Output Point Status 11
Keypad Status 11
Area Status 12
Zone Status 12
24-Hour Zone Status 13
Add an Image Capture Device 13

5 Configure Software 14
Configure Time Change 14
Add a Calendar 14
Add a Schedule 15
Customize the User Interface 16
Configure Password Policies 16

6 Configure Automation 17
Set Up Automated Tasks 17
Automatically Generate Card Numbers 18

7 Configure Maps 18
Add a Map 18
Images in Map Editor 19
Configure a Map 19
Controls 20
Device States 20
Monitor Facilities Using Maps 21

8 Configure Events and Alarms 22
Event Types 22
Alarm States 22
Configure Alarm Instructions 23
Set Up Event and Alarm Priorities 23
Create a Report 25
Enable Video Reports 26

9 Configure Personnel and Users 26
Configure Departments and Organizations 26
Add Organizations to Personnel 27
Edit Personnel Group 27
Configure a User Code Profile 27
Enroll Personnel 28
Customize Personnel Records 29
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Up Chroma Key</td>
<td>30</td>
</tr>
<tr>
<td>Assign Badges</td>
<td>30</td>
</tr>
<tr>
<td>Add Privileges to Badges</td>
<td>30</td>
</tr>
<tr>
<td>Create an Operator Login and Profile</td>
<td>31</td>
</tr>
<tr>
<td>Create Restricted Profiles</td>
<td>32</td>
</tr>
<tr>
<td>Create a Profile for Badge Privileges</td>
<td>32</td>
</tr>
<tr>
<td>Create a Profile for Events and Alarms</td>
<td>33</td>
</tr>
<tr>
<td>Import Personnel and Badges</td>
<td>35</td>
</tr>
<tr>
<td>Sync User Removal with Profile Removal</td>
<td>36</td>
</tr>
<tr>
<td><strong>10 Configure Badges</strong></td>
<td>37</td>
</tr>
<tr>
<td>Create a Badge Template</td>
<td>37</td>
</tr>
<tr>
<td>Use Badge Templates</td>
<td>37</td>
</tr>
<tr>
<td>Design a Badge</td>
<td>37</td>
</tr>
<tr>
<td>Add a Badge</td>
<td>39</td>
</tr>
<tr>
<td>Edit Badge Information</td>
<td>40</td>
</tr>
<tr>
<td>Add Effective or Expiration Times for Badges</td>
<td>40</td>
</tr>
<tr>
<td>Edit Badge Group</td>
<td>41</td>
</tr>
<tr>
<td>Configure Badges to Allow Null PIN</td>
<td>41</td>
</tr>
<tr>
<td>Customize Text Links</td>
<td>42</td>
</tr>
<tr>
<td>Badge Status</td>
<td>42</td>
</tr>
<tr>
<td>Set Up Badge Printing</td>
<td>43</td>
</tr>
<tr>
<td>Print a Badge</td>
<td>43</td>
</tr>
<tr>
<td>Print Badges in Batches</td>
<td>44</td>
</tr>
<tr>
<td>Assign a Temporary Badge</td>
<td>44</td>
</tr>
<tr>
<td>Return a Temporary Badge</td>
<td>45</td>
</tr>
<tr>
<td>Delete Personnel with Badge</td>
<td>45</td>
</tr>
<tr>
<td><strong>11 Configure More Advanced Options</strong></td>
<td>45</td>
</tr>
<tr>
<td>Use Filters</td>
<td>45</td>
</tr>
<tr>
<td>Create a Profile Template</td>
<td>47</td>
</tr>
<tr>
<td>Program Templates</td>
<td>48</td>
</tr>
<tr>
<td>Set Up Locations</td>
<td>49</td>
</tr>
<tr>
<td>Bind Profiles to Locations</td>
<td>50</td>
</tr>
<tr>
<td>Set Up Partitions</td>
<td>51</td>
</tr>
<tr>
<td>Add a Custom Alert Sound</td>
<td>53</td>
</tr>
<tr>
<td>Create Credential Watch Levels</td>
<td>53</td>
</tr>
<tr>
<td>Add and Configure the Historical Events Driver</td>
<td>54</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>Maintain the Historical Events Driver</td>
</tr>
<tr>
<td></td>
<td>Prune the Database</td>
</tr>
<tr>
<td></td>
<td>Program Card Formats</td>
</tr>
<tr>
<td></td>
<td>Set Up a Cell-Only Panel</td>
</tr>
<tr>
<td></td>
<td>Set Up a Panel with a Remote Key</td>
</tr>
<tr>
<td></td>
<td>Configure Single Sign-On</td>
</tr>
<tr>
<td></td>
<td>Edit Network Encryption Passphrase</td>
</tr>
<tr>
<td></td>
<td>Audit Trails and Reports</td>
</tr>
<tr>
<td></td>
<td>View Audit Trails</td>
</tr>
<tr>
<td></td>
<td>Create a Personnel Access Report</td>
</tr>
<tr>
<td></td>
<td>Create a SQL-Based Report</td>
</tr>
<tr>
<td></td>
<td>Report Types</td>
</tr>
<tr>
<td>12</td>
<td>Troubleshoot Entré</td>
</tr>
<tr>
<td></td>
<td>Client Not Connecting</td>
</tr>
<tr>
<td></td>
<td>Using the Log Files</td>
</tr>
<tr>
<td>13</td>
<td>Entré NOC Features</td>
</tr>
<tr>
<td></td>
<td>Assign Key Fobs to Badges</td>
</tr>
<tr>
<td></td>
<td>Add a User Code Manually</td>
</tr>
<tr>
<td>14</td>
<td>Compatibility</td>
</tr>
<tr>
<td>15</td>
<td>Entré Glossary</td>
</tr>
</tbody>
</table>
Part 1. Welcome to Entré

The Entré User 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 serial and network. At the software level, Entré is designed to be flexible and extensible with a modular open architecture and multiple database support.

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

1.1 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 XR150/XR550 Series 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.

XR150/XR550 Series panels communicate with the following Entré devices:

- DMP Driver
- Panel
- 24-Hour Zone
- Area
- Zone

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 2008 R2
- Client OS: Windows 10
- Microsoft SQL 2008
- Apache Tomcat 8.5

For information about Entré compatibility with specific versions of XR150/XR550 firmware, refer to "Compatibility".

**Note:** Entré Access and Security Management now has Java built-in and no longer requires users to download Java.

### 1.2 Languages

Entré 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

## Part 2. Learn Entré Fundamentals

### 2.1 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

**Note:** 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.

2.2 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.
2.3 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.

2.4 Search

Use the Search option to search the rows currently displayed. Select the drop-down arrow and select Edit Search Fields to customize sorting.
2.5 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.

2.6 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/entre.

Part 3. Navigate Entré

3.1 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.

3.2 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. Press **OK**.

Add device command widget
1. In the first cell, select **Add**.
2. Select **Device Command**, then press **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 press **OK**.
6. To close **Filter - Device**, press **OK**.
7. In **Command**, select **Choose**.
8. Select **Lock**. Press **OK**.
   - **Note**: 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**, press **OK**.

Add report widget
1. In the second cell, select **Add**.
2. Select **Report**, then press **OK**.
3. In **Report**, select **Choose**.
4. Select a report to add to the panel. For this example, select Profiles - Enabled located in the Management tree.

5. Press OK.

6. To close Add - Report Widget, press OK.

7. In the toolbar, press 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.

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

**Part 4. Configure Hardware and Devices**

The following sections provide instructions on how to add specific devices.
4.1 Add Devices

4.1.1 Add a Panel

To add a panel, see the instructions below:

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.
   a. The panel Name should be Panel XXXX (where XXXX is the panel number).
   b. Enter the IP address in the Host field.
   c. Enter the Account Number of the panel.
4. Select Next. Entré will attempt to connect to the panel.
5. Select Next in each new menu until the final menu appears then select Finish.

For more information about adding a panel, see: Add a Panel

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.

4.1.2 Add an Output Point

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.

4.1.3 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.
4.1.4 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.

4.1.5 Add a Zone
1. Go to the Hardware Tree.
2. Right-click the parent panel and select New Arming Zone.
3. Fill out the Add - Arming Zone information and select Save and Close.

4.1.6 Add a 24-Hour Zone
1. Go to the Hardware Tree.
2. Right-click the parent panel and select New 24-Hour Zone.
3. Fill out the Add - 24-Hour Zone information and select Save and Close.

4.2 Manage Devices
4.2.1 Swap a Panel
For information about swapping a panel, see the following link: Swap a Panel.

4.2.2 Delete a Panel
To delete a panel, stop the panel and then right-click the panel and select Delete. This will also delete all associated hardware and disassociate any attached profiles, automation rules, etc.
For more information about removing a panel for versions older than Entré 8.8.1, see the following link: Remove a Panel.

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

4.2.4 Delete a Keypad
Right-click the keypad and select Delete.
4.2.5  Delete an Area
Right-click the Area and select **Delete**.

4.2.6  Delete a Zone
In an area, right-click the Zone and select **Delete**.

4.2.7  Delete a 24-Hour Zone
In an area, right-click the 24-Hour Zone and select **Delete**.

4.3  Device Status
4.3.1  View Device Status
Device statuses can be viewed in real time in the Hardware Tree and Hardware List without having to perform another search.

4.3.2  Panel Status
Panels have seven different device status values.

**Device Status Values**

- **Disabled**: Driver has been disabled in the software.
- **Failed**: Driver has encountered an unrecoverable error and has failed.
- **Started**: Driver has started and is running.
- **Starting**: Driver is in the process of starting.
- **Stopped**: Driver has stopped.
- **Stopping**: Driver is in the process of stopping.
- **Unknown**: State of the driver is not known to the system because the parent device is in a state such as unknown, stopped, or failed.

4.3.3  Camera Status
Cameras record digital video files to be stored on the DVR. The parent device of a CCTV Camera is always the DVR. There are no device types which have a CCTV Camera as a parent device.
Device Status

Cameras have the following device status values.

- **Online**: Camera is online and communicating normally.
- **Offline**: Camera is offline.
- **Recording**: Camera is recording video to the DVR.
- **Idle**: Camera is communicating normally, but not in a recording state.
- **Failed**: Communication to the camera failed.
- **Unknown**: Camera is offline and not communicating.

### 4.3.4 Output Point Status

Output points 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.

Device Status

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.

### 4.3.5 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.
Device Status
Readers have the following device status values.

- **Disabled**: Device has been disabled in the software.
- **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.

### 4.3.6 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.

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

- **Armed**: Area is armed.
- **Disarmed**: Area is disarmed.
- **Disabled**: Device has been disabled in the software.
- **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.

### 4.3.7 Zone Status
A separate circuit or branch of a security system, usually for the purpose of isolating and/or identifying alarms or trouble in a system. A zone is a length of cable onto which different types of security or fire devices are connected. This zone is attached to the panel on its own set of screw terminals and given a zone name that can be displayed on system keypads, such as: **FRONT DOOR**. Multiple zones are typically assigned to an area so that all of their protection devices combine to provide for the complete protection of persons or property inside.
The parent device of a zone is always an area. There are no device types that have a zone as a parent device.

**Device Status**

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

- **Normal:** Device is operating normally.
- **Disabled:** Device has been disabled in the software.
- **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.

### 4.3.8 24-Hour Zone Status

24-Hour Zones are not turned on or off by arming or disarming the system. For example: fire zones, panic zones, and temperature control zones. The parent device of a 24-Hour Zone is always a panel. There are no device types that have a 24-Hour Zone as a parent device.

**Device Status**

24-Hour Zone device states include both commands and device states. A 24-Hour Zone supports the following commands, available by right-clicking the device in the **Hardware** module.

- **Bypass:** Bypass faulted zones in the selected areas until they are disarmed. The event reported will be **Zone Command: Bypass Zone**. In addition, the bypassed zone remains bypassed until the area is disarmed.

- **Reset:** Resets the zone. The event reported will be **Zone Command: Reset Zone**.

### 4.4 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. Select **TWAIN Source**. All selected drivers installed on the machine will be displayed. Select the driver associated with the capture device, then press **OK**.

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

6. Go to **Management > Personnel**.

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

### Part 5. Configure Software

#### 5.1 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**.

#### 5.2 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 cultural or 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. It's best to define all known holidays in advance for the expected lifetime of the system.

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. Press **Save and Close**.

### 5.3 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 XR150/XR550 Series panels, select **Time 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, press **Save and Close** to add the interval to the schedule. Repeat this step for as many distinct intervals as necessary.
7. Press **Save and Close**.
5.4 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 the Badges - Custom section to configure the custom fields as desired.
   - Note: To enable the Return Badge button in the Badges module, select the Show return temporary badge in badges module.
8. Press Save.
9. Restart Entré.

5.5 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. Press Save.
4. Restart Entré.
5. In File, select Change Password.
6. Enter the Old password, then enter the New password. Confirm the new password, then press OK.
7. Log out, then log in with the updated password.
Part 6. Configure Automation

6.1 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 5.

1. Go to Configuration > Hardware.
2. Right-click the Driver Manager and select New Automation Driver from the drop-down list. 
   Note: Only one Automation Driver is necessary in a system.
3. Name the Automation Driver. To setup email notifications, consult your network administrator for SMTP Server settings.
4. Press 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.
   Note: 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:
   a. Ensure that the Enabled checkbox is selected, then name the automation rule.
   b. Select New. Select Periodic, then press OK.
   c. Select Monthly, then select a Day of month and a Time of day for the trigger to occur.
   d. Press OK.
   e. In Actions, select Add.
   f. Select an action type. For this example, select Report, then press OK.
10. In Report, select Choose, then choose a report for the automated task to automatically run.
11. Press OK, then press Save and Close.
12. If report notification is desired, select New in Notification, then select a type of notification for the automated task. For this example, select E-mail, then press OK.

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

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

### 6.2 Automatically Generate Card Numbers

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

1. Go to System Configuration > Card Number Generator.

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

3. Press Save.

4. Restart Entré.

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

6. In the toolbar, select Add.

7. Select a Template, then press OK.

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

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


### Part 7. Configure Maps

#### 7.1 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.

Add a map
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. Press **OK**.

### 7.2 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

### 7.3 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.

   **Note:** 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 the **Commands** section, then select and drag the command into the map. Configure the command as needed. **Note:** Separate layers can be used in order to hide device commands from view.

5. Once the devices are selected in the **Command** section, 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 Under the Location** field, select a location.

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

### 7.4 Controls

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.

### 7.5 Device States

The inside fill color represents the device state. The outer ring color represents the device alarm state.
7.6 Monitor Facilities Using Maps

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

Monitor Facilities Using Maps

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.

<table>
<thead>
<tr>
<th>Inside Color</th>
<th>Outside Color</th>
<th>Device Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Alarm(s)</td>
<td></td>
</tr>
<tr>
<td>Orange</td>
<td>Acknowledged alarm(s)</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>No alarms</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>Unknown, fault or active state</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>Armed and inactive state</td>
<td></td>
</tr>
<tr>
<td>Light Blue</td>
<td>Disarmed and active state</td>
<td></td>
</tr>
<tr>
<td>Dark Blue</td>
<td>Disarmed and inactive state</td>
<td></td>
</tr>
</tbody>
</table>
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.

Part 8. Configure Events and Alarms

8.1 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.

8.2 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 pressing delete.
Alarm States
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.

Note: The default filter in the Alarms module hides cleared alarms, so these are generally unseen.

8.3 Configure Alarm Instructions
Configure alarm instructions in the Alarm Instructions module.
1. Go to Advanced > Alarm Instructions.
2. Select Add.
3. Enter a name for the alarm.
4. In the Text field, enter instructions to be displayed in the Events, Alarm, and Manage Alarms windows.
5. Ensure that the event or alarm that the instructions apply to is defined in Applicability.
6. Press Save and Close.

8.4 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:
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. Press Save and Close.
8.5 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.
8.6 Enable Video Reports

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

First enable Video system reports:
1. Go to the Edit - Panel window.
2. Select System Reports.
3. Enable Video system reports.

Then 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.

Part 9. Configure Personnel and Users

9.1 Configure Departments and Organizations

Note: While this example will take place in the Departments module, the same steps apply in the Organizations module.

1. Go to Management > Departments.
2. Select Add.
3. Name the department.
4. Configure Comments and Partition as needed.
5. Press Save and Close.
9.2 Add Organizations to Personnel

Add organizations and departments to personnel records.

2. Right-click a personnel record and select Edit.
3. Select the Occupational section, then select the personnel's associated Organization and Department.
   Note: Organization must be selected before Department.
4. Press Save and Close.

9.3 Edit Personnel Group

Edit a personnel group

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

9.4 Configure a User Code Profile

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

2. Select Add.
3. Name the user code profile General Profile.
4. To enable the new user code profile, select Enabled.
5. Select the options that you want to apply to the profile.
6. To restrict the profile to work during a specific time period, select Valid During and specify a time.

© 2021 Digital Monitoring Products
7. Select **Access areas** and **Arm and Disarm** areas as needed.
   **Note:** To enable **Arm and Disarm** areas, go to **Properties** and select **Arm and Disarm**.

8. If necessary, configure user code profiles in **Output Groups**.

9. Press **Save and Close**.

10. To assign **General Profile** to badges, go to the **Personnel** module.

### 9.5 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 press **OK**.
5. To preview the photo, press **Next**.
6. Press **Finish**.

**Use a Photo from Image Capture**

**Note:** Image capture is only compatible with 32-bit systems.

1. Go to **Management > Personnel**.
2. Select **Add**.
3. Enter information into the following required fields:
   - **First name**
4. Select **Capture**. Use the built-in tools to pan, tilt, and zoom to the appropriate location. Once satisfied with the camera settings, press **Capture** to take a picture. A preview of the picture will be displayed.

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

6. Press **Save**.

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

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

9. Press **Finish**.

### 9.6 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.

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

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

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

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

5. Edit the name of the **Column** header and **Form** label. The column header is displayed at the top of the column row in the table view. The **Form** label is displayed on the detail window of personnel records.

6. Press **Save**, then restart Entré.

7. Go to **Management > Personnel**.

8. Double-click a personnel record.

9. Go to **Custom** and verify that the edited **Custom Personnel Fields** are displayed in the personnel detail window.
9.7 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.
   
   **Note:** Color fields use the hexadecimal color system. For example, white (R 255, G 255, B 255) is represented as #ffffff.

3. Press **Save**.

4. Restart Entré.

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.

9.8 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. Press **Save and Close**.

4. Press **Save and Close**.

9.9 Add Privileges to Badges

Add privileges to a badge in the Personnel module.

In **Privileges**, select the options that you want each authority level to access, then press **Save and Close**. Press **Save and Close**.
9.10   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. Press 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 press 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, press Select and assign the login to a personnel record.

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

10. Select the profile that the login should to have access to. A profile can be assigned to more than one location.

11. Press Save and Close.

12. To verify changes and operator permissions, log out of Entré, then log in as the new operator.
9.11 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

9.11.1 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 press OK.
4. Name the profile Badge Privileges.
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. Select Allow access to module. You can filter the type of events the profile can view by selecting Default Filter.
2. Go to Management > Badges. Select Allow access to module.
3. In Personnel, select Allow access to module.
4. In Audit Trail, select Allow access to module.
5. Go to Configuration > Access Levels. Select Allow access to module.
Configure the Data Types tab
1. Expand the Data Types tree.
2. In Access Level and 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. Press Save and Close.

Create a login for the badge privileges profile
1. Go to Configuration > Login.
2. Select Add.
3. Name the login Badge Privileges and enter a password.
5. Press Save and Close.
6. To test the profile, log out of Entré, then log back in with the new profile.

9.11.2 Create a Profile for Events and Alarms
Create a profile that is only allowed to view events and alarms.

Create an Event/Alarm Profile
1. Go to Configuration > Operator Profiles.
2. Select Add.
3. In Template, select Most restrictive, then press OK.
4. Name the profile Events and Alarms.
5. Ensure that the Enabled checkbox is selected.

Configure the General section
1. In Events/Alarms, then 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. Press Save and Close.

Create a login for the Events/Alarms profile
1. Go to Configuration > Login.
2. Select Add Name, name the login Events and Alarms, and enter a password.
3. In Profiles, select Event and Alarms.
4. Press Save and Close.
5. To test the profile, log out of Entré, then log back in with the new profile.

9.12 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.
1. Go to Configuration > System Configuration > Personnel.
2. Select Use CSV personnel import wizard, then press Save.
3. Restart Entré.
5. Go to Add > CSV Import Wizard.
6. Select Browse. If the CSV file has a header row, ensure File has a header row is selected. Open the CSV file, then press Next.
7. 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**.

8. 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*.

9. 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.

10. Press **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**.

11. Press **Finish**.

### 9.13 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. Press **Save**.
Part 10. Configure Badges

10.1 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. Press OK.
6. Press Save and Close.

10.2 Use Badge Templates
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 press OK.
4. Make changes as needed.
5. Press Save and Close.

10.3 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 press **OK**. The following tools are available from the top of the **Badge Design Editor**:

   a. Display current color
   b. Selection tool
   c. Shapes: Rectangle, Circle, Ellipse, Line, Polygon
   d. Polyline
   e. Add Text and Image
   f. Quadratic and Cubic Bezier curve
   g. Color picker
   h. Add Image and Text Links
   i. 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 the properties sections 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 the properties sections to configure the image as needed.

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

13. To exit the **Badge Design Editor**, select the Close Window icon.
### 10.4 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. To open the module, go to **Management > Badges**.

1. Go to **Management > Badges**.
2. Select **Add**.
3. Select a badge template, then press **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.
     - **Note**: 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 the **Privileges** section.
6. Select **Save and Close** to save the badge configuration.
   - **Note**: Multiple badges can be added to each personnel record.
10.5 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 press **Save**.

5. Restart Entré.

10.6 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. Press **Save**.

4. Restart Entré.

5. To configure the hardware to check and store badge dates, go to **Configuration > Hardware**.
10.7 Edit Badge Group

Edit a 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 the General, Badge Printing, Access Level Groups, User Code Profiles, or Advanced sections as needed.
5. Press OK. A dialog pops up to display the number of badges that were processed or affected.

10.8 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 press Save.
3. Restart Entré. Once the application has been restarted, badges can be added without a PIN.
10.9 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 Expression 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 press 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. Press OK.

7. Edit other badge design settings as needed.

8. Press Save All.

10.10 Badge Status

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

Badger validity

- **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.
10.11 Set Up Badge Printing

Use the Badge Printers section to enable badge printing.

1. Go to Edit > Preferences > Badge Printers.
2. In Configurations, select Add.
3. Select a printer and press Print. In Page Setup, configure the printer, then press OK.
4. Name the setting and press OK. The printer configuration will be added to Configurations.
5. Select the printer and press OK.
6. Go to Management > Badges and select an existing badge or add a new badge to be printed.
7. Select Badge Printing.
8. Select a design for the badge, then press Print.
9. A dialog pops up to configure the default printer. To continue badge printing, select Yes.
10. In Select print configuration, select the printer.
11. To initialize printing, press OK.

10.12 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.

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

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 press OK.
10.13 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. Restart Entré.

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

10.14 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.


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. Press Next.

5. Select a temporary badge, then press 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. 
   Note: 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, press Next. Edit information as needed.

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

10.15  Return a Temporary Badge

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

1. Go to Management > Badges or Management > Personnel.
   
   Note: If using the Badges module, configure it to allow temporary badges to be returned. Go to Configuration > System Configuration, select the Badges section, then select Show return temporary badge in badges module. Press 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.

10.16  Delete Personnel with Badge

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

1. Right click on 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.

Part 11. Configure More Advanced Options

11.1  Use Filters

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

Press 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.


5. Configure the default filter for operator profiles as needed, then press 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. Press 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.


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

6. Select OK.

7. Select the Device section. 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.
   
   **Note:** 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 the **General** section:

- **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.

### 11.2 Create a Profile Template

Use the **Profile Templates** module to create templates.

#### Create a profile template

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

2. Select **Add**. Select a predefined template. For this example, choose **Most restrictive**, then press **OK**.

3. Name the template, then configure template options by selecting **Edit Template**.

4. In **Profile**, select **Enabled** to enable the profile template. Otherwise, the profile remains disabled.

#### Configure the profile

Use the **General**, **Module**, **Device Commands**, or **Data Types** sections. Each section allows specific settings to be enabled or disabled.

1. Go to **Device Commands**.
2. Select a device, then configure the profile’s command abilities by selecting the appropriate options from **Allow command to be issued**. For this example, the profile is allowed (**Yes**) to issue a **Cancel All Batches** command.

**Note:** To configure the default, open the **General** section, select **Miscellaneous**, then check the **Allow issuing device commands as default** checkbox on the left side of the window.

3. If **Allow issuing device commands as default** is selected, the default for the profile’s command abilities will be **Yes**. If deselected, the default will be **No**.

4. To configure a filter for the device command, select **Filter**.

5. To define which data types the profile will be authorized to view and modify, go to **Profile** and select a data type, then select permissions for the profile. For this example, select **Event**, then select both **View** and **Modify** to enable the profile to view and modify events.

6. Press **OK**, then press **Save and Close**.

### 11.3 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. Press **Add**.
3. Choose the device with programming to save as a template.
4. Name the template.
5. Press **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. Press **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 press Next.

4. Name the device, then press Next.

5. Choose appropriate options in Location.


### 11.4 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. **Note:** 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. Press 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. For this example, double-click **DC Driver**.
3. Go to **Location**, then select a location or press **Choose** to select locations from a hierarchical tree.
4. Press **Save and Close**.

**Note:** 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

### 11.5 Bind Profiles to Locations

Bind a profile to a location using the **System Configuration** and **Logins** modules.

**Enable Profile Binding**

1. Go to **Configuration > System Configuration > Logins**.
2. Select **Allow profiles to be bound to locations per assignment**.
3. Press **Save**.
4. Restart Entré.

**Bind a profile to a location**

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

1. Go to **Management > Logins**.
2. Select a login from the table, then select **Edit**.

3. Go to **Profiles** and select **Add**. If a profile is already assigned to the login, select it, then select **Edit**.

4. Select a profile or select **New** to create a new profile.

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

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

7. To finish binding the profile to the location, press **Save and Close**.

### 11.6 Set Up 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 > Partitions**.

2. Select **Add**.

3. Name the partition and enter comments as needed.
   
   **Note:** 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 press **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. Press **Save and Close**.

**Assign badges to a partition**

1. Go to **Badges**, then select **Add** or **Edit**.
2. In **Partition**, select a partition.
3. Select a partition for the schedule that will be used for the access level. For best results, verify that the same partition is used throughout. Press **Save and Close**.
4. Press **Save and Close**.
5. Log out of Entré then log in with the partitioned login.
6. Verify that adding an object defaults to the login’s partition. Notice that objects previously made with a different partition should not show up.
   **Note:** 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.
11.7  Add a Custom Alert Sound

Add customize 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. Press 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 press Save and Close.

11.8  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, continue to Create Watch Levels.

1. Go to Configuration > System Configuration > Miscellaneous.
2. Select Enable Credential Watch Levels.
3. Restart Entré.

Create Watch Levels

1. Go to Advanced > Credential Watch Levels.
2. Select Add. Name the watch level and associate it with a color.
3. Press **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. Press **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 press **Save and Close**.

### 11.9 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. Press **Save and Close**.

6. Right-click the driver and select **Start**.

#### Add automatic rules
Create **Historical Event Driver** commands that execute through the **Automation Driver**. For this example, five automatic 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**. Name the automation rule **Copy 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. Press **OK**.
7. Next to **Actions**, select **Add**.
8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.
9. Press **OK**.
10. Next to **Command**, select **Choose**, then select **Start Copying Live Events**.
11. Press **OK**, then press **Save and Close**.
12. Press **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 **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. Press **OK**.

7. Next to **Actions**, select **Add**.

8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.

9. Press **OK**.

10. Next to **Command**, select **Choose**, then select **Stop Copying Live Events**.

11. Press **OK**, then press **Save and Close**.

12. Press **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 **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. Press **OK**.

7. Next to **Actions**, select **Add**.

8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.

9. Press **OK**.

10. Next to **Command**, select **Choose**, then select **Start Pruning Live Events**.

11. Press **OK**, then press **Save and Close**.

12. Press **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 **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).
   
   **Note:** The trigger time must be set to stop pruning after the selected time to start pruning.
6. Press **OK**.
7. Next to **Actions**, select **Add**.
8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.
9. Press **OK**.
10. Next to **Command**, select **Choose**, then select **Stop Pruning Live Events**.
11. Press **OK**, then press **Save and Close**.
12. Press **Save and Close**.

**Truncate Historical Events**

The final automation rule will be configured to truncate historical events.

1. Go to *Configuration > Automation Rules*.
2. Select **Add**. Name the automation rule **Prune Live Events**.
3. Next to **Trigger**, select **New**, then select **Periodic** for the trigger interval.
4. In **Periodic**, go to **Interval** and select **Monthly**. Define the **Day of month** and **Time of day** that the trigger should occur. For this example, select day 1, then enter 05:00 (05:00 AM).
5. Press **OK**.
6. Next to Actions, select Add.

7. In Device Command, select Single, then select Choose. Select the Historical Events Driver.

8. Press OK.

9. Next to Command, select Choose, then select Truncate Historical Events.

10. Press OK, then press Save and Close.

11. Press 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.

### 11.10 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. Press Save and Close. To run the report, right-click the report and select Run.
11.11 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 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. Press OK.
7. Next to Actions, select Add.
8. In Device Command, select Single, then select Choose. Select the Historical Events Driver.
9. Press OK.
10. Next to Command, select Choose, then select Start Pruning Historical Events.
11. Press OK, then press Save and Close.
12. Press 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 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).

   **Note:** The trigger time must be set to stop pruning after the selected time to start pruning.

6. Press **OK**.

7. Next to **Actions**, select **Add**.

8. In **Device Command**, select **Single**, then select **Choose**. Select the **Historical Events Driver**.

9. Press **OK**.

10. Next to **Command**, select **Choose**, then select **Stop Pruning Historical Events**.

11. Press **OK**, then press **Save and Close**.

12. Press **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 **Legacy Events**.

3. In **Item type**, select **Events (Historical)**, then press **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. Next to **Trigger**, select **New**.

6. In **Type** drop-down, select **Periodic**.

7. In **Interval**, select **Monthly**. Define the **Day of month** and **Time of day** that the report should run, then press **OK**.

8. From the **Action** field, select **Add**, select **Report**, then press **OK**.

9. Select **Choose**, then select the **Legacy Events** report.

10. Press **OK**, then press **Save and Close**.
11. Press **Save and Close**.

### 11.12 Program Card Formats

Program up to eight different card formats. For more information, refer to the appropriate module installation guide from [DMP.com/guides](http://DMP.com/guides).

**Add a card format**

1. Go to **Configuration > Hardware > DMP Driver**.
2. Select **Edit**, then select **Card Formats**.
3. 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.
4. Press **Save and Close**.

### 11.13 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.

**Note**: 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 Tech APP and Dealer Admin.

**Set Up the Wireless License Key**
1. Go to **System Configuration > DMP Communication**.

2. Enter the **Securecom Wireless License Key**.

3. Select **Save**.

4. Log out of all Entré clients and the Entré Application Server to restart the service.

### 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.
   
   **Note:** Entré recognizes the newest SIM codes for AT&T and Verizon.

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 actived SIM populates in the **Cell Module** field.
   
   **Note:** 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. Press **Save and Close**. Press 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**.
   
   **Note:** Panel communication is slower with **Cell**. It may take up to 30 seconds to respond.

2. Right-click on the new panel. Go to **Panel Configuration > Retrieve Configuration**.
3. Press OK.  
   **Note:** Retrieving can take up to 4 minutes with cellular communication, depending on the amount of configured hardware devices on the panel.

### 11.14 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 the **Remote Options** section and enter your remote key.
6. In the Entré tab, select the appropriate communication type and enter information.
7. Press **Save and Close**.

**Retrieve Panel Programming**

1. In the **Hardware Tree**, right-click the new panel. Go to Panel Control > Start.  
   **Note:** Panel communication is slower with Cell. It may take up to 30 seconds to respond.
2. Right-click the new panel. Go to **Panel Configuration > Retrieve Configuration**.
3. The **Retrieve Configuration** dialog pops up to confirm programming retrieval. Press **OK**.  
   **Note:** Retrieving can take up to 4 minutes with Cell, depending on the amount of configured hardware devices on the panel.

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

2. Go to **Remote Options** and edit the **Remote key**.

3. Go to **Configuration > Hardware > Hardware - Tree**. Right-click **localhost - DMP Driver** and press **Restart**.

4. To send the new remote key, push the hardware configuration to the panel.

**11.15 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. Press **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. 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. Press **Save**.

For additional information, see the guide: **How-To Guide: Single Sign On**.
11.16  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.

11.17  Audit Trails and Reports

11.17.1  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 which will be viewed, 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.

11.17.2  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. Set Max. Result to a manageable maximum. A Max. result of -1 displays unlimited results.
4. In Item type, select Events.
5. Select Edit filter.
6. 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.

   **Note:** **This week** equals Sunday to the present day, not the past seven days.

7. In **Log**, press **Choose** and select the appropriate access granted log code.

8. In **Available items**, press the Add icon to open the **Access** tree, then expand the **Access Granted** tree.

9. To add an event to **Selected items**, double-click an event. For example, double-click **Access granted, door used** (log code: MS.TX07090613), then press **OK**.

10. 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.

    **Note:** 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.

11. To limit the report to specific devices, go to **Device** and select a device from **Type**, then press **OK**.

    **Note:** A DC cannot have access events. If a report is not being made for a specific device, select **Access Point**.

12. 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 press **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.

13. Select **Report Settings**, then 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

14. Press **OK**, then press **Save and Close**.

15. To run the report, select the report and press **Run**. To save the report, select **Report**.
11.17.3 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)
   ```
   
   **Note:** 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 press OK.

7. Enter a user prompt for the parameter, then specify the Device type.
   
   **Note:** 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 press OK.


10. To run the report, go to Reports and press Run. The Report Parameters window opens and prompts the user to select a predefined device to report on. Select the device and press OK.

11.17.4 Report Types

The Reports module displays reports saved in the system. Reports may be one of the following types.

Report 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.

**HQL-based**
Defined using explicit HQL.

**SQL-based**
Defined using explicit SQL.

---

**Part 12. Troubleshoot Entré**

**12.1 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.

**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.

### 12.2 Using the Log Files

There are three 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.

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 **appserver.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.

**Note:** 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**.

### Part 13. Entré NOC Features

#### 13.1 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. Select **Find**.

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

5. In **Badges**, select the badge to assign to the key fob. Press **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 press 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. Press **OK**.

6. Continue to program the additional buttons using the sections, as applicable. When you are finished, press **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.

### 13.2 Add a User Code Manually

This feature must be turned on by NOC software support services. Use this feature to manually change the user code displayed in Entré.
Manually add a user code

2. Select Add.
3. Enter a first and last name. Select Badges, then select Add.
4. In the User Code section, you can manually add or generate a user code. Type in a number the user code you would like to assign.
   **Note:** Do not enter a user code already assigned to another user. The system will warn you if you attempt to do so.
5. Fill in the rest of the required fields, then press Save and Close.

Part 14. Compatibility

Panel firmware versions are compatible with the following Entré software versions. See Compatibility Chart: LT-2233.

Part 15. 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.

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.

Cameras

Cameras record digital video files to be stored on the DVR. The parent device of a CCTV Camera is always the DVR. There are no device types which have a CCTV Camera as a parent device.

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 the Miscellaneous section 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.

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

© 2021 Digital Monitoring Products
Command initiates a download of everything.

Download Firmware
Command initiates a download of the most current firmware to a DC.

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.

DVR
Digital Video Recorder. A DVR records video from CCTV Cameras to disk and allows for viewing of live or past video.

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 Entré. 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 Entré. 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 press 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.

Profile Templates Module

Define profile templates. A profile template defines common properties of a profile in Entré. The profile template drop-down will open anytime a profile is added in the system. Navigate to Advanced > Profile Templates to open the module.

Proximity

A technology that allows the presence of certain objects to be sensed by a device without having direct contact.
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.

Reset
Clears the database on a DC.

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.

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.
Site

A site is a single instance of the Entré Access and Security Management database. It generally corresponds to a single geographical location, such as: a building complex, building, or part of a building. Most installations of Entré Access and Security Management only have a single database and hence a single site. For larger configurations, multiple sites are used. For example: if a company has offices around the world, each office would have a separate Entré Access and Security Management database and thus a separate site.

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.

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.

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.

View Query

Filter tool that allows operators to view the actual filter definition as SQL.

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.