an issue with the system.

The frame also allows you to view and edit M5 Parameter values within the application itself. To view the list of available parameters, select the dropdown menu and from the following options select: *All Groups*, *ADHOC*, *ATTACHMENTS*, *DATABASE*, *DEFAULTS*, *EDGE*, *EXTERNAL_AUTH*, I*NSTALLATION*, *LIMITS*, *LOCALIZATION*, *LOGON*, *MULTI-CURRENCY*, *REPORTING_SERVER*, AND *USER_PREFERENCES*.

After you make you selection the parameters will load on the *M5 Params* i-frame. To change or edit a parameter select the **Value** field of the parameter you want to change. A description of the parameter and its options appears to the right of the i-frame when you select in the row. **Scope** is not an editable field.

When you are finished entering a value, select **SAVE** to update the changes.

Two fields on the M5_PARAMS table allow you to specify how they want users to sign in.

1. *CE_EMAIL_DOMAIN* specifies the email domain, such as M5assetworks.com. This email domain is ADDED TO or REMOVED FROM the sign on value the user types in when signing on to M5.
2. The **LOGON_DOMAIN_SPECIFICATION** field specifies whether the domain should be added or removed from the value the user types in.

The options are:

- A - Add the CE_EMAIL_DOMAIN value to the user id if a domain was not specified.
- R – Remove all domain specifications.
- N - Do nothing (default). Leave the value as the user typed it.

Example of A

- Application user as created in m5 is johndoe@assetworks.com.
- ce_email_domain is assetworks.com.
- logon_domain_specification is A.
- User types in johndoe / password on the M5 logon page.
- System appends @assetworks.com onto the login value, and logs user in as johndoe@assetworks.com.

Example of R

Using the same user as above:

- If user typed johndoe@assetworks.com as the login name, the system would REMOVE @assetworks.com, making the login user johndoe, and because the user does not exist, user get an invalid logon message.
- Actual use for R would be having users set up WITHOUT a domain specified on the application user, but user login using the domain. M5 then removes the domain so the user can log in successful (for example, if user is set in M5 as jane.doe and user logs in as jane.doe@assetworks.com the system will remove the @assetworks.com portion the user typed in, and log user in successfully as jane.doe).

N treats the value the user types in as the value to be used. It does not alter it, so value typed in must exist as an application user.

M5 Parameter Query Screen

The *M5 Params Maintenance Screen* frame displays critical information on the M5 System. It's a very important frame and is often used in troubleshooting to view technical settings that were made during the installation. No parameters can be changed from this frame. Refer to *M5 Parameter Maintenance*.

The **M5_PARAMS** table contains customizable settings that affect all companies in the database. It contains information about installation directories, machine names and shared directories. It must be configured before M5 is started. The easiest way is to use SqlDeveloper for an Oracle database or Query Analyzer for SQL Server.

For more information please contact M5 Support or consult the *M5 Installation Procedure Install Guide* for more information about the M5 Install and configuring the M5_Params.

Section 7. System Performance

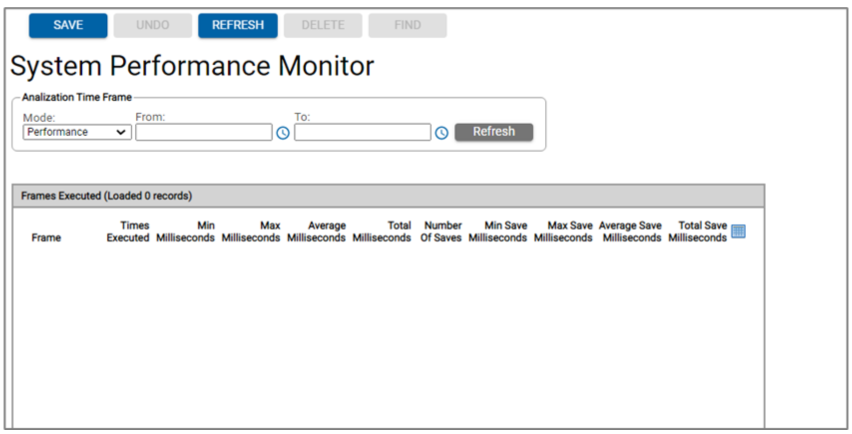
System Performance Monitor

This frame is used to troubleshoot system performance issues. It is used to capture the performance statistics within a given time frame.

For this data to be captured, a setting must be activated on the application server. Since it is recording system activity, it will affect the system performance, so it is recommended that the monitoring be turned off as soon as the troubleshooting activities are completed.

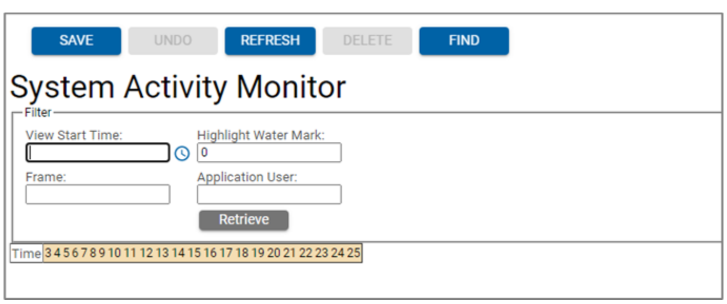
When you open the frame, you need to select the time frame you want to monitor. You can select a **From** and **To** date and time from the **Clock** icon and AM/PM squares, or you can also use the **Now** button to quickly choose the current date and time.

When the range is set, you will see the statistics appear in the columns. Remember to turn the monitoring off when you are through with your troubleshooting.



System Activity Monitor

The *System Activity Monitor* frame should only be used under the guidance of the M5 Installation and Support Team. It requires the activation of the Record_Performance parameter.



Active User Query

This frame displays the application users currently logged into M5 and the last frame they accessed. This is an administrator level frame that shows all active users in M5. It is not company specific.

If the **?** appears in the **User** column, it means that a user went to the logon screen but never logged on. Multiple rows of the same user means they are logged in multiple times. This can happen when they do not close the previous session or something happened that prevented them from being able to log off normally. If the browser crashes or power is lost to the computer this will happen.

View Log Files in M5

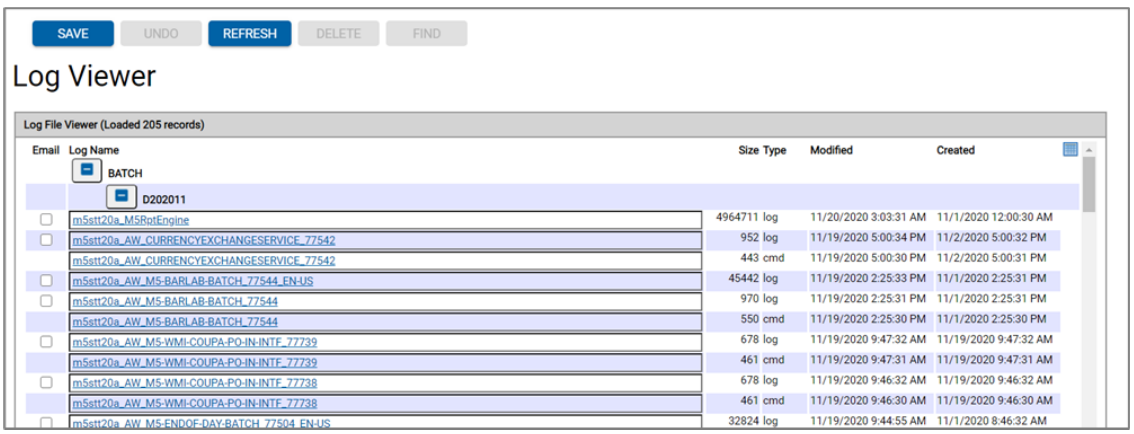
The *Log Viewer* frame allows for the viewing of log files within the M5 application. Log Viewer functionality stores logs in a standardized location and the new frame allows users to view, download, and Email log files from M5.

Logs are broken into the following sections:

- Batch
- Business Components
- Interfaces
- M5Web
- Other

To view a log file, select the **Plus (+)** icon next to the section you want to view. The list of available files display. Select the link to download and view a specific log file.

To email a log file, select the checkbox in the **Email** column. Enter an **Email To** and **Email From** email address, and **Subject** of the email. Select the **Send Email** button.



For more information on the setup and configuration for this frame, see the *Configure Log File Viewer QRG* for more details.

Section 8. Security Logging

Security Logging allows the System Administrator to select a security event and log its activity. M5 comes with a standard list of security events that can be activated and set for monitoring. After the events are selected they can be viewed as they occur.

There are two frames used to achieve this. First the **Events** must be selected *in Log Event Maintenance* then they can be viewed in *Log Event Viewer*.

Log Event Maintenance

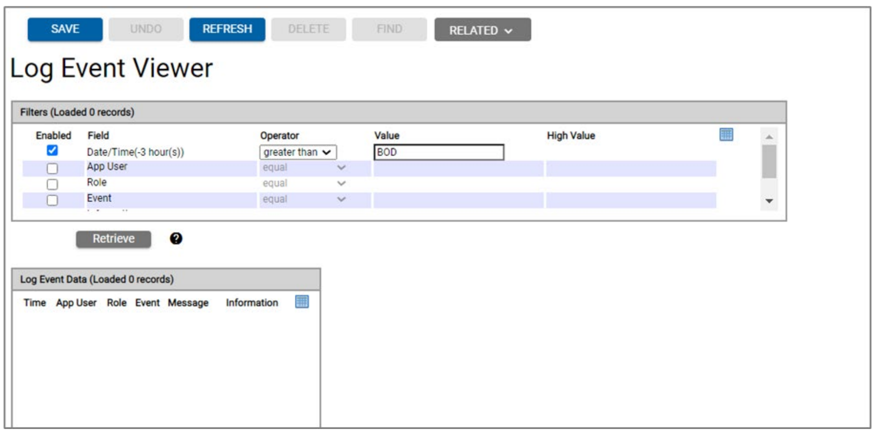
The *Log Event Maintenance* frame is used to activate logging of security events. In the **Log** column select *Y* (Yes) or *N* (No) to turn logging on and off for the event. The events that can be logged have been created by AssetWorks and cannot be modified by the customer.

Log Event Viewer

After the event is set to be logged, it can be filtered and displayed using the *Log Event Viewer* frame. Filtering allows you to view only records matching a certain criteria. One filter must be selected to retrieve log information. Select the **Enabled** checkbox to select your filter and configure the numeric operator and values to match your desired criteria. Select the **Retrieve** button to display the event matching your selections.

The *Log Event Data* i-frame displays records that match your filter.

Note: There is no automated purge process for the log event table. To prevent the tables from growing too large rows need to be manually cleared periodically by your DBA.



Section 9. Table Auditing (for Oracle Clients only)

Numerous transactions are already audited in journal tables whose data does not change after the record has been created. After a transaction has been written to one, it remains forever.

Examples:

- **meter_jnl** - Any change to a unit's meter.
- **part_jnl** - All inventory transactions, including creation of new parts and cross-references, issues, returns, order requests, orders, receipts, transfers, adjustments to quantity or price, and merges of one part number into another.
- **unit_capital_jnl** - Changes to a unit's capitalized value, whether manually or from work orders.
- **unit_status_hist** - Changes to a unit's status or status-triggering dates, such as in-service date.
- **o_labor_chg**, **o_part_chg**, and **o_comm_chg** - Charges to work orders.
- **acc_lab_chg**, **acc_part_chg**, and **acc_comm_chg** - Charges to indirect accounts.
- **f_comm_prod_chg, f_unit_prod_chg** - Fuel charges to units.

Some tables that look like transaction tables can be modified through the application so they cannot be relied upon as an audit trail.

For example, **unit_asgn_hist** is a table that keeps the start and end dates of unit associations to owning and using departments, but users can change these dates through a frame. If in doubt, consult AssetWorks to confirm whether a particular table's records do not change once created.

For tables that are not reliable journal tables, a standard M5 table called **audit_table_column** contains the audit trail data. It can be customized on the Table Column Audit frame.

For purposes of the audit record, the updating session is the one running on the application server or batch server. In other words, the host is not the user's PC running M5 but is the server running the application components.

Table Column Audit

The *Table Column Audit* frame is used to designate the columns that will be established or removed from the audit data. The *Table Fields Audit* section allows you to enter the **Table Name** to audit. After the table is entered the *Table Columns* i-frame displays.

The checkboxes control if you wish to see when the data in the field was:

- **Add?** – When data is added.
- **Delete?** – When data is deleted.
- **Update?** – When data is modified.

Select **SAVE** when you have defined the data columns for your audit.

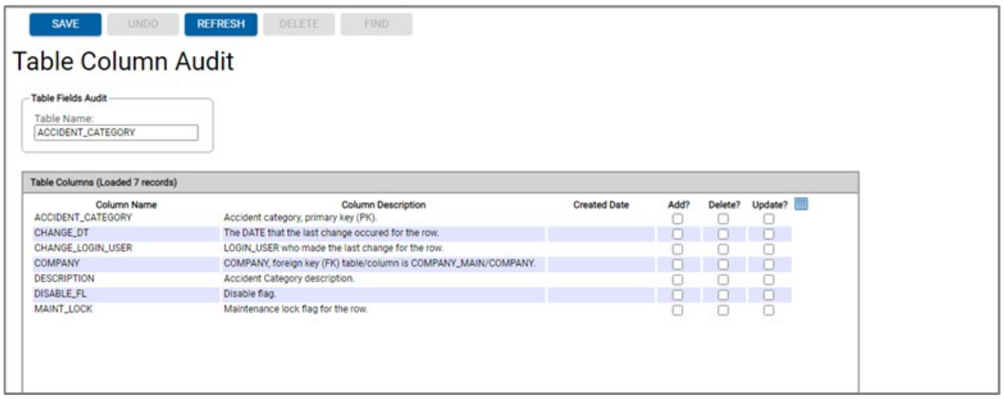


Table Column Audit Query

After you define your table audit Columns you can use the *Table Audit Column Query* frame to display the audit records.

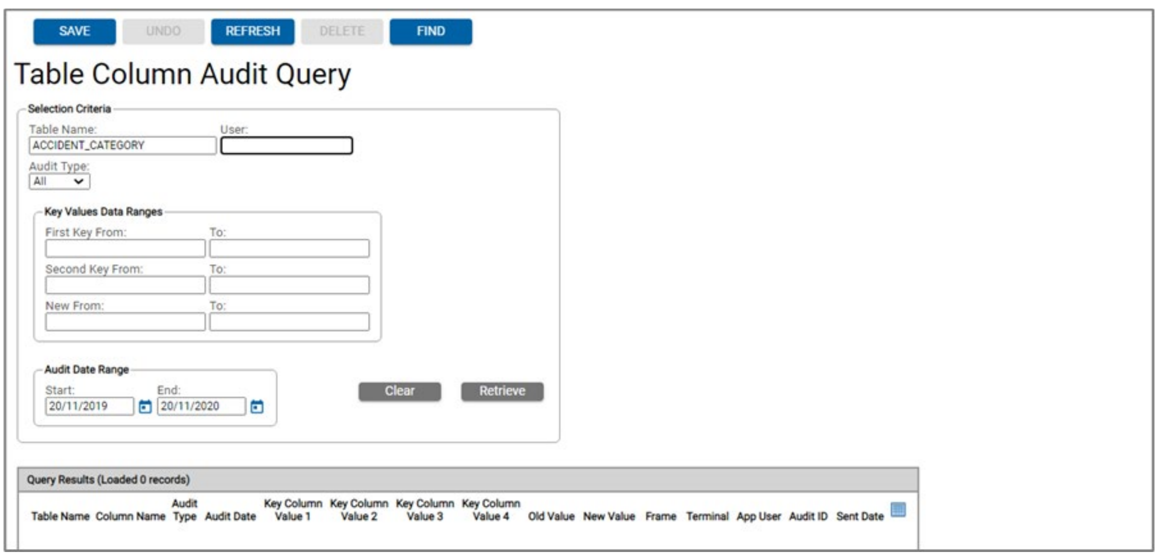
1. Enter a **Table Name** to select the table.
2. You are able to select a specific user by entering the name in the **User** field or select from the List of Values.
3. From the **Audit Type** dropdown select *All*, *Insert*, *Update*, or *Delete*.

The table that is selected determines what is shown in *First Key* values. This value is usually the primary key for the table. For example, if **unit_dept_comp_main** is selected then the first key values heading changes to **UNIT_NO Values**. The user could then enter what unit numbers to query and view who made changes to those particular units.

Second Key values is a range of values of the second segment of the primary key. For example, if **unit_item.value** is audited, the first key value is the unit number and the second key value is the name of the unit item.

New data values will search both the **old_value** and **new_value** for the data entered.

4. Enter the date range of audits you would like to view in the **Audit Date Range** fields. It defaults to a calendar year ending on the current date.
5. Select the **Retrieve** button to display the **Query Results**.

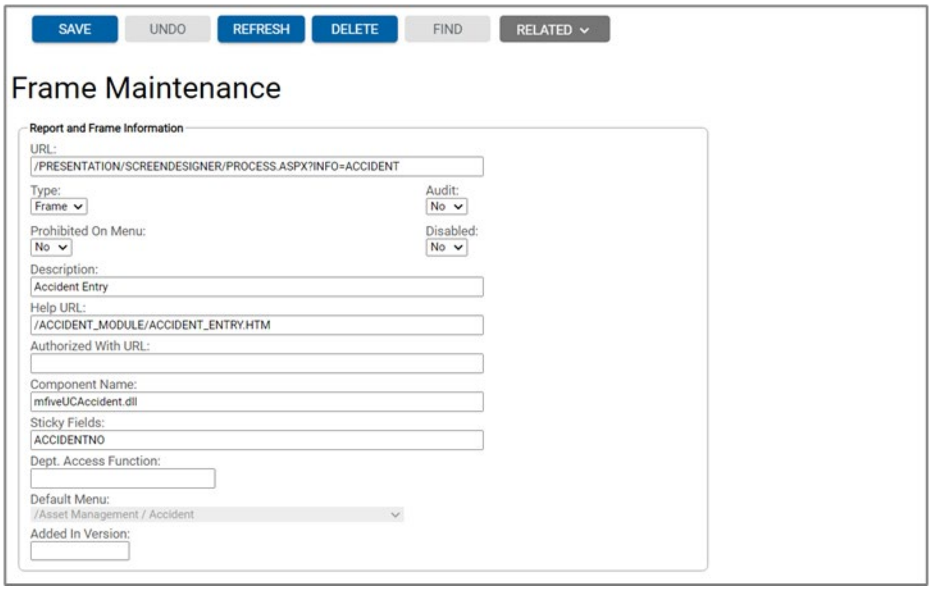


Section 10. Frame Maintenance

Frame Maintenance can be used to change the description of a frame, report, or link in the M5 system. It can be used to add new frames and reports. Normally the System Administrator would not need to make changes to this frame and AssetWorks recommends that these settings be left with the default values.

When M5 is upgraded for a patch or a new release, the Run M5 Objects process updates *Frame Maintenance* with all new frames and reports. There is an option in this Object update that restores the frame descriptions to the M5 default values.

If it is necessary, open the *Frame Maintenance* frame and follow the steps to edit a frame.



Report and Frame Information

Complete the steps.

1. Select the **URL** field to see the list of valid URL’s. Double-click the selection.
2. The **Type** choices in the dropdown menu are: *Frame*, *Report*, and *Link*. The *Link* option allows the user to add this link to a menu.
3. Use the **Audit** feature with great caution as it will journal every detail and can cause performance issues within the database.
4. **Prohibited on Menu** does not allow this frame to be added to a menu.
5. Use the **Disabled** dropdown to disable this frame.
6. The **Description** can be changed, as applicable. The description changes for the frame on the menu, frame, and report title.
7. The **Help URL** is the link to the help document for this frame.
8. The **Authorized with URL** has to do with frames within frames. For example, *Work Order Main* displays frames for standard jobs and warranty. Those frames are not authorized to be located on a menu but associated to the *Work Order Main URL*.
9. **Component Name** is the main DB component behind the scenes.
10. **Sticky Fields** are used to transfer URL information as in an email including keys to identify specific information being entered or used on a frame. These are programmed in the M5 frame. The client cannot arbitrarily add a sticky field.
11. **Dept. Access Function**. If you are using DAF (Department Access Function) security, then enter the security function that this frame is to take on. Please review the *DAF Security* functionality in this manual for further assistance.
12. **Default Menu** is a future enhancement to create a standard default menu.
13. **Added in Version** indicates which release this frame was added.
14. Select **SAVE** to update the frame records.

To Delete a Frame

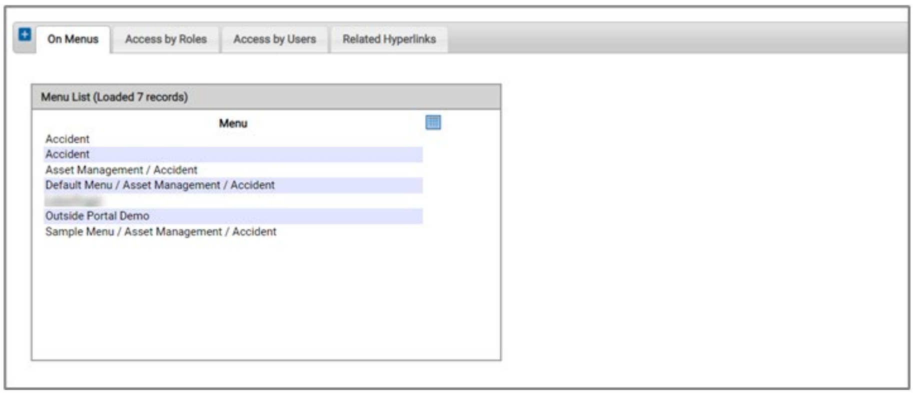
Complete the steps.

1. Select the frame **URL** for the frame.
2. Select the **DELETE** button on the toolbar. The Action Required window opens.
3. Select **Delete** to confirm the deletion and save the changes.

Frame Maintenance tabs

The following tabs are available on *Frame Maintenance*:

- **On Menus** – Allows you to view what menus this frame appears on.
- **Access by Roles** – Allows you to view what user roles have access to this frame.
- **Access by Users** – Allows you to view what application users have access to on this frame. You can also view the role associated with the application user and what level of access they have (for example, FULL).
- **Related Hyperlinks** – Allows you to configure the list of related frames that display on the selected frame when the user hovers over the **Related** dropdown at the top of the frame. To add a frame, double-click in the field to select from the List of Values. Define the **Query String**, and **Send Screen** fields (sticky fields). Select the **New Window** checkbox for the frame to open in a new window. Select **SAVE** when finished.



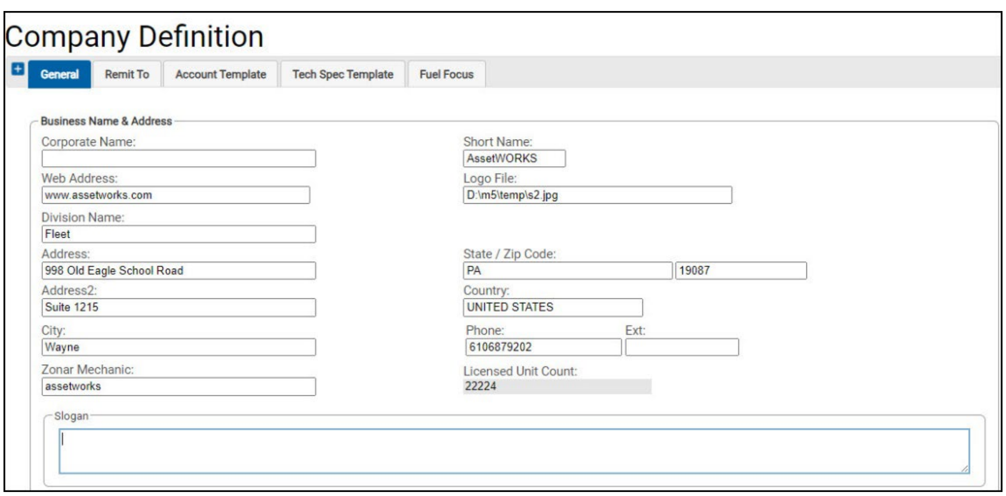
Section 11. Company Definition

This frame is used to set up basic information about the company. The information entered on this frame appears on the *Work Order Invoice Report* and the division name is printed on the top right of every Crystal Report.

General tab

The Company *Business Name & Address* information displays:

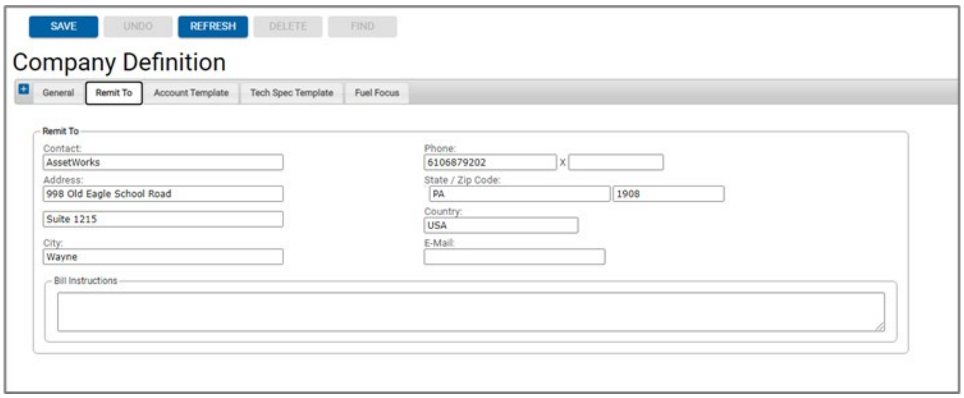
- Corporate Name
- Short Name or any abbreviation desired
- Web Address
- Division Name
- Logo File location
- Address
- State / Zip Code
- Country
- City
- Phone and extension number
- Zonar Mechanic
- Licensed Unit Count
- Slogan



Remit To tab

The accounting department *Remit To* information displays:

- Contact
- Phone and extension number
- Address
- State / Zip Code
- Country
- City
- E-Mail address
- Billing Instructions (free form field)



Account Template tab

Selecting the **Use Direct Account Table** checkbox leaves the valid direct account number stored in the direct account table. No client configuration changes are necessary to keep existing account numbers. If you wish to use segmented account numbers, the **Use Direct Account Table** checkbox should be clear.

Note: Do not add segments if the users do not intend to use the template function. Adding segments when using the direct account table can cause issues with the *Direct Account Table* functionality.

The maximum number of segments is set to 20. The maximum number of characters including any delimiter is 100. All of the M5 Database fields for the **Dir_Acct_No** have been increased.

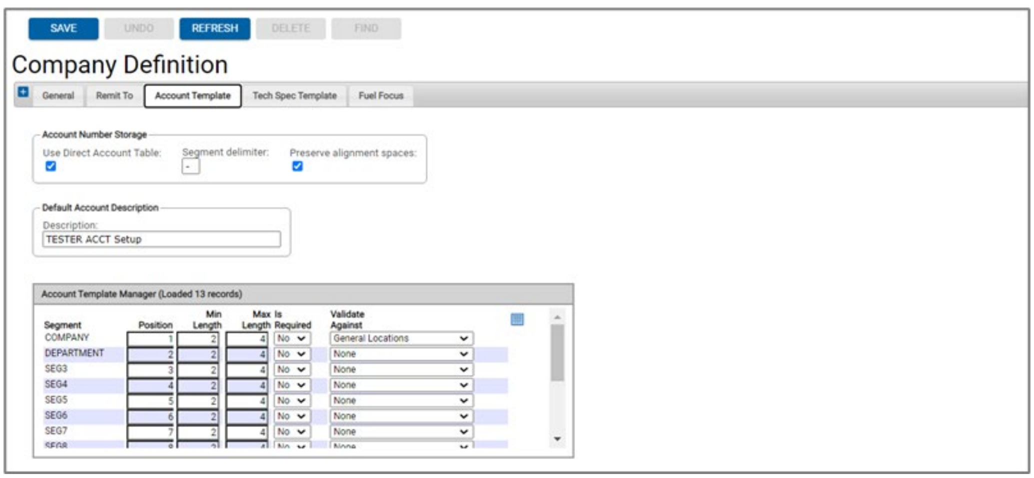
Enter the type of delimiter wanted between each segment such as a dash or a slash.

Complete the remaining fields.

1. Select the **Preserve alignment spaces** checkbox if you want placeholders. For example, in the example above for segment 1, the minimum length is 4 with up to 20 characters. If you want to hold the remaining 16 spaces, then select the checkbox. By preserving the spaces, all account numbers will have the same length.
2. Enter a **Description** of the default account template.
3. Enter the **Segment** name.
4. Enter the **Position** in which the user should enter this particular segment.
5. Enter the **Min Length** of the segment.
6. Enter the **Max Length** of the segment.
7. If this segment **Is Required**, set the value to *Yes*.

Validate Against determines that validation is to occur for a given segment. The options for this field are:

- **None** – No Validation
- **Departments** – Validated against Dept_Main
- **General Locations** – Validated against Gen_Loc
- **Organizational Hierarchy** – **Orig. Level** values are dynamically loaded based upon the users **Org_Hier** table.



Tech Spec Template tab

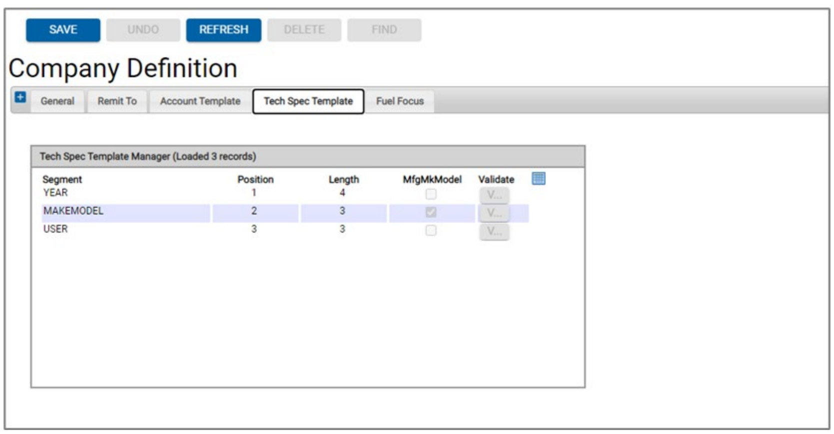
Customers rely heavily on reporting by Tech Spec, MfgMkModel (MMM). They are used in the definition of a standard job. Normally your M5 project or support team will assist you in creating the tech spec template on the **Tech Spec Template** Tab.

System Flag 5268 must be set to **Y** in order to create a new tech spec structure. The tech spec is normally structured in multiple segments.

For example, the image displays a structure with three segments defined. The total length of the tech spec is 13 characters, you can add three additional segments for this tech spec.

You are able to select an existing segment and modify it. You can also select the **Validate** column to add or modify a validation code for the segment. If you have character length still available on your frame you can select the bottom row and enter the new *Tech Spec* name in the **Segment** field.

1. Enter the label of the first segment of the tech spec in the **Segment** field.
2. Enter the starting position in the **Position** field.
3. Enter the length of the segment in the **Length** field.
4. If the segment should be validated against the manufacturer, make and model table, then select the **MfgMkModel** checkbox.
5. To create your own list of values for the segment, select the **Validate (V)** icon in the **Validate** column.
6. Select **SAVE** to complete your update.

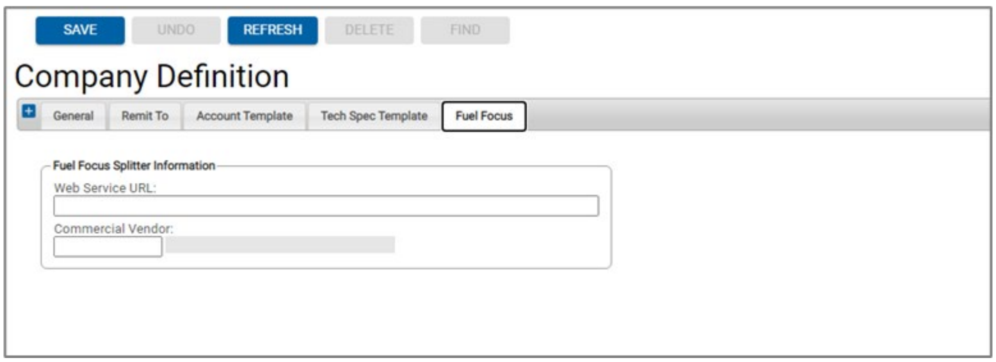


Fuel Focus tab

The **Fuel Focus** tab is used for splitting fuel information between servers. Each server will have its own database containing duplicate information for the commercial fuel vendors.

Complete the steps.

1. Enter the **Web Service URL** of the server to be connected to.
2. Enter the **Commercial Vendor** that resides in the second database. The vendor is used for the internal unit fuel charge in the primary database. The vendor must reside in both databases
3. Select **SAVE** to complete your update.



Section 12. Calendars

Fiscal Calendar

The *Fiscal Calendar* frame defines each fiscal period and is used for reporting. This calendar must be set for each year prior to the start of the first fiscal period.

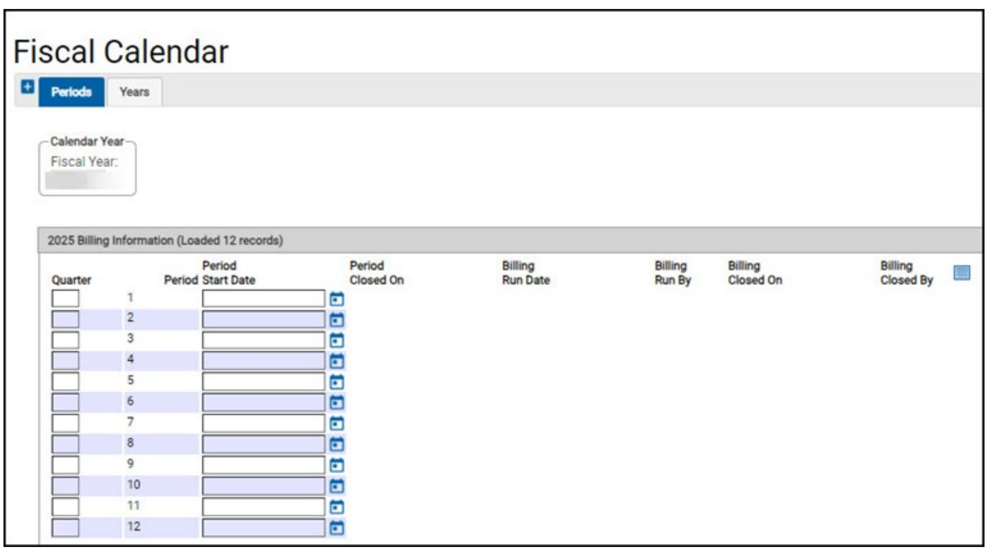
Periods tab

Complete the steps.

1. Enter the **Fiscal Year**. Within the *Action Required* window, select **Create** to create the fiscal year.
2. Enter the **Quarter**. The **Quarter** must be 1, 2, 3, or 4.
3. Enter the **Period**. System Flag 1012 defines the number of periods in the fiscal year (12 or 13).
4. Enter the **Period Start Date**. The **Period Start Date** must be the first day of the month or fiscal period.
5. Select **SAVE**.

The **Period Closed On** date field displays after the *End of Period* process is run. See *Running End of Period*.

The **Billing Run Date**, **Billing Run By**, **Billing Closed On**, and **Billing Closed By** fields display after the billing process is run. See *Running Billing*.



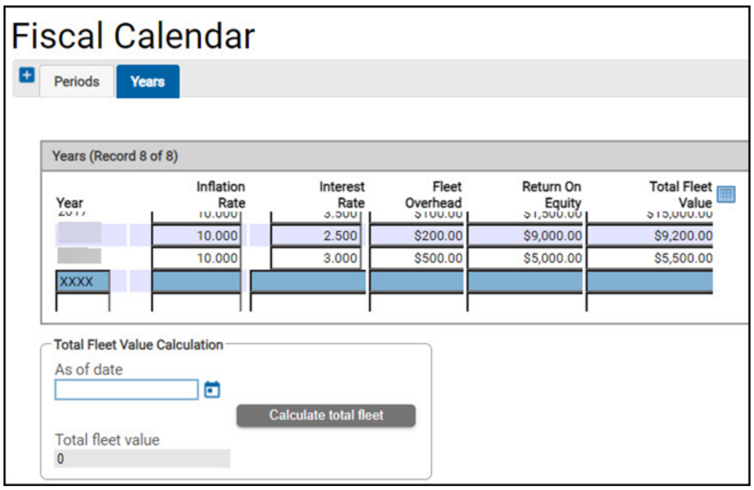
Years tab

The **Years** tab allows you to define the **Fiscal Year**. It is a customer-specific area for aid in calculating vehicle lease rates. It can be loaded with inflation, interest, overhead and equity to determine fleet value.

Complete the steps to complete the creation of your fiscal calendar.

1. Enter the fiscal **Year**.
2. Complete the **Inflation Rate**, **Interest Rate**, **Fleet Overhead**, **Return On Equity**, and **Total Fleet Value** fields.
3. Select **SAVE**.

Total Fleet Value Calculation displays the *Total fleet value* when you select the **Calculate total fleet** button.

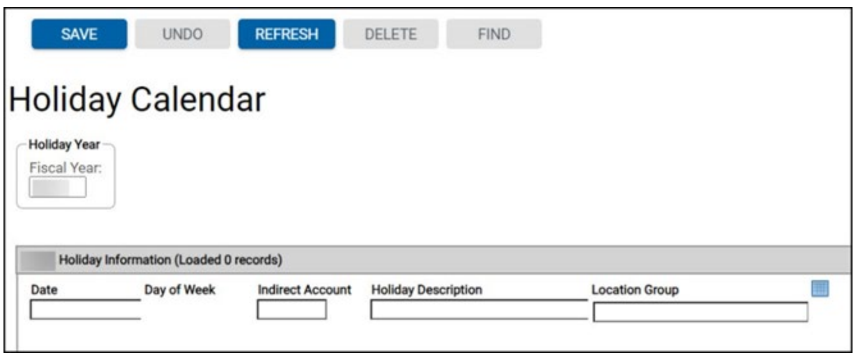


Holiday Calendar

The **Holiday Calendar** frame tracks all company holidays for the *Fiscal Calendar* that is used when running the employee schedules. The *Planned Absences* batch process uses these dates in order to put the holidays on the *Employee Time Card*.

Complete the steps.

1. Open the *Holiday Calendar* frame to add dates.
2. Enter the **Fiscal Year**.
3. Select the **Date** field in the empty row to enter a date from the calendar. The **Day of Week** automatically displays.
4. Enter the **Indirect Account** code for the holiday.
5. Enter the **Holiday Description**.
6. Enter a **Location Group** or select from the Group Location List.
7. Select **SAVE**.



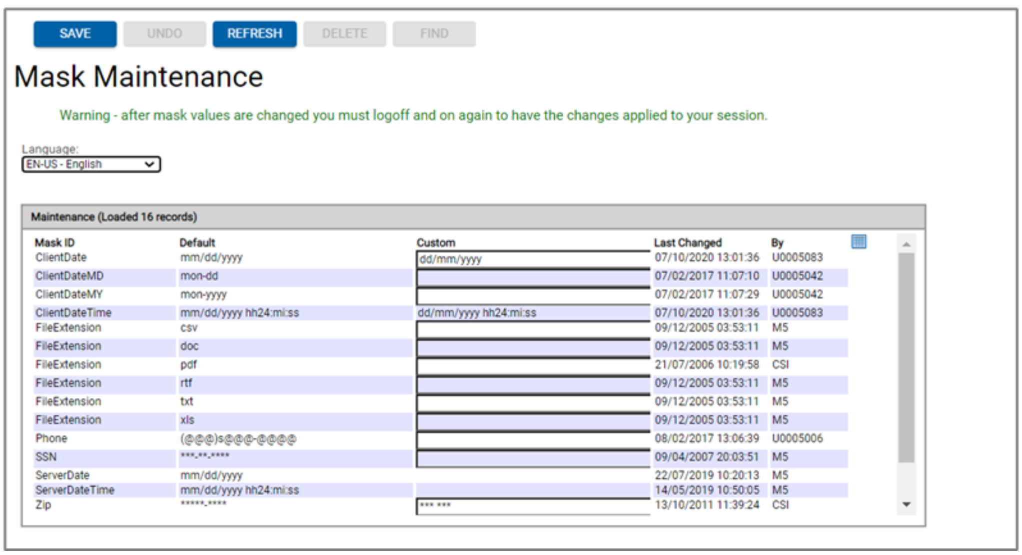
Section 13. Settings

System Mask Maintenance

The *System Mask Maintenance* frame contains the formats for displaying time settings, date settings, currency, phone number, and address values on frames and reports. M5 is delivered with default settings for the *United States* but our customers located outside of the U.S. will need to configure these settings accordingly.

The most common change made in mask maintenance is how the date displays. The *Client Date Mask* controls this display. When you first open the *System Mask Maintenance* frame, select a default **Language**. Search the **Mask ID** column for the mask you wish to modify. Insert the new mask structure in the **Custom** column.

⚠ Be careful modifying any mask structure that refers to server settings or file extensions. Select **SAVE** to update the mask records.



Mask ID	Default	Custom	Last Changed	By
ClientDate	mm/dd/yyyy	dd/mm/yyyy	07/10/2020 13:01:36	U0005083
ClientDateMD	mon-dd		07/02/2017 11:07:10	U0005042
ClientDateMY	mon-yyyy		07/02/2017 11:07:29	U0005042
ClientDateTime	mm/dd/yyyy hh24:mi:ss	dd/mm/yyyy hh24:mi:ss	07/10/2020 13:01:36	U0005083
FileExtension	csv		09/12/2005 03:53:11	M5
FileExtension	doc		09/12/2005 03:53:11	M5
FileExtension	pdf		21/07/2006 10:19:58	CSI
FileExtension	rtf		09/12/2005 03:53:11	M5
FileExtension	txt		09/12/2005 03:53:11	M5
FileExtension	xls		09/12/2005 03:53:11	M5
Phone	(@@@)s@@@-@@@@		08/02/2017 13:06:39	U0005006
SSN	***-**-****		09/04/2007 20:03:51	M5
ServerDate	mm/dd/yyyy		22/07/2019 10:20:13	M5
ServerDateTime	mm/dd/yyyy hh24:mi:ss		14/05/2019 10:50:05	M5
Zip	*****-****	*** ***	13/10/2011 11:39:24	CSI

State/Country Codes

The *State/Country Codes* frame is a valid list of states within a specific country. The state codes are delivered with *Canada*, *Mexico*, and *USA* already loaded. Customers from other countries can review and add countries and state codes as applicable.

Open the *State/Country Codes* frame and select the **Country** field to view the **State Code** and **Description**.

Complete the steps to create a new country code.

1. Select the blank row in the **Country Codes** table.
2. Enter the **Code** number, **Country** name, and **State Code Length**.
3. To add a **State Code** for a country, select the **Country** code. The *Valid State Code* i-frame displays the **State Code**.
4. Scroll to the bottom of the **Valid State Code** list to add new state codes, as applicable.
5. Select **SAVE**.

To Delete a Code

Complete the steps.

1. To delete a **State Code** or **Country Code** select the code.
2. Select **DELETE**. The row displays as red.
3. Select **SAVE** to complete the deletion.

Time Interval

Units of time in M5 are calculated automatically and stored in the database tables as milliseconds. The *Time Interval* frame allows the user to change how it displays on a frame and on reports. This does not change the data in the tables.

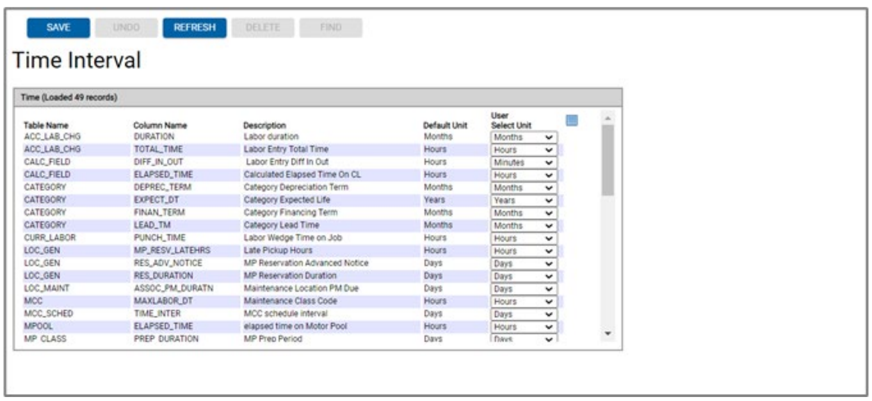
The columns which display on the *Time Interval* frame:

- Table Name
- Column Name
- Description
- Default Unit
- User Select Unit

Modify Table List

Complete the steps.

1. Select the **Table Name** to customize from the *Time* list.
2. From the **User Select Unit** dropdown select an interval: *Minutes*, *Months*, *Hours*, *Days*, *Years*, *Seconds*, and *Milliseconds*.
3. Select **SAVE**.



Time Zones

The time zone setting in M5 is always the time zone where your PC resides. The **Time Zone** field for locations on the *Location Main* frame still exist since there are reports that use that field.

Many reports include the date they were produced. Some reports display only dates while others display date and time. No matter how the date and time is shown we must decide if it should be adjusted to the user's time zone or if it should be the exact value in the database.

For example, if a user in PST runs an immediate report that another user in EST has generated, then the user will see the EST times on the report.

If a user in PST runs a scheduled report, then the time will be in the PST time zone. However, if a PST user views a report generated by a user in EST, then that report displays EST times.

If, however, a report that displays a shift (employee, unit, or location) then we do not compute the time zone difference but instead show the same date and time no matter where the user is viewing the report (eastern or pacific time zone).

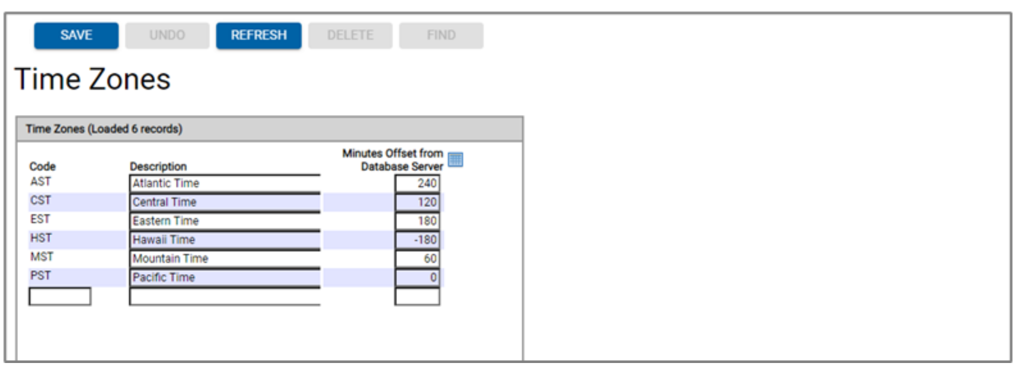
From the system **Time Zones** frame:

- The time zone where the database server is located should be set to 0 (zero).
- The other time zones are offset from the database server time zone in minutes. In the example, the database server is located in the Eastern Time Zone. CST (Central), MST (Mountain), and PST (Pacific) are offset in -60 minute increments. AST (Atlantic) is offset by +60 minutes.

Add a Time Zone

Complete the steps.

1. Enter a **Code** in a blank row.
2. Enter a **Description**.
3. Enter the **Minutes Offset from Database Server**.
4. Select **SAVE**.



System Translation Maintenance

The *Translation Maintenance* frame is used to change the field labels on frames and reports to your native language or simply to make it more useful for your organization to match terminology that is common to your environment.

Changing these default values changes the field label on the given frame. Please keep in mind that the M5 Support Group will not be aware of this new field label. You need to inform them of the new label so they will understand the details of the support issue you are discussing.

Open the *Translation Maintenance* frame, the **Locale** defaults to your language. Double-click the **Frame** field if you are selecting by frame name. Select your frame from *Localized Strings* i-frame.

If you select by search criteria, one or all of the following can be used to perform the query.

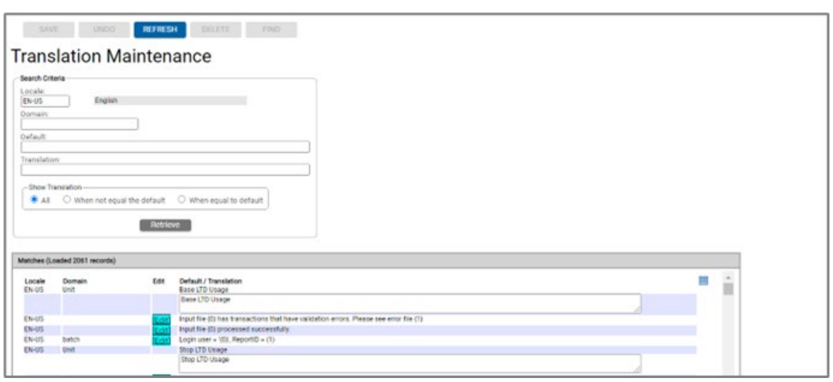
- Domain is the M5 frame or report name.
- Default is the default label value.
- Translation is the new label value you enter.

If you want to change the **Default** field label on all the frames where it occurs leave **Domain** blank and enter the label name in the **Default** field. **Select All** and **Retrieve**. Enter the new default value and it will be changed on all the frames.

Show translation is useful if you are looking for labels that have been changed previously or if you want to see the ones that still have default values.

Complete the steps.

1. Enter the information to query. Select translation to show and select **Retrieve**.
2. The list of domains, defaults and translations display. The field names are not shown here, only the labels for them. So you must be familiar enough with the frames to recognize the correct label.
3. Select **Edit** to change the default setting. After the default has been changed, it becomes the translation.
4. Select **SAVE**.



Section 14. Interface

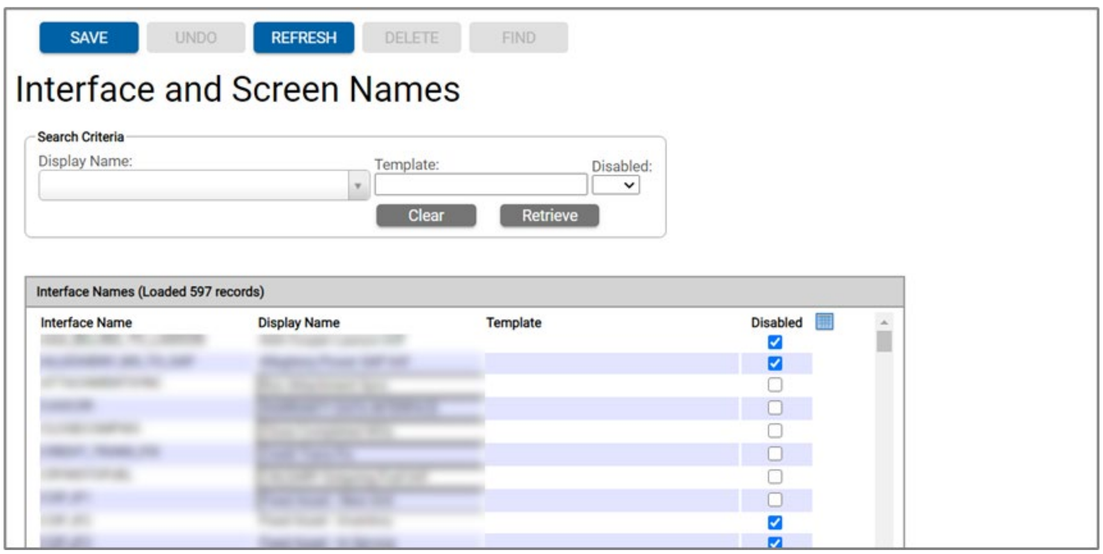
Interface and Screen Names

Interface and Screen Names are maintained by your M5 Support Group. The user is only allowed to modifying the display name and disable or activate the interface. The **Display Name** will appear in the Interface menu choices on the *Interface Manager* frame for any Interface that is not disabled. Templates are used by inbound Interfaces and can only be modified by the M5 Support Group.

Open *Interface and Screen Names* and select the interface name from the **Display Name** dropdown. You can locate the interface by scrolling the list of available names or using the search criteria section at the top to narrow your results. You can filter on **Display Name**, **Template**, and **Disabled** (Y/N).

Note: You must enter a **Display Name** first before you can filter by **Template**.

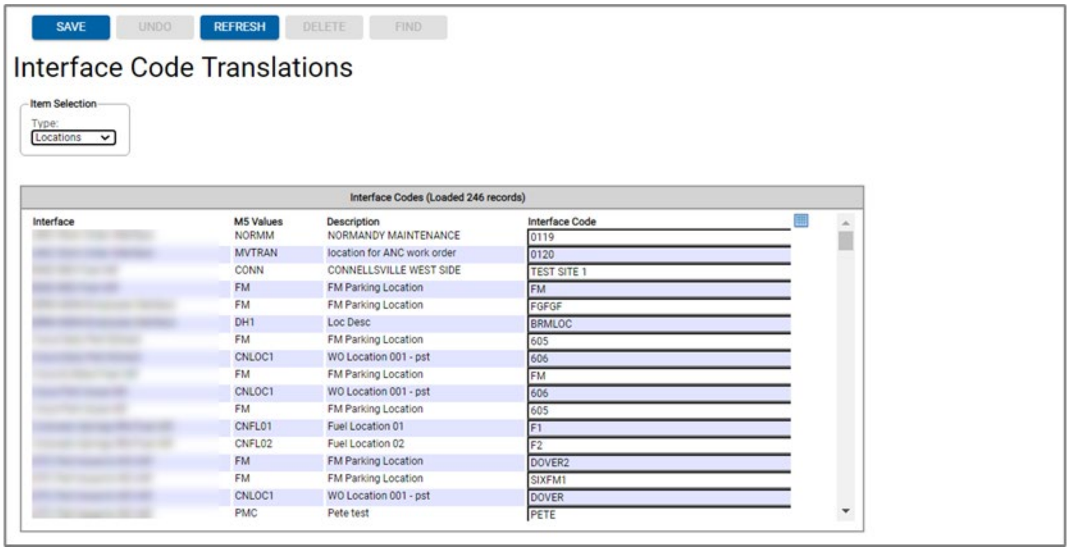
When the row is highlighted you can change the **Display Name** or disable the interface. When complete, select **SAVE**.



Interface Code Translations

This frame is used to configure data codes that are received through the various system interfaces. Normally M5 Support will assist in the creation of the **Interface** and the **Interfaces Codes**. The codes that are used by outside vendors must be translated into valid M5 codes before processing can occur. This is most commonly used with *Fuel Interfaces* but other choices are available: *Products*, *Locations*, *Departments*, *Vendors*, and Other. Use the Type dropdown menu to make the selections.

To add a new interface code, locate the correct interface and select the **Interface** code field and enter your new value. Select **SAVE**.



Interface Manager

The *Interface Manager* frame allows the user to set up parameters for each interface and displays the *Current Execution Schedule* for the interfaces. All currently active interfaces display on the dropdown list in the **Interface** field. After the interface is selected the parameters display. The parameters are different for each interface. Some may require a path for the input file or an email address for the output file. Some may only require a start and end date.

If you receive a new interface from a vendor make sure complete documentation is provided so M5 Support can assist you in configuring it properly.

Below *Interface Parameters* is the *Current Execution Schedule*. This indicates if the interface is currently running or shows the last time it was run. The table shows the interface:

- ID
- Description
- Status
- Schedule Date
- Last Run
- Frequency
- If it Excludes Holidays and the Submitted By user
- Priority Run Desc.

If the status is complete, we recommended that the row be deleted. Select the row to delete, and then select **DELETE**. The row displays as red. Select **SAVE** to complete the deletion.

You will configure your new run schedule within **Schedule Details**. The run interval has a dropdown option to select, *Once*, *Minutes*, *Hours*, *Days*, and *Months*. Select the option you want and enter the run interval to the left. Select the checkbox to exclude holidays and weekends to prevent it from running on those days. Enter the **First execution date/time** or select the **Schedule/Reschedule** button to default the current date and time.

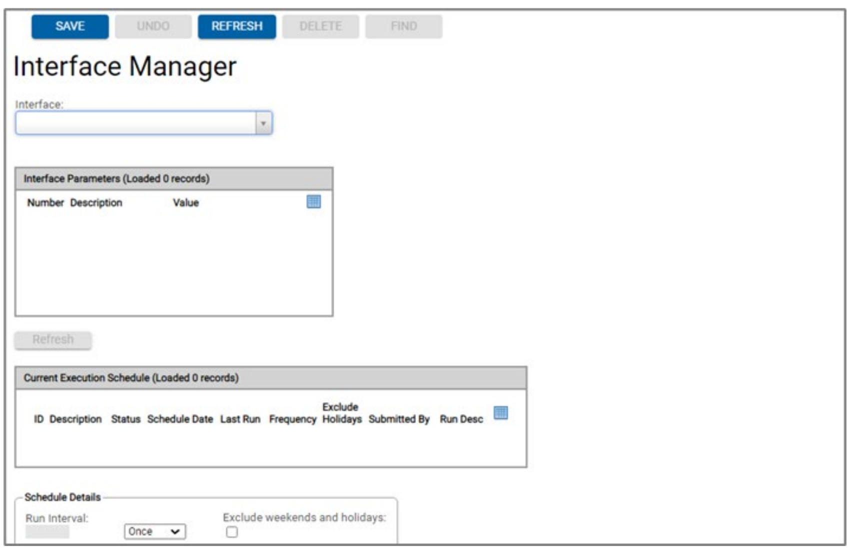
After selecting the **Schedule/Reschedule** button the data is automatically saved and submitted with the given parameters. The current execution schedule displays the information just submitted. Select the **Refresh** button to refresh the frame showing the current execution's status. The interface is now submitted and depending on the setting of the Windows scheduler, the interface will run.

The back-end process that executes the interface programs consists of five different processes.

Complete the steps.

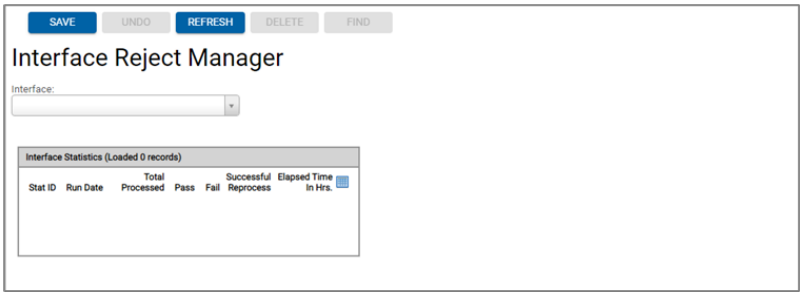
1. The Windows Scheduler. This is set up by the customer and dictates the interval by which the M5 Report Engine will be called.
2. On execution the M5 Report Engine checks to see if there are any new rows in the **saves_reports** table with the status other than error or complete.
3. If a new row is found the Command file is executed based on the parameters of the interface. The command file then passes the parameters onto an executable interface program.
4. The specific executable runs with the parameters received.
5. When the executable file processing is complete it generates an output log file. This file is made available to the customer as designated in the design specification documents.

To prevent an interface from being executed go to the *Interface and Screen Names* frame and disable it.



Interface Reject Manager

Interface Reject Manager allows you to correct errors that have occurred in custom interfaces. It is provided if required as part of the Interface Specification document.



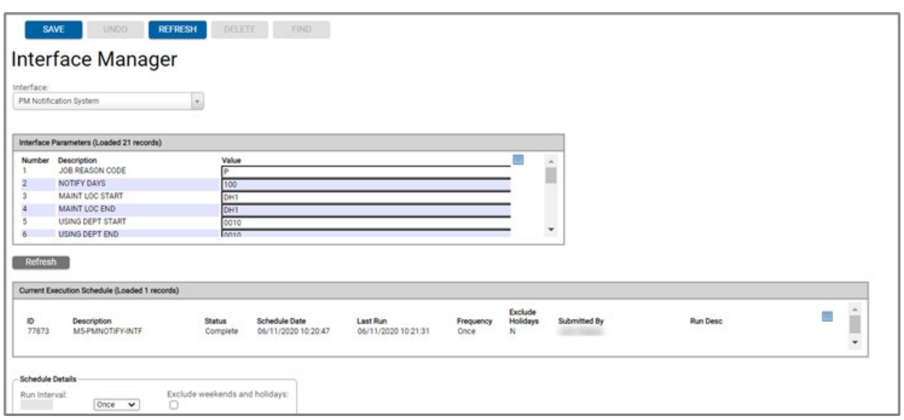
Repeat Repair Data Gen

The *Repeat Repair Data Gen* process gathers information on repeat repairs based on System Codes for the type of systems and the number of days between repairs. After this process is complete the system generates warnings of repetitive repairs and reports can be run to see this information.

PM Notify

The *PM Notify* program sends emails that alert people when an upcoming preventative maintenance job is due. It works for other job types as well. The PM Notify program is launched using the *Interface Manager* frame. Open *Interface Manager* and select *PM Notification System* as the **Interface**.

The email sources can be **D** for Using Department, **L** for Parking Location, or **O** for Operator. If the value is **D** the report displays units grouped by Using Department and is sent to the Using Department email address. If the value is **L** the units will be grouped by Parking Location and they are sent to the Parking Location email address. If the value is **O** the report is sent to the Operator’s email address, provided the operator has a valid setup in *Employee Main*. If not, the email will be sent to the Department email address.



Section 15. Batch Processes

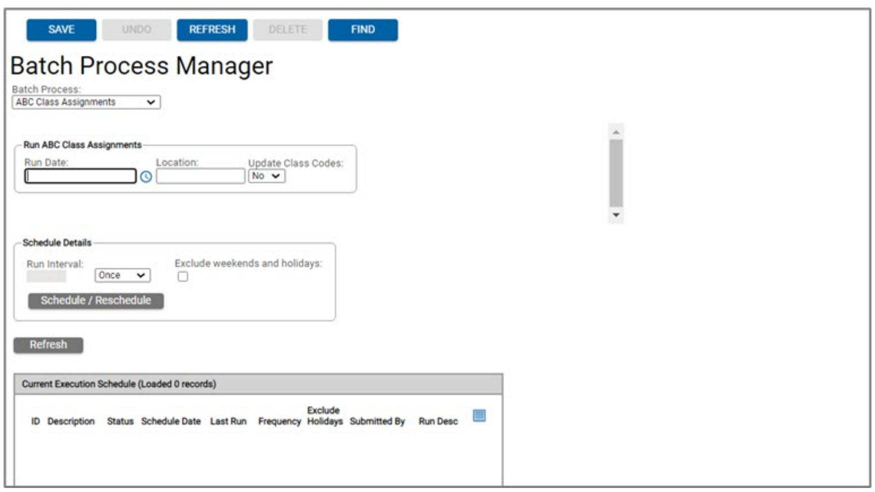
Batch Process Manager

The M5 System has several internal batch processes that are critical to the overall integrity and functionality of the system. The configuring, scheduling and execution of these batch processes is controlled through the *Batch Process Manager*.

Different Batch Processes have different parameters to configure but maintaining and executing them is done through the same general steps.

Open the *Batch Process Manager* frame and select the **Batch Process** field to select a process. If there is a current schedule for that batch process, you will see a notice. It can be deleted or rescheduled as needed.

- To create a new schedule delete any current schedule then set up the new one.
- Each process has different parameters to be entered.
- Select the run interval.
- Select the Exclude weekends and holidays checkbox, if required.
- Select Schedule/Reschedule.



ABC Class Assignments

The *ABC Class Assignments* batch process produces a report that allows the user to preview how the ABC class codes will be assigned to stock parts. In the *Batch Process Manager* select **ABC Class Assignments**. Select the **Clock** icon to select the day and time to run the batch.

Next you can enter a **Location,** select from the List of Values, or leave it blank for all locations.

Note: The default value for the **Update Class Codes** field is *No*.

This setting allows you to verify code assignments before updating them. You can make corrections and run this again as many times as you need to.

You can set the **Run Interval** and frequencies to run the batch, **Exclude weekends and holidays**, and select the **Schedule/Reschedule** button. When you are satisfied with code assignments you can set the update value to *Yes* and run the batch to update the codes.

The value in this batch field ignores the setting in System flag 5038. System Flag 5038 only controls whether the update is performed during the End of Period batch process.

Allocation

The **Allocation** batch process is a customer specific process used for distributing costs to allocation pools or groups. The **Allocation Pool** is created by AssetWorks when requested by the customer and can be configured and executed through the *Batch Process Manager*.

Archiver

The **Archiver** batch process moves and stores older data that no longer needs to be readily available in active M5 tables. The program moves the data from various tables based on the type of transaction. M5 provides the ability to archive eight types of data transactions.

1. Fuel Transaction Detail
2. Indirect Account Detail
3. Parts Detail
4. Replacement fund
5. Telematics
6. Unit Availability Detail
7. Unit Detail
8. Work Order Detail

Close Billing Period

The **Close Billing Period** batch process should be run after all billing transactions for the current period have been verified as accurate. When this batch is selected, the user is prompted to make sure they understand that when this process runs no further changes will be allowed in this period. After this batch process is executed the billing transactions are posted to the accounting ledgers and cannot be changed. Any adjustments will have to be made in the next billing period and both entries will appear in the audit trail.

Complete the steps.

1. When you select the **Close** button the billing header displays the fiscal year and period for which billing will be closed.
2. The **Last Bill Run Date** displays.
3. Enter the **Schedule Start Date For Billing Close**. Selecting the field defaults to today's date and time.
4. Select the **Run Interval**.
5. Select the **Exclude weekends and holidays** checkbox, if applicable.
6. Select the **Schedule/Reschedule** button.
7. Select **SAVE**.

End of Day

The **End of Day** batch process updates specific data into certain tables on a daily basis. By default this process automatically runs every day at the time specified unless it is changed. It produces an email when completed. The email is sent to the user specified in the *Application User Maintenance* frame.

The **End of Day** process performs the following tasks:

- Calculates unit downtime accumulated since the last end of day was run.
- Updates part statistics with the last physical inventory date if no last physical inventory date is present.
- Updates **Parts_Usage_Occ** table to identify failures of major parts.
- Update **Unit_Dept_Comp_Main** with current values of **Department** numbers from **Unit_Assign_Hist**.

When you select the **End of Day** batch process you will see a message if there is already a schedule active for it. Select **OK** to delete and reschedule to process.

Complete the steps.

1. Delete the existing schedule before creating a new one.
2. Enter the **Date/Time** to reschedule the end of day process.
3. Select the **Run Interval**.
4. Select the **Exclude weekends and holidays** checkbox, if applicable.
5. Select the Schedule/Reschedule button.
6. When the **End of Day** process has finished running, the user who ran it receives an email indicating that the process completed successfully or there were errors.
7. If there are any errors reported they can be corrected and the process can be run again.

The **End of Day** batch process will not run during a system backup. So be sure to schedule it before or after your system backup runs. It is also recommended to run the end of day process at a time when the system is in limited use.

End of Period

The **End of Period** batch process must be run no earlier than the first day of a new fiscal period. End of Period automatically closes the oldest currently open period. The tasks for end of period include:

- Verifying there is a unit history record for each unit for the current period.
- Propagating shift table information forward for the module flag designated amount of time.
- Running **Eop_Inv_Proc**, a process that performs inventory processing and cleanup by:
    - Rolling usage quantities by period and setting current period usage to zero.
    - Deleting transfers which have been rejected or completed over the number of days indicated by the *Inventory Management* module flag, Del. expired POs/Trans after (duration).
- Rolling period start quantities/inventory dollar value by period.
- Getting current on-hand quantity and unit price to calculate the current period start quantity/inventory dollar value. The going price and Rav are calculated in the **Part_Get_Price** process according to the pricing method set for the Inventory Management system flag - Type of pricing to use for inventory valuation. These valid pricing methods include:
    - Location Standard: Locstd - Unit$ = Location Unit $
    - Location Average: Locavg - Unit $ = Location Calculated Unit $
    - System Standard: Sysstd - Unit $ = Part Unit $
    - System Average: Sysavg - Unit $ = Part Calc Unit $
- Incrementing the period roll counter (**Pd_Roll_Ct**) to annualize usage.
- Calculates depreciation for all units that have a depreciation type of **S** (Straight -line), and that do not have a SOLD status.

System Flag 5290 – "Calculate depreciation based on capital journal?" determines how the depreciation of capitalized value is calculated. If set to N for purposes of depreciation, the capitalized value of the unit is the purchase cost plus capital adjustments at the time the end-of-period is run. This preserves existing functionality. If set to **Y**, the capitalized value of the unit only includes the changes made prior to the end of the period being closed, excluding those after the period was closed and before EOP was run. The **Y** setting also enables EOP to "catch up" and process depreciation for periods prior to the period being closed, including those values as a depreciation adjustment for the period being closed.

This flag cannot be changed by users because of the potential duplication of values if the flag is changed from **N** to **Y**. Only new customers or customers that have not otherwise implemented depreciation calculations in M5 should consider changing the flag:

- Updates the line items in the *Budget* frame (some applications do not have this frame) if the appropriate budget flags are set in System Flags.
- Updates *Maintenance Class Code* history.
- Sums past five years of unit history for reporting purposes (rolling five year window).
- Closes the period (nothing else can be charged to a closed period).
- Renames the user log file that keeps track of users.
- Updates the Last End of Period run.
- A batch process called **Part_Hist** can be run separately by setting System Flag 5032.

End of Period Process

Complete the steps.

1. Select **End of Period** in the *Batch Process Manager*. The fiscal year and period display.
2. Enter the date/time to start running the process. Today's date and time will default. Make adjustments if necessary.
3. Select the run interval.
4. Select the **Exclude weekends and holidays** checkbox, if required.
5. Select the **Schedule/Reschedule** button.

M5 sends an automatic email when the process has completed to the person who started the process. The email address comes from the *Application User Maintenance* frame. The email indicates if the process was completed successfully or had errors.

Forecaster

The **Forecaster** batch process predicts when a standard job is due for a unit, department, or component. The **Forecaster** uses the *Standard Job MCC* and the *Standard Job Tech Spec* to create work requests with a future due date. This date is calculated based on a time interval, the primary or secondary meter usage or fuel consumption. The set up of the Standard Job MCC and interval must be done prior to running the forecaster in order to have work requests generated. If the MCC setting is left at the default of zero the Forecaster will not calculate usage at all. The job may be set as recurring or one time only.

In the *Batch Process Manager* select **Forecaster** from the list of batch processes, the **Run Date** field displays. Press tab to select the current date and move to the **Email Notification** field. The email notification will let the user know if the process ran successfully or failed. The default schedule interval is once. Select **Schedule** to execute.

The Forecaster is a powerful tool for ensuring that your units remain in compliance with warranties and in optimal working condition. See the *Forecaster Application User Guide* for further details on using this tool to its fullest extent.

Part History

The **Part History** batch process allows the user to close the Part History on exactly the last day of the month separate from the **End of Period** process. System Flag 5032 must be set for this to occur. See the **End of Period** process for more details. To run it, select **Part History** in the Batch Process Manager. The **Fiscal Year** and **Period** display.

Complete the steps.

1. Enter the **Date/Time to Start Run**.
2. Select the **Run Interval**.
3. Select the **Exclude weekends and holidays** checkbox, if required.
4. Select the **Schedule/Reschedule** button.

Parts Requisitions

The **Parts Requisition** batch process automatically creates requisitions, requisitions and purchase orders, or part transfers within the **Parts Inventory** module. When reordering is done manually the quantities are based on **Standard Order Quantities** from the *Part Inventory Location Manager* frame.

When reordering is scheduled automatically the quantities are based on the **Economic Order Quantities** established by the ABC classification and historical transactions. When you select **Parts Requisitions** in the *Batch Process Manager*, the **Run Date** field displays with today's date selected. Modify the date if desired or press tab to select what you want to generate with this run.

Complete the steps.

1. Select *Requisitions Only*, *Requisitions and PO's*, or *Transfers Only* from the **Generate** dropdown.
2. Enter the location in the **Location** field or a range of locations in the **To Location Range** field. A vendor can be specified in the **Vendor** field.
3. Select the **Run Interval** and the **Exclude weekends and holidays** checkbox, if applicable.
4. Select the **Schedule/Reschedule** button.

Planned Absence

The **Planned Absence** batch process updates employee holidays and vacation schedules. These appear on the *Labor Time Card* frame. It must be run on a daily basis.

After the process is scheduled it automatically runs every day. Use the *Holiday Calendar* frame to set the company holidays to automatically appear as part of the Employee Absence. This frame sample has a schedule set up to run daily.

Complete the steps.

1. To create a **Planned Absence** batch process, enter the **Date/Time to Start Run**.
2. Select the **Run Interval**.
3. Select the **Exclude weekends and holidays** checkbox, if applicable.
4. Select the **Schedule/Reschedule** button.

As part of your regular maintenance you can delete one time jobs that are not set to recur. See the *System Run List of Jobs* frame to complete this maintenance.

Repeat Work

Used in conjunction with enhanced *Repeat Repairs* functionality and System Flag 5212.

Run Billing Period

The **Run Billing Period** batch process produces a detailed report displaying all the items in the current billing period. It is not directly connected to the **End of Period** process. It can be run anytime you would like to examine the details of the items in the current billing period. The **Current Billing Period** is based on the last time you closed a *Billing Period* by running the **Close Billing Period** batch process. The report produced by **Run Billing Period** gives you the opportunity to find any mistakes in billing transactions before posting them to the current billing period ledgers.

The **Run Billing Period** process populates data into specific tables based on the configuration of the billing structure in the M5 System. After the **Run Billing Period** process is finished the reports should be carefully reviewed to make sure the data is correct. If not, corrections can be made and the **Run Billing Period** batch can be executed again as often as needed. After the data is verified the billing can be finalized by running the **Close Billing Period** process. After the **Close Billing Period** process is complete no additional changes can be made to the current period. Any changes discovered after this have to be corrected as adjustments in the new period and both items, the incorrect original charge and the corrected charge will appear in the audit trail.

Complete the steps.

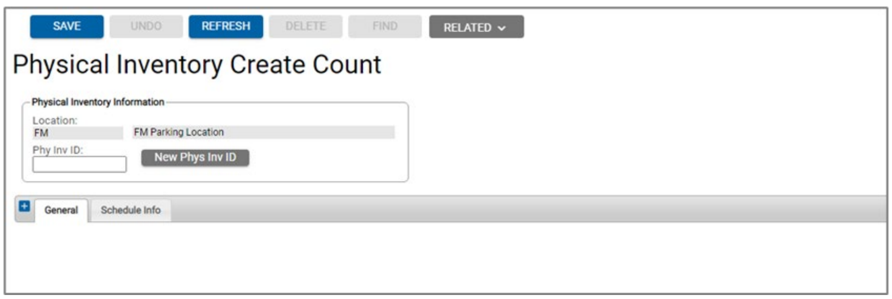
1. Select *Run Billing Period* from the **Batch Process** dropdown.
2. The **Billing Header** displays the current **Fiscal Year** and **Fiscal Period** for the billing transactions that display on the reports.
3. The **Run Type** setting is determined by the previous history of this batch. For example, *Re-Run Billing* displays as the type because it was already executed in the current Billing Period. The *Last Bill Run* information is shown here.
4. If the billing period has not already been closed you can set up the details discussed in the next steps. Most importantly, the **Run Type** includes *Run Billing* in addition to *Re-Run Billing*.
5. Enter the **Date/Time to Start Billing**. Selecting the field defaults to the current date and time.
6. Select the **Process Open Work Orders?** checkbox if you want the billing to include charges on open work orders.
7. **Daily Run Parameters** allows billing to be configured to run on a daily basis. You can select the **Mark Daily Run Transactions As Billed?** checkbox and control the end date of run.
8. Select the **Run Interval**.
9. Select the **Exclude weekends and holidays** checkbox, as applicable.
10. Select the **Schedule/Reschedule** button.

Unit/Component Record Purge

This batch process allows for the purge of disposed of (sold) assets after a determined amount of time has passed since the date of sale. The process selects and then permanently deletes asset records based on the defined batch process parameters when the user schedules the program.

Physical Inventory Create Count

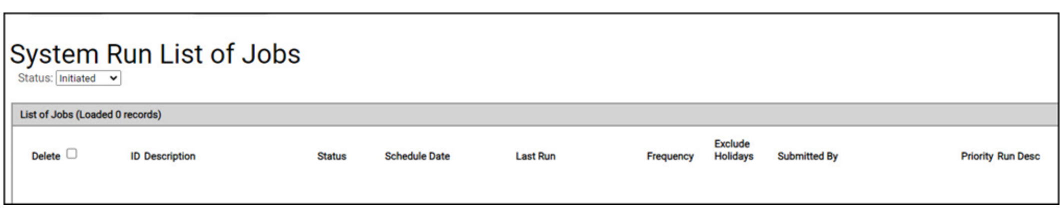
The **Physical Inventory Create Count** frame is used to create your count sheets and select the parts to be counted for your inventory. On the **General** tab select the **Method** you are going use and configure the schedule details on the **Schedule Info** tab. Select the **Schedule/Reschedule** button to run it as configured. Select **SAVE**.



System Run List of Jobs

The *System Run List of Jobs* frame displays all batch processes, status, run date, and submitted by. This frame can be used to determine what scheduled processes are set up to run and what is currently running.

Scheduled reports or reports still running can be deleted from here by highlighting the row and selecting the **DELETE** button. The row displays as red. Select **SAVE** to update the deletion.

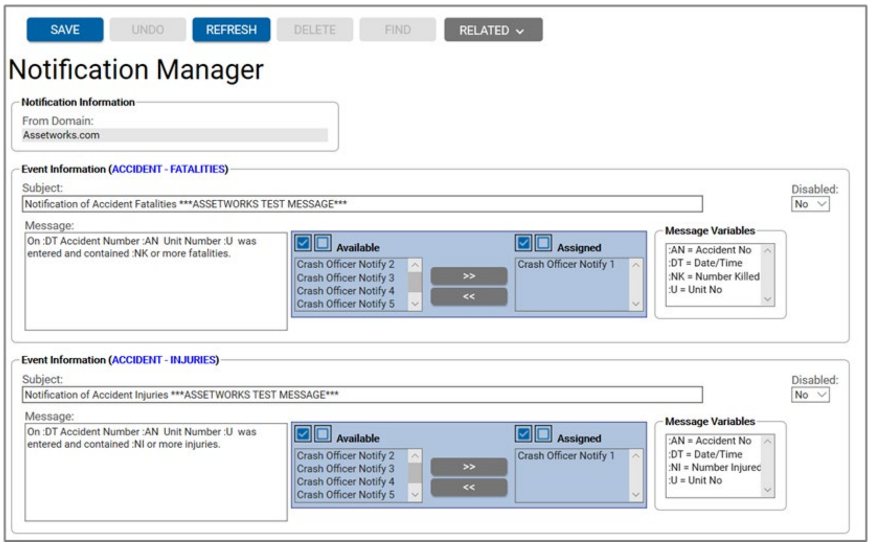


Section 16. Notification Manager

The **Notification Manager** frame functionality sends emails (notifications) to certain users when specific events take place within the system. These events can be reviewed using the *Notification History Query* frame.

There are several notifications that exist where special set up is required in order to use the event notification. These notifications require special items to be created and the value of these items can determine who the notification is sent to.

A notification event can be disabled so that it will not be used.



Available Notifications

The *Notification Manager* frame allows the user to enable or disable any of the notification events. The user cannot create their own notification; however, they can edit any of the notification **Subject** lines or **Message** content provided that are not disabled.

The variable used in the **Subject** line and **Message** will show the exact value for which the event occurred. For example, :U means the exact unit number will be shown in the email message.

Multiple emails can be sent to different people for certain notification events. For example, an email message can be sent for when a unit is sold. The message can be sent to both the owning department contact of the unit as well as the maintenance location contact.

Note: When you select the **Exclude from Unit Notifications** checkbox on *Category Main*, a notification is not sent for the category code.

Available Notifications list

Available Notification	Description
Accident Entry	When an accident is created, up to three people can be notified.
Acquire Unit	When an acquisition date is entered into Unit Main, one person can be notified.
Acquire Unit Fuel Card	When a fuel card is entered for a unit, one person can be notified. Two items are required.
Activate Unit	When a unit is put into service and has a replacement unit, one person is notified.
Activate Unit Commuter	When a unit is put into service, one person is notified.
Appointment Request Approved	Generated when a Maintenance Appointment Request is approved.
Appointment Request Cancelled	Generated when a Maintenance Appointment Request is cancelled.
Appointment Request Denied	Generated when a Maintenance Appointment Request is denied.
Appointment Request Made	Generated when a Maintenance Appointment Request is created.
Appointment Request Rescheduled	Generated when a Maintenace Appointment Request is created.
Budget Unit	When a unit is budget status, one peron is notified.
Class Changed	When any of the five user classes is changed.
Decommission Unit	When a decommissioned designated job is on a WO, one person can be notified.
Disp Unit – Close Card	When a unit is flagged, one person is notified to review the fuel card. One item is required.
Driver Event Approaching Expiry	Generated when a created driver event is approaching the expiry date.
Driver Event Expired	Generated when a created driver event expires.
Equipment Checked Out	Generated when an Equipment Request record is fulfilled (checked out).

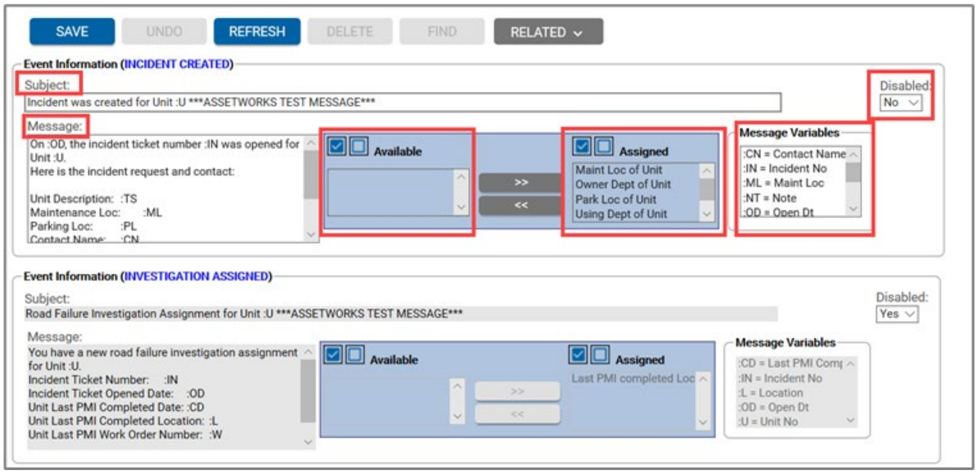
Available Notification	Description
Equipment Request Created	Generated when an Equipment Request record is created.
Fees	Generated when a fee charge or violation has been entered for the employee on the received date.
ICU Health Check	When an ICU reports a health check, up to one person can be notified.
ICU Low Battery	When a hose has a low battery condition, up to one person can be notified.
ICU Pulser Failure	If a has a pulser failure and up to three fuelings did not occur, up to one person can be notified.
ICU EM Status	Generated to provide updates on an ICU status change out of emergency mode.
Incident Created	Generated when an incident is created.
Investigation Assigned	Generated when a road failure investigation is assigned to a unit.
Invoice Correction Required	Generated when an invoice requires correction.
Invoice Rejected	Generated when an invoice is rejected.
Issue Request Rejected	When a part issue request is rejected, up to two people can be notified.
Keyvalet Controller Offline	Generated when the controlloer goes offline.
Keyvalet Failed Return	When a motor pool ticket cannot be completed by key valet, one person is notified.
Keyvalet Vehicle Keys Not Returned	Generated when the keys are not detected in the key box, either because they were not returned or returned improperly.
Motor Pool Cancelled	If a motor pool ticket is cancelled, up to two people can be notified.
Motor Pool Created	When a motor pool ticket is opened, up to two people can be notified.
Motor Pool Reservation Completed	When a motor pool ticket is completed, up to two people can be notified.

Available Notification	Description
Motor Pool Unit Assigned	When a vehicle is assigned to a motor pool ticket, up to two people can be notified. See System Flag 5513.
Motor Pool Unit Updated	If the Unit number that was assigned has been changed, up to two people can be notified.
Motor Pool Ticket Past Due	Generated when a motor pool ticket is past the return date or time.
Order Unit	When a unit is ordered status, one person can be notified.
Order Unit Fuel Card	When a new fuel card is assigned to a unit, one person can be notified.
Parking Loc Changed	When a parking location is changed for a unit, up to one person can be notified.
Part Request Created	Generated when a part request has been requested.
Part Request Ready	Generated when the part request is moved to a READY status.
Part Requisition Approved/Rejected	When a part requisition is approved or rejected, up to two people can be notified.
Part Requisition on Order	When a part requisition is added to a PO, up to one person can be notified.
Part Requisition Rejected	When a part requisition is rejected only, up to two people can be notified.
Part Transfer Request Created	Generated when a new part transfer request is created.
Reading out of Range	If a telematics reading is out of range, one person can be notified.
Request Approval Needed	If a unit request is awaiting approval, one person can be notified.
Request Rejected	If a unit request is rejected, up to three people can be notified.
Sell Unit	If a unit is sold, up to seven people can be notified.
Sensor Alarm	Generated for the location receiving the sensor alarm through Veeder Root into FleetFocus.
System Alarm	Generated for the location receiving the system alarm through Veeder Root into FleetFocus..

Available Notification	Description
Tank Alarm	When a tank has set off an alarm based on an event, up to one person can be notified.
Time Sheet Entry Rejected	Generated when a time sheet enty is invalid.
Unit Availability Status Change	When unit availability of an unit has changed, up to four people can be notified.
Unit Delivered	When an arrival date is assigned to a unit, one person can be notified.
Work Order Cancelled	Generated when a work order is cancelled.
Work Order Completed	Generated when a work order is completed.
Work Order Due Date Changed	Generated when a change to the due date is detected.
Work Order Opened	Generated when a work order is opened.
WR Created from Test Failure	Generated when a completed test suite creates work requests as a result of failed tests.

See *Notification Variables, Qualifications, and Recipients* for a complete listing of notifications and where the emails are retrieved from within the application.

Notification Break Down

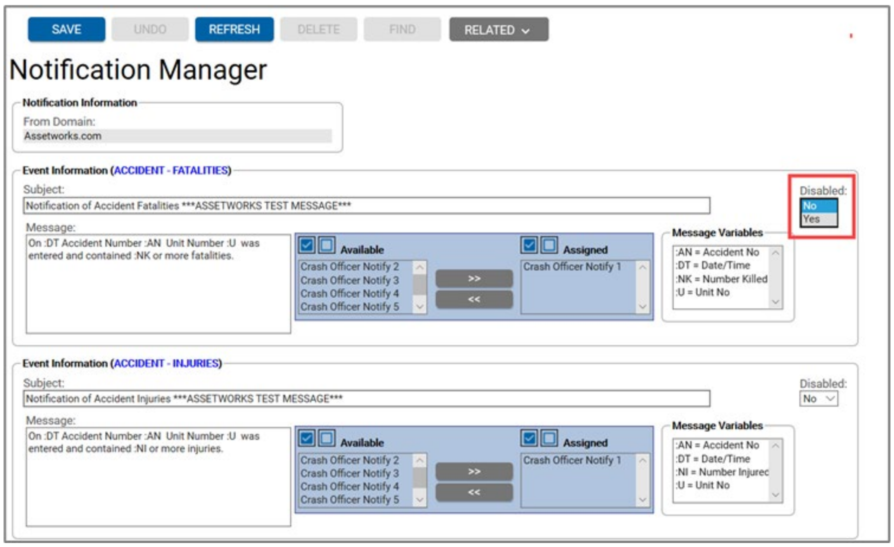


Notification field	Description
Subject	Subject line of the email generated. You can edit this field.
Message	Body of the email generated. You can edit this field.
Available	List of entities that can be notified.
Assigned	List of entities that will be notified.
Disabled	**Yes** – Disable a notification. **No** – Enable a notification. **Location** –System Flag 5496 is set to Y. Additional configuration is required on the Notifications tab of the Location Main frame.
Message Variables	List of variables that can appear in the message. **Note:** Variables are replaced with the actual values when the notification is generated.

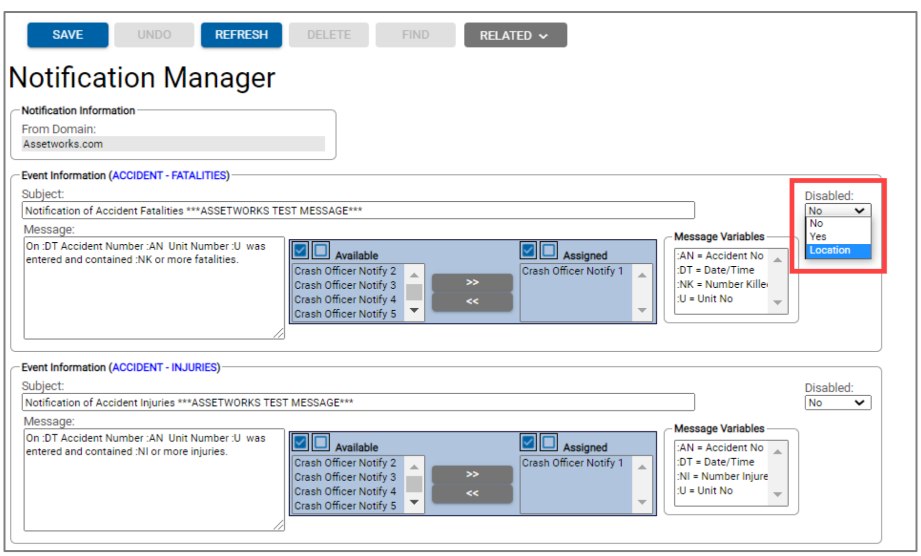
Disable or Enable a Notification

From the **Disabled** dropdown of a specific notification, complete the steps.

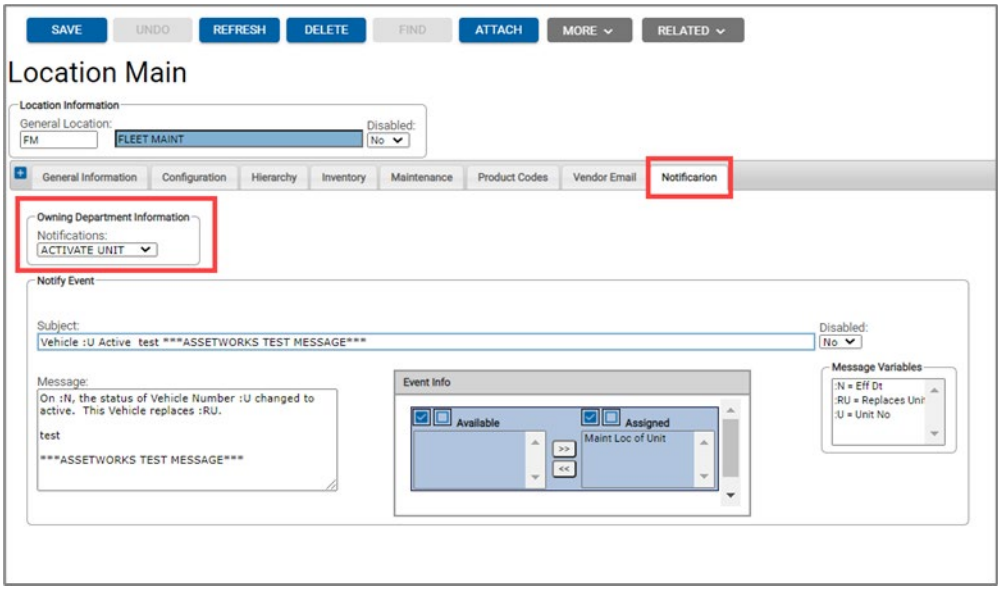
1. Select *Yes* to disable a notification.
2. Select *No* to enable a notification.
3. Select *Location* for a location specific notification. The **Location** is set on the *Location Main* frame.



Location Option



Location Main



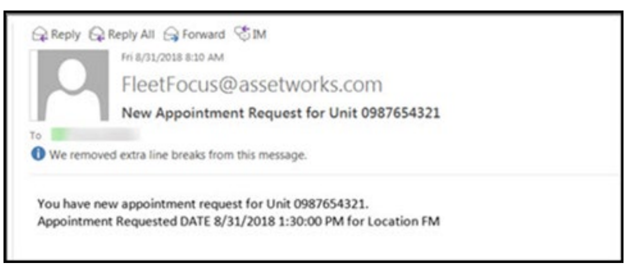
Edit Subject or Message

You can edit the notification **Subject** or **Message** when the notification is not disabled. If **Disabled** is *Yes*, the notification information is read-only.

When the system sends the email, the real data pertaining to that event will replace the variable. For example, the :U variable means the message will display the real unit number in the email message.

After making any changes, select **SAVE**.

Email Notification Example

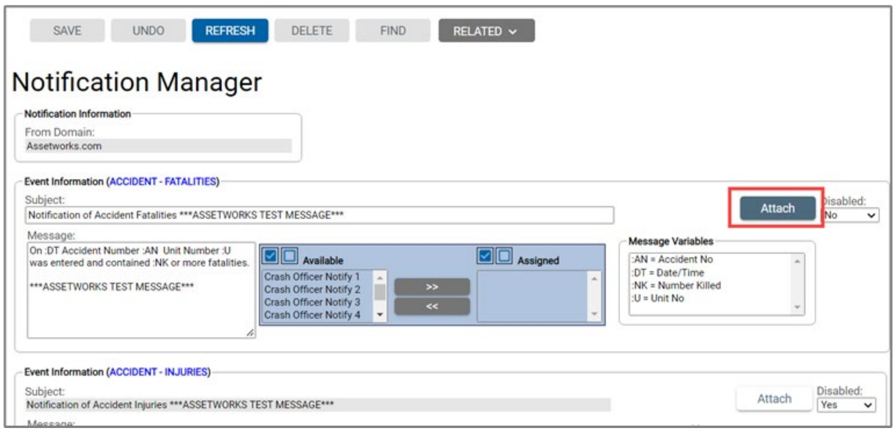


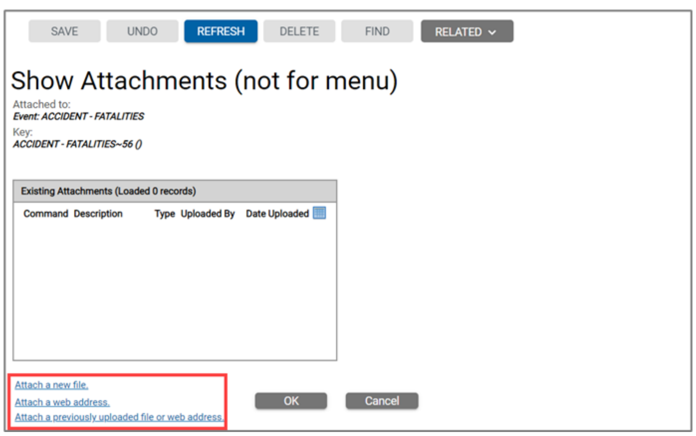
Add Attachments

You can add additional documentation to be included with the notification email in the form of attachments.

To add attachments to a specific notification, complete the steps.

1. Make sure the notification is enabled.
2. Select the **Attach** button.
3. In the *Show Attachments* window, use the links at the bottom to add the necessary attachments.
4. When finished, select **OK** to return to the *Notification Manager* frame.





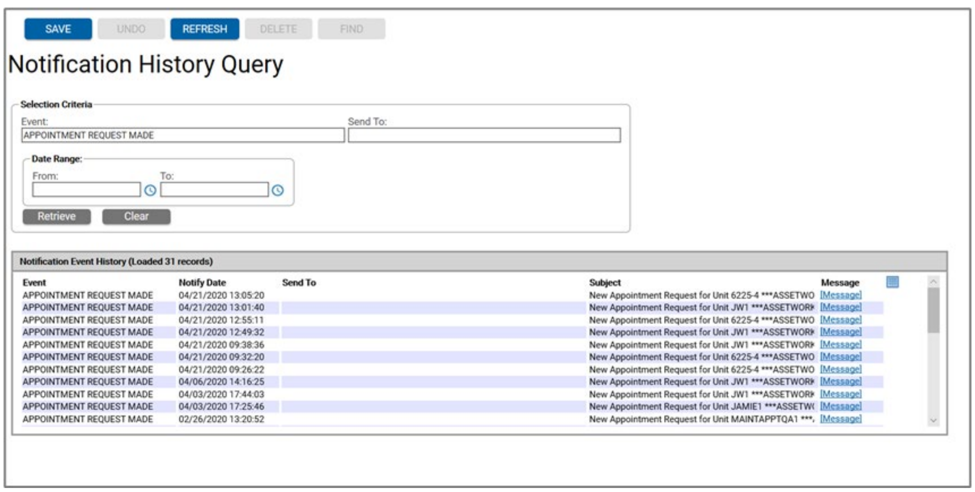
Notification History Query

Notification events that have occurred can be viewed using the *Notification History Query* frame.

The *Notification Event History* i-frame displays each notification event that has been sent including the **Event** name, **Notify Date**, **Send To** email address, and **Message** link. The **Message** link opens the *Notification History Message Information* window that allows you to view the message. You can filter the information by **Event**, **Send To**, and **Date Range**.

Complete the steps to generate the *Notification Event History* query.

1. Enter the **Event** name or double-click in the field to select from the Notification Event List of Values.
2. Optionally, enter an email address in the **Send To** field.
3. Narrow your results by entering a **Date Range**.
4. Select **Retrieve** to display the results matching your criteria. The results display in the *Notification Event History* i-frame.
5. To generate a new query, select **Clear** and enter new criteria.



Notification Variables, Qualifications, and Recipients

Event	**Message Variables**	**Qualification Variables**	**Email Address field**	**Special Qualifier**
ACCIDENT – FATALITIES	AN = Accident No. DT = Date/Time NK = Number killed U = Unit No.	Crash Officer 1 through 6	Email address associated with corresponding **Accident Item** from *Item Master Definition*.	System Flag 5476
ACCIDENT – INJURIES	AN = Accident No. DT = Date/Time NI = Number injured U = Unit No	Crash Officer 1 through 6	Email address associated with corresponding **Accident Item** from *Item Master Definition*.	System Flag 5475
ACCIDENT ENTRY	AN = Accident No. DT = Date/Time U = Unit No.	Supervisor of Operator, Administration and owning dept of unit	*Employee Main* email of supervisor of operator; accident item value = DCAS ACCIDENT EMAIL; department item value = CARS PREVENTION EMAIL.	
ACQUIRE UNIT	A = Arrival Date U = Unit No. RU = Replaces Unit ML = Maint Location	Maint Loc of Unit Using Dept of Unit Owner Dept of Unit	*Location Main* email address.	
ACQUIRE UNIT FUEL CARD	C = Card No. U = Unit No. O = Order Date PL = Parking Location	Park Loc of Unit	Location item value where item = FUEL CARD ADMINISTRATOR.	Unit item value = Y where item = FUEL CARD REQ'D.
ACTIVATE UNIT	N = Effective Date RU = Replaces Unit U = Unit No.	Maint Loc of Unit	*Location Main* email address.	

Event	**Message Variables**	**Qualification Variables**	**Email Address field**	**Special Qualifier**
ACTIVATE UNIT COMMUTER	N = Effective Date U = Unit No.	Park Loc Unit Act	*Location Main* email address of parking loc.	Activity code = COMMUTING
APPOINTMENT REQUEST APPROVED	AD = Appointment Date L = Location U = Unit Number	Maint Loc of Unit Park Loc of Unit Using Dept of Unit Owner Dept of Unit Vehicle Operator	Location Main email Department email Employee email	
APPOINTMENT REQUEST CANCELLED	AD = Appointment Date L = Location U = Unit Number	Maint Loc of Unit Park Loc of Unit Using Dept of Unit Owner Dept of Unit Vehicle Operator	Location Main email Department email Employee email	
APPOINTMENT REQUEST DENIED	AD = Appointment Date L = Location U = Unit Number	Maint Loc of Unit Park Loc of Unit Using Dept of Unit Owner Dept of Unit Vehicle Operator APPT Contact	Location Main email Department email Employee email	
APPOINTMENT REQUEST MADE	AD = Appointment Date L = Location U = Unit Number	Maint Loc of Unit Park Loc of Unit Using Dept of Unit Owner Dept of Unit Vehicle Operator APPT Contact	Location Main email Department email Employee email	
APPOINTMENT REQUEST RESCHEDULED	AD = Appointment Date L = Location U = Unit Number	Maint Loc of Unit Park Loc of Unit Using Dept of Unit Owner Dept of Unit Vehicle Operator APPT Contact	*Location Main* email *Department* email *Employee* email	

Event	**Message Variables**	**Qualification Variables**	**Email Address field**	**Special Qualifier**
BUDGET UNIT	B = Budget Date PL = Parking Loc U = Unit No.	Park Loc of Unit	*Location Main* email address.	
CLASS CHANGED	N = Effective Date NV = New Value OV = Old Value U = Unit No.	Class1 of Unit Class2 of Unit Class3 of Unit Class4 of Unit Class5 of Unit	*Department Main* email address of owning dept of unit.	If you only want notification when class 2 is changed, for example, then you select Class2 of Unit.
COMMERCIAL REQUEST FOR SERVICE REQUIRES APPROVAL	E = Emp No EN = Emp Name ML = Maint Loc W = WO No	Employee Supervisor, Location Item Service Request, Maintenance Location	**Employee's Supervisor Email** from *Employee Main*. Email address associated with the Location Item SERVICE REQUEST, and *Location Main* email.	
DECOMMISSION UNIT	J = Job code W = Wo No. N = Effective Date U = Unit No X = WO Comp Date	Park Loc of Unit Lease Admin	Location item value where item = LEASE ADMINISTRATOR.	
DISP UNIT - CLOSE CARD	U = Unit No. D = Disposal Date C = Card No.	Owner Dept of Vehicle Dept Item Bank	Department Item value where item = BANK EMAIL.	DISP UNIT - CLOSE CARD

Event	Message Variables	Qualification Variables	Email Address field	Special Qualifier
DRIVER EVENT APPROACHING EXPIRY	C = Pre-expiry notification D = Driver Number DN = Driver Name ED = Expiry Date NF = Notification T = Driver Event Type TD = Driver Event Type Date	Driver Department Driver Employee Supervisor Training Coordinator	Department Email Driver Email Employee’s Supervisor’s Email Email for Department Item TRAINING COORDINATOR that corresponds to employee/driver’s department on Employee/Driver Main.	
DRIVER EVENT EXPIRED	C = Pre-expiry notification D = Driver Number DN = Driver Name ED = Expiry Date NF = Notification T = Driver Event Type TD = Driver Event Type Date	Driver Department Driver Employee Supervisor Training Coordinator Email	Department Email Driver Email Employee’s Supervisor’s Email Email for Department Item TRAINING COORDINATOR that corresponds to employee/driver’s department on Employee/Driver Main	
DRIVER EVENT HIGH RISK	D = Driver Number DN = Driver Name DT = Date/Time E = Emp No. T = Driver Event Type	Driver Driver Department Employee Supervisor Training Coordinator Email	Driver Email Employee’s Supervisor’s Email Email for Department Item TRAINING COORDINATOR that corresponds to employee/driver’s department on Employee/Driver Main	

Event	Message Variables	Qualification Variables	Email Address field	Special Qualifier
EQUIPMENT CHECK OUT	E = Emp No EN = Emp Name U = Unit No UD = Unit Desc L = Location LD = Location Desc	Employee Supervisor(s) Location Requesting Employee	Requesting Employee Employee Supervisor Email Address Location	
EQUIPMENT REQUEST CREATED	E = Emp No EN = Emp Name EQ = Equip Type EQD = Equip Type Desc SK = SKU SKD = SKU Desc L = Location LD = Location Desc	Employee Supervisor(s) Location Requesting Employee	Requesting Employee Employee Supervisor Email Address Location	
FEES	E = Emp No FC = Fee Code FI = Fee Chg ID FS = Sub-Code IA = Issuing Authority LL = Login Loc RD = Received Date U = Unit No VD = Violation Date	Fee Contact Email Fee Department Email Fee Employee Email Fee Unit Operator Email Login Location Email Using Dept of Unit		Facilitates the delivery of standard documents to recipients associated with the Fee entry.
ICU HEALTH CHECK	DT = Date/Time ED = ICU Event Data IC = ICU No IE = ICU Event L = Location	ICU Event	Email set up for event on PRODUCT SETUP FUEL ISLAND.	FuelFocus

Event	**Message Variables**	**Qualification Variables**	**Email Address field**	**Special Qualifier**
ICU LOW BATTERY	H = Hose IC = ICU No. IE = ICU Event L = Location N = Effective Date	ICU Event	Email set up for event on *PRODUCT SETUP FUEL ISLAND*.	FuelFocus
ICU PULSER FAILURE	H = Hose IC = ICU No. IE = ICU Event L = Location N = Effective Date	ICU Event	Email set up for event on *PRODUCT SETUP FUEL ISLAND*.	FuelFocus
ISSUE REQUEST REJECTED	EN = Emp Name IR = Issue Request No. P = Part No. PE = Part Description	Reserve Ref No. Request Emp	*Department Main* email address. *Employee Main* email address of requestor.	Reserve Ref No. notification is only for a rejected part request for a department.
KEY VALET FAILED RETURN	MP = MP Ticket	Motor Pool Location	*Location Main* email address of MP location.	Key Valet
MOTOR POOL CANCELLED	MP = MP Ticket U = Unit No.	Motor Pool Location Request Emp/Dr No	*Location Main* email address of MP location. *Employee Main* email address of requestor.	
MOTOR POOL CREATED	EN = Emp Name MD = Msg Detail	Motor Pool Location Request Emp/Dr No	*Location Main* email address of MP location. *Employee Main* email address of requestor.	
MOTOR POOL RESERVATION COMPLETED	EN = Emp Name MD = Msg Detail MP = MP Ticket	Motor Pool Location Request Emp/Dr No	*Location Main* email address of MP location. *Employee Main* email address of requestor.	

Event	Message Variables	Qualification Variables	Email Address field	Special Qualifier
MOTOR POOL UNIT ASSIGNED	EN = Emp Name MD = msg Detail MP = MP Ticket	Motor Pool Location Request Emp/Dr No	*Location Main* email address of MP location. *Employee Main* email address of requestor.	
MOTOR POOL UNIT UPDATED	MP = MP Ticket NV = New Val OV = Old Val PD = Pickup Date	Motor Pool Location Request Emp/Dr No	*Location Main* email address of MP location. *Employee Main* email address of requestor.	
ORDER UNIT	U = Unit No. O = Order Date PL =Parking Location	Park Loc of Unit	*Location Main* email address.	
ORDER UNIT FUEL CARD	C = Card No. U = Unit No. O = Order Date PL = Parking Location	Unit Fuel Card Admin	Location Item Value where item = FUEL CARD ADMINISTRATOR.	Unit item value = Y where item = FUEL CARD REQ'D (Y/N).
PARKING LOC CHANGE	N = Effective Date NV = New Value OV = Old Value U = Unit No.	Park Loc of Unit	*Location Main* email address for old value and new value.	
PART REQUEST CREATED	E= Emp No EN = Emp Name IL = Inv Loc P = Part No PE = Part Description W = WO No	Inv Loc Restock Employee Supervisor Email Location Item PART REQ CREATED	*Location Main* email address.	

Event	**Message Variables**	**Qualification Variables**	**Email Address field**	**Special Qualifier**
PART REQUEST READY	E= Emp No EN = Emp Name IL = Inv Loc P = Part No PE = Part Description W = WO No	Inv Loc Restock Employee Supervisor Email Location Item PART REQ CREATED	*Location Main* email address.	
PART REQUISITION APPROVED/ REJECTED	AL = Approve List L = Location RL = Reject List RN = Part Req No.	Inv Loc Restock Part Req Approved	*Location Main*, email restock messages to email. *Application User* email address of person generated part requisition.	
PART REQUISITION ON ORDER	AL = Approve List L = Location PO = PO Number	Inv Loc Restock	*Location Main*, email restock messages to email.	
PART REQUISITION REJECTED	L = Location RL = Reject List RN = Part Req No UN = Requestor	Inv Loc Restock Part Req Approved	*Location Main*, email restock messages to email. *Application User* email address of person generated part requisition.	
PART TRANSFER REQUEST CREATED	E = Emp No. EN = Emp Name ILF – Inventory Location (from) ILT = Inventory Location (To) P = Part No PE = Part Description	Employee Supervisor(s) Inv Loc Restock (From) Inv Loc Restock (To)	Inv Loc Restock (From) Inv Loc Restock (To) Employee Supervisor Email *Location Main* email	
READING OUT OF RANGE	ML = Maint Loc U = Unit No.	Maint Loc of Unit	*Location Main* email address of Maint Loc.	Telematics

Event	**Message Variables**	**Qualification Variables**	**Email Address field**	**Special Qualifier**
REQUEST APPROVAL NEEDED	UR = Unit Request No. U = Unit No.	Unit Req Approval	Employee Main email address where the application user employee number field matches and database user as Tier 2 privilege.	
REQUEST REJECTED	UR = Unit Request No. U = Unit No.	Request Emp Requestor Unit Req Approval	*Employee Main* email address where the application user employee number field matches the unit request record.	
SELL UNIT	S = Sell Date U = Unit No.	Maint Loc of Unit Park Loc of Unit Location Item County Owner Dept of Unit Dept Item Acct. Dept Item Flt. Mgr Location Item DMV	*Location Main* email address. Location item value where item in DMV Email, County email. Dept item value where items = Fleet Manager, Accounting Contact.	
SENSOR ALARM	ED = ICU Event Data IC = ICU No IE = ICU Event L = Location N = Eff Dt SS = Sensor	ICU Event	Email set up for event on *Product Setup Fuel Island.*	
SYSTEM ALARM	ED = ICU Event Data IC = ICU No IE = ICU Event L = Location N = Eff Dt	ICU Event	Email set up for event on *Product Setup Fuel Island*.	

Event	Message Variables	Qualification Variables	Email Address field	Special Qualifier
TANK ALARM	ED = ICU Event Date IC = ICU No. IE = ICU Event L = Location N = Effective Date T = Tank	ICU Event	Email set up for event on *Product Setup Fuel Island*.	
UNIT AVAILABILITY STATUS CHANGE	CM = Comment N = Effective Date SD = Status Desc ST = Status	Operator Supervisor Unit Avail Notify Vehicle Operator Vehicle Parking Location	Email from *Employee Main*.	Employee must be designated as an operator.
UNIT DELIVERED	U = Unit No. A = Arrival Date PL = Parking Location ML = Maint Location	Maint Loc of Unit	*Location Main* email address.	
WORK ORDER CANCELLED	DT = Date/Time L = Location U = Unit No W = WO No	Unit Item High Priority Unit Using Dept (WO) Vehicle Operator (WO)	Email address assigned to the Unit Item HIGH PRIORITY EMAIL. Work Order Using Department Email. Email of Employee Assigned as Operator of the Unit on the Work Order.	**Send WO Notifications** checkbox must be selected on the **Location Main Maintenance** tab.

Event	**Message Variables**	**Qualification Variables**	**Email Address field**	**Special Qualifier**
WORK ORDER COMPLETED	DT = Date/Time L = Location MA = Maint APPT ID U = Unit No W = WO No	Appointment Contact Unit Item High Priority Unit Using Dept (WO) Vehicle Operator (WO)	Email for the **Appointment Contact** on *Maintenance Request Appointment*. Email address assigned to the Unit Item HIGH PRIORITY EMAIL. Work Order Using Department Email. Email of Employee Assigned as Operator of the Unit on the Work Order.	**Send WO Notifications** checkbox must be selected on the **Location Main Maintenance** tab.
WORK ORDER DUE DATE CHANGED	CR = Change Code Reason Description	Location Controller Owning Department Using Department Vehicle Operator	Email addressed assigned to Location Item LOCATION CONTROLLER. Owning Department Email assigned to **Unit** on *Work Order*. Using Department Email assigned to **Unit** on *Work Order*. Email of Employee Assigned as Operator of the Unit on the Work Order.	
WORK ORDER OPENED	DT = Date/Time L = Location U = Unit No W = WO No	Unit Item High Priority Unit Using Dept (WO) Vehicle Operator (WO)	Email address assigned to the Unit Item HIGH PRIORITY EMAIL. Work Order Using Department Email. Email of Employee Assigned as Operator of the **Unit** on the **Work Order**.	**Send WO Notifications** checkbox must be selected on the **Location Main Maintenance** tab.

Event	Message Variables	Qualification Variables	Email Address field	Special Qualifier
WR CREATED FROM TEST FAILURE	DT = Date/Time L = location T = Test Suite Description U = Unit No. WR = Work Request	Maint. Loc of Unit Owner Dept of Unit Using Dept of Unit Vehicle Operator	*Location Main* email address *Department Main* email address *Employee Main* email address	

Section 17. Email

Email Group

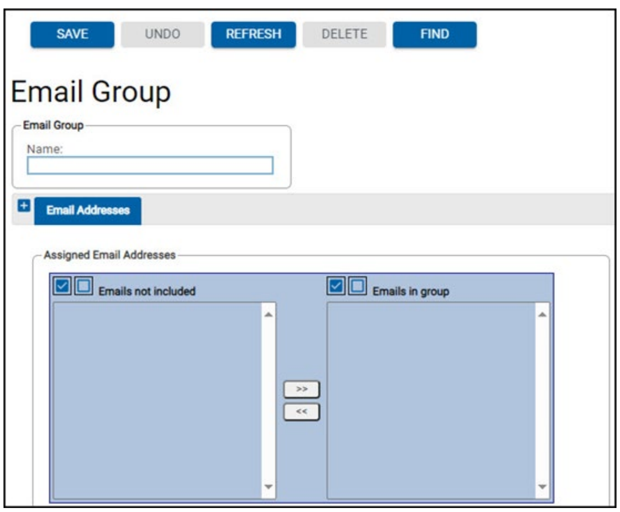
The *Email Group* frame allows you to manage email groups and assign email addresses to those groups. The *Email Group* functionality applies to each email, email notification, and email address field in M5.

System Flag 5249 controls when to use only validated email addresses and email groups.

When the System Flag is set to **Y**, only email addresses created in the *Email Address Maintenance* frame or an *Email Group* can be used. If not, any email address or email group can be entered within the application, but email groups will not function.

Note: When System Flag 5410 is set to **Y**, if the value entered is an email address (without the domain) and it corresponds to an email group, the email group and not the singular email address is used.

If you are using LDAP authentication with System Flag 5249 set to **Y**, this prevents you from logging on to the system if your email address has not been entered in the *Email Address Maintenance* frame.



Email Address Maintenance

The *Email Address Maintenance* frame manages a list of email addresses that are used for reports and other features of the M5 System. If System Flag 5249 is set to **Y**, the user is prompted to select an **Email Address** from the list of addresses entered here. In order to add an address open the *Email Address Maintenance* frame. Enter a new **Email Address** on the last blank row of the table. Existing email addresses can also be disabled. Select **SAVE** to update the records.

There is a limit to the total length of the email address on this frame. Currently it can only be 30 characters long.

Note: This is a separate email process than the one that sends an email to the Application User's email address for scheduling notifications. These use the email address provided on the *Application User Maintenance* frame.

Special Character Rules

An **Asterisk (*)** cannot be used as the first character of a key field.

A **Forward Slash (\)** is only allowed to specify a host name where it is always **Double Slash (\\)**.

A single **Forward Slash (\)** can be used in directory names but they are automatically converted to forward slashes.

Characters **;^~|** are prohibited in all fields.

Characters **;^~<>'|** are prohibited in fields that are validated by using the database lookup.

Appendix A. Role Privileges

See the *Role Privileges Table* for a complete listing of role privileges.

Appendix B. System Flags

See the *System Flags Table* for a complete listing of system flags.

Appendix C. M5 Params

Variable Name	Description	Comment
ACTIVATION_KEY	This code supplied by AssetWorks activates special features or options in the product that you have licensed.	
ADHOCBI_API_SITE	Defines the API site that contains the new version Adhoc software.	Defaults to /M5AdhocBIApi.
ADHOCBI_RPTDB_USE	Use a reporting database for adhoc reports? (Y or N)	Setting this to Y also requires adding the connection string for the reporting database to M5_INIT.RPT_CONNECT_STRING. An existing connection string in Izenda will need to be deleted on Adhoc Query Admin screen, and recreated using Sync Datasources.
ADHOCBI_SITE	Defines the core site that contains the new version Adhoc software.	Defaults to /M5AdhocBICore.
ADHOCBI_SUPER_USERS	List of Adhoc Super Users who will have access to settings tab.	
ADHOCBI_TENANT_ID	The TENANT ID to use for Adhoc.	Defaults to COMPANY CODE.

Variable Name	Description	Comment
ADHOC_REPORT_PATH	The directory where Legacy Adhoc reports are stored. This directory, much like the ATTACHMENTS_DIR must be a shared directory available to all servers. This parameter only needs be valued if you are licensed for Adhoc reporting in FleetFocusM5. There is a component of the activation key to allow Adhoc access.	If M5 is installed in a load balanced environment, this directory must be a shared directory, so the reports are available to all servers. This directory must be writable by the identity that runs the M5 IIS web services.
ADHOC_SITE	Defines the site that contains the Adhoc software.	Defaults to /M5Adhoc.
ADHOC_WEB_SERVER_LIST	When running Adhoc in a web farm this parameter must list the rs.aspx page for each machine in a comma delimited list. If not running in a server farm this parameter should be null.	Example: http://m5apb01/m5web/adhoc/rs.aspx http://m5atb02/m5web/adhoc/rs.aspx http://m5atb03/m5web/adhoc/rs.aspx
ADMIN_ SETTINGSREFRESHSECS	Number of seconds to preserve user's settings in server cache, 0-3600.	Set to 0 during setup so changes take effect immediately.
ADMIN_ SETTINGSSHOWALERTS	Show response pop up for system vehicle alerts?	
ASSET_TYPE_SQL	This is used by the Performance Measures and Monitor module of FleetFocus. It needs to be valued with a SQL Statement that describes the asset type used by PMM. AssetWorks will work with the client to properly set this value. PMM is a licensed module that requires an appropriate activation key to access the module.	

Variable Name	Description	Comment
ATTACHMENTS_ALLOW_URN	Allows association to a file that has not been uploaded into M5.	If "N" the "attach windows file" link will not be shown. This should normally be "N" or null because it has additional security requirements and is problematic if the files are moved or deleted outside M5 This option requires that all end users that need to view these files have security to read them directly. This will not work if you cannot open the file from your machine with your windows credentials. If "Y", the user will be allowed to associate files that are not uploaded into M5 with an M5 record the same way normal attachments are handled. This option is only available in Internet Explorer. Forward slashes must be used. A third option is available for this parameter and that is to specify a directory root. In this mode all URN attachments must exist in this one directory.
ATTACHMENTS_DIR	The directory under ATTACHMENTS_ROOT where attachments are to be stored.	If M5 is installed in a load balanced environment, this directory must be a shared directory, so the attachments are available to all servers. This directory must be writable by the component's identity account and readable by an M5 web user. For non-authenticated sites, it must be readable by the IIS anonymous user account. The highest level of the value specified here must be the same as the virtual directory name used to view the files. **Note:** Use forward slashes only.

Variable Name	Description	Comment
ATTACHMENTS_EXTENSIONS	This is a semi-colon delimited list of file extensions that may be uploaded to the server. This list will default to allow all files to be uploaded except executables.	Executables are never uploaded to the server. Executables extensions include com, exe, bat, cmd and dll files.
ATTACHMENTS_ROOT	This is normally the Web Site root for example ("c:/inetpub/wwwroot").	This must be the real directory, not the virtual directory as addressed by the web server. If not specified, the file attachment feature will not be available.
CE_EMAIL_AUTHENTICATION	Email authentication type used to access the mail server when Crystal Enterprise emails report output. 0 = no authentication 1 = Plain text 2 = Login If "0" is selected, CE_EMAIL_USER and CE_EMAIL_PASSWORD are not relevant.	
CE_EMAIL_BODY	Email body text used when a report is delivered to a user via email.	This can have links to where the user can obtain the free Crystal report viewer.
CE_EMAIL_DOMAIN	This is the domain name of the site's SMTP server.	
CE_EMAIL_OVERRIDE _SENDER	Override email from address for all reports.	Normally this should not be set. The email address will then become the email address of the user running the report. If it is necessary to override this value, this can be set to a value such as "server@yourdomain.com".
CE_EMAIL__PASSWORD	This is the password to the SMTP mail server if authentication is required.	
CE_EMAIL_PORT	The port the SMTP server listens on. The default is 25.	

Variable Name	Description	Comment
CE_EMAIL_SERVER	This is the name of the site's SMTP server.	
CE_EMAIL_SSL	Send email using SSL.	Y or N.
CE_EMAIL_USER	This is the user id to the SMTP mail server if authentication is required.	N/A
CE_GROUP_IMMEDIATE_JOB	The Crystal Enterprise server group that handles Run Immediate reports.	This value is determined during the BOE or CRS install.
CE_GROUP_LONG_JOB	The Crystal Enterprise server group that handles long running or low priority reports.	This value is determined during the BOE or CRS install.
CE_GROUP_MEDIUM_JOB	The Crystal Enterprise server group that handles medium priority reports.	This value is determined during the BOE or CRS install.
CE_M5CRYSTAL_HOST	This overrides the protocol and host name used to make requests to the M5Crystal website.	If unspecified the default is the WEB_HOST parameter and if that is null, then it will use the protocol and host used to log into M5.
CE_SUPPORT_RPT_FORMAT	N=Not Supported (Default) Y=Supported	If you choose to turn this on you must understand it is your responsibility to provide the software to support the .rpt format. This means if users receive a .rpt formatted file via email the user must have at least the Free Crystal viewer installed on their desktop. If the users schedule .rpt formatted reports to the in-bin, the web server must either have Crystal Reports installed to process these files or they must create a new IIS mime type that associates the .rpt extension to application/crystal. This mime type will allow IIS to service the extension and allow the client to either open the file with their locally installed software or save it to their disk.
CODE_LOCALE_IDS	Sets the three locale_ids used when displaying code descriptions in other languages. The local ids are separated by a semi-colon.	**Note:** You need to set this to match the locale you are supporting. For instance, if you allow ES-MX to roll-up to ES you must enter ES here.

Variable Name	Description	Comment
CRYSTAL_EXTERPRISE_APS	The name of the Crystal Enterprise machine that M5 will connect to for all users.	This is the APS name entered while installing BOE or CRS. This is not an IP address and it does not begin with back slashes.
CRYSTAL_ENTERPRISE_BIN_DIR	The directory structure under the BIN_ROOT where the bin output is stored. This is easier if you think of this as just the share name. The top-level directory specified here will become the Virtual Directory name on the M5 IIS server.	Example: /CE_BIN
CRYSTAL_ENTERPRISE_BIN_LOCAL	Local path that is located on the Crystal server. This is used to write the output from the Crystal Services without needing to use the URN created by the concatenation of “bin_root” and “bin_dir”.	This should normally be null. Set this only if changing the user in the Central Management Console does not solve the permission problem when trying to write to the M5 in-bin.
CRYSTAL_ENTERPRISE_BIN_QUOTA	This parameter allows an installation to enter a space quota for in-bin directories.	The default is 0 which means unlimited. If 100 is entered, each folder can contain up to 100 megabytes. If the quota is exceeded the user must delete files to drop below the limit or they will not be allowed to view reports in that folder.
CRYSTAL_ENTERPRISE_BIN_ROOT	The machine name that owns the shared bin area.	Example: \\M5CEBIN **Note:** It can only be a local specification if the web server and the crystal server are on the same machine.
CRYSTAL_ENTERPRISE_ODBC	The ODBC name to be used for all reports executed in Crystal Enterprise.	
CRYSTAL_EXTERPRISE_OUTPUT_PATH	A directory on the Crystal Enterprise machine where report output can be written.	This directory should be shared so the end user can access the output file. Set this value and any output path in the application user to null to turn off the "file" feature.

Variable Name	Description	Comment
CRYSTAL_ENTERPRISE _RPTDB_ODBC	The ODBC name for the reporting database to be used for all scheduled reports to be executed in Business Objects Enterprise or Crystal Report Server.	
CRYSTAL_ENTERPRISE _RPTDB_USE	Use a reporting database for schedule reports? (Y or N)	Setting this to Y also requires adding the connection string for the reporting database to M5_INIT.RPT_CONNECT_STRING and creating an ODBC connection on the Crystal/BOE server. After configuration, reports will need to be rescheduled
CRYSTAL_ENTERPRISE _VERSION	The version of Crystal Enterprise that M5 will be connecting with.	Valid values are BOE (Business Objects Enterprise) or CRS (Crystal Report Server).
DEFAULT_HOMEPAGE	This is the homepage that will be used for clients that did not license screen designer and for all users that do not have a private home page specified in their application user definition.	Defaults to AWHP_DEFAULT1
DEFAULT_LOCALE_ID	Default Locale used for batch jobs.	Defaults to EN-US.
EMPLOYEE _CONTINUOUSCLOCK	Required employees to punch into something when punching out, except for a Clock out button.	N/A
ENCODING	Defines the character encoding being done to support the characters needed by the language.	For English it should be ISO-8859-1. For Unicode it should be set to UTF-16.
EXTERNAL_AUTH	Semi-colon delimited list of external authentication methods to be used. The user id is extracted from the HTML headers or interface and the logon screen is not presented to the user.	The value(s) entered here must be supported authentication types. Refer to the section on external authentication for more information.

Variable Name	Description	Comment
EXTERNAL_AUTH_LDAP _BASE_USER	A USER_APP record that will be used as the basis for creating a new user if allowing automatic user creation.	If not using LDAP or SAML authentication this parameter can be left blank. For LDAP or SAML authentication this must be a valid user even if the create feature is off.
EXTERNAL_AUTH_LDAP _CREATE_USER	When using LDAP or SAML authentication a "Y" in this parameter indicates that the shadow M5 USER_APP record should automatically be created if the user has never logged on before.	If not using LDAP authentication this parameter can be left blank. If this is not a "Y" the M5 user record must be manually created before the user can connect. If you are using active directory, this is now functioning the same as NT authentication which may be a simpler setup and more secure choice for your installation.
EXTERNAL_AUTH_LDAP_DE F_ROLE	When the M5 LDAP or SAML interface creates a new application user record the role will be set to this value.	The role can be mapped to an LDAP attribute. This parameter value will only be used when the mapped value is blank or was not supplied by the LDAP interface.
EXTERNAL_AUTH_LDAP _PATH	When using LDAP authentication this is the path to connect to the LDAP server.	Example: LDAP://adserver.mydomain.com:3389/cn=Users, dc= asd, dc=east.
EXTERNAL_AUTH_NOT_M5_ USER_URL	This is a URL where the user will be redirected when the user id extracted from the HTTP headers is not a valid M5 user id.	If specified, it must begin with http://. If LDAP authentication is implemented with the "CREATE_USER" option, the M5 user will automatically be created making the value of this parameter moot.
EXTERNAL_AUTH_NO_USER _URL	This is a URL where the user will be redirected if the user id information is not found in the HTTP headers when the system is in external authentication mode.	If specified, it must begin with http://.
EXTERNAL_AUTH_SAML_IDP _URL	This is the URL M5 will use to transfer to the SAML identity provider.	

Variable Name	Description	Comment
FROM_EMAIL_NAME	The name that will be used as the email "from" for some processes.	Defaults to "FleetFocus".
GENERAL_ATACHMENT_ HOST	Server where the attachments are located.	Probably the M5 application server.
GENERAL_MESSAGEPOLLIN GINTERVAL	The number of seconds between each poll of the database for messages.	Default of 60 seconds.
INSTALL_ROOT	The physical directory where MFIVE is installed.	Normally C:/MFIVE or C:/INETPUB/WWWROOT. This is the physical directory above the compiled web code tree.
INTERFACE_FILE_ROOT	The root directory for interface files	
INVENTORYCOUNT_COMPLE TEDSINCE	Location Inventory Counts, and My Inventory Counts pages show counts completed in the last X days.	
INVENTORYCOUNT _INDIRECTCODE	The default Indirect Account if inventory count has none defined.	
JS_SERIALIZER_MB	Sets the JavaScript Json Serializer max length in megabytes. The minimum value is 16 and the maximum is 200.	
LOGON_DOMAIN_ SPECIFICATION	Provide options to make entry of the user id more compatible with other applications the user accesses every day.	A = Add the CE_EMAIL_DOMAIN value to the user id if a domain was not specified. R = Remove all domain specifications. N = Do nothing (default) This is only used for LDAP and M5 authentication. LDAP and M5 user processing is done before authentication. SAML is done after so this parameter will not affect the user id that gets entered at the IDP site.

Variable Name	Description	Comment
LOGON_FAILURE_LIMIT	The number of consecutive times a user may enter a wrong password before having their account locked.	After the account is locked it must be unlocked by an M5 administrator. If this parameter is not defined it will default to 3.
LOGON_IMAGE	The name of the image file or files (in the image virtual directory) that will be displayed on the logon page. If you specify multiple images they must be delimited with a semi-colon. Multiple images will be displayed in sequence.	The image file may be any valid format that can be displayed by the browser. This parameter is site specific meaning the m5site may be specified in the “scope” field. If the site value is not found, the parameter with a scope of an asterisk will be used.
LOGON_INACTIVE_DAYS	If an account has not been used for this number of days, it cannot be used again without administrator’s interaction.	Default is 90 days. This parameter does not apply if using external authentication.
LOGON_MENU_IMAGE	The name of the image file displayed on the top left of the M5 screen above the user’s menu. If you need to differentiate your different M5 environments, you may specify a background color with the image name. For instance, you could specify “menu_frame_logo.png;green”. Assuming the image file is transparent, this command would change the background to green without the need of creating an alternate image. Prefix the path with “../../images/”.	Defaults to “menu_frame_logo.png”. If you specify a background color it must be separated from the image name with a semi-colon. The image must be transparent to support this feature. You may specify the color as a named color or using the #rrggbb hex format.
LOGON_MULTIPLE_TIMES	A value of “N” prevents the same application user from having multiple simultaneous sessions.	Primarily used for clients that have a user license.

Variable Name	Description	Comment
LOGON_REMEMBER_USER _ID	Controls if the “Remember my logon information” checkbox is displayed on the logon screen.	Valid values are Y, N, and U. If the installation does not allow security information being stored in cookies this should be set to an “N”. A value of U means only to remember the user ID and not the password. When using external authentication and this value is defined as Y, it is forced to be a U so that non M5 passwords never stored in M5. This parameter is site specific meaning the m5site may be specified in the “scope” field. If the site value is not found the parameter with a scope of an asterisk will be used.
LOGON_TWO_FACTOR	Two factor authentication mode for M5 users	The scope of this parameter is site. Null = none (default) EMAIL = All users are sent a one-time code that is required to logon. EMAIL_BY_ROLE = Users that have a role that specifies two factor authentication will be sent a one-time code required to logon. The email is sent to the application user’s email.

Variable Name	Description	Comment
LOGON_TWO_FACTOR _PORTAL	Two factor authentication mode for portal users.	The scope of this parameter is site. Null = none (default) EMAIL = All users are sent a one-time code that is required to logon. EMAIL_BY_ROLE = Users that have a role that specifies two factor authentication will be sent a one-time code required to logon. Note: The role is the role of the surrogate user. The email is sent to the email address on the EMP_MAIN table.
LOGON_USER_CHANGE_PW	A value of “Y” adds a checkbox to the logon page that allows the end user to change their application password.	Valid values are "Y" and "N". When using external authentication this parameter is ignored. This parameter is site specific meaning the m5site may be specified in the “scope” field. If the site value is not found the parameter with a scope of an asterisk will be used.
LOGVIEWER_DIRECTORIES	This specifies the list of servers to view logs from. UNC path(s) to the M5TMP folder separated by semicolon.	Semicolon separated list of network shares(s).
LOGVIEWER_EXCLUDED _PREFIXES	Specifies the log prefix folder(s) to exclude from the viewer, separated by semicolon.	Semicolon separated list of categories (<Prefix Folder>) to exclude from the Log Viewer frame. Only applies when INFO=ANY is used.
LOGVIEWER_FILE_DIR	This specifies the root level folder name for log files stored under the M5TMP folder. If unspecified the default is "M5LOGS". If specifying, recommendation is to use site name.	Root Folder definition. (Primarily needed for ASP clients). If left blank, the <Root Folder> will default to 'M5LOGS'

Variable Name	Description	Comment
MASTER_COMPANY	For Oracle Enterprise installations that share code tables between multiple VPD companies this specifies the code of the company that owns and can maintain the shared tables.	If the installation is not using Oracle Enterprise or is not using shared code tables, this parameter should be left blank.
MAX_DASHBOARD _PROCESS_PER_RUN	Controls the maximum dashboards that will be processed in one execution of BinScan. A value of 0 means all expired dashboards will be processed. If not specified this value will default to 20. **Note:** REPORT_BIN_SCAN_MINUTES controls how often BinScan runs.	This value will help the BinScan Page from timing out. The value must be high enough so the dashboard process can get through all the dashboards before they start expiring again.
MAX_DASHBOARD_RECS	The maximum number of rows that can be returned by any dashboard SQL in XML mode.	This does not cancel the query; it prevents the creation of XML rows in the table. If not specified, defaults to 5000.
MAX_LOV_RECS	The maximum number of rows that can be returned by any "list of values" request.	If a request is made that returns more rows than allowed a message is displayed at the end of the list indicating the list is not complete.
MESSAGE_ENCRYPTION	This controls the encryption level on all messages sent to the web server. When this parameter is changed, the change will not be picked up until the user logs off and back on.	0=No encryption. This should only be used for problem diagnostics. 1=Session encryption. All messages from the user session are encrypted with the same random key. This is the default value. 2=Utilize a nonce where the encryption key changes for every page.
MULTI_CURRENCY_ACTIVE	A value of Y activates the multi-currency features of M5. To activate this feature involves creating database triggers and several other setup steps.	

Variable Name	Description	Comment
MULTI_CURRENCY_BASE _CURRENCY	The three-character base currency.	The multi-currency feature of M5 requires database changes so this option cannot just be turned on to activate the feature.
OFF_HOURS	"Off peak hours" when Crystal Reports should be run.	This time is expressed in 24-hour clock format. This value is used when a user pressed the "Off Hours" button when scheduling a Crystal report.
ORACLE_USER_DEFAULT _QUOTA	The space limit an Oracle user may consume in the default tablespace.	This value is only used when the user id is created.
ORACLE_USER_DEFAULT _TABLESPACE	The default tablespace for Oracle accounts that are created through the M5 application.	This value is only used when the user id is created.
ORACLE_USER_TEMP_TABL ESPACE	The temporary tablespace for Oracle accounts that are created through the M5 application.	This value is only used when the user id is created.
PAGE_PAGESIZE_DEFAULT	Records to show per page as a default.	
PAGE_REFRESHSECONDS	A page with a refresh button automatically refreshes every this many seconds.	
PAGE_TACH_TOOLBARREFR ESHSECS	How often should the assigned tasks count be refreshed?	
PARTS_REQUEST _APPROVALREQUIRED	Do part requests require approval at all?	
PARTS_REQUEST _MAKEREADYNEEDED	Does the storekeeper need to move it to READY manually when available/	
POPULATE_SECURITY _FIELDS	Indicates to the buildSecureField method that it should maintain the FRM_WITH_SECURABLE_FIEL DS and FRM_SECURABLE_FIELDS tables. Valid values are "Y" and "N".	Automatically inserts default data for new frames. **Note:** The field name is used as the column name so it will not be internationalized. **Note:** This feature does add overhead to page generation because extra SQL commands must be executed to determine if the tables are up to date.

Variable Name	Description	Comment
PROJECT_HELP	The directory name (path) of the M5 help site.	The value is normally /M5Help/WebHelp
PROJECT_HELP2	The help directory for the first additional locale.	
PROJECT_HELP3	The help directory for the second additional locale.	
PW_EXPIRE_DAYS	This defines how many days a user password will remain valid.	A value of null or 0 means the user password will never expire. This is a global default for all users. If a value is specified in the USER_APP table, it will override this value for that user.
PW_TEMP_DAYS_VALID	This controls the number of days a temporary password will be valid before the account is disabled. A temporary password is created when an administrator does both of the following actions: 1) Creates a new account or changes the password on an existing account. 2) Selects the "Force password change next login" checkbox.	0=forever 1=just today 2=2 days 3=3 days, etc. The temp password is valid to midnight on ending day.
RECORD_PERFORMANCE	Indicates if user activity should be recorded. Each visit to a page and XML routine will be recorded as user activity. Valid values are "Y" and "N".	This adds a lot of overhead to the system and should only be set to a “Y” at AssetWorks’ advice. This feature does provide useful information when trying to diagnose a problem. If this feature is turned off the Show User Activity frame will not function.

Variable Name	Description	Comment
REPORT_BIN_SCAN _FUNCTIONS	This parameter can be used to limit what functions the background process called Bin Scan performs. The options are specified as one string separated by semi-colons. An N means do not perform this function. This should only be set if functions are not used or they are causing performance issues.	The scope of this parameter is site. BIN = Look for new reports in the user's private in-bin GRPBIN = Look for new reports in shared group bins. DASH = Dashboards NOTE = Notification count on navigation bar TODO = To do list (future) The delivered default for this parameter is BIN=Y;GRPBIN=Y;DASH=Y;TODO=Y;NOTE=Y
REPORT_BIN_SCAN _MINUTES	The number of minutes that elapse between automatic server requests being made by an M5 user to update the bin icon state. This process also marks folders as containing something new. Users will be able to retrieve new output from the bin even if this process has not run but they will not be notified of the output availability by the icon changing appearance. This number should not be too low as is does create a fair amount of server overhead as the number of M5 users increases.	The default value is 5. The minimum is 4. This is the rest time after executions completes and the next execution begins.
RUN_IMMEDIATE_REFRESH _LIMIT	The number of times the Run Immediate Viewer process will poll the server looking for report output before it assumes the report failed.	Default is 50.
SAVE_TIMEOUT_SECONDS	The number of seconds the client side screen will wait for a save action to respond.	The default is approximately 120 seconds.
SERVER_CHAT	The URL of the server that is supporting the M5 chat service. This is only the base name such as http://m5prod.whatever.com.	Must include protocol such as, http://.

Variable Name	Description	Comment
SCHEDULER_API_KEY	This is the Scheduler API Key.	
SCHEDULER_API_URL	This is the Scheduler API URL.	
SCHEDULER_KEY	This is the FullCalendar Scheduler License Key.	
SQLSERVER_DATABASE_NAME	The name of the SQL Server database. For an Oracle installation this value is not used.	This must match the “initial catalog” that is specified in the OLEDB connect string.
SUBMIT_API_KEY	The SHA256 Hash code to validate the M5SubmitService API.	
SUBMIT_API_URL	The url to be used for the install location of the M5SubmitService API.	
TIMEOUT_MINUTES	The number of minutes an M5 user can be idle without timing out.	A value of null or 0 means the user session will never timeout. This is a global default for all users. If a value is specified in the USER_APP table, it will override this value for that user.
UIA_REJECT_URL	The URL to be used when resubmitting rejected interface records.	It is the URL of the iPortal web service on the batch server.
UNICODE_DB	This must be a “Y” if the database being used is using the Unicode character set.	
USERPREF_ AUTOCOMPLETE	Sets the default for all users so the autocomplete function is on (“Y”) or off (“N”).	Default is “Y”.
USERPREF_DASHBOARD_GRID	Sets the default for dashboards to a 4x4 grid for all users. Users can overwrite by changing their preference. “Y” or “N”.	Default is N.
USERPREF_RIBBON_COLOR	Sets the default color for the M5 ribbon for all users. The value is a number starting with 1 and corresponds to the colors on the profile screen going left to right.	Default is 1.
USREPREF_SHOW_ICONS	Set the default for all users so they see icons in the M5 ribbon instead of the ellipses […].	Default is “N”.

Variable Name	Description	Comment
WARN_USER_LICENSE _EMAIL	The email address that will receive warning messages about the user license percent being exceeded.	
WARN_USER_LICENSE _PERCENT	If you have an M5 user license this parameter defines a threshold when exceeded will send an email to the address defined by the WARN_USER_LICENSE_EMAIL parameter.	Value is 1-99. The site must have log event LON turned on.
WEB_HOST	This overrides the protocol and the server name the user is logged into. It is mainly used to diagnose problems on load balanced servers and should otherwise be blank.	
WORKORDER.POPUPCREATEALERT	Show response pop up for system vehicle alerts when creating work orders?	
WO_POPUPCREATEALERT	Show response pop up for system vehicle alerts when creating work orders?	
WO_ REPAIRREASONDEFAULT	Visit reason on new work order.	
WO_TASK_LABOR _AFTERWOFINISHDAY	Value ignored if user does not have ANY-WO-LABOR-DATE authorization.	

Section 18. Updates

The following updates apply to *System Administration Application User Training*.

Release	Section	Description
25.0	Section 11. Company Definition, General tab	Added Licensed Unit Count and updated image.
24.3	System Version	Replaced the System Version image.
24.3	Available Notifications List Notification Variables, Qualifications, and Recipients	Added PART TRANSFER REQUEST CREATED notification.
24.3	Available Notifications List Notification Variables, Qualifications, and Recipients	Added new notifications: • EQUIPMENT CHECKED OUT • EQUIPMENT REQUEST CREATED
24.3	Available Notifications List Notification Variables, Qualifications, and Recipients	Added new notifications: • PART REQUEST CREATED • PART REQUEST READY
24.3	Available Notifications List Notification Variables, Qualifications, and Recipients	Added new notifications: • SENSOR ALARM • SYSTEM ALARM
24.2	Appendix A – Role Privileges	Added role privilege SER PART AUTH.
24.2	Appendix C: M5 Parameters	Added new M5 Parameters: • ADHOCBI_RPTDB_USE • CRYSTAL_ENTERPRISE_RPTDB_USE • CRYSTAL_ENTERPRISE_RPTDB_ODBC
24.0	Setting and Maintaining System Flags Appendix B – System Flags	Updated the reference to the System Flags Table. Removed the System Flags table. Updated the reference to the System Flags Table.
24.0	Privileges tab Department/Chat Groups Customer Data View Users M5 Parameter Query Frame View Log Files in M5	Updated the reference file title names.
24.0	Email Group	Updated the functionality of System Flag 5249.

Release	Section	Description
23.2	Appendix B – System Flags	Updated System Flag 5010 user value and role privilege.
23.2	Appendix A – Role Privileges	Added role privilege UPD CMR PREFIX.
23.2	Holiday Calendar	Added Location Group to the Holiday Calendar.
23.2	Email Group	Added Email Group section.
23.1	Appendix B – System Flags	Added System Flags 5520, 5521, and 5522.