

## EntraPass Integration for victor v6.0

### User Guide

## **Notice**

The information in this manual was current when published. The manufacturer reserves the right to revise and improve its products. All specifications are therefore subject to change without notice.

## **Copyright**

Under copyright laws, the contents of this manual may not be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form, in whole or in part, without prior written consent of Johnson Controls.

© 2022 Johnson Controls. All right reserved. JOHNSON CONTROLS, TYCO, and AMERICAN DYNAMICS are trademarks of Johnson Controls.

## **Customer Service**

Thank you for using American Dynamics products. We support our products through an extensive worldwide network of dealers. The dealer through whom you originally purchased this product is your point of contact if you need service or support. Our dealers are empowered to provide the very best in customer service and support. Dealers should contact American Dynamics at (800) 507-6268 or (561) 912-6259 or on the Web at [www.americandynamics.net](http://www.americandynamics.net).

## **Trademarks**

Windows® is a registered trademark of Microsoft Corporation. PS/2® is a registered trademark of International Business Machines Corporation.

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Johnson Controls will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Johnson Controls. are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

# Contents

---

<b>Overview</b>	<b>5</b>
EntraPass integration introduction	5
Assumptions	5
EntraPass requirements	5
victor Application Server	5
victor Unified Client	5
Licensing	5
<b>Installation</b>	<b>7</b>
Installing the EntraPass integration driver	7
<b>Initial configuration</b>	<b>9</b>
Initial Configuration	9
<b>EntraPass integration configuration</b>	<b>10</b>
Adding an EntraPass Server	10
Testing EntraPass connectivity	11
<b>EntraPass commands</b>	<b>12</b>
Show recent transactions	13
Generate site view	14
<b>Maps</b>	<b>17</b>
Configuring Maps	17
<b>Event configuration</b>	<b>18</b>
Configuring EntraPass alert settings	18
Enabling and disabling alerts for EntraPass devices	18
Enable or disable by object editor	19
Enable/Disable by right-click action:	19
Using the Events/Schedule Setup Editor	19
Creating an EntraPass action	20
Event/Action Pairing Editor	21
Using the Event/Action Pairing editor	21
Events setup	21
Event status mapping	22
<b>EntraPass Settings</b>	<b>23</b>

---

EntraPass General Settings .....	23
EntraPass Sync Settings .....	25
EntraPass Alerts Settings .....	25
<b>Swipe and Show .....</b>	<b>26</b>
<b>EntraPass Device States .....</b>	<b>27</b>
EntraPass Server States .....	27
Gateway States .....	27
Connection States .....	27
Controller States .....	28
Door States .....	29
Input States .....	31
Relay States .....	32
<b>EntraPass Alerts .....</b>	<b>33</b>
<b>Troubleshooting .....</b>	<b>38</b>
<b>Appendix A .....</b>	<b>39</b>
KT 400 Controller configuration with DSC PowerSeries .....	39
EntraPass Setup .....	39
<b>Appendix B .....</b>	<b>41</b>
Configuring EntraPass for remote victor Client operation .....	41
Configuring Ports with an SSL Certificate .....	42

## EntraPass integration introduction

The victor EntraPass Integration driver provides a powerful, flexible and easy to use Graphical User Interface (GUI) for managing your EntraPass infrastructure through victor unified client from American Dynamics.

## Assumptions

This documentation covers the installation of victor EntraPass Integration and an overview of the EntraPass integration features and benefits. It is assumed that the end users and installers of the EntraPass Integration have relevant experience and a good working knowledge of victor unified platform, Windows operating system and experience configuring Physical Security Environments. Partners, Customers and Resellers configuring Tyco products should have completed relevant Tyco product training.

## EntraPass requirements

This integration supports connection to EntraPass systems through the EntraPass REST API, by utilizing the EntraPass Smartlink service. The connection is to the EntraPass Smartlink service therefore server and network/port must be configured to allow the connection from the victor application server to the EntraPass Smartlink application. An EntraPass operator must be configured on the EntraPass server to allow the connection to victor.

The integration between victor and EntraPass supports alert filtering that is configured on the victor server.

## victor Application Server

victor Application Server stores all data, operator profiles, roles and event information and video recorder/camera objects.

Dual modes of user authentication allow users to log in using Active Directory credentials or via a 'Basic' method which does not require a domain controller.

Operator profiles are portable which allows users to move from one victor client to another and their credentials follow them, regardless of the PC.

Restrict what devices and features an operator can access by assigning roles using victor's included policy management. Permissions can be set system wide for EntraPass objects.

Any feature can be limited and updated as situations warrant. victor also journals and tracks what has happened on your systems, such as operator activities, commands issued to EntraPass systems, creating an audit trail.

## victor Unified Client

victor Unified Client connects to the victor Application Server, allowing event management, observation and monitoring.

## Licensing

The EntraPass driver is a licensed integration for victor. Please contact American Dynamics support for a EntraPass Driver Server license. Once the new license is applied all Framework / Extension services will restart. In the Server configuration application, the EntraPass Driver Service will display Stopped. Check the box and click Start.

---

**Note:**

The Server Configuration Application must be Run as Administrator to make this change.

---

The EntraPass integration driver can be installed on the victor Application Server. You can download the driver from <http://www.americandynamics.net>

**Note:**

It is recommended to stop the CrossFire Framework Service and close the Server Configuration Application before running the driver installer.

## Installing the EntraPass integration driver

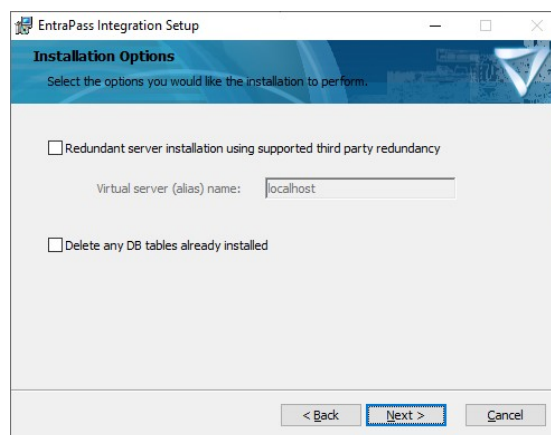
- 1 Right-click `EntraPass_Integration-x.x.x.x_AD.exe` and select **Run as Administrator** to launch the installer. The Setup dialog opens.
- 2 Select the **I agree to the license terms and conditions** check box and click **Install**.
- 3 Click **OK** to shut down CrossFire services.

**Figure 1: Welcome window**



- 4 Click **Next**.

**Figure 2: Installation Options window**

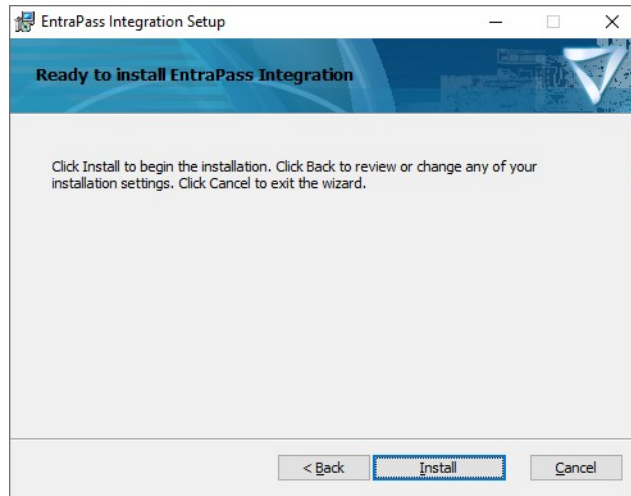


- 5 If the integration is being installed on a redundant server select **Redundant Server** option and enter the virtual server name in the **Virtual Server (alias) name** field. The **Delete any DB tables already installed**

check box should be selected if you want to install a completely new version of the EntraPass tables and overwrite a current install. If this is a new installation, leave this check box clear.

- 6 Click **Next**. On the **Ready to install** window, click **Install**.

**Figure 3: Ready to install window**



- 7 The installation is complete. To close the installer, click **Finish**.



After installation, victor requires some initial configuration before use.

## Initial Configuration

---

**Note:**

Services may start automatically following installation depending on Windows configuration.

---

- 1 Right-click on the Server Configuration Application desktop icon and select **Run as Administrator**.
- 2 Select **Start** next to **CrossFire Framework Service** and **CrossFire Server Component Framework Service**. Status changes from **Stopped** to **Start Pending** and then **Running**.
- 3 When both CrossFire services are displaying as status **Running**, select the **Enabled** check box and click **Start** next to **EntraPass Driver Service**. Status changes from **Stopped** to **Start Pending** and **Running**.
- 4 Repeat Step 3 for each extension service that corresponds to hardware connected to your system.  
For example, **American Dynamics VideoEdge Driver Service** for American Dynamics VideoEdge video recorders.
- 5 Close the Server Configuration Application.
- 6 To start victor, double-click the victor Unified Client desktop icon.

# EntraPass integration configuration

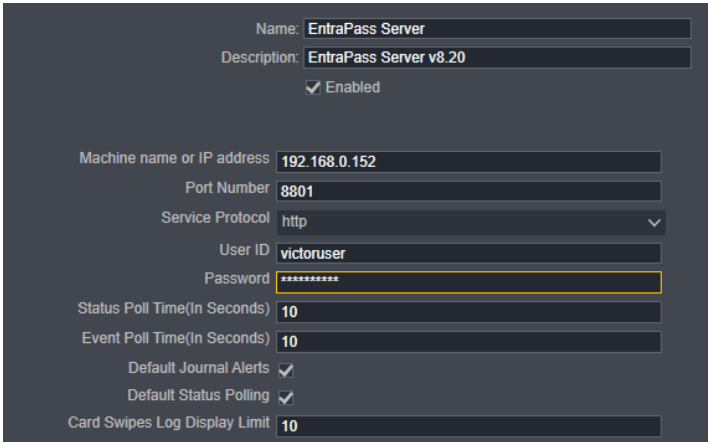
EntraPass servers and all underlying hardware configured and connected to EntraPass can be added to victor.

For the victor integration with EntraPass the Smartlink application must be installed on the EntraPass server. An EntraPass operator's credentials are also required for connection to victor. Any commands or actions carried out on EntraPass devices from victor are logged in EntraPass under this operator. Refer to the EntraPass documentation for adding operators to EntraPass and victor Web Service API installation steps.

## Adding an EntraPass Server

To add an EntraPass connection to victor, complete the following steps:

- 1 Click the **Create new item** icon.
- 2 Select **EntraPass Server**.
- 3 Enter a **Name** and optionally a **Description**.
- 4 Select the **Enabled** check box.
- 5 Enter the **Server IP or hostname**.
- 6 Select **Service Protocol** option.
- 7 Enter the **User ID** and **Password** for the EntraPass connection. These are the credentials of the EntraPass operator required for the victor connection. If the EntraPass server is on a domain, use domain credentials for an operator.
- 8 Enter the **Status Poll Interval** in seconds field to adjust the rate at which the driver polls the EntraPass server for hardware status updates. The default value is 10 sec.
- 9 Enter **Event Poll Time** in seconds field to adjust the rate at which the driver polls the EntraPass server for new events. The default value is 10 sec.
- 10 Set the **Default Journal Alerts** option. This sets the default behavior for all sub-devices which by default use this server setting. Sub-devices can optionally be configured to override this setting.
- 11 Set the **Default Status Polling** option. This sets the default behavior for all sub devices which by default use this server setting. Sub-devices can optionally be configured to override this setting.
- 12 Set the **Card Swipes Transactions Storage** field to set how many card swipes to store in the database for the Card Swipe transaction display.



The screenshot shows a configuration form for an EntraPass Server. The form has a dark background with light-colored text and input fields. The fields are as follows:

- Name:** EntraPass Server
- Description:** EntraPass Server v8.20
- Enabled:** ☒
- Machine name or IP address:** 192.168.0.152
- Port Number:** 8801
- Service Protocol:** http (dropdown menu)
- User ID:** victoruser
- Password:** [masked with asterisks]
- Status Poll Time(In Seconds):** 10
- Event Poll Time(In Seconds):** 10
- Default Journal Alerts:** ☒
- Default Status Polling:** ☒
- Card Swipes Log Display Limit:** 10

- 13 Click the **Save** icon. The EntraPass server is saved and appears in the Device List.

- 14 Upon successful connection to the EntraPass server, EntraPass devices and personnel sync to victor.
- 15 Any personnel or supported devices subsequently added to the EntraPass server, sync automatically to victor.

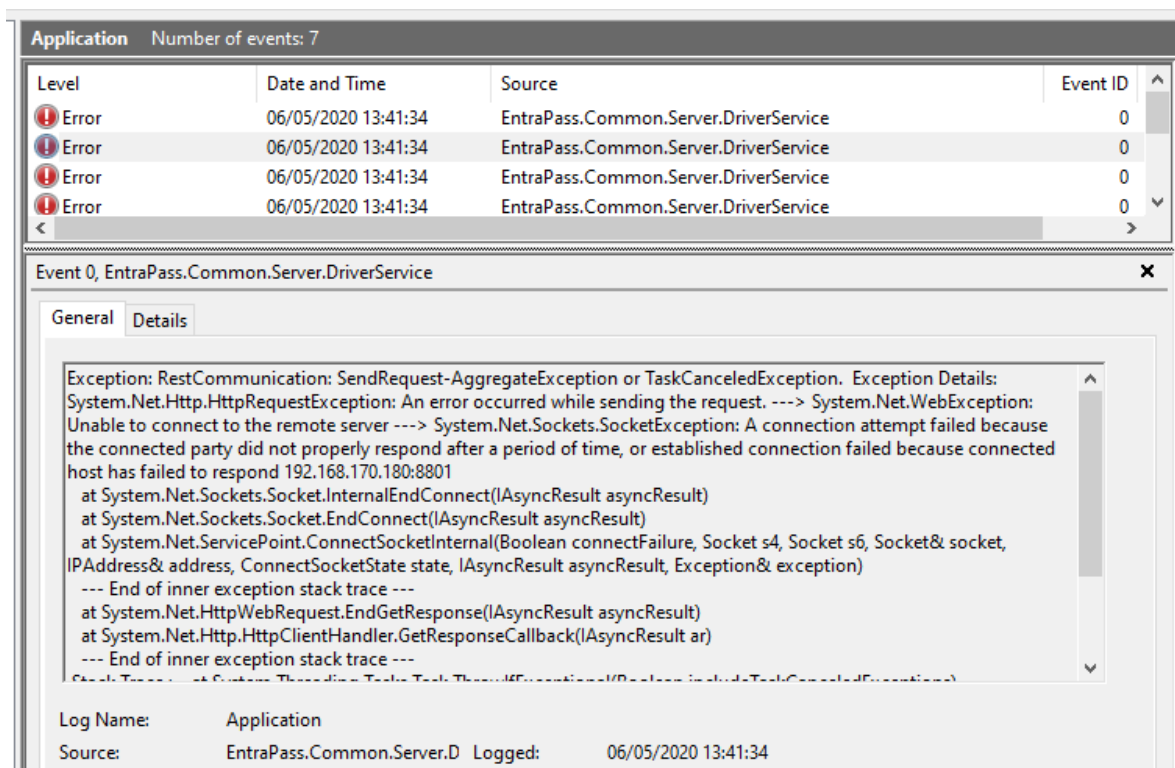
## Testing EntraPass connectivity

- 1 If the device list does not load you can open the Microsoft **Event Viewer** to check for errors, click **Windows Logs > Application logs**.

### Note:

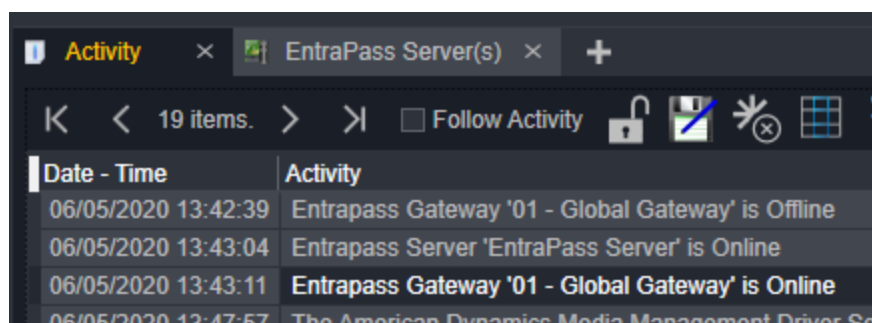
See EntraPass Settings section to configure diagnostic logs to appear in the Event Viewer for more information.

Figure 4: Event Viewer



- 2 To check if the EntraPass events are coming into the Journal, navigate to **New Tab** and **Activity Viewer**.

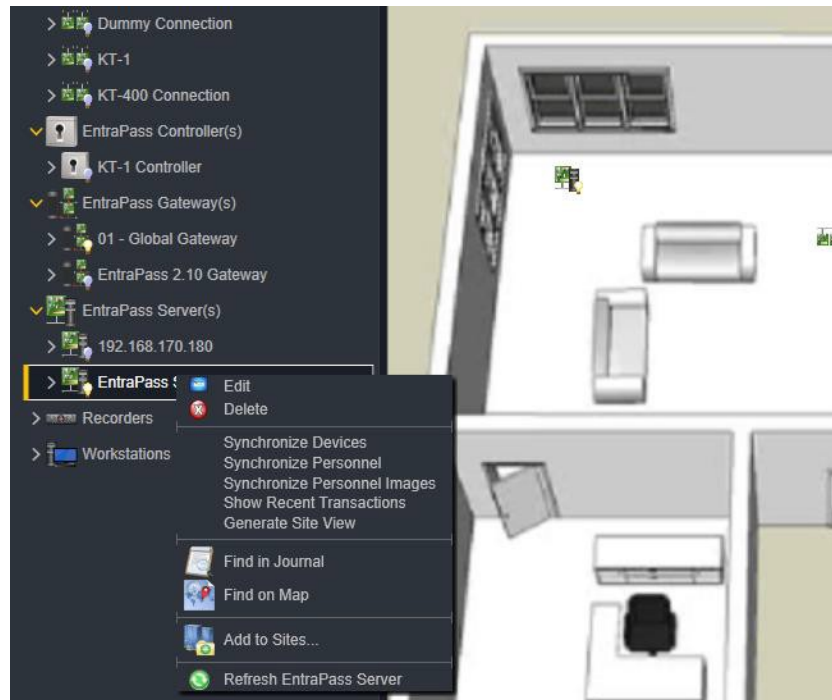
Figure 5: Activity Viewer



# EntraPass commands

EntraPass commands are commands issued by victor to EntraPass objects. EntraPass Commands can be accessed by right clicking an object from the **Device List** or from victor **Maps**.

**Figure 6: EntraPass commands**



All devices have the following common commands: Edit, Delete, Find in Journal, and Find on Map.

**Table 1: Server commands**





Command	Description
Synchronize Devices	Imports all supported devices from the EntraPass Server into victor as EntraPass objects.
Synchronize Personnel	Imports all EntraPass personnel from the EntraPass Server into victor as victor personnel.
Synchronize Personnel Images	Import user images and set as primary victor personnel image for that user.
Show Recent Transactions	The command opens the card swipe transaction display.
Generate Site View	Auto populate the victor Site Groups List with all devices

# Show recent transactions

This command opens a badge swipe transaction view and can be used as alternative to the Swipe and Show feature in victor. This view also displays the EntraPass card swipe outcome information. This window dynamically refreshes to show the latest card swipe transactions at the top.

Figure 7: Recent transactions window

Recent Transactions

Door	Card Holder	Card Number	Transaction Details	Image	Timestamp
KT-1 Door	Doras McEnter	00C7:20772	Admitted - Access granted		2020-05-14T14:26:51
KT-1 Door	Doras McEnter	00C7:20772	Admitted - Access granted		2020-05-14T14:26:31
KT-1 Door	Mr NoAccess	0063:25549	Rejected - Access Level - Access denied bad access		2020-05-14T14:26:21
KT-1 Door	Doras McEnter	00C7:20772	Admitted - Access granted		2020-05-14T14:26:11

<<< <

1 of 1

> >>

Close

# Generate site view

This command auto populates the Site Groups List with the EntraPass devices.

Figure 8: Icon



All devices are added the site view under the parent child hierarchy of devices in EntraPass with the server as the top level folder.

Figure 9: Locating devices

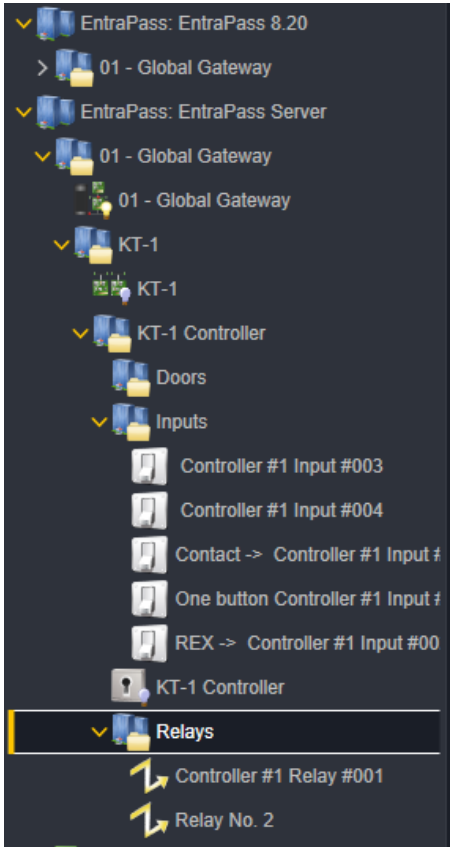


Table 2: Connection commands

Command	Description
Suppress Alerts	Suppress alerts for this connection.
Reactivate Alerts	Reactivate suppressed alerts for this connection.

Table 3: Controller commands

Command	Description
Suppress Alerts	Suppress alerts for this controller.
Reactivate Alerts	Reactivate suppressed alerts for this controller.

**Table 4: Door commands**

Command	Description
Arm	Arm the door (Note: To perform Arm action, Doors need to be associated with an external intrusion panel connected with a KT- 400 controller.)
Disarm	Disarm the door. (Note: To perform Disarm action, Doors need to be associated with an external intrusion panel connected with a KT-400 controller.)
Lock Door	Lock this door.
Unlock Door	Unlock this door.
Unlock Door Temporarily	Momentarily unlock this door.
Enable Reader	Enable the reader
Disable Reader	Disable the reader
One Time Access	Trigger one time access
Suppress Alerts	Suppress alerts for this door.
Reactivate Alerts	Reactivate suppressed alerts for this door.
Start Swipe and Show Admit / Reject	Open Swipe and Show Admit / Reject for this door.
Start Swipe and Show Admit	Open Swipe and Show Admit for this door.
Start Swipe and Show Reject	Open Swipe and Show Reject for this door.

**Table 5: Input commands**

Command	Description
Suppress Alerts	Suppress alerts for this input.
Reactivate Alerts	Reactivate suppressed alerts for this input.
Continuous	Set input to continuous supervision.
No Supervision	Shunt an input
No Supervision-Delay	Temporarily shunt an input.
Normal	Set input to normal.

**Table 6: Relay commands**

Command	Description
Suppress Alerts	Suppress alerts for this relay.
Reactivate Alerts	Reactivate suppressed alerts for this relay.
Activate	Activate the relay.
Activate Temporarily	Activate the relay temporarily.
DeActivate	Deactivate the relay.

---

**Note:**



EntraPass hardware objects imported into victor are read-only and cannot be edited from victor.

---



EntraPass objects are supported on victor Maps and the Find on Map feature. Objects respect all standard victor hardware behaviors such as annunciation, alarms, right click actions and drag and drop.

## Configuring Maps

- 1 Select one of the following options:
  - To create a new map, complete the following steps:
    - a. From the Navigation bar, click the **Create New Item** button, and then click **Map**.
    - b. Enter map **Name** and **Description**.
    - c. Select  to Import a map.
    - d. Browse to and select the required image.
    - e. Click **Open**.
    - f. Select **Import**. File imports and displays in map editor.
  - To edit an existing map, complete the following steps:
    - a. Select **Map** from the **Show All Items** tab
    - b. Right-click the Map and click **Edit**. The Map editor opens.
- 2 To add an EntraPass object onto the map click . The Icon Selector opens.
- 3 Click an object icon to add that object to the map.
- 4 Right-click the icon and select **Drop on Map**. The Template Icon Editor opens.
- 5 Click **Select Object**. The object selector displays.
- 6 Select the victor object to link to the icon and click **OK**.
- 7 Use the Icon editor to assign or change other attributes as required.
- 8 Click **OK** and then click **Save**.

---

**Note:**

Refer to the victor configuration manual for a detailed guide on adding and configuring maps.

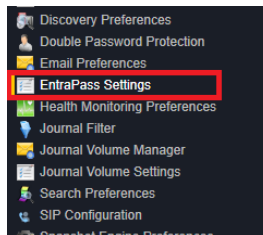
---

# Event configuration

You can use the EntraPass integration to configure EntraPass alerts at device level and at global level. This affects the alert processing at the victor EntraPass driver level. Incoming alerts are filtered in the driver based on this configuration and either journalled or not journalled into victor.

## Configuring EntraPass alert settings

- 1 Click the **System Configuration** icon, select **Settings**, and select **EntraPass Settings**



- 2 Under **EntraPass Alerts Settings** is the alert list editor window.

A screenshot of the 'EntraPass Alerts Settings' window. It features a table with three columns: 'Device Type', 'Alert Name', and 'Enabled'. The 'Device Type' column lists various EntraPass components. The 'Alert Name' column lists specific alert events. The 'Enabled' column contains checkmarks indicating that all listed alerts are currently enabled.

Device Type	Alert Name	Enabled
EntraPass Server	EntraPass Server-Alert-Card definition modified	✓
EntraPass Gateway	EntraPass Server-Alert-Visitor card definition modified	✓
EntraPass Connection	EntraPass Server-Online State-Offline	✓
EntraPass Controller	EntraPass Server-Online State-Online	✓
EntraPass Door	EntraPass Server-Synchronization Status-Synchronization Failed	✓
EntraPass Relay	EntraPass Server-Synchronization Status-Synchronized	✓
EntraPass Input	EntraPass Server-Synchronization Status-Synchronizing	✓
Card Swipe		

- 3 Enable or disable EntraPass alert types by selecting the EntraPass object type and then select or clear the **Enabled** check box for that object.
- 4 When complete click **Save** to save the configuration.

## Enabling and disabling alerts for EntraPass devices

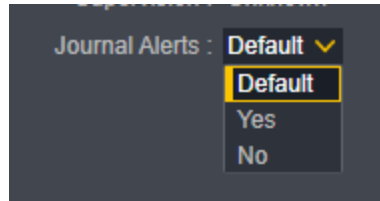
This can be set either by the device object editor or right-click action. These procedures apply to the following EntraPass devices:

- Connection
- Controller
- Input
- Relay
- Door

## Enable or disable by object editor

- 1 From the Device tree, dynamic view, or a map, right-click an EntraPass device and select **Edit**.
- 2 In the device editor, select one of the following options from the Journal Alerts list:
  - Default
  - Yes
  - No

Figure 10: Journal Alerts options

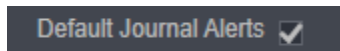


---

### Note:

The default option uses the setting configured at the parent EntraPass Server settings.

---

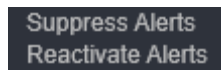


- 3 This enables or disables the creation of victor journal entries for that device.

## Enable/Disable by right-click action:

- 1 From any EntraPass device right-click on the device from the device tree, dynamic view or map and select Suppress/Reactivate Alerts from the command list.


Figure 11: Suppress and reactivate alerts






- 2 This enable/disables the creation of victor journal entries for that device. Note: this right-click action actually sets the edit field described above.

## Using the Events/Schedule Setup Editor


Using the Event Schedule Setup Editor and the Event/Action pairing editor you can build multiple event configurations quicker and easier than building single event configurations one at a time for EntraPass objects.

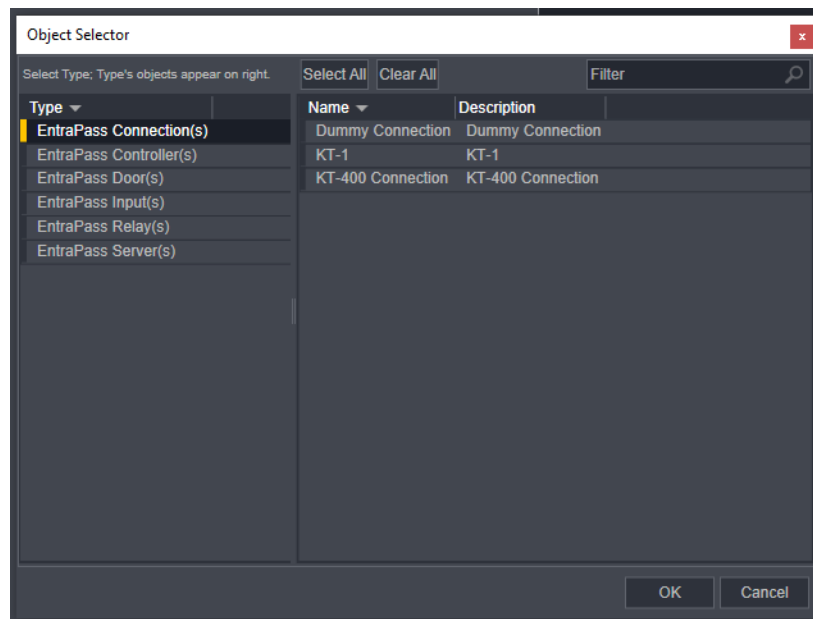
- 1 Select **System Configuration**.
- 2 Select **Events/Schedule Setup**. The Events Setup editor displays.
- 3 To select a device to configure, select one of the following options:
  - Double-click the **Devices** node and use the object selector to select the device
  - Drag a device from the **Devices** list onto the Events/Schedule Setup editor.
- 4 Select  in node of the device added and use the check boxes in the dropdown to assign alerts as required.

- 5 Select **Add Alerts**. Selected alerts are displayed under the Alerts node.
- 6 Select  in the Alerts node and use the Object Selector to assign Actions.
- 7 Repeat as required. Use  and  to add and remove objects.
- 8 Use merge and clone options as required to copy configurations:
  - Merge and clone target configuration
  - Duplicate source configuration to all targets/
  - Remove configuration on source and target
- 9 Use to add/remove schedules as required. Refer to "Scheduling" for more information on using and configuring event schedules.
- 10 Select **Save**.

## Creating an EntraPass action

You can create EntraPass Integration specific actions to link system events with actions you want to trigger.

- 1 Select **EntraPass Action** from the **Create New Item** tab.
- 2 Enter a **Name** and **Description**.
- 3 Click the  icon to add device(s) for this action.
- 4 Select one or many devices to include in the action:



- 5 Select the action to execute. As an example, for a relay the following actions are available:
  - Activate
  - Deactivate
  - Activate Temporarily
  - Suppress Alerts

- Reactivate Alerts




6 Select **Save**.

## Event/Action Pairing Editor

The Event/Action pairing editor is used to tie together system events with actions.

**Note:** Event/Action association can only be made in this editor.

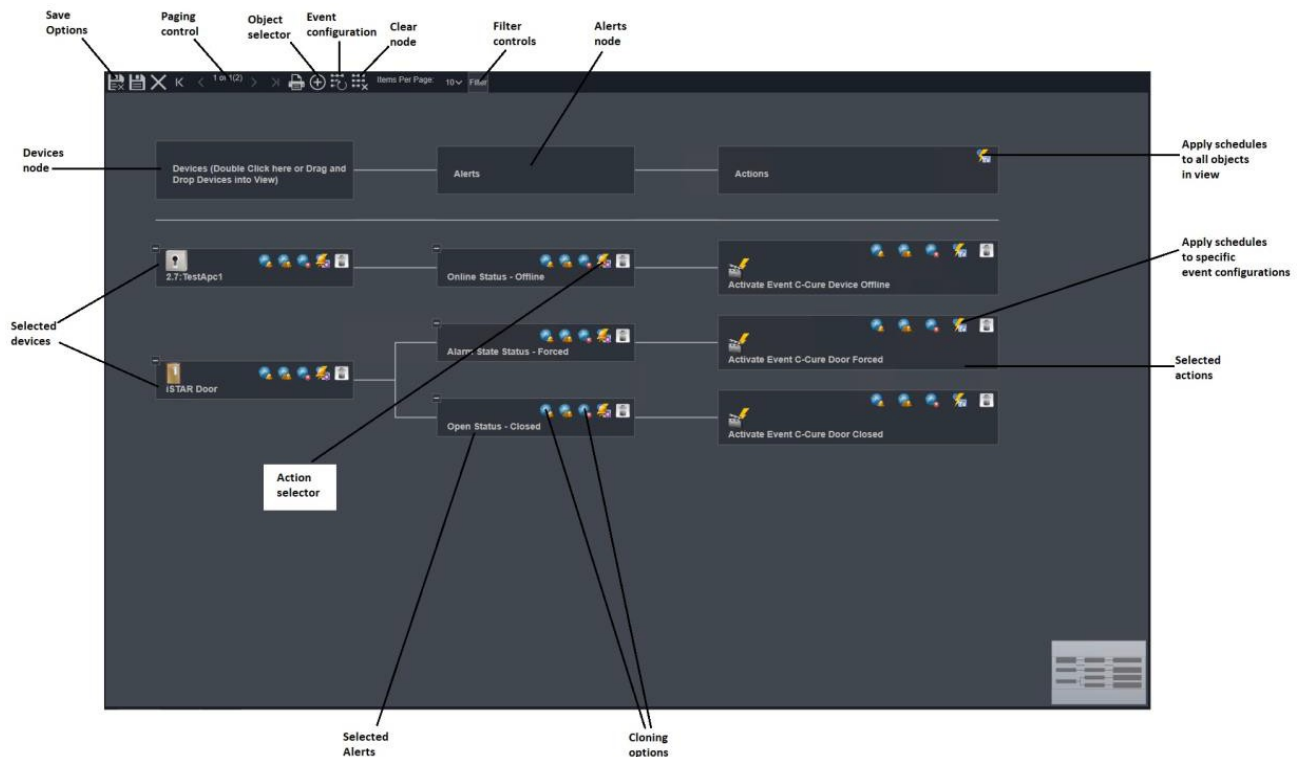
### Using the Event/Action Pairing editor

- 1 Select **Event** from the **Create New Item** tab.
- 2 Select **Event/Action Pairing** from the top toolbar. Editor opens.
- 3 Click the **Events** node and use the Object Selector to select events as required.
- 4 Select  in the **Event** node and use the Object Selector to assign event **Actions**.
- 5 Repeat as required. Use  and  to add and remove objects.
- 6 Select **Save**.

## Events setup

The Events/Schedule setup editor provides a dynamic, visual method of batch linking Devices, Alerts and Actions as well as to set up event scheduling

Figure 12: Events setup



## Event status mapping

This integration is not compatible with event status mapping. You can acknowledge or close events in victor, but this does not affect the EntrsPass system.

# EntraPass Settings

Settings allow you to configure of a range of system wide settings from a single editor. Settings are available from the System Configuration icon. For the EntraPass Integration for victor these settings are helpful to increase logging level that gets exported to the Windows Event Viewer.

## EntraPass General Settings

EntraPass Settings are Global Integration-wide settings for EntraPass Objects, Select System Configuration and Settings to display the following configuration options:

▼ EntraPass General Settings

Diagnostics Logging Level to Event Viewer	Warning ▼
Encryption Enabled	<input checked="" type="checkbox"/>
HeartBeat Timeout (sec)	180
Reconnect Interval (sec)	60
Batch size	25
Number of cards to read	100
Number of images to read	5
Image batch sync request timeout (sec)	181
Interval for image batch response (sec)	2
Device status batch size	100
Status sync queue count	2
Sync batch size	6
Personnel Name Parse Method	Firstnames Lastname ▼
Delete Personnel Removed from EntraPass On Sync	<input checked="" type="checkbox"/>
Reset Latest Alert Time (min)	10

**Diagnostics Logging Level to Event Viewer** – Allows users to enable/disable Diagnostic level logging in the Event Viewer and set the logging level

Diagnostics Logging Level to Event Viewer

Warning ▼

Select from the drop-down:

- **Debug** – Everything is logged for the driver
- **Information** – Errors, warnings and information messages are logged
- **Warning** – Errors and warning messages are logged
- **Error** – Only error messages are logged
- **None** – nothing logged to the Event Viewer

**Note:** This setting is applied once Save is clicked, there is no driver restart required.

**Encryption Enabled:** Use this variable to set whether the login process to the EntraPass server uses encryption. Default is enabled.

**Heartbeat Timeout (sec):** Use this variable to set a server state to Offline, if driver does not receive any message for this duration from the last received message packet. Default value is 180 (in seconds).

**Reconnect Interval (sec):** Use this variable to define the duration of server reconnection retry after it goes to Offline. Default value is 60 (in seconds).

**Batch size:** Number of devices status responses to process at a time. Default is 25.

**Number of cards to Read:** Use this variable to define the number of Personnel that must be read in each request during personnel Sync. Default value is 100.

**Number of images to read:** Use this variable to define the number of simultaneous Personnel Images that must be requested in a batch during image sync. Default value is 5.

**Image batch sync request timeout (sec):** Use this variable to define the duration the batch image request must wait for the batch response to complete. Default value is 180 (in seconds).

**Interval for image batch response timeout (sec):** Use this variable to define the time interval after which driver checks whether image batch response is complete or not. After it is complete, next batch of images could be started. Default value is 2 (in seconds).

**Device status batch size:** Use this variable to define batch size of EntraPass devices that must be sent in request URL for device status updates. Default value is 100.

**Status sync queue count:** Use this variable to define number of queues that run in parallel per EntraPass Server for processing status updates of EntraPass Server objects. Default value is 2.

**Sync batch size:** Use this variable to define the number of parallel Sync calls to the server and is dependent on the number of concurrent client licenses that a customer has in EntraPass Server. Default value is 5.

**Personnel Name Parse Method:** Use this variable to define how the personnel names are parsed from EntraPass victor Personnel first name / last names fields. The cardholder name field in EntraPass is a single text field for the full name. This allows the name to be parsed into first / last names in victor if the names follow one of the format options below:

Options are:

- None: no parsing, the EntraPass name is set for both first and last name fields in victor as did the previous released version of the driver (Default value)
- Firstnames Lastname: parse using the format <First name(s)> <space> <Last name>
- Lastname Firstnames: parse using the format <Last name> <space> <First name(s)>
- Lastname, Firstnames: parse using the format <Last name> <comma> <First name(s)>
- Firstnames, Lastname: parse using the format <First name(s)> <comma> <Last name>

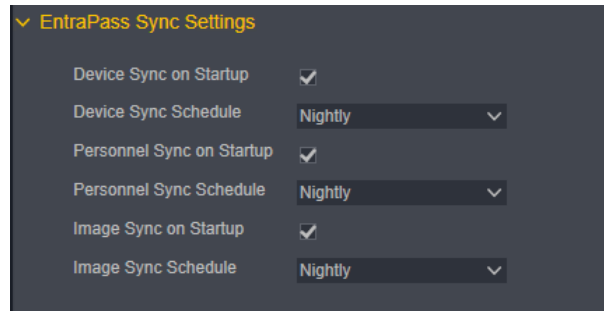
**Delete Objects Removed from EntraPass on Sync:** Use this variable to enable/disable deletion of objects in victor during synchronization if those objects have been removed from EntraPass. Default value is disabled.

**Reset Latest Alert Time (min):** Devices that receive EntraPass alerts (Connections, Controllers, Doors, Inputs, Relays) have the status property "Latest Alert" which shows the most recent alert received for that device. This property can be used for adding alert based annunciations to the map objects. This variable sets the time after which the property gets reset back to None. Default value is 10 minutes. Setting to 0 disables the variables getting reset.



## EntraPass Sync Settings

Sync settings configures the device and personnel synchronization setting on driver startup and on a schedule



The screenshot shows the 'EntraPass Sync Settings' window. It contains six settings, each with a checkbox and a dropdown menu. The settings are: Device Sync on Startup (checked), Device Sync Schedule (Nightly), Personnel Sync on Startup (checked), Personnel Sync Schedule (Nightly), Image Sync on Startup (checked), and Image Sync Schedule (Nightly).

Setting	Value
Device Sync on Startup	<input checked="" type="checkbox"/>
Device Sync Schedule	Nightly
Personnel Sync on Startup	<input checked="" type="checkbox"/>
Personnel Sync Schedule	Nightly
Image Sync on Startup	<input checked="" type="checkbox"/>
Image Sync Schedule	Nightly

**Device Sync on Startup** – Use this variable to define whether user wants to do auto sync devices whenever a server comes Online from Offline state. Default value is true.

**Device Sync Schedule** – Use this variable to select a victor Schedule to use to start device synchronization. The synchronization starts when the victor Schedule Active state is triggered. Default value is Nightly.

**Personnel Sync on Startup** – Use this variable to define whether user wants to do auto sync personnel whenever a server comes Online from Offline state. Default value is true.

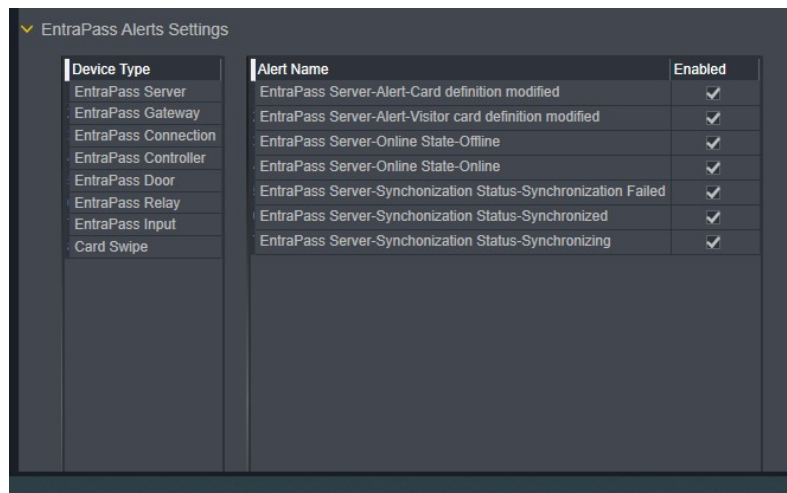
**Personnel Sync Schedule** – Use this variable to select a victor Schedule to use to start personnel synchronization. The synchronization starts when the victor Schedule Active state is triggered. Default value is Nightly.

**Image Sync on Startup** – Use this variable to define whether user wants to do auto sync personnel images whenever a server comes Online from Offline state. Default value is true.

**Image Sync Schedule** – Use this variable to select a victor Schedule to use to start personnel synchronization. The synchronization starts when the victor Schedule Active state is triggered. Default value is Nightly.

## EntraPass Alerts Settings

Allows users to enable/disable EntraPass events that will be journaled in victor.



The screenshot shows the 'EntraPass Alerts Settings' window. It contains a table with three columns: Device Type, Alert Name, and Enabled. The table lists various alert types and their corresponding alert names, with the Enabled column showing a checked box for each.

Device Type	Alert Name	Enabled
EntraPass Server	EntraPass Server-Alert-Card definition modified	<input checked="" type="checkbox"/>
EntraPass Gateway	EntraPass Server-Alert-Visitor card definition modified	<input checked="" type="checkbox"/>
EntraPass Connection	EntraPass Server-Online State-Offline	<input checked="" type="checkbox"/>
EntraPass Controller	EntraPass Server-Online State-Online	<input checked="" type="checkbox"/>
EntraPass Door	EntraPass Server-Synchronization Status-Synchronization Failed	<input checked="" type="checkbox"/>
EntraPass Relay	EntraPass Server-Synchronization Status-Synchronized	<input checked="" type="checkbox"/>
EntraPass Input	EntraPass Server-Synchronization Status-Synchronizing	<input checked="" type="checkbox"/>
Card Swipe		

Enable/disable EntraPass alert types by selecting the EntraPass object type and then selecting/unselecting the Enabled column option.

# Swipe and Show

When a user swipes the card on the reader, the corresponding swipes appear in the Swipe and Show tab.

**Note:** For the Swipe and Show to function, ensure the following:

- Personnel and personnel images are synchronized.
- Swipe and Show tab is open.

## Procedure 1 Viewing Swipe and Show

- 1 Select **Swipe and Show** from **New tab** screen.
- 2 Choose one of the following options:
  - Monitor all Doors for Admits
  - Monitor all Doors for Rejects
  - Monitor all Doors for Admits/Rejects.



The details of the Personnel with the image appear in the Swipe and Show tab.

# EntraPass Device States

The following sections lists the states supported by each of the EntraPass object types in victor and the object state icons supported. The order shown in the state image tables below reflect the order in which image is selected to be displayed for each object type.

## EntraPass Server States

State	State Values
Devices Sync Status	Synchronization Status Unknown Synchronization Failed Synchronizing Synchronized
Communication State	Online Offline Unknown
Personnel Sync Status	Synchronization Status Unknown Synchronization Failed Synchronizing Synchronized
Personnel Image Sync Status	Synchronization Status Unknown Synchronization Failed Synchronizing Synchronized

## Gateway States

State	State Values
Communication State	Online Offline Unknown

## Connection States

State	State Values
Communication State	Online Offline Unknown
Latest Alert	Loopcommunicationfailure Loopcommunicationrestore Loopcommunicationtrouble

## Controller States

State	State Values
Communication State	Online Offline Unknown
Tamper Status	Unknown Yes No
AC Failure	Unknown Yes No
Hard Reset	Unknown Yes No
Tamper Schedule	Unknown Yes No
Ac Schedule	Unknown Yes No
Latest Alert	Controllercommunicationfailed Controllercommunicationrestored ControllerACpowerfailed ControllerACpowerrestored Tamperswitchinalarm Tamperswitchrestored Hardresetcontroller Softresetcontroller Controllersuccessfullyreloaded Controllerreloadfailure Controllerfirmwarereloadstart Controllertrouble Controllertroublerestored Controllerhardresetbyoperator Controllersoftresetbyoperator Controllerreloadedbyoperator Controllerreaderkeypadunlockedbyoperator Controllerreaderpowerresetbyoperator Controllerdetailedstatusrequestedbyoperator Controllerpassbackforgivenbyoperator Controllercardslistrequestedbyoperator Controllercardsmovedbyoperator Controllercardslistcancelledbyoperator Controllernotassignedrequestedbyoperator ControllerAuxiliarypowerfailure ControllerAuxiliarypowerrestored ControllerprealarmACpowerfailure ControllerprealarmACpowerrestored Controllermodulecombuspowerfailure Controllermodulecombuspowerrestored Controllerreaderpowerfailure Controllerreaderpowerrestored Controllerbatterypowerfailure Controllerbatterypowerrestored Controllerepromreadingfailure ControllerdatetimeRtCreadingfailure Controllerexecuteprogramparityfailure Controllerexecuteprogrammestartup

## Door States

State	State Values
Open State	Close Forced Open Too Long Pre Alarm Open Too Long Still Open Open Unknown
Lock State	Lock Lock First Man In Unlock Operator Unlock Schedule Unlock Input One Time Access Unlock On Access Unlock Double Swipe Unlock Triple Swipe Unlock Temporarily Unknown
Reader Disable	Unknown Yes No
Armed	None Yes No
Latest Alarm	Doorarmedalarminterface DoorDisarmedalarminterface Doorexitdelaystartalarminterface Doorexitdelayendalarminterface Doorentrydelaystartalarminterface Doorentrydelayendalarminterface Dooralarmalarminterface Dooralarmrestoredalarminterface Requesttodisarmalarminterface Doorforcedopenrestored Doorclosednormalcondition Doorforcedopen PreAlarmonDoorOpenTooLong Dooropentoolong Dooralarmonrelock Doorunlockedbyschedule Doorlockedbyschedule RequesttoexitdeniedbyInterlock Doorlockdevicefailure Doorlockdevicenormalcondition Doorrelock Doorunlockedbyevent Doorunlockedtemporarilybyevent Doorunlockbyinput Doorlockbyinput Doorgroupunlockbyinput Doorgrouplockbyinput Doorlockbyalarmsystemarmed Doorlockedbyoperator Doorunlockedbyoperator Dooronetimeaccessbyoperator Readerenabledbyoperator Readerdisabledbyoperator Doorreturnedtoschedulebyoperator Doorarmedbyoperator

State	State Values
	Doordisarmedbyoperator Doortogglebyoperator Doortemporarilyunlockedbyoperator Doubleswipeactiongranted Tripleswipeactiongranted

## Input States

State	State Values
Supervision	Normal Continuous None Reverse Unknown
Input State	Normal Normal Not Supervised Alarm Alarm Not Supervised Trouble Trouble Supervised Tamper Tamper Supervised Activated Activated Not Supervised Unknown
Shunted by	Input Input Tempo Manual Manual Tempo Door Disarmed Entry Delay Exit Delay None Unknown
Latest Alarm	Inputrestoredorinnormalcondition Inputinprealarm InputinalarmReturntoservice Inputinalarm Inputshuntedbyinput Inputunshuntedbyinput Inputgroupshuntedbyinput Inputgroupunshuntedbyinput Inputintrouble Inputshuntedtemporarily Inputunshuntedtemporarily Inputshuntedonexitdelayalarminterface Inputunshuntedonexitdelayalarminterface Inputshuntedondisarmalarminterface Inputunshuntedondisarmalarminterface Inputshuntedonentrydelayalarminterface Inputunshuntedonentrydelayalarminterface Inputdeactivated InputactivatedReturntoservice Inputactivated Inputreturntoschedulebyoperator Inputreturntonormalbyoperator Inputshuntedbyoperator Inputcontinuooussupervisionbyoperator Inputreverseconditionbyoperator Inputshuntedtemporarilybyoperator Inputshunttogglebyoperator Inputtamperinalarm Inputtamperrestored Inputtroublerestored Inputunshunted

## Relay States

State	State Values
State	Deactivate Activate Operator Activate Schedule Activate Input Activate Area Activate Event Activate Alarm System Activate Alarm System Status Activate Alarm System Postpone Activate Alarm System Entry Delay Activate Alarm System Exit Delay Activate Alarm System Arming Delay Activate Alarm System Prevent Arming Activate Alarm System Alarm1 Activate Alarm System Alarm2 Activate Alarm System Bell Unknown
Activate Temp	Yes No Unknown
Latest Alarm	Relayactivatedbyschedule Relaydeactivatedbyschedule Relayactivatedbyinput Relaydeactivatedbyinput Relayactivatedbyopenarea Relaydeactivatedbyclosearea Relayactivatedbyanevent Relaytemporarilyactivatedbyanevent Relaydeactivatedbyanevent Relaytemporarilyactivatedbydooraccessextendeddelay Relaydeactivatedaftertemporarilyaction Relaytemporarilyactivatedbyinput Relayactivatedbyalarmsystem Relaytemporarilyactivatedbyalarmsystem Relaydeactivatedbyalarmsystem Relaytemporarilyactivatedbykeypadkey Relayactivatedbyfullarea Relaydeactivatedbynotfullarea Relaydeactivatedbyoperator Relayactivatedbyoperator Relaytemporarilyactivatedbyoperator Relayreturnedtoschedulebyoperator Relaytogglebyoperator



## EntraPass Alerts

List of supported EntraPass Alerts:

Connection Alerts
Loopcommunicationfailure
Loopcommunicationrestore
Loopcommunicationtrouble

Controller Alerts
Controllercommunicationfailed
Controllercommunicationrestored
ControllerACpowerfailed
ControllerACpowerrestored
Tamperswitchinalarm
Tamperswitchrestored
Hardresetcontroller
Softresetcontroller
Controllersuccessfullyreloaded
Controllerreloadfailure
Controllerfirmwarereoloadstart
Controllertrouble
Controllertroublerestored
Controllerhardresetbyoperator
Controllersoftresetbyoperator
Controllerreloadedbyoperator
Controllerreaderkeypadunlockedbyoperator
Controllerreaderpowerresetbyoperator
Controllerdetailedstatusrequestedbyoperator
Controllerpassbackforgivenbyoperator
Controllercardslistrequestedbyoperator
Controllercardsmovedbyoperator
Controllercardslistcancelledbyoperator
Controllernotassignedrequestedbyoperator
ControllerAuxiliarypowerfailure
ControllerAuxiliarypowerrestored

Controller Alerts
ControllerprealarmACpowerfailure
ControllerprealarmACpowerrestored
Controllermodulecombuspowerfailure
Controllermodulecombuspowerrestored
Controllerreaderpowerfailure
Controllerreaderpowerrestored
Controllerbatterypowerfailure
Controllerbatterypowerrestored
Controllerepromreadingfailure
ControllerdatetimeRtCreadingfailure
Controllerexecuteprogramparityfailure
Controllerexecuteprogrammestartup

Door Alerts
Doorarmedalarmininterface
DoorDisarmedalarmininterface
Doorexitdelaystartalarmininterface
Doorexitdelayendalarmininterface
Doorentrydelaystartalarmininterface
Doorentrydelayendalarmininterface
Dooralarmalarmininterface
Dooralarmrestoredalarmininterface
Requesttodisarmalarmininterface
Doorforcedopenrestored
Doorclosednormalcondition
Doorforcedopen
PreAlarmonDoorOpenTooLong
Dooropentoolong
Dooralarmonrelock
Doorunlockedbyschedule
Doorlockedbyschedule
RequesttoexitdeniedbyInterlock
Doorlockdevicefailure

Door Alerts
Doorlockdevicenormalcondition
Doorrelock
Doorunlockedbyevent
Doorunlockedtemporarilybyevent
Doorunlockbyinput
Doorlockbyinput
Doorgroupunlockbyinput
Doorgrouplockbyinput
Doorlockbyalarmsystemarmed
Doorlockedbyoperator
Doorunlockedbyoperator
Dooronetimeaccessbyoperator
Readerenabledbyoperator
Readerdisabledbyoperator
Doorreturnedtoschedulebyoperator
Doorarmedbyoperator
Doordisarmedbyoperator
Doortogglebyoperator
Doortemporarilyunlockedbyoperator
Doubleswipeactiongranted
Tripleswipeactiongranted

Input Alerts
Inputrestoredorinnormalcondition
Inputinprealarm
InputinalarmReturntoservice
Inputinalarm
Inputshuntedbyinput
Inputunshuntedbyinput
Inputgroupshuntedbyinput
Inputgroupunshuntedbyinput
Inputintrouble
Inputshuntedtemporarily

Input Alerts
Inputunshuntedtemporarily
Inputshuntedonexitdelayalarmininterface
Inputunshuntedonexitdelayalarmininterface
Inputshuntedondisarmalarmininterface
Inputunshuntedondisarmalarmininterface
Inputshuntedonentrydelayalarmininterface
Inputunshuntedonentrydelayalarmininterface
Inputdeactivated
InputactivatedReturntoservice
Inputactivated
Inputreturntoschedulebyoperator
Inputreturntonormalbyoperator
Inputshuntedbyoperator
Inputcontinuoussupervisionbyoperator
Inputreverseconditionbyoperator
Inputshuntedtemporarilybyoperator
Inputshunttogglebyoperator
Inputtamperinalarm
Inputtamperrestored
Inputtroublerestored
Inputunshunted

Output Alarms
Output Alarms
Relayactivatedbyschedule
Relaydeactivatedbyschedule
Relayactivatedbyinput
Relaydeactivatedbyinput
Relayactivatedbyopenarea
Relaydeactivatedbyclosearea
Relayactivatedbyanevent
Relaytemporarilyactivatedbyanevent
Relaydeactivatedbyanevent

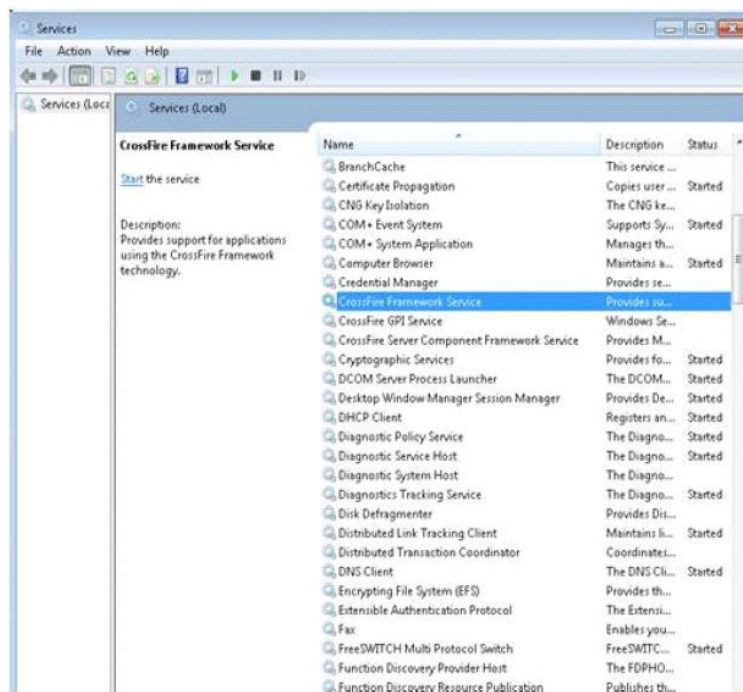
Output Alarms
Relaytemporarilyactivatedbydooraccessextendeddelay
Relaydeactivatedaftertemporarilyaction
Relaytemporarilyactivatedbyinput
Relayactivatedbyalarmsystem
Relaytemporarilyactivatedbyalarmsystem
Relaydeactivatedbyalarmsystem
Relaytemporarilyactivatedbykeypadkey
Relayactivatedbyfullarea
Relaydeactivatedbynotfullarea
Relaydeactivatedbyoperator
Relayactivatedbyoperator
Relaytemporarilyactivatedbyoperator
Relayreturnedtoschedulebyoperator
Relaytogglebyoperator

This section provides troubleshooting information for issues that may occur in the EntraPass Integration.

**Problem:** Sometimes the installation may fail if the CrossFire service does not stop on time and throws a time out error.

**Solution:** Ensure that you have completed the following steps:

- Check if the CrossFire service is stopped from services panel in case of installation failure. Refer to CrossFire Services screenshot below.
- Wait till the CrossFire service is stopped and then trigger the installation again. This will work fine as the service is stopped already.



**Problem:** EntraPass Server is not communicating with victor.

**Solution:** Ensure that you have completed the following steps:

- Validate firewall settings. Add required ports in Inbound and Outbound port list of firewall.
- Ensure IP Address or System Name are correct.
- Ensure that the current network configurations are able to validate the Machine Name provided in Machine Name or IP Address field of the EntraPass Server editor.
- Ensure that the required services are running on EntraPass server.

## KT 400 Controller configuration with DSC PowerSeries

### Requirements

- EntraPass Server is installed.
- A DSC PowerSeries alarm panel and an IT-100 module.
- Door contact is connected on KT-400.
- RS-232 cable and 740-1047 adapter (p/n CBLK-IT100).
- Up-to-date KT-400 firmware.

### Procedure 1 Hardware Setup

To connect the IT-100 to the KT-400 and the DSC PowerSeries Intrusion panel, follow the steps below:

- 1 Connect the IT-100 to the alarm panel:
  - a Power down the alarm panel.
  - b Connect the IT-100 module to the DSC PowerSeries Intrusion panel using a 4-wire KEYBUS connection. Connect the RED, BLK, YEL and GRN terminals to the KEYBUS terminals of the DSC PowerSeries Intrusion panel.
  - c Power up the alarm panel.
- 2 To connect the IT-100 to the KT-400, refer to last page of the DSC IT-100 manual.  
**Note:** The IT-100 can be connected at a maximum distance of 98.4ft (30m) at 9600 rate from the KT-400. Refer to the DSC IT-100 manual for more information.

## EntraPass Setup

For the EntraPass setup see Setting up DSC Integration through a KT-400 Controller manual or contact the Kantech support team.

### KT-NCC Controller Configuration

The current EntraPass Integration supports the following use cases:

- Import of Sites, Controllers, Doors, Inputs and Output configuration.
- Control commands to doors and outputs.
- Status and event notifications from EntraPass.
- KT-NCC network communications controller.

## What is the KT NCC?

Kantech KT-NCC is a powerful way to expand an EntraPass Global edition system. Instead of relying on a PC for communication between the controllers and server, KT-NCC network communicator module is in control.

KT-NCC manages communication between the EntraPass software and the door controllers.

All the events from the controllers are stored in the KT-NCC for additional security in the event of communication failure between the controllers and the server. KT-NCC supports any combination of up to 128 controllers.

For more information about the KT NCC, go to <http://www.kantech.com/>.



### Configuring EntraPass for remote victor Client operation

This section describes the steps required to configure EntraPass Server for use with victor unified Client over a secure (https) connection.

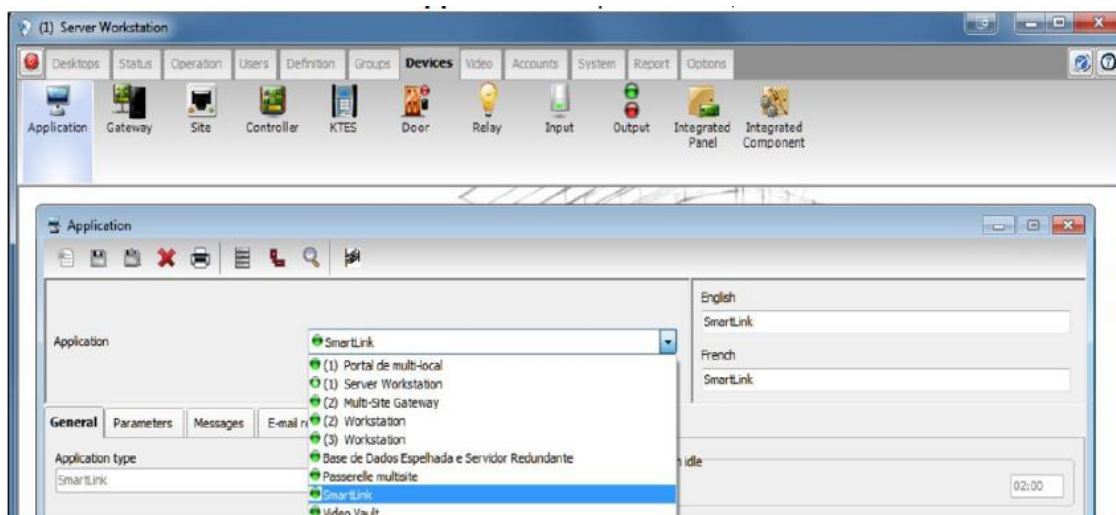
#### Prerequisites

- EntraPass Server
- victor Unified Client
- Kantech SmartService and SmartLink Running

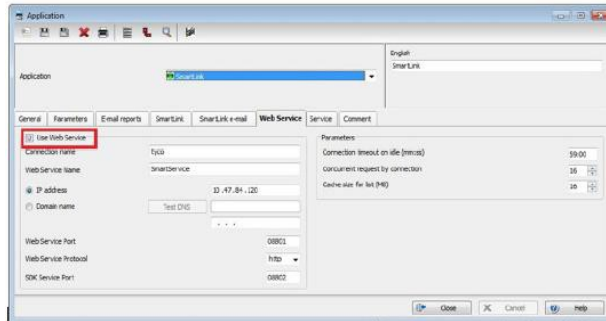
**Note:** SmartLink and WebStation must have been previously registered in EntraPass for the SmartLink Webstation tab to be available. Refer to the EntraPass Reference manual for more information.

#### Procedure 1 Configuring EntraPass for remote victor Client operation

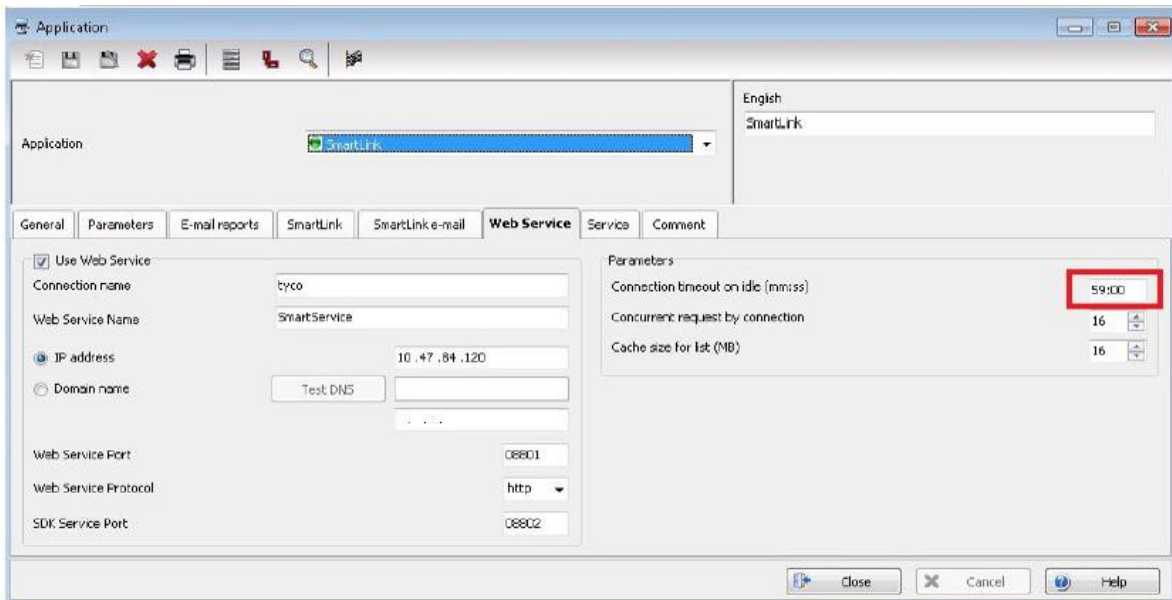
- 1 Log in to the EntraPass Server Workstation.
- 2 Select **Devices**, and then select **Application**.



- 3 Select **SmartLink** from the **Application** list.
- 4 Click the **Web Service** tab.



- 5 Ensure that the **Use Web Service** check box is selected.



- 6 Set **Connection Time Out on Idle** to the maximum value, 59 minutes

## Configuring Ports with an SSL Certificate

To configure a port, the tool you use depends on the operating system that is running on your machine.

Depending on the Operating system of your machine, different tools can be used. For Windows Server 2003 or Windows XP - use the HttpCfg.exe tool that is installed with Windows Server 2003.

For more information refer to Microsoft Windows Support Tools documentation.

### Prerequisites

- A valid SSL certificate on IIS.
- Port 8801 is open.
- Administrator privileges on the server.

**Note:** Modifying certificates stored on the computer requires administrative privileges.

## Procedure 2 Getting a Certificate's Thumb-print

- 1 View certificates in the MMC snap-in:
  - a Open a Command prompt window
  - b Type mmc and press Enter. You must have Administrator privileges to view certificates.
  - c On the File menu, click Add/Remove Snap In. Click Add.
  - d In the Add Standalone Snap-in dialog box, select Certificates. Click Add.
  - e In the Certificates snap-in dialog box, select Computer account and click Next.
  - f Optionally, you can select My User account or Service account. If you are not an administrator of the computer, you can manage certificates only for your user account.
  - g In the Select Computer dialog box, click Finish.
  - h In the Add Standalone Snap-in dialog box, click Close. On the Add/Remove Snap-in dialog box, click OK.
  - i In the Console Root window, click Certificates (Local Computer) to view the certificate stores for the computer.
  - j (Optional.) To view certificates for your account, repeat steps 3 to 6. In step 7, instead of selecting Computer account, click My User account and repeat steps h to j.
  - k (Optional.) On the File menu, click Save or Save As. Save the console file for later reuse.
- 2 Retrieving a certificate's thumb-print
  - a Open the Microsoft Management Console (MMC) snap-in for certificates.
  - b In the Console Root window's left pane, click Certificates (Local Computer). Click the Personal folder to expand it.
  - c Click the Certificates folder to expand it.
  - d In the list of certificates, note the Intended Purposes heading. Find a certificate that lists Client Authentication as an intended purpose. Double click the certificate.
  - e In the Certificate dialog box, click the Details tab.
  - f Scroll through the list of fields and click Thumb-print.
  - g Copy the thumbprint of the certificate into a text editor, such as Notepad.
  - h Remove all spaces between the hexadecimal characters. (One way to accomplish this is to use the text editor's find-and-replace feature and replace each space with a null character.) `httpcfg set ssl -i 0.0.0.0:8801 -h 0000000000003ed9cd0c315bbb6dc1c08da5e6`
  - i In Windows Vista, use the Netsh.exe tool, as shown in the following example: `netsh http add sslcert ipport=0.0.0.0:8801 certhash=0000000000003ed9cd0c315bbb6dc1c08da5e6 appid={00112233-4455-6677- 8899-AABBCCDDEEFF}`

## Binding an SSL certificate to a port number and support client certificates

- In Windows Server 2003, Server 2008 or Windows XP, to support clients that authenticate with X.509 certificates at the transport layer, follow the preceding procedure but pass an additional command-line parameter to HttpCfg.exe, as shown in the following example: `httpcfg set ssl -i 0.0.0.0:8801 -h 0000000000003ed9cd0c315bbb6dc1c08da5e6 -f 2`
- In Windows 7, to support clients that authenticate with X.509 certificates at the transport layer, follow the preceding procedure, but with an additional parameter, as shown in the following example: `netsh http add sslcert ipport=0.0.0.0:8801 certhash=0000000000003ed9cd0c315bbb6dc1c08da5e6 appid={00112233-4455-6677-8899-AABBCCDDEEFF} clientcertnegotiation=enablefV`