

EntraPass web User Manual

Building Technologies & Solutions
www.kantech.com
2024-09-27

A16382MLTM
A
8.72



A16382MLTM-A



Contents

New in EntraPass web 8.72.....	9
Getting started.....	9
System requirements.....	9
Installing EntraPass web.....	9
Security hardening guide.....	9
Views.....	10
Banner.....	10
Options.....	11
Function navigation.....	11
Function header.....	11
Function arrow.....	12
Mandatory fields.....	12
Switch account.....	12
Switching accounts.....	12
Cardholder.....	12
Adding a cardholder.....	13
Enabling go Pass.....	13
ioSmart Mobile Credential.....	14
Adding an identification photo.....	14
Access level.....	14
Options.....	15
Badge.....	15
Tenants.....	16
Additional information.....	16
Comments.....	16
Editing a cardholder.....	16
Generating an audit trail report.....	16
Event.....	17
Video.....	17
Adding a camera to a layout.....	18
Requesting playback recordings.....	18
Controlling a Pan-Tilt-Zoom (PTZ) camera.....	19
View.....	19
Map.....	19
Adding a map.....	21
Adding a component to a new map.....	21
Editing a map.....	22
Duplicating a map.....	22
Deleting a map.....	22
Operations.....	22

Viewing doors, relays, and inputs.....	22
Manually perform actions on doors.....	23
Manually perform actions on elevator doors.....	24
Manually perform actions on relays.....	24
Manually perform actions on inputs.....	25
Intrusion.....	25
Viewing partitions, virtual keypads, and zones.....	25
Manually perform actions on the DSC NEO and PowerSeries partitions.....	26
Manually perform actions on the DSC MAXSYS partitions.....	26
Manually perform actions on a virtual keypad.....	27
Manually perform actions on the DSC NEO zones.....	27
Report.....	27
Generating a quick report.....	27
1 - Filter selection.....	28
2 - Customize.....	28
3 - Processing.....	28
4 - Completed.....	28
Generating a cardholder report.....	28
1 - Report types.....	29
Entire database report.....	29
1 - Report type, entire database.....	29
2 - Customize, entire database.....	29
3 - Processing.....	29
4 - Completed.....	29
Door report.....	29
1 - Report type, Door.....	30
2 - Customize, Door.....	30
3 - Processing.....	30
4 - Completed.....	30
Card type report.....	30
1 - Report type, Card type.....	30
2 - Customize, Card type.....	31
3 - Processing.....	31
4 - Completed.....	31
Access level report.....	31
1 - Report type, Access level.....	31
2 - Customize, Access level.....	31
3 - Processing.....	32
4 - Completed.....	32
Generating a component report.....	32
1 - Report type.....	32
Door - Based on access level.....	32

Door - Based on card type.....	33
2 - Processing.....	33
3 - Completed.....	33
Generating a custom report.....	33
1 - Report selection.....	33
2 - Processing.....	34
3 - Completed.....	34
Action scheduler.....	34
Adding an action.....	34
Access level.....	35
Selecting a component.....	35
Access levels view.....	35
Adding an access level.....	35
Editing an access level or adding an additional door.....	35
Duplicating an access level.....	36
Deleting an access level.....	36
Doors view.....	36
Editing Access level schedules and floors.....	36
Schedule.....	36
Selecting a component.....	37
Adding a schedule.....	37
Editing a schedule.....	38
Duplicating a schedule.....	38
Deleting a schedule.....	38
Holiday.....	38
Adding a holiday.....	38
Editing a holiday.....	39
Duplicating a holiday.....	39
Operator.....	39
Adding an operator.....	40
Password options.....	40
Validation date.....	40
Tenant list.....	40
Adding a tenant list.....	41
Editing a tenant list.....	41
Duplicating a tenant list.....	41
Deleting a tenant list.....	41
Adding a tenant.....	41
Options.....	42
Hardware setup.....	43
Sites and gateways.....	43

Adding a connection.....	43
Editing a site.....	43
Connections.....	43
Adding a connection.....	43
Communication.....	44
Gateway.....	45
Association.....	45
Additional information.....	45
Comments.....	45
Controllers.....	45
Adding a controller.....	45
1 - Controller.....	45
2 - Door options.....	46
3 - Review.....	46
Editing a controller.....	46
Configuration.....	47
Wi-Fi.....	47
Readers.....	47
Defining readers with Kantech ioSmart protocol.....	47
Defining readers with OSDP.....	48
Wireless lock.....	48
Association.....	48
Comments.....	48
Doors - Relays - Inputs.....	48
Doors.....	49
Editing a door.....	49
Contact.....	50
Request To Exit (REX).....	50
Keypad.....	51
Multi-swipe.....	51
Intrusions.....	52
Association.....	52
Comments.....	52
Relays.....	52
Editing relays.....	52
Activation.....	53
Association.....	53
Comments.....	53
Inputs.....	53
Editing inputs.....	53
Timing.....	54

Shunt.....	54
Association.....	54
Comments.....	54
Site info.....	54
Technical support.....	55
Privacy Notice.....	57
Copyright.....	57
OSS disclosure.....	57
End-User License Agreement.....	57

New in EntraPass web 8.72

The EntraPass web 8.72 release provides improved software stability and customer bug fixes.

Getting started

EntraPass web is a web-delivered platform that provides remote real-time access to manage common security tasks and reports from any computer connected to the Internet. This manual provides information about how to install and use EntraPass web.

System requirements

Before you install install EntraPass web, ensure that your device meets the following basic system requirements:

- Core i3 8th Generation processor or better
- 8 GB RAM
- 250 GB hard disk drive space
- Windows® 10 Home or later, or macOS® Mojave or later

❗ **Note:** If your device does not meet these requirements, it may impact your experience with EntraPass web.

Installing EntraPass web

1. On the **EntraPass web download** page, click the **DOWNLOAD** button. Download EntraPass web from the web server where you installed SmartLink. If you encounter problems, click the **Having problems installing EntraPass web?** link.

❗ **Note:** There is one installer version available for download, as the video package DLL used in EntraPass web requires a 32-bit operating system. The 32-bit installer works on a 64-bit operating system.

2. Choose to save the file to your local machine, or run immediately.
3. **Optional:** If you saved the file, click the **EntraPass web** installer package.
4. When the installation finishes, open the client. In the **Log on** window, your system's name appears. If you have more than one system installed, a list of systems appears. Click the system you want.

❗ **Note:** If your system does not appear on the list, click the **Pencil** icon, and copy and paste the system name and URL address into the **System name** and **URL** fields. Click **Save**.

5. Enter your **Username** and **Password**. Click **Login**.

Security hardening guide

About this task:

Kantech recommends the following setup, configuration, and installation measures to ensure the highest level of security for EntraPass. Failure to comply with the following security configuration may result in a weakened operational state with related security vulnerabilities. For more information, refer to your product installation guide for specific instructions.

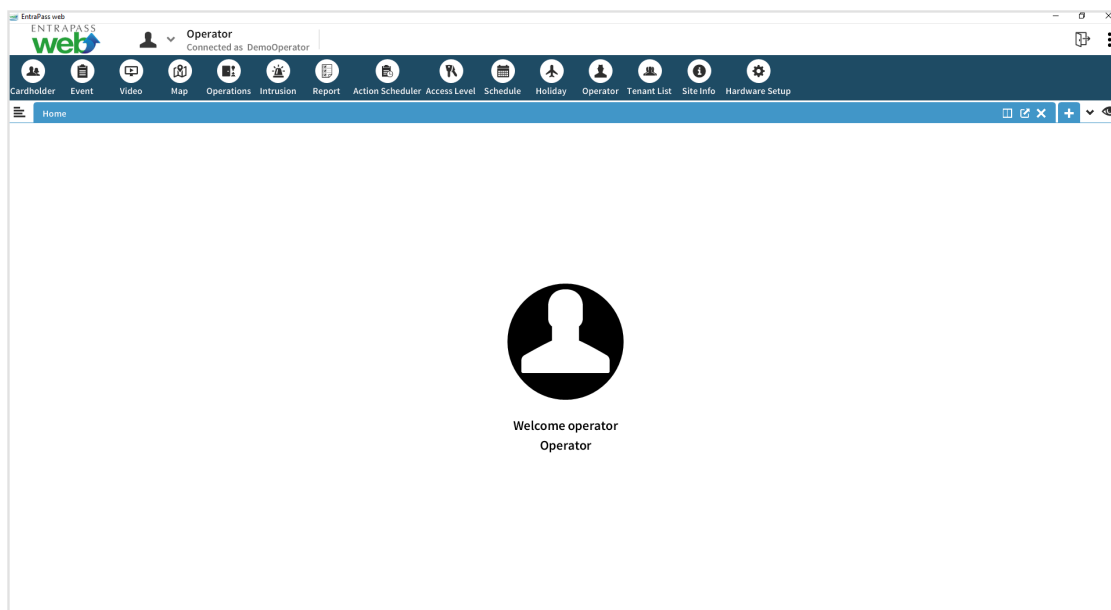
To comply with recommended security standards, complete the following steps:

1. Deploy EntraPass on a Virtual Local Area Network (VLAN).
2. For an encrypted layer of security during data transit, use Hypertext Transfer Protocol Secure (HTTPS) instead of HTTP. You must obtain a Secure Socket Layer (SSL) certificate from a certificate authority (CA), and generate it for the EntraPass web website. For information about how to implement SSL in IIS (Internet Information Services), refer to Microsoft's website. <https://support.microsoft.com/en-nz/help/299875/how-to-implement-ssl-in-iis>
Note: This link is for reference only. Contact Microsoft for support on how to implement SSL.
3. Change default passwords during installation.

Views

The home page displays the banner, the function navigation, the function header, and the function tab sections. The content displayed, and highlighted in these sections changes, but the structure remains consistent.

Figure 1: EntraPass web home page



Banner

The banner section contains the following icons:

- **Operator:** Click to change a **Password**, to **Add photo**, or to **Log out**.
- **Log out:** Click to exit the system.
- **More options:** Click for the following functions:
 - **Options:** Click for more options. For more information, see [Options](#).
 - **Help:** Click to open the *Entrapass web User Manual*.
 - **Exit:** Click to exit the application.

Options

Use **Options** for the following functionality:

- Define the e-mail notification for **Watchlist** recipients.
- View device software details.
- Reset operator settings and warning messages.
- Install software required for some advanced features.

E-mail notification

About this task:

The **e-mail notification** sends a message to defined recipients when an alarm occurs on any item included in the **Watchlist**.

1. In the **Recipients** field, enter an e-mail address. Enter each e-mail address on its own line.
2. From the **Schedule** list, select an associated schedule. The system sends the notification within the schedule start and end time.

Software version

View details of all EntraPass software devices.

Settings

1. For **Operator settings**, click **Reset** to clear operator settings, for example, customized columns and tags.
2. For **Warning dialogs**, click **Reset** to reinstate warnings that were dismissed using the **Don't show again** option.

Installation

Some advanced features require the installation of a package. Click **Install** for the package you want:

- **VideoEdge package** contains the American Dynamics software development kit (SDK).
- **Exacq video package** contains evapi.dll and the EntraPass dynamic-link libraries (DLLs) required for the DVR video features.
- **Virtual Keypad package** contains the EntraPass DLLs required for the intrusion features.

Function navigation

The function navigation contains the operational, configuration, and installation functions available on EntraPass web.

Function header

The function header displays the following items:

- **Switch Account** icon. For more information, see [Switch account](#).
- The selected function tab
- **Split screen** tab
- **Undock** tab
- **Close** tab
- **Add** tab
- **Function** arrow
- **Watchlist** icon. Set up the watchlist in **Operations**.

Function arrow

To view a list of tab functions, click the **Function** arrow:

- **Split tab horizontally**
- **Split tab vertically**
- **Close tab**
- **Close all tab**
- **Close other tabs**
- **Dock all**
- The last section displays all open tabs. Select a tab from the list to bring it into focus.

Function tab

The function tab manages the selected function, and may have many panes. The selected function tab is blue, other open tabs are black.

Mandatory fields

A field with a blue tag containing an asterisk indicates a mandatory field.

Switch account

Use **Switch account** to change from one account to another account. You must have more than one account set up in EntraPass workstation, and the user must have permission to switch accounts.

Note: For more information about creating accounts, refer to the *Account* section in the *EntraPass Administration Guide*.

Switching accounts

1. On the function header, click the **Switch account** icon to open the **Switch account** pane.
2. From the account list, select an account and double-click. Click **Yes** to the **Switch Account** message.
3. Click the **Switch account** icon again to hide the pane.

Note: To return to system level, open the **Switch account** pane, and click the **Return to system** link.

Cardholder

Use **Cardholder** to add, import, or export a user's card details. Cardholder features include access levels, usage restrictions, privileges, badge printing, tenants, and personal information.

The top section of the **Cardholder** tab contains the following buttons:

- **Card view:** displays the **Photo**, **Cardholder name**, **Card type**, **State**, and **Card number** of defined cardholders in a grid format.
- **Table view:** displays the **Photo**, **Cardholder name**, **Card type**, **State**, **Start date**, **End date**, **Card number** and **Using end date** in a table format. For a full list of available columns, right-click on the table header for the context menu.
- **Add:** opens the **Add cardholder** tab, where you can add a new cardholder and define associated options.
- **Import:** imports cardholders in a CSV format.

- **Export:** exports cardholders in a CSV format. The file contains the title of each exported column that you can use as a template for an import.
- **Search:** enter part of a word, or the entire word. The system filters automatically one second after writing in the field, and lists the results alphabetically.
- **Search in:** use to refine your search. The list uses labels applied in the **Additional Information** section.
- **Quick filter:** filters using six common parameters.
- **Reset:** clears all search and filter results.

When you select a cardholder, the following buttons appear:

- **Edit**
- **Last transactions**
- **Print badge**
- **Duplicate**
- **Delete**

Adding a cardholder

1. Click the **Cardholder** tab, and click the **Add** button.
2. In the **Name** field, enter the full name of the cardholder.
3. In the **Card number** field, choose between a five or six digit numerical Wiegand 26-bit format, or a 32-bit global card format. The default card format is HHHH:DDDDD (hexadecimal and decimal 32-bit) for v7.40 and later. For more information about card formats, refer to the *Defining a card display format* in the *Options* section of the *EntraPass Administration Guide*.
4. In the **End date & Exp. Hour** field, select the date you want the card to expire. If you select an end date, the card ceases to function after this date.
5. In the **E-mail** field, enter an e-mail address.
6. In the **Card Type** field, select the appropriate type from the list.
7. **Optional:** For hattrix systems, in the **Filter** field, select the appropriate building to assign to the cardholder.
8. Select the **Trace** check box, if you want to generate an event every time the user presents the card at a reader. You can request and generate a report containing the card traced event.
9. Select the **Lost/Stolen** field, if the user reports the card as lost or stolen. The card ceases to function.

Enabling go Pass

1. Select the **go Pass** check box to use a smartphone as a card. When you select **go Pass**, the following fields are mandatory:
 - **E-mail**
 - **Language**
 - **E-mail notification**
 - **Card number**
 - **End date & Exp. hour**
2. Select the **E-mail notification** check box to receive log on credentials when registering go Pass. EntraPass automatically enters the cardholder's credentials into the go Pass application.
3. From the **Language** list, choose English or French.

ioSmart Mobile Credential

In the **Direct BLE** section, you can use the ioSmart credential features to add extra security or allow users to access doors when they are offline by configuring the **Key Cycle** and **Key Lifespan** fields:

- ▶ **Important:** The **Use Key Cycle** check box is selected by default to enable both the **Key Cycle** and **Key Lifespan** configurations. These features provide optimal security. Do not disable them unless required.
 - **Key Cycle** is an hourly interval of time for which a new key for Bluetooth Low Energy (BLE) authentication is generated. For example, if you enter **4**, then a new key is generated every four hours. You can enter a Key Cycle value between 1 and 72 hours. A low Key Cycle number results in a higher level of security because a new key generates more often.
 - **Key Lifespan** is how long a BLE key is valid. For example, if you enter **8**, then the key is valid for eight hours. The minimum value for Key Lifespan is the same as the Key Cycle value, and the maximum value is twice the Key Cycle value, up to 120 hours. For example, if the Key Cycle is 20 hours, then you can enter a Key Lifespan value between 20 and 40 hours. Enter a high Key Lifespan number for users with inconsistent internet access, such as in remote areas, to allow the user to access a door while offline for up to five days (120 hours).
- ① **Note:** For optimal security results, use a short Key Cycle and Key Lifespan. The Key Cycle default value is 12 and the Key Lifespan default value is 24.
 - To edit the Key Cycle and Key Lifespan values at an account level, click **Account>Options** and the go Pass settings appear.
 - To edit the Key Cycle and Key Lifespan values at a user level, click **Card>Card number** and the go Pass settings appear.
- ① **Note:** To use the ioSmart Mobile Credential feature, you must have the following specifications:
 - go Pass version 2.20 or later
 - ioSmart firmware version 1.09 or later
 - KT-1 version 3.07 or later
 - KT-400 version 3.01 or later

Adding an identification photo

1. Click the **Camera** icon, and choose to import a photo or take a photo if you have a camera on your PC.

Result

For a cardholder, complete the following sections:

- **Access level**
- **Options**
- **Badge**
- **Tenants**
- **Additional information**
- **Comments**

Access level

About this task:

Use access levels to determine where and when the card is valid. The default access level is **always valid**. Cardholders with always valid access, have access to all doors at any time. To restrict access, you must create a specific access level, and configure door exceptions. To create an access level, complete the following steps:

1. Click **Access level** in the lower-left section of the tab, and choose the appropriate site, multi-site gateway, or global gateway. To create sites, see [Sites and gateways](#).
2. From the **Select an access level** list, select the appropriate access level.
3. If you selected a multi-site gateway, click the arrow link to add an additional access level, or a door exception, and click **Add**. A maximum of five access levels are available.
4. **Optional:** If you selected a global gateway, click the arrow link to add a secondary access level, or a door exception, and click **Add**. A maximum of 13 access levels are available.
5. **Select an access level** from the list.
6. In the **Door Exceptions** area, click **Add** to configure door exceptions and schedule.
7. From the **Select door** list, select a door.
8. From the **Select schedule** list, select a schedule. To create a schedule, see [Schedule](#).
9. Choose to either **Include** or **Exclude** the selected door and schedule.

Options

1. In the **Validation date** area, the **Start date** indicates the card creation date. Click the calendar to choose the date.
2. In the **End date** field, click the calendar to select the date you want the card to expire.
3. To delete a cardholder from EntraPass when the card reaches expiry date, select the **Delete when expired** check box. Use this option with the **End date** field. If a card expires and is not deleted, previous events generated by this card are stored in the archive file.
4. To limit the number of times a cardholder can use the card within the validation date, select the **Enable usage restriction** check box, and in the **Maximum card usage** field, enter the number.
5. If you want the counter to return to zero when the cardholder reaches the limit, select the **Reset to zero** check box.
6. In the **PIN parameters** area, select the **Wait for keypad** check box to force users to enter a PIN to access all doors. Enter the cardholder's four or five digit personal identification number in the **PIN** field.
 - ① **Note:** The system denies access to the door until the cardholder enters the correct PIN. PIN access is only required when the door is defined with a reader and a keypad. Use **Hardware Setup** to define a door with a reader and a keypad. The keypad schedule must also be valid for the door.
7. In the **Privileges** area, select **Extended Delay** to facilitate a cardholder with a physical disability. Define the appropriate delay for the door in **Hardware Setup**.
8. To override a defined passback configuration, select the **Disable passback** option.
9. To swipe a card two or three times on a KT-400 or KT-1 reader, select the **Multi-swipe** check box.
10. To override door security measures, select the **Privilege operation** check box. Set the Supervisor level according to the cardholder's privileges.


Badge

1. From the **Layout** list, select a layout.

2. To preview and print the badge, click **Preview badge**.
3. To choose a predefined barcode or enter a custom barcode, click **Add barcode**.
4. To upload a new signature, click the **Add signature** link.
5. For hatatrix systems, select the **Request print badge** check box to print the badge.
6. To activate the cardholder's badge in the system, click **Activate badge**.

Tenants

1. To link the cardholder to a tenant, click **Link a tenant**.
2. To find a tenant, complete one of the following:
 - Enter a name in the **Search** field.
 - Select a group from the **Tenant list**. A results table lists all the tenants in that group with associated **ID**, **PIN**, **Phone number**, and **Access schedule**.
3. To create a new tenant profile, click **Quick add**.
 - a. In the **Tenant name** field, enter a name.
 - b. In the **ID** field, enter an ID.
 - c. In the **PIN** field, enter a four to six digit number.
 - d. In the **Phone number** field, enter a phone number.
 - e. From the **Access schedule** list, select a schedule.

 **Note:** You can complete the tenant's profile in the **Tenant List** function.
4. To edit a tenant, select the tenant and click **Quick edit**. Follow Steps 3 a to e.

Additional information

About this task:

For additional information, use fields with editable labels for company specific requirements:

- Corporate Edition, 10 fields.
 - Global Edition, 40 fields.
1. Hover the mouse over the field label, and a **Pencil** icon appears. To open the **Edit information** label, click the **Pencil** icon.
 2. In the **Primary language** field, enter the label you want.
 3. **Optional:** In the **Secondary language** field, enter the label in a different language.

Comments

Use the free text comment box for content not catered for in the previous sections.

Editing a cardholder

To edit a cardholder, complete the following steps:

1. Click the **Cardholder** tab, and select a cardholder from the table or grid view.
2. Click **Edit**.

Generating an audit trail report

About this task:

Define who has access to the **Audit Report** icon in the EntraPass Workstation in the **System** tab.

1. To open an audit window, click the **Audit trail** button.

The window has two tables, the first table contains the following card information:

- **Date and time:** the date and time the operator created, modified, or deleted the card.
- **Operator:** the name of the operator who made the change.
- **Changed** the number of fields that were changed.

The second table contains the following card information:

- **Data type:** the database data type;
 - **TimeStamp**
 - **Integer**
 - **Object**
 - **Components**
- **Field name:** the name of the GUI field.
- **Old value:** the value before the change occurred.
- **New value:** the value when the system saved the change.

The results show the last five modifications that occurred on the card.

2. To print the entire contents of the card audit trail to a CSV file, right-click a table entry.

Event

The **Event** tab receives and displays system events that are current, or historical. The table columns include: **Date and time**, **Event**, and **Description**. Different colors on event rows indicate different events. The configuration in the EntraPass workstation server determines the events displayed.

The top section of the **Event** tab contains the following buttons:

- **Display map**
- **Display live**
- **Display replay**
- **Display cardholder**
- **Display device**

When you select an event, buttons relevant to the event appear. When you click the button, the associated map, video, cardholder, or device opens in a new tab.

Video

Use **Video** to define video views for viewing and monitoring purposes. You can associate components including sites, and controllers with video views. Define the video server and cameras using EntraPass workstation.

The top section of the **Video** tab contains the following buttons:

- **Cameras** button: displays a list of existing cameras in the left panel.
- **Views** button: displays a list of existing views in the left panel. A view is a saved layout with preferred cameras and servers.
- **Camera layout** option buttons: If more cameras exist than the layout displays, the system displays the first cameras. See the following list for nine different layout options:
 - One camera
 - Four cameras
 - Six cameras
 - Seven cameras

- Eight cameras
- Nine cameras
- Ten cameras
- Thirteen cameras
- Sixteen cameras
- **Clear** button: removes all cameras from the displayed view. If you clear the view, the **Add as a view**, **Full screen**, and **Playback** buttons become unavailable.
- **Add as a view** button: click to add a new layout with preferred cameras and servers.
- **Full screen** button: displays the current layout in full screen.
- **On screen display** check box: select to display the server name, and the camera name next to each camera.
- **Playback** button: displays the playback view for all cameras in the selected view.

Adding a camera to a layout

1. Click the **Video** tab, click the **Cameras** button, and click the camera layout option you want.
2. Drag a camera from the left panel and drop it into one of the sections in the layout. If you select a camera, the **Full screen**, **Replay** and **Playback** buttons appear.
3. To bring the camera view to a full screen window, click **Full screen**. To return to the original layout, press the **Esc** button on the keyboard.
4. To view the last 30 seconds of recording, click the **Replay** button. To control viewing, use the **Play**, **Pause** button, and play bar.
5. To open the playback window, click the **Playback** button.

Requesting playback recordings

1. On a layout, select a camera, and click the **Playback** button. A request for playback applies to all cameras displayed. The playback window appears, and contains the following functions:
 - a. **Start date**: is the current date.
 - b. **Start hour**: is the current time minus one hour.
 - c. **Duration**: the default duration is one hour. Select up to a maximum of 99 hours 59 minutes.
 - d. **Start**: sends the playback request to the DVR.
 - e. **Cancel**: cancels a request in progress.
 - f. **Play toolbar**: contains Fast rewind, Rewind, Pause, Play and Fast forward buttons.
2. To request the previous hour's recording, click **Start**.

- ① **Note**: During a playback session, live video function stops and the **Export video** button, and the **Snapshot** button appear. The playback recordings appear on the lower section of the window. A timeline appears at the top. A **Rewind** button is at the beginning of the timeline and a **Forward** button is at the end. Use the **Rewind** and **Forward** buttons to move left or right on the time scale. When the player starts, a progress bar indicates the time position. Playback bars under the timeline represent the camera or cameras. The following colors on the playback indicate motion triggers:
- **Gray**: no recording.
 - **Green**: no motion or alarm event recorded.
 - **Blue box**: motion detected.
 - **Red box**: alarm detected.

3. To export the video, click the **Export video** button, and save to your local machine.
4. To export a snapshot of the current view, click the **Snapshot** button, and save to your local machine.
5. To exit **Playback**, click the **Live** button.

Controlling a Pan-Tilt-Zoom (PTZ) camera

1. To activate the PTZ controls, select a PTZ camera. A **virtual joystick** with arrows in four directions and a circle in the center appears.
2. Move the center of the joystick in the direction you want to move the camera. To zoom the camera in and out, use the mouse wheel, or press the + and - signs on the keyboard.
3. To preset different camera positions, click the **Preset** icon on the lower-right section of the screen. All the presets associated with the PTZ camera display.
4. To add a new preset position, click the + icon , enter a new name and click **Save**. To view additional commands, select a preset from the menu list:
 - **Add**: a dialog box opens and prompts you to enter a name for the new preset.
 - **Rename**: a dialog box opens and prompts you to enter a new name for the preset.
 - ① **Note**: The **Rename** option is available for Exacq cameras only.
 - **Update/Replace**: if you confirm the prompt, the system saves the current position of the camera in the preset.
 - **Delete**: if you confirm the prompt, the system deletes the current preset.

View

1. Click the **Views** button for a list of saved layouts with selected cameras.
2. To select a view, click the view, or hover over the view and wait for the mouse pointer to change to a cross. You can now drag the view to the layout.
3. To delete a view, select the view and right-click for the context menu. Click **Delete**.

Map

A graphic map corresponds to a secured area of the system where components are located on a connection. With maps, you can view the exact location of a component, for example a door, an input, a camera, an alarm partition, and a zone.

You can perform manual operations directly from the component and execute tasks with or without confirmation. When you right-click the component, a context menu appears with a list of appropriate operations. You can assign a specific action to the icon by using the double-click action, when editing a map.

You can create as many maps as you need. Each map displays up to 250 components, including using live video as a background. The option to import graphics, or maps from other programs is also available. Choose from the following formats: BMP, EMP, WMF, JPEG, GIF, PCX, PNG, TIF, and PCD.

For category component icons, see the following table. A context menu for each icon lists the various operations available for each component. The icon changes to reflect a status change.

Table 1: Component icons












Icon	Name	Component description	Context menu actions
	Door	Door locked	Lock Unlock One time access Temporary unlock Back to schedule Set unlock schedule Clear unlock schedule Arm Disarm Enable reader Disable reader Display live Disable door contact Door contact back to schedule Last access Full access Edit in new tab
	Elevator	Elevator locked	Same as door actions
	Relay	Relay	Activate Deactivate Temporary activate Back to schedule Full status Edit in new tab
	Input	Input	Normal supervision Continuous supervision No supervision No supervision temporarily
	Map	Indicates a lower level map.	Display map
	Camera	Camera indicates the location of a camera.	Display live
	Video view	—	Display live
	Video server	—	
	Intrusion panel	—	Full status

Table 1: Component icons

Icon	Name	Component description	Context menu actions
	Intrusion components	Partition	Partition armed away Partition armed stay Partition armed no entry delay Partition armed with code Disarm partition with code Full status <i> ⓘ</i> Note: Actions vary according to the type of intrusion panel.
	System	—	Default double-click action Pointer position Remove icon

The top section of the **Map** tab contains the following buttons:

- Add
- Edit
- Duplicate
- Delete

The left pane contains a list of the existing maps.

Adding a map

1. Click the **Map** tab, and click the **Add** button.
2. The system automatically displays the first item on the list. Click the list to select another map.
3. In the **Primary language** field, enter a name for the map.
4. Optional: In the **Secondary language** field, enter a name in a different language.
5. Click the **Add map image** button and add the appropriate map.
6. If you want to change the map, click the **Change map image** button. If you want to remove the map, click **Remove map image**. Click **Save**.

Adding a component to a new map

1. Go to the component category in the left pane, and drag and drop the component to a specified location on the map. Once you have used the component, it is no longer available in the left pane.
2. To identify the name of the component, hover the mouse over the component.
3. To assign a double-click action to a component, right-click the component for the context menu, click **Default double-click action**, and click the appropriate component action.
4. To point the component icon in the correct direction, select the component, and click the appropriate pointer position: **Top**, **Bottom**, **Left**, **Right**.
5. To remove a component icon, click **Remove icon**. Click **Save**.
 ⓘ **Note:** If a component category is unavailable, it means you have not defined it in **Hardware setup**, or EntraPass web does not support the component.

Editing a map

1. Click the **Map** tab, select a map from the left pane, and click the **Edit** button.
2. Repeat Steps 1 to 5 in **Adding a component to a new map**.

Duplicating a map

1. Click the **Map** tab, select a map from the left pane, and click the **Duplicate** button.
2. Click the **Duplicate** button. The **Duplicate map** tab appears.
3. In the **Primary language** field, enter a name for the new map.
4. Optional: In the **Secondary language** field, enter a name in a different language. Click **Save**.

Deleting a map

1. Click the **Map** tab, and select a map from the left pane.
2. Click **Delete**. A message appears asking **Do you want to delete this map?** Click **Delete** again to confirm the deletion.

Operations

Use **Operations** to view, and to perform operations on the doors, relays, and inputs in a site or gateway in real-time. To modify doors, relays, and inputs, go to the **Hardware setup** function.

The top section of the **Operations** tab contains the following list and check boxes:

- **All sites and gateways**
- **Doors**
- **Relays**
- **Inputs**

Viewing doors, relays, and inputs

1. On the **Operations** tab, select one of the following from the **All sites & gateways** list:
 - **All sites & gateways.**
 - **An individual site.**
 - **An individual gateway.**

① **Note:** The first time you use the list, **All sites & gateways** is the default, but for subsequent usage, the system remembers your last choice.
2. Depending on what you want to view, select one or all of the following component check boxes:
 - **Doors**
 - **Relays**
 - **Inputs**

Result

The components associated with that site or gateway appear, with icons to indicate their status.

When you select a component, the component appropriate actions appear in the top section of the **Operations** tab.

Select one or all of the following three icons on the top section of the component appropriate to your requirements:

- **Pin:** to pin the component to the beginning of the list.
- **Magnifying glass:** to view a full status on the component.
- **Watch:** to watch important events from the component.

See the following table for component colors that indicate different states.

Table 2: Component color

Component color	State
Gray	Disconnected
Black	Normal/Ready/Deactivated
Blue	Activated
Orange	Pre-alarm/Stay
Red	Alarm

See the following sections for manual actions you can perform on doors, relays, and inputs. Depending on your action choice, icons appear in the lower section of the component box.

Manually perform actions on doors

When you select a door, the following door actions appear in the top section:

- **Lock:** Manually locks the selected door.
- **Unlock:** Manually unlocks the selected door.
- **One time access:** Allows a single access to the selected door. When a cardholder triggers the contact, the one time access expires.
- **Temporary unlock:** Temporarily unlocks a door for a specified time. Enter a time delay in the digit field. When the delay expires, the door relocks automatically.
- **Back to schedule:** To revert to the defined locking schedule for the selected door.
- **Unlock schedule, Set:** Selects an unlock schedule for the selected door.
- **Unlock schedule, Clear:** Clears any previously set unlock schedule.
- **Arm:** Sends an arming request to the alarm panel.
- **Disarm:** Sends a disarming request to the alarm panel.
 - ⓘ **Note:** **Arm** and **Disarm** are available only for wireless locks, or doors controlled by a KT-1 or KT-400 under a multi-site gateway.
- **Display live:** If you defined video in the door settings, the video displays live.
 - ⓘ **Note:** If a button is unavailable, it means the door is already in that state.

The following actions are available in the context menu. Right-click the door to view the following actions:

- **Enable reader:** Sends an enable request to the reader.
- **Disable reader:** Sends a disable request to the reader.
- **Disable door contact:** Disables the door contact.
- **Door contact back to schedule:** Reverts to the defined normal schedule for the contact
- **Last access:** Indicates the cardholder who last accessed the door.
- **Full status:** Provides a summary of the current actions defined for the door.

Note: If a button is unavailable, it means the reader is already in that state.

- **Edit in new tab:** Opens the **Hardware setup** tab, where you have access to all doors, relay, and inputs settings. If the **Edit in New tab** is unavailable, it means the user does not have access to the **Hardware setup** function.

Manually perform actions on elevator doors

When you select an elevator door, the following elevator door actions appear in the top section of the screen:

- **Lock:** Manually locks the selected floors from the list.
When you select an elevator door, the following elevator door actions appear in the top section of the screen:
- **Lock:** Manually locks the selected floors from the list.
- **Unlock:** Manually unlocks the selected floor group from the **Floor Group** list, or the selected floors from the **Floor List**.
- **One time access:** Allows a single access to the selected floor group from the **Floor Group** list, or the selected floors from the **Floor List**. When a cardholder triggers the contact, the one time access expires.
- **Temporary unlock:** Temporarily unlocks the selected floor groups from the **Floor Group** list, or the selected floors from the **Floor List**. Enter a time delay in the digit field. When the delay expires, the elevator door relocks automatically.
- **Back to schedule:** Reverts to the defined locking schedule for the selected floors.

The following actions are available in the context menu. Right-click the elevator door to view the following actions:

- **Disable floor:** Manually disables the selected floor groups from the **Floor Group** list, or the selected floors from the **Floor List**.
- **Enable floor:** Manually enables the selected floors.
- **Enable reader:** Sends an enable request to the reader.
- **Disable reader:** Sends a disable request to the reader.
- **Last access:** Indicates the cardholder who last accessed the door.
- **Full status:** Provides a summary of the current actions defined for the door.
- **Edit in new tab:** Opens the **Hardware setup** tab to access all door, relay, and input settings. If the **Edit in new tab** is unavailable, the user does not have access to the Hardware setup function.

Manually perform actions on relays

Select a relay, and the following relay actions appear in the top section:

- **Activate:** to activate a relay, which was previously deactivated by an operator, event, schedule, or input in alarm.
- **Deactivate:** to deactivate a relay, which was previously activated by an operator, event, schedule, or input in alarm.
- **Temporary activate:** to temporarily activate a relay, or group of relays for a specified time. Enter a time delay in the digit field. When the delay expires, the relay deactivates automatically.
- **Back to schedule:** to revert to the defined schedule for the selected relay.

Note: If a button is unavailable, it means the relay is already in that state.

In addition to the above relay actions, the following actions are available in the context menu. Right-click a relay to view the following actions:

- **Full status:** provides a summary of the current actions defined for the relay.
- **Edit in new tab:** opens the **Hardware setup** tab, where you have access to all doors, relay, and inputs settings. If **Edit in New tab** is unavailable, it means the user does not have access to the **Hardware setup** function.

ⓘ **Note:** If a button is unavailable, it means the relay is already in that state.

Manually perform actions on inputs

Select an input, and the following input actions appear in the top section:

- **Normal supervision:** to revert to the defined state in the **Hardware setup** function.
- **Continuous supervision:** to monitor the selected input at all times.
- **No supervision:** to terminate the supervision of the selected input, regardless of its schedule, and start monitoring with the next pre-defined schedule.
- **Temporary no supervision:** to stop temporarily the supervision of the selected input. Enter a time delay in the digit field. When the delay expires, the input reverts to the defined schedule automatically.

ⓘ **Note:** If a button is unavailable, it means the input is already in that state.

In addition to the above input actions, the following actions are available in the context menu. Right-click the door to view the following actions:

- **Full status:** provides a summary of the current actions defined for the input.
- **Edit in new tab:** opens the **Hardware setup** tab, where you have access to all doors, relay, and inputs settings. If **Edit in New tab** is unavailable, it means the user does not have access to the **Hardware setup** function.

Intrusion

Use **Intrusion** to view and manually change in real-time the status of some actions on partitions, virtual keypads, and zones in a multi-site or global gateway.

The top section of the **Intrusion** tab contains the following list and check boxes:

- **Gateways**
- **Partitions**
- **Virtual keypads**
- **Zones**

Viewing partitions, virtual keypads, and zones

1. On the **Intrusion** tab, select a gateway from the gateway list.
2. Depending on what you want to view, select one or all of the following component check boxes:
 - **Partitions**
 - **Virtual keypads**
 - **Zones**

- ① **Note:** The components associated with the selected gateway appear, with icons to indicate their status. When you select a component, the appropriate component actions appear in the top section of the **Intrusion** tab.
3. Select one or all of the following three icons on the top section of the component appropriate to your requirements:
- **Pin:** to pin the component to the beginning of the list.
 - **Magnifying glass:** to view a full status on the component.
 - **Watch:** to watch important events from the component.

Result

Different component colors indicate the following states:

- Gray: offline
- Green: ready
- Black, when a zone is in alarm and the system is not armed: not ready
- Orange: armed with either entry or exit delays
- Blue: armed
- Red: in alarm

- ① **Note:** If an armed partition has a false alarm, and the zone returns to normal, the partition stays in the **In alarm** status until the partition is disarmed. When a cardholder enters the first zone of an armed partition, the system activates the entry delay.

Manually perform actions on the DSC NEO and PowerSeries partitions

Select a partition, and the following partition actions appear in the top section:

- **Partition armed away:** to arm the area when all cardholders leave the area.
- **Partition armed stay:** to arm the perimeter of the area while cardholders remain in the area.
- **Partition armed no entry delay:** to arm the area when no one else will enter the area.
- **Partition armed with code:** to use a code to arm the site.
- **Disarm partition with code:** to use a code to disarm the site.

- ① **Note:** If a button is unavailable, it means the partition is already in that state.

In addition to the above partition actions, the following actions are available in the context menu. Right-click the partition to view the following action:

- **Full status:** provides a summary of the current actions defined for the partition.

Manually perform actions on the DSC MAXSYS partitions

Select a partition, and the following partition actions appear in the top section:

- **Partition armed with code**
- **Disarm partition with code**
- **Output 1 Toggle**
- **Output 2 Toggle**
- **Output 3 Toggle**
- **Output 4 Toggle**
- **Output 5 Toggle**

- **Output 6 Toggle**
- **Output 7 Toggle**
- **Output 8 Toggle**

Note: If a button is unavailable, it means the partition is already in that state.

In addition to the above partition actions, the following actions are available in the context menu. Right-click the partition to view the following actions:

- **Full status:** provides a summary of the current actions defined for the partition.

Manually perform actions on a virtual keypad

About this task:

Select a keypad, and a **Keypad** button appears in the top section:

1. To use the virtual keypad, click the **Virtual keypad** button.
2. When finished, click the **Exit** button on the virtual keypad.

Manually perform actions on the DSC NEO zones

Select a zone, and the following zone actions appear in the top section:

- **Zone bypass:** to exclude a specific zone before arming the system.
- **Zone unbyypass:** to clear a bypass.

Note: If a button is unavailable, it means the zone is already in that state.

In addition to the above zone actions, the following actions are available in the context menu. Right-click the zone to view the following actions:

- **Full status:** provides a summary of the current actions defined for the zone.

Report

Use the Report function to generate the following report types:

- **Quick report:** generate a quick report based on basic events.
- **Cardholder report:** generate a detailed cardholders report.
- **Component report:** generate a door list report based on access level or card type.
- **Custom report:** generate a custom report based on an existing template.

Generating a quick report

About this task:

Four buttons in the upper function section indicate which stage of the report you are currently defining. The following list outlines the stages:

1. **Filter selection**
2. **Customize**
3. **Processing**
4. **Completed**

1 - Filter selection

1. In the **Event selection** area, select the event or events you want in the report. If you want to include all events, select the **All events** check box.
2. In the **Interval** area, choose one of the following options:
 - **Start date & time**, and **End date & time** fields: to select specific start and end dates.
 - **Last 24 hours**, is the default choice.
 - **Last 72 hours**
 - **Last 5 days**
 - **Last 7 days**
3. In the **Event type** area, choose one of the following options:
 - **Normal**: includes events that occurred under normal circumstances.
 - **Abnormal**: includes events that occurred outside normal circumstances.
 - **Normal & Abnormal**: includes events that occurred under normal circumstances, and outside normal circumstances.
 - **Watchable**: includes events listed in the Watchlist.
4. In the **Output** area, select one of the following options from the **Output destination** button:
 - **Local**: to save the report to your computer.
 - **Email**: to send the report from the server.
5. Click **Next**.

2 - Customize

1. In the **Select columns** area, click the **Add/Subtract** button to open the column list.
2. Labels with a tick next to them appear in the report. Click the label once to select it, and click again to clear it. The **Date** label is mandatory.
3. Click **Next** to proceed to the **Processing** stage, or click **Previous**, to return to the **Filter selection** section.

3 - Processing

During the **Processing** stage, you see a process circle indicate the process activity. Once completed the system automatically proceeds to the **Completed** stage.

4 - Completed

1. The generated report appears. Choose one of the following export options:
 - **Export as PDF**
 - **Export as Excel**
2. Click **Finish**.

Generating a cardholder report

About this task:

Four buttons in the upper function section indicate which stage of the report you are currently defining. The following list outlines the stages:

1. **Report type**
2. **Customize**

3. **Processing**
4. **Completed**

1 - Report types

In the **Choose cardholder** list based on area, choose one of the following options to base the report:

- **Entire database:** to select all users for the report.
- **Door:** to select a specific door, or doors for the report.
- **Card type:** to select a specific card type for the report.
- **Access level:** to select a specific access level for the report.

Entire database report

To print a report of the entire database, complete the following steps:

1 - Report type, entire database

Select **Entire database**, and click **Next** to proceed to the **Customize** stage.

2 - Customize, entire database

1. In the **Select columns** area, click the **Add/Subtract** button to open the column list.
2. Labels with a tick next to them appear in the report. Click the label once to select it, and click again to clear it. The **Name** label is mandatory.
3. In the **Define filters** area, select the parameters to filter the report results. Parameters are grouped into five categories:
 - **By card state**
 - **By cardholder state**
 - **By feature**
 - **By group**
 - **By field**
4. To select a parameter, select the check box, or select from the parameter list.
5. Click **Next** to proceed to the **Processing** stage, or click **Previous**, to return to the **Report type** stage.

3 - Processing

During the **Processing** stage, you see a process circle indicate the process activity. Once completed the system automatically proceeds to the **Completed** stage.

4 - Completed

1. The generated report appears. Choose one of the following export options:
 - **Export as PDF**
 - **Export as Excel**
2. Click **Finish**.

Door report

To print a report for an individual door, all doors in a site, or all doors in all sites, complete the following steps:

1 - Report type, Door

About this task:

In the **Choose door** area, you see a list of all sites and their associated doors.

1. Under the site name, click the arrow to view defined doors for the site.
2. To select each door individually, select the check box next to the door.
3. To select all doors in a site, select the **Select all** check box, next to the arrow label.
4. To select all doors in all sites, select the **Select all doors** check box.
5. To view sites only, click the **Collapse all** view.
6. To view sites and doors, click the **Expand all** view.
7. Click **Next** to proceed to the **Customize** stage.

2 - Customize, Door

About this task:

In the **Choose door** area, you see a list of all sites and their associated doors.

1. In the **Select columns** area, click the **Add/Subtract** button to open the column list.
2. Labels with a tick next to them appear in the report. Click the label once to select it, and click again to clear it. The **Door** and **Name** labels are mandatory.
3. In the **Define filters** area, select the parameters to filter the report results. Parameters are grouped into five categories:
 - **By card state**
 - **By cardholder state**
 - **By feature**
 - **By group**
 - **By field**
4. To select a parameter, select the check box, or select from the parameter list.
5. Click **Next** to proceed to the **Processing** stage, or click **Previous**, to return to the **Report type** stage.

3 – Processing

During the **Processing** stage, you see a process circle indicate the process activity. Once completed the system automatically proceeds to the **Completed** stage.

4 – Completed

1. The generated report appears. Choose one of the following export options:
 - **Export as PDF**
 - **Export as Excel**
2. Click **Finish**.

Card type report

To print a report for an individual card type, or all card types, complete the following steps:

1 – Report type, Card type

About this task:

In the **Choose card type** area, you see a list of all card types defined in the system.

1. To select each card type individually, select the check box next to the card type.

2. To select all card types, select the **Select all card types** check box.
3. Click **Next** to proceed to the **Customize** stage.

2 - Customize, Card type

1. In the **Select columns** area, click the **Add/Subtract** button to open the column list.
2. Labels with a tick next to them appear in the report. Click the label once to select it, and click again to clear it. The **Card type** and **Name labels** are mandatory.
3. In the **Define filters** area, select the parameters to filter the report results. Parameters are grouped into five categories:
 - **By card state**
 - **By cardholder state**
 - **By feature**
 - **By group**
 - **By field**
4. To select a parameter, select the check box, or select from the parameter list.
5. Click **Next** to proceed to the **Processing** stage, or click **Previous**, to return to the **Report type** section.

3 – Processing

During the **Processing** stage, you see a process circle indicate the process activity. Once completed the system automatically proceeds to the **Completed** stage.

4 – Completed

1. The generated report appears. Choose one of the following export options:
 - **Export as PDF**
 - **Export as Excel**
2. Click **Finish**.

Access level report

To print a report for an individual access level, all access levels in a site, or all access levels in all sites, complete the following steps:

1 – Report type, Access level

About this task:

In the **Choose access level** area, you see a list of all sites, and their associated access levels.

1. Under the site name, click the arrow to view defined access levels for the site.
2. To select each access level individually, select the check box next to the access level.
3. To select all access levels in a site, select the **Select all** check box, next to the arrow label.
4. To select all access levels in all sites, select the **Select all access levels** check box.
5. To view sites only, click the **Collapse all** view.
6. To view sites and doors, click the **Expand all** view.
7. Click **Next** to proceed to the **Customize** stage.

2 – Customize, Access level

1. In the **Select columns** area, click the **Add/Subtract** button to open the column list.

2. Labels with a tick next to them appear in the report. Click the label once to select it, and click again to clear it. The **Access level name**, **Name**, and **Card number** labels are mandatory.
3. In the **Define filters** area, select the parameters to filter the report results. Parameters are grouped into five categories:
 - **By card state**
 - **By cardholder state**
 - **By feature**
 - **By group**
 - **By field**
4. To select a parameter, select the check box, or select from the parameter list.
5. Click **Next** to proceed to the **Processing** stage, or click **Previous**, to return to the **Report type** section.

3 – Processing

During the **Processing** stage, you see a process circle indicate the process activity. Once completed the system automatically proceeds to the **Completed** stage.

4 – Completed

1. The generated report appears. Choose one of the following export options:
 - **Export as PDF**
 - **Export as Excel**
2. Click **Finish**.

Generating a component report

About this task:

Three buttons in the upper function section indicate which stage of the report you are currently defining. The following list outlines the stages:

1. **Report type**
2. **Processing**
3. **Completed**

1 – Report type

In the **Select type** area, choose from the following options:

- **Door – Based on access level**
- **Door – Based on card type**

Door – Based on access level

About this task:

In the **Choose access level** area, you see a list of all sites and their associated doors.

1. Under the site name, click the **arrow** to view defined doors for the site.
2. To select each door individually, select the check box next to the door.
3. To select all doors in a site, select the **Select all** check box, next to the **arrow** label.
4. To select all doors in all sites, select the **Select all doors** check box.
5. To view sites only, click the **Collapse all** view.

6. To view sites and doors, click the **Expand all** view.
7. Click **Next** to proceed to the **Customize** stage.

Door - Based on card type

About this task:

In the **Choose card type** area, you see a list of all card types.

1. To select a card type, select the check box next to the label.
2. To select all card types, select the **Select all card types** check box.
3. Click **Next** to proceed to the **Processing** stage, or click **Previous**, to return to the **Report type** section.

2 – Processing

During the **Processing** stage, you see a process circle indicate the process activity. Once completed the system automatically proceeds to the **Completed** stage.

3 – Completed

1. The generated report appears. Choose one of the following export options:
 - **Export as PDF**
 - **Export as Excel**
2. Click **Finish**.

Generating a custom report

About this task:

You must configure custom reports in the EntraPass workstation. Three buttons in the upper function section indicate which stage of the report you are currently defining. The following list outlines the stages:

1. **Report selection**
2. **Processing**
3. **Completed**

1 – Report selection

1. In the **Choose report** area, select a report from the list. The list of reports available depends on your company's requirements.
2. In the **Interval** area, choose one of the following options:
 - **Start date & time**, and **End date & time** fields: to select specific start and end dates.
 - **Last 24 hours, is the default choice.**
 - **Last 72 hours**
 - **Last 5 days**
 - **Last 7 days**
3. In the **Output** area, for all reports, select one of the following options from the **Output destination** button:
 - **Local**: to save the report to your computer.
 - **Email**: to send the report from the server.
4. Click **Next**.

2 – Processing

During the **Processing** stage, a process circle indicates the process activity. Once completed the system automatically proceeds to the **Completed** stage.

3 – Completed

1. The generated report appears. Choose one of the following export options:
 - **Export as PDF**
 - **Export as Excel**
2. Click **Finish**.

Action scheduler

Use **Action Scheduler** to create one-off actions, or recurring actions. You can apply tags to actions and use the tags to filter the type of actions displayed. To enable action scheduler in EntraPass web, assign the security level **Action scheduler operation** to the user in EntraPass workstation.

The top section of the **Action Scheduler** tab contains the following buttons:

- **Add**
- **Export as PDF**
- **Export as Excel**

Adding an action

1. Click the **Action Scheduler** tab, and click the **Add** button.
2. In the **Primary language** field, enter the action name.
3. Optional: In the **Secondary language** field, enter the action name in a different language.
4. In the **Schedule** area, select the action you want to occur.
5. In the **date** field, select the day, and enter the time to complete the action. The action you select determines the names of the date field, and if you need to complete an additional time field.
6. Select a tag from the **Tag** list. Each new name generates a new tag. Fifty tags is the maximum amount possible.
7. If you want to delete an action once it has executed, select the **Delete action when expired** check box.
8. If you want the action to repeat, select a type of recurrence from the **Frequency** list. These are the frequency options:
 - None
 - Daily
 - Weekly
 - Monthly
 - Annually
9. In the **Counter** field, select how many recurrences.
10. In the **Components** area, click **Add** to open the **Select component** window.
11. Click a component to select, click again to clear. You can select one component, or multiple components. Click **Select**, and click **Save**.

Access level

Access levels determine where and when a card is valid. The default access level is **Always valid**. Cardholders with **Always valid** access, have access to all doors at any time. To restrict access, you must create a specific access level, and configure door exceptions. To define an access level, select a door and assign a schedule and if appropriate, a floor group to it. Use the function **Access Level** to add, edit, duplicate, or delete an access level.

The top section of the **Access Level** tab contains the following field and buttons:

- **Select component**
- **Add**
- **Edit**
- **Duplicate**
- **Delete**

Selecting a component

Select a site from the **Select a component** list. The following items appear:

- **Access levels view**
- **Doors view**
- **Search field**

Access levels view

The access levels view displays a list of existing access levels. Select an access level, and in the right pane, view all doors assigned to that access level, and their corresponding schedule and floors group.

Adding an access level

1. From the **Select a component** list, select a site.
2. Click the **Access levels view**, and click the **Add** button. A table with a list of doors for that site appears.
3. In the **Primary language** field, enter a name for the new access level.
4. Optional: In the **Secondary language** field, enter a name in a different language.
5. Select one of the doors. A **Schedule Assign** button appears, and if the site has more than one floor, the **Floor group Assign** button appears.
6. Click the **Schedule Assign** button, and select a schedule from the list on the left pane. For elevator doors, click the **Floor group assign** button.
7. View the right pane for schedule details, click **Select**, and **Save**.
8. In the site table, blue rectangles indicate an assigned schedule. Hover the mouse over the blue rectangles to view schedule times.
9. In the site table, select the door again, and click the **Floor group Assign** button.
10. Select the floor group from the list, click **Select**, and **Save**.
11. In the site table, a white square in the **Floors** column indicates an assigned floor group. Hover the mouse over the white square to view floor group.

Editing an access level or adding an additional door

1. From the **Select a component** list, select a site.
2. Click the **Access levels view**, and select an access level from the list.

3. Click the **Edit** button. A table with a list of doors for that site appears.
4. Repeat steps 5 to 11 in **Adding an access level** task.

Duplicating an access level

1. From the **Select a component** list, select a site.
2. Click the **Access levels view**, and select an access level from the list.
3. Click the **Duplicate** button. The **Duplicate access level** tab appears.
4. In the **Primary language** field, enter a name for the new access level.
5. Optional: In the **Secondary language** field, enter a name in a different language. Click **Save**.

Deleting an access level

1. From the **Select a component** list, select a site.
2. Click the **Access levels view**, and select an access level from the list.
3. Click **Delete**. A message appears asking **Do you want to delete this access level?** Click **Delete** again to confirm the deletion.

Doors view

The doors view displays a list of existing doors and elevators. Select a door or elevator and in the right pane, view all access levels assigned to that door, and their corresponding schedule and floors group.

Editing Access level schedules and floors

1. Select a site from the **Select a component** list.
2. Click the **Doors view**, and select a door from the door list. All access levels assigned to that door, and their corresponding schedule display. If appropriate, their floors group display.
3. Select a schedule from the **Schedule** list of the access level you want to change.
4. Select a floor group from the **Floors** list of the access level you want to change. Click **Save**.

Schedule

A schedule indicates when the system executes certain operations, for example:

- Automatically unlocking doors
- Permitting access to employees
- Running automatic reports
- Monitoring inputs

It also determines when the system acknowledges events, or when to activate relays controlling different functions, for example lighting and heat. A schedule can have up to 20 intervals. Each interval has a start and end time. You can select each of these intervals for seven days of the week, and for four holidays. You can program 99 schedules per site, and an unlimited number of system schedules.

EntraPass web supports two types of schedule:

- **System schedules:** for global functions that are not loaded in controllers.
- **Site schedules:** for sites, define up to 99 schedules per site. You must enable the advance schedule for site schedules in EntraPass workstation. Go to **Options**, click **System parameters configuration**, and click **Schedule**.

Table 3: Schedule categories and associated functions

System schedules for global functions	Site schedules for hardware components
Event parameters	Power supervision-controllers
Operators login	Unlock-doors
Video triggers	REX-doors
Workstation	Activation mode-relay
—	Monitoring-input

If you assign or define schedules, make sure you select the proper category for the schedule. For example, if you assign or define a system schedule, the schedule is available for components in this category. If you select a schedule for hardware components, the system groups the schedules by site. If you define two sites in the system, the system creates two separate groups of schedules for each site.

The top section of the **Schedule** tab contains the following field and buttons:

- **System**
- **Add**
- **Edit**
- **Duplicate**
- **Delete**





Selecting a component

Select a gateway or site from the **Select component** list. The system lists existing schedules assigned to that site. Select a schedule, and in the right pane, view the schedule table.

Adding a schedule

1. Click the **Schedule** tab, and click the **Add** button.
2. In the **Primary language** field, enter a name for the new schedule.
3. **Optional:** In the **Secondary language** field, enter a name in a different language.
4. Select the **Extended** check box to setup a schedule with 20 intervals. This is the default setting.
5. In the **Interval** field, enter a start time, and an end time.
6. Select the check boxes for the days of the week, and the holidays you want for the new schedule, or use the **Period** field.
7. The **Period** field is a quick selection option.

Table 4: Quick selection

	Click to select seven days of the week, and four holidays.
	Click to select seven days of the week.
	Click to select five business days of the week.
	Click to clear all selections.

8. To add a new interval, click the **Add interval** button. Repeat steps 5 to 7. Click **Save**.

Editing a schedule

1. Select a system or site from the **Select component** list, and select a schedule from the schedule list.
2. Click the **Edit** button.
3. Repeats 5 to 7 in the **Adding a schedule** task for each interval.

Duplicating a schedule

1. Select a site from the **Select component** list, and select a schedule from the schedule list.
2. Click the **Duplicate** button. The **Duplicate schedule** tab appears.
3. In the **Primary language** field, enter a name for the schedule.
4. Optional: In the **Secondary language** field, enter a name in a different language. Click **Save**.

Deleting a schedule

1. Select a site from the **Select component** list, and select a schedule from the schedule list.
2. Click **Delete**. A message appears asking **Do you want to delete this access level?** Click **Delete** again to confirm the deletion.

Holiday

Use holidays to assign extra days to a schedule. The system treats holidays differently to other days. It is best practice to program holidays at the beginning of the year. This makes it easier to adjust for floating holidays for the current year. Four holiday types are available.

Choose to define a holiday globally as a system holiday, or by sites. EntraPass treats holidays in different sites separately, for example, you can define a particular day as a holiday for one site, but as a regular day for another.

The top section of the **Holiday** tab contains the following buttons:

- **Add**
- **Edit**
- **Duplicate**
- **Delete**

To select a holiday, use the **Search** field, or the holiday list in the left pane.

- **Search** field: enter part of a word, or the entire word. The system filters automatically one second after writing in the field, and lists the results alphabetically.
- **Site** list: automatically lists all holidays defined in the system alphabetically.

Adding a holiday

1. Click the **Holiday** tab, and click the **Add** button.
2. In the **Primary language** field, enter a name for the holiday.
3. **Optional:** In the **Secondary language** field, enter a name in a different language.
4. Select the holiday from the date field.
5. If you want the holiday to repeat annually, select the **Recurring** check box.
6. If you have a hatrix system, click the **System** button. The **Switch** button appears. **Sites** is the default value.

7. In the appropriate row, click one of the following holiday types:
 - **None**. This is the default value.
 - **Hol 1**
 - **Hol 2**
 - **Hol 3**
 - **Hol 4**
8. Click **Save**.

Editing a holiday

1. Select a holiday from the left pane.
2. Click the **Edit** button. A table with a list of assigned system and sites for that holiday appears.
3. Repeat steps 4 to 8 in **Adding a holiday** task.

Duplicating a holiday

1. Select a holiday from the left pane.
2. Click the **Duplicate** button.
3. On the **Duplicate holiday** tab, in the **Primary language** field, enter a name for the holiday.
4. **Optional:** In the **Secondary language** field, enter a name in a different language. Click **Save**.
5. Repeat Steps 4 to 8 in **Adding a holiday** task.

Operator

An operator is someone who uses EntraPass web. Different operator types include the following:

- Web- Installer
- Web- Administrator
- Web- Operator

An installer has the highest level of security, with administrator next, and then operator.

Use the function **Operator** to view, add, and edit an operator's details.

The top section of the **Operator** tab contains the following buttons and fields:

- **Card view:** displays the operator's **Photo**, **Operator name**, **Login name**, and **E-mail** in a card format.
- **Table view:** displays the operator's **Photo**, **Operator name**, **Login name**, and **E-mail** in a table format.
- **Add:** opens the **Add operator** tab, where you can add a new operator and define associated options.
- **Search:** enter part of a word, or the entire word. The system filters automatically one second after writing in the field, and lists the results alphabetically.
- **Search in:** use to refine your search, select one of the following: **Operator name**, **Login name**, or **Email**.
- **Reset:** clears all search and filter results.

When you select an operator, the following buttons appear:

- **Edit**
- **Delete**

Adding an operator

1. Click the **Operator** tab, and click the **Add** button.
2. If you want to define the operator and activate immediately, click **Enable**. **Enable** is the default state.
3. If you want to define the operator and not activate immediately, click **Disable**.
4. In the **Name** field, enter the full name of the cardholder.
5. In the **Login name** field, enter a unique name with a minimum of six characters.
6. In the **Password** field, enter a minimum of seven characters.
7. In the **Confirm password** field, re-enter the password.
8. In the **Email** field, enter an e-mail address. E-mail is mandatory only if you select the **EntraPass web**, or **EntraPass go** check boxes.
9. The **Database Language** automatically defaults to the primary language.
10. Select a **User Interface Language**. The system uses this language for the user interface, reporting, and email notifications. By default, the User Interface Language is the same as the Database Language.
11. Select one of the following security levels from the **Security level** list:
 - **Administrator**
 - **Guard**
 - **Installer**
12. Select a workspace from the **Workspace** list.
13. To e-mail the operator a link to install EntraPass web, select the **EntraPass web** check box.
14. To e-mail links to the operator to install EntraPass go, select the **EntraPass go** check box.

Password options

1. To request a password change from the operator at the next login, select the **Change password at next login** check box.
2. To disable the system if the operator enters an incorrect password, select the **Disable on bad password** check box. Enter how attempts the system allows before disabling.
3. If you want to time limit the operator's password, select the **Days before password reset** check box. Enter how many days in the field, maximum is 120 days.

Validation date

If you want to end the operator's access to the system, select the **Operator** expiration date check box. Enter the end date.

Tenant list

A tenant is a resident in an apartment building, or an employee in a company. A tenant list represents the tenants inside a building. Depending on the amount of doors in a building, you can have one tenant list, or many tenant lists for a building. EntraPass pushes tenant lists to the Kantech Telephone Entry System (KTES), where a tenant can grant access to a visitor.

The top section of the **Tenant list** tab contains the following icons:

- **Add list**
- **Edit list**
- **Duplicate list**

- **Delete list**
- **Add tenant**
- **Edit tenant**

To select a tenant list, use the **Search** field or the tenant list in the left pane.

- **Search** field: enter part of a word, or the entire word. The system filters automatically one second after writing in the field, and lists the results alphabetically.
- **Tenant** list: automatically lists all tenant lists defined in the system alphabetically.

Adding a tenant list

1. Click the **Tenant List**, and click the **Add list** button.
2. In the **Name** field, enter the full name of the cardholder.
3. In the **Primary language** field, enter a name for the new tenant list.
4. Optional: In the **Secondary language** field, enter a name in a different language.
5. In the **ID length** field, select a number from one to five. This is the tenant's identification code and a visitor uses it to call the tenant.
6. In the **PIN length** field, select a number from four to six. This is the tenants Personal Identification Number (PIN).
7. Select a Wiegand display format from the **Wiegand display format on LCD** list. Click **Save** to return to the **Tenants List configuration** tab. The system automatically assigns a **Master tenant** to a new tenant list.

Editing a tenant list

1. Select a tenant list from the left pane.
2. Click the **Access levels view**, and select an access level from the list.
3. Click the **Edit list** button.
4. Repeat steps 5 to 7 in **Adding a tenant list** task.

Duplicating a tenant list

1. Select a tenant list from the left pane.
2. Click the **Duplicate list** button.
3. In the **Primary language** field, enter a name for the new tenant list.
4. Optional: In the **Secondary language** field, enter a name in a different language. Click **Save**.

Deleting a tenant list

1. Select a tenant list from the left pane.
2. Click **Delete list**. A message appears asking **Do you want to delete this tenant list?** Click **Delete** again to confirm the deletion.

Adding a tenant

1. Select a tenant list from the left pane, and click **Add tenant**.
2. If you want to define the tenant and activate immediately, click **Enable**
3. If you want to define the tenant and not activate immediately, click **Disable**.
4. In the **Name** field, enter the full name of the tenant.

5. In the **ID** field, enter the tenant's ID. This is the tenant's identification code and a visitor uses it to call the tenant.
6. In the **PIN** field, enter the tenant's PIN. This is the tenants Personal Identification Number (PIN).
7. In the **Card number output** area, select one of the following options:
 - In the **Card number** field, enter the card number.
 - Click **Link with a cardholder**, select a cardholder from the table, and click **Link**. The cardholder's name appears in the **Card number output** area.
8. In the **Phone number** field, enter the tenant's phone number. Select a schedule for the phone number.
9. In the **Second phone number** field, enter a second number for the tenant. Select a schedule for the phone number.
 - ① **Note:** When a visitor wants to call a tenant, they use the KTES directory. If there is no answer from the first phone number, the KTES uses the second phone number. The absence of a first phone number means the KTES cannot call the tenant.

Result

You can save the tenant at this stage without completing the additional options. The system automatically saves the option defaults for the tenant.

Options

1. From the **Start date** field, select a start date . Today's date is the default.
2. From the **End date** field, select an end date . The **End date** is when the tenant is no longer valid and cannot access the system.
3. From the **Administration level** list, select one of the following:
 - **Tenant**
 - **Maintenance**
 - **Owner**
 - **Installer**
4. From the **Do not disturb schedule** list, select a schedule. Use this to put the tenant in a "Do not disturb" status.
 - To remove the tenants name from the directory list, when in a **Do not disturb schedule**, select the **Hide from list (do not disturb schedule)** check box.
5. In the **Card number output** area, select one of the following options:
 - In the **Card number** field, enter the card number.
 - Click **Link with a cardholder**, select a cardholder from the table, and click **Link**. The cardholder's name appears in the **Card number output** area.
6. If you want to display the current tenant's name, select the **Show tenant** check box.
7. If you want to prioritize the tenant in the KTES, select the **Prioritize in display list** check box. The KTES displays non-prioritized tenants in alphabetical order.
8. If you want to activate a relay, or generate a traceability event, select the **Trace** check box.
9. If you want to extend the number of telephone rings, select the **Extended ring** check box.
10. If you want to extend the unlock time for a door, select **Extended door access** delay.

Hardware setup

Use **Hardware Setup** to add and edit sites, connections, and controllers. You can view and edit doors, relays, and inputs.

The column layout directs the logical configuration of components. First, add a site, then a connection, then a controller, with their associated doors, relays, and inputs.

You can add multiple sites, and the content in the succeeding column depends on, which site or gateway you select. The content in the **Controllers** column depends on, which connection you select, and the content in the **Doors – Relays – Inputs** column depends on, which controller you select.

Sites and gateways

A site is composed of one or many physical connections.

A gateway controls communications between the door controllers and the server. In the case of a network communication interruption with the server, the gateway assumes complete management of a site. EntraPass Corporate Edition uses a multi-site gateway, and EntraPass Global edition and hatrix use a global gateway.

Adding a connection

1. Click the **Add** button to create a new site.
2. In the **Primary language** field, enter the site name.
3. Optional: In the **Secondary language** field, enter the site name in a different language.
4. Complete the **Site information** fields appropriate to the site. Click **Save**.

Note: Use EntraPass workstation to create and edit a gateway.

Editing a site

Select the site, and click the **Edit** button.

Connections

See the following table for information about the five available connection types and compatible gateways.

Table 5: Connection types and compatible gateways

Connection type	Multi-site gateway	Global gateway	KT-NCC
IP address, KT-1	Yes	Yes	Yes
IP address, KT-400	Yes	Yes	Yes
IP address, IP Link	Yes	No	No
IP address, KTES	Yes	No	No
Direct, RS-232 or USB	Yes	Yes	Yes

Adding a connection

About this task:

If you selected a gateway, you cannot add a connection. Select a site to add a connection.

1. In the **Connections** panel, click the **Add** button.
2. In the **Primary language** field, enter a name for the connection.
3. Optional: In the **Secondary language** field, enter a name in a different language.
4. In the **Connection information** area, select the gateway type from the **Gateway** list.
5. If you have a hatrix system, enter the zip or postal code in the **Billing ZIP or postal code** field.
6. Select a time zone from the **Time zone** list.
7. In the **Connection type** area, select the controller connection tab you want to connect. For each connection type, complete the following sections:
 - a. **Communication**
 - b. **Gateway**
 - c. **Association**
 - d. **Additional information**
 - e. **Comments**

Result

For a direct connection, complete the following sections:

- **Communication**
- **Association**
- **Additional information**
- **Comments**

Communication

About this task:

In the **Communication** section, to define a connection, complete the following steps:

1. In the **MAC address** field, enter the MAC address of the controller.
2. Select a baud rate from the **Controller's loop baud rate** list, the default is 19200.
3. Choose **UDP** or **TCP** from the **Protocol** field.
4. In the **Port** field, enter the controller's **port** number.
5. In the **IP configuration** field, choose **Static** or **DHCP**. Select **DHCP** to obtain the IP address automatically. If you select **Static**, contact your system administrator for details to complete the following fields:
 - a. **IP address**
 - b. **Subnet mask**
 - c. **Gateway (router)**
 - d. **DNS server**

In the **Communication** section, complete the following steps for a direct connection:

1. In the **Communication port** field, enter the controller's port number.
2. Select a baud rate from the **Controller's loop baud rate** list, the default is 19200.

Gateway

In the Gateway section, the default IP address is 172.16.254.1, if you want to change this, select the **Override gateway IP address** check box. Choose from the following options:

- Select **IP address**, and enter the new address in the **IP address** field.
- Select **Domain name**, and enter the domain name, click **Test DNS** to test the connection.

Association

1. In the **Association** area, select a graphic map from the **Map** list.
2. Select a camera from the **Camera/Video view** list.

Additional information

In the **Additional information** pane, enter information that may be useful for identifying the connection type.

Comments

In the **Comments** pane, enter information that may be useful for identifying the connection type.

Controllers

Controllers provide audio-visual feedback on an access decision. A red LED indicator on the reader indicates a locked door, or that the system has denied access. A green LED indicator on the controller indicates an unlocked door. You can install a local door alarm that provides an audible warning if the door is forced open, or remains open after access.

The controller definition informs EntraPass of the controller's usage, and what devices are associated with it, for example, doors, inputs, relays, and output devices.

Adding a controller

Three buttons in the top function section indicate which stage of the controller setup you are currently defining. The following list outlines the stages:

- [1 - Controller](#)
- [2 - Door options](#)
- [3 - Review](#)

1 - Controller

1. In the **Primary language** field, enter a name for the controller.
2. Optional: In the **Secondary language** field, enter a name in a different language.
3. In the **Controller type** area, select the tab for the controller type you want to connect.
4. In the **Serial number** field, enter the serial number of the controller. Find the serial number on the controller label.
5. For a KT-2 controller, the **Use ioSmart in RS-485** check box appears. Select the check box if you want to use the ioSmart reader in RS-485 mode.
6. For a KT-400/KT-4 controller, select the **Controller Sub Type** from the drop-down list. KT-400 is selected by default.

7. For a KT-1 or KT-400/KT-4 controller, from the **COM2 Protocol** drop-down, select one of the following protocol options:
 - None
 - Kantech ioSmart
 - OSDP
8. Select a reader from the **Reader type** list.
9. Click **Next**.

2 - Door options

1. In the **Option** area, if you want a door contact, select the **Door contact** check box.
2. If the door has a request to exit detector, select the **REX contact** check box. This input must be local; it must be one of the inputs on the controller operating the door.
3. If you want to enable an exit reader and you selected a KT-2 or KT-400/KT-4 controller with Kantech ioSmart protocol, select the **Enable exit reader** check box.
4. Choose the appropriate method for the selected controller:
 - If you selected a KT-1, KT-2, or KT-400/KT-4 controller with Kantech ioSmart protocol, and you selected to use an ioSmart reader in RS-485 mode, enter an entry serial number in the **Entry** field, and an exit serial number in the **Exit** field.
 - If you selected a KT-1 controller with OSDP protocol, select the **Entry** and **Exit** addresses from 0-126 and enter the **Entry** reader and **Exit** reader serial numbers.
 - If you selected a KT-400/KT-4 controller with OSDP protocol, select the **Address** from 0-126 and enter the **Reader serial number**.
5. Click **Next**.

3 - Review

Review your options in the graphic and summary pane. Click **Finish**.

Editing a controller

About this task:

If you want to disable a controller, click the **Disable** button. **Enable** is the default setting. If you want to edit any other setting, complete the following steps:

1. In the **Controller name** area, enter a name in the **Primary language** field.
2. Optional: In the **Secondary language** field, enter a name in a different language.
3. In the **Controller information** area, you can edit the following information:
 - For a KT-400/KT-4 controller only, select the controller sub-type from the **Controller Sub Type** drop-down.
 - Enter the serial number of the controller in the **Serial number** field. You can find the serial number on the controller label.
4. To update firmware, in the **Firmware** area, use the following options:
 - **Update controller firmware:** This button appears when the firmware of the **Controller's current version** is lower than the **Available version**.
 - **Update module firmware:** This button appears when the firmware of the **ioSmart current version** or **ioSmart (Gen2) current version** is lower than the **Available version**.
5. Click **Save**.

Configuration

About this task:

In the **Configuration** section, complete the following steps to edit a controller type.

1. In the **Reader types** area, select a reader from the **Reader type 1** list.
2. If appropriate, select a different reader from the **Reader type 2** list, and the **Reader type 3** list.
3. If you have more than three reader types, click **Add**, and select from the **Reader type 4** list.
4. If exit readers exist on site, and you want to use them, select the **Enable exit readers** check box.
5. In the **End-of-line resistor** area, select one of the following options:
 - **None**: A dry contact, no end-of-line resistor.
 - **Single**: 5.6K, single end-of-line resistor.
 - **Double**: Two 5.6K, double end-of-line resistors.
6. For a KT-1 or KT-400/KT-4 controller, in the **COM2 Protocol** area, select one of the following options:
 - Kantech ioSmart
 - OSDP
7. In the **Keypad** area, select a keypad from the **Keypad type** list.
8. Optional: In the **Escape Key** list, select a number or character.
9. In the **Modules** area, select a baud rate from the **Baud rate** list. For the Kantech ioSmart protocol, the default is 115200. For OSDP protocol, the default is 9600.
10. If you use an ioSmart card reader in RS-485 mode, select a reader template from the **Reader template** list.
11. Click **Save**.

Wi-Fi

About this task:

The **Wi-Fi** section is only available for a KT-4 controller. To connect the KT-4 controller with Wi-Fi, complete the following steps:

1. In the **Wi-Fi Configuration** pane, enter the **SSID** and **Password**.
2. Click **Save**.

Readers

Use the following information to define readers to the door controller you are editing.

Defining readers with Kantech ioSmart protocol

About this task:

For a KT-1, KT-2, or KT-400/KT-4 controller with Kantech ioSmart protocol, in the **Reader** section, complete the following steps to define an ioSmart reader:

1. In the **Serial number** field, enter the reader's serial number.
2. Select a door from the **Door** drop-down list.
3. If your ioSmart reader includes a keypad, select the **Keypad** check box.
4. In the **Terminals** area, to configure the reader's inputs, select from the **I1** list:
 - **Disabled**
 - **Single input**

- **Dual input**
5. To configure the reader's outputs, select from the **I2O** list:
 - **Disabled**
 - **Single input**
 - **Dual input**
 - **Lock output**
 - **Relay**
 6. To add an ioSmart reader to the controller, click **Add** and repeat Steps 1 to 5.

Defining readers with OSDP

About this task:

To define a reader with OSDP for a KT-1 or KT-400/KT-4 controller, in the **Reader** section, complete the following steps:

1. From the **Address** drop-down list, select the reader address.
2. In the **Serial number** field, enter the reader's serial number.
3. Select a door from the **Door** drop-down list.
4. To add an OSDP reader to the controller, click **Add** and repeat steps 1 to 3.

Wireless lock

About this task:

In the **Wireless lock** section, complete the following steps to define a wireless lock.

1. The **Device** column represents the number of the lock.
2. The **Primary description** and the **Secondary description** represent the name of the door.
3. If you want to define a contact to the lock, select the **Contact** check box for the door.
4. If you want to define a REX to the lock, select the **REX** check box for the door.
5. Enter the lock's ID in the **ID** field.
6. To delete a lock, click the **Delete** icon, and click **Delete** again to confirm the message **Do you want to delete this wireless lock?**
7. To add a wireless lock, click **Add**. Repeat Steps 3 to 5.

Association

1. In the **Association** area, select a graphic map from the **Map** list.
2. Select a camera from the **Camera/Video** view list.

Comments

In the **Comments** pane, enter information that may be useful for identifying the door.

Doors - Relays - Inputs

To view all doors, relays and inputs associated with the controller, select the **Doors**, **Relays**, and **Inputs** check boxes, individually or collectively.

Doors

Define a door for any of the following purposes:

- An elevator door
- In/Out door
- Entry door for anti-passback.
- Exit door for anti-passback.
- Access door

You have the option to secure the door at all times, or only during defined schedules. The common locking devices used are electric door strikes, and electromagnetic locks. You can configure a door with a reader on one side or both sides. For doors equipped with two readers, you must define the outer reader as an entry reader and the inner reader as an exit reader.

Editing a door

1. To edit a door, select the door, and click **Edit**.
2. In the **Primary language** field, enter a name for the door.
3. Optional: In the **Secondary language** field, enter a name in a different language.
4. In the **Lock information** area, select an unlock schedule from the **Unlock schedule** list.
5. If you select the **First person** in check box, the door remains locked until the first card is granted access, while an unlock schedule is valid.
6. Set the **Grace period** counter for the time you want to permit a valid access before the scheduled unlock time.
7. Enter the time you want the door to unlock in the **Unlock time** field.
8. If you want to extend the unlock time, enter the time in the **Extended unlock time** field.
9. Select the relay that you want to follow the lock output, from the **Relay to follow lock output** list.
10. Choose the **Fail-safe** option, or the **Fail-secure** option in the **Door lock** field. Choose the appropriate option for your door type to lock the door when the power fails.

Table 6: Door lock types

Door lock	Lock type
Fail-safe	Strike lock
Fail-secure	Electromagnetic lock

Result

For each door, complete the following sections:

- [Contact](#)
- [Request To Exit \(REX\)](#)
- [Keypad](#)
- [Multi-swipe](#)
- [Intrusions](#)
- [Association](#)
- [Comments](#)

For an elevator, complete the following sections:

- **Elevator**

- [Keypad](#)
- [Association](#)
- [Comments](#)

Contact

About this task:

A door contact monitors several door conditions, for example, door forced open, door open too long, and interlock options like mantrap. An interlock option ensures that the cardholder closes and locks one door, before the system grants the cardholder access to the second door. The door contact protects the investment made to control access to the door. The door lock, card reader, or keypad provide security and prevent unauthorized entry to a closed and, locked door. To define a door contact, complete the following steps:

1. Select a contact from the **Door contact** list.
2. Select a schedule from the **Shunt schedule** list. A shunt schedule outlines the time zone that you want the system to ignore the door.
3. Select the **Door open reading** check box, if you want the system to read cards while the door is open. When you select the check box, EntraPass generates the "Access granted" event. If you clear the check box, EntraPass generates the event "Access granted - Door open".
4. Select the **Door unlock reading** check box, if you want the system to read cards while the door is unlocked manually by the operator or, by a valid unlock schedule. When you select the check box, the system generates the "Access granted - Door unlocked" event on access. If you clear the check box, EntraPass does not generate any event.
5. Select the **Unlock on access door open** check box, if you want the system to unlock the door when a cardholder opens the door.
6. In the **Open time** field, enter how long you want the door to remain open following a permitted access, or a valid request to exit request.
7. In the **Extended open time** field, enter the extended time you want the door to remain open.
8. Select the **Pre-alarm door opened too long** check box, if you want the door piezo to sound when half the defined open time passes. The piezo sounds until the door is closed.
9. Enter the delay time before triggering the **Pre-alarm door opened too long** in the **Delay** field.

Request To Exit (REX)

About this task:

A signal from the REX device indicates that someone wants to exit through a controlled door. Motion detectors and push buttons provide the REX signal. You can configure doors with an unlock time reset, each time the primary or secondary REX is triggered. You can define two types of REX contacts, a primary and a secondary. The KT-400 and KT-1 controllers support the secondary REX feature. To define the REX options, complete the following steps:

1. In the **Primary REX options** area, select a door contact from the **REX contact** list. This is the input the REX detector is connected to. This input must be local; it has to be one of the inputs on the controller operating the door.
2. Select a schedule from the **REX contact supervision schedule** list. When the schedule is valid, the controller detects the REX signals originating from the exit contact. This option applies only to a door defined with a REX contact.
3. Select a schedule from the **REX bypass message schedule** list. When the schedule is valid, events are not stored in archives. When the schedule is invalid, the system sends events to the gateway for archives.

4. If you select the **Unlock on REX** check box, the door is unlocked if the controller validates the REX. Use this option on interior exit doors, shipping doors, and push doors used by delivery personnel. The system permits the exit and generates a “request to exit granted” event, rather than a “door forced open” event.
5. If you select the **Resettable REX function** check box, the unlock time is restarted on a valid request to exit. Define open and unlock times in Doors in the Hardware Setup function. Select this option for high traffic doors, for example, manufacturing doors where many users need to exit during a short time, to prevent unwanted "door open too long" or "door forced open" events.
 - ① **Note:** This function is available only if you select **On door closing** in the **Relock on REX option**.
6. Choose **On door opening** or **On door closing** in the **Relock on REX** field.

Keypad

If you select a keypad type, when defining the controller associated with the door, the keypad tab appears. To configure which option permits access to a door, choose from the following options:

- Select **Reader only** if you want to grant access using only a reader. A reader only installation is the most common application.
- Select **Reader or keypad** if you want to grant access using a reader or a keypad. A keypad access is less secure than a reader access as the user may share their PIN and cannot permit further use, compared to lending a card and getting it back.
- Select **Reader and keypad** if you want to grant access using a reader and a keypad. You must define a valid “keypad schedule”. Adding a keypad to a reader increases the level of security.
- If you select a keypad option, the **Card and pin schedule** list appears. To limit the requirement for a PIN code, select a schedule.

Multi-swipe

About this task:

Use multi-swipe to define the actions that result when a cardholder double swipes their card, or triple swipes their card. To define multi-swipe, click the **Enable** button and complete the following steps:

1. Select a schedule from the **Schedule** list. The schedule applies to **Double swipe parameters** and **Triple swipe parameters**, and must be valid when the cardholder swipes the card a second time or third time for the corresponding action to occur.
2. In the **Double swipe parameters** area, select one of the following action options to occur when the cardholder double swipes their card.
 - a. **No action**
 - b. **Arming alarm system or partition:** arms the door manually, or arms panel partitions. For a global gateway or a KT-NCC gateway, you must configure the door as an arming reader in one or more alarm systems. The system first verifies the swipe conditions, and then the arming conditions of the alarm system.
 - c. **Toggle door lock:** switches the lock from the current state to the alternative state. For example, if the door is in a locked state, it unlocks it. If the door is in an unlocked state, it locks it.
 - d. **Tempo unlock door:** temporarily unlocks the door for a specified time.
 - e. **Toggle relay:** switches the relay from the current state to the alternative state. For example, if the relay state is activate, it switches to deactivate; if the relay state is deactivate, it switches to activate.

- f. **Tempo activate relay:** temporarily activates a relay, or group of relays, for a specified time.
 - g. **Lock door:** relocks the door after valid access.
 - h. **Unlock door:** unlocks the door after valid access.
 - i. **Activate relay:** activates the relay, only if the relay state is deactivate.
 - j. **Deactivate relay:** deactivates the relay, only if the relay state is active.
3. If you select **Toggle relay, Activate relay, or Deactivate relay**, the **Relay** list appears. Select the appropriate relay from the list.
 4. In the **Delay** field, enter the maximum time between two card swipes. Two beeps sound to indicate a double swipe, three beeps sound to indicate a triple swipe. A long beep indicates denied entry.
 5. Select the **Relock on access on double swipe** check box to lock the door before executing the double swipe action.
 6. Complete Steps 2 to 4 to define **Triple swipe parameters**.

Intrusions

About this task:

Use **Intrusion** to define the parameters for your intrusion device.

1. Select a key from the **Arming request keypad** key list.
2. Select an input from the **Arming request input** list.
3. Select a schedule from the **Arming request schedule** list.
4. Select an access level from the **Arming access level** list.
5. Select an access level from the **Disarming access** level.

Association

1. In the **Association** area, select a graphic map from the **Map** list.
2. Select a camera from the **Camera/Video** view list.

Comments

In the **Comments** pane, enter information that may be useful for identifying the door.

Relays

Relays control or trigger systems electromechanically or electronically. Edit relays to change the state of a relay or group of relays manually. The window displays in real-time, by displaying active relays in black and inactive relays in grey.

Editing relays

1. In the **Doors – Relays – Input** column, select the **Relays** check box.
2. Select the relay, and click **Edit**.
3. In the **Relay name** area, enter a name for the door in the **Primary language** field.
4. Optional: In the **Secondary language** field, enter a name in a different language.
5. In the **Operating mode** area, choose one of the following modes in the **Mode** field.
 - **Normal:** deactivated by default
 - **Reverse:** activated by default

Result

For each relay, complete the following sections:

- **Activation**
- **Association**
- **Comments**

Activation

1. Enter a time in the **Temporary activation timer** field, to activate a relay or group of relays for a temporary duration. Activate this setting in the input **Operating mode**.
2. In the **Automated activation mode** area, select a schedule from the **Schedule** list.
3. In the **Disable action relay** list, select a schedule where you want the exception to occur.

Association

1. In the **Association** area, select a graphic map from the **Map** list.
2. Select a camera from the **Camera/Video** view list.

Comments

In the **Comments** pane, enter information that may be useful for identifying the relay.

Inputs

Door controllers monitor the state of input points, for example: door contacts, interlocks, alarm points, motion detectors, temperature sensors, door REXs, and other devices with dry contacts.

Table 7: Recommended input usage

KT-1		KT-300			KT-400		
Contact	REX	Contact	REX	Door	Contact	REX	Door
I1	I2	I1	I2	1	I1	I2	1
		I3	I4	2	I5	I6	2
					I9	I10	3
					I13	I14	4

Editing inputs

1. In the **Doors – Relays – Input** column, select the **Inputs** check box.
2. Select the input, and click **Edit**.
3. In the **Primary language** field, enter a name for the door.
4. Optional: In the **Secondary language** field, enter a name in a different language.
5. In the **Operating mode** area, choose **Closed** or **Opened** in the **Normal condition** field to set the normal state of the input.
6. In the **Event message** field, choose **Alarm** or **Activation**. When you configure event parameters with an input in alarm, or input activated, the system only displays the inputs corresponding to the criteria.
7. Select a schedule from the **Monitoring schedule** list. This schedule specifies when the system supervises the condition of the input. When the schedule is valid, a change in an input condition generates an “input in alarm” or “input restore” event.

8. Select the relay you want to activate from the **Activate relay** list.
9. Select the **Activate relay temporarily** check box if you want to activate the relay according to the temporary activation parameters defined in the **Edit relay** window.

Result

For each relay, complete the following sections:

- **Timing**
- **Shunt**
- **Association**
- **Comments**

Timing

1. In the **Loop response time** area, enter a time in the **Alarm response time** field. This time is the delay before the system generates the input and alarm event.
2. Enter a time in the **Restore response time** field. This time is the delay before the system generates the input restore events.

Shunt

1. In the **Shunt** area, select an input from the **Shunt input** list. This defines the enabled input that the system will not monitor.
2. Select the **Shunt input temporarily** check box, when you want the system to ignore the input.
3. Select the **Reset delay for shunt temporarily** check box, when you want to reset the delay on a temporary shunt. The **Temporary shunt timer** field must be set to invoke the delay.
4. Enter a time in the **Temporary shunt timer** field, to specify the time when the system does not monitor the input. Setting the timer to 0:00:00 instructs the relay to follow the input state. The maximum value for the shunt timer is 18:12:15 for the KT-400 or the KTES.

Association

1. In the **Association** area, select a graphic map from the **Map** list.
2. Select a camera from the **Camera/Video** view list.

Comments

In the **Comments** pane, enter information that may be useful for identifying the input.

Site info

Use **Site Info** to view site parameters entered in the **Hardware Setup** function.

To select a site, use the **Search** field or the site list on the left panel.

- **Search** field: enter part of a word, or the entire word. The system filters automatically one second after writing in the field, and lists the results alphabetically.
- **Site** list: automatically lists all sites defined in the system alphabetically.

In the **Site name** area, the site name defined in **Hardware Setup** appears in the **Primary language** field. If you defined a **Secondary language**, it appears.

View the **Site information** area, for more information about the site.

Technical support

See the following technical support contact details and opening hours in your region, or go to:

https://kantech.com/Support/Contact_Technical_Support_Advanced.aspx.

United States and Canada

Table 8: United States and Canada telephone numbers

Region	Call type	Business hours: 08:00 to 20:00 (EST)
United States and Canada	Toll free	+1 888 222 1560
United States and Canada	Toll free	+1 800 507 6268 option 4

Latin America and Caribbean

For technical support, contact us at one of the following email addresses or use the phone number for your region.

- For access technical support, email access-support@jci.com.
- For video technical support, email video-support@jci.com.
- For technical training inquiries, email latam.certificaciones@jci.com.

Table 9: Latin America and Caribbean telephone numbers

Region	Call type	Business hours: 08:00 to 20:00 (EST)
Latin America and Caribbean	Toll free	+1 800 507 6268
Latin America and Caribbean	Toll free	+1 800 392 2873
Argentina, Buenos Aires	Direct	+54 11 5199 3104
Brazil, Sao Paolo	Direct	+55 11 3181 7377
Chile, Santiago	Direct	+56 2 3210 9662
Colombia, Cali	Direct	+57 2 891 2476
Colombia, Medellin	Direct	+57 4 204 0519
Costa Rica, National VOIP	Direct	+506 4 000 1655
Dominican Republic, Santo Domingo	Direct	+1 829 235 3047
El Salvador, San Salvador	Direct	+503 2 136 8703
Guatemala, Guatemala City	Direct	+502 2 268 1206
Mexico, Mexico City	Direct	+52 55 8526 1801
Panama, Panama City	Direct	+507 836 6265
Peru, Lima	Direct	+51 1 642 9707
Venezuela, Caracas	Direct	+58 212 720 2340

Europe, Middle East, and Africa

For technical support, contact us at one of the following email addresses or use the phone number for your region.

- For technical post-sales inquiries, email video-support@jci.com.
- For technical training inquiries, email emea.training@jci.com.
- For all licensing inquiries, email sp-licensing-support@jci.com.

Table 10: Europe, Middle East, and Africa telephone numbers

Region	Call type	Business hours: 08:00 to 18:00 (CET)
Europe, Middle East, and Africa	Toll free	+800 2255 8926
Europe, Middle East, and Africa	Direct	+31 475 352 722
Bahrain	Direct	(0)800 04127
Belgium	Direct	+0800 76 452
Denmark	Direct	+45 4494 9001
France	Direct	+0800 90 79 72
Germany	Direct	+0800 1806 757
Greece	Direct	00800 312 294 53
Ireland	Direct	+1800 94 3570
Israel	Direct	+972 772 201 350
Italy	Direct	+39 0230 510 112
KSA	Direct	+96 6800 8500 509
Kuwait	Direct	(0)22062915
Lebanon	Direct	01 426 801, new dial tone and then dial 8552 3436 77
Nordic Countries	Direct	04494 9001
Oman	Direct	(00) 8007 4364
Qatar	Direct	(00) 800100841
Russia	Direct	81 0800 2052 1031
South Africa	Direct	+27 (0) 10 100 3292
Spain	Direct	+900 99 31 61
Turkey	Direct	+00800 3192 3007
United Arab Emirates	Direct	(0)800 0310 7123
United Kingdom	Direct	+44 330 777 1300

Asia Pacific

For technical support, contact us at one of the following email addresses or use the phone number for your region.

- For video technical support, email video-support@jci.com.
- For technical training inquiries, email apac.training@jci.com.
- For all licensing inquiries, email sp-licensing-support@jci.com.

Table 11: Asia Pacific telephone numbers

Region	Call type	Business hours: 09:00 to 18:00 (CST China Standard Time) and 09:00 to 19:00 (IST India Standard Time)
Asia Pacific	Toll free	+ 800 2255 8926
Australia	Direct	+1 800 580 946
China	Direct	+86 21 6163 8644
India	Direct	+91 80 4199 0994
Oceania and New Zealand	Direct	+64 9942 4004

Privacy Notice

The personal data processed by this application by Johnson Controls as controller will be processed in accordance with the Johnson Controls Privacy Notice at <https://www.johnsoncontrols.com/legal/privacy>. By installing this software, you acknowledge that you have read and understood the Johnson Controls Privacy Notice. If your consent is required under applicable law for the processing and/or transfer (including international transfer) of such personal data, and strictly to the extent that consent is required under applicable law, your above actions are your consent.

Copyright

© 2024 Johnson Controls. All rights reserved. JOHNSON CONTROLS and KANTECH are trademarks of Johnson Controls.

OSS disclosure

To view a list of all open source software components used in this product and their corresponding licenses, see the *EntraPass Web OSS Disclosure Statement* on [johnsoncontrols.com](https://www.johnsoncontrols.com).

End-User License Agreement

Software Terms

Use of this software that is in (or constitutes) this product, or access to the cloud, or hosted services applicable to this product, if any, is subject to applicable end-user license, open-source software information, and other terms set forth at <http://johnsoncontrols.com/techterms>. Your use of this product constitutes an agreement to such terms.

