

Manitou - Central Station Supervisor Training Guide

Table of Contents

Manitou - Central Station Supervisor Training Guide	1
Course Introduction.....	3
Getting to know the Manitou Supervisor Workstation.....	3
Introduction.....	3
Prerequisite Skills.....	3
What you should understand at the completion of this course	3
Manitou System Manager.....	4
Getting to Know the Services That Make Manitou Run	4
What is the MSM (Manitou System Manager)?	4
Finding the MSM	4
Elements of the MSM.....	4
Starting and Stopping MSM Services.....	6
Manitou System and Receiver Configuration	7
Setting Up Manitou.....	7
Objectives	7
Logging into the Supervisor Workstation.....	7
Configuration form.....	7
Configuring Receivers	9
Manitou Options	17
Configuring Manitou for Your Business.....	17
Introduction.....	17
Color and Account Creation Options.....	17
Accounting Options.....	19
Alarm Handling and Tracking Options	19
Contact Point Device Defaults Options	25
General Options.....	25
Purge Options.....	27
Signal Processing Options	29
System Options	31
Additional Options	34
Permissions, User Groups and Users	39
Defining What Each Person May See or Do	39
Introduction.....	39
Permissions	39
User Groups	43
Users	44
Event Maps, Categories and Codes	47

Building Signal Structure	47
Introduction.....	47
Event Maps.....	47
Event Categories.....	49
Event Codes	51
Watchdog Messages	54
Ensuring the Right Messages to the Right People	54
Introduction.....	54
What are Watchdog Messages?.....	54
Watchdog Message Definitions.....	54
Configuring Watchdog Messages.....	57
Configuring Watchdog Alarms	58
Troubleshooting in Manitou.....	60
Where to look to find your answers	60
Introduction.....	60
Raw Data Log.....	60
System Application Log	61
System Log	62
Audit Trail Log	63
Other Supervisor Workstation Features	65
What else can Manitou do?.....	65
Introduction.....	65
Script Messages	65
Monitoring Types.....	65
Control Panels	66
Contact Point Types.....	66
Subtypes	67
Workstations.....	67
User Status	68
Group and Class Codes	69
Global Holidays	69
Resolution Codes.....	69
Transmitter Protocol Types	69
Receiver Types.....	69
Report Templates.....	69
Appendix 1	71
Vocabulary	71

Course Introduction

Getting to know the Manitou Supervisor Workstation

Introduction

Welcome to the Manitou Supervisor Workstation course. This course introduces the key elements of the Manitou Supervisor Workstation and their impact on the system as a whole.

Prerequisite Skills

This course assumes that the learner had a solid understanding of their operations, receivers, and could be required to manage information within the Supervisor Workstation. We encourage all users to have completed at least the Data Entry courses to better understand what data is housed within the Operator Workstation.

What you should understand at the completion of this course

This course provides a basic understanding of the features housed within the Supervisor Workstation and how they interact with the application as a whole. Upon completion of this course learners should understand:

- What the purpose of the MSM is and what services present within it.
- Where to configure the Manitou system services.
- Where the Receivers and Receiver Line prefixes are configured.
- Understand the purpose and general best practices for the global Manitou options.
- How to create and edit Permissions profiles for use on Manitou and BoldNet users.
- How to tie Permissions profiles to User Groups and set their parameters.
- How to tie a User Group to an individual User.
- What the purpose of Event Maps are when translating signals.
- The importance of Event Categories.
- How Event Codes are created and configured.
- Why setting Watchdog messages correctly is vital to learning of any system, or alarm processing, challenges.
- How to troubleshoot basic items within Manitou.

Manitou System Manager

Getting to Know the Services That Make Manitou Run

What is the MSM (Manitou System Manager)?

The Manitou System Manager, most often referred to as MSM, is an application that runs on the Manitou Servers and allows the ability to start and stop services. This is a key feature used when practicing failover of the Manitou servers.

Finding the MSM

The MSM is, most often found on each Manitou server. Some organizations also have an Operator MSM configured on a workstation in the active central station for operators to be able to start services, but not stop them, in the case of an emergency.



To launch the MSM, on the server:

- Log into the Manitou Server.
- Locate and double click the MSM Icon.

Elements of the MSM

Notice that the application shows the active system with buttons across the top. This allows the ability to refresh the configuration, start and stop services, as well as restarting services, and viewing the properties of the individual services. We cover this in detail when we get into the Supervisor Workstation Configuration portion of this course.

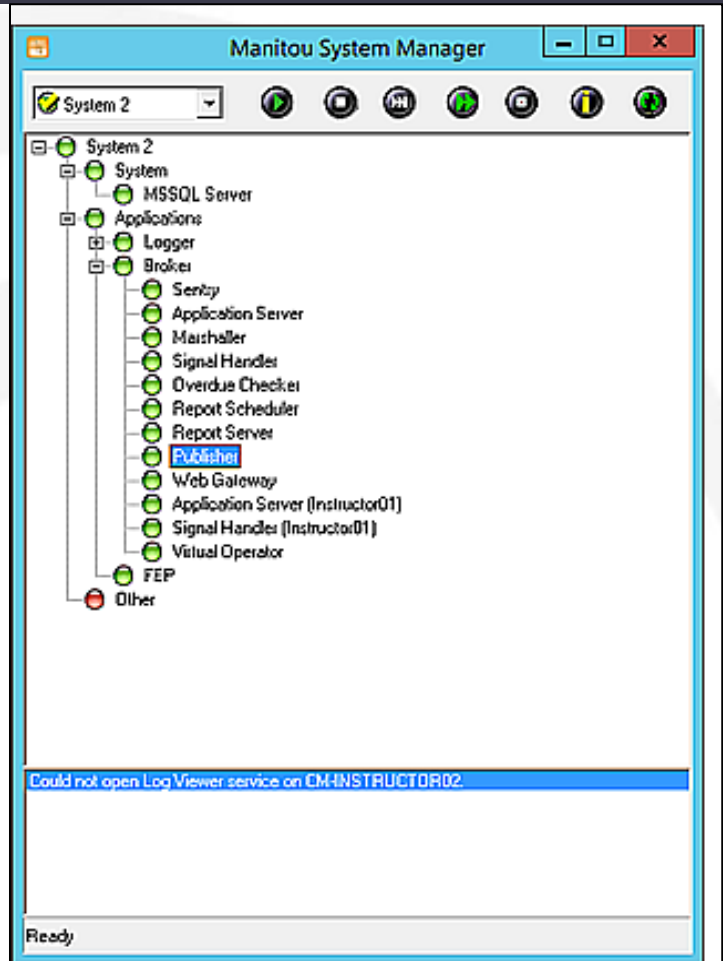
The MSM application tree is broken out into Three Specific Sections: System, Applications, and Other. The Other section is available for tracking external products in the Manitou MSM. This is not, currently, in use at this time.

System Section

The System Section specifically houses the details on the Microsoft SQL Server™ instance used for Manitou. The Database startup is automatic and is the first element to start when starting the MSM.

Application Section

The Application section contains all the portions of Manitou utilized for this configuration. This too is broken out into sections, within this configuration they are: Logger, Broker, and FEP. Each portion may have other dependent services underneath them.



- **Logger**

The Logger service, itself, is responsible for tracking all communications between the applications and services and the Manitou database. The Logger service should run constantly in order to troubleshoot issues.

The Logger section is expandable to reveal the Log Viewer. The Log viewer displays all the communications actively occurring between the applications, services, and the database. We recommend only opening the Log Viewer when actively researching items. Leaving it running continuously can cause the logger to lose time with the transactions.

- **Broker**

The Broker section of the MSM houses all the items that run the core parts of Manitou. If the Broker is not running on the MSM, no other services below it can run.

Some of the Manitou services are mission critical and affect the processing of alarm signals. These services, if unable to be restarted in the active MSM, receive after hours support. Services that receive 24 Hour Support:

- **Broker** - If this is not running, no other services run below it.
- **Signal Handler and/or Marshaller** - These services are required for signals to translate and deliver to operators for handling.
- **FEP** - If this is unavailable, the system is not receiving signals and the receivers are buffering them, which will cause the receivers to ring warning notifications.
- **Application Server** - No one can log into Manitou with out a running application server.
- **MediaGateway**, when delivering high priority events as a receiver.
- **Sentry**, only if a mistake is made and all operators logout and no new operators can log in.

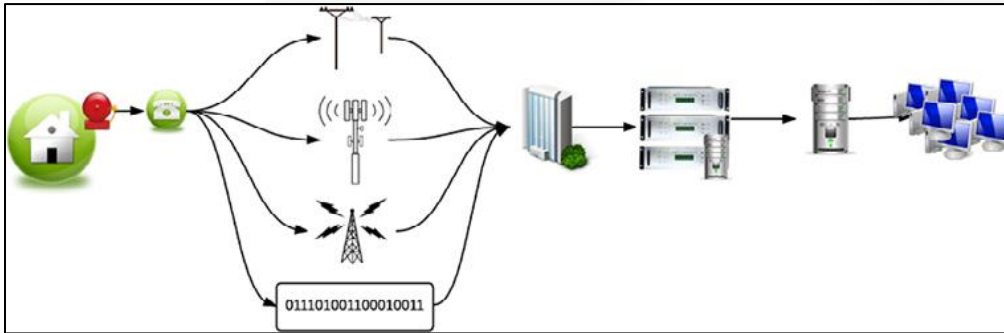
Other services within Manitou are supported only during business hours. These are considered an inconvenience but do not rise to the level of mission critical. These are:

- **Report Server, Report Scheduler, and Publisher** - Responsible for sending and scheduling reports from Manitou.
- **Web Gateway** - Dealers and customers will be unable to log into the BoldNet portion of Manitou until resolved.
- **Virtual Operator** - Also known as the "Auto Client," which automates many action pattern elements.
- **Overdue Checker** - This looks for things that are late or require a change of status.

Please note that the Overdue checker not only looks for things that are late, it also looks for things that have expired, such as On Test timers. Therefore, it is very important to get this sorted as quickly as possible. During the down period, supervisors should keep an eye on the On Test queue and manually return expired items to full service.

FEP Section

FEP stands for Front End Processor. This is how Manitou receives and acknowledges signals passing into Manitou. Below is a simple flow of an alarm from a property, through on the various communication paths, to the Central Station, where the Receivers (and/or the MediaGateway) receive the signal and the FEP acknowledges the receiver and hands the event off to the Signal Handler for processing and delivery to the account's activity and alarm operators for handling, as necessary.



Systems may have multiple Front End Processors for their systems. A couple examples of the need for additional FEPs are:

- Multiple site locations for the receivers.
- Primary and Backup configuration.

A simple way to define the FEP is: the software element that "thanks" the receiver for events passed to automation.

Starting and Stopping MSM Services

Whether for a failover or for just routine maintenance, there will be times where it is required to stop, start, or restart of a Manitou service. To do so:

1. Log into the Manitou Server housing the MSM
2. If not already loaded, launch the MSM. *Please note that services MUST only be started and stopped on the ACTIVE server configuration. To determine the Active server, log into the Supervisor Workstation and load the Configuration form and the configuration that loads by the default (depicted by a green light in the drop down) is the active server.*
3. Locate the stopped service (red light), or locate the service to restart, right click and perform the desired action.

Manitou System and Receiver Configuration

Setting Up Manitou

Objectives

During this module we cover:

- Where and how to configure the Services that make up Manitou.
- How to enter Receiver Line Prefixes and DNIS Maps.
- What to prepare before adding receivers to Manitou.
- How to enter Receivers.
- How to link secondary FEP configurations to the first.
- How to configure specific Receiver Lines underneath a Receiver.

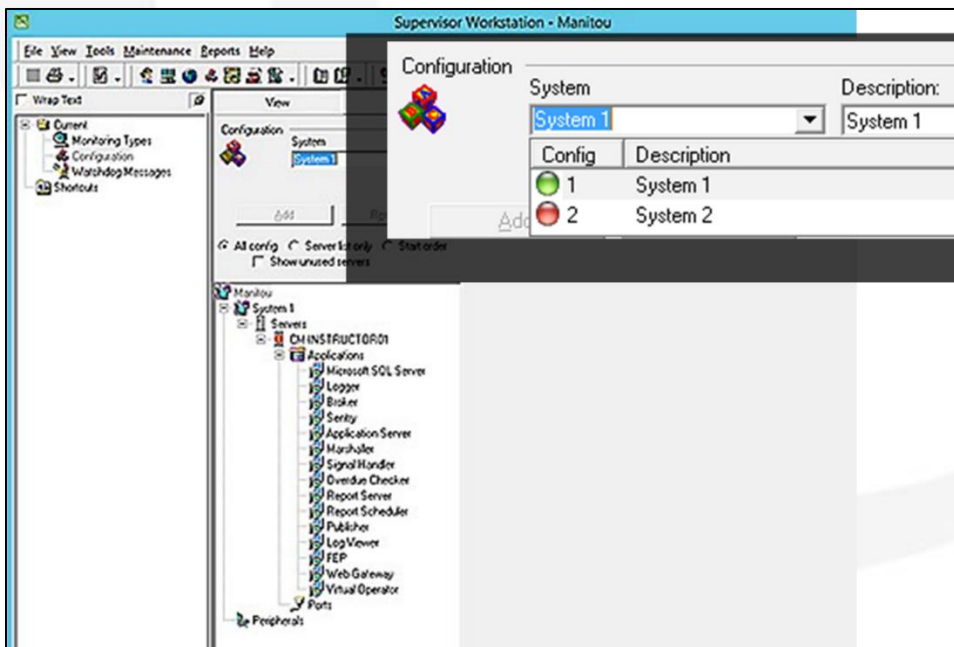
Logging into the Supervisor Workstation

There is a separate icon for the Supervisor Workstation. In general, it is found on the desktop of any machine installed with the Manitou Operator Workstation. It may also be possible to navigate to the Supervisor Workstation from the Start button, programs, Bold Technologies, Supervisor Workstation.



Configuration form

The Manitou Configuration form is how the Manitou Services are defined based on your purchased items and server distribution. Each Configuration is designed to mirror one another for failover purposes. Configurations may be configured as Stand-alone or Distributed. In order to determine which configuration is active, drop down the System list. The item with the green light is the current active system.



Stand-alone Configuration

A Stand-alone configuration simply means that all Manitou Services run on a single-server at one time.

Distributed Configuration

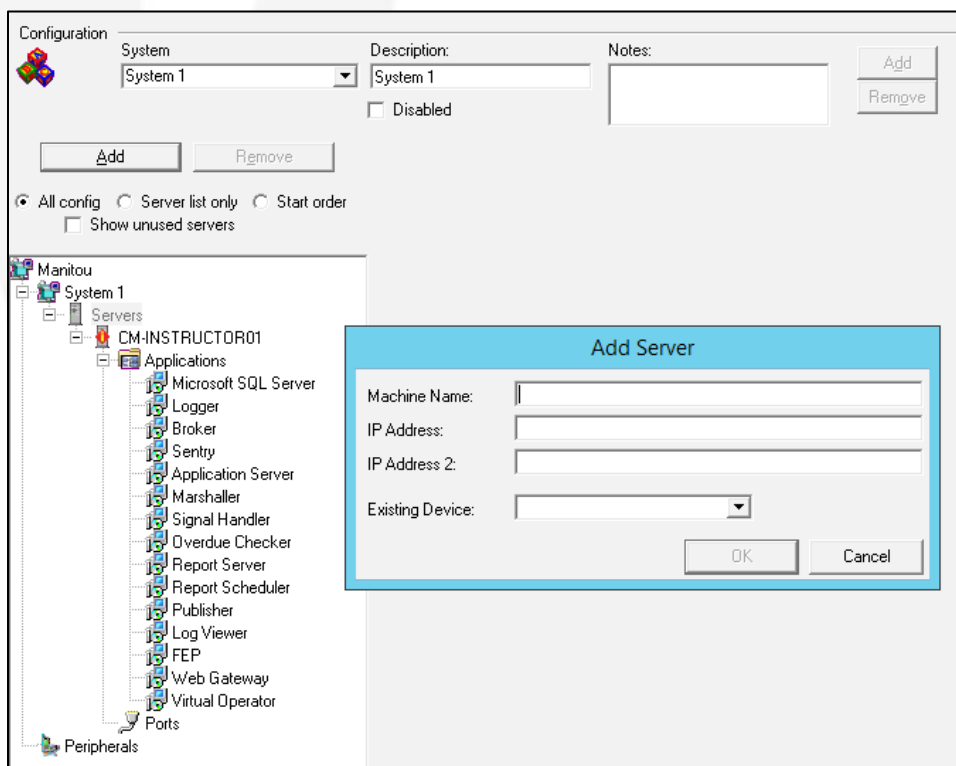
A Distributed configuration allows some services to run on different servers than the active Broker server.

Adding Servers to a Configuration

When adding new servers to your system they require creation within Manitou in order to utilize them for Manitou. To add a server to Manitou do the following:

1. Ensure the Configuration form is in Edit Mode.
2. Select the Servers "node" in the Configuration Tree.
3. Click Add.
4. Enter a Machine Name. Manitou Name resolves on the network.
5. Enter the primary IP address.
6. If applicable, enter the secondary IP address.
7. Click OK.
8. Save the record.

If the server is already configured, it is possible to select the configured server from the "existing device" drop down list.



Adding Manitou Services to a Configuration

Manitou is comprised of several elements that work together to receive and manage signals to alarm handling operators. The key services that allow Manitou to run and process signals are:

- **Broker** - Considered the "brains" of the system and is responsible for verifying licensing.
- **Sentry** - Must run on the same server as the Broker. This handles the requests for login from the Application Server and provides tokens for access to Manitou.
- **Application Server** - allows the Manitou clients, and Supervisor Workstations, to run.
- **FEP** - Front End Processor receives and determines the formatting of each signal as the receiver (or MediaGateway) passes off the events to Manitou.
- **Marshaller** - Works as a "traffic cop" controlling the flow of signals from the FEP to the Signal Handler, or Signal Handlers.
- **Signal Handler** - Processes signals into Manitou applying rules and behaviors based on configuration of attributes and commands.

To add a service to your Manitou Configuration, do the following:

1. Ensure the record is in Edit Mode.
2. Click the Applications Node in the tree.
3. Drop down the Application Type and select the correct application.
4. Click OK.
5. Based on the System Configuration document, set the applicable path and parameters.
6. Repeat for all configurations by dropping down the System dialog and selecting each Configuration and repeating the steps above. *It is vital that all configurations have all the services. If they are not the same, there could be a loss of functionality when the system is failed over.*
7. Save the record.

Start Order on the Manitou Configuration

- | | |
|-------------------------|----------------------|
| 1. Microsoft SQL Server | 8. Overdue Checker |
| 2. Logger | 9. Report Scheduler |
| 3. Broker | 10. Publisher |
| 4. Sentry | 11. Virtual Operator |
| 5. Application Server | 12. Web Gateway |
| 6. Marshaller | 13. Log Viewer |
| 7. Signal Handler | 14. FEP |

Please note that your configuration may have different services in a different order. That is perfectly okay. The recommended service order groups them together in logical order.

Configuring Receivers

Receiver configuration is how signals find their applicable customer records. Therefore it is vital to know all the elements of the Receiver Configuration form. The Receivers form is found within the Supervisor Workstation

under the Maintenance Menu, then Setup, and then Receivers. It is also possible to use the shortcut button



found on the toolbar.

FEPs

All receivers get configured underneath a FEP. In many cases, the additional FEP configurations are not added until after a site is ready to switchover to Manitou. In order for the FEP to communicate properly from the receivers into Manitou there must be a FEP configuration for each machine that runs a FEP. To add a FEP:

1. Navigate to the Receivers form and click the System node and click Edit.
2. Click Add.
3. Enter a clear description. Most often this is FEP 1, FEP 2, etc.
4. The system automatically determines what FEP number is next and allows the ability to add multiple FEP entries. We encourage entering the first FEP then copying it for other configurations after the receivers are added.
5. Click Save.

Receiver Line Prefixes and DNIS

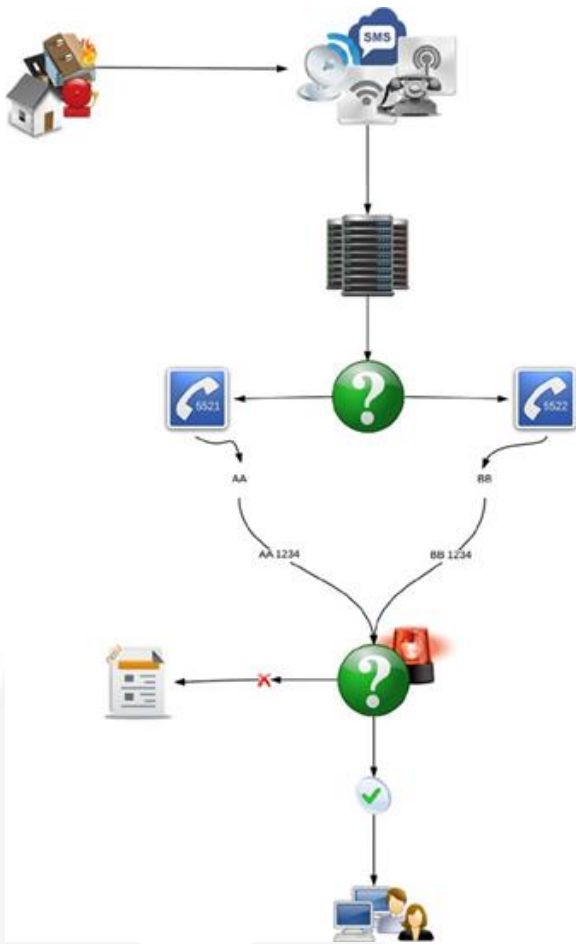
In order for signals to find their way to their proper customer records, there must be a unique way to identify and tell the difference between the signals presented. Consider this, when an alarm panel sends in an alarm the number it dials, or the receiver line it dials into defines the difference between an alarm number (often called the panel account number) 1234 on one versus 1234 on another.

- **Receiver Line Prefixes**

Receiver Line Prefixes help identify and tell the difference between customer records. There are bound to be duplicate alarm panel account numbers reporting into an alarm system as businesses grow. In order to tell the difference, a prefix must be assigned, at some point, in order to identify these differences. Receiver Line prefixes can be anything that will help the company logically separate the accounts. In our example we use AA and BB as prefixes to discern the difference between each account reporting a number of 1234. Prefixes may be assigned on the receiver, specific lines on the receiver, or through the use of DNIS.

- **DNIS**

DNIS is also known as Dialed Number Identification Service. Put simply, this allows the ability to provide installers with a telephone number to dial that is solely tied to their accounts, and, based on that number, a prefix is assigned to the record changing the 1234 to a complete combination of AA 1234, AA being the receiver line prefix assigned to the dialed number provided to the installer.



Adding Receiver Line Prefixes to Manitou

Before adding a receiver Line prefix to Manitou, it is important to first take some time to understand your current and planned future business practices. Receiver line prefixes should be logical enough for people to understand but not too complex that they are hard to manage. Some third-party monitoring companies will preface their Receiver line prefix with a D or I (for Dealer or Installer) then follow it with a series of numbers, starting at a number like 001. Others will use initials for the company. The following steps detail how to add Receiver Line prefix into Manitou:

6. Launch the Receivers form and click Edit.
7. Select the Receiver Line Prefixes node and click Add.
8. Manitou will pick the next logical prefix based on previous data, entry. You are not required to use that prefix. Enter the Prefix desired and enter a description. Hint: If you are entering more than one prefix and they can be logically added end the prefix with a number that can properly increment.

9. Update the number to add based on your needs.
10. Click OK.
11. If you have the Trigger and Max Customer details, generally required by UL, update the values on the record.

The screenshot shows a dialog box titled "Rec Line Prefixes". It contains the following fields and values:

- Receiver Line Prefix: AA1
- Description: Dealer 1
- Trigger 1: 0
- Trigger 2: 0
- Max Customers: 0
- Max O/C Customers: 0

12. Save the record.

Adding DNIS Numbers to Manitou

Before adding DNIS Numbers to Manitou there are two things to know:

13. How many DNIS digits are configured on your receiver?
14. What are the DNIS digits? Does it look like 01234 or 51234?

It is absolutely crucial to understand how the DNIS digits are presenting to Manitou. This is often found by receiving signals with DNIS digits and reviewing the raw signal. To add a DNIS record to Manitou do the following:

1. Launch the Receivers form and click Edit.
2. Select the DNIS node and click Add.
3. Enter the DNIS digits following the correct format for the number of DNIS digits passed from the receiver.
4. Enter a description.
5. Select a Receiver Line Prefix to assign to the DNIS.
6. Click OK.
7. If you a specific Monitoring Group or Dealer for those signals, select them.
8. Save the record.

The screenshot shows a dialog box titled "DNIS Maps". It contains the following fields and values:

- DNIS: 86753
- Receiver Line Prefix: Default Prefix
- Monitoring Group: Monitoring Group 0
- Description: DNIS 86753
- Dealer: SSS Security System Service

What to Prepare Before Adding a Receiver

A Receiver record in Manitou needs several pieces of information and some additional elements to successfully save it into Manitou:

- The Receiver Type needed to translate signals. The Receiver type applies the standard rules for signals coming off the receiver.
- How the signals are communicating to automation.
 - **Serial** - Physical cable off the back of the receiver. Often processed through a DIGI.
 - **TCP/IP (In)** - Communicates over network pathways. In means that Manitou 'listens' to that port for information to be passed INTO Manitou.
 - **TCP/IP (Out)** - Communicates over network pathways. Out means that Manitou connects to the port and ASKS for information to pass into Manitou.
 - **Demo** - Should NEVER be used in a live environment. This is used to pass a signal file through and is often utilized in a training system to allow operators to practice with realistic events.
- Port and Speed settings. *If unsure of these settings, the receiver documentation should contain the information. If not, try 9600, 8, none, and 1. That is a good starting point.*
- The default Receiver Line Prefix to use if no other rules override it.
- Within which Monitoring Group the signals should present. Most businesses have this set to the default Monitoring Group of 0 (zero).
- A System Receiver Default account where orphaned signals will land if there is not a matching customer account for a received prefix and transmitter ID combination.

For assistance creating the System default account, please reference other similar accounts. Most often their ID is something like SYS-REC1. It is possible to create a new account based on an existing. Each Receiver default account must have a transmitter.

In general, they are a default prefix and the transmitter ID of 99999nn replacing the Ns with the number of the receiver.

Adding a Receiver

After compiling the key data and preparing the default account for the receiver then you are ready to add a Receiver. To do so:

1. In Edit mode select the FEP to which to add the Receiver, then click add.
2. Pick the Receiver Type used to manage incoming signals.

RCode	Description
ADEMCO	Ademco 685
AES7701-ADM	AES 7701 in Admeco 685 Mode
AES7701-RAD	AES 7701 in Radionics Mode
BASE10	BASE10
BOLDIP	Bold IP Receiver
BTDIRECTOR	BT Director
CP	CP Receiver

3. Enter a clear description of the receiver. We suggest a description that helps someone find the physical receiver within the operations.

Add Receiver

Receiver type: BOLDIP

Description: Bold IP Receiver 1

Starting Number: 3

Number to Add: 1

OK Cancel

4. The next available receiver number auto-populates. If this order is correct, leave it there, if not change it to the correct receiver number.
5. The Number to add allows you to add multiple receivers with the same receiver type at one time. In this example we are adding one.
6. Click OK.
7. The Receiver page loads and is ready to configure the remaining items. If the port type is Serial, it is possible to leave it at the default otherwise drop down the Port type and select the correct type.

Receivers

Receiver Number: 3

Receiver Type: BOLDIP

Description: Bold IP Receiver 1

Port Type: Serial

Port:

Port Settings:

Port (Secondary):

Port Settings (Secondary):

Soft Command Receiver Code:

Disabled

Defaults:

Default Receiver Line Prefix:

Default Monitoring Group: Monitoring Group 0

Default Designation for Unknown Signals:

Receiver Line Prefix:

Transmitter ID:

Linked Receiver:

FEP Number:

Receiver Number:

8. Enter the Port settings, or IP address for the communication pathway.
9. Select the Default receiver line prefix to apply to signals that are not otherwise overwritten by individual lines. *Note: Several receivers send signals through communication pathway and will only have the default receiver line prefix.*

The screenshot shows the 'Receiver' configuration window. It is divided into several sections:

- Receiver Information:** Receiver Number (1), Receiver Type (MLR2), Description (Surgard), Port Type (Serial), Port (COM1), Port Settings (BR9600,NOPARITY,BIT8,STOP1), Pot (Secondary), Pot Settings (Secondary), and Soft Command Receiver Code (Disabled).
- Defaults:** Default Receiver Line Prefix (Surgard), Default Monitoring Group (Monitoring Group 0).
- Default Designation for Unknown Signals:** Receiver Line Prefix (Default Prefix), Transmitter ID (99999), and Default Receiver Account.
- Linked Receiver:** FEP Number and Receiver Number dropdown menus.

10. If necessary, change the receiver to a specific Monitoring group.
11. Lookup and find the Receiver Default account you created. *If you don't see it in the list presented when clicking the lookup icon, review the account in the Manitou Operator Workstation and ensure the account type is SYSTEM.*
12. Once all data is correct and in place, click Save.

You may notice that there is an additional section within the Receiver form called Linked Receiver. This is used on other, redundant, FEP configurations to remove the need to list the individual receiver lines in every configuration. This reduces the number of data entry errors.

This screenshot shows the same Receiver configuration form as above, but with the 'Linked Receiver' section populated. The 'FEP Number' dropdown is set to 'FEP' and the 'Receiver Number' dropdown is set to 'Surgard'. A large white arrow points to the 'Receiver Number' dropdown.

Adding Lines to a Receiver

Once the receiver is in place, it is possible to add specific lines to the receiver. If the majority of the lines are using the default Receiver Line Prefix those do not need to be specifically configured. It is only necessary to configure the lines that deviate from the default. To add a line to a receiver:

1. Be sure the record is in edit mode, select the receiver to which to add the line then click Add.
2. Select the appropriate Receiver Line Prefix for the line.

3. Enter a clear description. In general, people use the line card number.
4. Select the line number upon which to start adding.
5. Enter the number of lines to add.
6. Click OK.
7. Repeat as necessary and then Save the record.

The Receiver Line options are configured, as needed, for the line. Please see a supervisor for additional details on the options, when needed.

Manitou Options

Configuring Manitou for Your Business

Introduction

This section discusses each of the Manitou options, why they are important and common settings. Options covered in this section are:

- Color and Account Maintenance
- Accounting
- Alarm Handling
- General
- Purge
- Signal Processing
- System
- Other

Located at the bottom of each option, there is a “Further Description” button. When clicked, the button reveals details of each option.

Further Description

Color and Account Creation Options

Color Options

The default option form, upon arriving on the Options form is the Color options. The Color Options allow the configuration of Alarm Queue, Customer Activity Log, Watchdog Messages, Report Queue, and Maintenance Issues color selections. Always keep in mind those who are color-blind when making choices on colors in Manitou.

Simply edit the form and choose foreground and background colors that help visually identify the features.

The screenshot shows the 'Color Options' configuration form in Manitou. It is organized into several sections, each with a list of items and their corresponding foreground and background color selection boxes. A 'Reset to Default Colors' button is located at the bottom right of the form.

Section	Item	Foreground	Background	
Alarm Queue/Customer	Warning Level	Yellow	Black	
	Danger Level	Red	Black	
	Suspended Alarm	Blue	Black	
	Unavailable Alarm	Grey	Black	
	High Priority	Magenta	Black	
	Zone in Alarm	Red	Black	
	Disaster	Black	Black	
	Customer Log	Summary/Header	Black	Black
	Customer Log	Detail Item	Black	Black
	Customer Log	Current Alarm	Black	Black
Watchdog	New Level 1	Red	Black	
	New Level 2	Yellow	Black	
	Acknowledged	Black	Black	
	Report Queue	Normal	Black	
Report Queue	Failed	Red	Black	
	Complete	Green	Black	
	Detail Item	Black	Black	
Maintenance Issues	Resolved	Black	Black	
	Unresolved	Black	Black	
	On Test	Black	Black	

Account Creation/Maintenance Options

There are several Customer account creation related options that help define ease of use and define standards. The following is a brief description of each and their reason for being:

- **Auto-Generate Contract Number**

This option, when enabled, allows the account serial number assigned by the database to represent the customer account ID number.

- **Contact (Person/Individual User Defined Fields)**

Individuals on a customer's contact list may have up to 200 configurable items that may not be in the core of Manitou for data. An example of these fields may be medications the person takes, when doing Medical monitoring.

- **Customer User Defined Fields**

Like the Contact person, it is possible to maintain 200 points of data that may not otherwise have a location for the data within the regular customer record.

- **Customer Warning Threshold**

Every Manitou System is licensed for a maximum number of allowed customer records. This threshold is designed to generate "watchdog messages" when a company is reaching that upper limit. Depending on the size of your organization the default value of 100 may be a bit closer that is comfortable.

- **Display Customer Logs in their Local Time**

When set to yes, which is the most common setting, the customer activity logs display in a customer's time zone as opposed to the central station's time zone. This allows operators to review activity with a customer without having to calculate the time difference.

- **Drop Down to Combination Data Entry/Search Field Threshold**

This option, when sent to a number, determines when an authority, agency, branch, dealer, and the like, fields will switch from a drop down to a combination field that allows the typing of a corresponding code or launch a search dialog to retrieve the correct entity.

- **Maximum Number of Days of Activity to Transfer from System Account to Customer**

This option determines how much activity to retrieve out of the default system account, if signals landed there before the addition of a transmitter on a customer record. This setting is defined individually at each site based on their size and signal volume. Most often the default setting, of 21 days, is acceptable. However, some sites have had to raise or lower that number to meet their business and processing needs.

- **New Customer Monitoring Status**

When creating new customer records some sites want the record to be set to pending, while others want the accounts set to active so as to not miss any events. This option allows the selection of 4 different options:

- **Default Active** - automatically checks the box to make it active upon saving the record. This can be ticked off manually by the data entry person.
- **Default Pending** - automatically unchecks the box to make the account pending upon saving the record. This can be ticked on manually by the data entry person.
- **Always Active** - hides the check box to make the account active and does so automatically.
- **Always Pending** - hides the check box to make the account active and automatically makes the account pending.

See your leadership team for how your business would like to set this option.

- **Require Customer Edit Comments**

Manitou is excellent at tracking the "what" changed elements of the customer data. However, the "why" needs to come from the comments related to the changes operators make. This option will force the entry of some level of comments to explain the changes made, each time the account is saved. The recommended setting for this option is Yes as it will help ensure the most information is available if it becomes necessary to defend the actions taken on an account.

- **Require Operator to Type Password Before Validation**

Some sites have a requirement that the validation of a password must be manually entered prior to editing a customer record. This is a more secure behavior, however, it is also cumbersome to those making data changes to customers daily. When set to No, the option still forces the validation dialog but pre-populates the operator's user ID and password.

- **Require Password Before Viewing a Customer Record**

Still, other sites may require a password validation before a user/customer can view the customer details. When set to Yes, the customer record will not load any data until the validation dialog is successfully validated to a customer or operator's password. The previous option determines if the operator must type the password before viewing.

Accounting Options

Accounting options work directly with the integration of an accounting package such as, our partner, SedonaOffice. The two options here: Accounting Company ID required and Display Accounting status are most often determined by each individual business. Please see your management team for more information if you integrate with an accounting package.

Alarm Handling and Tracking Options

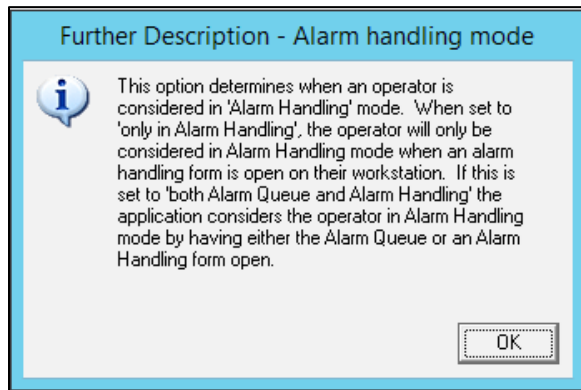
Alarm Handling and Tracking options define what an alarm handler is, how to track alarms, and set timeouts.

Alarm Handling Options

- **Alarm Handling Mode**

The Alarm Handling Mode option has two options to make a user an official "alarm handler." They are: Active only within the Alarm Handling form, or Active when the operator has the Alarm Queue. Some

businesses wish to have alarms delivered to operators based on the "oldest, highest priority," standard. When that is the case, they often select the first option of the Alarm Handling form only.



- **Alarm Notifications**

The Alarm Notifications option allows a site to determine how operators are prompted with key information. There are a few options to consider:

- **Pop-up dialog** - this is the most forward-facing way to present key alarm information to an operator's attention. These pop-up notifications include all comments and alarm-based notifications such as additional signaling and the like.
- **Ribbon (Acknowledgment Optional)** - This changes the pop-up dialog to a simple ribbon down the right-hand side of the page with applicable notifications flashing to indicate there is information to review. The optional feature doesn't require that an operator select any of these items, when flashing, in order to process or close the alarm. This allows the operator to complete alarm processing unfettered by notifications.
- **Ribbon (Acknowledge Notification Before Next Action)** - like above, the ribbon bar is on the right-hand side of the alarm form, flashing the items that need attention. This option setting requires that an operator click/navigate to review the flashing messages before attempting to complete each action.
- **Ribbon (Acknowledge Notification Before Closing Alarm)** - like the two other ribbon options; however, this option requires the operator review each flashing item before they may close the alarm. This can speed up response times but can also delay the delivery of important information until too late.

- **Alarm Queue Display Style**

The Alarm queue display style allows the alarm queue to show all alarms as individual lines or grouped by their Master customer.

- **Alarm Queue Color Scheme**

Operations have the option to set their alarm queue color scheme to what will work best for their operators. The two settings are: Event Based and Age Based (the default setting is Age Based).

The Event Based alarm queue selection takes the color setting on each alarm and presents the alarms to the alarm queue in that color. This does require some effort to ensure that all alarm colors meet your company color standards.

The Age Based alarm queue selection changes the colors in the queue based on the global settings for colors. As an alarm begins to age, based on the time settings on the event codes, the alarms will change from white background with black text to the warning color (default color yellow) to the danger color (default color red) as alarms age in the alarm queue. In order for this to be the most effective the time out settings on each event should be reviewed and set to the timing appropriate for the event and category.

- **All Action Pattern Commands Are Optional**

This option is rarely set to Yes, unless the organization is small enough that completing the action patterns as written are the exception to the rule. When set to yes, an operator may close the alarm at any time in the process despite any outstanding actions to complete.

- **Actions Allow the AutoClient to Close Alarms that Have System Ignored**

This option, when set to Yes, allows the Virtual Operator (AutoClient) to complete an alarm.

Close action for alarms that have "system ignored" actions. The possible impact is that the system ignored actions may be caused by a failure to reach that contact or email.

- **Allow Operator (Password) Validated Pre-Cancels**

This option, when set to Yes, allows an operator's password to validate a pre-cancel of an alarm. When set to No, the pre-cancel form requires a password of the customer or keyholder to create a pre-cancel event.

- **Allow Operator Validated Temporary Schedules**

This option, when set to Yes, allows an operator's password to validate a temporary schedule change. When set to No, the Temporary Schedule form requires a password of the customer or keyholder to create an open/close schedule change.

- **Ask for Fire/Police/Medical Reference**

These three options determine if the Authority response dialog displays to an operator. We highly recommend setting these to Yes as it allows the ability to track permits, enter dispatch details, and cancel dispatches, when appropriate.

- **Auto Dial Auto-Dialer**

This option allows the system to immediately begin dialing telephone numbers when an operator launches and action pattern with a contact phone number. Please see your IT/ Telephony team to determine if this is an option for your telephone system.

- **AutoClient Continues Processing Alarm Event if Maintenance Issues Exist for Account**

This option, when set to Yes, allows the Virtual Operator to continue to work an action pattern despite there being an active Maintenance issue for the customer record.

- **Automatically Transfer Two-Way Audio Call**

This option, when set to Yes, transfers a telephone call to the operator receiving the corresponding alarm. When set to No, the operator must accept the call transfer. Please see your IT/Telephony team to determine if this is an option for your telephone system.

- **Call Attempt Count**

Each business determines how many unsuccessful calls an operator makes before moving to another contact and failing (completing) the contact. This option determines the global number that Manitou processes automatically.

- **Call List Must Contact**

Some organizations have persons on a call list that require contact by an operator. This option, when set to Yes, will globally force the contact be contacted or the action overridden in order to close the alarm.

- **Default PSAP Service**

When sites utilize PSAP (Public Safety Answering Point) to provide the appropriate authority based on the customer's location, or GPS coordinates, they use a PSAP database. This option selects which database to utilize.

- **Disable Auto-Purge of Pre-Cancel Disable**

Pre-cancel events have a global option (reviewed later in this lesson) setting that automatically expires a pre-cancel event to prevent failures to respond to alarms. This option, when set to Yes, requires an operator or supervisor to manually remove the pre-cancel events.

- **Disable Prompting the User to Send Contact Extension when Auto-Dialing**

The Manitou Auto-dialer can prompt a user to send the extension tones. This option, when set to Yes, disables that prompt.

- **Duress Code Policy**

The Duress code policy option contains the message that prompts the operator they validated a Duress password and what their next steps should be. *Most commonly the Duress Code policy reads something like: 'You validated a Duress code. Thank the customer, hangup and DISPATCH immediately!'*

- **Force Password Validation if Last Operator in Monitoring Group**

This option only applies to sites that have more than one Monitoring group in use. Monitoring Group 0 (zero) is the default group and does not prompt when the last user is logging out of Alarm Handling as this may be the necessary case in the event of a failover or other emergent situation. When this option is set to Yes, the system prompts last operator in any other Monitoring group for their password validation to close out of the group.

- **Maximum Number of Call List Levels**

This option prevents the creation of a recursion in the database. This determines how far the signal handler can progress through a call list calling another call list calling another until the system stops and presents the call list found last.

- **Maximum Open Alarms**

This option determines how many active alarm handling forms an operator may have open. We recommend a minimum of two (2) in this option. This allows for the auto-get to load a new alarm as it is closing the previous.

- **Monitoring Group Overflow Allowed**

This option, when set to Yes, allows signals to flow back from other Monitoring groups back into Monitoring group zero. *An example of this would be a group, like a school district, that monitors themselves during the day, but when they go home for the evening, they want the alarms to go to the 24/7 operation for handling.*

- **Off Test Warning**

This timeout determines how many minutes after a customer record returns to service, after being On Test, new alarms would generate a warning that the site was recently On Test.

Please note, this only applies to those On Test records that expire and are returned to service by Manitou. When technicians manually return systems to service accounts do not generate a warning on new alarms.

- **Require Comments When Closing an Alarm**

Manitou offers many opportunities to enter comments through the alarm handling process; therefore, forcing this option to Yes, may not be required.

- **Required Resolution Code When Closing an Alarm**

This option helps ensure that operators are applying appropriate resolution codes to every alarm.

- **Schedule Change Requirements by Type**

These options allow the selection of which types of events require a schedule change in order to close the alarm event.

- **Schedule Change to be Applied to All Schedules**

This option allows the global setting that when a schedule change is made to a single area for the account, it applies to all areas with schedules.

- **UL Warning Text**

It is important for operators handling UL (and ULC) alarms to understand that the account is UL and the response times are tracked. The script message selected for use on this option should contain pertinent UL related information. Remember, keep these messages succinct and to the point. An example UL message might be: "This is UL account, please process accordingly."

Alarm Tracking Options

- **Alarm Tracking Cancellation**

This option allows the ability to set when tracking should cancel after closing the last alarm in the queue for a customer record. The options are: Don't ask - don't cancel, Don't ask - cancel, and Ask.

Don't ask - don't cancel - keeps the tracking with the operator so that new signals track directly to that operator who is most familiar with the account at that point. This can be very useful if utilizing the Escalate command in your action patterns. The tracking will only remain with that operator through the timeout period if any new alarms do not present.

Don't ask - cancel - automatically cancels the alarm tracking once an operator closes the last alarm in the queue for the customer record. This is useful in keeping tracking records down to a minimum.

Ask - prompts the operator when closing the last alarm in the queue for that customer if they wish to keep their tracking. They can then decide if they should. This still only maintains the tracking for the timeout period, if no other alarms arrive.

It is very important to understand the meaning of the last alarm in the queue for the customer record. A suspended alarm is not closed. Tracking maintains until the closure of the last alarm for a customer record. If an operator has an alarm on hold for an extended period of time that customer can remain tracked to them. It is best to teach a habit of exiting alarm handling when stepping away from the workstation to prevent alarms "waiting" for a tracked operator.

- **Alarm Tracking Mode**

Alarm Tracking mode determines if tracking is automatic or has to be manually created by operators. We encourage the use of Automatic for this option because without tracking operators will not be able to clear all related alarms when they close the first, oldest, highest priority event. This means an operator would have to open and process every alarm event for every customer.

- **Alarm Tracking Timeout**

The alarm tracking timeout sets the number of minutes to keep tracking tied to the tracked operator after the last alarm in the queue for the customer record closes.

- **Limbo Tracking Option**

The Limbo tracking option determines if Manitou should maintain alarm tracking to a workstation, between an operator's logout and another operator's login, and which alarm priority (or higher) cancels the tracking to prevent alarm processing delays. For example, if an operator logs out of Manitou and the next operator logs into the same workstation, the tracking will maintain as long as the account doesn't generate a burg, fire, medical, or panic alarm (priorities 4-1).

- **Limbo Tracking Timeout**

The Limbo tracking timeout defines the maximum number of seconds the tracking maintains on that workstation. A recommended period is 60 seconds or less.

Contact Point Device Defaults Options

With the addition of the AutoText and OpenVoice (outbound) features came additional contact point types. These options set defaults for each type.

AutoText Options

There are three options for the AutoText features:

- **Autotext Default Output Device Type**

This option allows the ability to select the default passageway for AutoText messages. Currently, this is only the Manitou MediaGateway.

- **Autotext Default Script Message**

This option allows the select of the "when all else fails" script message in order to ensure that events sending AutoText notifications has something to send.

- **Autotext Default Service Device**

This option allows the selection of which Universal Connector pathway to follow when sending the messages.

OpenVoice Options

There are three options for the OpenVoice (outbound) features:

- **Openvoice Default Output Device Type**

This option allows the ability to select the default passageway for OpenVoice messages. Currently, this is only the Manitou MediaGateway.

- **Openvoice Default Script Message**

This option allows the select of the "when all else fails" script message in order to ensure that events sending OpenVoice notifications has something to send.

- **Openvoice Default Service Device**

This option allows the selection of which Universal Connector pathway to follow when sending the messages.

AutoText and OpenVoice are add-on features that allow communications to customers through electronic means.

General Options

The general options contain some items that don't have a specific category under other headings.

- **Customer with “Pending” Status May be Made Active Upon Receipt of a Signal**

This option allows the ability to make an account active automatically based on the receipt of a signal. The three options are: Never, Any Signal, Not "On Test" Signal.

Never means exactly that. Your operations chose not to utilize this automatic feature and all accounts will be made active manually, or upon creation.

Any Signal means that any signal that passes through the receiver to that receiver line prefix and transmitter ID will automatically activate the account. This can be useful to ensure a new account isn't left pending when it is signaling into the monitoring center.

Not "On Test" Signal means that once an account is placed on test then taken off test again, the next signal that passes through the receiver to that receiver line prefix and transmitter ID will automatically activate the account. This is useful to ensure that when the installing technician is done with their install the system will activate immediately following the next event that passes into the monitoring center.

Please note that the Pending status acts like a deactivated account. The signal handler will not process signals into the account when the status is pending. If a technician is to see signals into the account they will need to have an active or inactive account placed on test.

- **Default On-Test Time**

Based on business practices the Default On-Test time may be set to a specific number of hours. Many sites will set this between 1 and 4 hours. This simply populates the On Test form with the time. Operators may change this at the time they create the On Test entry.

- **Monitoring Company Person May Access Dealer Accounts**

When a company offers "full-service" to their end customers as well as monitors "third party" accounts, technicians for the monitoring company may need the ability to put third party accounts on test. This option allows a technician to, through remote access, view third party accounts as well as those tied to the monitoring company. This is a business practice decision that the company leaders make.

- **On-Test Protection**

This option, when set to Yes, ensures that technicians accessing Manitou through BoldNet or BoldNet Mobile may only place accounts on test that have a corresponding Maintenance issue created for the account.

- **Script Message for Maintenance Issue Assignment**

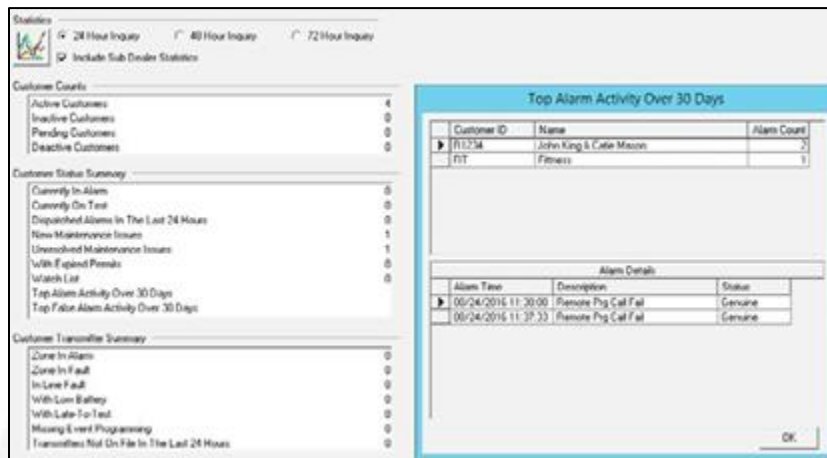
In order to prevent blank emails going to technicians when they are assigned a Maintenance Issue, select a script message that enters into the body of the email when emailing the notification. Technicians are automatically notified of a Maintenance Issue assignment when their ID is assigned to an issue.

- **Statistics – Customers to Display on ‘Top’ Lists**

This relates to the Dealer Statistics page within the Operator Workstation. The number selected here determines the number of customers to include in the 'top' list.

- **Statistics - Days Used to Calculate on 'Top' Lists**

This option determines how many days to use as a calculation parameter for the 'top' statistics.



Purge Options

The purge options contain items that determine when to remove elements from Manitou.

- **Alarm Activity Detail to Keep (Days)**

This option sets the number of days for Manitou to keep for analysis purposes. This does not mean that the activity is purged from the customer records.

- **Database Backup Instructions String**

This option relates to a period of time where the database backups had to be completed through a Windows task. This is no longer the case as Microsoft SQL Server has Maintenance plans that work effectively.

- **Database Backup Time of Day**

This too relates to an older process, but it is useful to list what time of day the expected database backups occur for reference.

- **Number of Days Before Purging Temporary Open/Close Schedules**

When an operator creates a temporary Open/Close schedule through data entry or alarm handling, this generates a permanent record that when completed is not necessary to keep. There is still a reference in the customer activity log of the change. This option when set to 6, the most common setting, it keeps the schedule in the account for just about a week before purging.

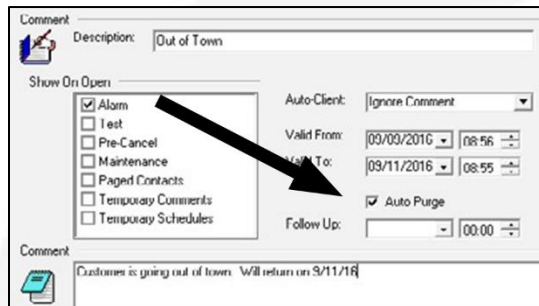
- **Number of Hours Before Purging Expired Reminders**

Reminders are used for many reasons, within customer records. A few examples are: to create a daily alarm for an operator to call and check on a persons welfare, create an annual reminder for Fire testing, or to monthly check a personal protection unit. These items can be set to expire. When they do, this option determines how many hours to keep them after the have expired. Once this time expires, the item deletes

from the database. When this option is set to zero (0) the expiration will not purge ever. The only way to purge it would be to manually remove it.

- **Number of Hours Before Purging Expired Temporary Comments**

Temporary comments are just that, temporary. Therefore, it is possible for Manitou to clear out the expired items flagged for purging. This option sets how many hours to wait before purging temporary comments marked for purge.



- **Number of Hours to Keep Completed Scheduled Reports**

When a report runs successfully and is handed to the publishing destination there is no need to keep the reports in the report queue for an extended period of time. In many cases, this option is set to 1 hour.

- **Number of Hours to Keep Failed Reports**

Unlike the completed reports, a failed report does require attention by a supervisor or other responsible party. Therefore, the most common setting for this is 96 hours as it allows for a responsible person to be away for a weekend and still be able to review any failures.

- **Number of Hours to Keep On-Demand Reports**

On-demand reports are run ad hoc when a customer or team member needs it. Once again, if everything is right and the report ran and made it to the Publisher, there is no need to keep it in the report queue for a long time. This option is often set to 1 hour.

- **Number of Hours to Keep Previewed Reports**

A previewed report may require a bit more time to sit in the queue just in case someone may need to review it for any reason. This option is often set to 2 hours.

- **Number of Months of Customer/Raw Data/System Logs to Keep**

These three options are for reference only and will not automatically purge any data from the database. This can be used to set a standard that when your business is ready to purge data these values as a baseline. *Purging data from the database is currently a service Bold offers to customers.*

- **Paged Contacts Expiration**

This option sets a time period, in minutes, that will keep a "paged contact" within the listing, then it will purge out. Paged contacts are created when sending pager messages or leaving a message on a voice mail for a customer.

Signal Processing Options

The Signal Handler is a vital part of the Manitou System it determines how to process the alarm/signal events. The Signal Processing options allow sites to set global standards for many items.

- **Address Lookup for GPS Signals and Alarms**

When set to Yes, the system performs a lookup for the address linked to the GPS coordinates for all signals and alarms. This works in conjunction with GPS related services in Manitou.

- **Cancel and Abort Time Limit**

Many event codes contain signal processing attributes that allow alarms to auto-cancel and/or abort if the signal is not yet touched by an operator and receives an acceptable restore event. This time limit, set in minutes, determines how long those attributes have to allow the cancellation and/or abort. This global option varies from site to site. Some will have this set to 60 or 90 minutes while others will have this set to less than 10 minutes.

- **Check Transmitter Default Event Programming Before Dealer Event Programming**

After a signal processes through its translations within the Transmitter Type and/or Customer Transmitter, the Signal Handler must then determine where to assign the Action Pattern. This is done through the Event Actions Programming found under the customer, dealer, or Transmitter type. When selected yes, the pecking order goes from Customer, Dealer, Transmitter to Customer, Transmitter, Dealer. *When there are no Event Actions Programming lines at any of these levels the Signal Handler assigns the Global Action pattern assigned to the Event Code. Still, the signal handler will check for action patterns on the customer and dealer that have the same global code to provide the most specific action pattern required.*



Event	Area	Zone	Alarm	Action ID	Instructions
-------	------	------	-------	-----------	--------------

- **Do Not Bypass Duplicate Event Check for Video and Audio Alarms**

When set to Yes, this option causes the system to perform a check for duplicate events for video and/or audio related alarms. When the option is set to No, the user should expect to see every event, even when duplicate, because of its association to a Video or Audio event. And when set to Yes, the duplicates follow the duplicate rule set in the Generate Duplicate Alarms option.

- **Dual Reporting Signal Timeout**

It is possible to link signals on the Transmitter or Customer that are expected to signal on both transmitters when either one receives a signal. If the second signal doesn't arrive Manitou can produce a "Missing Dual Signal" alarm. This option determines how long the Signal Handler will wait for the second signal before generating this warning.

- **Early Open/Close and Late Open/Close Windows**

These four options: Early Close Window, Early Open Window, Late Close Window, and Late Open Window, determine how many minutes surrounding an Open/Close schedule will an Unscheduled Open or Close event be presented to Manitou as an Early or Late event. This is still, by default, an exception, however, generating a different event allows the ability to tie a different action pattern based on the event's proximity to the acceptable schedule.

- **Fill Caller ID 1**

This option enables the Signal Handler to add the Caller ID received within an event to add to the Caller ID 1 field if the field is blank.

- **Generate Alarm Event Upon Expiration of the Temporary Comment Follow-Up Date**

When set to Yes, this option causes the Signal Handler to create an alarm with the event code of "**EFUP" where the Action Pattern may be to call and verify the comment will expire as expected on the end date.

- **Generate Duplicate Alarms and Generate Duplicate Events**

These two options are significantly different. A Duplicate Alarm is an event that is EXACTLY the same. Same event Code, Same Zone, same everything. On the other hand, a Duplicate Event need only have the same action pattern. Therefore, the recommended settings are:

Generate Duplicate Alarms = No

Generate Duplicate Events = Yes

- **Generate Maintenance List Items**

When an account signals and open, close, or transmitter test event, Manitou can automatically generate a Maintenance Issue drawing attention to the possibility of a missing chargeable service. The options allow the choice of Open/Close or Test signals, both, or neither.

- **Ignore Called ID Mismatches**

This option is often set to Yes due to the potential for bad data in the database to generate every event with mismatch to generate an alarm to an operator's attention. This includes non-alarm events like open, close, test, etc.

- **Log Signals That Are Not on File**

This option relates directly to the events presenting into Manitou that do not have a matching receiver line prefix and transmitter ID to map the event to an actual customer record. During a new site's transition to Manitou this option is set to No in order to catch any signals that may not be mapped correctly through the receiver into Manitou. After transitioning to Manitou live, sites often switch this option to Yes as operators have no way of processing the alarms other than generating a notification for someone to research the data.

- **Pre-Cancel Timeout**

This timeout, in minutes, determines how long to keep a Pre-cancel event active before purging it. The possible impact of a time set too long is that a real event could come in while the pre-cancel is active and the operator may cancel the alarm on this authorization. We recommend this time be as short as possible to avoid this.

- **Prevent Duplicate Video Alarms from Being Forced to an Operator**

This option, when set to Yes, will not force duplicate alarms to an operator when they contain video content.

- **Prevent the System from Forcing Video and Audio Alarms to an Operator's Screen**

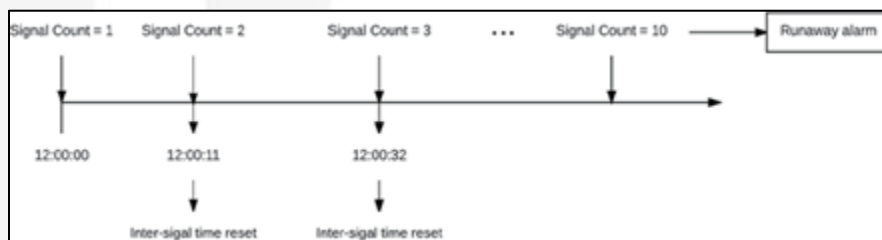
This option pertains specifically to the Virtual Operator's ability to take the first actions, when possible, on a video or audio alarm. When set to Yes, the Virtual Operator may process its actions before delivering the alarm to an operator with the video or audio data.

- **Redirect Event Codes for Non-Intelligent Signals**

Used exclusively for small businesses that monitor basic alarm systems. When enabled, set to Yes, an additional column of data displays on the zone list that allow the zones to be pointed directly to a single event category. This is not recommended for sites receiving signals like Ademco Contact ID or SIA.

- **Runaway Inter-Signal Time and Runaway Signal Count**

These two options work together to determine how many signals within the inter-signal timeout constitute a Runaway event that operators must action.



- **Track Additional Panel Statuses**

Most sites leave this option set to No given that the additional panel statuses do not have a restore and clear capacity. Therefore, the events would remain in the Zone status of the customer record indefinitely.

- **Two-Trip Signal Timeout**

This option sets the number of seconds that the first signal flagged to participate in Two-trip delay will wait before logging as a single event if the second event doesn't arrive. This is a global setting. We suggest using the confirmed command when a more specific timeout is required.

System Options

The system options pertain to the global settings for several Manitou features.

Dealer Billing Options

The Dealer Billing options relate to licensed, and integrated, Accounting packages where the company uses Manitou to generate data for Dealer Billing.

- **Dealer Billing by Monitoring Service**

When set to Yes, this option will run dealer billing based on the Monitoring services tied to the corresponding customer records. No means that the billing runs against the individual class codes related on the customer records.

- **Dealer Billing Prorating**

Setting this option to Yes enables proration of the dealer billing charges.

- **Dealer Billing Standard Annual Cycle**

This specifies the month to start the standard annual billing cycle for dealer billing.

- **Dealer Billing Standard Quarter Cycle**

This specifies the month to start the standard quarterly billing cycle for dealer billing.

- **Dealer Billing Standard Semi-Annual Cycle**

This specifies the month to start the standard semi-annual billing cycle for dealer billing.

- **Dealer Billing Summary Billing**

When set to Yes, this option produces billing invoices in summary format for recurring charges only.

- **Next Dealer Billing Cycle to Generate**

This is the date for the next Dealer billing cycle. This creates the "line in the sand" for producing Dealer Billing cycles. It is only required to set this for the first cycle. See the Dealer Billing documentation for more details.

Other System Options

- **Do not Warn if an Alarm Arrives for a Deactivated Customer**

When an alarm arrives for a customer record that is deactivated, the system, when the option is set to No, generates a Watchdog warning stating that the alarm arrived but was not processed. We encourage sites to keep this set to No when they are transitioning from another software system to ensure people are researching the warnings. Once live on Manitou, set this option to Yes, to prevent desensitizing operators to Watchdog messages.

- **Last Overdue Signal Check**

This option displays in GMT (Greenwich Mean Time), therefore this time can appear to be in the future or in the past. This simply documents the Overdue Checker last activity.

- **Resolution Code Group Setup**

Resolution codes may be configured into multiple groups. Keep in mind the Resolution Code Groups allow the creation of six (6) groups with a total of 8 characters across the groups. For example, if the first resolution code group that has a single character that simply documents the validity of the alarm event it may have three (3) configured individual letters F for False, for Actual, and U for Unknown. Then perhaps the second resolution code group is a more descriptive cause analysis code. It may have two (2) characters to allow for more codes, such as: WE for Weather related causes, PD for Police Dispatched, and the like.

If a resolution code group already exists, and there are resolution codes created within that group it is not possible to change the code group size. To change a resolution code group size remove all the codes within the group, save, then edit this option. We strongly recommend planning your needs before making changes to the resolution codes and the group sizes.

- **Validate the Resolution Code is Complete**

When an operation has more than one resolution code group it is possible to then require that all groups be completed by an operator before closing the alarm. (This also ties into the "Require a Resolution Code" option described earlier.)

- **Use External Browsers for URLs**

The browser, contained in versions older than 1.64, is a wrapped version of Internet Explorer (IE) that does not support some of the current functionality on many web sites, especially video. Therefore, setting this option to Yes, allows for a URL to load into a desktop browser that supports these newer technologies.

- **Workflow Functionality**

This option set's Manitou to allow for a Workflow window to be available in the Alarm Handling form and enables the creation of Workflow components. ManitouNEO replaces this functionality.

PBX Options

- **PBX Assistant**

When licensed, this option determines which operator type(s) is(are) activated to display the PBX call control panel.

- **PBX Assistant**

This option determines if the operator is automatically set to Ready or if the operator will manually set themselves to ready. The three options are: Never, At Logon to Manitou Operator Workstation, or Register Alarm Handler.

Web Options

- **Web Membership Database Details**

This option automatically populates with the Web Membership database details upon its connection to the BoldNet Web Gateway.

- **Web Timeout**

In order to protect customer data, the system is equipped with a timeout to log users out of BoldNet after the defined minutes of inactivity.

Additional Options

The previous sections detail the most commonly addressed and adjusted options. This section details the additional options and their significance to end users.

Location/GPS Options

Location and GPS options require definition when Manitou is licensed for Location services and/or GPS tracking.

- **Bing Location Services Key**

This option details the BING license key utilized for Location services.

- **Google Location Services Key**

This option details the GOOGLE license key utilized for Location services.

- **GPS Fine Lookup Event**

This option configures which event code should trigger a "fine" lookup. The event code itself should also be configured to perform a fine lookup through Transmitter Programming Commands.

- **Mapping Types**

This is the type of Mapping software to use for Manitou. This does not relate to the mapping used in Disaster Mode.

Output Details Options

In order for outgoing emails, faxes, and pager messages to be from a recognizable source it is necessary to configure these options with company specific details.

- **Email – From Address**

The email from name is the email address that would populate if someone hit reply on a received email. ☒ Many sites choose to use a ["no-reply@monitoringcentername.com"](mailto:no-reply@monitoringcentername.com) to help discourage people replying to that address. Others have a staff member, or group of staff members, who is responsible for any replies that come to that address.

- **Email – From Name**

This is the name that publishes on an email. Sites vary on what they enter based on their business practices. Some enter a generic name like "Monitoring Center" or "Central Station," while others will be specific to their business name.

- **Email – Subject to Include Customer’s Street Address**

This option, when set to Yes, can help further specify the information provided by including the street address within the Subject line. This is very useful to those who many have several businesses, or residences, monitored by the same organization.

- **Fax – Company Name**

Like the Email From Name, this is the name that lists on the page of the fax going to the end person.

- **Fax – Delivery Report Address**

If the faxing services, employed at your organization, have the ability to email delivery reports to an address, this may be configured here.

- **Fax – Delivery Report Type**

The Delivery report type is going to determine how to pass through the delivery confirmations.

- **Fax – Department Name**

If the faxing services have the ability to include details of which department sent, configure the department name within this option.

- **Pager – Company Name**

Also like the Email Company Name, this option sets the company name included on pager messages, where applicable.

- **Pager – Default Message**

This is the Script message that is used when no other overrides exist.

- **Publisher File Directory**

This is the place configured on each Manitou Server where temporary report files may reside until publishing of the reports is confirmed. In general, the address is either c or d:\TEMP\ PUBLISHER\. Once set, this file name should not change unless it is updated here as well.

- **Third Party Fax Driver Details**

When using something other than Windows Faxing services it is helpful to document these details within Manitou.

Password Options

Manitou Passwords may be forced to be as complex as Windows passwords.

Passwords

Can re-use passwords: Yes No

Minimum alpha characters:

Minimum numeric characters:

Minimum symbolic characters:

Minimum password length:

Require mixed-case

Login retries before lockout: Unlimited retries

Lockout period (mins): Lockout indefinitely

- **Can Re-Use Passwords**

When set to Yes, operators may re-use passwords when forced to change them through their user settings. When set to No, Manitou maintains a used password list and will not allow operators to change their password to something that was used in the past.

- **Minimum Alpha/Numeric/Symbolic Characters (and Mixed Case)**

This allows the ability to set standard requirements for complex passwords. When the number of alpha characters is 2 or greater than it is also possible to require mixed case.

- **Minimum Password Length**

The minimum password length defaults to the minimum number of alpha, numeric, and symbolic characters required. It is possible to set these higher than the minimum combination.

- **Login Retries and Lockout Period**

These two options set the maximum times an operator may type their password incorrectly before locking out the user. Once locked out the lockout period determines the number of minutes to lock out the operator.

The unlimited retries is insecure and not recommended for use in a security environment.

Lockout indefinitely requires that a supervisor log into the Supervisor Workstation to unlock the locked out user. This is usually done in conjunction with a password reset.

Reporting Options

The reporting options set standards for size and sorting.

- **Do Not Send Empty Customer Activity Reports**

This option pertains only to Customer Activity reports. When set to Yes, the Publisher reviews the content of reports before emailing them out to an end customer and will not send reports without information within them.

- **Include Primary Receiver Line Prefix/Transmitter ID with Customer Name**

As opposed to many older software platforms, Manitou has the ability to have a single site address with all their related equipment. In order to reduce confusion, this option allows the inclusion of the primary receiver line prefix and transmitter ID next to the Customer name. The options are: don't include it (0), place it before the customer name (1), or place it after the customer name (2).

- **Maximum Report Size**

This option defines how big a report is allowed to be before the Report Server quits with an error that the report is too large. This is to prevent the reports, running against the database, from bogging down the database and thereby the Manitou system. Many sites use 50 Megabytes (MB) as their maximum.

- **Report Segment Size**

Alternatively, the report segment size is how large a report can be before it is broken down into smaller chunks for emailing purposes. This option is most often set to the smallest maximum attachment size allowed. At this time, that is about 10 MB.

- **Script for Email Body Text**

In order to prevent spam filters from removing an emailed report, it is necessary to have content in the body of an email. This script message contains the Report Name as a field that updates at the time of the publishing of the report to an email. ☒ Please note, the only dynamic part of the report script is the Report name. No other variables change, on the fly, for this message.

- **Size in Kilobytes, at Which Reports Will Zip for Email Publication**

This is an older option when attachment size was a premium. When set to negative one (-1), reports never zip. When set to zero, reports always zip. Any other value is the size limit before reports are zipped for publication.

- **Sort Order of Reports**

This option has two choices: alpha or numeric. If your customer ID numbers are mixed between numeric and alpha it may be best to choose numeric. When choosing alphabetical, 1, 101, 1000, 1001, 10000, sort before 2.

Response Options

The response options set standards for sites using NACOSS reporting of response times. This is generally just sites located within the UK.

- **Fast (Fire, Other, Panic/Social)**

These options set the timing, in seconds, for expected dispatch response times.

- **Medium (Fire, Other, Panic/Social)**

These options set the timing, in seconds, for expected non-threatening alarm dispatch response times.

Version/Revision Options

The version/revision options set standards for the database version and client revisions to warn when a client is out of date with the rest of the system.

- **Client (Dealer, Operator or Supervisor) Revision**

This revision number, when configured, sets the minimum revision allowed. If someone attempts to connect with a revision lower than the set number they receive a notification that their client is out of date and requires an update. Please note, this is a manual feature and would require update after running a patch update each time.

- **Version of the Database**

This should coincide with the key Manitou version you have. This is automatically updated when a new release updates the database version.

Voice Recordings Option

This option sets the location of the Voice Recording database when integrating with SureVoice.

Watchdog Options

The Watchdog option section contains the option of setting the number of months of watchdog logs to keep. Like the other purge options, this is a reference only field and will not purge any data automatically.

Permissions, User Groups and Users

Defining What Each Person May See or Do

Introduction

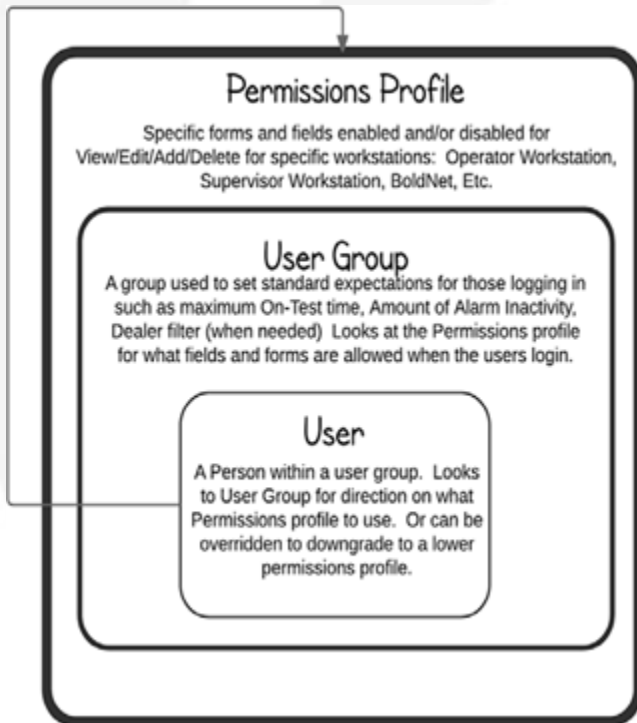
This chapter details how to configure permissions profiles, apply those profiles to user groups, and link users to user groups.

Permissions

Permissions are found within the Supervisor Workstation under the Maintenance Menu, under Setup, then Permissions. The default view, when loading the Permissions form, displays the {Global Template Defaults} profile.

Permissions profiles are the "top-level" of the hierarchy enabling access to the elements of the Manitou system.

The image below shows the different elements of this relationship.



The Profile specifies the form and field access. The User Group sets standards for those in the group and ties to a default profile for that group. The User is grouped within an User Group and either uses the default profile or is overridden to downgrade permissions.

The Permissions Form

The Permissions form is divided into three key sections. The profile section, the Profile Permissions, and the Profile Permission details.

- **Profile**

The profile section allows the addition of a permissions profile and the selection of existing profiles.

- **Profile Permissions**

The profile permissions section is a tree view of all available permissions. Within the profile permissions section there is a find feature that allows the ability to search for any label or topic within the permissions.

- **Profile Permission Details**

The Details section contains all the different permissions with the applications where it is possible to enable visible, addable, editable, and delete-able.

Creating a Permissions Profile

To create a Permissions profile:

1. Ensure the Permissions form is in Edit mode.
2. Within the Profile section, click Add.
3. Enter a name of the Profile. Be clear and descriptive so it makes sense to others.
4. Click OK.
5. The default permissions profile sets the standard permissions from the default.
6. Save the record.

Understanding the Permissions

We do not go into detail of each permission within this course. However, in general, the permissions are broken down into the key sections where they are located in the application(s).

- **Application Section**

The Application section contains the permissions related to the File menus and options within the Web-based applications.

- **Maintenance Section**

Maintenance relates to all data entities within all applications. The section is broken down into its sub groups: Administrative, Agency, Authority, Branch, Customer, Dealer, Deleted Customers, General, Global Keyholder, Maintenance Issues, Options, and Quick Load.

- **Administrative** permissions contain most items found within the Supervisor Workstation.
- **Agency, Authority, Branch, Dealer, Deleted Customers, Monitoring, Maintenance Issues, and Global Keyholder** permissions pertain to their related data within the Operator Workstation.
- **Customer** permissions are the most detailed. There are some permissions that will override others. *Please note that the customer Address and Language permissions are required to be visible and editable in order to enable other edit capacity within the customer records.*
- **General** permissions relate to Geo-fencing.
- The **Option** permission allows the restriction of creating new cities during the data entry process.

- **Operations Section**

The Operations permissions pertain to the items related to handling alarms within the Manitou Operator Workstation. This section breaks down into several sub-sections:

- **Administrative** relates to operational items within the Supervisor Workstation.
- **Alarm Handling, Alarm Queue, and Alarm Tracking** enables and disables specific alarm permissions.
- **Graphical Incident Queue** relates to those using Manitou PSIM and relate to their alarm handling queue options.
- **On Test** relates to the ability to add, edit, or delete On Test records.
- Some sites disable the **Paged Contacts** as they don't use the feature.
- **Pre-cancel** permissions relate to the ability to add, edit, and delete the records. The option determines if an operator password may validate and create them.
- **Reverse Channel** relates to the ability too see and interact with the commands that reach out to equipment in the field.

- **System Reports Section**

The System Reports section allows the ability to enable and disable what users may see and touch when running reports. The Report Type permissions are granular enough to hide specific reports from end users.

- **Templates Section**

Templates are created within BoldNet when the user is allowed. This allows them to create a standard account creation process for BoldNet users.

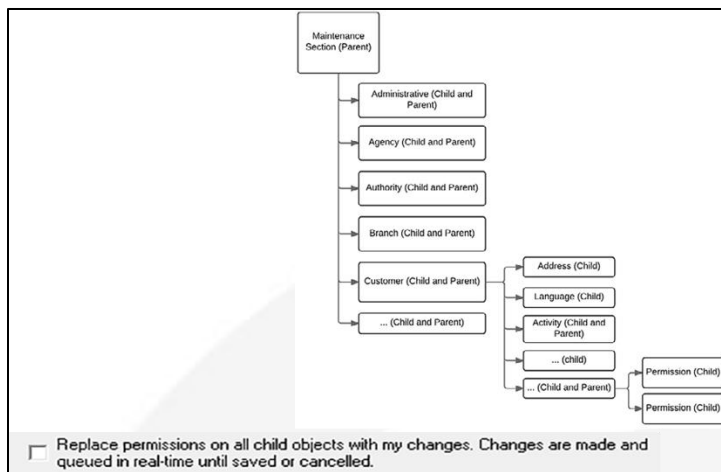
- **Tools Section**

The Tools section includes the ability to enable and/or disable access to features like: Change Customer ID, Dealer Takeover, and Manual signals.

Editing Permissions

It is a good practice to start with a completely enabled permissions profile then start locking down specific items as needed.

Manitou has the concept of Parent/ Child relationships when it comes to permissions. Like all elements of Manitou, the Permissions profile has a tree-like structure that has a high-level topic called a parent and sub topics underneath that are considered children. Children can also be parents.



To edit permissions:

1. Load the Permissions form and click Edit.
2. Drop down and select the appropriate Permissions profile.
3. Locate and select, or deselect, the appropriate permissions. ☒ Please note if using the replace permissions check box, that you select that BEFORE you change permissions, or you will have to select/deselect the permissions again.
4. Repeat as necessary.
5. Save the Record.
6. Test. *It is important to check changes made to permissions so that there aren't unexpected issues with the changes.*

After creating and editing a permissions profile the next step is to add it to a User Group or User.

Where are Permissions Profiles applied?

Permissions profiles are applied to:

- User Groups
- Individual Users
- BoldNet Users

User Groups and Users have their permissions profiles applied within the Supervisor Workstation. BoldNet Users are configured within the individual records where they have access. For example, an individual end customer will require their BoldNet user created within the Contact List of their individual customer record(s). Technicians for the Monitoring Company, or Dealer, require configuration within the Contact List within the Monitoring Company or Dealer records. The same is true of Branch users. Global Keyholders have their credentials created within their Global Keyholder record.

It is possible to review all the configured BoldNet Users from within the Supervisor Workstation. The Web Membership form is found under the Maintenance menu. While you can edit and add web users here, users will not work correctly without their context of, customer, dealer, branch, global keyholder, or monitoring company contact lists.

BoldNet Users with a permissions profile may only make changes based on that profile when they have the "Can edit customer" permission enabled on the contact list. Similarly, BoldNet users may only place accounts On Test from the Web when the "Can put customer On-Test" permission is active.

User Groups

User groups have permissions profiles tied to them as well as some standard settings. User Groups are found underneath the Maintenance Menu within the Supervisor Workstation. Within the user Groups form there are four specific sections: User Group, Security Restrictions, Profiles, and Options.

The screenshot shows the 'User Groups' configuration interface. On the left is a navigation tree with items: 0 - System, 1 - Administrator, 2 - Supervisor, 3 - Operator, 4 - Data Entry, 5 - Trainee, 6 - Dealer. The main area is titled 'User Groups' and contains the following fields and sections:

- User Group:** User Group: 3, Description: Operator
- Security Restrictions:** Dealer, Branch, Access, Alarm Handling, Accounts User ID (all dropdown menus)
- Profiles:** Permission Profile: Operator
- Options:**
 - Give audio beep if alarms available
 - Can choose own password
 - Maximum logged on time (minutes): 0
 - Maximum inactivity time (minutes): 0
 - Maximum alarm inactivity time (seconds): 0
 - Exit alarm handling on timeout:
 - Maximum job on test time (minutes): 480
- Accept Call Types:**
 - Unknown
 - Cancel Alarm
 - Confirm Alarm
 - Key holder Change
 - Schedule Change
 - Customer Change
 - System Test

- **User Group** details the number of the group and the description of the group. You may update the description to a more specific to your business practices.
- **Security Restrictions** are used to filter for a specific dealer or branch and if they will have access to edit customers or handle their own alarms. If they have access to accounting their specified user ID for that can be added.
- **Permissions Profile** is where to select the profile to use for the permissions created within the Permissions form. This is the default profile used by any user that resides in this group.
- **Options** set standards for how the users in the group behave:
 - **Give audio beep if alarms available** allows those who do not handle alarms to avoid hearing the audio beep each time an alarm enters the alarm queue.
 - **Can choose own password**, enabled, is highly recommended so that operators must add a password that only they know. This is much more secure than assigned passwords.
 - **Maximum logged on time (minutes)** allows the monitoring center to force breaks or shifts by reminding users that they will be logged out unless they extend. Zero (0) means that the maximum logged on time will never occur.
 - **Maximum inactivity time (minutes)** locks an operator's workstation if they do not actively work on the system for the prescribed number of minutes. A Zero (0) setting disables this

functionality. Please note that when the system is locked, either through this function or manually, ONLY their operator password can unlock it again. If the operator leaves the workstation in this state, the only option is to Task Manager kill their session.

- **Maximum alarm inactivity time (seconds)** takes an idle alarm away from an operator when this option is set to any value greater than zero. Many sites set this to approximately 180 seconds to allow for slow customer, or authority, response, without leaving alarms sitting on an operator's workstation indefinitely. Please note that operators are warned with a 10 second countdown that the alarm will be removed. They are given the opportunity to keep the alarm or defer it back to the alarm queue. If they don't respond to the dialog within the 10 second countdown, the alarm removes the tracking and defer the alarm to be made available for the next available operator.
 - **Exit alarm handling on timeout** determines if the operator remains an alarm handler if they had an alarm removed from them.
- **Maximum job on test time (minutes)** sets the upper limit for how long an operator may place an account on test under their user credentials. Any value between 1 and 1440 restricts the user within that group to placing accounts on test to that maximum. Common settings are: 240 (4 hours), 480 (8 hours), and 1440 (24 hours). When set to zero (0) the group's users have unlimited access to place accounts on test indefinitely.
- **Accept Call Types** is not yet implemented. The concept behind this is that when using a PBX or other call routing feature the group has assigned call groups for routing calls to the right person.

Each group may have different permissions profiles and settings. Once created and set as needed the groups may then be tied to Users.

Users

The Users form, also found underneath the Maintenance menu within the Supervisor Workstation, allows the creation and maintenance of users logging into Manitou from within a monitoring center.

The screenshot shows the 'User' configuration form. It is organized into several sections:

- User:** Fields for User ID (BOLD), Name (Bold Technologies), Contact Point, and Extension.
- Password Information:** Fields for Change Interval (Never), Password, Confirm Password, Change at next logon (checkbox), and Locked Until (00:00).
- Security Restrictions:** Fields for User Group (Administrator), Permission Profile (Administrator), Dealer, Branch, Access, Alarm Handling, and Accounting Access.
- Options:** Fields for High Priority (1), Low Priority (0), Alarm Queue Read Only (checkbox), and Allow IM (checked).
- Locales:** Fields for Locale (English (United States)), Country (United States of America), and Alternates (English (United States)).

The Users form contains five key sections: User, Password, Security Restrictions, Options and Locales (also known as languages).

- The **User** section contains:
 - **User ID** which is what the operator uses to identify themselves when logging into Manitou. This is the value assigned to that user within the customer and other activity logs within Manitou. ☒ Some sites choose to use initials, numbers, or other naming standard. See your leadership team for the rules within your organization.
 - **Name.** This should be the user's full name. It does not publish within the activity log like the User ID does.
 - Contact Point and Extension are optional fields that can be used to maintain personal contact information as needed.
- **Password** Information contains:
 - **Change Interval** which establishes when Manitou prompts an operator to change their password. Most regulatory entities require passwords be changed, at a minimum, quarterly.
 - **Password and Confirm Password** is used to enter a password for a user. This is completely obfuscated (hidden) from view therefore typing these passwords twice confirms the password is correct.
 - **Change at next logon** ensures that operators are forced to change their password to something no one knows before they log into Manitou the first time.
 - It is possible to use **Locked Until** to prevent a user from accessing Manitou until a specific date and time or is automatically enabled by the lockout setting in the Password options.
- **Security Restrictions** are exactly like those found within the User Group with the **User Group** and **Permissions** profile added. *The only time it is necessary to change the permissions Profile from <User Group's Profile> is when a user is for some reason downgraded to a more restricted profile. This is most often when the user is a trainee but will be part of the general Operator group. When they complete their training period, a supervisor can then reset their profile back to the <User Group's Profile>.*
- **Options** allow:
 - **High and Low Priority** restrictions. This ensures operators may only handle alarms within the priorities they are allowed. When left blank, operators may handle all alarm priorities. This too is often used for new operators during their training period.
 - **Alarm queue read only** restricts the user from accessing alarms and prevents them from pulling alarms down from the alarm queue.
 - **Allow IM** allows the user to type into the IM feature. This does not remove their ability to receive IM messages. They simply cannot reply.
- The **Locales** section enables the ability to select all the languages the operator may speak fluently. If your operations have fluent language speakers beyond your default language, on all shifts, you can utilize this feature through adding the languages for the operators and noting the languages the speak. If this is the case it is also possible to list the customer languages within their individual records. Alarms that deliver to operators only deliver to operators that speak the customer's language.

Creating a User

To Create a user within Manitou, do the following:

1. Locate and load the users form.
2. Click Edit.
3. Click Add.
4. Enter the User ID, following your company's practices.
5. Enter the full name of the user.
6. Click OK.
7. Set the Password Change interval.
8. Enter the password twice.
9. Select "Change at next logon."
10. Select the correct User Group for the User.
11. Set any applicable options.
12. If the user speaks more than one language select their alternate locales within the Locales section.
13. Save.
14. Provide the information to the appropriate user and ensure they can login.

The screenshot shows the 'Add User' dialog box. The left pane has fields for 'ID:' and 'Name:' with 'OK' and 'Cancel' buttons. The right pane, 'Password Information', includes a key icon, 'Change Interval' (Never), 'Password:' and 'Confirm Password:' fields, a checked 'Change at next logon' checkbox, and an unchecked 'Locked Until' checkbox with a time field set to '00:00'.

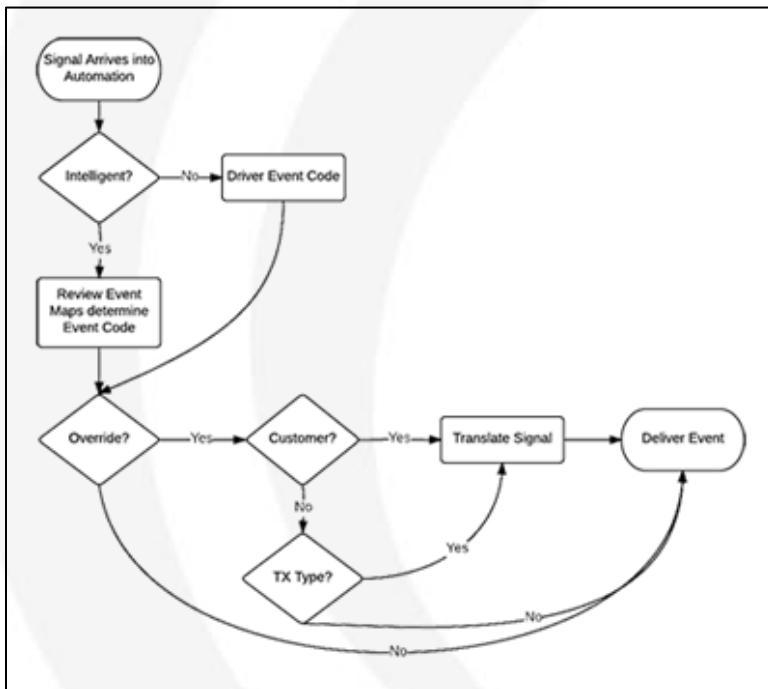
Event Maps, Categories and Codes

Building Signal Structure

Introduction

Manitou's key functionality is signal processing for alarm operators to manage. The Signal Handler translates the signal and then determines which event to process to an operator. During this chapter, we learn about Event Codes, Event Categories, and Event Maps. The way a signal processes into Manitou is as follows:

For Manitou to know which event to present to an account there are several decision points along the way. Each signal type and receiver has a default driver that does some basic organization of the signal and translation of some standards. After that, the Signal Handler looks to see if the event is Intelligent or non-intelligent. Please feel free to review the basic signal processing details from the Data Entry training for more detail. When the signals are intelligent, this is where the Event Maps come into play.



Event Maps

Event Maps allow the management of disparate (varied) signaling formats into a single common format. The Event Maps take the intelligent signals passed into Manitou then reviews and translates these events.

Why use Event Maps?

There are many different formats and teaching operators on each format can be time consuming and frustrating. Event Maps level the field and ensure that all events signaling into an operator look similar and intuitive. This flattens to learning curve such that new operators could handle an alarm their first day without confusion.

How Event Maps Work

Event Maps take the intelligent signal and translate them to common "SIA-like" codes. SIA set a common standard that was intuitive. For example, BA stands for Burglar Alarm, FA stands for Fire Alarm, etc. Manitou Event Codes are very similar but may have more than two characters to manage for more detailed formats like Ademco Contact ID. Ademco Contact ID has over 1000 configurable codes preceded with an E for Event, R for Restore, and P for Status events. This can take some time for a new operator to learn and understand and in general the events fall into specific groupings such as 130-139 are all some form of Burglar events. Using the Manitou Event Maps allows a business to customize how the largest percentage of events come into Manitou.

Configuring Event Maps

Prior to configuring Manitou Event Maps it is best to understand the company's standard practices when it comes to configuring systems in the field. For this example we use Ademco Contact ID, to demonstrate the functionality. To update the Event Maps:




1. Navigate to the Event Maps form. (SWS > Maintenance Menu > Events > Event Maps.
2. Click Edit.
3. Select the Event Map type. (ACID - Ademco Contact ID for this example)
4. Scroll to the Event Code to update, or scroll to the bottom of the form to add a new Event Map.
 - a. **Column 1 - Message** - This is the incoming raw event seen in the "key" part of the alarm within the signal.
 - b. **Column 2 - Decode Qualifier** - This value is always zero (0) and is required for every Event Map.
 - c. **Column 3 - Event Code** - The event to present to the customer record and operator.
 - d. **Column 4 - Description** - If the Event code description is fine, there is NO need to enter a description in this column. When a value is here it will override the standard alarm description.
 - e. **Column 5 - Attributes** - Options are U, for User, and S, for Special IR Fast.
 - i. User notifies the Signal Handler that the event is a User event and changes the zone number to a User number.
 - ii. Special for IR Fast is used in countries utilizing IR Fast and the enhanced delivery of Ademco Contact.
 - f. **Column 6 - Comment** - This information does NOT show to an operator during the alarm handling process. This is simply information that is only available within this form.

Event Maps					
Protocol Format: <input type="text" value="Ademco Contact ID"/>					
Device: <input type="text"/>					
Message	Decode Qualifier	Event Code	Description	Attributes	Comment
P576	0	R56	Access Zone Shunt	U	
P577	0	R57	Access Pt Bypass	U	
P578	0	R58	Zone Bypass (Pres)	U	
P579	0	R59	Zone Bypass (Pres)	U	
P601	0	TR	Manual Test		
P602	0	TE2	Periodic Test		
P603	0	TE3	Periodic Test RF		
P604	0	TE4	Fire Test		
P605	0	TE5	Fire Walk Test		
P606	0	TE6	Listen In to Follow		
P607	0	TE7	Walk Test Inside		
P608	0	TE8	Test w/Inside		
P609	0	TE9	Listen/Video/Whistle		
P623	0	R53			
P901	0	S	Download End		
P913	0	S	Spwr Pt Test End	U	
P914	0	S	Holdup Test End	U	
P915	0	S	Big Test Print End		
P916	0	S	Spwr Test Print End		
P917	0	S	Big Disp End		
P918	0	S	Fire Disp End		
P919	0	S	Unrpted Disp End		
P920	0	C	Chung w/Whistle		
P922	0	R	Suppr Pt Alarm Pleasr		
P924	0	R	Suppr Pt Trouble Plst		
P925	0	R	Holdup Pt Bypass Plst		
P926	0	R	A/C Fail for 4 hrs		
P927	0	R	Output Tr Pleasr		

5. Make all changes necessary.
6. Click Save.

The above instructions are for the Monitoring Company 90% rules. But what if a Dealer has programmed an Event different than the standard, or the Dealer installed a bad code into the panel? Manitou allows the ability to configure Dealer specific Event Maps. To override an Event Map by a dealer:

1. Navigate to the Event Maps form.
2. Click Edit.
3. Select the Event Map to adjust.
4. Enter or Select the Dealer within the Dealer section.
5. Enter the event code(s) requiring adjustment and make the necessary changes.
6. Save the record.

Event Maps						
 Protocol Format: <input type="text" value="Ademco Contact ID"/>						
Dealer: <input type="text" value="SSS"/> Security System Service						
Event Maps						
	Message	Decode Qualifier	Event Code	Description	Attributes	Comment
	E122	0	BT	Silent Trouble		
	E13E	0	BA <input type="text"/>			
	*					

These dealer overrides override the default event map as it is more specific. *Please note that it is possible to program customer and transmitter programming to override all event maps by using a # sign. Raw event programming does effect some of Manitou's ability to automate processes.*

Bold recommends a thorough review of all applicable Event Maps on an annual basis to ensure all elements are as desired and to update any new mapping.

Event Categories

Event Categories help set standards for processing events. They also allow the grouping of events based on their category for reporting purposes. Event Categories group together Event Codes for reporting and disaster preparation.

The Event Categories form sets standards for the events housed within them.

The screenshot shows a software interface for configuring Event Categories. The interface includes a menu bar (View, New, Edit, Delete, Save) and a list of event categories on the left. The main configuration area is for the 'BTRB' category, with fields for Description, Monitoring Group, Analysis Code, Default Action Pattern, Default Suspend Time, and Default help for Event Category. There are also checkboxes for 'Operator cancel from queue allowed' and 'Allow close if no actions defined'. Below these are sections for 'Soft Command' (Client Processing, Signal Processing) and 'Disaster Mode' (Disaster Mode Type, Suspend Time, Priority Offset).

- **Event Category** - defines the code to apply to event codes that should reside within the category.
- **Description** - is a clear definition of what the category should hold.
- **Monitoring group** - allows all signals within that Event Category to route to a Monitoring group other than the standard group, when applicable.
- **Analysis Code** - is rarely used but can be used to define resolution standards.
- **Default Action Pattern** - defines the action pattern to use when no action pattern is found any place else. This is most often left blank. When an alarm reaches an operator without an Action Pattern, something went wrong that needs review.
- **Default Suspend Time** - helps speed the suspension of alarms within the alarm handling process by setting a general standard by category. If left at the default the setting is defaulted to 1 minute.
- **Default help for Event Category** - is an instruction that is true for EVERY event within this Event Category. Only update this information if you wish to have this comment deliver to an operator on every alarming event for that category. Remember, the average attention span is less than 8 seconds for most. The more people have to read and comprehend, the more mistakes are made.
- **Operator Cancel from Queue Allowed** - enables the bulk canceling of events from within the Alarm Queue if their priority is between 5 and 99 and within this event category.
- **Allow close if no actions defined** - would allow the Virtual Operator to close an alarm if there is no Action Pattern assigned or the action pattern has no actionable items. The challenge with this is that an event could go unnoticed due to a bad action pattern.
- **Soft Commands** - add some global settings to the event category. These are most often configured within the individual event codes.
 - **Client Processing** - sets the global reporting flags.
 - **Signal Processing** - sets the attributes that would be true for ALL events within the category.

- **Disaster Mode** - sets the "when all else fails" standards when a customer's events are actively participating in Disaster Mode.
 - **Disaster Mode Type** - flags any events, for customers within an Disaster Mode area, as being a part of Disaster Mode.
 - **Auto-Log** - takes any event, for customers within a Disaster Mode area, and logs the event to history and doesn't present alarms to operators.
 - **Ignore** - ignores Disaster Mode completely.
- **Suspend time (seconds)** - determines how long an event, within the category for customers located within the Disaster Mode area, delays suspended in the alarm queue before releasing for an operator. This is rarely used but can be useful when dealing with very full alarm queues.
- **Priority Offset** - is one of the most useful tools for Disaster Mode as it can lower the priority of Disaster Mode area events so that events outside of the Disaster Mode area get handled first.

To add an Event Category:

1. Navigate to the Event Categories form. (SWS > Maintenance Menu > Events > Event Categories)
2. Click Edit.
3. Click Add.
4. Give the Event Category an simple code. There is a maximum of 20 characters allowed.
5. Enter a clear description of the category and click OK.
6. Complete all applicable fields.
7. Save the record.

The newly created Category does not contain any event codes. The next section discusses how to tie Event Codes to Event Categories.

Event Codes

Event codes are the most specific element of this chapter. Event codes are what present to Operators in the event of an alarm or log to history.

The left-hand side of the form houses all the Manitou Event codes. There are some very basic rules that define each type of Event Code listed in Manitou:

- Event codes starting with a % (percent sign) are, in general, generated from the Receiver itself.
- Event codes starting with an * (asterisk) are, in general, generated by a process within Manitou. For example, the Overdue Checker tells the signal handler that an account has not tested in its prescribed period of time, then the Signal Handler generates a *LT event for a Late to Test. *Systems converted from another software package may see * events in their converted data. These are used when there is not enough information in the conversion data to determine a more specific event code.*
- **SIA-like Event** codes are generated by event maps or signal translations within customer or transmitter type programming.

The Event Codes form contains all the possible configuration details necessary to present a quality event to an operator or customer activity log:

- **Event Code** - is the event abbreviation that defines the event.
- The **Description** - is a 27 character more detailed definition of the event.
- Every event must fall within an Event Category. This field determines where to look for the category default settings.
- **Zone State code** - is a rarely used feature that simplifies the event to an alarm, restore, trouble, etc... This is rarely used because sites tend to be much more specific to meet customer and dealer needs.
- **Alarm** - has four options: Yes, alarm to deliver to an operator, No, not an alarm, Residential, the event is only an alarm for an operator if the customer record is residential, and Commercial/Other, the event is only an alarm if the customer record is not residential.
- **Priority** - is set for every event, alarming or not, to establish where the event should fall within the alarm queue, should it ever be an alarm. Remember there are 99 priorities to use within Manitou.

- **Default Action Pattern** - too should be defined for every event code, even if it is, by default, not an alarm. This ensures operators have some sorts of instructions to follow in the event it ends up an alarm at some point.
- **Generic Signal Instructions** - should only be added when the information is 100% required every time the alarm trips to an operator.
- **Transmitter Programming Commands** - allows the ability to configure items like, CanCancel, on the event codes, as opposed to having to program them on the Transmitter Type or Customer programming.
- **Signal Processing Attributes** - empower event codes based on the company, dealer, or customer needs.
- **Customer Attributes** - refer to grouping events for Reporting purposes.

- **Seconds before new/viewed/actioned alarms change to...** - establishes time periods before changing the age of an alarm from new, to aging, to old. The default settings for most events are 60 to 90 seconds and then 90 to 180 seconds. Bold strongly encourages a complete review of all event codes to ensure the non-emergent alarms aren't aging at the same rate. The difference between new/viewed and actioned alarms is when an event is new and viewed, no contacts or dispatches are done yet. Actioned means at least one contact action was completed. Those times, in general should be a bit longer than the new/viewed events.
- **Alarm Color** - establishes custom colors for viewing alarms in the queue, when the option setting is by event, and while handling alarms. Bold, also, strongly encourages the review of all colors and establishing standards for all types of events. The default color is Red with White text and this may be the same color as a high priority fire alarm which can cause operator confusion.
- **Disaster Mode** - overrides what is on the Event Category. When the Type is set to Default the event code looks to the Event Category for its rules. The other types are the same as defined within the Event Categories.

To create an Event Code:

1. Navigate to the Event code form. (SWS > Maintenance Menu > Events > Event Codes)
2. Click Edit.
3. Click Add.
4. Enter an Event Code and Description then click OK.
5. Select and Enter the appropriate information. Required fields are:
 - a. Event Category.
 - b. Alarm - Yes/No/Res/Comm
 - c. Priority
 - d. Warning Levels
6. Be careful to set the Default Action Pattern, any applicable Signal Processing attributes, and the Alarm Colors.
7. Click Save.

Watchdog Messages

Ensuring the Right Messages to the Right People

Introduction

This chapter details the many Watchdog Messages and suggested settings.

What are Watchdog Messages?

Watchdog messages are configured messages generated by Manitou to provide detailed warnings about how things are running within Manitou.

Watchdog Message Definitions

This section details all the individual messages housed on the Watchdog messages form:

- **10001** Process %1 on %2 is Not Detected on the System! - Notifies users of a process like the Signal Handler, Fep, Overdue Checker, etc.. that is no longer communicating with the Manitou system.
- **10002** No activity for '%1' of priority %2 for monitoring group %3 being handled by %4! - Notifies the users that a signal being handled by an operator has stopped progressing.
- **10003** FEP Limit Exceeded, attempt to add FEP %1 denied. - When adding a FEP to a receiver configuration, if the system is not licensed, this message generates.
- **10004** FEP %1 on %2 Keepalive Timeout! Connection problem with the Marshaller. - When the Marshaller and the Signal Handler cannot maintain contact with each other the Marshaller generates a Watchdog message to draw someone's attention.
- **10005** FEP %1 on %2 Lost Connection with the Marshaller. - When the Marshaller and the FEP cannot maintain contact with each other the Marshaller generates a Watchdog message to draw someone's attention.
- **10007** No One Handling Alarms in Monitoring Group %1. - If a site uses Monitoring Groups and there should be someone in each Monitoring group at all times, the Watchdog generates this warning to draw attention to the issue.
- **10014** %1 is Out-of-Sync with the Broker. - When services running on Manitou get out of sync with the Broker, there could be data corruption or failure.
- **10015** No Default Customer (%1:%2), Processing Complete, Signal Not Processed. - Each receiver should have a Default System account to have a "home" for orphaned signals. When this is not the case, the system generates this warning to notify of the failure to process an event.
- **10016** Signal Arrived For %1 Customer (%2), Signal Not Processed. - When an account is deactivated, the Signal Handler no longer processes those signals into an account. This warning generates when the global option to do so is set to No.
- **10017** Late-To Customer (Serial No. %1), Not Found, Signal Not Processed. - There are times when a customer is removed but the Overdue Checker still has a timer. This generally only happens on items deleted from the database as opposed to through the front-end.
- **10018** Serious Error, 'Unknown Event Code' (%1), Default Event Definition Used. - This is a rarely generated warning as Manitou will most often deliver an unknown (**) event to an operator when no

event code is found within the driver or event maps.

- **10019** No Overdue Checker/Delivery thread detected on the System! Late-To's and internally delayed signals will not be processed! - When the Overdue Checker fails to connect late and pending removal items are not generated. That means if an account was placed On Test for an hour, and the Overdue Checker is not running the account will not return to service as expected after the hour period expires.
- **10020** Failed to restart process %1 on %2! - Manitou attempts to automatically restart services, that exit, three times. When it cannot successfully restart a Manitou service it generates this Watchdog message.
- **10022** Remaining Customer Limit is %1. - This provides a warning that the number of customers, active and inactive, is approaching your licensed limit.
- **10023** Maximum Number of %1 Exceeded. - This is a license warning and identifies what item violated its license.
- **10024** Signal Not Processed! Enter Manually (%1). - This is a very serious error. If the Signal Handler was unable to process a signal there may be a bigger issue involved. In general, one warning is not too much of a concern but if this happens multiple times in a short period there is cause for concern.
- **10025** Process %1 on %2 has exited! - This warning could be serious or may just require a restart of the service/process within the MSM.
- **10026** (Non-Manitou) Process %1 on %2 has exited! - This message is related to non- Manitou processes watched by the MSM.
- **10027** The Broker lost its connection to the Bold Monitor service. - The Bold Monitor Service is how the different servers connect to one another. It is not possible to launch the MSM without the Bold Monitor service.
- **10028** Database Commit failure from Signal Handler! One or more signals may be lost! RawId: %1 - This is a serious notification. If signals are not processing into Manitou properly, losses can occur.
- **10029** Various messages from the DB Manager
- **10030** DB instance %1 has failed! - When a database instance fails, data loss or corruption may occur.
- **10031** No secondary DB instances are available - failover to secondary DB unavailable - Most often this relates to High Availability configurations. If the secondary instance is not available, it won't be possible to failover in an emergency.
- **10032** Primary DB auto fail over to %1! - This is a notification of an automatic failover when a site is configured for High Availability.
- **10033** Various messages from the Event Centre
- **10034** The system clock has been changed! Alarm handling and other timeouts could be affected!
- **10035** Alarm Progress Problem for '%1' of priority %2! - This is an operational message notifying all logged in users that alarms are not progressing. Setting the Warning and Danger levels within the Event Codes are very important if attempting to utilize this feature with alarms.
- **10036** Potential Signal Processing Problem (%1). - This is a good warning but doesn't constitute an emergency if you check the FEP Commander and the Raw Data log and signals are still processing into Manitou.
- **10037** No Signal Handling threads detected on the System! Signals will not be processed! - This is an emergent warning. If signals cannot get into Manitou, your site is "down." At times, this only needs a simple restart of the Signal Handler to refresh the information.

- **10038** User %1 has exceeded %2 login failure limit of %3 failures in a session from IP address %4. Possible hack attempt. - This warning is most often generated by an operator's repeated attempts to log into Manitou and failing to enter the correct user ID and password combination.
- **10039** Access Control Synchronization Failure (Serial No. %1). - If your site has an integrated Access Control System, this warning identifies a possible issue when attempting to sync between the access control system and Manitou.
- **10040** License violation. FEP %1 receivers list reduced by %2 due to insufficient licensing. - The Broker notifies the user and generates a warning when someone attempts to configure more Front End Processors than their license allows.
- **10041** FEP %1 at IP Address %2 %3. It is attempting to connect to the Marshaller. - This issue often generates when a server has a dual NIC card and the second IP Address is not documented for the server inside Manitou. All Manitou servers are required to have static IP addresses to prevent reboots causing signaling failures.
- **10042** Failed to update Alarm Counts (Serial No. %1). - This can be a serious message if the alarm counts are failing to update, this could be indicative of an issue with the database or the services running Manitou.
- **10044** Failed to insert Alarm Activity (Serial No. %1, LSeqNo %2). - If the system cannot write to the customer logs this could be due to a missing or corrupt table. This, most often, requires Support assistance.
- **10045** Maximum retry count for creating recurring reached (Serial No. %1). - This relates to the Dealer Billing module for generating recurring items based on the Dealer settings.
- **10046** Failed to create recurring (Serial No. %1). - This, too, relates to the Dealer Billing module and the recurring creation based on Dealer settings.
- **10047** Signal Handler failed to activate customer [%1] - When set, the automatic settings, from within the Options form, should enable a new account based on those rules. If the Signal Handler encounters an error, this warning generates.
- **10048** Reminder Customer (Serial No. %1), Not Found, Signal Not Processed. - If for some reason a customer record doesn't clean up properly some items like Reminders can be orphaned within the database. If this occurs and the reminder attempts to create the event, this warning points toward the failure.
- **10050** Failed to load alarm %1 with Broker - This could be a minor issue or something more serious. Alarm Operators receive the "Broker failed to allocate an alarm" and that is most often because they are trying to click a line of an alarm still closing out as someone has completed it or has it in their possession. This is potentially more serious.
- **10051** %1 Signal Handler Threads on machine %2 not able to get a working DB resource. - This can be a serious issue if all the Signal Handling threads cannot get a database resource to allow processing.
- **10052** Multiple Listen-In sections found, subsequent section ignored [%1:%2:%3]. - This is a warning that, possibly, multiple people are attempting to handle events on a single customer with audio.
- **10053** Caller Id Customer (Serial No. %1), Not Found, Signal Not Processed. - This rarely generated message indicates that the caller ID was not found on the customer record and the Signal Handler stopped processing it. It is a good idea to see what may have caused this.
- **10054** Binary Data Customer (Serial No. %1), Not Found, Signal Not Processed. - This rarely generated message indicates that the customer record for the Binary data was not found on the customer record

and the Signal Handler stopped processing it.

- **10055** Listen-In Customer (Serial No. %1), Not Found, Signal Not Processed. - This rarely generated message indicates that the customer record for the listen-in data was not found on the customer record and the Signal Handler stopped processing it.
- **10056** Sub-Account Customer (Serial No. %1), Not Found, Signal Not Processed. - This rarely generated message indicates that the customer record for the Sub-account was not found on the customer record and the Signal Handler stopped processing it.
- **10057** No active System Account customer could be found to process expired Follow- up signal. - This is generated when the receiver doesn't have a default account related to it in order to process an expired Follow Up (related to the Temporary Comments).
- **10058** Signal Arrived For %1 Customer (%2), Signal Not Processed. - This is most commonly triggered when a deactivated customer still has a Receiver Line Prefix and Transmitter ID tied to it and the panel out in the field is still signaling.
- **10059** Broker SimpleCall Exception (%1 - Params: %2) Exception Error: %3 - %4 - %5
- **10099** Publishing of '%1' report (%2) failed. - This is an excellent warning to notify supervisors and monitoring center leadership. This may indicate an issue with the publisher or the outgoing pathway.

Now that you know a bit more about the messages themselves, next let's review the possible settings.

Configuring Watchdog Messages

Each message may be configured to either pop-up, scroll on the watchdog message bar, or generate an alarm.

Pop-up

Pop-up displays a dialog to the logged in users for the selected groups. This should be for mission-critical items like Processes not detected, signaling issues, etc. The best part of the Pop-up feature is the tracking of the presentation of the warning and the acknowledgment by the operator.

The screenshot shows the 'Event Codes' configuration window. On the left is a list of event codes, with 'BT - Burglary Trouble' selected. The right pane shows the configuration for this code:

- Event Code: BT
- Description: Burglary Trouble
- Event Category: Burg troubles
- Zone State Code: (empty)
- Alarm: Yes
- Priority: 4
- Default Action Pattern: Burg
- Generic Signal Instructions: (empty)
- Transmitter Prog. Commands: (empty)
- Signal Processing Attributes: X
- Customer Attributes: B
- Seconds before new/viewed alarm changes to: (empty)
- Warning Level: 90
- Danger Level: 180
- Alarm Color: (blue button)
- Foreground: (white box)
- Background: (blue box)
- Disaster Mode: (empty)
- Disaster Mode Type: Default
- Suspend Time: 0 seconds
- Priority: 4

Scroll bar

The scroll bar option is most often used for non-mission- critical issues that simply require notification to those logged in.

Alarm

Alarm is the most flexible choice as each Type code is considered the "zone" number for configuring what actions to take when the issue presents to an operator. The events are programmed within the SYS-REC1 account and can have any number of events translated tied to any action patterns necessary. Not all events have a restore. When they are not available the drop down disables.

User Groups

Each Watchdog message may be configured for all or only specific user groups. Checking the box for the groups that need to see the message determines who see the messages, when set to Pop-up or Scroll.

We strongly encourage your site reviews each of these messages and determine who should receive the messages and how.

Configuring Watchdog Alarms

When your business practices call for a Watchdog Message to alarm, they may be configured within the Manitou Operator Workstation to generate an alarm with any appropriate action pattern necessary. For this example we set the 10019 "No Overdue Checker/Delivery thread detected on the System!" message to alarm. As noted before, the 10019 equates to the zone number and the configuration occurs within the SYS-REC1 customer record. Message 10019 has an alarm and a restore. The choices are System Alarm (*Z) and System Restore (*Y). Once configured within the Supervisor Workstation to Alarm then it is possible to program the event within the Operator Workstation SYS-REC1 customer record.

Watchdog Message Types

Type Code: 10001

Description: Process %1 on %2 is Not Detected on the System!

Alert Type: Pop-Up

User Groups:

- System
- Administrator
- Supervisor
- Operator
- Data Entry
- Trainee
- Dealer

Event Code: []

Restore Code: []

To add a programming translation to a Watchdog event, do the following:

1. Open the Manitou Operator Workstation.
2. Navigate to the SYS-REC1 customer record.



3. Navigate to the Systems and Programming.
4. Click Edit.
5. Enter a new line with the DES column filled in with a *Z event code.
6. Tab to the zone column and enter the Watchdog number.
7. Tab to the Event column and select the event to present to the account and operator. In this example, we created a new event code called WDOG.
8. If necessary, enter a line into the Event Actions programming to override the default action pattern with a new action pattern appropriate for this event.
9. Click Save.

Once configured, when the Watchdog issue triggers, a new alarm generates and provides the operator, or Virtual Operator, with the applicable Action Pattern.

Troubleshooting in Manitou

Where to look to find your answers

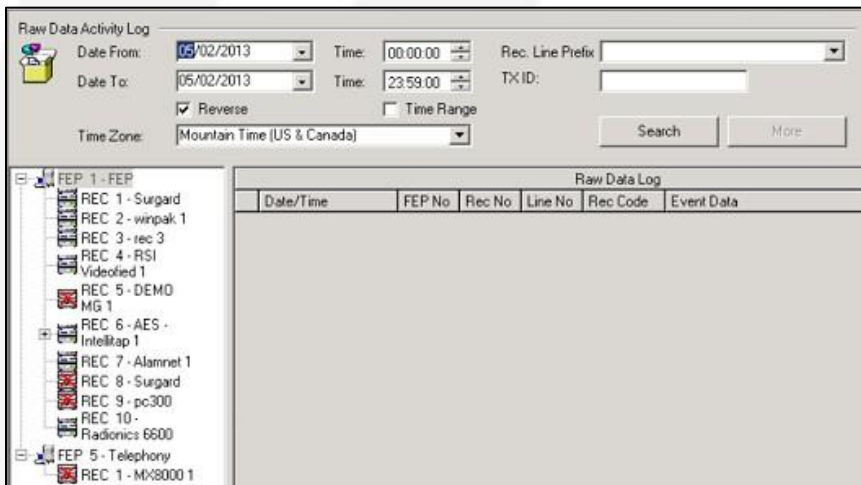
When issues arise where do you go to figure out what happened?

Introduction

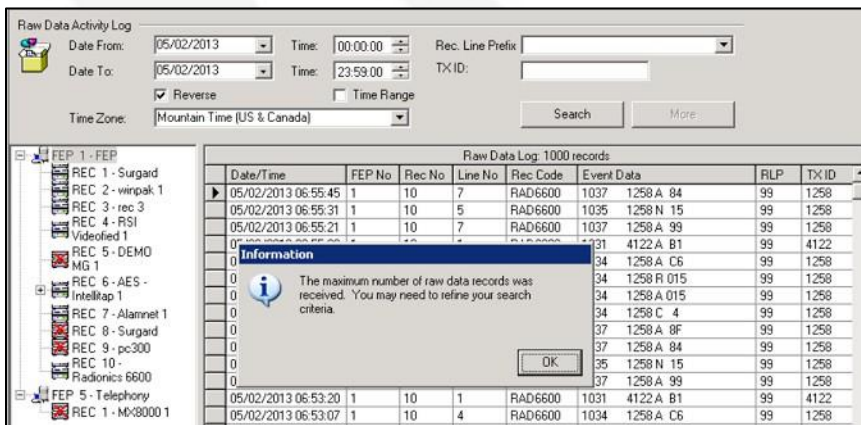
This chapter introduces the troubleshooting features found within Manitou to help troubleshoot when things don't go as expected. There are four key features found in the Supervisor Workstation that help narrow down issues: Raw Data Log, System Application Log, System Log, and Audit Trail

Raw Data Log

The Raw Data Log houses all signals processed into Manitou. The Raw Data Log contains three portions: filtering options, The FEP list, and the results pane.



To load results, select the active FEP, or the receiver on the active FEP, then click Search. There are times, when the result set is too large. If this is the case, the maximum number records warning displays. The default time settings are the current day from midnight to midnight. It is possible to search for individual transmitter IDs or a combination of receiver line prefix and transmitter ID to narrow down the results.



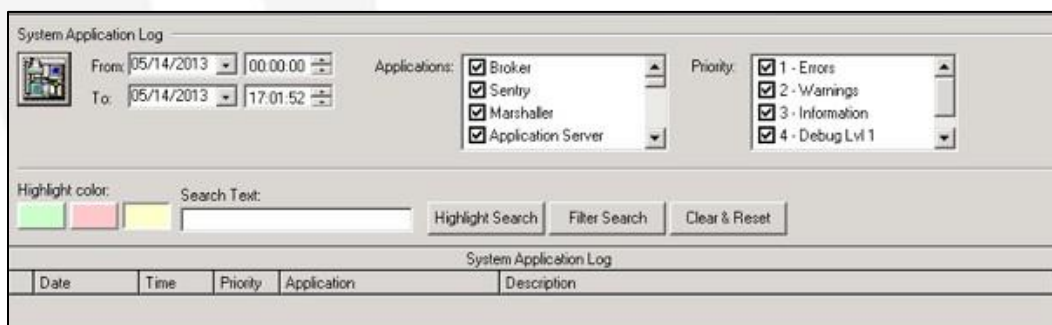
The log details show the date/time, FEP number, Receiver number, the physical line card (when applicable), the code the receiver is using to decode the event, the event data and the receiver line prefix and the transmitter ID. These results show the raw signal as it passed into the system and handed off to the Signal Handler.

Raw Data Log: 1000 records									
Date/Time	FEP No	Rec No	Line No	Rec Code	Event Data			R/LP	Tx ID
05/02/2013 06:55:45	1	10	7	RAD6600	1037	1258 A	84	99	1258
05/02/2013 06:55:31	1	10	5	RAD6600	1035	1258 N	15	99	1258
05/02/2013 06:55:21	1	10	7	RAD6600	1037	1258 A	99	99	1258
05/02/2013 06:55:08	1	10	1	RAD6600	1031	4122 A	B1	99	4122
05/02/2013 06:54:56	1	10	4	RAD6600	1034	1258 A	C6	99	1258
05/02/2013 06:54:44	1	10	4	RAD6600	1034	1258 R	015	99	1258
05/02/2013 06:54:32	1	10	4	RAD6600	1034	1258 A	015	99	1258
05/02/2013 06:54:19	1	10	4	RAD6600	1034	1258 C	4	99	1258
05/02/2013 06:54:09	1	10	7	RAD6600	1037	1258 A	8F	99	1258
05/02/2013 06:53:56	1	10	7	RAD6600	1037	1258 A	84	99	1258
05/02/2013 06:53:44	1	10	5	RAD6600	1035	1258 N	15	99	1258
05/02/2013 06:53:32	1	10	7	RAD6600	1037	1258 A	99	99	1258
05/02/2013 06:53:20	1	10	1	RAD6600	1031	4122 A	B1	99	4122
05/02/2013 06:53:07	1	10	4	RAD6600	1034	1258 A	C6	99	1258
05/02/2013 06:52:56	1	10	4	RAD6600	1034	1258 R	015	99	1258
05/02/2013 06:52:44	1	10	4	RAD6600	1034	1258 A	015	99	1258
05/02/2013 06:52:32	1	10	4	RAD6600	1034	1258 C	4	99	1258

If the signal you're seeking is not showing here, there is one last place to look for the event called the Receiver (or FEP) DEBUG file. This is found on the active server running the FEP. The FEP Debug files are found, usually, on the c or d drive in a folder called FEPFILES. It is safest to copy the file elsewhere then open it with NOTEPAD. If the FEP DEBUG file doesn't contain the missing alarm, it was not acknowledge by the FEP and not processed into Manitou.

System Application Log

Found only within the Supervisor Workstation, the System Application Log presents data collected by the Logger and displays it based on the parameters selected. The Log Viewer found on the Manitou servers too displays the Logger details but cannot be searched or filtered.



The default view is the current day from midnight to the current time when the form loads. This log is also limited to a maximum 1000 lines so filtering is important. The filter features for collecting results are:

- From/To date and time - If looking at all services, this can be reduced to a single minute in time.
- Applications - These allow the removal of Manitou services that do not apply to your search needs at the time. When right-clicked the select none and select all are available. Select or de-select the appropriate services as needed.
- Priority - is often left with all the boxes selected as this sort of search is used to find details that did not generate an error within Manitou.

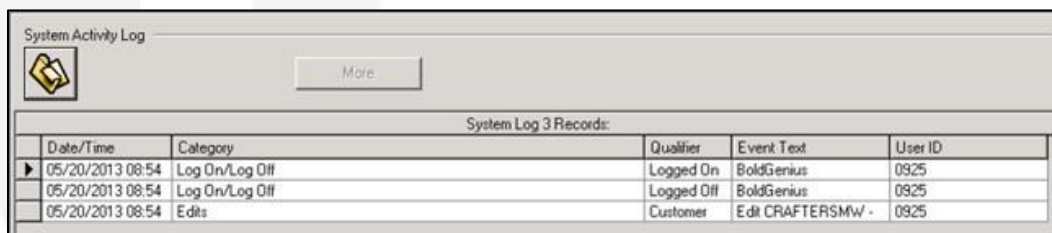
Once the log populates with results the second section of filtering allows for the entry of a specific text string like "error" or "failed" and then you may either highlight the items with that string or filter it. Clear and reset clears the text sting and returns you back to the original results.

System Log

The System Log, found within the Manitou Operator and Supervisor Workstations under the Tools Menu, is used to track nearly all actions take within Manitou. These include:

- Log on/off into and out of Manitou.
- Report server successes and failures.
- Publisher successes and failures.
- Watchdog messages generated and acknowledged.
- Edits made to any records.
- Report Scheduling items.
- User Messages typed into the IM feature.
- Entry and exit into and out of Alarm Handling Mode.
- Reverse commands triggered.
- Miscellaneous items, such as Manual Signals created by users.
- PBX Assistant items.

The default view is today from midnight to current time. The button, located on the top left- hand side of the form is a refresh/reload button. You may also press F5 on your keyboard to do the same. The More button enables when the number of lines loaded exceeds 1000. This allows you to load more as you need.



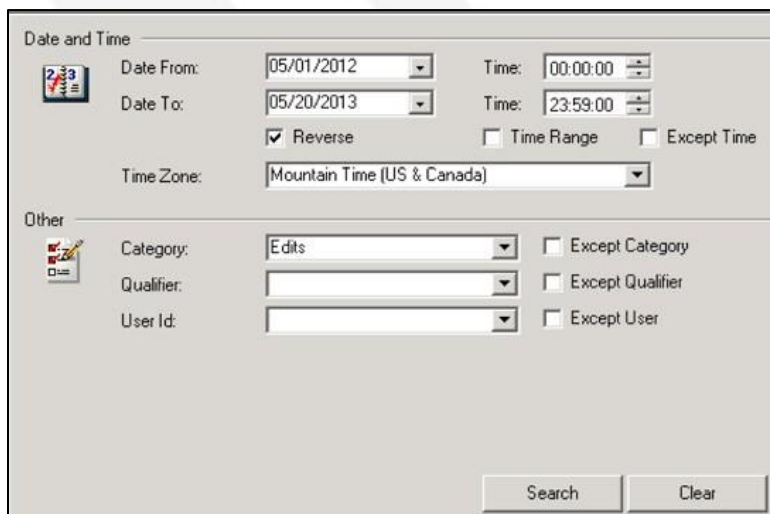
System Activity Log

More

System Log 3 Records:

Date/Time	Category	Qualifier	Event Text	User ID
05/20/2013 08:54	Log On/Log Off	Logged On	BoldGenius	0925
05/20/2013 08:54	Log On/Log Off	Logged Off	BoldGenius	0925
05/20/2013 08:54	Edits	Customer	Edit CRAFTERSMW -	0925

It is possible to filter the System Log by clicking the Filter tab and setting date/time, and specific filters.



Date and Time

Date From: 05/01/2012 Time: 00:00:00

Date To: 05/20/2013 Time: 23:59:00

Reverse Time Range Except Time

Time Zone: Mountain Time (US & Canada)

Other

Category: Edits Except Category

Qualifier: Except Qualifier

User Id: Except User

Search Clear

Like the System Application Log, the date/time filters also contain the ability to change the sort direction from oldest to newest or newest to oldest. Time Range allows the selection of multiple dates with a specific time period only. The except time allows the opposite. It looks for all items that do NOT include that time range.

The Other section allows the select of the many different categories above, one at a time, as well as selecting an item to except (exclude) from the results. Some Categories have additional qualifiers to further filter the results and if one is looking for actions taken only by a single user, they may be selected from the User ID field.

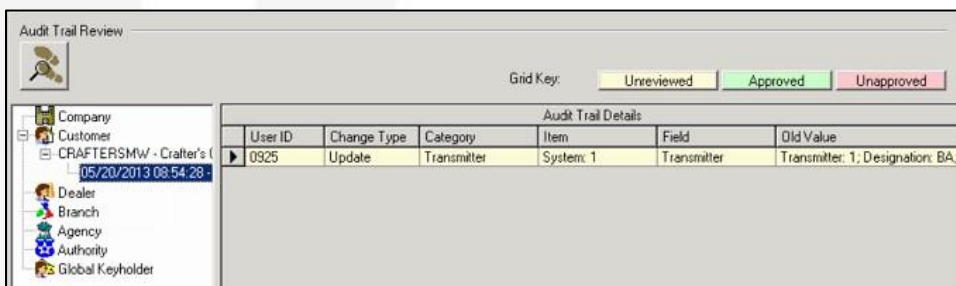
After receiving results, double clicking a log line reveals more details when applicable. For example, if an operator selects an edit line and double clicks it, information from the Audit trail load.

Audit Trail Log

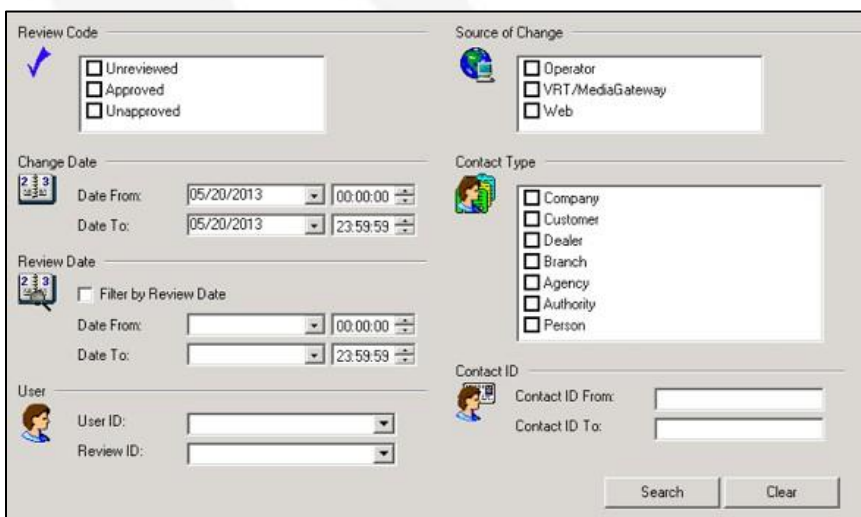
The Audit Trail log, found in both the Manitou Operator and Supervisor Workstation, tracks all changes made to all entities managed within the Manitou Operator Workstation. These include:

- Customer
- Dealer
- Authority
- Global Keyholder
- Monitoring Company
- Branch
- Agency

The Audit Trail default view loads blank but highlights the entity types changed within this 24 hour period of midnight to current time. Sections with a plus sign may be expanded to reveal the individual audit trail records.



It is also possible to filter the Audit trail for other dates and times as well as from what sources, such as from the BoldNet (Web) interface.



The audit trail contains the "what" happened to a customer, or other entity, record, but the "why" something changed must come from the notes operators add when saving records.



Other Supervisor Workstation Features

What else can Manitou do?

Previous chapters covered how to manage the most common areas within the Manitou Supervisor Workstation. But what about Script Messages, Control Panels, Transmitter Protocol Types, and the many other features?

Introduction

This chapter introduces several other Manitou Supervisor Workstation elements. These features often support other elements of the Manitou system and may be visited only a few times a year.

Script Messages

Many options covered in this course reference Script Messages. But what are they and what do they do? Script Messages, found under the Maintenance menu, allow Manitou to automatically populate current details from an alarm or customer record and send a detailed message to a customer via email, text, or even fax. Creating the Script Messages within the Supervisor workstation creates a global standard that should work for 80 to 95% of messages of that type.



Monitoring Types

The Monitoring types form, found under the Maintenance Menu > Setup > Monitoring Types, is used to create the services that may be billable items to a monitoring company's customers. Manitou delivers a number of default Monitoring types for the most common services. Monitoring Types automatically load into a customer record's services based on the data entry completed. For example, if a customer has a daily test required on their account, as soon as an operator enters 1 day into the Transmitter Test field, the service automatically populates onto the customer record. Some centers connect their Manitou system with an integrated accounting package. If this is the case and billable items have specific codes within the accounting package, this may be configured on the matching services (monitoring type) within the Manitou Supervisor Workstation.

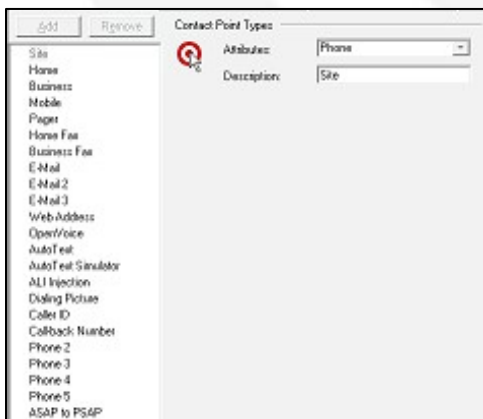


Control Panels

Many monitoring companies use Control Panels to identify what equipment resides at a customer location. The Control Panel form is found under the Maintenance Menu. These, when created, are available within the Operator Workstation customer records on the Systems form. The Control panel form is quite straight forward, it contains a type, description, comment (often containing disarm/ troubleshooting information), and properties. Properties set maximum allowable items such as the transmitters, areas, zones, and users allowed. When set to unlimited no warnings present when a user attempts to add additional entries for these items within the customer record.

Contact Point Types

Every phone number, email address, pager, web address, and ms text messaging number/details have an assigned Contact Point Type (CPTType). The CPTType, found under the Maintenance Menu > Setup > Contact Point Types, applies specific standards to the different types of contact points. For example, if a site would like to take advantage of our Outbound OpenVoice service, the phone numbers to be called will need to have the property of Retransmission to function properly. Manitou allows as many CPTypes as a site needs. Adding new CPTypes is simple. Edit the form, click Add, Select the attribute from the list, enter a description, and save.



Subtypes

The Subtypes form contains labels for nearly all features in Manitou, that are allowed to be configured. The Subtype categories are:



- **Agency Types** - Companies with access to customer records for things like guarding, janitorial, regional management, etc.
- **Customer Premises Types** - Type of building the premises represents, such as Residential and Commercial.
- **Dealer Types** - Service companies that install and service alarm systems for end customers.
- **Keyholder Types** - Individuals with access to a property or number of properties. Contact is a person with a phone number, Keyholder is a person who may respond to the alarm, often with a password to cancel alarms, etc...
- **Name Suffixes and Person Titles** - If customers have suffixes, or person titles like Dr., that are outside of what is provide by default it is possible to add more.
- **Reverse Command Types** - this is rarely updated by end monitoring companies but are used to configure standards for items that use Reverse Commands to go from Manitou out to equipment residing in a customer's site.
- **UL Grades** - also ULC lists the grades used to define the different levels of UL monitoring a site may offer. The defaults listed within Manitou are simply placeholders and can be edited if needed.
- **Client Application Types** - define the different pathways end users take to access Manitou and the data held within.
- **Workflow Component Categories** - a listing of the categories used for those with the Workflow functionality deployed. *Please note this feature is going to be replaced by Enhanced Action Patterns within the Manitou NEO version.*
- **Action Pattern Categories** - when created, allow the ability to sort action patterns into groups for ease of use and data maintenance.
- **Maintenance Service Types** - is used to determine what level of service a customer may need when the record has a Maintenance Issue pending. Some examples of these would be: Battery Replacement, Annual Fire Inspection, etc...

Existing Subtypes may be edited to match a company's vocabulary. *Please note any Subtype with a number less than 100 may not be removed as it is part of the installed standards.*

Workstations

The Workstations form is where any newly installed workstation, running Manitou, must be authorized to allow access into Manitou. When there is a new workstation available the line shows in green in the Workstation table. When authorizing a workstation there are a few choices:

- **Unapproved** - This workstation is not allowed to access Manitou.
- **Non-protected Area** - This workstation resides outside of the secured area (monitoring center) therefore cannot have access to alarm handling features.
- **Protected Area** - This workstation resides within the secured area and has access to Alarm Handling features.
- **Disabled** - This workstation is no longer accessing Manitou.

Disabled workstations are often just removed from the Workstations table. To remove a Workstation simply load the form and in Edit mode click the line to remove and press the Delete key on your keyboard. We do recommend removing workstation records when a workstation is taken out of commission or re-imaged with a new name. When the record remains and you attempt to authorize the new workstation an error occurs.

User Status

The User Status form, found under the View Menu within the Supervisor Workstation allows supervisors to view and interact with each operator's workstation session.

The screenshot shows the 'User Status' form. At the top, there are buttons for 'Not Handling Alarms', 'Manual Alarm Handler', 'Paused Alarm Handler', and 'Auto Get Alarm Handler'. Below this is a table with columns: User, Session ID, Alarm Handler, Computer, Workstation Description, Client Type, Security Level, and Extension. Two sessions are listed: Session ID 661 (No Alarm Handler, Pending Workstation, Supervisor Workstation, Protected Area) and Session ID 666 (Yes Alarm Handler, Pending Workstation, Manitou CS Client, Protected Area). Below the table is a 'Session Details' section for session 666, showing 'Logon time: 9/7/16 11:01:48'. The 'Alarm Mode' section includes 'Currently handling alarm' (set to No), 'Paused' (set to No), and 'Select mode' (set to Manual). The 'Alarms Handled' section shows a grid of input fields for Total and Per hour counts across 10 priority levels (Priority 1 to Priority 10), all currently set to 0. The 'Customers' section includes fields for Edited (2), Added (0), Deleted (0), and On Test (0).

When an operator logs into Manitou or the Supervisor Workstation a session adds to the User Status form. Upon selecting a session, details populate below.

The **Session Number** is a unique ID to that user and client login.

The **Date and Time** of the session start is the time the operator logged into the workstation.

Edits made are found within the **Customers** section including customers edited, added, deleted, and placed On Test.

Their alarm handling status shows within the **Alarm Mode** section. If an operator is paused a supervisor can manually un-pause their session and the system will begin to present alarms to the operator again. If an operator is in Manual alarm handling mode and they should be in auto-get it is possible to manually change that as well from this form.

The **Alarms Handled** section details what the operator has managed during their session. This can be a good measurement tool if it appears one operator seems to be handling more high priority alarms than others, supervisors can take immediate action.

Group and Class Codes

Group and Class codes are used to organize customer records for reporting and billing purposes. They get configured within the Supervisor Workstation. These are defined by each individual business practice. See your leadership team for more information on how these are, or are not, utilized within your organization.

Global Holidays

The Global Holidays form, found under the Maintenance Menu, allows the setting and updating of holidays that customers utilize during the year. We strongly encourage reviewing these annually to ensure any holidays that move land on the right day and date each year.

Resolution Codes

After updating the option for resolution code groups, the resolution codes form allows the entry and update of any resolution codes. We encourage annual review of your resolution codes for their effectiveness and clarity. If a code is not used on a single alarm in 2 years, it is no longer useful to keep.

Transmitter Protocol Types

When new types of technologies integrate with Manitou they may require a Transmitter Protocol Type to allow for event mapping the new integrated signals. The Transmitter Protocol Types form is under the Maintenance Menu > Setup > Transmitter Protocol Types. When adding a new type there are some required fields. The Type has to have a unique ID, a clear description, and the appropriate Event Type. Most often, when creating new types, the most common Type selection is Event Type (must be defined in Event Maps). Once created it is possible to see, and select, the new type within the Event Maps form.

Receiver Types

There may be times when a site has multiple receivers and each receiver processes their signals into Manitou differently. This may cause the need to create a new Receiver Type in Manitou. This form is under the Maintenance Menu > Setup > Receiver Types. The form itself allows the selection of the same driver with different parameters. Once this is saved, the new type can be applied to a Receiver.

Report Templates

Manitou has over 80 "canned" reports that catch a large number of customer needs. However, from time to time companies find that they are making the same changes to these reports again and again. Manitou offers Report templates to set these standards on the canned reports, import SnapReporter BSR files, or, if licensed, SQL Reporting services RDL files. To create a report template out of a "canned" report, do the following:

1. Navigate to the Report Templates form under the Reports menu and click edit.
2. Single click the report to template and click Add.
3. Be sure to rename the Report with a descriptive name.
4. Make the appropriate edits.
5. Click Save.
6. Acknowledge the warning, if it presents, about the report running on the entire database.
7. Load the System Reports form and expand the plus sign, and ensure that the new report shows.

Remember the System Reports form must be opened fresh in order to see the new report.

This report is now available to all users to run the report with the default parameters created by your changes.

If a report fails to work, the issue could be related to updates made but not yet refreshed in Manitou. To update the report templates: Edit the Report Templates form, click the Restore Defaults button, then save.



Appendix 1

Vocabulary

Checkbox – Multi-option selector.

Radio Button – Single option selector.

Menu – Listing of forms or choices.

Binary – a representation for numbers using only two digits (usually, 0 and 1)

Customer ID – Account Number

Customer Record – Compilation of forms that make up the data needed to manage alarms for a specific address (customer).

Serial Number – Unique Database assigned record identifier.

Alarm – Event that requires an operator’s attention.

Signal – Event that does not require an operator’s attention.

Transmitter – Also known as: “Dialer,” “Radio,” “GSM,” etc... The piece of equipment that is used to communicate signals to the monitoring station.

Transmitter Type – Set of default data tied to the account/transmitter for signal processing and standard parameters.

Transmitter ID – Account number transmitted from the equipment.

Receiver Line Prefix – Unique identifier to tell the difference between individual receivers and/or lines for appropriate account management.

Transmitter Protocol Type – Optional field listing the type of signals expected from the transmitter.

System – Overarching grouping for the types of signals managed. Event Monitoring, GPS, Access Control and Other are the current System Types. Event Monitoring is standard alarm Monitoring.

Panel Type – Listing of equipment used for the individual system. Contains basic standards of maximum transmitters, areas, zones and the like.

Zone – Physical locations where the alarm events arrive.

Area – Partitions of a panel that contain zones.

Tracking – Keeps alarms from the same account tied to the same operator.

UL/ULC – Underwriters Laboratory.

Sequence Number – Unique number to ensure signals and other data items remain in the proper order.

Resolution Codes – Codes used to identify the cause and reason for an event. Often used for reporting.

Paged Contacts – Those persons where an attempt was made to contact them via a pager, or message left on voicemail.

Pre-Cancel – Ability to cancel an alarm that may not have yet arrived based on customer validation.

On Test – Account, or portions of an account, disabled for testing or maintenance.

Jump To Menu – Customer, or other entity, record right-hand listing of forms.

Front End Processor (FEP) – The service that listens to and acknowledges the receiver.

DNIS (Dialed Number Identification Service) – Number provided to an installer to call the receiver. Based on the dialed number the system routes to specific Receiver Line Prefixes.

Entity – A non-human that has access to a customer record, such as Dealer, Agency, Branch, Authority, Global Keyholder, etc.

Master Customer – A customer record that stands alone by itself or relates to other accounts, often based on proximity.

MediaGateway – Bridge system that allows Manitou receive events from multiple sources.

UniversalConnector – System that allows Manitou to integrate through connectors to things like SMS messaging systems, email accounts, and the like.

Proprietary – A business that monitors themselves. Examples are College campuses, retail chain business, etc...

Full Service – A business that installs, services, and monitors their account base.

3rd Party – A business that offers many installing companies monitoring services.

PSIM (Physical Security Incident Management) – Graphical incident queue alarm management.

Static IP – An Internet Protocol address specifically configured on a workstation or server to permanently define the location of that device.