

IndigoVision

**PAC SecureNet
Integration Module**

Administrator's Guide



IndigoVision

THIS MANUAL WAS PUBLISHED ON 8/13/2018.

DOCUMENT ID: IU-IM-MAN031-4

Legal Considerations

LAWS THAT CAN VARY FROM COUNTRY TO COUNTRY MAY PROHIBIT CAMERA SURVEILLANCE. PLEASE ENSURE THAT THE RELEVANT LAWS ARE FULLY UNDERSTOOD FOR THE PARTICULAR COUNTRY OR REGION IN WHICH YOU WILL BE OPERATING THIS EQUIPMENT. INDIGOVISION LTD. ACCEPTS NO LIABILITY FOR IMPROPER OR ILLEGAL USE OF THIS PRODUCT.

Copyright

COPYRIGHT © INDIGOVISION LIMITED. ALL RIGHTS RESERVED.

THIS MANUAL IS PROTECTED BY NATIONAL AND INTERNATIONAL COPYRIGHT AND OTHER LAWS. UNAUTHORIZED STORAGE, REPRODUCTION, TRANSMISSION AND/OR DISTRIBUTION OF THIS MANUAL, OR ANY PART OF IT, MAY RESULT IN CIVIL AND/OR CRIMINAL PROCEEDINGS.

INDIGOVISION IS A TRADEMARK OF INDIGOVISION LIMITED AND IS REGISTERED IN CERTAIN COUNTRIES. INDIGOUltra, INDIGOPRO, INDIGOLITE AND CYBERVIGILANT ARE REGISTERED TRADEMARKS OF INDIGOVISION LIMITED. CAMERA GATEWAY AND INTEGRA ARE UNREGISTERED TRADEMARKS OF INDIGOVISION LIMITED. ALL OTHER PRODUCT NAMES REFERRED TO IN THIS MANUAL ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.

SAVE AS OTHERWISE AGREED WITH INDIGOVISION LIMITED AND/OR INDIGOVISION, INC., THIS MANUAL IS PROVIDED WITHOUT EXPRESS REPRESENTATION AND/OR WARRANTY OF ANY KIND. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS, INDIGOVISION LIMITED AND INDIGOVISION, INC. DISCLAIM ALL IMPLIED REPRESENTATIONS, WARRANTIES, CONDITIONS AND/OR OBLIGATIONS OF EVERY KIND IN RESPECT OF THIS MANUAL. ACCORDINGLY, SAVE AS OTHERWISE AGREED WITH INDIGOVISION LIMITED AND/OR INDIGOVISION, INC., THIS MANUAL IS PROVIDED ON AN "AS IS", "WITH ALL FAULTS" AND "AS AVAILABLE" BASIS. PLEASE CONTACT INDIGOVISION LIMITED (EITHER BY POST OR BY E-MAIL AT TECHNICAL.SUPPORT@INDIGOVISION.COM) WITH ANY SUGGESTED CORRECTIONS AND/OR IMPROVEMENTS TO THIS MANUAL.

SAVE AS OTHERWISE AGREED WITH INDIGOVISION LIMITED AND/OR INDIGOVISION, INC., THE LIABILITY OF INDIGOVISION LIMITED AND INDIGOVISION, INC. FOR ANY LOSS (OTHER THAN DEATH OR PERSONAL INJURY) ARISING AS A RESULT OF ANY NEGLIGENT ACT OR OMISSION BY INDIGOVISION LIMITED AND/OR INDIGOVISION, INC. IN CONNECTION WITH THIS MANUAL AND/OR AS A RESULT OF ANY USE OF OR RELIANCE ON THIS MANUAL IS EXCLUDED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS.

Contact address



IndigoVision Limited
Charles Darwin House,
The Edinburgh Technopole,
Edinburgh,
EH26 0PY

TABLE OF CONTENTS

	Legal Considerations	2
	Copyright	2
	Contact address	2
1	About this guide	5
	Safety notices	5
	References	5
2	Overview	6
	Compatibility	6
	System requirements	6
	PAC SecureNet	6
	Licensing	6
3	Installation	8
	Upgrading from 1.0	9
	System Configuration File	9
	Tolv Events	9
	Multiple Alarm Servers	10
	Upgrading from 2.0	10
	System Configuration File	10
	Fromlv Relays Configuration File	10
	License the integration module	10
4	Configuration	11
	System configuration file (System.conf)	11
	Alarms to IV configuration file (Tolv.conf)	11
	Relays actions from IV configuration file (FromlvRelays.conf)	11
	To IV Alarm Servers configuration file (TolvAlarmServers.conf)	12
	IndigoVision Control Center configuration	12
	Create a new external system	12
	Create a new zone and external detector for Tolv events	12
	Create external detectors for all types of events	12
	Create external relays	12
	Provide Authorization Key File	12
5	System Configuration Files	14
	System configuration file (System.conf)	14
	Alarms to IndigoVision configuration file (Tolv.conf)	16
	To IV Alarm Servers configuration file (TolvAlarmServers.conf)	16
	Relay actions from IndigoVision configuration file (FromlvRelays.conf)	17

	Logging configuration	19
6	Troubleshooting	21
	Service does not start	21
	Alarms not appearing in Control Center	21
	PAC SecureNet Integration Module is slow to start	22
	Unable to connect to the PAC SecureNet server	23
	Unable to control doors, areas or outputs in a PAC SecureNet installation using external relays in Control Center	23
	Unable to acknowledge a PAC SecureNet active alarm by acknowledging or clearing a zone	24
	License issues	25
	Check that the Sentinel HASP Dongle is Active	25

1

ABOUT THIS GUIDE

This guide is provided for system administrators integrating the PAC SecureNet system with the IndigoVision Control Center suite.

Safety notices

This guide uses the following formats for safety notices:



Indicates a hazardous situation which, if not avoided, could result in death or serious injury.



Indicates a hazardous situation which, if not avoided, could result in moderate injury, damage the product, or lead to loss of data.

Notice

Indicates a hazardous situation which, if not avoided, may seriously impair operations.



Additional information relating to the current section.

References

The following documents are referenced in this document. The paths are to the default locations where the documents can be found.

1. Control Center Help
Start >IndigoVision >Control Center >Control Center Help
(located on the Control Center Workstation)
2. IndigoVision Control Center Installation Guide
Available on the Control Center CD
3. Integration Modules
<http://www.indigovision.com/products/integration>
4. PAC SecureNet Integration Module User Guide (HF100 Ver 4.6)

2 OVERVIEW

The PAC SecureNet Integration Module allows events from a PAC SecureNet system to be integrated into IndigoVision Control Center suite. It also allows Control Center operators to acknowledge active alarms in PAC and remotely action PAC SecureNet doors, areas and outputs from within Control Center. This document explains how to install and configure the PAC SecureNet Integration Module.

Compatibility

Please ensure you have properly installed, configured, and licensed the PAC SecureNet system.

System requirements

The PAC SecureNet Integration Module can be installed on the following Windows® operating systems with the latest service packs applied:

- Windows® Server 2016
- Windows® Server 2012 R2
- Windows® Server 2012
- Windows® Server 2008 R2
- Windows® 10 (64-bit)
- Windows® 8.1 (64-bit)
- Windows® 7 (64-bit)

If a firewall is enabled on your system, ensure that the Integration Module executable **IndigoVision.IntegrationCore.exe** is added to the list of exceptions.

PAC SecureNet

The PAC SecureNet Integration Module is compatible and has been tested with PAC SecureNet Server 4.6.333.

A PAC OEM Interface License is required to enable the interface used by the Integration Module.

You can install the PAC SecureNet Integration Module on either the same machine as the PAC SecureNet server, or on a different machine.

Licensing

The PAC SecureNet Integration Module is a licensed product, which can be installed on a physical or virtual machine.

Install the license key on the same machine as the PAC SecureNet Integration Module using License Manager.

If you are using a licensed USB dongle from an existing installation, you do not need a software license key for the PAC SecureNet Integration Module.

Notice *The PAC SecureNet Integration Module must not be run on the same server as any other licensed IndigoVision software.*

3 INSTALLATION

If you have an IndigoVision PAC SecureNet Integration Module USB license dongle, ensure it is inserted into the machine that the software is to be installed on before starting the installation.

Before you install the Integration Module, you must first configure the PAC SecureNet server:

1. Locate the PAC SecureNet installation folder. By default this is **C:\Program Files (x86)\PAC SecureNet**.
2. Navigate to **Bin\bin.NET** and open **ApplicationInterfaceHost.exe.config**.
3. Locate all the transport elements (**<transport .../>**) in the bindings section (**<bindings>**).
4. If the **sslProtocols="Tls11"** attribute does not exist on any of the transport elements, add it.

The end result should look similar to the following:

```
<transport clientCredentialType="None" sslProtocols="Tls11" />.
```

5. Save your changes.
6. Restart the PAC SecureNet service using the PAC Service Manager. This will enable secure and reliable communication between the integration module and the PAC system.

To install the Integration Module:

1. Insert the IndigoVision Integrations DVD, or download the module from the IndigoVision website.
 - ▶ For more information, see "References" on page 5If you are using the Integrations DVD, navigate to **PAC SecureNet** and select **Install PAC SecureNet**.
2. Run the **setup.exe** file and follow the on screen instructions.

The Integration Module is installed to: **C:\Program Files (x86)\IndigoVision\Integration\PAC SecureNet** by default.
3. If the Microsoft .NET 4.5.2 Framework or later is not installed then you are prompted to install it.
4. The PAC SecureNet Integration Module automatically installs a PAC OEM interface certificate, provided by Stanley Security Products. If Windows cannot validate the PAC OEM Interface certificate that is installed automatically, you must click **Yes** to confirm before you can proceed. Alternatively, contact Stanley Security Products to obtain a certificate and manually install it for the Local System user.

Once the installation is complete, configure the Integration Module:

1. Add the PAC SecureNet Integration Module as an OEM System within PAC SecureNet.

You should have stored the Authorization Key File in the PAC SecureNet Integration Module Authorization Key folder.

- ▶ For more information, see "Provide Authorization Key File" on page 12

2. Request and install a software license for the PAC SecureNet Integration Module using the License Manager tool.
 - ▶ For more information, see *"License the integration module"* on page 10
3. Configure the PAC SecureNet Integration Module.
 - ▶ For more information, see *"Configuration"* on page 11
4. Start the IndigoVision PAC SecureNet Integration Module service using the Windows Services.

Upgrading from 1.0

The following configuration files must be considered when upgrading the PAC SecureNet Integration Module from 1.0 to 2.1.

System Configuration File

When upgrading from version 1.0, the existing System Configuration File is renamed to **System.conf.legacy** and you must configure the new **System.conf**.

- In the section [AlarmServer], the IP parameter is now optional and is for System Events.
- In the section [SecureNetServer], the existing parameters are no longer used. SecureNetHost and SecureNetPort are optional parameters for connecting to a remote SecureNet server.
- In the section [System], if the machine has multiple IP addresses, configure the IntegrationModuleIP parameter with the IP address of the Integration Module machine.
- In the section [SystemEvents], the fields BMOOffline and BMOOnline have been renamed to IMOffline and IMOnline respectively.
- The logging level is now configured through a separate file.
 - ▶ For more information, see *"Logging configuration"* on page 19.
- A new [Relays] section needs to be manually added to the **System.conf** file. Specify EnableFromIvRelays=true to enable FromIv Relay actions.
- A new [Events] section needs to be manually added to the **System.conf** file. Specify EnableAlarmActionsFromIv=true to enable acknowledgement of alarms from Control Center.

In addition, the existing **Tolv.conf** file is moved in the Tolv folder. You can use the Windows shortcut to edit it.

- ▶ For more information, see *"System configuration file (System.conf)"* on page 11

A new FromIv Relays configuration file is also available. If FromIv Relays were enabled in the System Configuration File then this file must be configured.

- ▶ For more information, see *"Relay actions from IndigoVision configuration file (FromIvRelays.conf)"* on page 17

Tolv Events

Existing **Tolv** and **TolvAlarmServers** files are compatible, and they are not modified during the upgrade process.

Multiple Alarm Servers

Starting from PAC SecureNet Integration Module version 2.0, multiple Alarm Servers are supported. This allows the Integration Module to support more events (up to 10000 for each Alarm Server) or to forward the same PAC SecureNet alarm to different Alarm Servers.

The mapping between Tolv events and Alarm Servers is in a new file called **TolvAlarmServers** that can be configured using the Windows shortcut, under **IndigoVision PAC SecureNet Integration**.

- ▶ For more information, see "To IV Alarm Servers configuration file (TolvAlarmServers.conf)" on page 12

Upgrading from 2.0

The following configuration files must be considered when upgrading the PAC SecureNet Integration Module from 2.0 to 2.1.

System Configuration File

- A new [Relays] section needs to be manually added to the **System.conf** file. Specify `EnableFromIvRelays=true` to enable FromIv Relay actions.
- A new [Events] section needs to be manually added to the **System.conf** file. Specify `EnableAlarmActionsFromIv=true` to enable acknowledgement of alarms from Control Center.

FromIv Relays Configuration File

A new **FromIv Relays** configuration file is available. If FromIv Relays were enabled in the System configuration file then this file must be configured.

- ▶ For more information, see "*Relay actions from IndigoVision configuration file (FromIvRelays.conf)*" on page 17

License the integration module

To run the IndigoVision PAC SecureNet Integration Module, you must have a valid license. This can be a hardware license or a software license which allows the PAC SecureNet Integration Module to run on a specific machine.

You can manage the license using the License Manager tool, which is installed as part of the PAC SecureNet Integration Module standard installation.

1. Create a Client to Vendor file (c2v) that contains a fingerprint of the machine. This is then sent to IndigoVision Sales Orders.
2. Apply a Vendor to Client file (v2c) provided by IndigoVision.

You can transfer a license from one machine to another using the License Manager tool.

4 CONFIGURATION

To integrate PAC SecureNet with IndigoVision Control Center, configure the following:

- System configuration file
 - ▶ For more information, see "*System configuration file (System.conf)*" on page 11
- Alarms to IV configuration file
 - ▶ For more information, see "*Alarms to IV configuration file (Tolv.conf)*" on page 11
- To IV Alarm Server configuration file
 - ▶ For more information, see "*To IV Alarm Servers configuration file (TolvAlarmServers.conf)*" on page 12
- IndigoVision relay actions of interest.
 - ▶ For more information, see "*Relay actions from IndigoVision configuration file (FromIvRelays.conf)*" on page 17

System configuration file (System.conf)

This file contains all the system configuration parameters.

- ▶ For more information, see "*System configuration file (System.conf)*" on page 14

Alarms to IV configuration file (Tolv.conf)

This file contains the mapping between the PAC SecureNet event and the IndigoVision external system input. It contains the data that will map the event received from the PAC SecureNet system to the IndigoVision system.

- ▶ For more information, see "*Alarms to IndigoVision configuration file (Tolv.conf)*" on page 16

Relays actions from IV configuration file (FromIvRelays.conf)

This file contains a list of IndigoVision external relay output numbers. Each number is associated with the corresponding action to perform on the PAC SecureNet system.

- ▶ For more information, see "*Relay actions from IndigoVision configuration file (FromIvRelays.conf)*" on page 17

To IV Alarm Servers configuration file (TolvAlarmServers.conf)

This file contains a list of Alarm Server IP addresses. Each Alarm Server has a mapping to an Alarms to IV configuration file. This can be the default Tolv.conf configuration file mentioned above.

- ▶ For more information and an example file, see *"To IV Alarm Servers configuration file (TolvAlarmServers.conf)"* on page 16

IndigoVision Control Center configuration

If the IMOnline, IMOffline, 3rdPartyOffline or 3rdPartyOnline external system inputs are defined in the system configuration file and are of interest, then they must be configured in Control Center.

Create a new external system

The IP address entered is the IP address of the host running the Integration Module. Refer to the Control Center online help about creating a new external system.

Create a new zone and external detector for Tolv events

Add a new zone for each unique alarm that must be reported in Control Center.

Within the zone, create a new external detector for the external system above with the external event ID.

It is recommended that the zone name description configured in Control Center closely matches the event of interest. This will help to ensure there is no confusion in correlating events.

Create external detectors for all types of events

After the Tolv configuration file has been edited with all the supported events, configure an IndigoVision Alarm Server using the IndigoVision Import Alarm Sources tool.

The Import Alarm Sources tool can be found in the IndigoVision Integrations DVD.

Every time an event is added to the Tolv configuration file, run the tool again to update the IndigoVision NVR-AS.

Create external relays

Add a new external relay in Control Center for each relay action configured in the *FromIvRelays.conf* file.

- ▶ For more information about creating external relays, refer to the Control Center help.

Provide Authorization Key File

The PAC SecureNet Integration Module connects to the PAC SecureNet system using an Authorization Key File. You generate this file by adding the Integration Module as an OEM

System within PAC SecureNet. Store the file in the **Authorization** folder for the Integration Module.

To generate and store the Authorization Key File:

1. Within PAC SecureNet, navigate **Tools > Manage OEM Interfaces**.
2. Click **Add**.
3. Enter a suitable **System Name** such as `IndigoVision` and ensure **Read Write** is selected.
4. Save the file as ***indigovision.oemkey***.
5. On the machine where the IndigoVision PAC SecureNet Integration Module is installed, navigate **Start > IndigoVision PAC SecureNet Integration Module > Authorization Key folder for PAC SecureNet Integration**
6. Copy the ***indigovision.oemkey*** Authorization Key File to this folder.

5 SYSTEM CONFIGURATION FILES

This section contains examples of the configuration files required by the PAC SecureNet Integration Module.

System configuration file (System.conf)

This file lists the configurable system parameters that are independent of alarms and events.

The usage of the parameters listed in the sample configuration file below is explained in their comments:

Figure 1: Example of a System Configuration file

```
[AlarmServer]
#
# The IP address of the primary Alarm Server (NVR-AS) must be specified if any
# SystemEvents are defined
#
# IP=0.0.0.0
[System]
#
# IntegrationModuleIP is the IP of this machine that should be used to send
# events. It should match the External System which is configured in Control
# Center.
# Note: This must be specified for machines with multiple IP addresses. It may
# be omitted for machines with just a single IP address.
#
# IntegrationModuleIP=0.0.0.0
[SecureNetServer]
#
# The host name or IP address of the machine running PAC SecureNet.
# If no value is provided, the local host name will be used.
#
# SecureNetHost=0.0.0.0
#
# The remote port number to connect to PAC SecureNet if an alternate port has
# been configured on the PAC SecureNet server.
# If no value is provided, the default port number '5150' will be used.
#
# SecureNetPort=5150
[Events]
#
# OPTIONAL: Whether to enable FromIv alarm actions to acknowledge active alarms
# in the PAC SecureNet system.
# Default is "false" which means that FromIv alarm actions are disabled.
# To enable FromIv alarm actions set EnableAlarmActionsFromIv to "true".
```

```
#
# EnableAlarmActionsFromIv=true
[Relays]
#
# Relay actions within Control Center can be used to control the PAC SecureNet
# system.
#
# OPTIONAL: Whether to enable FromIv relay actions.
# Default is "false" which means that FromIv relay actions are disabled.
# To enable FromIv relays, set EnableFromIvRelays to "true" and configure
# relays in the FromIvRelays.conf file.
#
# IMPORTANT: If relay actions are enabled and the IndigoVision NVR-AS is
# installed on this machine then the IntegrationModuleIP must be configured
# to use a different IP address to the NVR-AS.
#
# EnableFromIvRelays=true
[SystemEvents]
#
# SystemEvents are events that may be sent to Control Center to report the
# status of, or problems with, the Integration Module.
#
# The number assigned to a system event is a user-defined event number that
# corresponds to an External Detector input number in the Alarm Server.
#
#
# If IMOffline is defined, an event with this number will be sent to the
# Alarm Server whenever the Integration Module is about to go offline.
# Reasons for going offline include a manual service stop request, the
# host PC shutting down, or the USB dongle license or software license is
# removed or no longer valid.
#
# IMOffline=1
#
# If IMOnline is defined, an event with this number will be sent to the
# Alarm Server whenever the Integration Module has successfully started up.
#
# IMOnline=2
#
# If the 3rdPartyOffline property is defined, an event with this
# number will be sent to the NVR/Alarm Server whenever PAC SecureNet system
# is disconnected.
#
# 3rdPartyOffline=3
#
# If the 3rdPartyOnline property is defined, an event with this
# number will be sent to the NVR/Alarm Server whenever PAC SecureNet system
# is connected.
#
# 3rdPartyOnline=4
```

Alarms to IndigoVision configuration file (Tolv.conf)

The installation provides one default alarm to IndigoVision configuration file located in the Tolv folder, by default. The file is called **Tolv.conf**.

There is one mapping entry per line in the mapping file. Each entry is a comma-separated pair.

Figure 2: Example of an Alarms to IndigoVision Configuration file

```
# This file contains the ToIv mapping of PAC SecureNet alarms to
# IndigoVision external event input numbers.
#
# InputNumber, OrganisationUnit:Area:AlarmPoint:AlarmType, Optional Description
#
# Each entry consists of three comma separated elements:
#
# 1. The first element of each entry is the positive integer
# corresponding to the External Event input in the Alarm Server.
#
# 2. The second element is a string equal to the PAC SecureNet event
# or alarm name.
#
# SecureNet event or alarm name contains four parts.
# The first three parts are the names of the Organization Unit,
# Area and AlarmPoint where an alarm is raised in PAC SecureNet.
# The last part is alarm condition or alarm type.
#
# 3. An optional third field, separated by another comma can be added with
# a description of the event mapping.
#
# Example:
#
# 10, SecureNet:Sale:Sale Side Window:Door forced
# 11, SecureNet:Sale:Sale Door:Door forced
# Example of an event with the optional description:
# 12, PAC:Engineer:Engineer Side Window:Door forced, Door forced Engineer Mode
# The EventName cannot contain the characters ':', '\', '{', '}' or ','.
# The following octal escape codes can be used to represent these characters.
# Character ':': => \072
# Character '\': => \134
# Character '{': => \173
# Character '}': => \175
# Character ',': => \054
# Example using octal escape codes for the EventName "PAC:Second
# floor,meeting:reserved:Door:Door forced":
# 13, PAC:Second floor\054meeting\072reserved:Door:Door forced
```

To IV Alarm Servers configuration file (TolvAlarmServers.conf)

This file contains a list of IndigoVision Alarm Server IP addresses that receive PAC SecureNet events. Each Alarm Server IP address is associated with an Alarms To

IndigoVision configuration file.

Figure 3: Example of a To IV Alarm Servers Configuration file

```
#
# List of each Alarm Server (NVR-AS) and its ToIv file (without .conf extension)
#
# Each entry consists of up to three comma separated fields
#
# The first field is the IP address of the Alarm Server (mandatory).
#
# The second field is the Alarms To IV configuration file excluding file
# extension of ".conf" (mandatory). All Alarms To IV configuration files
# are located in the "ToIv" folder.
# For example an entry of "ToIv" indicates that the
# Alarms To IV configuration file is .\ToIv\ToIv.conf
#
# The optional third field can be used to provide a description.
#
# Note that it is possible to set up all Alarm Servers to use the one default
# Alarms To Iv configuration file by entering "ToIv" as the second field
# for all entries.
# IP address, ToIv file, Description (optional)
# Example using all three fields:
#
# 0.0.0.0, ToIv, Default ToIv\ToIv.conf
# Example using two fields:
# 0.0.0.0, ToIv
```

All entries should include a valid IP address. Anything written after # is treated as a comment.

Relay actions from IndigoVision configuration file (FromIvRelays.conf)

The installation provides a default Relay actions from IndigoVision configuration (FromIvRelays.conf).

There is one mapping entry per line in the file. Each entry is a comma-separated pair.

Figure 4: Example of a From IV Relays configuration file

```
# This file maps IndigoVision external relay outputs to actions within the
# PAC SecureNet system.
# The following formats are used to define the relay outputs:
#
# OutputNumber, Target:OrganizationUnit:TargetName
# OutputNumber, Target:OrganizationUnit:TargetName:Action
# OutputNumber, Target:OrganizationUnit:TargetName:Action:Duration
#
# The first element of each entry is a positive number corresponding to an
# external relay output in the IndigoVision Control Center system.
# The second element contains information about the action to perform in the
# PAC SecureNet system, in response to the relay action in Control Center system:
# - a target to identify the action's target. 'DOOR' if the action's target is a
# door,
# 'AREA' if the action's target is an area, 'OUTPUT' if the action's target is an
# output
```

```
# - the name of the organization unit the action's target belongs to in the
# PAC SecureNet system.
# - the name of the action's target in the PAC SecureNet system.
# - the action to perform on the target. This is only valid if the target is
# either a door or an area
# - optionally, the duration (in minutes) of the action to perform on the target.
# This is only valid for the Open action for both doors and areas.
# Door Actions
#
# OutputNumber, DOOR:OrganizationUnit:DoorName:Action
# OutputNumber, DOOR:OrganizationUnit:DoorName:Open:Duration
#
# The PAC SecureNet Integration Module can request the following actions to be
# performed on a door within a PAC SecureNet system:
# - Secure
# - Open
# - Bolt
# When the relay in the Control Center system is activated, the mapped action
# is attempted on the mapped door.
# When the relay in the Control Center system is deactivated, the mapped door
# is restored to normal operation.
# Area Actions
#
# OutputNumber, AREA:OrganizationUnit:AreaName:Action
# OutputNumber, AREA:OrganizationUnit:AreaName:Open:Duration
#
# The PAC SecureNet Integration Module can request the following actions to be
# performed on an area within a PAC SecureNet system:
# - Secure
# - Open
# - Bolt
# - Arm
# - Disarm
# When the relay in the Control Center system is activated, the mapped action
# is attempted on all doors within the mapped area.
# When the relay in the Control Center system is deactivated, all the doors in
# the mapped area are restored to normal operation.
# Deactivation is not allowed for a relay mapped to an Arm or Disarm action.
# When configuring a relay with the action Open an optional duration can be
# provided. When the Duration parameter is provided the target will be
# opened for the specified number of minutes, after which it will be
# automatically restored to normal operation.
# Output Activations and Deactivations
#
# OutputNumber, OUTPUT:OrganizationUnit:OutputName
#
# The PAC SecureNet Integration Module can request that an output in the
# PAC SecureNet system is activated or deactivated.
# When the relay in the Control Center system is activated, a request will be
# sent that the mapped output is activated.
# When the relay in the Control Center system is deactivated, a request will be
# sent that the mapped output is deactivated.
# Examples:
```

```

# 1, DOOR:TestOrganizationUnit:512MkII_Door_1:Secure, Secure the 512MkII_Door_1 door
of the TestOrganizationUnit organization unit
# 2, DOOR:TestOrganizationUnit:Main Door:Open, Open the Main Door door of the
TestOrganizationUnit organization unit
# 3, DOOR:TestOrganizationUnit:Stairway:Bolt, Bolt the Stairway door of the
TestOrganizationUnit organization unit
# 4, DOOR:TestOrganizationUnit:Main Door:Open:60, Open the Main Door door of the
TestOrganizationUnit organization unit for 60 minutes
# 5, AREA:TestOrganizationUnit:Main Entrance:Secure, Secure all doors within the Main
Entrance area of the TestOrganizationUnit organization unit
# 6, AREA:TestOrganizationUnit:Secondary Entrance:Open, Open all doors within the
Secondary Entrance area of the TestOrganizationUnit organization unit
# 7, AREA:TestOrganizationUnit:Hall:Bolt, Bolt all doors within the Hall area of the
TestOrganizationUnit organization unit
# 8, AREA:TestOrganizationUnit:Main Entrance:Open:60, Open all doors within the Main
Entrance area of the TestOrganizationUnit organization unit for 60 minutes
# 9, AREA:TestOrganizationUnit:Hall:Arm, Arm the Hall area of the
TestOrganizationUnit organization unit
# 10, AREA:TestOrganizationUnit:Hall:Disarm, Disarm the Hall area of the
TestOrganizationUnit organization unit
# 11, OUTPUT:TestOrganizationUnit:OutputRelay1, Activate/Deactivate the output
OutputRelay1 of the TestOrganizationUnit organization unit
# The RelayAction cannot contain the characters ':', '\', '{', '}' or ','.
# The following octal escape codes can be used to represent these characters.
# Character ':': => \072
# Character '\': => \134
# Character '{': => \173
# Character '}': => \175
# Character ',': => \054
# Example using octal escape codes for an organization unit called
Unit1:office1,office2
# 12, DOOR:Unit1\072office1\054office2:Main Door:Open

```

The first element of each entry uniquely identifies the External Relay Output in the IndigoVision System. The second element is a string that identifies whether the action's target is an AREA, a DOOR or an OUTPUT, the organization unit, the name of the target and the action to be performed on the specified target within the specified organization unit within the PAC SecureNet system.

If the action's target is an OUTPUT, no action should be specified here, as outputs only support activation and deactivation which correspond to the external relay activation and deactivation in Control Center.

Logging configuration

Logging is configured with a separate file, which allows you to customize logging and to manage backup log files. To access this file, navigate to the following location:

Start > All Programs > IndigoVision PAC SecureNet Integration > Logging Configuration for PAC SecureNet Integration

To adjust the logging level, modify *level* in the root section. This can be changed to one of the following values:

- **DEBUG:** Verbose logs with comprehensive details on operations.
- **INFO:** Details successful events and behavior as well as all warnings and errors.

- **WARN:** All messages logged are warning or error messages that indicate that the PAC SecureNet Integration Module may not be functioning correctly and may require action.
- **ERROR:** Only capture messages where a failure has occurred and action may be required.
- **FATAL:** Critical errors where the integration module cannot continue.

For example, to increase the default logging level to include the default logging level to include confirmation of events sent successfully:

```
<level value="INFO"/>
```

You can customize the retention of log files by editing the following values:

- **maximumFileSize:** The size of individual log files before a new file is created.
- **maxSizeRollBackups:** The number of backup files to be kept. Older files will be removed when this limit is hit and new files are required.

It is not recommended that any other settings are changed unless advised by IndigoVision

Once you have successfully configured logging, you can access the log files at any time navigating to the following location:

Start > All Programs > IndigoVision PAC SecureNet Integration > Logs folder for PAC SecureNet Integration

6 TROUBLESHOOTING

This section provides troubleshooting information for the PAC SecureNet Integration Module.

Service does not start

If the IndigoVision PAC SecureNet Integration Module does not start properly from Windows Services, then open the most recent log file and look at the latest two messages marked as FATAL.

If the following message is seen, the Authorization Key File has not been created:

```
2017-10-06 14:59:46,194 [FATAL][IntegrationCore.Core.EventManager]: The
Authorization Key File 'indigovision.oemkey' could not be found. The file
should be created within PAC SecureNet and stored in:
C:\ProgramData\IndigoVision\Integration\PAC SecureNet\Authorization
```

- For more information about setting up the Authorization Key File, see "Provide Authorization Key File" on page 12

If no FATAL level log messages are available:

1. Open Windows **Event Viewer**
2. Navigate to **Windows Logs > Application**
3. Find one or more events logged at ERROR level and with **Source** IndigoVision IntegrationCore Service
The **General** field describes why the service is not starting.

Alarms not appearing in Control Center

If alarms are not appearing in Control Center then the following end-to-end check for a single alarm may help to determine the source of the problem.

1. Enable INFO level logging.
 - For more information, see "*Logging configuration*" on page 19
This allows the Integration Module to log all alarms received from the monitored system, not just those that have been mapped in the event configuration file.
2. Verify that the Integration Module service is running.
Refer to the IndigoVision Control Center Installation Guide for more information about IndigoVision Firewall Requirements.
 - For more information, see "*References*" on page 5
3. Verify that the Integration Module is sending events to the nominated Alarm Server by opening the most recent Integration Module log file.
Check for messages stating that the alarm has been sent.

```
2016-12-31 11:16:23,838 [INFO ][IntegrationCore.Core.Event.BindingKit]: ToIv
stateless event sent to Alarm Server '10.1.219.11' with external input number
'104' from IP '10.1.219.1'. UTC time of the event was '31/12/2016 11:16:23'.
```

If the event is not in the log file then:

- a. Using the PAC SecureNet GUI, check that the PAC SecureNet server has an OEM Interface license installed in **Tools > Manage OEM Interface**.

The IndigoVision PAC SecureNet Integration Module will exist if it was correctly installed.

- b. Check that there is no port conflict on the PAC SecureNet Integration Module machine. Assuming the default port of 5150, use a command window to enter:


```
netstat -ab.
```

A TCP entry for port 5150 should be seen with the process `IndigoVision.IntegrationCore.exe`.

- c. Refer to PAC SecureNet documentation on how to set up and configure the PAC SecureNet system.

If the event is in the log file then the Alarms To IV configuration file (`ToIv.conf`) is not correctly configured to forward this event to the IndigoVision system, in which case you will see a log message like the following:

```
2016-12-30 10:42:08,335 [INFO ][IntegrationCore.Core.EventManager]: ToIv event
'SecureNet:Sale:Sale Side Window:Door forced' is not configured to send to any
Alarm Server.
```

4. Verify that the corresponding zones and external detectors have been created, that the zones have been set, and the external detectors have been enabled in Control Center.

In **Setup**, select the relevant site in the **Alarms** tab of the Site Explorer then:

- a. Select the **External Systems** tab and ensure that an External System with the IP address of the PC running the PAC SecureNet Integration Module has been created.
- b. Select the **Zones** tab and ensure that a zone has been created containing an external detector with the Input Number being the external input number configured for the event.
- c. Ensure that the zone belongs to the nominated Alarm Server.

Right-click the zone and select **Properties > Zone**. Ensure that the Alarm Server is the same as that configured in the To IV Alarm Servers configuration (`ToIvAlarmServers.conf`) file for the PAC SecureNet Integration Module.

5. Verify that the System user is authorized to write to the log file regardless of the current login user's authorization.

PAC SecureNet Integration Module is slow to start

If no internet access is available, a standard security check may cause the PAC SecureNet Integration Module service to be slow to start, taking up to one minute.

To resolve this, disable **Check for publisher's certificate revocation**, which is typically found in the **Advanced** tab of Internet Options. However, this must be disabled for the Windows user running the service, which by default is Local System.

To disable **Check for publisher's certificate revocation** for the Local System user, edit the registry key:

1. Start the Windows **Registry Editor** (`Regedit.exe`).
2. Navigate to **HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\TrustProviders\Software Publishing**.
3. Double-click the value called **State**.
4. Set the Value data to 23e00 for hexadecimal or 146944 in decimal.
5. Click **OK**.

6. Quit Registry Editor.

Optionally, perform the same steps for the default registry key: ***HKEY_USERS\DEFAULT\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing***.

If you have configured a different user to run the service, ***Check for publisher's certificate revocation*** must instead be disabled for that user.

If you are able to log into Windows with this user account, use the method described to disable the option.

Unable to connect to the PAC SecureNet server

If you are unable to connect to the PAC SecureNet server, check the following:

1. Check the log file for `ERROR` level messages and follow the advice in the error message.
2. If the following message is seen, the PAC OEM Interface certificate is not correctly installed.

```
2017-10-10 13:49:17,654 [ERROR]
[PACSecureNetIntegration.Connection.ConnectionManager]: Unable to connect to
PAC SecureNet. An error with the PAC SecureNet server certificate was
encountered.
```

- Using the same Windows user that the service uses, run the ***LoadCertificate.cmd*** script.

By default, the user is Local System. Use the Windows Services control panel to change this user.

By default, the script is available in ***C:\Program Files (x86)\IndigoVision\Integration\PAC SecureNet Integration\Certificate***

- If no error messages are seen, enable `INFO` level logging.
 - ▶ For more information, see "Logging configuration" on page 19
- Check for messages stating that the connection is made successfully.

```
2017-10-10 14:58:44,327 [INFO ]
[PACSecureNetIntegration.Connection.ConnectionManager]: Successfully connected
to PAC SecureNet.
```

3. If the following message is seen, the PAC SecureNet server may not have been configured appropriately for communication with the Integration Module.

```
2017-10-10 13:49:17,654 [ERROR]
[PACSecureNetIntegration.Connection.ConnectionManager]: Failed to connect to
PAC SecureNet.
```

For more information about configuring the PAC SecureNet server for use with the Integration Module, see ***"Installation" on page 8***

Unable to control doors, areas or outputs in a PAC SecureNet installation using external relays in Control Center

If you get an error within Control Center such as 'Failed to perform action: ExternalRelayName: Activate', do the following:

1. Verify that the IndigoVision PAC SecureNet Integration Module is running and online.
2. Verify the `EnableFromIvRelays` option in the System Configuration file is set to `true`.

3. Check the From IV Relays Configuration file to ensure that the relay output number configured matches the external relay within Control Center.

If you get a success message within Control Center but the action is not being performed on the PAC SecureNet system, do the following:

4. Enable `INFO` level logging.
 - For more information, see "Logging configuration" on page 19
 This allows the Integration Module to log all relay actions and success/ error responses from the PAC SecureNet system.
5. Verify that the Integration Module is sending relay actions to the PAC SecureNet system by activating the relay and then checking the logs for messages relating to success or failure. For example,

```
2018-04-19 10:56:02,762 [INFO ]
[PACSecureNetIntegration.FromIvRelays.FromIvRelayModule]: Performing Open
action on Door '512MkII_Door_1' within Organization Unit 'Test Office'
```

If the PAC SecureNet server has reported that the operation has completed successfully, refer to the PAC's documentation. If the action fails, then ensure that the Organization Unit, Target and Action fields in the FromIvRelays mapping are correct. The Action field should not be specified if the action's target is an output.

6. Check the target status within the PAC SecureNet server - refer to the PAC's documentation for more details on how to do this.
7. If the action's target is an output, verify that the output is enabled in the PAC SecureNet server. Only enabled outputs can be activated or deactivated by the Integration Module.

Unable to acknowledge a PAC SecureNet active alarm by acknowledging or clearing a zone

If acknowledging or clearing a zone in Control Center does not acknowledge the corresponding active alarm in the PAC SecureNet system:

1. Verify that the IndigoVision PAC SecureNet Integration Module is running and online.
2. Verify the `EnableAlarmActionsFromIv` option in the System Configuration file is set to `true`.
3. Enable `INFO` level logging.

- For more information, see "Logging configuration" on page 19

This allows the Integration Module to log all FromIv actions and success responses from the PAC SecureNet system.

For example:

```
2018-05-01 13:58:03,746 [INFO ]
[PACSecureNetIntegration.FromIvActions.FromIvActionsModule]: The active alarm
on alarm point 'Door1' within area 'Secondary Entrance' of the organization
unit 'Test Office' has been successfully acknowledged
```

If no active alarm has been found corresponding to the acknowledged or cleared zone, an error message with further details will be displayed in the log file:

```
2018-05-02 10:10:08,716 [ERROR]
[PACSecureNetIntegration.FromIvActions.FromIvActionsModule]: Skipping zone
action for Test Office:Secondary Entrance:PAC512_\173LANG_DOOR\175_2:Door
forced as no corresponding active alarm could be found
```


License issues

You should not encounter license issues if the PAC SecureNet Integration Module is installed on a machine that has not had Sentinel HASP software installed previously.

However, possible issues may occur if the machine to be installed on has previously had Sentinel HASP software installed on it.

Before installing the PAC SecureNet Integration Module, uninstall IndigoVision software that is licensed with either a hardware or software license.

Check that the Sentinel HASP Dongle is Active

If the Sentinel dongle is working correctly, a red LED is illuminated on the dongle.

Check that the device drivers are listed in Device Manager:

1. Navigate to **Control Panel > System**.
2. Select the **Hardware** tab.
3. Select **Device Manager**.
4. Navigate to **Universal Serial Bus Controllers**, and expand the list.
5. Check that the following are listed:
 - SafeNet Inc. Sentinel HL Key
 - SafeNet Inc. HASP Key
 - SafeNet Inc. USB Key