ENTRÉ

OPERATIONS GUIDE

—

A Guide for Operators

TABLE OF CONTENTS
—

WELCOME TO ENTRÉ

This guide provides operators with a top-notch, intuitive interface where they can:

- Configure hardware and access rights
- Enroll and manage personnel
- Monitor alarms, device status, and system activity
- Search data and generate reports
- Manage security at a granular level

Additionally, Entré is flexible at the hardware level. It offers support for a variety of access control readers and other devices. It also allows for multiple methods of communication to controllers, including network. At the software level, Entré is designed to be flexible and extensible with a modular open architecture.

For more information about the capabilities of Entré, contact your DMP dealer or representative.

System Overview and Requirements

The host PC runs the application and the database. The database contains the hardware configuration, personnel, badge holder, privilege information, and historical information (events).

The server communicates with XR Series and TMSentry Control Panels and downloads information about configuration, badge holders, and user privileges. This allows panels to completely control all points in the system and make intrusion and access control decisions even if communication with the server is down. The server stores these transactions in the Entré database that are displayed in real-time and are available for reporting. The server also processes panel events.

Minimum Software Requirements

Hardware requirements depend on the type and size of your Entré configuration. For complete server architecture recommendations, refer to Entré Server Recommendations (LT-1639).

- Server OS: Windows Server 2016
- Client OS: Windows 10
- Microsoft SQL: All Microsoft Supported SQL Server Operating Systems
- Apache Tomcat 10

Java Requirements

Entré Access and Security Management does not have Java built in and requires users download Java 17 or an OpenJDK 17 alternative.

Panel Compatibility

Entré supports all panel versions but not all panel features. See LT-2233 Entré Compatibility Chart.

Languages

Entré Access and Security Management offers translations for two languages. When multiple languages are enabled, you can choose a language during the login process. A dual-language mode is also available, where all text is shown using both English and the language chosen at login. This mode is useful for technical support and training across linguistic boundaries.

Officially Supported Languages

- English
- Spanish
- Dutch
- French
- German

LEARN ENTRÉ FUNDAMENTALS

Start Entré

When you start Entré, you will see a splash page displaying start-up progress.

When prompted, log in with a valid username and password.

- The system administrator username is: **admin**
- The factory default password is: **pass**

You should change the factory default password after installing Entré. Username and password are case-sensitive.

Valid Login

- **Yes:** Entré displays the start page or the modules that were open during the operator's previous session.
- **No:** An error displays. Repeat the steps above, making sure that the username and password are correct and in the correct case. If problems continue, contact your system administrator. If the system administrator cannot resolve the issue, contact the Entré distributor or system installer.

User Interface

The typical user interface consists of the following components.

- **Window Title Bar:** Shows the module and application name.
- **Toolbar:** Contains a set of button functions that are specific to the module being used.
- **Status Bar:** Appears at the bottom of each module window and is divided into four panes.
    - **Pane 1:** If there are any uncleared alarms, this pane displays a colored or blinking icon showing the alarm status.
    - **Pane 2:** If there are any uncleared alarms, this pane displays text describing the number of alarms, as well as their state.
    - **Pane 3:** Shows the number of items in the table.
    - **Pane 4:** Displays the username of the logged-in operator, as well as the IP address or hostname of the workstation.
- **Table Columns:** Column visibility and order may be edited using the **Columns** button. Column width may be adjusted by dragging the edge of the column header. Selecting a column header will cause the column to be sorted either alphabetically or numerically. Selecting the column header a second time reverses the order.
- **Table:** Shows a list of items. Selecting an item within the table enables the use of certain buttons. Right-clicking an item will bring up a menu of actions performable upon that item. Each module has a different table.
- **Menu Bar:** From here, you can open new modules, close modules and/or the application, and retrieve Entré application help. The menu bar is the same for all modules.

Menu Navigation

Each Entré module has the same menu bar at the top of the window. The following options are in the menu bar.

- **File:** Manage application activities, such as closing windows, exiting the application, logging in or out, and password management.

- **Edit:** Configure peripheral tools specific to the workstation, such as capture devices, printers, and information scanners.

- **Navigation:** Access navigation features and capabilities.

- **Monitoring:** Manage alarms, events, and device status.

- **Management:** Administrate personnel within the Entré system.

- **Configuration:** Administrate system logistics.

- **Advanced:** Lists modules intended for advanced operators. Advanced modules allow the system to be customized.

- **Window:** Configure the display of windows and menus. For changes to take effect, restart Entré.

- **Help:** Application help and information.

Search

Use the **Search** option to search the rows currently displayed. Select the drop-down arrow and select **Edit Search Fields** to customize sorting.

Configure Columns

You can configure column visibility and order in most table-based modules.

1. In the toolbar, select **Columns**.

2. Next to each column name, toggle the column visibility as needed.

3. To change the column order, select a column and select **Up** or **Down**.

4. Select **OK**.

5. To adjust column width, drag the edge of the column header.

6. To sort table data by a specific column, select a column header. Data will be sorted in descending order, either alphabetically or numerically. To reverse the order, select the column header again. A directional arrow shows the currently sorted column as well as its direction.

Upgrade Entré

Software updates are available from DMP dealers and representatives. All events and configurations are preserved throughout the upgrade. To see if you qualify for an update, contact your dealer or representative. For more information on the upgrade process, visit DMP.com/products/entré-software.

NAVIGATE ENTRÉ

Start Page Module

The **Start Page** module provides easy access to all modules from its main window. It is the default module that opens when starting the application. Modules may be opened using the buttons on the left. Categories such as **Management** and **Configuration** contain additional modules that are visible when the categories are expanded. Multiple modules can be opened and viewed simultaneously. The available modules will vary depending on the software license purchased, as well as operator privileges.

Set Up Quick Launch

The **Quick Launch** module provides easy access to common modules and device commands. Go to **Navigation** > **Quick Launch** to open the module. To use the **Quick Launch** module, you must create a panel in the **Quick Launch Editor**. For this example, you will create a panel and add device command and report widgets.

Create a Panel

1. Go to **Configuration** > **Quick Launch Editor** > **New Panel**.

2. Name the panel and define the number of columns and rows to be displayed. Assign a location if applicable. Use the following for this tutorial:

   ‣ **Name**: Test

   ‣ **Number of columns**: 1

   ‣ **Number of rows**: 2

3. Select **OK**.

Add Device Command Widget

1. In the first cell, select **Add**.

2. Select **Device Command**, then select **OK**.

3. Enable **Multiple (by filter) of type**, then select **Device**.

4. In **Device**, select **Filter**, then select **Choose**.

5. Choose the doors that will respond to this command and select **OK**.

6. To close **Filter - Device**, select **OK**.

7. In **Command**, select **Choose**.

8. Select **Lock**. Select **OK**. Some commands require the parameters to be filled in. If this field is required, select **Choose**, then select a parameter.

9. To close the **Add - Device Command Widget**, select **OK**.

Add Report Widget

1. In the second cell, select **Add**.

2. Select **Report**, then select **OK**.

3. In **Report**, select **Choose**.

4. Select a report to add to the panel.

5. Select **OK**.

6. To close **Add - Report Widget**, select **OK**.

7. In the toolbar, select **Save**.

Edit Widgets

- To edit a widget's location, select **Edit** below the cell. Select **Location** to redefine the cell's row and column location.

- To change the panel's name or modify the panel's number of columns and/or rows, select **Properties** in the toolbar.

Utilize the panel by navigating to the **Quick Launch** module, located in the **Navigation** drop-down menu. The panel should appear as configured in the previous steps.

To modify the panel, return to the **Quick Launch Editor** module.

IMPORT MULTIPLE PANELS USING A CSV FILE
—

Multiple panels can be imported at once through an CSV file. Refer to the steps below to import panels using this feature:

📝 **Note:** Panels should be programmed to communicate with the Entré App Sever before the panel import.

Build the CSV and Properties Files

The CSV Panel Import requires two files:

- A CSV file containing the required connection information for each panel you intent to import into Entré
- A panel.csv.import.properties file to tell Entré the information contained in each column in your CSV file

The CSV file requires the following panel connection information:

- Panel Name
- Account Number
- IP Address
- Port

Optionally, you may also include the following connection information:

- Panel Serial Number
- Entré Passphrase (this is required if in-use on the panel and in the Entré driver)

There is an example **panel.csv.import.properties** file on the Entré App Server in the **sampledata** folder (Default location: C:\Program Files\DMP\Entre\sampledata). This file can be opened in your preferred text editor. The Serial Number and Passphrase lines are optional and are commented out by default with a '#' character at the start of the line. The example file includes the following information, where 'n' is the column number that information is in, (A=0, B=1, C=2, etc.):

- Name.column=n
- AccountNumber.column=n
- IPAddress.coluimn=n
- PortNumber.column=n
- #SerialNumber.column=n
- #EntréPassphrase.column=n

	A	B	C	D	E	F
1	Panel Serial	Panel Name	Account Number	Entre Passphrase	IP Address	Port
2	0123ABCD	ABC Company	12345	DMPABC12	172.0.0.2	2011
3	3210DCBA	XYZ Company	54321	DMPABC12	172.0.0.3	2011
4	5432EF00	123 Partners	65325	DMPABC12	172.0.0.4	3015
5	A4BC8E9A	Acme Corporation	56487	DMPABC12	172.0.0.5	2011

The order of the columns in the CSV file and their respective properties is irrelevent. Given the above CSV file, your panel.csv.import.properties file could be set up like this:

- Name.column=1
- SerialNumber.column=0
- PortNumber.column=5
- EntréPassphrase.column=3
- IPAddress.column=4
- AccountNumber.column=2

Create the Automation Rule

1. Go to **Configuration > Automation Rules**.
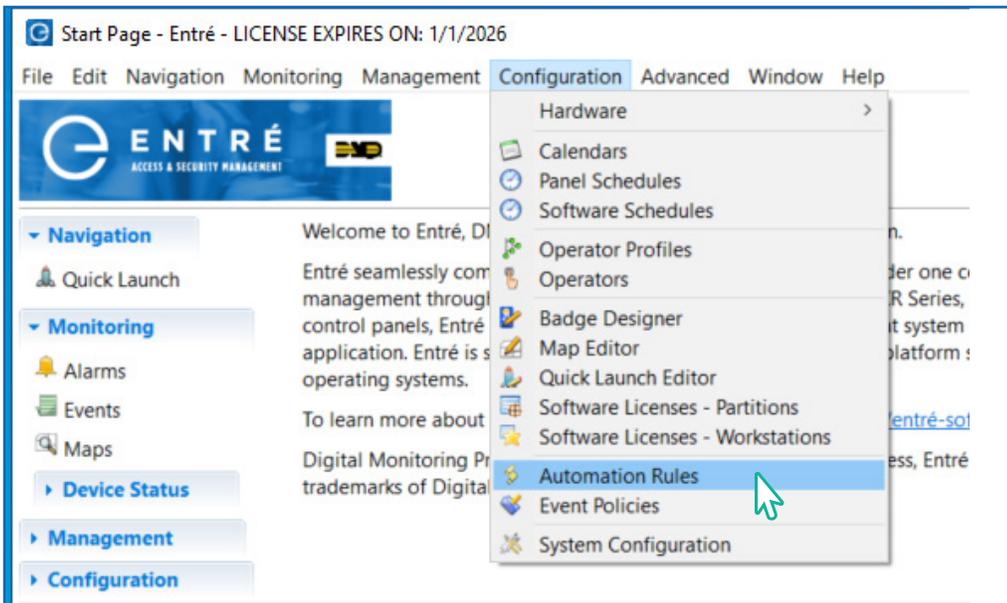
2. Select **Add**.

3. Name the **Automation Rule**.

4. In **Trigger**, select **New**.

5. Select the **Trigger Type**:
   - Period
   - Event
   - Manual
   - Software Schedule

6. Select **OK**.

7. In **Actions**, select **Add**.

8. In **Select Action Type**, select CSV Import. Select **OK**.

9. In **Type**, select **Panel Import**. If you do not see Panel Import as an option, ensure you have installed Entré Version 9.3 or higher.

10. Select the **Has header row** checkbox if your CSV file contains a header row.

11. In **Directory Path**, enter the path your CSV is located. This location should also have a properties file named **panel.csv.import.properties**.
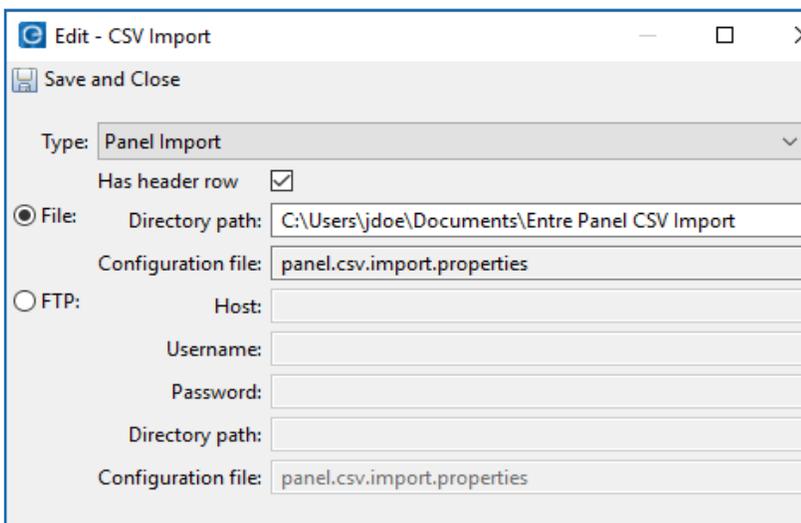
12. Select **Save and Close**.

13. To manually trigger the Automation Driver, right-click **Automation Driver** and select **Invoke Automation Rule**.

Create a Software Schedule

Creating a Software Schedule is optional, but it can be used to invoke an Automation Rule at a specific time.

1. Navigate to **Configuration** > **Software Schedules**.

2. Select **Add**.

3. Name the Software Schedule.

4. Select **Add** to add times.

5. Enter a **Start** and **End** time. The schedule will run at the start time.

6. In **Days of Week,** select your desired days to run the schedule. The **Holidays** option is displayed, but it is not currently functional.
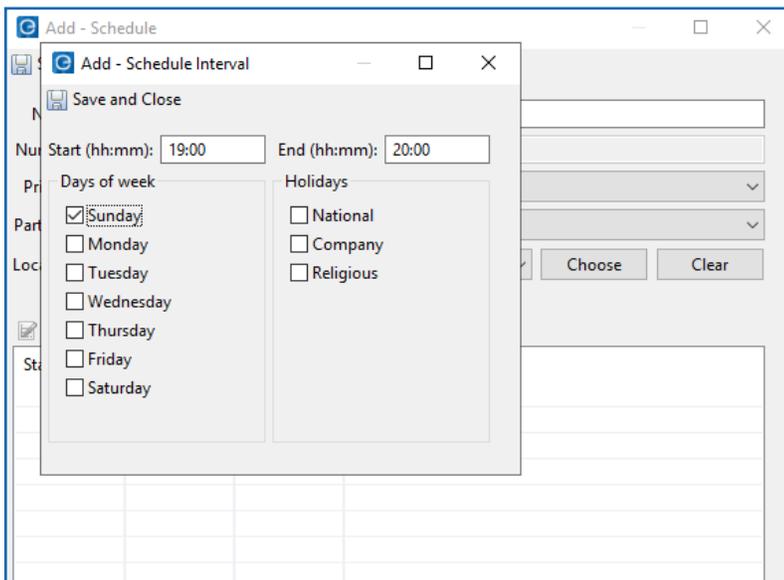
7. Select **Save and Close**.

ADD AND MANAGE A PANEL

Add a Panel

To add a panel, you can use the Hardware Tree or the Hardware List. Follow one of the options below, depending on what you want to use:

- Option A: Using the Entré Hardware Tree
- Option B: Using the Entré Hardware List
- Option C: Using the Entré NOC Hardware List

For information about connecting a cell-only panel to Entré, see "Set Up a Cell-Only Panel".

For information about setting up a panel with a Remote Key, see "Set Up a Panel with a Remote Key".

The following steps use the **New Panel Wizard Method**. If you are using the **New Panel** or **New Panel 150/350/550** method, enter a name and select the panel model in **General**. In **Communication**, enter the **IP Address** and **Account Number**, then select **Save and Close**.

📋 **Note:** Always perform a **Retrieve Configuration** from the panel *before* downloading. Downloading without retrieving first applies a default programming and may overwrite existing settings or cause system issues.

Option A: Using the Entré Hardware Tree

1. Open the **Configuration** menu, hover over **Hardware**, and select **Hardware - Tree**.
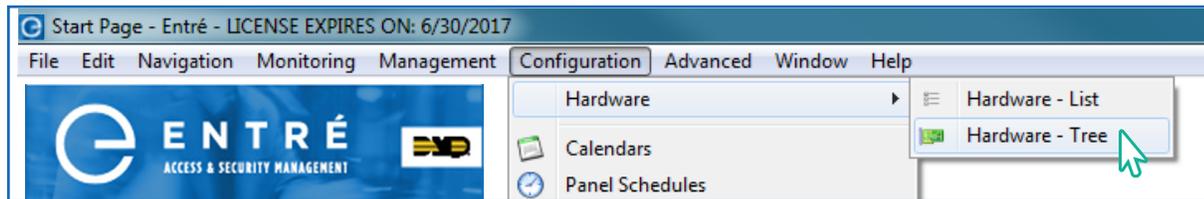
2. Right-click the **DMP Driver** and select **New Panel Wizard**.
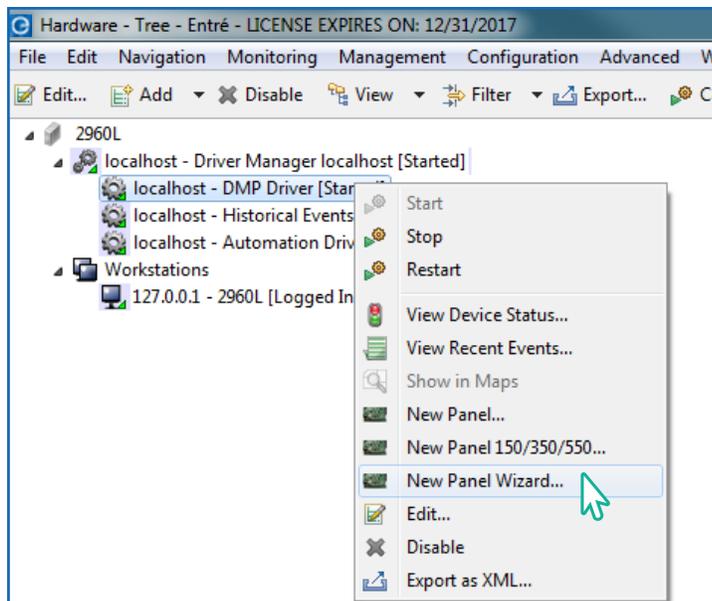
3. Enter the panel's information in the **DMP Panel Wizard** window.

- ‣ **Name**: Format the panel name to include the panel number in the name. *For example, Panel 1234.*
- ‣ **Host**: Enter the IP address.
- ‣ **Port:** Leave the default as **2011**. This should only be changed if the default is changed in the panel under Remote Options.
- ‣ **Account Number:** Enter your panel's account number.
- ‣ **Serial Number:** If adding a persistent connected panel, enter the serial number. Otherwise, leave blank.

  📝 **Note:** For persistent connected panels, set the **Port** in the Panel Wizard to **0** and the **Entré Incoming Port** in Remote Options of the panel to **0**.

- ‣ **Entré Passphrase:** If an Entré passphrase was entered into the panel under Remote Options and in the DMP Driver in Entré, enter the Entré Passphrase. Otherwise, leave blank.

4. Select **Next**. Entré will attempt to connect to the panel.

- ‣ If connection was successful, continue through the prompts and select **Finish** to complete the import process.
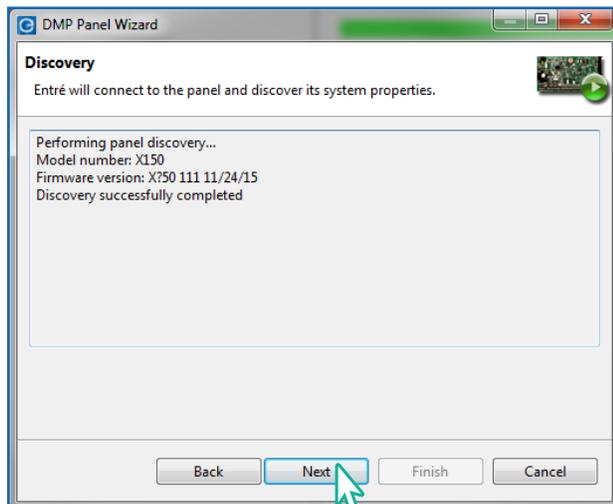
- ‣ If an **Unable to discover controller** message appears, there is an issue connecting. In Remote Link, confirm the connection in Remote Options, the panel account number, and the IP address.

Option B: Using the Entré Hardware List

Follow these steps to add a new panel to the hardware list.

1. Open the **Configuration** menu, hover over **Hardware**, and select **Hardware - List**.
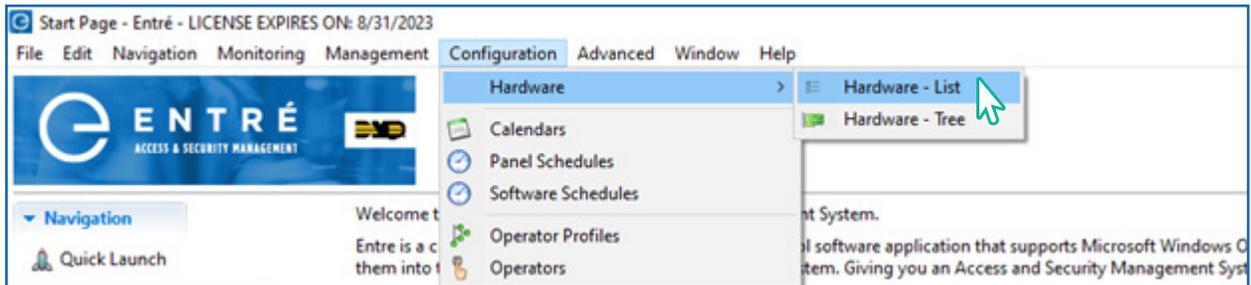
2. Select the drop-down beside Search and select **Quick Search All**.
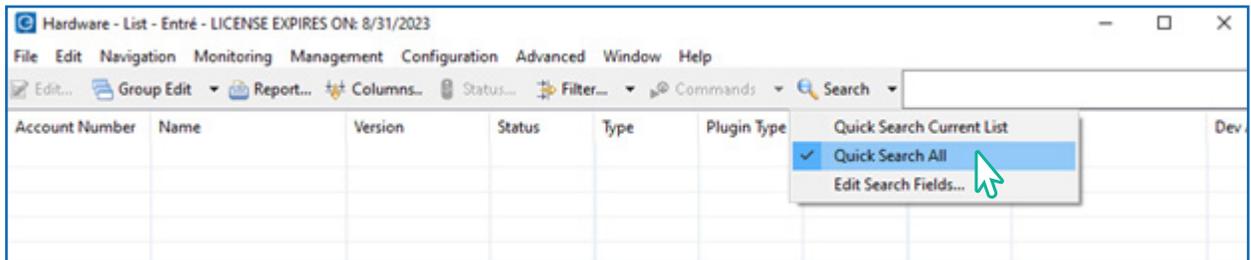
3. Enter **DMP Driver** into the search box and select **Search**.
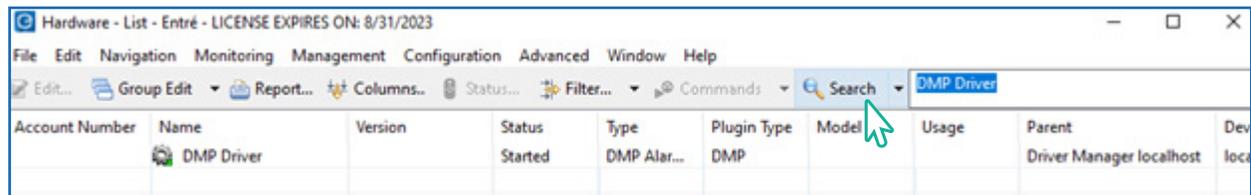
4. Right-click **DMP Driver** and select **New Panel Wizard**.
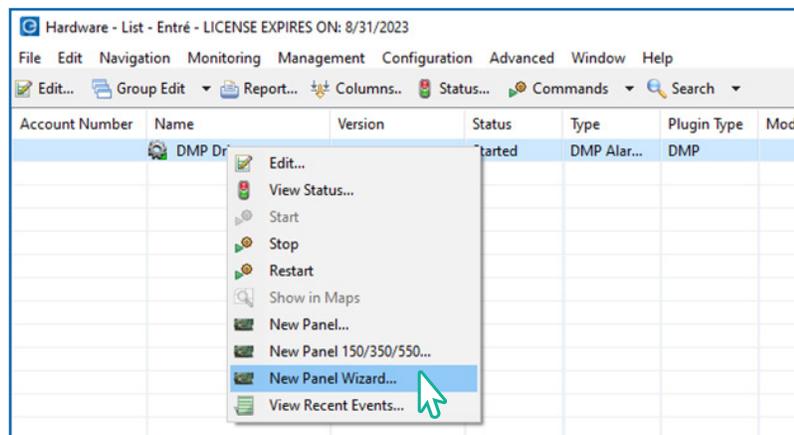
5. Enter the panel's connection information:

‣ **Name**: Format the panel name to include the panel number in the name. *For example, Panel 1234.*

‣ **Host**: Enter the IP address.

‣ **Port:** Leave the default as **2011**. This should only be changed if the default is changed in the panel under Remote Options.

‣ **Account Number:** Enter your panel's account number.

‣ **Serial Number:** If adding a persistent connected panel, enter the serial number. Otherwise, leave blank.

📝 **Note:** For persistent connected panels, set the **Port** in the Panel Wizard to **0** and the **Entré Incoming Port** in Remote Options of the panel to **0**.

‣ **Entré Passphrase:** If an Entré passphrase was entered into the panel under Remote Options and in the DMP Driver in Entré, enter the Entré Passphrase. Otherwise, leave blank.

6. Select **Next**.

7. Continue to select **Next** through the prompts. Then select **Finish**.

Option C: Using the Entré NOC Hardware List

Follow these steps to add a new panel to the hardware list in Entré NOC.

1. Open the **Configuration** menu, hover over **Hardware**, and select **Hardware - List**.
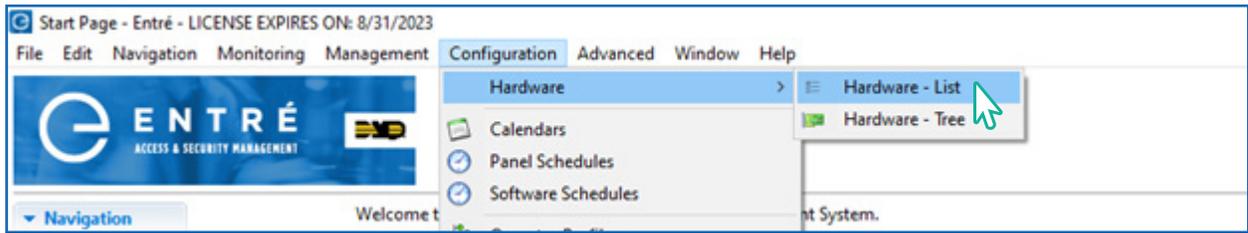
2. Search for **DMP Driver**. Be sure to turn off all options except for **Name**.
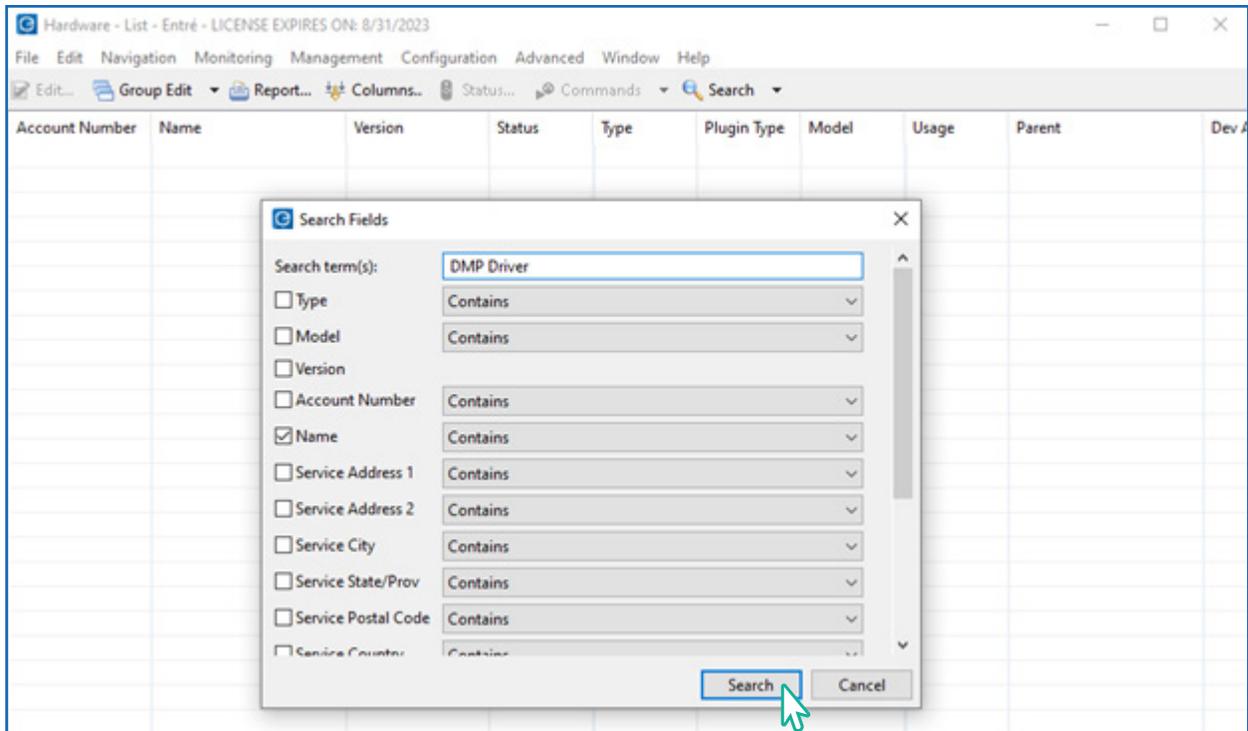
3. Right-click **DMP Driver** and select **New Panel Wizard**.
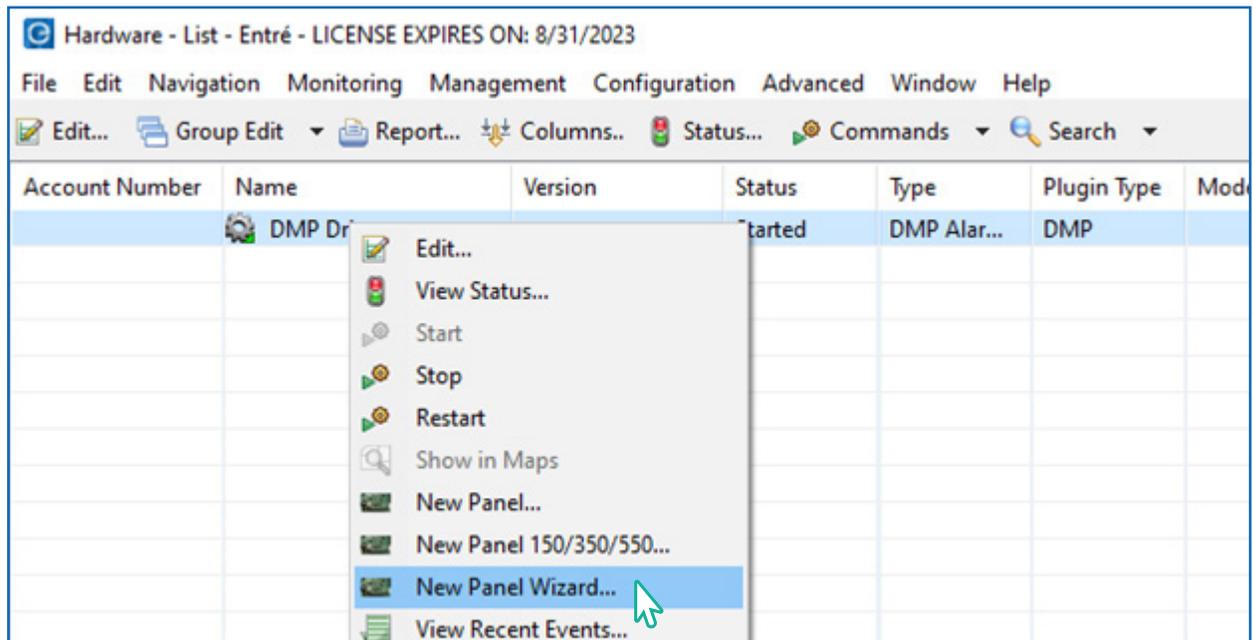
4. Enter your panel's connection information.

  ‣ **Name**: Format the panel name to include the panel number in the name. *For example, Panel 1234.*

  ‣ **Host**: Enter the IP address.

  ‣ **Port:** Leave the default as **2011**. This should only be changed if the default is changed in the panel under Remote Options.

  ‣ **Account Number:** Enter your panel's account number.

  ‣ **Serial Number:** If adding a persistent connected panel, enter the serial number. Otherwise, leave blank.

    📝 **Note:** For persistent connected panels, set the **Port** in the Panel Wizard to **0** and the **Entré Incoming Port** in Remote Options of the panel to **0**.

  ‣ **Entré Passphrase:** If an Entré passphrase was entered into the panel under Remote Options and in the DMP Driver in Entré, enter the Entré Passphrase. Otherwise, leave blank.

  | DMP Panel Wizard   — □ ✕ |
  | **Connection Settings** |
  | Please provide necessary settings for connecting to the DMP Panel. |
  | |
  | Name: [   ] |
  | Host: [   ] |
  | Port: [2011   ] |
  | Account Number:[   ] |
  | Serial Number: [   ] |
  | Entré Passphrase:[   ] |
  | |
  | < Back   Next >   Finish   Cancel |

5. Select **Next**.

6. Continue to select **Next** through the prompts. Then select **Finish**.

  | DMP Panel Wizard   — □ ✕ |
  | **Summary** |
  | The panel and its settings has successfully been configured. |
  | |
  | The panel has been installed and configured. |
  | |
  | Click "Finish" to exit the wizard |
  | |
  | < Back   Next >   Finish   Cancel |
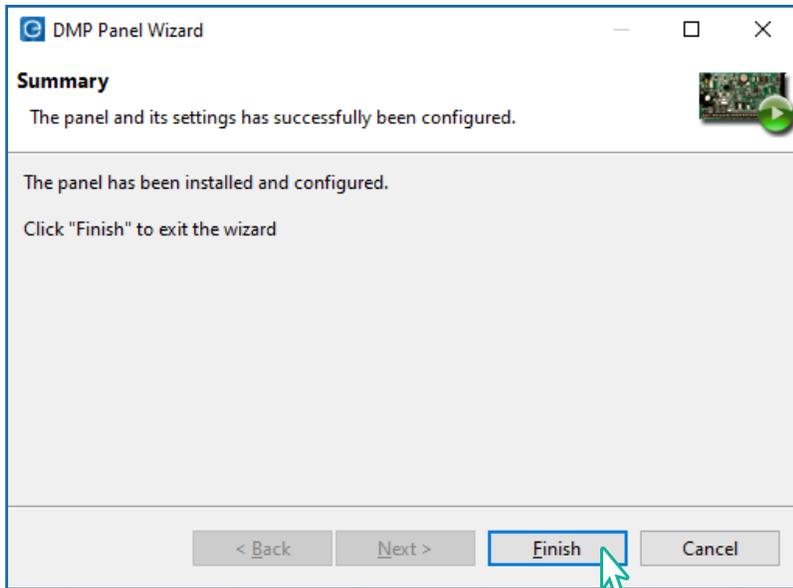
Panel Status

Panels have seven different device status values.

- **Disabled:** Panel remains in the software but no real-time events are displayed. The driver can be added back into the software without re-programming it. Only operators can disable a panel.

- **Failed:** Panel has encountered an unrecoverable error and has failed.

- **Started:** Panel has started and is running.

- **Starting:** Panel is in the process of starting.

- **Stopped:** Panel has stopped.

- **Stopping:** Panel is in the process of stopping.

- **Unknown:** State of the panel is not known to the system because the parent device is in a state such as unknown, stopped, or failed.

- **Awaiting Status:** State of the panel while the DMP Driver is starting or initially online until the panel checks in or fails to connect.

Swap a Panel

The process below shows you how to swap panels within Entré by deleting an old panel and then adding a new panel.

1. Delete the old panel, following the steps in [“Delete a Panel (Four Options)”](#).

2. Add the new panel, following the steps in “[Add a Panel](#)”.

Delete a Panel (Four Options)

In this section, choose one of the following to fit your specific needs to delete a panel:

- Option 1: Using the Entré Hardware Tree with Version 8.8.1 and Higher

- Option 2: Using the Entré Hardware Tree with Version 8.8.0 and Lower

- Option 3: Using the Entré Hardware List with Version 8.8.1 and Higher

- Option 4: Using the Entré NOC Hardware List with Version 8.8.1 and Higher

Option 1: Hardware Tree (8.8.1 and Higher)

For Entré versions 8.8.1 and higher, to delete a panel using the Hardware Tree:

1. Right-click the panel to display a drop-down menu.

2. Hover over **Panel Control**.

3. Select **Stop**.

4. Right-click the panel in the Hardware Tree and select **Delete**. This deletes all associated hardware and disassociates any attached profiles, automation rules, etc.

Option 2: Hardware Tree (8.8.0 and Lower)

For Entré versions 8.8.0 and lower, to delete a panel in the Hardware Tree, disable all of the programming associated with the panel in Entré.

Enable Deletion

1. Open the **Configuration** menu, select **System Configuration**.

2. Select **Miscellaneous**.

3. Enable **Allow deletion of terms that normally may only be disabled**.

4. Enable **Allow deletion of devices with events**.
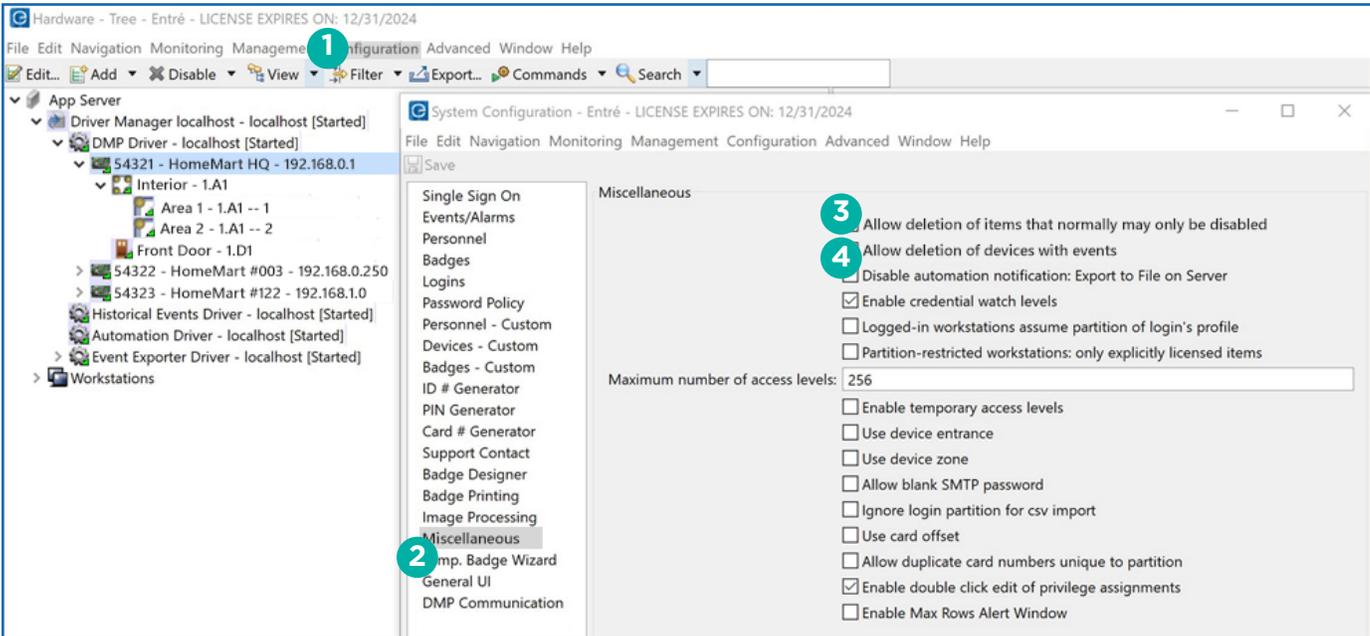
Stop the Panel

1. Right-click the panel to display a drop-down menu.

2. Hover over **Panel Control**.

3. Select **Stop**.
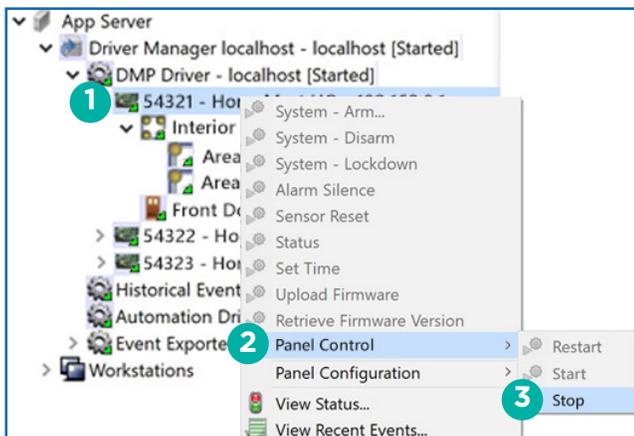
Disassociate Programming

1. Right-click the panel and select **Edit**.

2. Check that **System Reports**, **Display Keypads**, and **Status List** are cleared.

3. Select **Clear** to fully verify.
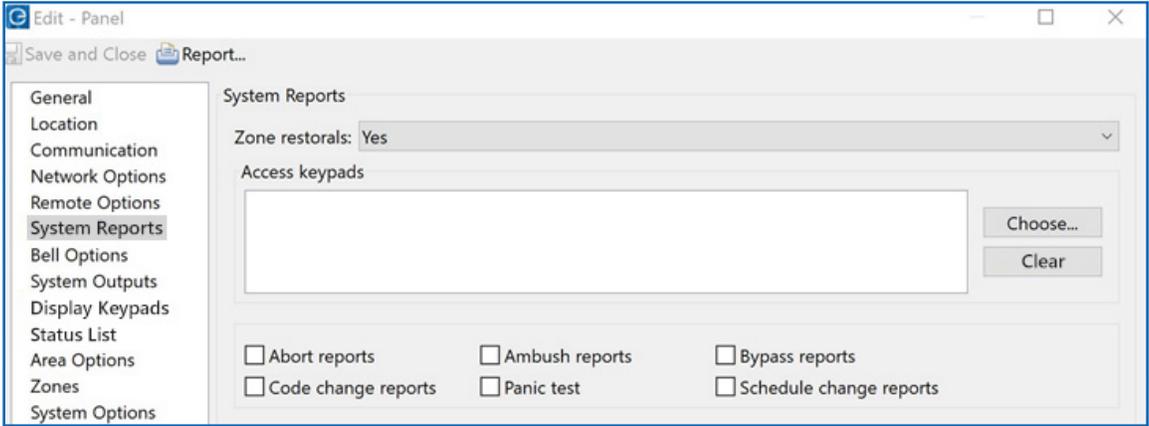
Acknowledge and Clear Alarms

1. Go to **Configuration** > **Hardware Tree** > **Monitoring** > **Alarms**.

2. Select **Ack All**.

3. Select **Clear All**.
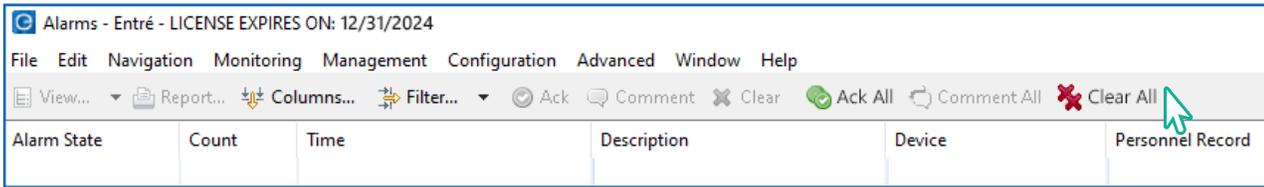
Delete Components and the Panel

1. In an area, right-click the following components in and select **Delete**. Components must be deleted in this order: **Zones**, **Outputs**, and **Devices**.

2. Right-click the area and select **Delete**.

3. Repeat these steps for each area and its components.

4. After each of the panel's areas are depleted, you may delete the panel from Entré. Right-click the panel and select **Delete**.
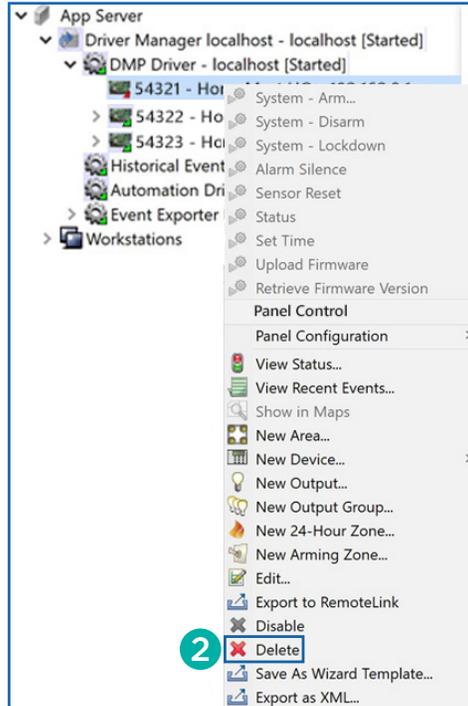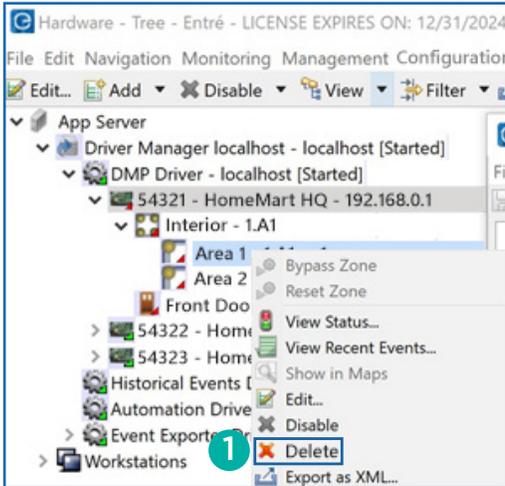
Option 3: Hardware List (8.8.1 and Higher)

For Entré versions 8.8.1 and higher, to delete a panel using the Hardware List:

1. Turn on deletion.

   a. Go to **Configuration** > **System Configuration**.

   b. Under **Miscellaneous**, turn on **Allow deletion of items that normally may only be disabled**.

   c. If this was not previously turned on, close out of the client and reopen so that this change will take effect.

4. Go to **Configuration** > **Hardware** > **Hardware List**.

5. Stop the panel. A panel cannot be online when trying to delete it.

   ‣ Right-click the panel to display a drop-down menu.

   ‣ Hover over **Panel Control**.

   ‣ Select **Stop**.

6. Right-click on your panel and select **Delete**.

7. Select **Yes** on the warning message.
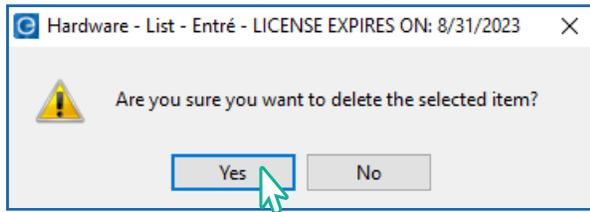
8. Close out of the module and re-open it to refresh the Hardware List. It will not refresh automatically.

Option 4: NOC Hardware List (8.8.1 and Higher)

For Entré NOC versions 8.8.1 and higher, to delete a panel using the Hardware List:

1. Turn on deletion.

   a. Go to **Configuration** > **System Configuration**.

   b. Under **Miscellaneous**, turn on **Allow deletion of items that normally may only be disabled**.

   c. If this was not previously turned on, close out of the client and reopen so that this change will take effect.
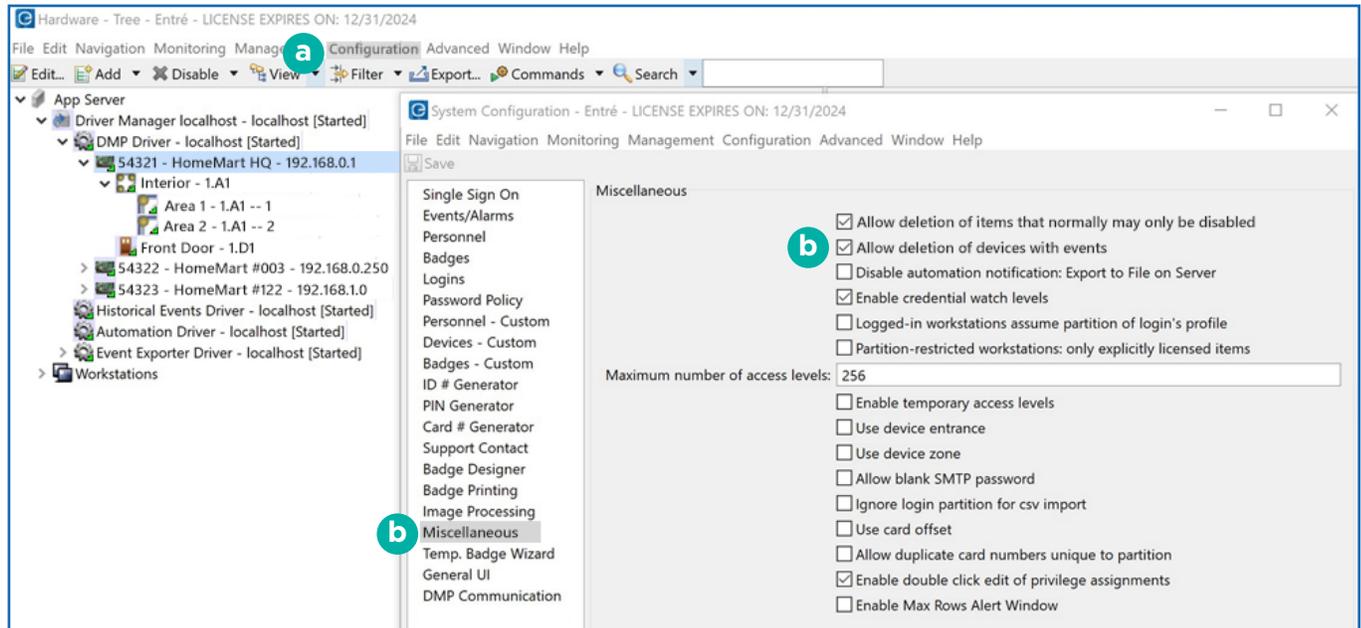
4. Go to **Configuration** > **Hardware** > **Hardware List**.
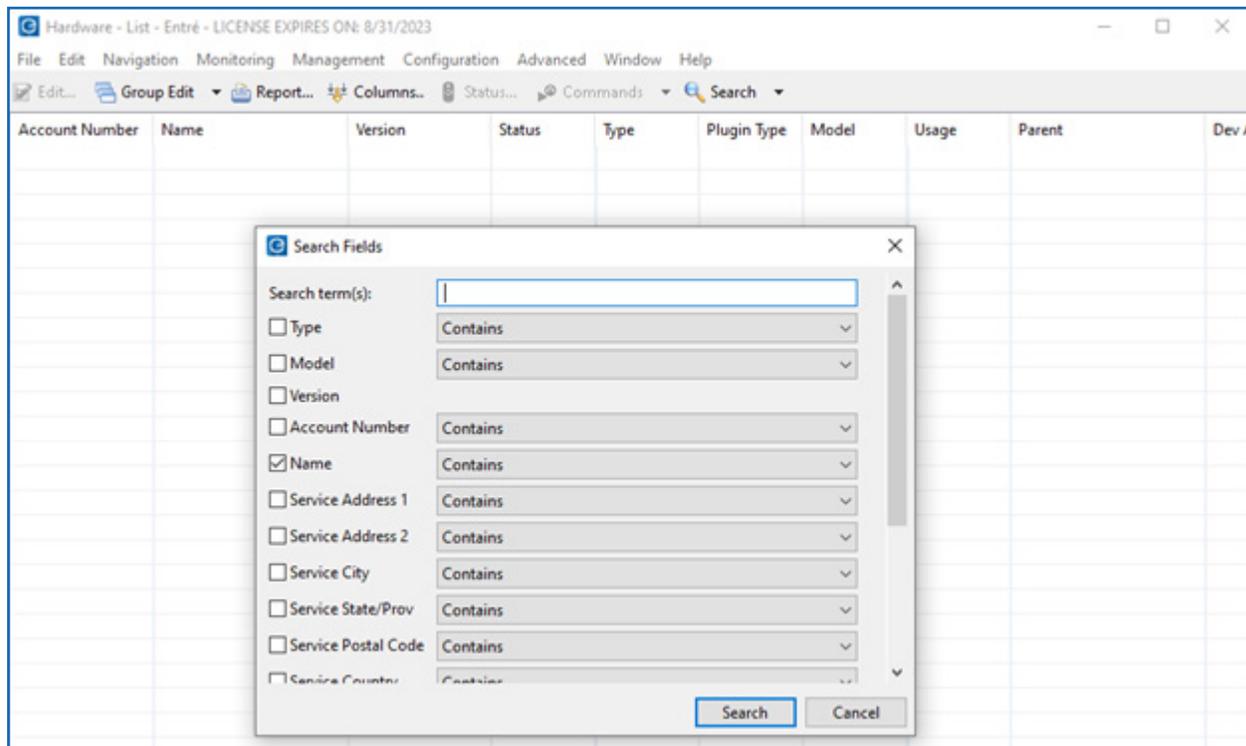
5. Enable search term(s) and search for the panel to be deleted. In the example, **Name** was used.
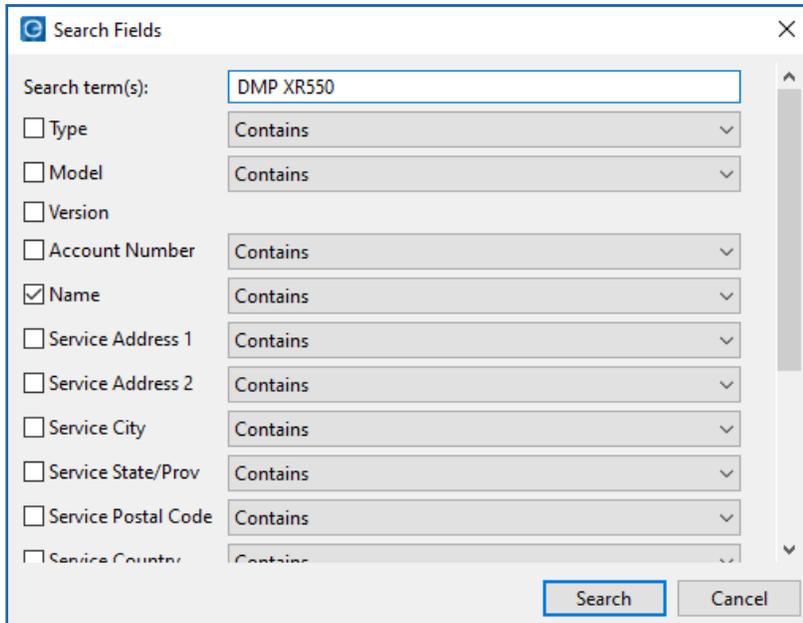
6. Stop the panel. A panel cannot be online when trying to delete it.

   ‣ Right-click the panel to display a drop-down menu.

   ‣ Hover over **Panel Control**.

   ‣ Select **Stop**.
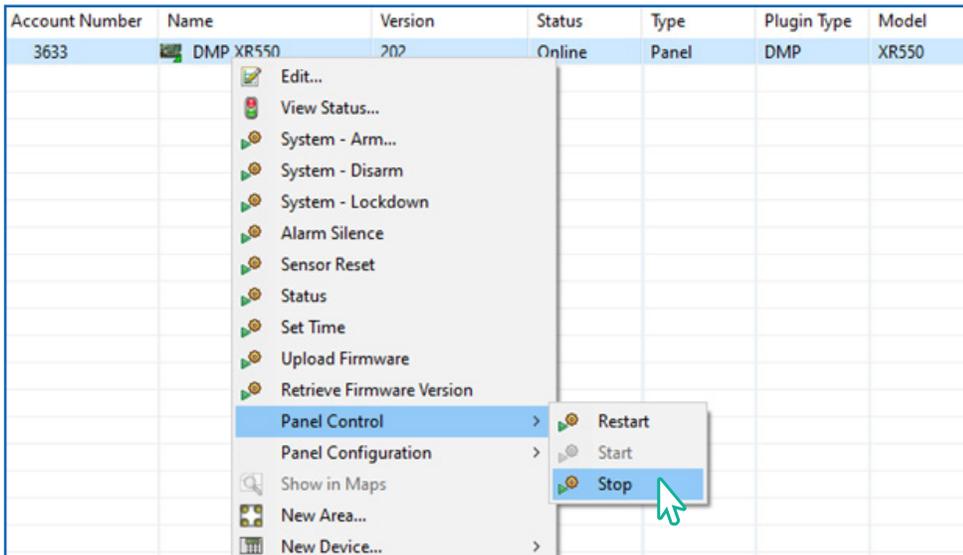
7. Right-click on your panel and select **Delete**.

8. Select **Yes** on the warning message.

9. Close out of the module and re-open it to refresh the Hardware List. It will not refresh automatically.

ADD AND MANAGE AN OUTPUT

Add an Output

1. Go to the Hardware Tree.

2. Right-click the parent panel and select **New Output**.

3. Fill out the **Add - Output** information and select **Save and Close**.

Output Status

Outputs are a Form C (SPDT) relay or switched ground (open collector) built onto a panel or output expander module that can be controlled by schedules, panel programming, or manually. The parent device of an output is always a panel. There are no device types that have an output as the parent device.

Outputs have the following device status values.

- **Steady:** Sends continuous power to the output.
- **Off:** Turns output off. For example, disabling an alarm bell.
- **Pulse:** Pulse the output at one second intervals.
- **Momentary:** Send power to the output once for one second.
- **Awaiting Status:** State of the output while the DMP Driver is starting or initially online until the panel checks in or fails to connect.

Delete an Output

In an area, right-click the **Output Point** and select **Delete**.

ADD AND MANAGE A KEYPAD

Add a Keypad

1. Go to the Hardware Tree.

2. Right-click the parent panel, hover over **New Device**, and then select **Keypad** in the side menu.

3. Fill out the **Add - Device** information and select **Save and Close**.

Keypad Status

A device with a keyboard and display that allows users to enter codes, arm and disarm areas, view current and past events, and perform system functions, such as: silencing alarm bells and changing user codes. Keypads can have LED, LCD alphanumeric, or vacuum fluorescent alphanumeric displays.

The parent device of a keypad is always a panel. There are no device types which have a keypad as a parent device.

Readers have the following device status values.

- **Disabled:** The device remains in the software but no real-time events are displayed. The device can be added back into the software without re-programming it. Only operators can disable a device.
- **Offline:** The device is offline, that is, not communicating with its parent sub-controller.
- **Online:** The device is online and communicating normally.
- **Unknown:** State of the device is not known to the system because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Awaiting Status:** State of the device while the DMP Driver is starting or initially online until the panel checks in or fails to connect.

Delete a Keypad

Right-click the keypad and select **Delete**.

ADD AND MANAGE AN AREA

Add an Area

1. Go to the Hardware Tree.

2. Right-click the parent panel and select **New Area**.

3. Fill out the **Add - Area** information and select **Save and Close**.

Area Status

A grouping of burglary zones that can be simultaneously armed or disarmed. For example, an area might consist of office doors and windows. When arming the area, these zones arm together and if opened, an alarm will sound.

The parent device of an area is always a panel. Zone device types have a panel as a parent device.

Area device states include commands and device states. Areas have the following device status values.

- **Armed:** Area is armed.
- **Disarmed:** Area is disarmed.
- **Disabled:** The device remains in the software but no real-time events are displayed. The device can be added back into the software without re-programming it. Only operators can disable a device.
- **Unknown:** The state of the area is unknown. State of the device is not known to the system because the parent device is in a state such as unknown, offline, stopped, or failed.
- Awaiting Status: State of the area while the DMP Driver is starting or initially online until the panel checks in or fails to connect.

Assign an Area to a User Code Profile

To assign areas to the appropriate User Code Profiles, follow the steps below:

1. Open the **Management** menu and select **User Code Profiles**.

2. Double-click the profile to open its settings, or right-click and select **Edit**.

3. Select **Choose** next to the **Access Areas** field.

4. Select the areas this profile will have access to and click **OK** to confirm.

5. Repeat this process for any Arm/disarm areas, Output groups, or Schedules that apply to this profile.

6. Select **OK**.

7. Select **Save and Close**.

Delete an Area

Right-click the area and select **Delete**.

ADD AND MANAGE A ZONE

Add a Burglary Zone

1. Navigate to **Configuration** > **Hardware** > **Hardware – Tree**.
2. Use the arrow to the left of the panel to see the areas.
3. Right-click on the area to assign zone to.
4. Select **New Zone**.
5. Fill in a name, select zone type, and enter any other necessary programming.
6. Select **Save and Close**.

Add an Arming Zone

1. Navigate to **Configuration** > **Hardware** > **Hardware – Tree**.
2. Right-click on the panel.
3. Select **New Arming Zone**.
4. Fill in a name and enter any other necessary programming.
5. Select **Save and Close**.

Zone Status

Zone device states include commands and device states. Zones have the following device status values.

- **Normal:** Device is operating normally.
- **Disabled:** Device remains in the software but no real-time events are displayed. The device can be added back into the software without re-programming it. Only operators can disable a device.
- **Bypass:** Device has been bypassed.
- **Unknown:** State of the device is not known to the system because the parent device is in a state such as unknown, offline, stopped, or failed.
- **Awaiting Status:** State of the zone while the DMP Driver is starting or initially online until the panel checks in or fails to connect.

Edit a Zone

To change a zone to a 24-hour zone, follow the steps below.

1. Clear any active alarms.
2. Go to **Edit Panel** and select **Edit Zones**.
3. Make the changes.

After making the change, download the changes to the panel.

1. Right-click the panel.
2. Go to **Panel Configuration** and select **Download Configuration**.
3. Select **Zones** from the list.
4. Select **OK**.

Delete a Zone

Right-click the zone and select **Delete**.

ADD AND MANAGE A 24-HOUR ZONE

—

Add a 24-Hour Zone

1. Navigate to **Configuration** > **Hardware** > **Hardware – Tree**.

2. Right-click on the panel.

3. Select **New 24-Hour Zone**.

4. Fill in a name, select zone type, and enter any other necessary programming.

5. Select **Save and Close**.

Edit a 24-Hour Zone

To change a 24-hour zone to an area zone, follow the steps below.

1. Clear any active alarms.

2. Go to **Edit Panel** and select **Edit Zones**.

3. Make the changes.

After making the change, download the changes to the panel.

1. Right-click the panel.

2. Go to **Panel Configuration** and select **Download Configuration**.

3. Select **Zones** from the list.

4. Select **OK**.

Delete a 24-Hour Zone

Right-click the 24-hour zone and select **Delete**.

ADD AN IMAGE CAPTURE DEVICE

Entré supports capture devices (badging cameras) that use TWAIN and video drivers. Before proceeding, ensure that all necessary camera drivers are installed.

1. Go to **Edit** > **Preferences** > **Image Capture**.

2. Ensure that the **Is present** checkbox is selected. If a vanity monitor is desired, check the **Use vanity monitor** checkbox. If the vanity should appear on a secondary monitor, check the **Use second monitor** checkbox.

3. Use the **Type** drop-down to select the source of the image capture device. The following options are available depending on the type operating system being utilized: **Video** or **TWAIN**.

4. If necessary, modify the width, height, and scale of the final image, then select **OK**.

5. Go to **Management** > **Personnel**.

6. Add a new personnel record to the system by selecting **Add**, then select **Capture** to verify that the configured driver opens and displays video.

CONFIGURE SOFTWARE

The following topics include various instructions about configuring the software's more general settings.

Configure Time Change

Allow **Time Change** in System Options programming. This allows the panel to get the time update from the Central Station receiver.

1. Go to **Edit - Panel** and find **Time Change** below **Hours from GMT**.

2. Select **Yes** or **No**.

Add and Manage a Calendar

Add a Calendar

The **Calendars** module is used to manage holidays.

Typically, only a single calendar needs to be defined. However, if a system crosses multiple geographical boundaries, or consists of multiple sites, then multiple calendars may be needed.

Because holidays can vary from year to year, a calendar needs to have each holiday defined for each year. Since the panel only has date slots for the month and day, enter holiday dates only for the current year.

1. Go to **Configuration** > **Calendar**.

2. Select **Add**.

3. Enter a name for the calendar.

4. Select **Holidays** as needed.

5. Enter the information about the specific holidays that you want the calendar to recognize.

6. Select **Save and Close**.

Assign a Calendar

To assign a calendar to the panel, follow the steps below:

1. Right-click the panel and select **Edit**.

2. Select **Calendars**.

3. Use the drop-down menus to assign calendar and holiday categories to the panel.

4. Click **Save and Close**.

Add and Manage Schedules

Add a Schedule

The **Schedules** module manages the schedules used throughout the application. Schedules are used when programming areas.

1. Go to **Configuration** > **Panel Schedules**.

2. Select **Add**.

3. Name the schedule.

4. Choose a **Usage** type:
   ‣ For XR Series panels, select **Time Schedule**.
   ‣ For TMSentry panels, select **Output Schedule** or **Permanent Schedule**.

5. Enter the desired start and end time for the interval using a 24-hour format. For example, **12:00 AM** is displayed as **00:00**.

6. Once the schedule interval is configured, select **Save and Close** to add the interval to the schedule. Repeat this step for as many distinct intervals as necessary.

7. Select **Save and Close**.

Assign an Area Schedule

The maximum number of schedules per area is 8.

1. Right-click the area icon in the Hardware Tree and select **Edit**.

2. Select **Area Schedules** and select **Add**.

3. Enter a schedule number (1-8) and select a time schedule from the Schedule drop-down list.

4. Select **Save and Close**.

Assign a Door Schedule

The maximum number of schedules per area is 16.

1. Right-click the keypad or door icon in the Hardware Tree and select **Edit**.

2. Select **Door Schedules** and select **Add**.

3. Select the appropriate time schedule from the drop-down list.

4. Select **Save and Close**.

Assign an Output Schedule

The maximum number of schedules you may assign per relay is 8.

1. Right-click the area icon in the Hardware Tree and select **Edit**.

2. Select **Output Schedules** and select **Add**.

3. Select a time schedule from the Schedule drop-down list.

4. Select **Save and Close**.

Send Schedules or Holidays to the Panel

Follow these steps to send schedules and holidays to the panel(s). Holidays are sent when you send the schedules to the panel.

1. Right-click on the panel, hover over **Panel Configuration**, and select **Download Configuration**.

2. Turn on the **Schedules** option.

3. Select **OK**.

4. If this is a new installation, make sure to turn on **Clear Schedules** to clear the current schedule out of the panel. This is very important for the first time schedules are sent to make sure that old data is cleared out of the panel.

Customize the User Interface

Use wizards and configure how new windows open.

1. Go to **Configuration** > **System Configuration** > **Personnel**.

2. Select the following options:
   - ‣ **Use single-screen personnel wizard**
   - ‣ **Use CSV personnel import wizard**

3. To allow custom personnel fields to be used in the personnel wizard, select **Use custom fields on personnel wizard**.

4. To configure the custom fields, go to **Personnel - Custom**.

5. Go to **Badges** and select **Use single-screen badge wizard**.

6. To allow custom badge fields to be used in the badge wizard, select **Use custom fields on badge wizard**.

7. Select **Badges - Custom** to configure the custom fields as desired.

8. To enable the **Return Badge** button in the **Badges** module, select the **Show return temporary badge in badges module**.

9. Select **Save**.

10. Log out of Entré and log back in.

Configure Password Policies

Configure password policies in the **System Configuration** module.

1. Go to **Configuration** > **System Configuration** > **Password Policy**.

2. Configure the password policy in accordance to security preferences.

3. Select **Save**.

4. Log out of Entré and log back in.

5. In **File**, select **Change Password**.

6. Enter the **Old password**, then enter the **New password**. Confirm the new password, then select **OK**.

7. Log out, then log in with the updated password.

CONFIGURE AUTOMATION

Set Up Automated Tasks

The automation rule capability must be enabled in your software license. Contact a DMP dealer or representative for more information.

The following topic describes how to add an Automation Driver to the hardware tree. If you've already created an automation driver, go to step 7.

1. Go to **Configuration** > **Hardware**.

2. Right-click the **Driver Manager** and select **New Automation Driver** from the drop-down list. Only one Automation Driver is necessary in a system.

3. Name the **Automation Driver**. To set up e-mail notifications, consult your network administrator for SMTP Server settings.

4. Select **Save and Close**.

5. Right-click the **Automation Driver** and select **Start**.

6. The status of the **Automation Driver** will change from **Unknown** to **Started**. To initialize Automation Rule changes, the Automation Driver must be stopped and restarted.

7. Go to **Configuration** > **Automation Rules**.

8. Select **Add**.

9. Complete the following tasks:

   ‣ Give the **Automation Rule** a name.

   ‣ Select **New** next to **Trigger**. Select **Periodic**, then select **OK**.

   ‣ Select **Monthly**, then select a **Day of month** and a **Time of day** for the trigger to occur.

   ‣ Select **OK**.

   ‣ In **Actions**, select **Add**.

   ‣ Select an action type. For this example, select **Report**.

10. In **Report**, select **Choose**, then choose a report for the automated task to automatically run.

11. Select **OK**, then select **Save and Close**.

12. If emailing reports is desired, select **New** in **Notification**, then select a type of notification for the automated task. For this example, select **E-mail**, then select **OK**.

13. Add an e-mail address for the **To**, **CC**, and/or **BCC** fields, then select **OK**.

14. Verify that all configurations are saved to the automated task, then select **Save and Close**.

Automatically Generate Card Numbers

You can automatically generate card numbers using the **System Configuration** module.

1. Go to **System Configuration** > **Card # Generator**.

2. Select **Is present**, then configure the **Minimum** and **Maximum** digits allowed per card number.

3. Select **Save**.

4. Restart Entré.

5. To generate card numbers, go to **Management** > **Badges**.

6. In the toolbar, select **Add**.

7. Select a **Template**, then select **OK**.

8. To automatically create a card number, go to **Card #** and select **Generate**.

9. Enter the user code and assign the badge to an active personnel file.

10. Select **Save and Close**.

CONFIGURE MAPS

Add a Map

The Map Editor module contains map, device, and layer data. Once a map is configured in the **Map Editor** module, it can be viewed in Maps module, located in the Management drop-down menu.

⚡ **Caution:** Do not use the Map Editor while other client workstations have the Map Viewer or Map Editor open. Use of the Map Editor while any other client workstations have the Map Viewer or Map Editor opened may result in concurrency conflicts and system errors.

1. Go to **Configuration** > **Map Editor**.

2. In the toolbar, select **New Folder**.

3. Name the new folder, then select **OK**.

4. In the toolbar, select **New Map**.

5. Name the map and add any necessary location information.

6. To select a background map image from a local file, go to **Background** and select **Choose**. Background images must be in .svg, .png, .jpg, or .bmp format.

7. Select **OK**.

Images in Map Editor

To ensure that Map Editor does not experience memory issues, use only single-layer images. These images can have dimensions up to 800p x 600p in the following formats:

- JPG
- BMP
- SVG

Configure a Map

After a map is configured in the **Map Editor** module, it can be viewed in **Management** > **Maps**.

1. To add hardware or access points to the map, expand the **Devices** or **Device Groups** tree, then select and drag each item to the point on the map which corresponds to its physical location.

2. Plot device commands that are associated to the mapped devices or device groups by expanding the **Commands** tree, then select and drag each command to its representational location. Each item category can be added to separate layers. This allows certain categories to be hidden from view. To hide a layer, right-click the layer icon (located on the left side of the layer title) or right-click the map, then select **Toggle Layer Visibility**.

3. Select the device type which the command will run against from the **Device** tree, then select and drag the command to the map.

4. To add a device or device group by using a device command, select the device type from the **Device** tree and drag it to the desired location on the map. Open **Commands**, then select and drag the command into the map. Configure the command as needed. Separate layers can be used in order to hide device commands from view.

5. Once the devices are selected in Command, select **Choose** and select the command the device should execute. If the command requires a parameter, select **Choose** to select the parameter.

6. Select **OK** to save and add the device command to the map.

7. To map locations, open the **Locations** tree, then select and drag hierarchical locations to the map.

8. If the graphic map should be associated with a location, right-click the map and select **Edit Map Properties**, then under the **Location** drop down, select a location.

9. Select **OK** to save the map properties and close the window.

Navigate the Map

Use specific controls to navigate around a map.

Zoom Marquee

Zooms a map to a specific rectangular area. While holding **Ctrl**, click and drag a rectangle on the map. When you release the mouse button, the map will zoom to fit the rectangle.

Scroll the Map

While holding **Shift**, select the map and drag to the desired location.

Commands can be issued to devices plotted on a map. Right-click a device icon to open a menu containing device commands. Device commands can also be issued on the map. Right-clicking the plotted device command is not necessary, selecting it once will issue the command.

Device Status

The inside fill color represents the device state. The outer ring color represents the device alarm state.

Inside Color	Outside Color	Device Status Description
	Red	Alarm(s)
	Orange	Acknowledged alarm(s)
	Green	No alarms
Red		Unknown, fault, or active state
Green		Armed and inactive state
Light Blue		Disarmed and active state
Dark Blue		Disarmed and inactive state

Monitor Facilities Using Maps

View real-time events and alarm conditions overlaid on graphical maps of the facility.

Go to **Monitoring** > **Maps**. From the Maps field, expand the Maps tree, then select a map.

To view specific layers, expand the Layers tree on the left side of the window. Each device plotted on the map is associated with a specific layer. If devices are plotted on a layer, an arrow will be listed near the layer title. This allows the layer to be expanded to show the devices in the tree. If a layer is hidden, then all devices plotted on the layer will be hidden from view.

The device states are color-coded with an inner and outer ring color. To change the state of a device or issue commands, right-click the device and select a command. These are the same as are available from the Hardware module.

CONFIGURE EVENTS AND ALARMS
—

Event Types

There are different types of events that may occur.

Event

A general occurrence within the system, often from external hardware.

Alarm

An event configured to be an alarm.

Alarm Annotation

Event caused by commenting, clearing, or acknowledging alarms.

Audit Record

Event caused by an operator modifying a record, such as a badge or personnel record.

Device Command

An event caused by an operator executing a device command.

Device Command Result

Notification of a completed device command.

Alarm States

The operator may change the state of an alarm or add a comment by using the toolbar. These and other options are available by right-clicking the alarm and choosing the option from the menu. These options are also available in the alarm detail window. Alternatively, alarms can be cleared by selecting Clear.

An alarm may be in one of several states:

Active

The alarm is new, unacknowledged, and unresolved. Appears blinking red.

Acknowledged

Operator is aware of the alarm, though it remains unresolved. Appears solid orange.

Cleared

Alarm has been acknowledged and resolved. Appears appear solid green. The default filter in the Alarms module hides cleared alarms, so these are generally unseen.

Configure Alarm Instructions

Configure alarm instructions in the Alarm Instructions module.

1. Go to **Advanced** > **Alarm Instructions**.

2. Select **Add**.

3. Enter a **Title**.

4. In the **Text** field, enter instructions to be displayed in the **Events**, **Alarm**, and **Manage Alarms** windows.

5. Choose the correct **Log Code** to apply instructions.

6. If you need to specify the panel, add that in **Device**.

7. Select **Save and Close**.

Set Up Event and Alarm Priorities

Set up event and alarm priorities in the Event Policies module.

1. Go to **Configuration** > **Event Policies**.

2. The **Event Policies** module allows the operator to specify the following options for each available event log code:
   ‣ Treat the log code as an alarm or an event
   ‣ Whether to save the event to the database
   ‣ Event priority
   ‣ Sound and color associated with the event
   ‣ If the event is specific to the device

3. Select **Event Policy**.

4. Make changes to the policy as appropriate:
   ‣ To cause events of this type to be recorded as alarms and displayed in the Alarms module, select **Is alarm**.
   ‣ If **Is alarm** is enabled, **Alert sound** specifies the sound to be played when an alarm of this type occurs.
   ‣ Use the Priority drop-down arrow to change the priority of the event or alarm. Positive priorities are above normal priority and negative priorities are below normal. Zero is normal.
   ⚡ **Caution: Is recorded** should only be disabled by advanced users under the advice of DMP technical support.

5. Select **Save and Close**.

Create a Report

Several Entré modules have the capability to create reports. In this example, we'll create an Events report. To include personnel photos in reports, open the **System Configuration** > **Miscellaneous** and select **Enable personnel photos in reports**.

1. Go to **Monitoring** > **Events**.

2. In the toolbar, select **Report**.

3. In **Title**, enter a name for the report.

4. In **Order By**, select how the items in the report will be grouped. For this example, select **Device**.

5. Select **Page break between groups** to organize each page of the report by its grouping.

6. Select **Show group by label** to display the group label with the events in the report.

7. In **Format**, specify how the report should be formatted for viewing. For landscape orientation, select **Record-style**. For portrait orientation, select **Table-style**.

8. To open the report in an external document window, select **Open as document**.

9. Select the document type to export. For this example, choose **PDF document**.

10. Select **OK**. Export time depends on the size and complexity of the report.

Enable Video Report

Enabling **Video Reports** will allow the panel to send video system reports to Entré when an event message has been received from a camera.

To enable Entré Video Reports:

1. Go to the **Edit - Panel** window.

2. Select **Remote Options**.

3. Select the **Entré** tab.

4. Enable **Entré Video Reports**.

5. Select **Save**.

IMPORT PERSONNEL USING CSV IMPORT

A large amount of personnel records can be added to Entré using a Comma Separated Value (CSV), also known as a comma delimited file. A CSV file can be extracted from all common database vendors. Once a personnel CSV file is extracted from a database, it can be added to Entré using the following process. Refer to the table at the bottom of the page for the possible CSV functions to use with the Import Wizard.

Before you begin, keep in mind which fields are for importing personnel and badge records.

- The Personnel ID, First name, and Last name are for the personnel record.
- The Card #, User code, User #, Profile, and Current profile are for the badge.

The CSV import not only can be used for adding personnel, but modifying, or removing as well. This allows you the option to handle thousands of updates to personnel as their positions or status change within the company.

Note: If adding more than one Profile to a Badge, an additional Profile column will need to be added to the CSV to add the extra Profile(s), up to 4 Profiles per Badge.

Modifying a Badge

If modifying a badge to a new profile, a column labeled *Current Profile* must be in the CSV. The correct User Code Profile in Entré that is already assigned to the badge must be entered in this column, with the new profile being assigned entered into the regular *User Code Profile* column. For example:

User Code Profile	Current Profile
Front Door Access	All Access

Deleting Personnel or Badges

If Deleting Personnel or Badges, you must add a column labeled *Delete* and add a *Y* in the data field of the record you want to delete.

Having First Name, Last Name, Personnel ID, and the Delete column will delete the entire personnel and all badges associated.

Having First Name, Last Name, Personnel ID, Card #, and the Delete column will delete the specific card number from that personnel and leave the personnel record alone.

	Personnel ID	First Name	Last Name	Card Number	User Code	Profile	Current Profile	Delete
Add Personnel	Required	Required	Required					
Update Personnel Name	Required	Required	Required					
Add Badge	Required	Required	Required		Required	Required		
Update Badge's Profile	Required	Required	Required			Required	Required	
Delete Personnel	Required	Required	Required					Required
Delete Badge	Required	Required	Required	Required				Required

Enable CSV Personnel Import Wizard

1. Go to **Configuration** > **System Configuration** > **Personnel**.

2. Make sure that **Use CSV personnel import wizard** is turned on. If it is not already, turn it on, select **Save**, and then log out and back in to Entré.
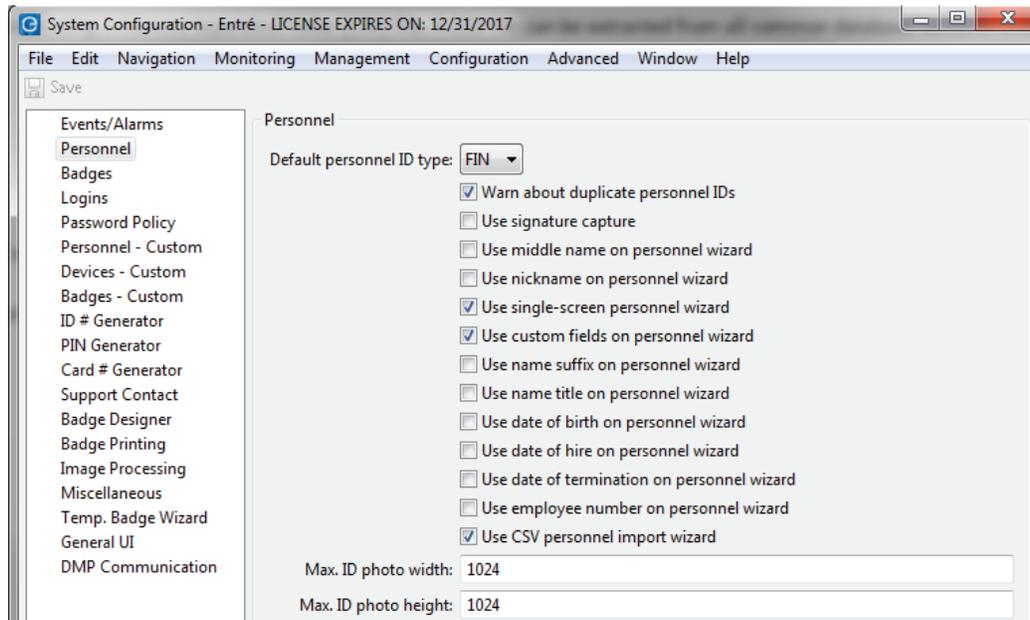
Configure the CSV File

1. Go to **Management** > **Personnel** > **Add** > **CSV Import Wizard**.
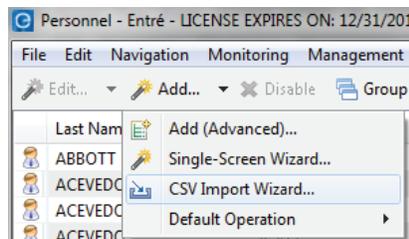
2. In the pop-up window, follow the prompts to choose your CSV file. Determine whether your CSV file has headers (rows of labels for the columns).
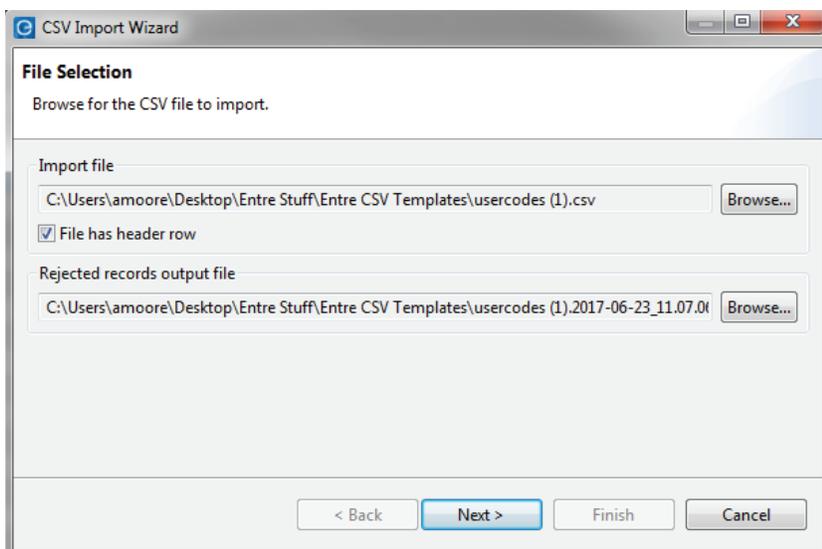
3. In the next screen of the **CSV Import Wizard**, the top window contains entries from the CSV file with generic column headings such as *Column 1, Column 2*, etc.

    ‣   The bottom left window displays the currently selected column number in the CSV file and the name of the CSV field. The **In header row** entry will be blank if the file's header row checkbox is not turned on in the previous step.

    ‣   The bottom right section of the window, **Import as**, contains field names from the Entré database.
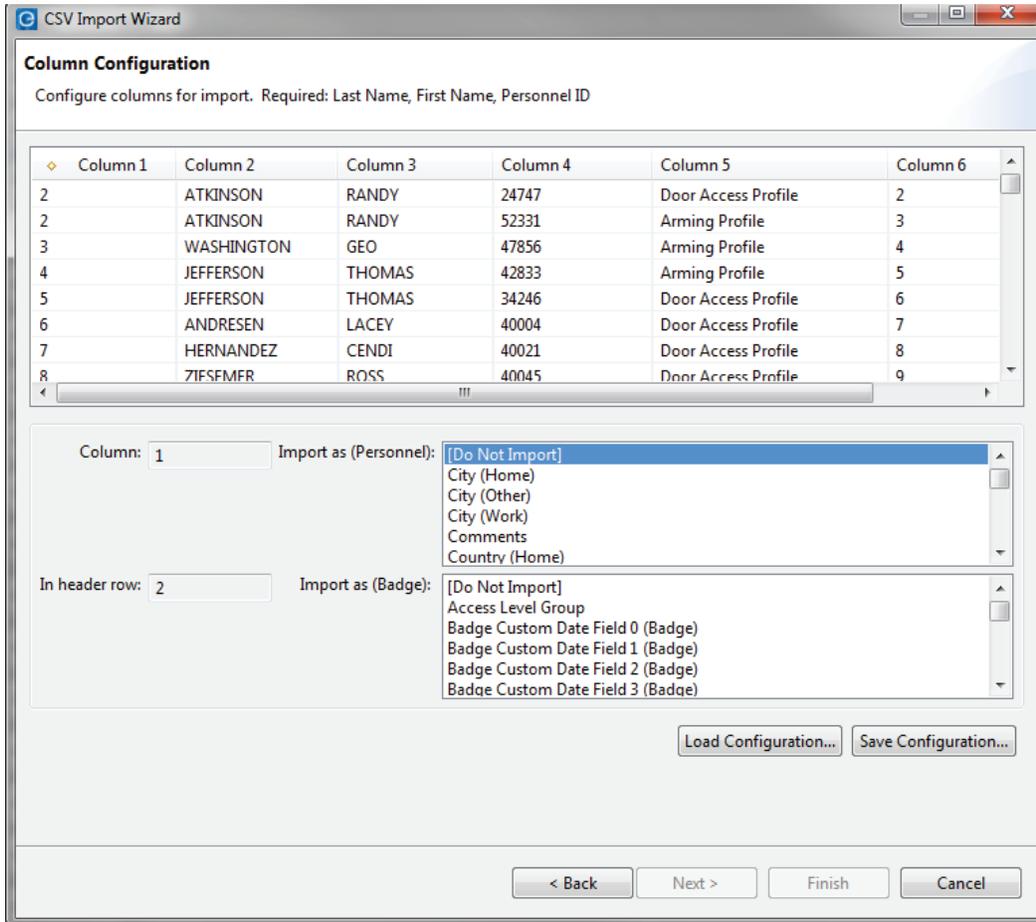
4. Assign the Entré database field that each CSV field will be imported into.

‣ Begin by selecting a CSV column in the top window. By default, *Column 1* will be selected, as is shown by the diamond symbol to the left of the column name.

‣ In the lower right window, select the Entré database field to which you want the selected CSV field to be imported.

‣ Repeat until all fields are assigned. All fields do not necessarily need to be imported. To not import fields, leave the default selection to **Do Not Import**. The **Next** button will not be enabled until all of the required fields displayed in the title area are assigned. Some common fields for a successful CSV import are:

    a. **(Personnel) ID #**

    b. **(Personnel) First Name**

    c. **(Personnel) Last Name**

    d. **(Badge) Card #**

    e. **(Badge) User Code** (Badge – DMP)

    f. **(Badge) User Code Profile** - These must be in the CSV files as profile names. For example, you cannot enter the number 1 to list a profile for a badge in Entré. The User Code Profile must be created before the import and given a specific name, such as *All Access*. Then in the CSV file the profile column will have the names of those existing profiles in Entré. In the example, there is *Door Access Profile* and *Arming Profile*. Those profiles were created in Entré prior to the CSV import and given the appropriate names.

    g. **(Optional)** - You can have additional columns designated for multiple items, such as **Partitions** or **Validity**. By default, we import badges as **Active**. If you need them to be **Inactive** for a particular reason, you would need to set that status appropriately, by adding the column and identifying it as such.
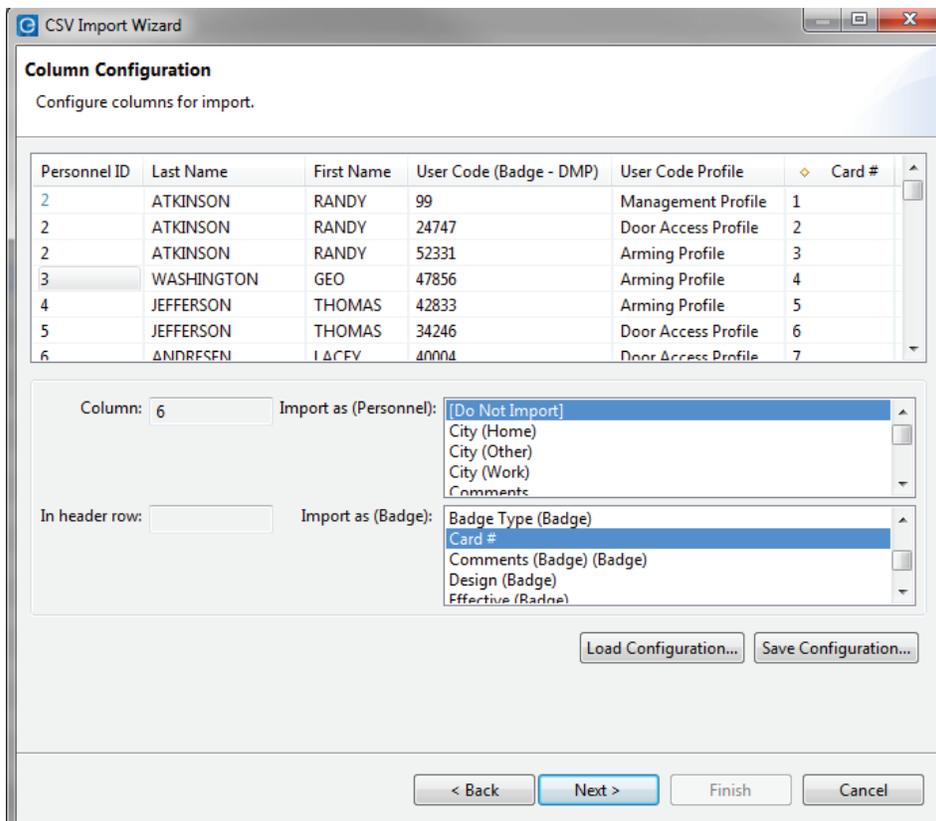
‣ Once all columns and tables are matched, select **Next** to continue.

‣ Personnel photos can be imported. Each photo must be in a JPG format. The CSV field that is assigned to the Entré database **Photo** field must contain the name of the photo file. In **Windows**, if a fully qualified path is not specified in the CSV field (For example: "c:\photos\123456789.jpg") then the location of the photos will be assumed to be on the desktop (For example: "C:\Documents and Settings\Desktop\123456789.jpg").

5. The next screen of the CSV Import Wizard displays the **New Records**, **Updated Records**, and **Invalid Records** shown below.
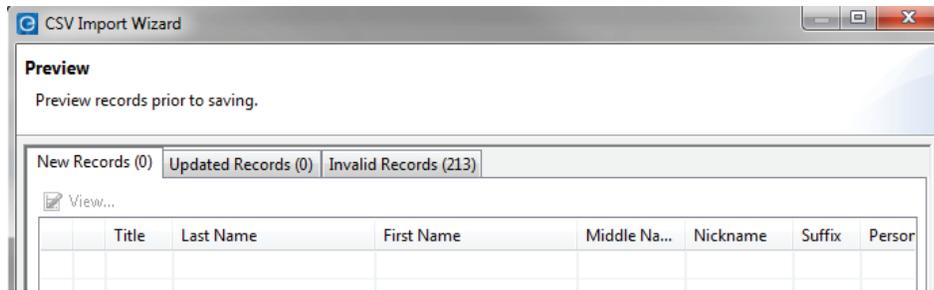
6. Each personnel record in the **New Records** and **Updated Records** has a checkbox associated with it. Uncheck this box to remove the personnel record from the import. A **View** is also provided to view the details of the imported personnel. If necessary, use the **Back** button to make changes as needed.

7. The **Invalid Records** tab displays all personnel records unable to import. A description of why the import failed for these individuals is also listed. An **Export** button is included to save the invalid records to a CSV file allowing for an operator to modify the invalid records and try the CSV import again.

8. Click the **Finish** button to complete the import and add the **Personnel Records** to the system.

CONFIGURE PERSONNEL AND USERS

Configure Departments

1. Go to **Management** > **Departments**.

2. Select **Add**.

3. Name the department.

4. Configure **Comments** and **Partition** as needed.

5. Select **Save and Close**.

Configure Organizations

1. Go to **Management** > **Organizations**.

2. Select **Add**.

3. Name the organization.

4. Configure **Comments** and **Partition** as needed.

5. Select **Save and Close**.

Add Organizations to Personnel

Add organizations and departments to personnel records.

1. Go to **Management** > **Personnel**.

2. Right-click a personnel record and select **Edit**.

3. Select **Occupational**, then select the personnel's associated **Organization** and then **Department**. Organization must be selected before Department.

4. Select **Save and Close**.

Enroll Personnel

The Personnel module allows operators to manage personnel records. Personnel records contain information regarding the site's personnel, general employees, contractors, and visitors. A personnel record may have associated credentials, such as badges or logins.

Use an Existing Photo

1. Go to **Management** > **Personnel**.

2. Select **Add**.

3. Enter information into the following required fields:

   ‣ **First name**
   ‣ **Last name**
   ‣ **SSN/FIN/ID**

4. Select **Import**, select the image, then select **OK**.

5. To preview the photo, select **Next**.

6. Select **Finish**.

Use a Photo from Image Capture

1. Go to **Management** > **Personnel**.

2. Select **Add**.

3. Enter information into the following required fields:

   ‣ **First name**
   ‣ **Last name**
   ‣ **SSN/FIN/ID**

4. Select **Capture**. Use the built-in tools to pan, tilt, and zoom to the appropriate location. Once satisfied with the camera settings, select **Capture** to take a picture. A preview of the picture will be displayed.

5. To retake the photo, select **Capture**.

6. Select **Save**.

7. Highlight the image location to be saved in the personnel record.

8. To preview the photo, select **Next**.

9. Select **Finish**.

Customize Personnel Records

Custom fields and dates are available on personnel, badge, and device detail windows. These fields can be modified according to the site.

Complete "Customize the User Interface" instructions to create a custom field before following the steps below.

1. Create custom field tabs in **Advanced** > **Custom Field Tab**.

2. Go to **Configuration** > **System Configuration** > **Personnel**.

3. Select the following options:
   ‣ **Use single-screen personnel wizard**
   ‣ **Use CSV personnel import wizard**

4. To allow custom personnel fields to be used in the personnel wizard, select **Use custom fields on personnel wizard**.

5. Go to **Configuration** > **System Configuration** > **Personnel - Custom**.

6. In **Personnel - Custom**, select a custom field or date.

7. To display the selected field in the application, select **Enabled**.

8. To manage custom fields with a dropdown menu, select **Drop-down**.

9. Edit the name of the **Column** header and **Form** label. The column header is displayed in the data type of the operator profile. The **Form** label is displayed on the detail window of personnel records.

10. Select **Save**, then log out of Entré and log back in..

11. Go to **Management** > **Personnel**.

12. Double-click a personnel record.

13. Go to a personnel record and verify that the edited **Custom Personnel Fields** are displayed in the personnel detail window.

Edit Personnel Records

1. Go to **Management** > **Personnel**.

2. To filter results, select **Filter**. Select **OK** to update the **Personnel** module.

3. To group personnel records, go to **Group Edit** > **Group Edit All Items**.

4. Edit information in the **General**, **Occupational**, or custom sections as needed.

5. Select **OK**. A dialog pops up to display the number of personnel records that were processed or affected.

Import Personnel and Badges

This section describes how to import and/or update personnel records using a Comma Separated Value (CSV) file and the CSV Import Wizard within Entré. To import personnel and badges with the CSV Import Wizard, complete the following steps.

Enable the Personnel Import Wizard

1. Go to **Configuration** > **System Configuration** > **Personnel**.

2. Select **Use CSV personnel import wizard**, then select **Save**.

3. Log out of Entré and log back in.

Import the Personnel and Badge Files

See "Import Personnel Using CSV Import" for more information.

1. Go to **Management** > **Personnel**.

2. Go to **Add** > **CSV Import Wizard**.

3. Select **Browse**. If the CSV file has a header row, ensure **File has a header row** is selected. Open the CSV file, then select **Next**.

4. To import data from specific CSV fields into corresponding columns from the Entré database, select a field in Import as and assign it to the correct column. The following columns are required: **Last name**, **First name**, and **Personnel ID**. To exclude columns, select **Do Not Import**.

5. To import photos, ensure files are in .jpg format. The location of the photo must be a fully qualified path such as *C:\Pictures\JohnSmith01.jpg*.

6. To import multiple badges per personnel record, the name field must match for each badge being imported. For example, if "John Smith" has two badges, his name is listed twice, once for each badge.

7. Select **Next**. The first 500 records will be organized into the following sections: **New Records**, **Updated Records**, and **Invalid Records**. To remove a personnel record from the import, clear the checkbox next to the personnel record. To fix invalid records in an editor before attempting to import them, go to **Invalid Records** and select **Export**.

8. Select **Finish**.

Assign Badges

Add a badge to a personnel record in the Personnel module.

1. Go to **Badges** and select **Add**.

2. Enter the **Card #** and **User Code**, as well as any other relevant information.

3. Ensure that the validity is **Active**. A validity of **Active** ensures that the badge is functional in the Access Control system. Any other validity, including **Destroyed**, **Inactive**, **Lost**, and **Stolen** will cause the badge to be denied access. Select **Save and Close**.

4. Select **Save and Close**.

Set Up Chroma Key

Chroma key is a visual effects technique used to replace backgrounds in images. Entré has chroma key capabilities which are used for processing personnel identification images.

1. Go to **Configuration** > **System Configuration** > **Image Processing**.

2. Select the appropriate chroma-key checkboxes and complete the related fields. If using chroma-key for signature images, select a **Signature Background Color** that corresponds to the screen color being used. Color fields use the hexadecimal color system. For example, white (R 255, G 255, Bb 255) is represented as #ffffff.

3. Select **Save**.

4. Log out of Entré and log back in.

5. To verify that chroma key was configured successfully, go to the **Personnel** module, select a personnel record to edit, and add an image. In the image preview, the background of the personnel image should be removed.

Set a User Code Profile

Configure a user code profile in the User Code Profile module.

1. Go to **Management** > **User Code Profile**.

2. Select **Add**.

3. Name the user code profile.

4. The new user code profile is turned on by default.

5. Select the options that you want to apply to the profile.

6. Select **Access areas** and **Arm and Disarm** areas as needed. To enable Arm and Disarm areas, go to **Properties** and select **Arm and Disarm**.

7. If necessary, add an **Output Group** to the user code profile.

8. Select **Save and Close**.

9. To assign the profile to badges, go to the **Badges** or **Personnel** module.

Add Privileges to User Code Profiles

Add privileges to a badge in the **Personnel** module.

In **Privileges**, select the options that you want each authority level to access, then select **Save and Close**.

Create Restricted Profiles

Create profiles with restricted permissions and assign them to logins.

In the following examples, we'll make two restricted profiles:

- A restricted profile with badge privileges only
- A restricted profile that has access to items associated with event and alarm activities

Create a Profile for Badge Privileges

Creating a profile with permissions limited to badge privileges ensures that the operator can only view and manipulate certain features of the Entré system.

Create a Profile from a Template

1. Go to **Configuration** > **Operator Profiles**.

2. Select **Add**.

3. In **Template**, select **Most restrictive**, then select **OK**.

4. Name the profile.

5. Ensure that **Enabled** is selected.

Configure the General Tab

1. Select **Events/Alarms**.

2. Deselect **Open Alarms Module**.

3. In **Help**, select the **Allow access to help documentation** and **Allow access to help PDF**.

Configure the Module tab

1. Go to **Monitoring** > **Events**.

2. Select **Allow access to module**. You can filter the type of events the profile can view by selecting **Default Filter**.

3. Go to **Management** > **Badges**.

4. Select **Allow access to module**.

5. In **Personnel**, select **Allow access to module**.

6. In **Audit Trail**, select **Allow access to module**.

7. Go to **Configuration** > **Access Levels**.

8. Select **Allow access to module**.

Configure the Data Types Tab

1. Expand the **Data Types** tree.

2. In **Access Level**, select **View**.

3. In **Badge**, select **View**, **Create**, **Modify**, and **Delete**. This will grant the profile full access to the Badges module.

4. In **Event**, select **View**.

5. In **Personnel Record**, select **View**, **Create**, **Modify**, and **Delete**. This will grant the profile full access to the Personnel Module.

6. Select **Save and Close**.

Create a Login for the Badge Privileges Profile

1. Go to **Configuration** > **Operators**.

2. Select **Add**.

3. Name the login and enter a password.

4. In **Profiles**, select the profile created for Badge Privileges access.

5. Select **Save and Close**.

6. To test the profile, log out of Entré, then log back in with the new profile.

Create a Profile for Events and Alarms

Create a profile that is only allowed to view events and alarms.

1. Go to **Configuration** > **Operator Profiles**.

2. Select **Add**.

3. In **Template**, select **Most restrictive**, then select **OK**.

4. Name the profile.

5. Ensure that the **Enabled** checkbox is selected.

Configure the General Section

1. In **Events/Alarms**, select the following options:

   ‣ **Allow annotations**

   ‣ **Allow multiple annotations**

   ‣ **Require comment on clearing alarms, if applicable.**

   ‣ **Open Alarms Module**

   ‣ **Open Manage Alarms window**

   ‣ **Open map**

   ‣ **Show recorded video**

   ‣ **Show live video**

   ‣ **Show camera grid**

2. In **Help**, then select the following options:

   ‣ Allow access to help documentation

   ‣ Allow access to help PDF

Configure the Module Section

1. In **Alarms**, select **Allow access to module**.

2. In **Event Photos**, select **Allow access to module**.

3. In **Events**, select **Allow access to module**.

4. In **Maps**, select **Allow access to module**.

5. Expand the **Device Status** tree, select each device the profile should have access to, then select **Allow access to module**.

6. Go to **Management** > **Personnel** and select **Allow access to module**.

7. In **Audit Trail**, select **Allow access to module**.

8. In **Reports** and check the following:

   ‣ **Allow access to module**

   ‣ **Allow execution of SQL-based reports**

9. Go to **Configuration** > **Event Policies** and select **Allow access to module**.

Configure the Data Types Section

1. Expand the **Data Types** tree, then select **Device**. Select **View**.

2. In **Event**, select **View**.

3. In **Event Policy**, select **View**.

4. In **Personnel Record**, select **View**.

5. In **Report**, select **View** and **Create**.

6. Select **Save and Close**.

Create a Login for the Events/Alarms Profile

1. Go to **Configuration** > **Operators**.

2. Select **Add Name**, name the login, and enter a password.

3. In **Profiles**, select the profile created for Event and Alarms access.

4. Select **Save and Close**.

5. To test the profile, log out of Entré, then log back in with the new profile.

Create an Operator Login and Profile

In order to create a new operator login, use an existing profile or create a new profile. Profiles determine an operator's access to the Entré application.

1. Go to **Configuration** > **Operator Profiles**.

2. Select **Add**. Select one of the following templates:

   ‣ **Most Restrictive:** Allows only restricted use of the application. It does not allow access to any modules and does not allow to change passwords.

   ‣ **Least Restrictive:** Allows almost unlimited use of the application. It allows access to all the modules and allows the profile to change passwords. This option is recommended for new profiles.

   ‣ **Default:** Gives minor use of the application. The profile is allowed to change the password, but it does not have access to any modules.

3. Select **OK**.

4. Enter a profile name, then select each module that the profile should have permission to access.

5. Select **Allow access to the application**, then select **Save and Close**.

6. Go to **Configuration** > **Operators**.

7. Select **Add**, then complete the following required fields:

   ‣ **Username**

   ‣ **Password**

   ‣ **Confirm password**

8. In **Assigned to**, select **Select** and assign the login to a personnel record.

9. To assign privileges to the login, go to **Profiles**.

10. Select the profile with the appropriate permissions for the operator. An operator can be assigned more than one location.

11. Select **Save and Close**.

12. To verify changes and operator permissions, log out of Entré, then log in as the new operator.

Sync User Removal with Profile Removal

To ensure that the personnel or user is removed when the associated profile or areas are removed, see the following steps.

1. Go to the **System Configuration** module.

2. Go to the **DMP Communication** menu item.

3. Select **Remove user from panel**.

4. Select **Save**.

5. Log out of Entré and log back in.

CONFIGURE BADGES

Design a Badge

The graphic design editor is located in the Badge Designer module. The editor enables you to create and manage badge designs.

1. Go to **Configuration** > **Badge Designer**.

2. Select **Add** and name the design.

3. In **Format**, select whether the design will be single-sided or double-sided. For this example, select **Single sided**.

4. Choose the design's **Orientation**. For this example, choose **Portrait**.

5. Specify the **Card size** and select **OK**. The following tools are available from the top of the Badge Design Editor:
   - Display current color
   - Selection tool
   - Shapes: Rectangle, Circle, Ellipse, Line, Polygon
   - Polyline
   - Add Text and Image
   - Quadratic and Cubic Bezier curve
   - Color picker
   - Add Image and Text Links
   - Show properties and resources

6. Use the tools and customize a badge design.

7. To add a logo to the badge template, select **Image**. Drag a rectangle selection over the location for the logo. Browse and select a .jpg, .png, or .svg file. To move the logo, drag a rectangle selection over the new location.

8. To add a dynamic text field, select the Text Link tool, then drag a rectangle selection over the location for the text. To configure the text link properties, go to the toolbar and select **Show properties**.

9. In **Property**, select a pre-configured badge property to display on the badge. From the second drop-down field, select the display format. For this example, select: **Last Name**, **First Name**, **Uppercase**. Use **Properties** to configure the text as needed.

10. Close the window by selecting the Close Window icon.

11. To add a signature or a personnel photo to the badge template, select **Image Link**, then drag a rectangle selection over the location for the image. Select **Show properties from the toolbar**, select an image type, then use **Properties** to configure the image as needed.

12. Go to **File** > **Save All**.

13. To exit the **Badge Design Editor**, select the Close Window icon.

Create a Badge Template

Create badge templates in the Badge Templates module.

1. Go to **Advanced** > **Badge Templates**.

2. Select **Add**.

3. Name the template, select a **Partition**, if any, then select **Edit Template**.

4. Configure the template accordingly.

5. Select **OK**.

6. Select **Save and Close**.

Use a Badge Template

Use a badge template to create a streamlined look across a company or organization.

1. Go to **Management** > **Badges**.

2. Select **Add**.

3. Select a template and select **OK**.

4. Make changes as needed.

5. Select **Save and Close**.

Add a Badge

The Badges module allows operators to manage all badges. Generally, the Personnel module is the preferred module for editing badge data. The Badges module is intended for specialized purposes, such as viewing or assigning unassigned badges. Multiple badges can be added to each personnel record.

1. Go to **Management** > **Badges**.

2. Select **Add**.

3. Select a badge template, then select **OK**. Complete the following required fields:
   ‣ **Card #**
   ‣ **Assigned to**: Browse personnel and assign the badge.
   ‣ **User Code**

4. Ensure that the validity is **Active**. A validity of Active ensures that the badge is functional in the Access Control system.
   ‣ **Effective Time**: Initiates at **00:00**.
   ‣ **Expires Time**: Terminates at **23:59**. To configure an activate/deactivate schedule for the badge, enter a date and time in the **Effective** and **Expires** fields. The badge will activate/deactivate accordingly.

5. To assign a user code profile to the badge, check the box next to the user code profiles in **Privileges** and the **User Code Profiles** tab.

6. Select **Save and Close** to save the badge configuration.

Assign a Badge to a Personnel

Follow these steps to add a badge to an existing personnel record.

1. Go to **Management** > **Personnel**.

2. Locate the personnel that will be updated. You can use the Search field.

3. Double-click the personnel or highlight the record, and select **Single-Screen Wizard** from the Edit drop-down menu.

4. In **Credentials**, open the **Add** drop-down menu and select **Single-Screen Wizard**.

5. Assign a **Card #** and **User Code** to the credential.

Note: In **User Code**, you can manually add or generate a user code. Type in a number for the user code you would like to assign. Do not enter a user code already assigned to another user. The system warns you if you attempt to do so.

6. For TMSentry panels, you can select the following user authority level permissions:

   ‣ **Master**: The highest authority level. The user is granted all system permissions.
   ‣ **Arm Only**: The user can only arm the system.
   ‣ **Temp Code**: Codes set up remotely can stay active for up to 7 days, then automatically expire. Codes active for more than 7 days can be set up only with the keypad. Any authority level except Master can be defined as a temporary code.

Note: If no authority level is selected, the user is set to Standard.

7. Assign a **User Code Profile** to this badge in **Privileges** and the **User Code Profiles** tab.

8. Click **Save and Close** on both open windows.

Note: If the same badge is used for an XR550 and TMSentry system, and the user code is five or more digits, only the first four numbers are sent to the TMSentry panel. If the code is less than four digits, zeroes are automatically added to the beginning of the code to make it four digits. Entré checks for duplicate codes.

Edit Badge Information

Update badge information when personnel changes occur or to correct errors as needed.

1. Double-click a badge in the **Badges** module.

2. To modify the card number of a pre-existing badge, go to **Configuration** > **System Configuration**.

3. Edit badge information as needed.

4. Open **Badges**, select **Allow card # to be changed after creation**, then select **Save**.

5. Log out of Entré and log back in.

Add Effective or Expiration Times for Badges

Effective/Expiration times allow the validity of badges to be determined by a start and end time and date. The following instructions are intended for a system administrator.

1. Go to **Configuration** > **System Configuration** > **Badges**.

2. Allow effective/expiration times to be configured for badges by selecting the following options:

   ‣ **Use effective times for badges:** Defines whether or not badges are configured with effective time constraints.

   ‣ **Use expiration times for badges:** Defines whether or not badges are configured with expiration time constraints.

3. Select **Save**.

4. Log out of Entré and log back in.

Badge Status

The current status of the badge is called the validity. A badge can be in one of five validity states.

- **Active**: Must be set to this value for access to be granted.
- **Inactive**: Will be denied access to any access point in system.
- **Lost**: Will be denied access to any access point in system.
- **Stolen**: Will be denied access to any access point in system.
- **Destroyed**: Will be denied access to any access point in system.

Edit Badge Group

1. Go to **Management** > **Badges**.

2. To filter results, select **Filter**. Select **OK** to update the Personnel module.

3. To group edit badges, go to **Group Edit** > **Group Edit All Items**.

4. Edit information in **General**, **Badge Printing**, **Access Level Groups**, **User Code Profiles**, or **Advanced** as needed.

5. Select **OK**. A dialog pops up to display the number of badges that were processed or affected.

Configure Badges to Allow Null Pin

Badges can be added without a PIN requirement.

1. Go to **Configuration** > **System Configuration** > **Badges**.

2. Select **Allow null PIN**, then select **Save**.

3. Log out of Entré and log back in. Once the application has been restarted, badges can be added without a PIN.

Customize Text Links

Create and customize a dynamic text link in the Badge Designer module.

1. In **Text Link Properties**, select **Custom Text Link**, then select the More icon.

2. To configure the text, choose an entry from the **Description** field, then select **Add Variable**. The value will be coded into the link and a sample will be displayed in **Exselection result** with sample values.

3. To add a space between values, select the **Add Space** button.

4. To add custom static text to the string, select Add Text, enter the text, then select OK.

5. To delete text or rearrange the order, select the text value from the List view field on the upper, left side of the window, then use the **Up**, **Down**, or **Delete** buttons as needed.

6. Select **OK**.

7. Edit other badge design settings as needed.

8. Select **Save All**.

Delete a Badge or Credential

Follow these steps to remove an existing badge or personnel credential from the system.

1. Go to **Management** > **Badges**.

2. Locate the badge that will be updated. You can use the **Search** field.

3. Right-click the badge and select **Delete**.

4. If the personnel record is also no longer needed, the record should be deleted. See "Delete Personnel with a Badge".

5. After deleting your badge or credential, verify your changes. See "Verify that Badge Changes Were Sent".

Delete Personnel with a Badge

Delete all credentials assigned to a person at the time of deleting the person.

1. Right-click the Personnel record.

2. Select **Delete** to present a list of badges and/or key fobs attached to the personnel.

3. Select **OK** to delete both or **Cancel** to close the message window.

4. After deleting your badge or credential, verify your changes. See "Verify that Badge Changes Were Sent".

Verify that Badge Changes Were Sent

After you add or remove a badge or credential, verify that your changes were sent.

1. Go to **Monitoring** > **Events**.

2. Open the **Filter** drop-down menu, hover over **Presets**, and then select **Credential Changes**.

3. Depending on the system message, follow the steps below:

    ‣ If the events show a **Remote programming complete** system message, the user code changes have been sent to the panel. Compare the name in Device Column to the name of the panel to confirm.

    ‣ If the events show a **User Code Sync Failure** or **Panel offline: Communication failure** system message, there is a communication problem between Entré and the panel. You will need to restart the panel to resolve the issue.

        a. Go to **Configuration** > **Hardware Tree**.

        b. Locate the panel to which the codes are being sent.

        c. If the panel shows as offline, right-click the panel, select **Panel Control**, and then select **Start**.
           If the panel shows as online, right-click the panel, select **Panel Control**, and then select **Restart**.

        d. If the panel starts and shows as online, the codes will be sent and the **Remote programming complete** message will display in the **Events** module.

        If the panel will not start or show as online, refer to the You can also contact your IT department for further assistance. Do not attempt to manually download configuration to the panel. This will cause users to be duplicated in the panel.

Troubleshooting Flow Chart

Panel is "Offline" in the Hardware Tree.

1. Right-click the panel.
2. Select **Panel Control**.
3. Select **Start**.

Is the panel online?

Yes → Continue with panel and user configuration.

No → Can Remote Link connect to the panel on port 2011?

No → Contact IT for further assistance.

Yes →

XR100/XR500 or XR150/XR550?

XR150/XR550 → Is the panel in alarm?

Yes → Disarm panel from Remote Link. Try to bring panel online in Entré.

No →

XR100/XR500 →

Are events from the panel showing up in Entré?

Yes → Contact IT for further assistance.

No →

Is the Entré information in Remote Link correct?

Yes →

No → Update any incorrect information. Try to bring panel online in Entré.

Does the Remote Link account # match the Entré account #?

Yes →

No → Update any incorrect information. Try to bring panel online in Entré.

Is there an Entré Passphrase in Remote Options?

Yes → Does the passphrase in Remote Options match the passphrase in Entré?

No →

Yes → Update any incorrect information. Try to bring panel online in Entré.

No →

Do any other panels have the same account #?

Yes → Update any incorrect information. Try to bring panel online in Entré.

No → Contact IT for further assistance.

Set Up Automatic Badge Disabler

These steps can be performed by someone with knowledge of Active Directory, however they might need assistance from a system administrator.

Set Up Active Directory

1. Copy and paste the files so the directory is **C:\Program Files\DMP\Entre\Entre.ActiveDirectory**.

2. Double-click **Entre.ActiveDirectory\Entre.ActiveDirectory.UserInterface\bin\Release\UserInterface.exe**. This is used to configure the service before it is installed.

3. Fill out the form:

    ‣ **Output File Path**: This will later be used by the Entré automation rule to disable the users.

    ‣ **Active Directory**:

        a. **User Name** and **Password** contain the credentials of the system admin which the service will use to query Active Directory.

        b. **Domain** contains the domain controller of Active Directory prefixed with **LDAP://**.

        c. **Match Field** contains the name of the field used by the service to query Active Directory. The value in Match Field links to the value of the Entré Active Directory Key.

    ‣ **Database**:

        a. **User Name** and **Password** contain the credentials used to access the Entré SQL database.

        b. **Server** contains the IP address of the Entré database.

        c. Leave **Instance** blank. If you are using more than on instance on the SQL server, you may enter the correct instance for your application.

        d. **Database** contains the name of the Entré database.

4. Select **Save**.

5. To install the service:

    ‣ In **Entre.ActiveDirectory**, go to **Entre.ActiveDirectory.WindowsService** > **bin** > **Release**.

    ‣ Right-click **EntreActiveDirectory-InstallService.bat** and select **Run as administrator**.

    ‣ Enter your admin credentials.

6. Run the service:

    ‣ In **Entre.ActiveDirectory**, go to **Entre.ActiveDirectory.WindowsService** > **bin** > **Release**.

    ‣ Right-click **EntreActiveDirectory-RunService.bat** and select **Run as administrator**.

    ‣ Enter your admin credentials. The service queries the Entré database for active users with a populated Active Directory Key. It will then query active directory for disabled accounts, and look for matches against the Active Directory Key, in this case samaccountname. If any matches are found, they are written to the **Output File Path**, **usersToDisable.csv**, and **application.log**. The service is configured to poll Active Directory and Entré database every 30 seconds. You can change the configuration in: **Entre.ActiveDirectory** > **Entre.ActiveDirectory. WindowsService** > **App.config <add key="Polling_Interval_Milliseconds" value="30000" />**.

7. Log out of Entré and log back in..

Test the Active Directory Connection

1. Create a user with a badge in Entré for testing. See "Enroll Personnel", "Add a Badge", "Assign a Badge to a Personnel", or other related topics as needed.

2. In **Edit - Personnel Record**, update the Active Directory Key for the test user. Once the service polls Active Directory and the Entré database again, the service will write any matches to **usersToDisable.csv**.

3. Create and run **Automation Rule** in Entré. This will read in the file **usersToDisable.csv** and the associated **csv.import.properties** file to disable the user in Entré. The users in the CSV file will be disabled.

Assign a Temporary Badge

Assign temporary badges to personnel who need access to an area for only a specific length of time. There are three types of badges: **Visitor**, **Temporary**, and **Standard**.

1. Go to **Management** > **Personnel**.

2. Double-click a personnel row.

3. Select **Badges**, then select **Assign Temporary**.

4. Select the pre-existing badge that will be replaced with a temporary badge. This process enables the temporary badge to adopt the selected badge's access level privileges. Select **Next**.

5. Select a temporary badge, then select **Next**.

6. In **Changes to be Applied**, select each option that corresponds to the configuration changes to be applied to both the personnel's regular badge and the temporary badge. The temporary badge's **Expiration date assignment** will expire at 23:59 (11:59 PM) on the specified day.

7. To preview the personnel's regular badge configuration, select **Next**. Edit information as needed.

8. To preview the temporary badge configuration, select **Next**. Make any final modifications as needed, then select **Finish**.

9. Select **Save and Close**.

Return a Temporary Badge

The Personnel and Badges modules have the ability to return temporary badges.

1. Go to **Management** > **Badges or Management** > **Personnel**.

   ‣ If using the **Badges** module, configure it to allow temporary badges to be returned.

      a. Go to **Configuration** > **System Configuration**.

      b. Select **Badges**.

      c. Select **Show return temporary badge in badges module**.

      d. Select **Save**, then restart Entré.

2. From either module, select **Return Badge from the toolbar**.

3. Follow the wizard's instructions to return the temporary badge and reactivate the personnel's regular badge.

Set Up Badge Printing

Use **Badge Printers** to enable badge printing.

1. Go to **Edit** > **Preferences** > **Badge Printers**.

2. In **Configurations**, select **Add**.

3. Select a printer and select **Print**. In Page Setup, configure the printer, then select **OK**.

4. Name the setting and select **OK**. The printer configuration will be added to Configurations.

5. Select the printer and select **OK**.

6. Log out of Entré and log back in.

7. Go to **Management** > **Badges** and select an existing badge or add a new badge to be printed.

8. Select **Badge Printing**.

9. Select a design for the badge, then select **Print**.

10. A dialog pops up to configure the default printer. To continue badge printing, select **Yes**.

11. In **Select print configuration**, select the printer.

12. To initialize printing, select **OK**.

Print a Badge

Badges for personnel are printed from the Badges module. During the design process or for testing, badge templates may be printed in the Badge Designer module without personnel information.

To print a badge, a badge template must have already been created in the Badge Designer module.

1. Go to **Management** > **Personnel**.

2. Double-click a personnel record.

3. Go to **Badges** and double-click a badge.

4. In **Badge Printing**, select the desired badge template.

5. Select **Print**.

6. Select a valid badge printer and select **OK**.

Print Badges in Batches

Batch printing is used to print multiple badges at one time. To setup batch printing it must first be enabled according to your software license. Contact your DMP dealer or representative for more information.

1. Go to **Configuration** > **System Configuration** > **Badge Printing**.

2. Ensure **Disable batch badge printing** is deselected.

3. Log out of Entré and log back in.

4. Go to **Management** > **Badges**.

5. Select multiple badges from the modules and select **Print Selected Items**.

6. To view batch printing history, go to **Advanced** > **Batch Badge Printing**.

Assign Key Fobs to Badges

In Entré NOC, you can assign key fobs to badges.

Assign Key Fobs to Badges

1. Go to **Management** > **Key Fobs**.

2. Select **Add**.

3. Select **Choose**. Enter a first or last name in the search box for a user that currently exists in the system.

4. Select **Find**.

5. Double-click on the personnel row that generates from the search.

6. In **Badges**, select the badge to assign to the key fob. Select **Save and Close**. The key fob is now assigned to the credential of the user.

Program Outputs on the Key Fob

1. Select the number of buttons to be programmed on the key fob.

2. Select an action for the button to perform. When you do so, additional fields will generate which allow you to choose the areas, outputs, or systems you want to target.

3. If applicable, program the select time as **Short** or **Long**.

4. To the right of the generated text fields, select **Choose** to assign the areas, outputs, or systems you want to target.

5. Choose the area, outputs, or systems you want the button to control. Select **OK**.

6. Continue to program the additional buttons using the sections, as applicable. When you are finished, select **Save and Close**.

Additional details

You have the following options in the **Add - Key Fob Control** window:

- **Serial Number**: All key fob numbers begin with 05.
- **Key Fob Number**: Enter a key fob number between 400-449.
- **Number of buttons**: Program 1, 2, or 4 buttons on a key fob.
- **Supervision Time**: Choose None, 60, or 240 minutes.

Edit a Key Fob

Editing an existing key fob and saving would remove the key fob from the panel. To keep existing key fobs in the panels, follow the steps below.

1. Create a **User Code Profile** for the panel.

2. Add at least 1 **Arm/Disarm Area**.

3. Assign the **User Code Profile** to a **Badge**.

4. Assign the **Badge** to a **Key Fob**.

5. Edit the **Key Fob** to include **Systems**, **Outputs**, and/or **Areas**.

6. Click **Save and Close** to update the key fob in the panel.

Since the key fob was previously sent to the panel based on access areas, the key fob number is in use and should not create a duplicate key fob in the panel.

Key Fob CSV Import

This feature allows key fobs to be imported into Entré with the **CSV Import** tool, which can be found in **Automation Rules**. Badges and personnel must be created before importing the key fob so Entré can use the user number associated with the badge.

You may have more than one key fob assigned to a person and it may be assigned to more than one panel. The buttons will function the same across each panel, but different outputs and areas may be selected.

The Prox in the key fob is added as a badge in the **Badge** module.

Key fob programming allows for 1, 2, or 4 buttons. These buttons can perform arming, disarming, toggle arm/disarm, panel status, panic, 2-button panic, emergency, 2-button emergency, trigger outputs, and sensor reset.

Key fobs are attached to panels through the personnel's badge which is assigned a user code profile. The user code profile must contain at least 1 arm/disarm area for the panel it is assigned to. This is how Entré filters the systems, areas, and outputs to be selected when programming the key fob's buttons. Key fobs will only send to panels with programmed buttons.

📝 **Note:** In previous versions of Entré, key fobs were automatically sent to the panel based on arm/disarm areas and access areas in the user code profile regardless of button programming. This assigned key fob numbers in panels that were not going to arm/disarm areas or have panics assigned to them.

The CSV file will have corresponding columns for each key fob option. The **keyfob.csv.import.properties** file and **sample_key_fob.csv** file can be found in the Entré **\sampledata** folder. This is a file containing the headings and order for the CSV import which is needed to set up the import.

To set up the CSV file, follow the guidelines below:

- Each key fob needs its own row
- Each panel a key fob is assigned to needs its own row
- Key fob supervision can be **0**, **60**, or **240** minutes
- Valid serial numbers are **05000000** - **05999999**

Key fob button options include:

- Arming (Specify select time and select areas)
- Disarming (Specify select time and select areas)
- Toggle Arm/Disarm (Specify select time and select areas)
- Status (Specify select time and select systems)
- Panic (Select systems and assign output with output action)
- Panic 2 Btn (Select systems and assign output with output action) MUST HAVE 2 PANIC BUTTONS
- Emergency (Select systems and assign output with output action)
- Emergency 2 Btn (Select systems and assign output with output action) MUST HAVE 2 EMERGENCY BUTTONS
- Output (Specify select time and assign output with output action)
- Sensor Reset (Specify select time and select systems)

Adding Key Fobs Using an Automation Rule for CSV Import

1. Navigate to **Automation Rules** and add a new **Automation Rule**.
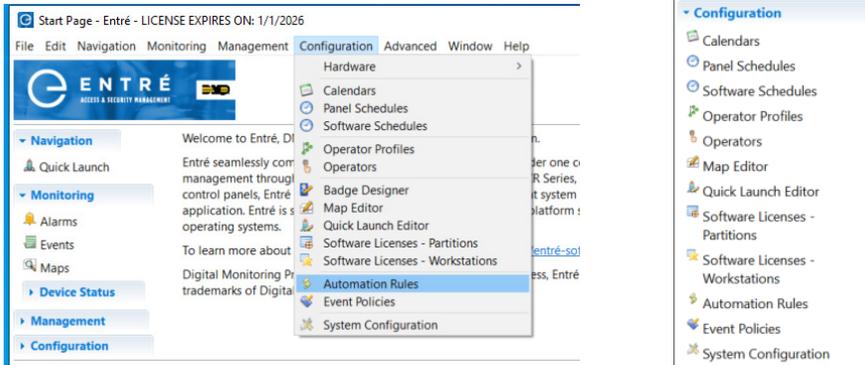
2. Add a **Name** and **Trigger**. At **Action**, click **Add** and select **CSV Import**. Then, select **Key Fobs**.
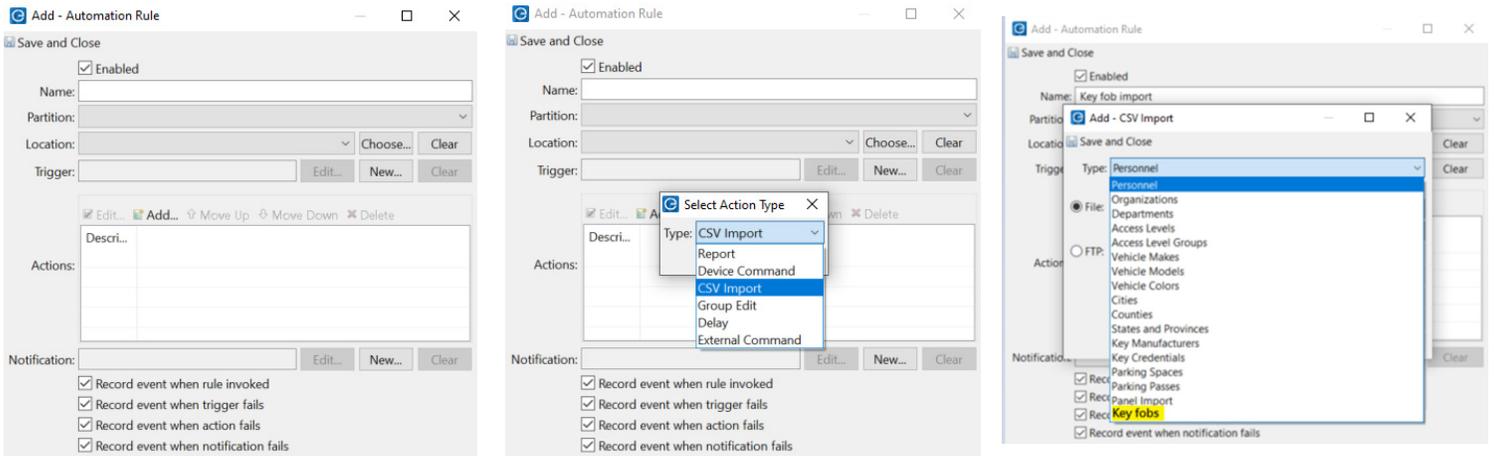
3. Enter the location of the key fob's CSV and **keyfob.csv.import.properties** files. Do not include the file name in the directory path. The Entré app server needs access to read and write to this directory. Both files need to reside in the same folder. If scheduling the import, ensure the updated CSV is in the same location before the next import is scheduled to occur.
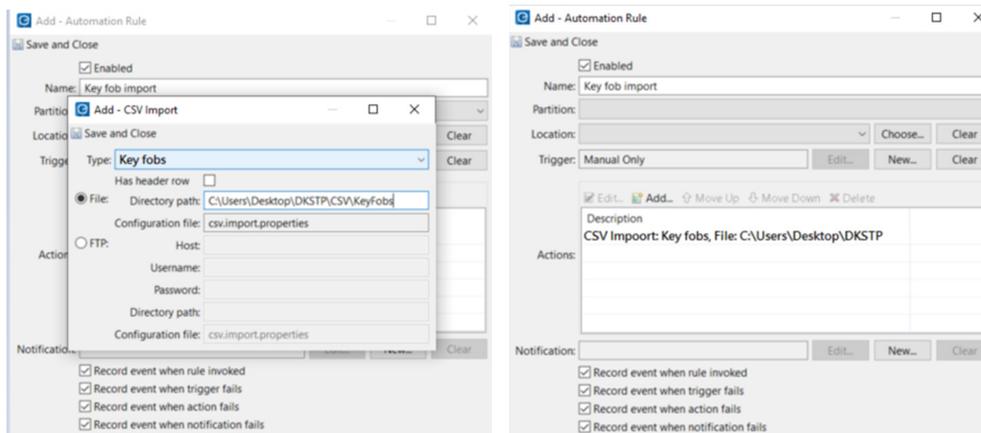
4. Click **Save and Close**. Any fobs that did not meet the requirements for a successful import will be exported to a reject file and corresponding err file. These files can be found in the same folder as the CSV file.

The CSV import uses a combination of key fob zone number, key fob serial number, and the assigned personnel's badge as card number and partition to identify key fobs. If the Entré installation is using partitions and the partition field is left blank, key fobs that are duplicated across partitions will show up causing the CSV file's line to be rejected. The same is true for badges and panels.

Ensure the personnel and badge being assigned to the key fob is active in Entré.

If using a temporary badge for a key fob, delete the key fob when the badge is returned. Reassigning a temporary badge to another person will not assign the key fob to the new person.

Add Rules
- If a key fob with the same combination of zone number, card number, and partition already exist, then the import line will be rejected
- Duplicate key fobs with the same zone number, serial number, and panel will be rejected

Update Rules
- If multiple key fobs with the same combination of zone number, card number, and partition already exist, then the import line will be rejected
- The number of buttons cannot be changed
- **Button Actions** cannot be changed
- **Button Output Action** cannot be changed
- Reassigning key fobs to different badges is not allowed

Delete Rules
- If multiple key fobs with the same combination of zone number, card number, and partition already exist, then the import line will be rejected
- If no account number is given, the key fob will be deleted
- If the account number is given, then all areas, keypads, outputs, output groups, and systems related to that account will be removed from the key fob
  - If the other panel's devices remain on the key fob, the key fob will be saved and only removed from the panel associated with the account number
  - If no devices remain on the key fob, then the key fob will be deleted from Entré

CSV Properties
The CSV properties are:

- KeyfobNumber: This is the zone number that will be assigned to the key fob in the associated panel. Valid values are **400** to **449**.
- SerialNumber: Serial numbers of the key fob. Valid values are 8 numeric characters starting with **05**, e.g. **05111111**.
- SupervisionTime: Supervision Time for the key fob. The valid values are:
  - 0 = None
  - 2 or 60 = 60 minute supervision time
  - 3 or 240 = 240 minute supervision time
- AccountNumber: Account number of the panel to associate the key fob to. If a button action is Emergency, Emergency 2 Btn, Panic, Panic 2 Btn, or Sensor Reset, the panel indicated by the account number will be added as a system for the button.
- Partition: Used to separate database information. Not necessary if not using partitions but is required if using partitions. The partition must match across the personnel, badge, user code profile, and panel. The first character of the function will be used to indicate that action should be taken. The valid values (not case sensitive) are:
  - A or ADD
  - D or DELETE
  - U or UPDATE

- CardNumber: Card number of the associated badge.

- NumberOfButtons: Number of buttons on the key fob. Available buttons are Top, Bottom, Left, Right. The valid values are:

  ‣ 1

  ‣ 2

  ‣ 4

- TopButtonAction: Action to perform when button is selected. The valid values are:

  ‣ UN = UNUSED

  ‣ ARM = ARMING

  ‣ DIS = DISARMING

  ‣ TGL = TOGGLEARMDISARM

  ‣ STA = STATUS

  ‣ PN = PANIC

  ‣ PN2 = PANIC 2 BUTTON (will cause a reject on one button fob)

  ‣ EM = EMERGENCY

  ‣ EM2 = EMERGENCY 2 BTN (will cause a reject on one button fob)

  ‣ OUT = OUTPUT

  ‣ RST = SENSOR RESET

- TopButtonSelect: First character of the string value will be used to indicate what the select time for the button should be. The valid values (not case sensitive) are:

  ‣ 0, S, or SHORT

  ‣ 1, L, or LONG

📝 **Note:** SHORT is not valid for buttons with actions of Panic, Panic 2 Button, Emergency, or Emergency 2 Button. The import tool will change the select time to LONG for those button types.

- TopButtonOutputAction: First character of the string value will be used to indicate what the select time for the button should be. If an action is **Blank**, it will default to **Off**. The valid values (not case sensitive) are:

  ‣ O = OFF

  ‣ M = MOMENTARY

  ‣ P = PULSE

  ‣ S = STEADY

  ‣ T = TOGGLE

📝 **Note:** Door outputs cannot have **PULSE** action. Output Groups cannot have **PULSE** or **TOGGLE** actions.

- TopButtonOutputs: Indicates which output from the panel will be associated with the button. Only one output per panel may be associated. For doors, the format will be **D** followed immediately by the **device number.** For outputs, the format will be **O** followed immediately by the **output number**. For output groups, the format will be **G** followed immediately by the **output group number**.

📝 **Note:** The panel will not trigger AX doors as an output unless added to an output group.

- TopButtonAreas: This is a pipe { | } delimited string. For example, **2|5|15** would associate areas **2**, **5**, and **15** to the panel.

Example of the **keyfob.csv.import.properties**:

KeyfobNumber.column=0

SerialNumber.column=1

SupervisionTime.column=2

AccountNumber.column=3

Partition.column=4

Change.column=5

CardNumber.column=6

NumberOfButtons.column=7

TopButtonAction.column=8

TopButtonSelect.column=9

TopButtonOutputAction.column=10

TopButtonOutputs.column=11

TopButtonAreas.column=12

BottomButtonAction.column=13

BottomButtonSelect.column=14

BottomButtonOutputAction.column=15

BottomButtonOutputs.column=16

BottomButtonAreas.column=17

LeftButtonAction.column=18

LeftButtonSelect.column=19

LeftButtonOutputAction.column=20

LeftButtonOutputs.column=21

LeftButtonAreas.column=22

RightButtonAction.column=23

RightButtonSelect.column=24

RightButtonOutputAction.column=25

RightButtonOutputs.column=26

RightButtonAreas.column=27

Example of CSV key fob file:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Key fob number	Key fob Serial Number	Supervision time	Account Number	Partition	Change	Card Number	Number of Btns	Top Btn Act	Top Btn prs tm	Top Btn output Act	Top Btn Output	Top Btn Area/s	Bott Btn Act
2	400	05005550	0	5550		A	5550	2	TGL	s	s		1|5	PN
3	401	05005551	2	5551		A	5551	1	TGL	l			1|2|13|4|5|6|7|8|9|10|11|12	
4	402	05005552	3	5552		a	5552	4	EM	s			1	DIS
5	409	05099999	0	5550		A	99999	4	PN	l	S	o1		EM
6	409	05099999	0	5551		u	99999	4	PN	l	S	d1		EM

CONFIGURE MORE ADVANCED OPTIONS
—

Using Filters

You can filter most Entré modules. Filters quickly sort through large quantities of items that would be impractical to view simultaneously.

Select the arrow next to Filter to access filter preset options:

- No Filter: Show all items without filtering.
- Default Filter: Display the profile's default view.

Configure an Operator Profile's Default filter

To configure the default filter for operator profiles, complete the following steps.

1. Go to **Configuration** > **Operator Profiles**.

2. Select a profile.

3. Select **Edit**.

4. Go to **Modules** > **Configuration** > **Operator Profiles**.

5. Configure the default filter for operator profiles as needed, then select **OK**.

Configure the Default Filter for Events

To configure the default filter for events, complete the following steps.

1. Go to **Monitoring** > **Events**.

2. Ensure that **Allow access to module** checkbox is selected, then select **Default Filter**.

3. A **Filter** window will open, allowing the operator to configure the following options as desired:

   ‣ **Presets**: Displays preset filtering options. A check mark next to the filter defines whether or not the filter is currently in use.

   ‣ **Preset Manager**: Allows configuration and manage preset filter.

   ‣ **Edit Filter**: View or edit the current filter.

   ‣ **Max. rows**: Specify the maximum number of items (rows) to be displayed for the current table.

4. Select **OK**, then select **Save and Close**.

Filter Events

For this example, we'll create a filter for access denied events within a selected time period.

1. Go to **Monitoring** > **Events** > **Filter**.

2. Select a time period for the filter. In **Window**, select **This month**.

3. Select **Choose**.

4. In **Access**, select **Access Denied**.

5. Select the right arrow to move **Access Denied** to the **Selected items** field.

6. Select **OK**.

7. Select **Device**. In Type, select **Device**.

8. Select **OK** to filter by the criteria selected. The window will close and the table view of the module will be updated to reflect the current filter. All incoming events will be filtered according to the current filter criteria.

Configure the Filter Criteria

When you are editing or viewing a filter, filter criteria can be configured. Select **Filter**, then choose one of the following filter exclusive actions in **General**:

* **View Query**: View and modify the filter SQL query. This feature is intended for advanced operators.

* **Save as Preset**: Save the current filter criteria as a preset for later use. Once a filter is saved as a preset, it may be selected from the **Filter** drop-down.

* **Reset**: Resets the filter to default settings.

Program Templates

To create and program a system with a template, complete the steps in the following sections.

Create a Template from Advanced Tab

1. Go to **Advanced** > **Hardware Wizard Templates**.

2. Select **Add**.

3. Choose the device with programming to save as a template.

4. Name the template.

5. Select **Save**.

Create a Template from the Hardware Tree

1. Go to **Configuration** > **Hardware** > **Hardware Tree**.

2. Right-click the system and select **Save as Wizard Template**.

3. Name the template.

4. Select **Save**.

Program a System with a Template

1. Go to **Configuration** > **Hardware** > **Hardware Tree**.

2. Right-click **DMP Driver** and select **New Panel Wizard from Template**.

3. Select a Template, then select **Next**.

4. Name the device, then select **Next**.

5. Choose appropriate options in **Location**.

6. Select **Finish**.

Create a Hardware Template from Advanced Tab

1. Go to **Configuration** > **Hardware** > **Hardware Tree**.

2. Right-click the system and select **Save as Wizard Template**.

3. Name the template.

4. Select **Save**.

Set Up Locations

Locations are used for facility management using a top-down style that divides objects in the system in accordance to their physical locations. This allows objects to be viewed by their assigned locations (e.g. 1st floor, etc.) rather than by device addresses.

Most data types in Entré have an associated location: devices, events, personnel records, credentials (badge, login), privileges (profile, access level), reports, and badge designs.

Profile access restricts users' ability to view device locations.

Create a Location

1. Go to **Advanced** > **Locations**.

2. Select **Add**. Name the location, then select one of the following types:

   ‣ **Region**

   ‣ **Campus**

   ‣ **Building**

   ‣ **Floor**

   ‣ **Area**

   ‣ **Sub-area**

3. Based on the option chosen, **Parent** displays the hierarchical parents of the selected type. For example, if a **Campus** is selected, the **Parent** only displays **Regions** that the operator has previously configured.

4. Select **Save and Close**.

5. Continue creating locations as needed. Once a hierarchical structure has been created, child locations can be added to each node by right-clicking the location and selecting **Add [Location]**.

Assign a Location to Hardware

1. Go to **Configuration** > **Hardware**.

2. Double-click the device that will be assigned to a location.

3. Go to **Location**, then select a location or select **Choose** to select locations from a hierarchical tree.

4. Select **Save and Close**.

The location associated with an event is generally set to correspond with the location of its device with the following exceptions:

- Any alarm duplicate or annotation has the same location as the original alarm

- Device commands have the location of the target device

- The location seen in the events module is the location associated with the event, not necessarily the location of the device

Bind Profiles to Locations

Locations are assigned using the same process as assigning a profile to a login.

1. Go to **Configuration** > **Operator Profiles**.

2. Double click on the **Operator Profile**.

3. In **Location**, you can assign the location one of two ways.

4. Use the drop-down menu to select the location.

5. Select **Choose**, then select the hierarchical location for profile binding.

6. Select **OK**, then select **Save and Close**.

Manage Partitions

Partitions work by separating objects into autonomous segments. This capability allows various organizations to share the application while maintaining discrete control of their own subsystems. Typically, a system administrator defines which partitions exist in the system, while items created by Entré users default to the partition of the user.

Partitions must be enabled in your software license. Contact your DMP dealer or representative for more information.

Set Up a Partition

1. Go to **Advanced** > **Customers**.

2. Select **Add**.

3. Name the partition and enter comments as needed. The **Partition number** is an automatically generated identification number.

4. Select **Save and Close**.

5. Repeat the preceding steps to create as many partitions as needed.

Assign a Partition to Hardware Devices

1. Go to **Configuration** > **Hardware**.

2. Edit a device, then go to **Location**.

3. In **Partition**, select a partition created in "Set Up a Partition".

Assign Parent Devices to Partitions

The following administrative step assigns parent devices to partitions. When a partitioned user adds items to Entré, the objects are automatically assigned to the user's partition.

1. Go to **Configuration** > **Operator Profiles**.

2. Double-click a profile.

3. Select a partition, complete the profile configuration, then select **Save and Close**.

4. To assign partitions to personnel, go to **Management** > **Personnel**. Double-click a personnel file.

5. Assign the personnel record to a partition.

6. Go to **Logins** and select **Add**.

7. Select the partition and configure the login as desired, then assign the profile to the login. For best results, verify the login and profile have the same partition.

8. Select **Save and Close**.

Assign Badges to a Partition

1. Go to **Management** > **Badges**, then select **Add** for new badge or **Edit** for an existing badge.

2. In **Partition**, select a partition.

3. Select **Save and Close**.

Assign Operators to a Partition

1. Go to **Configuration** > **Operators**.

2. Double click on the operator or click once and press **Edit**.

3. In **Partition**, select a partition.

4. Select **Save and Close**.

The partition associated with an event is generally set to correspond with the partition of its device with the following exceptions:

- Any alarm duplicate or annotation has the same partition as the original alarm.

- Device commands have the partition of the target device.

- Audit records have the partition of the login (not the profile and not the partition of the modified record). The partition seen in the events module is the partition associated with the event, not necessarily the device partition.

Add a Custom Alert Sound

Add customized alerts to Entré.

Add Alert Sounds and Assign them to Log Codes

1. Go to **Advanced** > **Alert Sounds**.

2. Select **Add**.

3. Select **Import WAV File**, then select the desired sound bite.

4. Select **Save and Close**.

Assigned the Alert Sound to a Log Code

1. Go to **Configuration** > **Event Policies**.

2. Select **Add**.

3. In **Alert sound**, select a sound bite to associate with the event policy.

4. Configure the event policy as necessary, then select **Save and Close**.

Add a Credential

Follow these steps to add a new personnel record credential.

1. Go to **Management** > **Personnel**.

2. Open the **Add** drop-down menu and select **Single-Screen Wizard**.

3. Enter the **First name**, **Last name**, **ID#**, and any other relevant information for the user.

4. In **Credentials** and under the **Badges** tab, open the **Add** drop-down menu and select **Single-Screen Wizard**.

5. Assign a **Card #** and **User Code** to the credential.

6. Assign a **User Code Profile** to this badge in **Privileges**.

7. Select **Save and Close** on both open windows.

Create Credential Watch Levels

Create credential watch levels in the Advanced menu.

Enable the Credential Watch Levels Module

If the Credential Watch Levels module is not present in Advanced, complete the below steps. If it is, see "Create Watch Levels".

1. Go to **Configuration** > **System Configuration** > **Miscellaneous**.

2. Select **Enable Credential Watch Levels**.

3. Log out of Entré and log back in.

Create Watch Levels

1. Go to **Advanced** > **Credential Watch Levels**.

2. Select **Add**. Name the watch level and associate it with a color.

3. Select **Save and Close**.

4. Go to **Management** > **Badges**.

5. Select a badge, then select **Edit**.

6. In **Watch level**, select a watch level to associate with the badge.

7. Select **Save and Close** to save the watch level to the selected badge.

8. To edit a credential watch level, double-click the watch level in **Credential Watch Level**. Edit settings accordingly, then select **Save and Close**.

Add and Configure the Historical Events Driver

The **Historical Events Driver** stores historical copies of events in a separate database table. Along with copying events, the Historical Events Driver can purge the copied events from the Events table, resulting in better performance from the table. Since the purged events are copied to a different table, legacy activity can still be reported.

Add and Configure the Historical Events Driver

1. Go to **Configuration** > **Hardware**.

2. Right-click the **Driver Manager** in the hardware tree and select **New Historical Events Driver**.

3. Name the **Historical Events Driver**.

4. Select **Driver** and modify the **Prune live events older than (days)** field to the number of days of live events desired (as configured in the live event table). This section also allows historical events to be truncated. Define the length of time in number of months that a historical event should be saved before it is cleared from the system. For example, entering *3* in the *Permanently delete historical events older than (months)* field means that historical events will remain in the system for three months before it is removed.

5. Select **Save and Close**.

6. Right-click the driver and select **Start**.

Add Automation Rules

Create Historical Event Driver commands that execute through the Automation Driver. For this example, five automation rules will be added.

Copy Live Events

The first automation rule will be configured to copy live events.

1. Go to **Configuration** > **Automation Rules**.

2. Select **Add**.

3. Name the automation rule.

4. Next to **Trigger**, select **New**.

5. Select from **Periodic**, **Event**, **Manual Only**, or **Software Schedule** for the trigger interval.

6. In **Periodic**, go to **Interval** and select **Daily**.

7. Make selections based on the above step.

8. Next to **Actions**, select **Add**.

9. Select **Type**.

10. Make selections based on the above step.

11. Select **OK**.

12. To send notifications, enter the information into **Notification** under **New**.

13. Select **OK**.

14. Select **Save and Close**.

Stop Copying Live Events

The second automation rule will be configured to stop copying live events. To do this, follow the steps as outlined for the first automation rule, however the **Time of day** selected will be the time to stop copying live events and the **Device Command** will be to **Stop Copying Live Events**.

1. Go to **Configuration** > **Automation Rules**.

2. Select **Add**. Name the automation rule (ex. *Stop Copying Live Events)*.

3. Next to **Trigger**, select **New**, then select **Periodic** for the trigger interval.

4. In **Periodic**, go to **Interval** and select **Daily**.

5. For **Time of day**, enter the time which the trigger should occur in 24-hour format. For this example, enter *23:00* (11:00 PM).

6. Select **OK**.

7. Next to **Actions**, select **Add**.

8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.

9. Select **OK**.

10. Next to **Command**, select **Choose**, then select **Stop Copying Live Events**.

11. Select **OK**, then select **Save and Close**.

12. Select **Save and Close**.

Prune Live Events

The third automation rule will be configured to prune live events.

1. Go to **Configuration** > **Automation Rules**.

2. Select **Add**. Name the automation rule (ex. *Prune Live Events*).

3. Next to **Trigger**, select **New**, then select **Periodic** for the trigger interval.

4. In **Periodic**, go to **Interval** and select **Daily**.

5. For **Time of day**, enter the time which the trigger should occur in 24-hour format. For this example, enter *21:00* (09:00 PM).

6. Select **OK**.

7. Next to **Actions**, select **Add**.

8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.

9. Select **OK**.

10. Next to **Command**, select **Choose**, then select **Start Pruning Live Events**.

11. Select **OK**, then select **Save and Close**.

12. Select **Save and Close**.

Stop Pruning Live Events

The fourth action will be configured to stop pruning live events. To do this, follow the steps as outlined in the previous section, however the Time of Day will be the time to stop pruning live events and the Device Command will be to Stop Pruning Live Events.

1. Go to **Configuration** > **Automation Rules**.

2. Select **Add**. Name the automation rule (ex. *Stop Pruning Live Events)*.

3. Next to **Trigger**, select **New**, then select **Periodic** for the trigger interval.

4. In **Periodic**, go to **Interval** and select **Daily**.

5. For **Time of day**, enter the time which the trigger should occur in 24-hour format. For this example, enter *05:30* (5:30 AM). The trigger time must be set to stop pruning after the selected time to start pruning.

6. Select **OK**.

7. Next to **Actions**, select **Add**.

8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.

9. Select **OK**.

10. Next to **Command**, select **Choose**, then select **Stop Pruning Live Events**.

11. Select **OK**, then select **Save and Close**.

12. Select **Save and Close**.

To run the automation rules, go to **Configuration** > **Hardware**. Ensure that the Automation Driver is started by selecting it and viewing its status on the right side of the Hardware module. If stopped, right-click the **Automation Driver** and select **Start**.

Maintain the Historical Events Driver

Maintain the Historical Events Driver by reporting on the driver's activity.

1. Go to **Management** > **Reports**.

2. In the toolbar, select **Add** > **Add Filter-based Report**.

3. Name the report and enter a description.

4. If there should be no limit on the number of events allowed in the report, set the **Max. results** field to **-1**, otherwise define the number of results that should appear in the report.

5. In **Item type**, select **Events (Historical)**. Optional report modifications are:

    ‣ Open or save the report as a document

    ‣ Edit the settings by selecting **Report Settings**

    ‣ Filter the results by selecting **Edit Filter**

    ‣ Add variable parameters by selecting **Variable Parameters**

6. Select **Save and Close**. To run the report, right-click the report and select **Run**.

Prune the Database

The following describes how to add a Historical Events Driver to prune the database and report on legacy events. To complete the example operation, a Historical Events Driver must be added and started in the Hardware module.

Prune Historical Events

The third automation rule will be configured to prune live events.

1. Go to **Configuration** > **Automation Rules**.

2. Select **Add**. Name the automation rule (ex. *Prune Live Events*).

3. Next to **Trigger**, select **New**, then select **Periodic** for the trigger interval.

4. In **Periodic**, go to **Interval** and select **Daily**.

5. For **Time of day**, enter the time which the trigger should occur in 24-hour format. For this example, enter *21:00* (09:00 PM).

6. Select **OK**.

7. Next to **Actions**, select **Add**.

8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.

9. Select **OK**.

10. Next to **Command**, select **Choose**, then select **Start Pruning Historical Events**.

11. Select **OK**, then select **Save and Close**.

12. Select **Save and Close**.

Stop Pruning Historical Events

The fourth action will be configured to stop pruning live events. To do this, follow the steps as outlined in the previous section, however the Time of Day will be the time to stop pruning live events and the Device Command will be to Stop Pruning Live Events.

1. Go to **Configuration** > **Automation Rules**.

2. Select **Add**. Name the automation rule (ex. *Stop Pruning Live Events*).

3. Next to **Trigger**, select **New**, then select **Periodic** for the trigger interval.

4. In **Periodic**, go to **Interval** and select **Daily**.

5. For **Time of day**, enter the time which the trigger should occur in 24-hour format. For this example, enter *05:30* (5:30 AM). The trigger time must be set to stop pruning after the selected time to start pruning.

6. Select **OK**.

7. Next to **Actions**, select **Add**.

8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.

9. Select **OK**.

10. Next to **Command**, select **Choose**, then select *Stop Pruning Historical Events*.

11. Select **OK**, then select **Save and Close**.

12. Select **Save and Close**.

Create a Report on Legacy Events

Next, create a report on legacy events. This report will be configured as an automation rule.

1. Go to **Management** > **Reports**.

2. Select **Add** > **Add Filter-based Report**. Name the report (ex. *Legacy Events*).

3. In **Item type**, select **Events (Historical)**, then select **Save and Close**.

4. To create an automation rule for legacy events, go to the **Automation Rules** module and select **Add**.

5. Name the rule.

6. Next to **Trigger**, select **New**.

7. In **Type** drop-down, select **Periodic**.

8. In **Interval**, select **Monthly**. Define the **Day of month** and **Time of day** that the report should run, then select **OK**.

9. From the Action field, select **Add**, select **Report**, then select **OK**.

10. Select **Choose**, then select the **Legacy Events** report.

11. Select **OK**, then select **Save and Close**.

12. Select **Save and Close**.

Program Card Formats

Program up to eight different card formats. For more information, refer to the appropriate module installation guide.

1. Go to **Configuration** > **Hardware** > **DMP Driver**.

2. Right-click the panel you want to program card formats for.

3. Select **Edit**, then select **Card Formats**.

> **Note:** If your panel is Version 192 or lower, the steps 2 and 3 will not be available in Entré. Instead, go to **734 Options** and find **Number of User Code Digits**. Enter a number between 4-12 digits in length. Default is **5**.

4. Complete the following fields:
   ‣ **Site code position**: Number between 0-255. Default is **1**.
   ‣ **Site code length**: Number between 1-24. Default is **8**.
   ‣ **Wiegand code length**: Total number of bits in Wiegand code. Number between 1-255. Default is **26**.
   ‣ **User code position**: Number between 0-255. Default is **9**.
   ‣ **User code length**: Number between 16-64. Default is **16**.
   ‣ **Require site code**: Select if you would like to use a site code. You can program up to eight 8-digit site codes. The site code range is 0-16,777,214.
   ‣ **Number of user code digits**: Number between 4-12 digits in length. The default is **5**.

5. Select **Save and Close**.

734 Options

You can now remotely manage new 734 Access Control Module configurations. To configure 734 Options, complete the following steps:

1. Go to the **Edit - Device** window.

2. In **734 Options**, go to the **Reader Protocol** drop-down menu and select **OSDP** or **Weigand**.

3. If you select **OSDP**, you can enter a custom **OSDP Passphrase** for the reader.

OSDP Options

Note: To use the OSDP programming fields below, 734 Access Control Module firmware Version 108 and XR Series firmware Version 253 (8/22/25) or higher is required.

You can now remotely manage some OSDP configurations.

OSDP Prox OFF/ON

1. Select the **Door** icon in **Configuration > Hardware - List or Configuration > Hardware - Tree module**.

2. Select **OSDP Prox Off/On**.

3. Select **Prox On** to allow the OSDP Reader to read credentials. Select **Prox Off** to leave this option disabled.

Send OSDP Configuration File

1. Select the **Door** icon in **Configuration > Hardware - List or Configuration > Hardware - Tree module**.

2. Select **Send OSDP Configuration File**.

Set Up a Cell-Only Panel

Entré Version 8.3.0 and higher supports a cellular-only remote connection to XR Series panels. Learn how to set up Entré and retrieve a cell-only panel.

The panel must be equipped with a DMP cellular module.

Before starting, Entré must be licensed for service from SecureCom Wireless. The key is available from your DMP sales representative. This is the same key used in Dealer Admin.

Set Up the Wireless License Key

1. Go to **System Configuration** > **DMP Communication**.

2. Enter the **Securecom Wireless License Key**.

3. Select **Test Activation Server** to check that Entré can communicate with the SecureCom Server.

4. To enable a forward proxy server, select the **Use Forward Proxy** checkbox and enter your IP or DNS Address in **SecureCom Cellular Activation Server Address**.

5. Select **Save**.

6. Log out of Entré and log back in.

Connect a Cell-Only Panel to Entré

1. Open Entré. Go to **Configuration** > **Hardware Tree**.

2. Right-click **DMP Driver** and select **New Panel 150/350/550**.

3. In **General**, name the system and select the model type.

4. Go to **Communication**. In the **Main account number** field, enter the account number of the panel.

5. Select **Cell Activation**. Enter the SIM/MEID code and select **Refresh**. This checks that the SIM is valid. Entré recognizes the newest SIM codes for AT&T and Verizon.

> **Note:** To use DualSIM operation for a TMSentry panel, select **Cell Activation** for Verizon and AT&T. Enter both SIM/MEID codes, then select **Refresh**. DualSIM is only compatible with panels with firmware Version 243 or higher.

   To choose a carrier option, go to **Configuration** > **Hardware** > **Hardware List** or **Hardware Tree**. Right-click the TMSentry panel with DualSIM operation. In the drop-down menu, select **Dual Sim Support**. A pop up displays to choose a carrier option. To select a single carrier, choose **Verizon** or **AT&T**. To use DualSIM operation, select **Both**.

6. After selecting **Refresh**, the **Name**, **Rate Plan**, and **Text Plan** fields populate automatically.

7. Select **Activate/Update** to register the SIM with SecureCom Wireless.

8. Select **Close**. The active SIM populates in the **Cell Module** field. Previous releases of Entré supported cellular connection as a backup. Entré Version 8.3 and higher supports backup from Remote Options.

9. Go to **Remote Options**.

10. In the **Entré** tab, select **Cell**.

11. Select **Save and Close**. Select **OK** when Entré prompts you to choose Plan 416 for communications.

Retrieve Panel Programming

1. In the **Hardware Tree**, right-click on the new panel. Go to **Panel Control** > **Start**. Wait for process to end. Cell may take longer than Network.

2. Right-click on the new panel. Go to **Panel Configuration** > **Retrieve Configuration**.

3. Select **OK**. Wait for process to end. Cell may take longer than Network.

Set Up a Panel with a Remote Key

When adding a new panel to Entré with the intent of using a remote key, do not use the New Panel Wizard. To prevent communication errors, complete the following steps in order.

Connect a Panel to Entré with a Remote Key

1. Go to **Configuration** > **Hardware Tree**.

2. Right-click **DMP Driver**. Select **New Panel 150/350/550**.

3. In **General**, give the panel a name and select the model type.

4. Go to **Communication**. In the **Main account number** field, enter the account number of the panel.

5. Go to **Remote Options** and enter your remote key.

6. In the **Entré** tab, select the appropriate communication type and enter information.

7. Select **Save and Close**.

Retrieve Panel Programming

1. In the **Hardware Tree**, right-click the new panel. Go to **Panel Control** > **Start**. Wait for process to end. Cell may take longer than Network.

2. Right-click the new panel. Go to **Panel Configuration** > **Retrieve Configuration**.

3. The **Retrieve Configuration** dialog pops up to confirm programming retrieval. Select **OK**. Wait for process to end. Cell may take longer than Network.

Change a Remote Key

⚡ **Caution:** Before editing the remote key, inform operators that you are performing maintenance on the panel and ensure there are no pending changes to personnel, badges, or profiles. To check for pending changes, run a report or download users and schedules.

1. Go to **Configuration** > **Hardware** > **Hardware - Tree**.

2. Double-click on the panel, or right-click on the panel and select **Edit**.

3. Go to **Remote Options** and select **Change** next to the **Remote Key** text box.

4. A pop-up appears. Follow the instructions in the pop-up then select **OK**.

5. The **Remote Key** text box can be edited now. Enter the **Remote Key**.

6. Select **Save and Close**.

7. Right-click on the panel and hover over **Panel Configuration**. Select **Download Configuration**.

8. Select **Hardware Configuration**, then select **OK**.

9. Stop and start the panel, and verify that the panel connects to Entré.

Configure Single Sign-On

Desktop Client

1. Go to **Configuration** > **System Configuration** > **Single Sign On**.

2. Select **Enable Single Sign On using Windows Login**.

3. Select **Save**.

Web Client

1. Go to **Configuration** > **System Configuration** > **Single Sign On**.

2. In **Assertion attribute mapping**, enter the **username ID**. To enable strict username matching, select **Strict**.

3. In **IdP entity id**, enter the **Entré SSO Service entity ID (URI)**.

4. In **IdP redirect url**, enter the web client's Apache Tomcat server address and port number.
   For example, https://entretomcatserver:2001.

5. In **Assertion consumer service url**, enter the service provider's authentication server address and port number.

6. In **SP entity id**, enter the service provider's **connection ID (URI)**.

7. Select **Save**.

For additional information, see LT-2494 Entré Installation, Setup, and Server Maintenance Guide for how to configure Single Sign-On.

Edit Network Encryption Passphrase

If network encryption is enabled via Panel Feature Key, the network passphrase can be edited.

1. Go to **Edit - Panel**.

2. Open the **Feature Keys** tab.

3. Select **Encryption** to enable it.

4. Open the **Network Options** tab. The Passphrase should match the receiver.

Add a Host Name

The host name acts as an alternative to an IP address, which allows the panel to retain connection and send network messages if the IP address changes without the use of a Static IP address.

Receiver Host Name

1. Double click the panel name. The **Edit - Panel** dialog box opens.

2. Select **Communication** in the left-hand menu.

3. Double click the **Net** communication path. A **Communication Path** dialog box opens.

4. Check **Use Hostname**.

5. Select **Edit** next to **Receiver info**. A pop-up opens.

6. Enter the **Hostname**.

7. Select **OK**.

8. Select **Save and Close**.

Entré Host Name

1. Double click the panel name. The **Edit - Panel** dialog box opens.

2. Select **Remote Options** in the left-hand menu.

3. Select the **Entré** tab.

4. Select **Use Hostname**.

5. Enter the **Entré Hostname**.

6. Select **Save and Close**.

Integrator Host Name

1. Double click the panel name. The **Edit - Panel** dialog box opens.

2. Select **Remote Options** in the left-hand menu.

3. Select the **Integrator** tab.

4. Select **Use Hostname**.

5. Enter the **Integrator Hostname**.

6. Select **Save and Close**.

PC Log Host Name

1. Double click the panel name. The **Edit - Panel** dialog box opens.

2. Select **PC Log Reports** in the left-hand menu.

3. Enter the **Hostname**.

4. Select **Save and Close**.

Audit Trails and Reports

View Audit Trails

The Audit Trail module displays real-time audit record events in an access control system. This includes the date, the time, and the state of the object before and after the edit. An audit record is a type of event. The different events and how they are to be processed are configured in the Event Policy Manager module.

1. Go to **Management** > **Audit Trail**.

2. Select an audit record, then select **View**.

3. To view the current settings of the audit trail, select **View Current**.

4. To view settings before an item changed or information was updated, select **View Before**.

5. To view settings after an item changed or information was updated, select **View After**.

Create a Personnel Access Report

Generate a report on personnel access.

1. Go to **Management** > **Reports**.

2. Go to **Add** > **Add Filter-based Report** and name the new report.

3. In **Item type**, select **Events**.

4. Select **Edit filter**.

5. Use the **Time** field to narrow the results to a specific time period. For this example, select **This week** from the Window drop-down. The **Start** and **End** fields can be used to customize the time period. **This week** equals Sunday to the present day, not the past seven days.

6. In **Log**, select **Choose** and select the appropriate access granted log code.

7. In **Available items**, select the Add icon to open the **Access** tree, then expand the **Access Granted** tree.

8. To add an event to **Selected items**, double-click an event. For example, double-click **Access granted**, **door used** (log code: **MS.TX07090613**), then select **OK**.

9. To limit the report to a personnel type, go to **Personnel Record** and define the type of personnel that should be included in the report. For this example, select Contractor from the Personnel type field. Skip this step if using variable parameters. Variable parameters requires the operator to type in the name of a personnel record for reporting purposes. Refer to Step 12.

10. To limit the report to specific devices, go to **Device** and select a device from **Type**, then select **OK**. A DC cannot have access events. If a report is not being made for a specific device, select **Access Point**.

11. To select variable parameters for the report, select **Variable Parameters**, then expand the **Personnel Record** tree and check the parameter fields. For example, select the **First Name** and **Last Name** fields, then select **OK**. This change will prompt the user to type in the name of the personnel record for the desired access report each time the report is run and allows more flexibility when designing common reports.

12. Select **Report Settings**, and choose one of the following report outputs:

    ‣ **Record-style**: Save the report in a portrait layout

    ‣ **Table-style**: Save the report in a landscape layout

13. Select **OK**, then select **Save and Close**.

14. To run the report, select the report and select **Run**. To save the report, select **Report**.

Create a SQL-Based Report

SQL-based reports are defined using explicit SQL. After creating and saving a report, it can be scheduled to run automatically in the Automation Rules module.

The following describes how to create a SQL-based Report to report on a device and variable parameters will be used to prompt the user to type in the name of a device when running the report.

1. Navigate to **Management** > **Reports**.

2. Select **Add**, then select **Add SQL-based Report**. Name the report and add a brief description.

3. Set **Max. Result** to a manageable maximum. A **Max. result** of **-1** displays unlimited results.

4. For **SQL**, enter a SQL query to generate the desired report variables. For this example, enter the following query into the SQL field: **select * from vx_dev where name=?** (Select all from the vx_dev table where the device name matches the user selection) For every parameter defined using Variable Parameters, use a prepared statement (question mark placeholder) to bind variables to user input.

5. Select **Variable Parameters**.

6. In **Type**, select the parameter type. For this example, select **Devices** and select **OK**.

7. Enter a user prompt for the parameter, then specify the Device type. Because variable parameters will replace the question mark placeholders in the SQL query, the number of parameters must match the number of question marks in the query.

8. In **Parameter**, select the parameter and select **OK**.

9. Select **Save and Close**.

10. To run the report, go to **Reports** and select **Run**. The **Report Parameters** window opens and prompts the user to select a predefined device to report on. Select the device and select **OK**.

Report Types

The Reports module displays reports saved in the system. Reports may be one of the following types.

Filter-based

Defined using a filter, similarly to the Filter toolbar button in many modules. This is the most straightforward way to define a report. Other SQL-based options are intended for more complex reports.

Object SQL-based

Defined using explicit SQL. Returns the unique IDs of the items to display. Report items are otherwise presented in a similar fashion as a filter-based report.

SQL-based

Defined using explicit SQL.

Set Up Secure Lightweight Directory Access Protocol

For information about setting up the Secure Lightweight Directory Access Protocol (LDAPS), see the following link: LT-2455 Single Sign-On, Active Directory, and LDAPS.

TROUBLESHOOT ENTRÉ

Client Not Connecting

Learn about messages presented to a user when a client is unable to connect to the server. Here are possible cannot connect to server messages followed by their resolutions.

Login Failed

Client and server are using different versions of software with different network protocols.

Resolution: The server is running a different version of the application than the client. Update the client or server to matching software versions.

For a web client, redeploy the .war file from the webapp folder of the Entré application server into the Tomcat server.

Connection Refused: Connect (Java.net.ConnectionException)

The client can't connect to the server because it is not currently running.

Resolution: Start the server. If the server is running, check server communication.

Authentication failed

Either the client cannot connect because the username or password was typed incorrectly or the login has expired.

Resolution: Try retyping the username and password. If authentication fails after multiple attempts, contact your Entré administrator.

Using the Log Files

There are four types of log files used by Entré.

- **vx.gui.log**: Log file of the client user interface.
- **vx.appserver.log**: Log file for the application server.
- **vx.adminapp.log**: Log file for database tasks, such as: upgrades, plugin upgrades, and database imports.
- **wrapper.log**: Log file for the application server.

Log files are written to the Logs in the Entré working directory. To locate a log file, open the Entré application server folder.

Open the log folder to view the log files. The most recent activity is logged in the first **appserver.log** file. Subsequent log files contain data historic to the preceding file. Log files data is capped at 1 MB (1,025 KB) per file. When a log folder reaches the data cap, a new log is created. For example, when **appserver.log** reaches the data cap, the data will roll over creating a new file called **apperserver.log.1**. The **appserver.log** file always contains the most recent data and the appserver.log file with the highest number to always contain the oldest appserver data.

To locate recent log instances, open the **appserver.log** file. Data populates in a descending manner causing recent data to be located at the bottom of the window.

The log directory may not contain all the logs described above because they are only written to the directory when the dependent application is running. For example, if only the Entré client is running, then the log file in the log directory will be: **vx.gui.log**.

ENTRÉ NOC FEATURES

Manual User Number Assignment

When using an automation, such as "Mastermind" to control the "Record of Truth" for Audits, you must use the Manual User Number assignment instead of Auto-Assign.

Example: If Mastermind says John Doe is #431 in the alarm panel, then you will specifically assign that name and user code to account #12345 in the exact slot of 431, even if there are unused slots between 20 and 430 for a user code to be assigned.

Note: Once Manual User Number assignment is enabled, Entré will not be able to Auto-Assign where in the panel that Badge/User is slotted.

Panel Auto-Start

When the DMP driver starts, Entré reaches out to all panels to get statuses of Areas and Zones. With Auto-Start, the panels show online and then will update statuses as events are received. This allows users with a large amount of panels to search and retrieve statuses for specific areas and zones instead of seeing them all at once.

Pre-Loading Modules

When not pre-loading modules is not reaching out for data, it will display a new search window. The operator can select which field to search by and choose Contains, Is, or Starts With. These results can be widened or narrowed with each additional field. Entré will scan what is entered into the search across all those table columns.

ENTRÉ GLOSSARY

—

A glossary of terms used in Entré Access and Security Management.

A

Absolute Address

Address of the device in relation to the root of the device tree. Absolute addresses are generally, but not necessarily, unique.

Alarm

An event that has been configured to be displayed as an alarm to the operator. Alarms may be in different states indicated by color and/or blinking and may be acknowledged, cleared, and commented on by the operator. Priority associated with the alarm indicates its severity or importance.

Anti-Passback (APB)

Mode of operation that hinders a badge holder from entering an access point, then "passing back" their badge to be used by another person. The consequences of violating the anti-passback conditions vary depending on the mode of anti-passback the access point is configured for.

Audit Record

A type of event that records an operator's modification of an object in the system, as well as the date, time, and state of the object before and after the edit.

B

Biometric

Biometric verification identifies a person by evaluating distinguishing biological traits, such as fingerprints. A biometric in Entré Access and Security Management refers to a type of credential used for biometric verification.

C

Card Format

Specific bit structure of a card. Card formats typically include: card number, facility code, and parity bits. Entré Access and Security Management supports Wiegand and magstripe card formats.

Card Number

Card number encoded within a badge.

Credential

A general category used to gain access to a physical or logical resource, such as a: login, badge, or biometric.

Credential Watch Levels module

Module that allows administrators to add and define credential watch levels. A credential watch level is a color presented when a credential is used in Entré. The color is displayed as a column in the following modules: Alarms, Events, and the Event Photos modules.

The Credential Watch Levels module is added to the Advanced menu by enabling the module on the System Configuration module. Select **Miscellaneous** and Enable Credential Watch Levels. The Credential Watch Levels module is opened by selecting it on the Advanced menu.

Credential Validity Types module

Module that allows administrators to add and define badge credentials. Navigate to Advanced > Credential Validity Types to open the module.

D

Default Gateway

In a network using subnets, the default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

Disabled

A temporary, Entré-specific status for a panel, area, zone, or device where the programming for each remains in the software but no real-time events are displayed. Events will be received by Entré, but real-time status is not updated. A panel, area, zone, or device can be added back into the software without re-programming it. Only operators can disable a panel, area, zone, or device.

DMP Driver

Digital Monitoring Products (DMP) driver. A process on the host computer that manages the sending and receiving of data between the panels and host computer. It sends user code and area information to the controllers and receives transaction data back from the controllers. The parent device of a DMP driver is always the Driver Manager.

Download Configuration

Command initiates a download of everything.

Download Firmware

Command initiates a download of the most current system firmware and system features that Entré supports. See the Compatibility Guide.

Driver

A host computer process used to communicate between the host computer and hardware devices. Different types of supported hardware generally have different drivers.

Driver Manager

A software device that manages all drivers in the system.

E

Encrypted Communication

Used to secure communication between the Entré Access and Security Management application server and the panel.

Event

A system activity which is recorded to the database and available for monitoring or reporting.

Events module

The Events module displays real-time events within the Access Control system. Navigate to Monitoring > Events to access the module.

Event Photos module

The Event Photos module displays real-time events along with personnel photos. The different events are configured in the Event Policy Manager module. Navigate to Monitoring > Event Photos to open the module.

F

Facility Code

A bit segment encoded on a card which represents a numerical identification of a facility. Generally, all cards issued for a single facility will have the same facility code.

Filter

Enables the operator to sort (filter) data via a defined set of criteria in order to locate specific instances.

FIN

Foreign Identification Number. Used as an alternative to Social Security Number (SSN).

G

Graphic Map Editor

Allows graphic maps to be imported and configured. A graphic map can have links to other maps and/or devices. The map links can be used to navigate between maps in the map viewer. The device links show real-time statuses of the device in the graphic maps viewer.

H

Hexadecimal

16-digit numbering system, where 0-9 represents zero through nine and A-F (a-f) represents ten through fifteen.

Historical Events Driver

The Historical Events Driver is a software device which stores historical copies of events in a separate database table. Along with copying events, the Historical Events Driver can purge the copied events from the Events table, resulting in better performance from the table. Since the purged events are copied to a different table, legacy activity can still be reported.

The parent device of a Historical Events Driver is always the Driver Manager. There are no device types that have a Historical Events Driver as the parent device.

L

LDAP

Lightweight Directory Access Protocol. LDAP is a networking protocol for querying and modifying directory services running over TCP/IP.

Localhost

Default hostname describing the local computer address.

Locations module

Module that manages locations in <%SOFTWARE%>. Navigate to Advanced > Locations to open the module.

M

Magnetic Stripe

A strip of magnetic recording material on which data can be stored.

Maps module

The Maps module allows operators to view real-time event and alarm conditions overlaid on graphical maps of the facility. Open the Maps module by selecting it from the Start Page or from the Monitoring drop-down menu.

Map Viewer

Allows facility maps to be viewed along with the location and statuses of facility devices. Maps can also contain links used to navigate to other maps.

Masked

A hardware state for monitor points and access points where active conditions will be reported to the software as masked (i.e. hidden).

O

Organization

Affiliation with which a personnel record can be associated.

P

Partition

Partitions are a way of dividing the system into subsets. Many items may have an associated partition, including: devices, personnel records, credentials, privileges, reports, and badge designs. A profile may be optionally restricted to a single partition which then only allows access to items associated with that partition. To give a login access to multiple partitions, associate it with multiple profiles where each profile is restricted to a single partition.

Partitions Module

The Partitions module manages all partitions within <%SOFTWARE%>. Navigate to Advanced > Partitions to open.

PIN

Personal Identification Number. Badges have an associated PIN which, depending on the configuration of an access point, is entered into the access point reader keypad.

Ping Utility

Determines whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. To use the ping utility, open a command window, type ping followed by the IP address and select Enter on the keyboard.

Privilege

Privileges define what a credential may have access to. Examples of privileges include: access levels and profiles.

Profile

Determines which Entré Access and Security Management modules an operator is permitted access to, as well as defining which commands the operator is allowed to issue.

Proximity

A technology that allows the presence of certain objects to be sensed by a device without having direct contact.

R

Reader

Device which receives a card number and/or PIN from a badge holder.

Relative Address

Address of a device relative to its parent device.

Relay

Device that responds to a small current or voltage change by activating switches or other devices in an electric circuit.

REX

Request-to-Exit. A type of door hardware, typically a button, that allows people to exit through an access point without using a badge.

S

Schedule

A set of time intervals that can be applied to a DC to make Access Control, triggering, and other decisions.

Scroll Lock

Tool that allows the operator to stop the scrolling of items in the window. New items will continue to be added to the window, but the window will not automatically scroll to show the most recently added item. This tool is not available in all modules.

SSN

Social Security Number. A nine-digit number issued to individuals by the U.S. government for tax and identification purposes.

Subnet

A portion of a network which shares a common network address with other portions of the network and is distinguished by a subnet number. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example: all devices with IP addresses that start with 100.100.100 would be part of the same subnet.

T

TCP/IP Communications

A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

Time Received

The time an event or alarm was actually received by the Access Control system and stored in the database. If the event was processed by an external device, such as a DC, this may differ from the occurrence time depending on delays and interruptions in communication between the host and the DC.

Top Alarm

Most important alarm in occurrence at a given device. Based on alarm state, time, and priority.

Top Alarm State

Status of the top alarm at a given device. Possible statuses are: active, acknowledged, and cleared. Each state has an associated color, possible blinking, and severity.

Not to be confused with device status, which is independent of operator actions in the application. For example: if a door is forced open and is then shut, the status will go from forced open to secure, but the top alarm state will reflect the forced open state until an operator clears it.

U

User Code Profile

Defines privilege of the badge holder. For example: a user code profile determines if a badge holder has permission to pass through an access area or if the badge holder can arm or disarm a panel.

Username

An identifiable sequence of characters used when logging into the application.

V

View Query

Filter tool that allows operators to view the actual filter definition as SQL.

W

Wiegand

Wiegand is a card format that stores card data using binary values. The information includes parity error detection, facility code, and the card ID. Each card has a particular format that must be configured in the Access Control panel in order to permit the panel to correctly interpret the card data. A very common Wiegand card format is a 26-bit format, with the first and last bit for parity, 8 bits for the facility code and 16 bits for the card number.