



American Dynamics

From Tyco Security Products

victor EntraPass Integration User Guide

v5.6

Revision A0

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.

© 2021 Johnson Controls. All Rights Reserved.

American Dynamics
6600 Congress Avenue
Boca Raton, FL 33487 U.S.A.

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.

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.

Introduction

EntraPass Integration Overview	1
Product Components	1
Features	2

Installation

Minimum Requirements	4
Hardware	4
Software	4
Prerequisites	4
Installation	4
EntraPass Configuration File	5

Operation

Administration Functions	7
Hardware Information	7
Adding EntraPass Servers	7
Victor Integration	9
Roles	9
Associations	9
Reports	10
Events	10
Predefined EntraPass Events	11
EntraPass Actions	11
Maps	12
EntraPass Objects	13
Swipe and Show	19
General Operation	19
Manual Actions	19
Doors	19
Inputs	20
Relays	20
Servers	21
Context (Right Click) Menu options	21
Controllers	21
Sites	22

Troubleshooting

Troubleshooting:	23
----------------------------	----

Appendix A

KT 400 Controller configuration with DSC PowerSeries	1
Requirements	1
Hardware Setup	1
EntraPass Setup	1
KT-NCC Controller Configuration	2
What is the KT NCC?	2

Appendix B

Configuring EntraPass for remote victor Client operation	1
Prerequisites	1
Configuring Ports with an SSL Certificate	2
Prerequisites	3
Binding an SSL certificate to a port number and support client certificates	4

Introduction

EntraPass Integration Overview

The EntraPass server integration provides advanced, seamless integration between victor and EntraPass servers allowing users to monitor and synchronize their devices from within the victor interface.

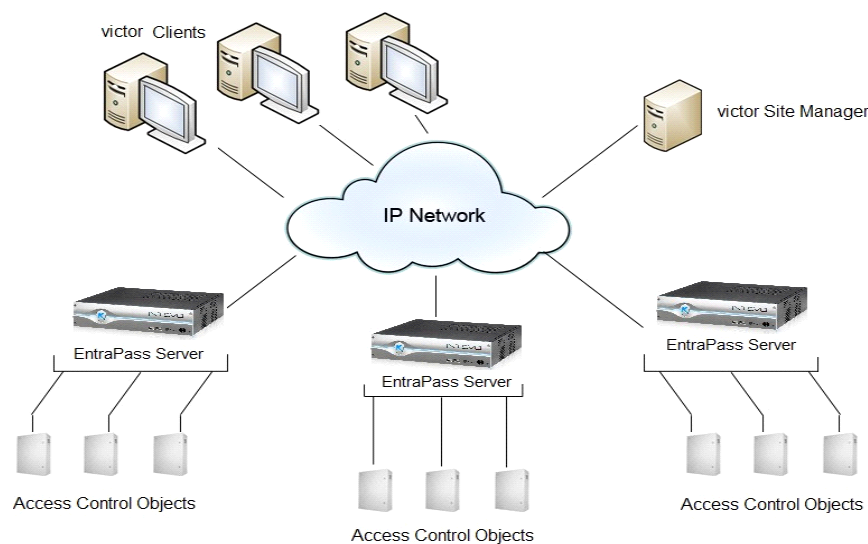
Product Components

EntraPass Client: Used to specify connection details to EntraPass server and perform synchronization actions.

EntraPass Objects: Physical or logical EntraPass entities within the victor environment.

EntraPass Server Component: Facilitates and maintains communication with the EntraPass unit and auto-creates Sites, Controllers, Doors, Inputs and Relay objects based on EntraPass unit properties.

Figure 3-1 System Overview



Features

The objective of the EntraPass Integration is to provide a standard, single interface between EntraPass and American Dynamic's victor Video Management product.

The following are the supported features:

- Supports features such as Create, Edit, or Delete a server object.
- Supports KT NCC Gateway.
- View and Delete feature for Gateway, Site, Controller, Door, Input, and Relay.

Note

When server has large number of objects (5000+), it is recommended to delete sites instead of deleting EntraPass server.

- Supports configuration of a server object by using either the Machine Name or IP Address.
- Manual and Auto Synchronization for server.

Note

In EntraPass Integration driver, it is recommended to perform sync operation on one server at a time.

- Supports the following manual actions for Door objects:
 - Lock
 - Unlock
 - Unlock Temporarily
 - Enable Reader
 - Disable Reader
 - Arm
 - Disarm Door
 - One Time Access
- Supports the following manual actions for Input objects:
 - Continuous
 - No Supervision
 - No Supervision-Delay
 - Normal
- Supports the following manual actions for Relay objects:
 - Activate
 - Deactivate
 - Activate Temporarily
- Supports Integration with victor **Roles**, victor **Object Association**, victor **Journal**, and victor Event Management.
- Supports the EntraPass Object Integration with the following victor features:
 - Maps
 - Find in Journal
 - Find on Map
 - victor Health Dashboard
- Supports the smart service binding in the form of https.
- Supports **Swipe and Show** feature, **Synchronization of Personnel** and **Synchronization of Personnel Images**.
- Supports predefined events for Servers, Sites, Controllers and Doors.
- Supports EntraPass Actions feature for Servers, Doors and Relays.
- Supports TLS 1.2 for security.

Installation

Minimum Requirements

Hardware

The EntraPass integration has the same hardware requirements as victor Application Server. Therefore, if the machine can successfully run victor then it will satisfy EntraPass integration requirements.

EntraPass integration requires approximately 50MB of available Hard Disk space.

Software

- EntraPass Server
- EntraPass victor Integration
- victor Application Server
- victor Unified Client

Prerequisites

- To install the EntraPass Integration on victor Application Server, you must install the .NET Framework 3.5 on victor server.
- The EntraPass installer must be installed on both victor Server and all victor Client machines.

Installation

Note

Refer to Appendix B for information on configuring EntraPass servers for use with victor Unified Client over a secure (https) connection.

Note

It is recommended to stop the CrossFire services before initiating the installation of EntraPass Integration.

Procedure 4-1 Adding EntraPass Integration to victor

Step	Action
------	--------

- | | |
|---|--|
| 1 | Close any currently running programs. |
| 2 | Open a web browser and navigate to http://www.americandynamics.net . |

- 3 Download the appropriate version of the EntraPass Integration software driver for your version of victor.
- 4 Launch the EntraPass Integration Software Driver. The Welcome to EntraPass Integration Setup window displays.
- 5 Click **Next**. The End User License Agreement (EULA) window displays.
- 6 Read the **EULA**.
- 7 Select the **I accept the terms in the license agreement** button, then click **Next**.
- 8 Click **Install**. The program begins to install, this may take several minutes. Once completed the **Install Shield Wizard Complete** window displays.

Note

Check-box **Start the Tyco CrossFire services** is selected by default. If this check-box is not selected, then the CrossFire services will not start automatically.

- 9 Click **Finish**.

Note

The install process stops all victor Server services, these services must be restarted on victor Server machines once the install is complete.

EntraPass Configuration File

The EntraPass Configuration file is located at Tyco/ Crossfire/ ServerComponents. This section describes the values that you can change in the EntraPass Configuration file:

Note

If you make any changes in the configuration file, you must restart the driver. Ensure that you change the values only after consulting with the product support team.

HeartBeatTimeOut: 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 180000 (in milliseconds).

ReconnectInterval: Use this variable to define the duration of server reconnection retry after it goes to Offline. Default value is 60000 (in milliseconds).

AutoSynchronization: Use this variable to define whether user wants to do auto sync whenever a server comes Online from Offline state. AutoSynchronization values are 'TRUE' and 'FALSE'. Default value is FALSE.

NumberOfCards2Read: Use this variable to define the number of Personnel that must be read in each request during personnel Sync. Default value is 100.

NumberOfImages2Read: 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.

Timeout4ImageBatchSyncRequest: 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).

TimeoutInterval4ImageBatchResponse: 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).

ComponentStatusBatchSize: 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.

StatusQueueCount: 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.

SyncBatchSize: 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 7.

Operation

Administration Functions

Save and Close: Saves the current object and closes the editor.

Save: Saves changes and keeps the editor open, allowing further changes to be made.

Save and New: Saves the current object and opens a new editor to create a new object with default values populated.

Close: Cancels changes and closes the editor without saving.

Hardware Information

Detailed hardware information is available for all configured EntraPass units.

Procedure 5-1 Accessing Hardware Information

Step	Action
1	Select EntraPass Servers from Show All.
2	Right-click the server you wish to view information for and select Edit . This information is also available by right-clicking on a server in the Device List and selecting Edit .

Adding EntraPass Servers

Procedure 5-2 Adding New EntraPass Servers

Step	Action
1	Select EntraPass Server from the Create New Item screen.
2	New Server Editor displays.
3	Enter a name for the server in the Name field.
4	Enter a description for the server in the Description field.
	Note The Enabled check-box is selected by default. To deactivate the server, deselect the check-box.
5	Expand the Details section.
6	Enter the IP Address of the server in the IP Address field.
7	Enter the Port Number (Minimum 1 character, Maximum 5).
8	Enter the UserID, which is the ID of the operator in the EntraPass application.

- 9 Enter the Password, which is the password of the operator in the EntraPass application.
- 10 Enter Event Poll Time.
- 11 Enter Service Protocol information.
- 12 Enter Status Poll Time.
- 13 You can review server status in the Server status section, refer table Table 1 Server Status on page 8.

Table 1: Server Status

Property	Value
Communication Status	Online
	Offline
	Unknown
Synchronization Status	Unknown
	Synchronizing
	Synchronized
	SyncFailed

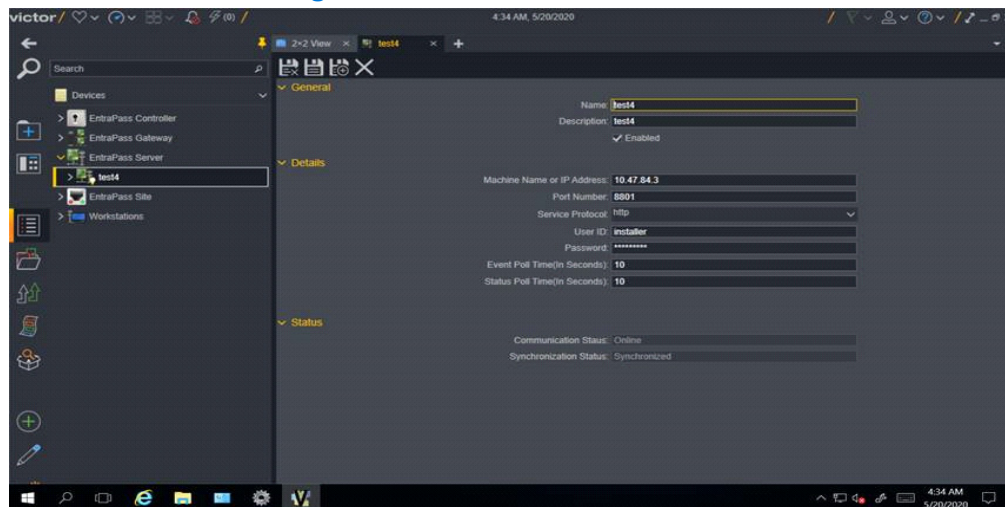
- 1 Click **Save**.

- End -

Editing EntraPass Servers

Procedure 5-3 Edit EntraPass Servers

You can configure server connection details from within victor, using the EntraPass Server Editor.

Figure 5-1 EntraPass Server Editor

Step	Action
------	--------

- 1 Select **EntraPass Server** from **Edit Existing Item** screen.

- 2 Click the **Server** to be edited.
- 3 Select the General expander to edit:
 - **Name** (Mandatory must be unique)
 - **Description** (Optional)
 - **Enabled status** (Default is enabled)
- 4 Select the **Details** expander to edit:
 - **Machine Name or IP Address** (Mandatory) - This is the network address of the Server, by default it is 127.0.0.1. The following validation rules will apply to the Panel's Machine Name or IP address field:
 - The **Machine Name or IP Address** must be unique for each panel within the victor environment otherwise the message returns **Machine Name or IP Address not unique**.
 - **Port Number** (Mandatory) - The Port number of the server Min=1 character, Max=5 characters
 - **Service Protocol** (Mandatory) - The protocol used to communicate with the server

Note

If https is selected, a dialog displays prompting the user to complete the EntraPass smart link configuration to https. For this protocol to function, a valid SSL certificate must be added to the Kantech server.

- **User ID** (Mandatory) - ID of the operator in the EntraPass application
 - **Password** (Mandatory) - Password of the operator in the EntraPass application
 - **Event Poll Time** (Mandatory) - Poll time to request or poll for EntraPass events
 - **Status Poll Time** (Mandatory) - Poll time to request or poll for EntraPass device status
- 5 Click **Save**.

Victor Integration

Roles

EntraPass objects privileges are associated with victor roles, therefore all context menu actions associated with EntraPass objects are added to existing victor roles which can be edited accordingly. For more information on Roles, refer to the victor Configuration and User Guide.


Associations

EntraPass servers support victor's **Object Association**. **Object Association** refers to linking unrelated victor objects with the intent of enabling incident building capability. Device associations are created within the victor editor of the source object (typically right click > edit). Up to 5 device associations can be made per object.

To create Object Associations in victor follow the below procedures:

Procedure 5-4 Create Object Associations

- 1 Navigate to the required source device on the victor Device List.

- 2 Right click the device and select Edit. The device editor opens.
- 3 Expand the Associations section.
- 4 Select icon 
- 5 Use the object selector to locate the object to be associated.
- 6 Click **OK**.
- 7 Repeat as required for up to 5 objects.

- End -

Reports

EntraPass objects are included in the report selection tool and support the victor Find in Journal feature. For more information on Reports and the Find in Journal feature, refer to the *victor Configuration and User Guide*.

Events




Events allow you to detect, monitor and record specific activities on the system.

EntraPass alarm activity can be used to trigger events within victor, these event types are fully integrated with victors Event Management system and respect all role /user permissions.

Event configuration in victor is a 2 step process:

- 1 Event/Action Pairing
- 2 Event Setup

Procedure 5-5 Configuring events

Step	Action
1	Select Event/Action pairing from configuration screen . The editor opens.
2	Double click the Events node. Object selector displays.
3	Use the Object Selector to select events as required.
4	Select  in the event node to assign actions.Repeat as required.
5	Click Save .
6	Select Event Setup from configuration screen. The event configuration window displays.
7	Click the Devices node and use the object selector to select the required device (or drag and drop from the device list).
8	Select  in the node of the device added and use the check-boxes in the drop down list to assign alerts as required.
9	Select Add Alerts . Selected alerts are displayed under the Alerts node.
10	Select  in the Alerts node and use the object selector to assign actions.
11	Click Save .

- End -

For further information on **Events**, refer to the *victor Configuration and User Guide*.

Predefined EntraPass Events

The following predefined EntraPass events are available for doors, site controllers, and servers:

- EntraPass Server Online
- EntraPass Server Offline
- EntraPass Site Online
- EntraPass Site Offline
- EntraPass Controller Online
- EntraPass Controller Offline
- Door Held Alarm
- Door Forced Alarm

Procedure 5-6 Viewing Predefined events


Step	Action
1	Select Event from Show All screen. Editor opens.
2	All configured events including predefined EntraPass events are displayed.
- End -	

EntraPass Actions

EntraPass Actions are available for the following objects:

- Servers
- Doors
- Relays

Procedure 5-7 Configuring EntraPass Action

Step	Action
1	Select EntraPass action from New screen. The editor opens.
2	Enter Name and Description for the EntraPass Action.
3	In the EntraPass Device field, Select  to add device. Object Selector displays.
4	Select desired object and click OK .
5	Repeat as required.
6	Select desired action from the EntraPass Device Action drop down list.

- 7 Click **Save and Close**.

- End -

Procedure 5-8 Editing EntraPass Action



Step	Action
1	Select EntraPass Action from Edit screen.
2	Click the EntraPass Action that you want to edit. The editor opens.
3	Select the General expander to edit Name and Description .
4	Select the Action expander to edit EntraPass Device and EntraPass Device Action .
5	Click Save and Close .

- End -

Maps

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.

Procedure 5-9 Configuring Maps

Step	Action
1	Select Map from the New screen. The editor displays.
2	Enter a Name and Description for the map.
3	Select  to Import a map .
4	Browse to and select the required image.
5	Click Open .
6	Select Import . File imports and displays in map editor.
7	Click Save .
8	The map drawing is now imported and you can now configure victor objects on it.
9	From the map editor, select icon  .
10	Icon selector displays.

Note

The Map editor can be accessed by selecting **Maps** from the **Build** tab, then selecting **Show All**. Right click on the map to be edited and select **Edit**.

- 11 Select the icon which matches the object type to be added.
- 12 Click **OK**.
- 13 Drag and drop to the required position on the map. Use resizing/positioning tools as required and then right-click the icon.
- 14 Click **Drop on map**. The Icon editor displays.
- 15 Click **Select Object**. The object selector displays.
- 16 Select the victor object to be linked to the icon and click **OK**.
- 17 Use the Icon editor to assign or change other attributes as required.
- 18 Click **OK** and then click **Save**.

Note

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

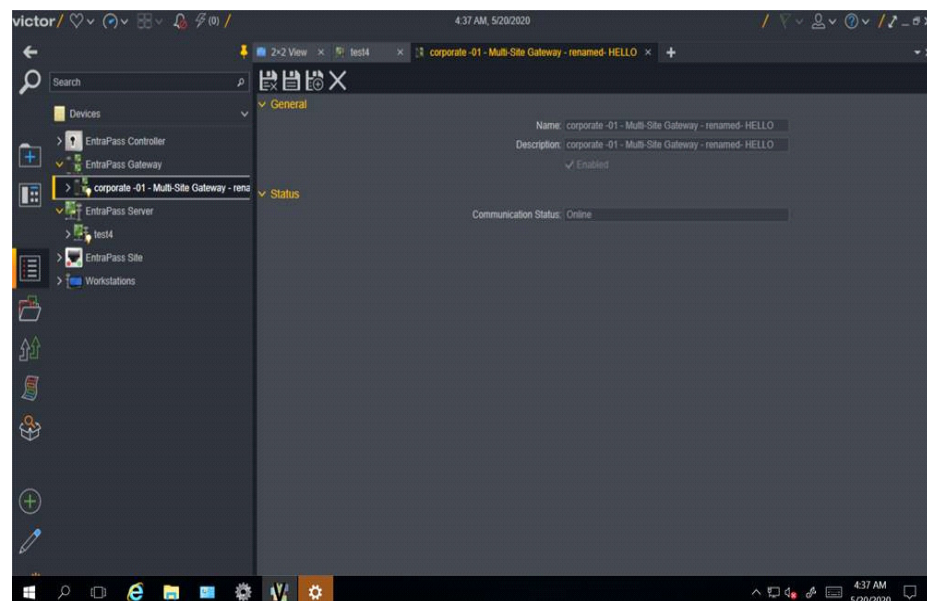
- End -

EntraPass Objects

Procedure 5-10 View EntraPass Gateway

Within the victor environment, **EntraPass Gateway** are view only.

Figure 5-2 EntraPass Gateway editor



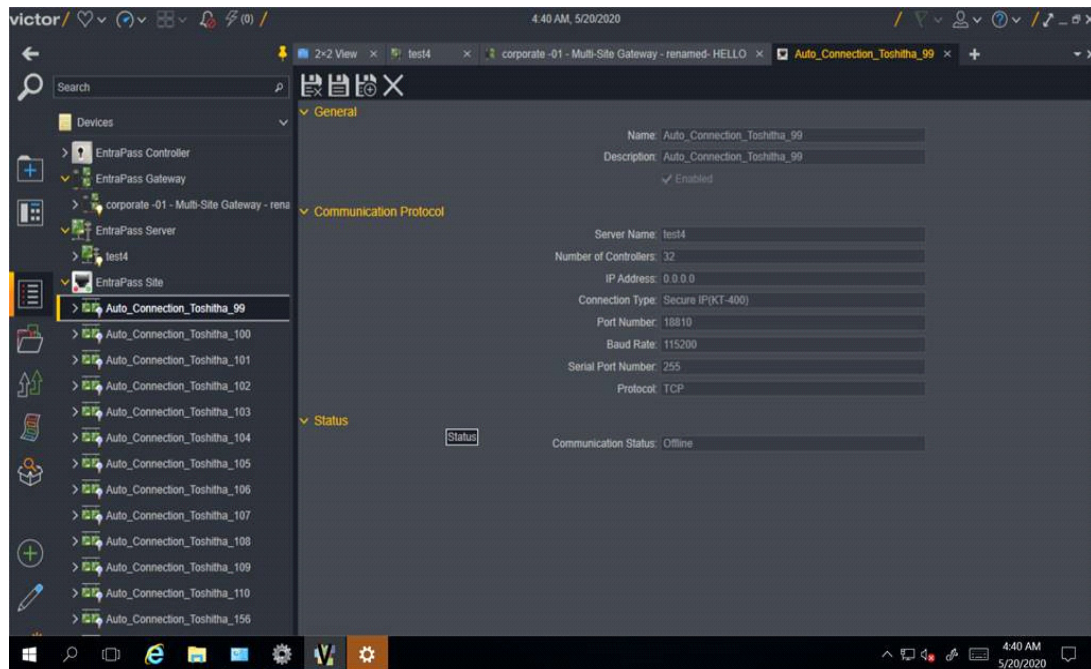
Step	Action
1	Select EntraPass Gateway from the Show All screen.
2	All configured EntraPass Gateway are displayed in an Object List . Use the expanders to view details within each section.
- End -	

Procedure 5-11 View EntraPass Sites

Note

Within the victor environment, **EntraPass Sites** are view only.

Figure 5-3 EntraPass sites editor



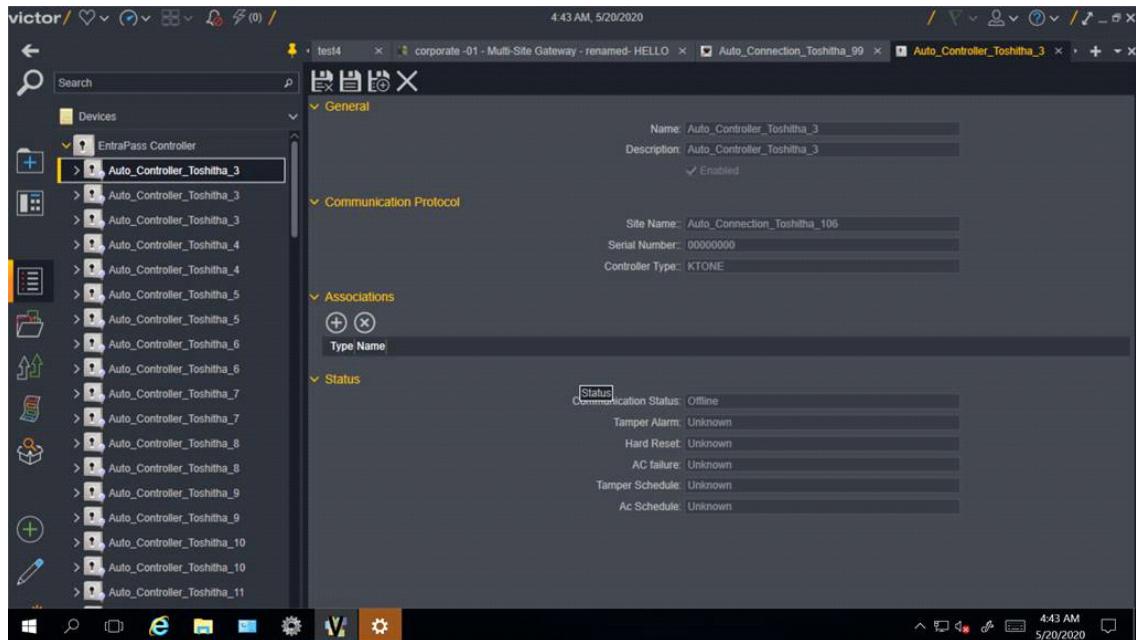
Step	Action
1	Select EntraPass Site from Show All screen.
2	All configured EntraPass sites are displayed in an Object List . Use the expanders to view details within each section.
- End -	

Procedure 5-12 View EntraPass Controllers

Note

Within the victor environment, **EntraPass Controllers** are view only.

Figure 5-4 EntraPass controller editor



Step Action

- 1 Select **EntraPass Controller** from **Show All** screen.
- 2 All configured EntraPass controllers are displayed in an Object List. Use the expanders to view details within each section.

Table 2: Controller Status

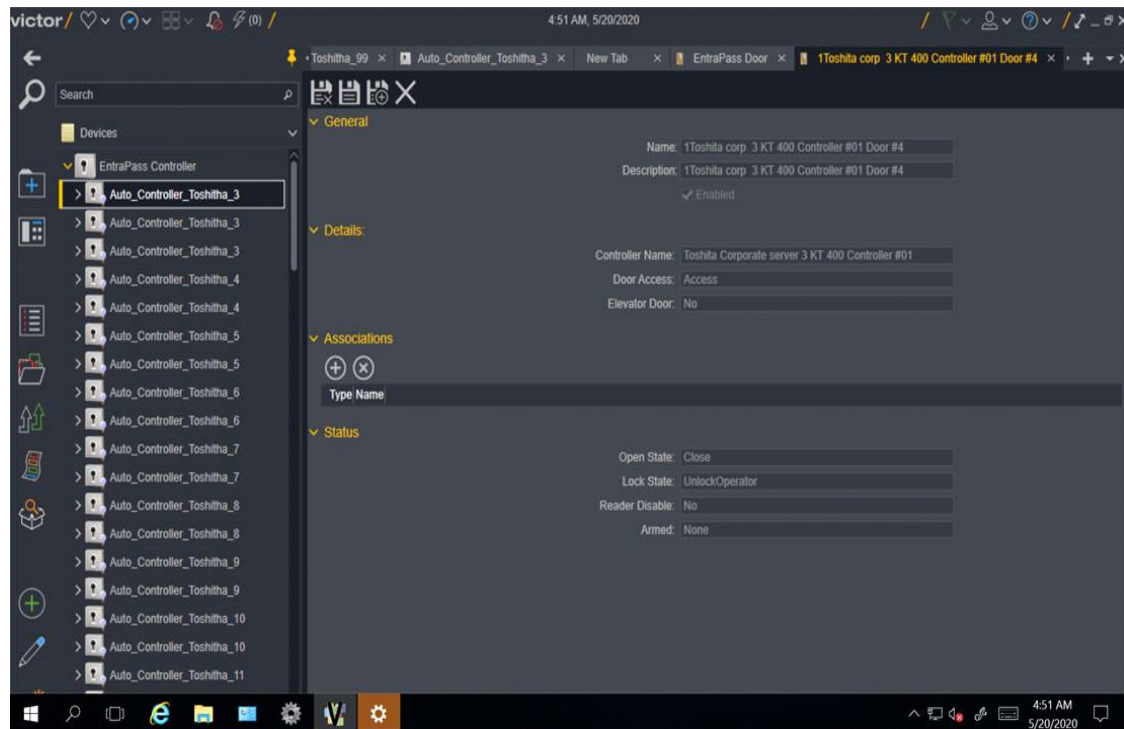
Property	Value
CommunicationStatus	Online
	Offline
HardReset	Yes
	No
TemperAlarm	Yes
	No
AC Failure	Yes
	No
Tamper Schedule	Yes
	No
AC Schedule	Yes
	No

- End -

Procedure 5-13 View EntraPass Doors

Note

Within the victor environment, **EntraPass Doors** are view only.

Figure 5-5 EntraPass door editor

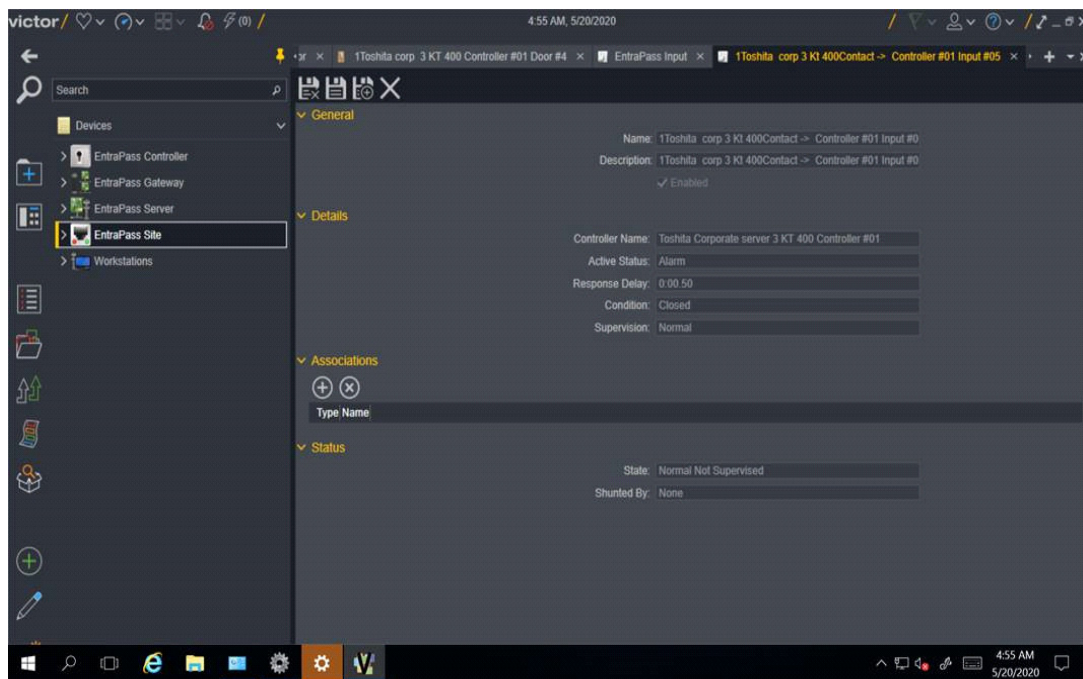
Step	Action
1	Select EntraPass Door from Show All screen.
2	All configured EntraPass Doors are displayed in an Object List . Use the expanders to view details within each section.
- End -	

Procedure 5-14 View EntraPass Inputs

Note

Within the victor environment, **EntraPass Inputs** are view only.

Figure 5-6 EntraPass Input Editor



Step	Action
1	Select EntraPass Input from Show All screen.
2	All configured EntraPass Inputs are displayed in an Object List. Use the expanders to view details within each section.
- End -	

Note

The following **Shunted by** statuses requires the KT-400 controller to be connected with the supported intrusion panels:

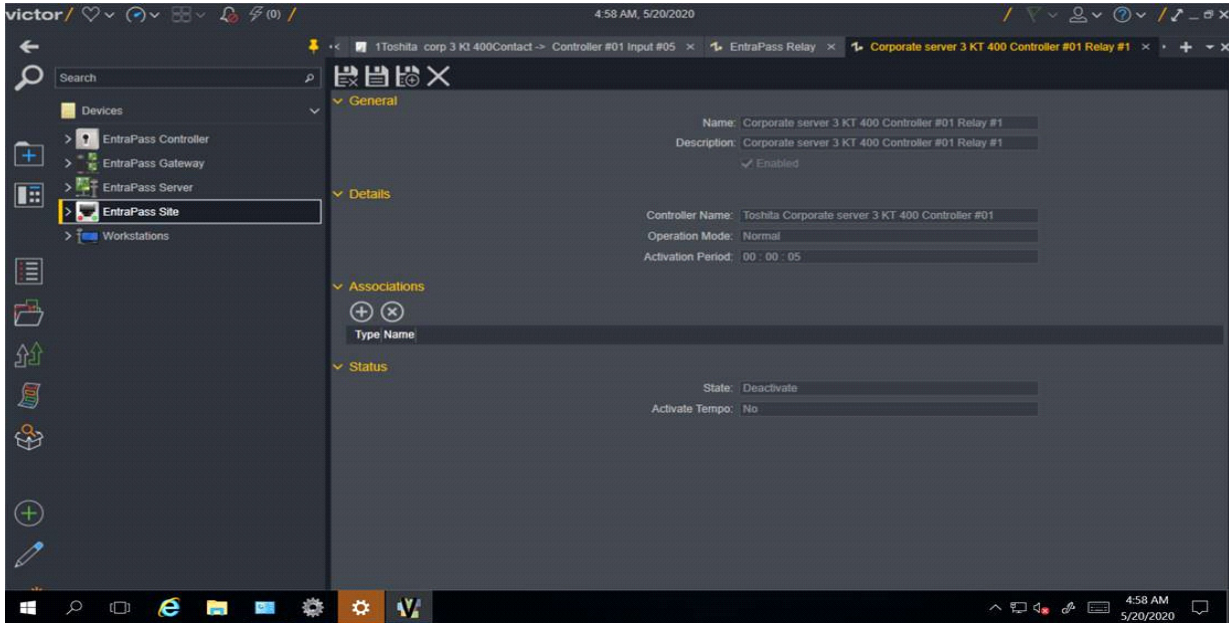
- Door Disarmed
- Shunted on Exit
- Shunted on Entry

Procedure 5-15 View EntraPass Relays

Note

Within the victor environment, **EntraPass Relays** are view only.

Figure 5-7 EntraPass Relay Editor



Step	Action
------	--------

- | | |
|---|---|
| 1 | Select EntraPass Relay from Show All screen. |
| 2 | All configured EntraPass relays are displayed in an Object List. Use the expanders to view details within each section. |

- End -

Procedure 5-16 View Personnel

Note

Within the victor environment, Synchronized Personnel are displayed in the **Personnel** Tab.

Step	Action
------	--------

- | | |
|---|--|
| 1 | Select Personnel from Show All screen. |
|---|--|

- 2 All Synchronized Personnel are displayed.

- End -

Swipe and Show

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

Note

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

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

Procedure 5-17 Viewing Swipe and Show

Step	Action
1	Select Swipe and Show from New tab screen.
2	Choose one of the following options: <ul style="list-style-type: none"> •Monitor all Doors for Admits •Monitor all Doors for Rejects •Monitor all Doors for Admits/Rejects.
3	The details of the Personnel with the image is displayed in the Swipe and Show tab.
- End -	

General Operation

After integration the following functions are available in victor Client:

Manual Actions

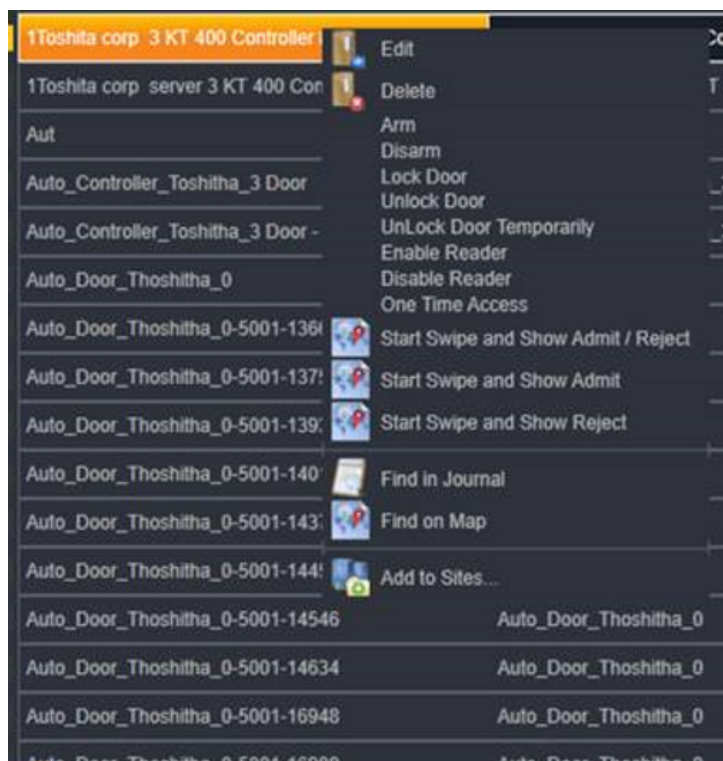
Doors

You can **Lock, Unlock, Temporarily Unlock Doors, Arm, Disarm, Enable Readers, One Time Access** and **Disable Readers** from the **Device List, Maps**, dynamic views and activity viewer.

Note

To perform **Arm** or **Disarm** actions, **Doors** need to be associated with an external intrusion panel connected with a KT-400 controller.

Figure 5-8 Manual actions: Doors



Inputs

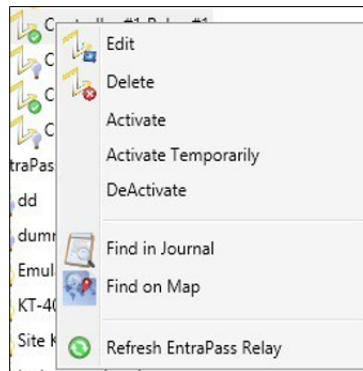
You can perform the following manual actions on an Input from Device List, Maps, dynamic views and activity viewer.

Figure 5-9 Figure 4-8 Manual actions: Inputs



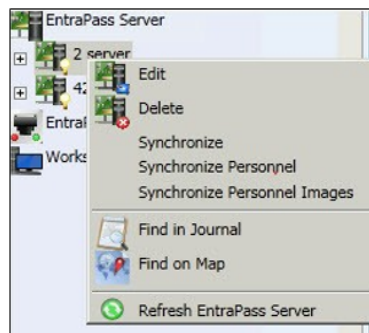
Relays

You can **Activate**, **Deactivate** and **Temporarily Activate Relays** from the **Device List**, **Maps**, **Dynamic Views** and **Activity Viewer**.

Figure 5-10 Figure 4-8 Manual actions: Relays

Servers

You can manually synchronize Server objects, Personnel, and Personnel Images from the Device List, Maps, Dynamic Views and Activity viewer.

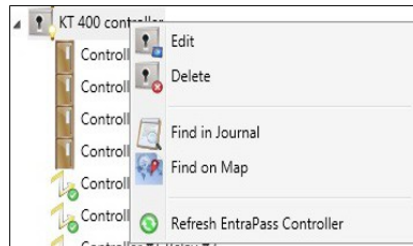
Figure 5-11 Manual Actions: Servers

Context (Right Click) Menu options

This section details context menu options available on EntraPass objects from the Device List, Maps, Dynamic Views and Activity Viewer.

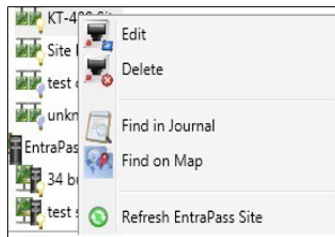
Controllers

Right-clicking Controllers offers the following options:

Figure 5-12 Context Menu: Controllers

Sites

Right-clicking Sites offers the following options:

Figure 5-13 Context Menu: Sites

Troubleshooting

Troubleshooting:

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

Problem:

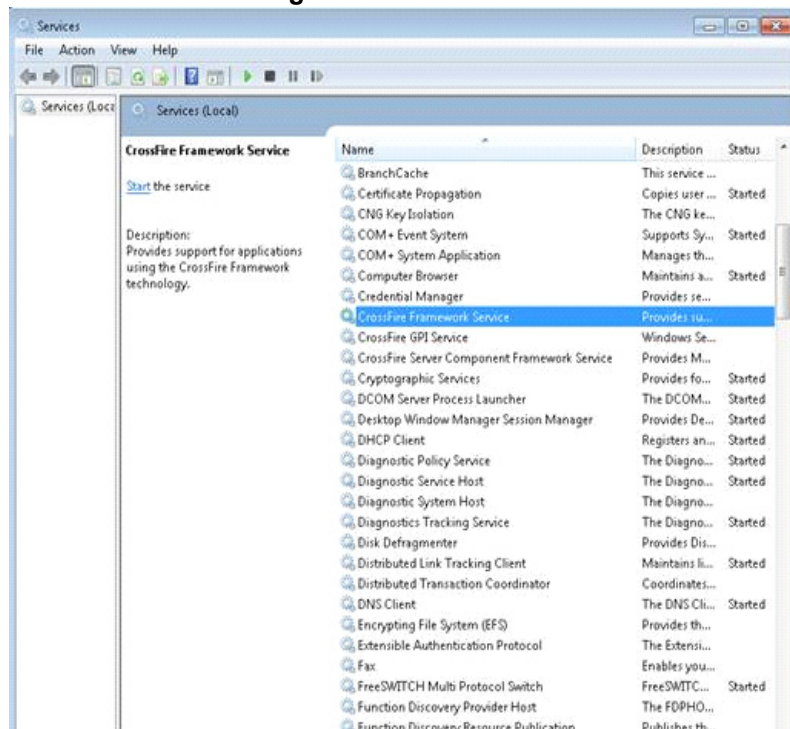
Sometimes the installation may fail if the CrossFire service does not stop on time and throws a time out error.

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 Figure 5-1 CrossFire Services on page 23.
- Wait till the CrossFire service is stopped and then trigger the installation again. This will work fine as the service is stopped already.

Figure 5-1 CrossFire Services



Problem:

EntraPass Server is not communicating with victor.

Solution:

Ensure that you have completed the following steps:

- 1 Validate firewall settings. Add required ports in Inbound and Outbound port list of firewall.
- 2 Ensure IP Address or System Name are correct.
- 3 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.
- 4 Ensure that the required services are running on EntraPass server.

Problem:

EntraPass Server is failed to synchronize.

Solution:

Ensure that you have completed the following steps:

- 1 Try changing the config file entry **SyncBatchSize** to a lower value.
- 2 Restart the driver.

Problem:

The controllers are not coming online, even when they are online in Kantech Server.

Solution:

Ensure that you have completed the following steps:

- 1 Try changing the Config file entry **ComponentStatusBatchSize** and **StatusQueueCount** to a lower value.
- 2 Restart the driver.
- 3 Try increasing Status Poll Time in Entrapass server configuration window to a higher value from default value.

Note

These changes depend on system resources and might impact the performance.

Appendix A

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.

Hardware Setup

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

Step	Action
1	<p>Connect the IT-100 to the alarm panel:</p> <ol style="list-style-type: none"> Power down the alarm panel. 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. 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.
<p>Note</p> <p>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.</p>	
- End -	

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/>.

Appendix B

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

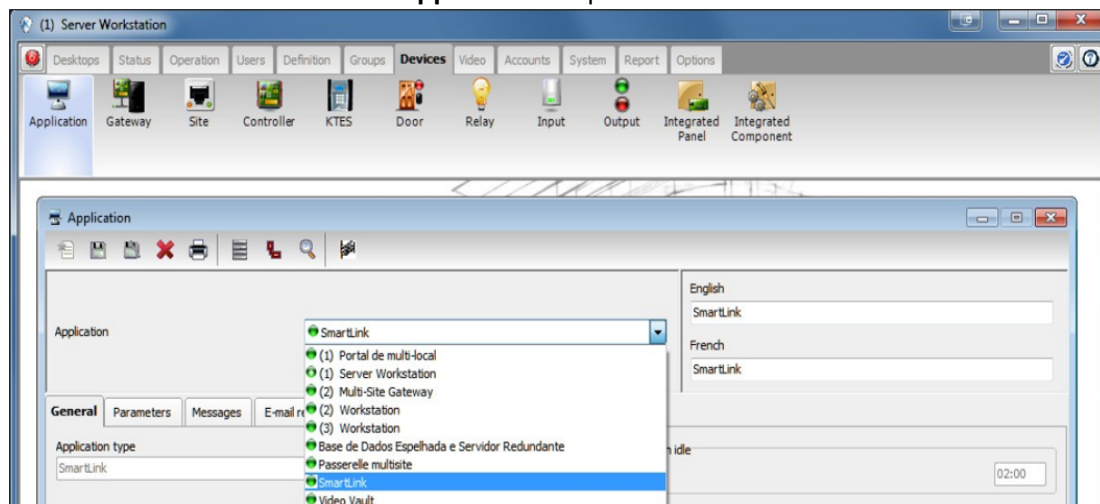
- EntraPass Server
- victor Unified Client
- Kantech SmartService and SmartLink Running

Note

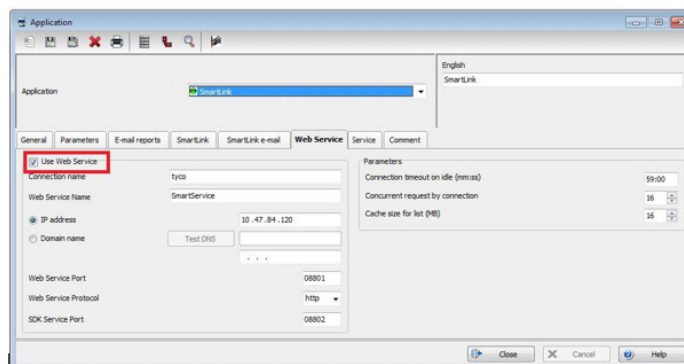
SmartLink and WebStation must have been previously registered in EntraPass for the SmartLink Webstation tab to be available. Refer to the EntraPass Reference manual for more information.

Procedure 7-1 Configuring EntraPass for remote victor Client operation

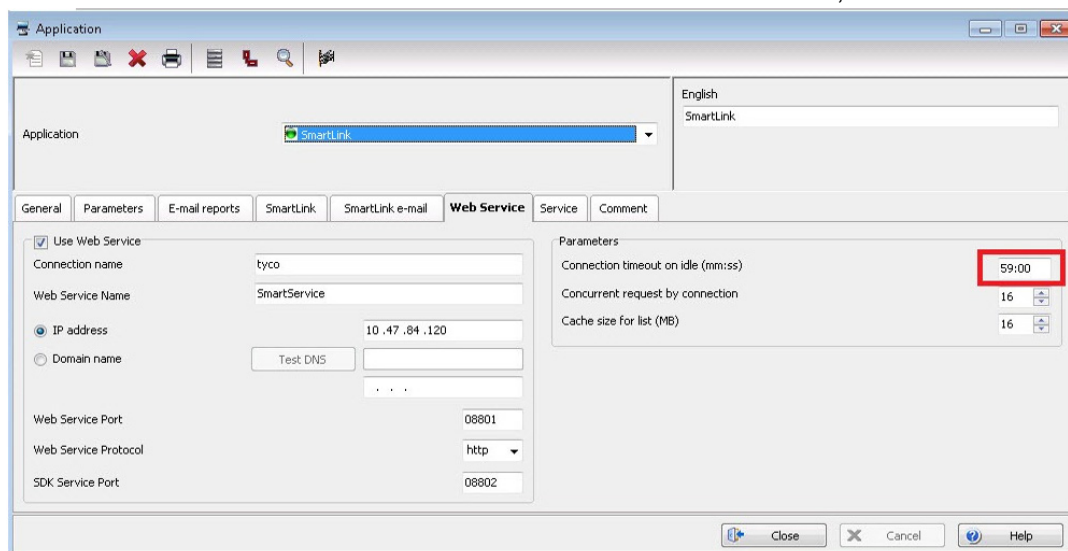
Step	Action
1	Login to the EntraPass Server Workstation.
2	Select Devices/Application .
3	Select SmartLink from the Application drop down list.



- 4 Click the **Web Service** tab.



- 5 Ensure that the **Use Web Service** field is checked.
- 6 Ensure that the Connection Time Out on Idle is set to the maximum, which is 59 minutes.



- End -

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 7-2 Getting a Certificate's Thumb-print

Step	Action
1	<p>View certificates in the MMC snap-in:</p> <ol style="list-style-type: none"> Open a Command prompt window Type mmc and press Enter. You must have Administrator privileges to view certificates. On the File menu, click Add/Remove Snap In. Click Add. In the Add Standalone Snap-in dialog box, select Certificates. Click Add. In the Certificates snap-in dialog box, select Computer account and click Next. 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. In the Select Computer dialog box, click Finish. In the Add Standalone Snap-in dialog box, click Close. In the Add/Remove Snap-in dialog box, click OK. In the Console Root window, click Certificates (Local Computer) to view the certificate stores for the computer. (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. (Optional.) On the File menu, click Save or Save As. Save the console file for later reuse.
2	<p>Retrieving a certificate's thumb-print</p> <ol style="list-style-type: none"> Open the Microsoft Management Console (MMC) snap-in for certificates. In the Console Root window's left pane, click Certificates (Local Computer). Click the Personal folder to expand it. Click the Certificates folder to expand it. 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. In the Certificate dialog box, click the Details tab. Scroll through the list of fields and click Thumb-print. Copy the thumbprint of the certificate into a text editor, such as Notepad. 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}

- End -

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=enable