

**IndigoVision**

**Paxton  
Integration Module**

**Administrator's Guide**



IndigoVision

THIS MANUAL WAS PUBLISHED ON WEDNESDAY, APRIL 17, 2019.

DOCUMENT ID: IU-IM-MAN018-3

### 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, INTEGRA AND CYBERVIGILANT ARE REGISTERED TRADEMARKS OF INDIGOVISION LIMITED. CAMERA GATEWAY IS AN UNREGISTERED TRADEMARK 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](mailto: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
<b>1</b>	<b>About this guide .....</b>	<b>5</b>
	Safety notices .....	5
	References .....	5
<b>2</b>	<b>Overview .....</b>	<b>6</b>
	Compatibility .....	6
	System requirements .....	6
	Paxton Net2 .....	6
	Licensing .....	6
<b>3</b>	<b>Installation .....</b>	<b>7</b>
	Installing on the same device as Paxton Net2 .....	7
	Installing on a different device from Paxton Net2 .....	7
	Upgrading from v1.0 .....	7
	License the integration module .....	8
<b>4</b>	<b>Configuration .....</b>	<b>9</b>
	Configuration Tool .....	9
	IndigoVision Control Center configuration .....	10
	Create a new external system .....	10
	Create a new zone and external detector for Paxton events .....	10
	Create external detectors for all types of events .....	10
	Create a new external relay .....	10
<b>5</b>	<b>System Configuration Files .....</b>	<b>12</b>
	Paxton event configuration files .....	12
	Remote control of Doors and LEDs .....	17
<b>6</b>	<b>Troubleshooting .....</b>	<b>19</b>
	Alarms not appearing in Control Center .....	19
	Paxton Integration Module is slow to start .....	20
	Unable to control a Net2 control unit within Control Center .....	20
	Unable to acknowledge a Paxton event by clearing a zone .....	21
	Unable to Silence an Access Control Unit .....	21
	License issues .....	22
	Check that the Sentinel HASP Dongle is Active .....	22
	Unable to store Paxton events using the Configuration Tool on machines without Paxton22	

Net2 installed .....

<b>A</b>	<b>Appendix</b> .....	<b>23</b>
	Supported event types .....	23
	Supported event sub-types .....	27
	Logging configuration .....	29

# 1 ABOUT THIS GUIDE

This guide is provided for system administrators integrating the Paxton Net2 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>**

# 2 OVERVIEW

The Paxton Integration Module allows events from a Paxton Net2 system to be integrated into IndigoVision Control Center suite. This document explains how to install and configure the Paxton Integration Module.

## Compatibility

Please ensure you have properly installed, configured, and licensed the Paxton Net2 system.

## System requirements

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

- Windows® Server 2012 R2
- Windows® Server 2012
- Windows® Server 2008 R2
- Windows® 10 (64-bit) version 1607 or later
- 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.

## Paxton Net2

The Paxton Integration Module is compatible and has been tested with Net2|Lite and Net2|Pro v6.00.7619. The

## Licensing

The Paxton 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 Paxton 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 Paxton Integration Module.

# 3 INSTALLATION

## Installing on the same device as Paxton Net2

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

To install the Integration Module:

1. Download the Paxton Net2 integration from Partner Extranet site.
  - ▶ For more information, see *"References" on page 5*
2. Run the **setup.exe** file and follow the on screen instructions.  
The Integration Module is installed to: **C:\Program Files (x86)\IndigoVision\Integration\Paxton** by default.
3. If the Microsoft .NET 4.7.2 Framework is not installed then you are prompted to install it.
4. Request and install a software license for the Paxton Integration Module using the License Manager tool.
  - ▶ For more information, see *"License the integration module" on page 8*
5. Configure the installation using the Configuration Tool.
  - ▶ For more information, see *"Configuration Tool" on page 9*
6. When prompted by the Configuration Tool, allow the integration to be restarted.

## Installing on a different device from Paxton Net2

The installation of the IndigoVision Paxton Integration relies on files provided by Paxton Net2. Before installing the integration, run the **PaxtonRedist.msi** from the installation directory. When opened, this will install the relevant dependencies. There is no user action required.

Once the application closes, follow the instructions for see *"Installing on the same device as Paxton Net2" on page 7*

## Upgrading from v1.0

When upgrading from version 1.0, the system must be reconfigured. The existing system configuration file is backed up to **IndigoVision\Paxton\Backup** folder under the **ProgramData** directory.

Reconfiguration can be performed using the Configuration Tool. This will guide you through the setup process.

- ▶ For more information, see "Configuration" on page 9

---

**Notice** *The configuration of Paxton and IndigoVision events and relay actions will be recognized by the Configuration Tool and will not need to be reconfigured.*

---

## License the integration module

To run the IndigoVision Paxton Integration Module, you must have a valid license. This can be a hardware license or a software license which allows the Paxton 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 Paxton 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 Order Management.
2. Apply a Vendor to Client file (v2c) provided by IndigoVision.

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

# 4 CONFIGURATION

To integrate Paxton alarms and events in to the IndigoVision Alarm Server:

1. Run the Integration Configuration Tool for Paxton Integration – see "Configuration Tool" on page 9
2. Configure IndigoVision Control Center:
  - a. Create a new external system – see "Create a new external system" on page 10
  - b. Create a new zone and external detector for each Paxton event – see "Create a new zone and external detector for Paxton events" on page 10

## Configuration Tool

The Integration Configuration Tool can be used to configure the events and system settings for the Paxton Integration:

1. Run the Integration Configuration Tool for Paxton Integration.  
***Start > All Programs > IndigoVision Paxton Integration > Configure Paxton Integration***
2. Optionally provide the Alarm Server IP for System Events.
  - System Events report the status of the Paxton Integration and its connection to Paxton.
3. Provide the Integration IP address of the Paxton Integration.
  - When the IndigoVision Paxton Integration is installed on a machine with multiple network adapters or multiple IP addresses, the Integration IP must be specified.
  - This must be the IP of the External System configured in Control Center.
4. If the System Alarm Server IP for System Events was provided, configure System Events:
  - Integration Online and Offline
  - Paxton Online and Offline
5. Provide the Paxton Net2 server IP address and user credentials.

---

**Notice** *IndigoVision recommends creating a user with adequate permission specifically for the IndigoVision Paxton Integration.*

---

6. Specify the IndigoVision Alarm Servers that will receive events.
  - Each Alarm Server supports up to 10,000 detectors.
  - If you require more than 10,000 Paxton alarms to be configured, or the Alarm Server has detectors for other sources configured, for example, Advanced Analytics or Digital Input detectors, then you can split the configuration of Paxton alarms across multiple Alarm Servers.

7. Configure the event mappings for each Alarm Server. The event mapping file is known as a Paxton events configuration file (events to IndigoVision).
  - The Paxton events configuration file for the Alarm Server opens in a new window.
    - ▶ For more information, see "*Paxton event configuration files*" on page 12
8. Optionally enable Alarm Actions from IndigoVision Control Center if you wish to acknowledge and delete Paxton Integration alarms from IndigoVision Control Center.
9. Optionally enable Relay Actions if you wish to remote control outputs and doors from IndigoVision Control Center.
10. Configure the relay mappings if required. The file opens in a new window.
11. Click **Finish** to close the dialog, save your settings and automatically start the Paxton Integration.

## IndigoVision Control Center configuration

If the Integration Offline, Integration Online, Paxton Offline and Paxton Online external system inputs are defined in the system configuration file and are of interest, then they must be configured in Control Center.

- ▶ For more information, see "*References*" on page 5

### Create a new external system

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

- ▶ For more information, see "*References*" on page 5

### Create a new zone and external detector for Paxton 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.

- ▶ For more information, see "*References*" on page 5

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 a new external relay

Add a new IndigoVision external relay for each relay action configured in the **FromIvRelays.conf** file. FromIv Relays for the Paxton Integration Module can only be activated therefore the automatically created Manual Action to Deactivate should be deleted.

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

Relays can be used to open, hold open and close doors.

- ▶ For more information about configuring relay actions, see *"Remote control of Doors and LEDs" on page 17.*

# 5 SYSTEM CONFIGURATION FILES

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

---

**Notice** *The System.conf, Tolv.conf, TolvAlarmServers.conf and FromlvRelays.conf will be automatically edited by the Configuration Tool.*

---

## Paxton event configuration files

This section covers the configuration for Paxton events that are sent from the Paxton system to the IndigoVision Control Center suite to activate detectors.

Paxton event configuration files contain information for mapping each Paxton event received from the Paxton system to the IndigoVision Control Center suite. A file must be configured for each Alarm Server.

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

**Figure 1:** Example of Paxton events to IndigoVision Configuration file

---

```
# This file contains the mapping of Paxton Net 2 alarms and events to IndigoVision
# external event input numbers.
#
# Each mapping entry consists of two (optionally three) comma separated
# fields.
#
# InputNumber, Net2 alarm, Optional comment
#
# The first element of each entry is a positive integer corresponding to an
# External Detector input number in the Alarm Server.
# The second element is a string equal to the ACU serial number, Event Type
# and Event Sub Type separated by ':'.
# The third field is used for comments and is ignored by the Integration Module.
# The example below shows how to configure the Integration Module to
# forward a 'AccessPermittedCardOnly' event with SubEventType 'NoAccessMade'
# generated in Paxton Access Control Unit with serial number 10101010.
# The event is forwarded as a new activation of detector number 100 in the
# IndigoVision Control Center system.
# 100, 10101010:AccessPermittedCardOnly:NoAccessMade
# 101, 17255887:Tamper:None, Tamper event for Paxton ACU 17255887
# 102, 17555955:DoorForced:None
# 103, 17555955:DoorOpened1:WithExitButton
```

```
# The full list of event types and event sub types is also available in the Paxton
# Integration Module Admin Guide.
#[Valid Net2 Event Types ]
#None
#ControlUnitReset
#SystemSetting
#RealTimeClockSet
#RealTimeClockError
#PublicHoliday
#ControlUnit
#ChecksumFailure
#AcuDiagnosticsAvailable
#CardSwiped
#DesktopReader
#ValidCodeEntered
#ValidPinEntered1
#AccessPermitted1
#AccessDenied1
#AccessDenied2
#AccessPermittedCardOnly
#ValidPinEntered2
#AccessPermittedCardCode
#AccessDeniedInvalidCard
#AccessDeniedInvalidPin
#AccessDeniedInvalidCode
#AccessPermittedPinOnly
#AccessPermittedCodeOnly
#DoorOpened1
#DoorRelock
#AccessPermittedAnpr
#AccessDeniedAnpr
#RequestAccessCheck
#AcuApbCleared
#Input5
#Input6
#Input7
#Input8
#Output1
#Output2
#Output3
#Output4
#Output5
#Output6
#Output7
#Output8
#DoorOpened2
#DoorClosed
#LockOpened
#LockClosed
#ReaderNotActive
#DoorBellPressed
#ReaderDetected
#KeypadDetected
```

```
#RelayToggled
#DoorNotOpened
#Relay1Toggled
#Relay2Toggled
#TriggerAndActionRuleWasRun
#TimeAndAttendance
#IntruderAlarm
#FirmwareUpdated
#SilenceAlarm
#FireAlarmInput
#FireDoor
#PinNotValid
#CardNotValid
#KeypadTimeOut
#Tamper
#MainsFailed
#DoorForced
#DoorLeftOpen
#ReaderTamper
#DuressCode
#KeypadHacker
#InputShort
#InputCut
#InputVoltageSubstitution
#InputPressed
#InputReleased
#AccessPermitted2
#AccessDenied3
#AccessDeniedLockdownInProgress
#DoorEnteredLockdownState
#DoorExitedLockdownState
#SetDoorOpenedTime
#AcuNotResponding
#AcuOnline
#CheckCommunicationsInterface
#IoBoardNotResponding
#IoBoardOnline
#IoBoardFirmwareUpdateSucceeded
#IoBoardFirmwareUpdateFailed
#CouldNotConnectToIoBoard
#CouldNotConfigureIoBoard
#IoBoardSettingsUpdated
#LoggedOnAsOemClient
#LoggedOffAsOemClient
#Operator
#AlarmActioned
#BackupSucceeded
#BackupFailed
#ArchiveSucceeded
#ArchiveFailed
#Server
#ServerError
#AddAcu
```

```
#AddAcuError
#ServerWarning
#SendMessageFailed
#ObjectChangedLowPriority
#Object
#ObjectChanged
#UserDetails
#Timezone
#AccessLevel
#AcuConfiguration
#Area
#Report
#Antipassback
#SystemOperator
#FirmwareUpgradeError
#SiteGraphics
#RequestDoorOpen
#OpenDoorGroup
#CloseDoorGroup
#LockdownInitiatedByUser
#LockdownEndedByUser
#RemoteSite
#EventTableCorrupted
#FlashCrcChanged
#EepromCrcChanged
#InvalidSession
#SessionStarted
#SessionComplete
#CompactStarted
#CompactComplete
#FactoryResetStarted
#FactoryResetComplete
#NanoDebugInformation
#QueuedEventsLost
#NanoCannotUnlock
#NanoCannotLock
#LowBattery
#BatteryCriticallyLow
#BatteryLevelUpdated;
#[Valid Net2 Event Sub Types]
#None
#PowerOn
#CopReset
#InvalidInstruction
#ClockFail
#SoftwareInterrupt
#RtcStop
#RtcIcError
#Initialised
#PublicHolidayStart
#PublicHolidayEnd
#ProximityWakeUp
#ScheduledWakeUp
```

```
#AccessLevelNotValid
#IndividualPermissionsNotValid
#CardDetailsNotFound
#CardDataAba
#CardPaxtonUserCard
#CardPaxtonNonUserCard
#CardThirdParty
#CardDataWiegand26
#CardDataError
#ClockIn
#ClockOut
#VehicleRegistrationNotRecognised
#Opened
#Closed
#AntipassbackLogical
#AntipassbackTimed
#AntipassbackLogicalTimed
#AntipassbackLostContactWithServer
#NoAccessMade
#GoneLow
#GoneHigh
#On
#Off
#WithTimezone
#WithNetworkInstruction
#WithExitButton
#WithNet2DoorEntry
#NotActive
#UserOnHoliday
#CardReportedLost
#Armed
#Disarmed
#AlarmStillArmed
#AnprAccessAttempt
#DuringOfflineMode
#LockdownInitiatedWithToken
#LockdownEndedWithToken
#LockDownStillActive
#BreakReceived
#Logon
#Logoff
#AlarmActionedBy
#InvalidDirectory
#StartStopError
#Started
#Stopped
#ClientConnected
#ClientDisconnected
#DatabaseCreated
#SoftwareUpdated
#BackupRestored
#AcuAddError
#NewAcuAddedSuccessfully
```

```
#TooManyDoors
#ModificationError
#Added
#Modified
#Deleted
#FirmwareRefresh
#Reinstated
#ModemStatus
#Connected
#Disconnected
#ConnectionFailed
#ConnectionCancelled
```

The complete list of support event types and event sub types is available in the Appendix.

► For more information, see *"Appendix" on page 23*

## Remote control of Doors and LEDs

The Paxton Integration allows operators to control doors and reader LEDs from Control Center using relays. This feature needs to be enabled and configured using the Integration Configuration tool.

► For more information, see *"Configuration Tool" on page 9*

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

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

**Figure 2:** Example of a From IV Relays configuration file

```
# This file maps IndigoVision external relay outputs to control doors within the
# Paxton Net2 system.
# The following formats are used to define the relay outputs:
#
# OutputNumber, SerialNumber:Action
# OutputNumber, SerialNumber:Action:AdditionalInfo
#
# 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 is a string containing the Serial Number of the ACU device
# to control and the name of the action to perform. Additional information may
# also be required, depending on the action.
# The Paxton Integration Module can perform the following actions on a Net2
# control unit:
# - DoorOpen
# - DoorHoldOpen
# - DoorClose
# - FlashAccessPermitted
# - FlashAccessDenied
# When configuring a relay with the action DoorOpen an optional duration can be
# provided. When the AdditionalInfo parameter is provided the door will be
# opened for the specified number of milliseconds.
# To flash the LED on a reader using FlashAccessPermitted or FlashAccessDenied
# action the reader number must be provided in the AdditionalInfo parameter.
# Examples:
```

```
# 1, 1796347:DoorOpen, Open the door with the serial number 1793647
# 2, 1796347:DoorHoldOpen, Open the door and keep it held open
# 3, 1796347:DoorClose
# 4, 1796347:DoorOpen:20000, Open the door for 20 seconds
# 5, 1796347:FlashAccessPermitted:1, Flash LED on Reader 1 for access permitted
# 6, 1796347:FlashAccessDenied:2, Flash LED on Reader 2 for access denied
```

The first element of each entry uniquely identifies the External Relay Output in the IndigoVision System. The second element is a string that identifies the ACU serial number and the action to perform.

# 6 TROUBLESHOOTING

This section provides troubleshooting information for the Paxton Integration Module.

## 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 29*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 refer to Paxton Net2 Server documentation on how to set up and configure the Net2 system.

If the event is in the log file then the Alarms To IV configuration file (Tolv.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 '1796347:AccessPermittedPinOnly:NoAccessMade' 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 Paxton 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 (**TolvAlarmServers.conf**) file for the Paxton Integration Module.

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

## Paxton Integration Module is slow to start

If no internet access is available, a standard security check may cause the Paxton 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\TrustProviders\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 control a Net2 control unit within Control Center

If you get an error within Control Center such as 'Failed to perform action Net2Door: Activate', do the following:

1. Verify that the IndigoVision Paxton Integration Module is running and online.
2. Verify that **EnableFromIvRelays** 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 Paxton Net2 control unit, do the following:

1. Enable INFO level logging.
  - ▶ For more information, see *"Logging configuration" on page 29*This allows the Integration Module to log all relay actions and success responses from the Paxton Net2 server.
2. Verify that the Integration Module is sending relay actions to the Paxton Net2 system by activating the relay and then checking the logs for messages relating to success or failure.

For example,

```
2017-01-04 15:07:29,923 [INFO ][PaxtonIntegration.Connection.Connection]:
Performing relay action to open door '1796347'.
2017-01-04 15:07:29,939 [INFO ][PaxtonIntegration.Connection.Connection]:
Relay action DoorOpen for 1796347 succeeded
```

If the Paxton Net2 server has reported that the operation has completed successfully, refer to Paxton's documentation. If the action fails then ensure that the serial number is correct.

No event is provided in Paxton Net2 when the door is opened or closed using a relay action. Check the door itself or view the status to see if it is Locked or Unlocked.

## Unable to acknowledge a Paxton event by clearing a zone

If clearing a zone does not acknowledge an event in Paxton Net2:

1. Ensure that the installed version of Paxton Net2 Access is v5.03.5214.
2. Verify that the IndigoVision Paxton Integration Module is running and online.
3. Verify that **EnableAlarmActionsFromIv** in the System Configuration file is set to true.
4. Enable INFO level logging.

► For more information, see *"Logging configuration" on page 29*

This allows the Integration Module to log all FromIv alarm actions and success responses from the Paxton Net2 server.

For example:

```
2017-01-17 09:11:09,101 [INFO ][PaxtonIntegration.Connection.Connection]:
Found 1 event matching '1796347:Tamper:None' in Paxton Net2 requiring
acknowledgment.
2017-01-17 09:11:09,134 [INFO ][PaxtonIntegration.Connection.Connection]:
Acknowledged ''1796347:Tamper:None'' in Paxton Net2.
```

If no events currently require acknowledging then the following log message will be seen:

```
2017-01-17 09:12:12,241 [INFO ][PaxtonIntegration.Connection.Connection]:
There are no events for '1796347:Tamper:None' requiring acknowledgment in
Paxton Net2.
```

If the event type does not support acknowledgements then the following log message will be seen:

```
2017-01-17 09:15:53,734 [INFO ]
[PaxtonIntegration.FromIvActionsModule.FromIvActionsModule]:
1796347:Tamper:None does not require acknowledging on Paxton Net2.
```

The following EventTypes can be acknowledged in the Paxton system:

- FireAlarmInput
- CardNotValid (with subtype CardReportedLost)
- Tamper
- MainsFailed
- DoorForced
- DoorLeftOpen
- AcuNotResponding

## Unable to Silence an Access Control Unit

Clearing a zone acknowledges events within Paxton Net2. If all events for an Access Control Unit are acknowledged as a result of clearing the zone, the Access Control Unit will be silenced.

If clearing a zone does not silence an Access Control Unit, do the following:

1. Ensure that the installed version of Paxton Net2 is v5.03.5214.
2. Verify that the IndigoVision Paxton Integration Module is running and online.
3. Verify that **EnableAlarmActionsFromIv** in the System Configuration file is set to true.
4. Check the Integration Module log file to see whether there are still events to be silenced.

For example:

```
2017-01-18 09:42:44,005 [WARN ][PaxtonIntegration.Connection.Connection]: ACU
'1796347' cannot be silenced as 2 events still require acknowledging.
```

5. Use Paxton Net2 Access Control to acknowledge any events that require acknowledgement and are not configured in your Tolv configuration.

## License issues

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

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

Before installing the Paxton 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

## Unable to store Paxton events using the Configuration Tool on machines without Paxton Net2 installed

While configuring Paxton alarm events on a machine without Paxton Net2 installed, an error may be presented stating the following:

```
The configured events are not valid: Paxton events have not been
configured for Alarm Server.
```

This issue occurs when the Configuration Tool is unable to locate the Paxton files installed by the Net2 application. It is possible to install on a separate device from Paxton Net2.

- For more information, see "Installing on a different device from Paxton Net2" on page 7.

# A APPENDIX

## Supported event types

---

<b>None</b>	None, or not set.
<b>ControlUnitReset</b>	Control unit reset
<b>SystemSetting</b>	System setting
<b>RealTimeClockSet</b>	Real time clock set
<b>RealTimeClockError</b>	Real time clock error
<b>PublicHoliday</b>	Public holiday
<b>ControlUnit</b>	Control unit
<b>ChecksumFailure</b>	Checksum failure
<b>AcuDiagnosticsAvailable</b>	ACU diagnostics available
<b>CardSwiped</b>	Card swiped
<b>DesktopReader</b>	Desktop reader
<b>ValidCodeEntered</b>	Valid code entered
<b>ValidPinEntered1</b>	Valid pin entered
<b>AccessPermitted1</b>	Access permitted
<b>AccessDenied1</b>	Access denied
<b>AccessDenied2</b>	Access denied
<b>AccessPermittedCardOnly</b>	Access permitted - card only
<b>ValidPinEntered2</b>	Valid PIN entered
<b>AccessPermittedCardCode</b>	Access permitted - card + code
<b>AccessDeniedInvalidCard</b>	Access denied - invalid card
<b>AccessDeniedInvalidPin</b>	Access denied - invalid PIN
<b>AccessDeniedInvalidCode</b>	Access denied - invalid code
<b>AccessPermittedPinOnly</b>	Access permitted - PIN only
<b>AccessPermittedCodeOnly</b>	Access permitted - code only
<b>DoorOpened1</b>	Door opened
<b>DoorRelock</b>	Door relock
<b>AccessPermittedAnpr</b>	Access permitted - ANPR
<b>AccessDeniedAnpr</b>	Access denied - ANPR
<b>RequestAccessCheck</b>	Request Access Check

---

---

<b>AcuApbCleared</b>	ACU APB cleared
<b>Input5</b>	Input 5
<b>Input6</b>	Input 6
<b>Input7</b>	Input 7
<b>Input8</b>	Input 8
<b>Output1</b>	Output 1
<b>Output2</b>	Output 2
<b>Output3</b>	Output 3
<b>Output4</b>	Output 4
<b>Output5</b>	Output 5
<b>Output6</b>	Output 6
<b>Output7</b>	Output 7
<b>Output8</b>	Output 8
<b>DoorOpened2</b>	Door opened
<b>DoorClosed</b>	Door closed
<b>LockOpened</b>	Lock opened
<b>LockClosed</b>	Lock closed
<b>ReaderNotActive</b>	Reader not active
<b>DoorBellPressed</b>	Door bell pressed
<b>ReaderDetected</b>	Reader detected
<b>KeypadDetected</b>	Keypad detected
<b>RelayToggled</b>	Relay toggled
<b>DoorNotOpened</b>	Door not opened
<b>Relay1Toggled</b>	Relay 1 toggled
<b>Relay2Toggled</b>	Relay 2 toggled
<b>TriggerAndActionRuleWasRun</b>	Trigger and action rule was run
<b>TimeAndAttendance</b>	Time and attendance
<b>IntruderAlarm</b>	Intruder alarm
<b>FirmwareUpdated</b>	Firmware updated
<b>SilenceAlarm</b>	Silence alarm
<b>FireAlarmInput</b>	Fire alarm input
<b>FireDoor</b>	Fire door
<b>PinNotValid</b>	PIN not valid
<b>CardNotValid</b>	Card not valid
<b>KeypadTimeOut</b>	Keypad time out
<b>Tamper</b>	Tamper
<b>MainsFailed</b>	Mains failed
<b>DoorForced</b>	Door forced

---

---

<b>DoorLeftOpen</b>	Door left open
<b>ReaderTamper</b>	Reader tamper
<b>DuressCode</b>	Duress code
<b>KeypadHacker</b>	Keypad hacker
<b>InputShort</b>	Input short
<b>InputCut</b>	Input cut
<b>InputVoltageSubstitution</b>	Input voltage substitution
<b>InputPressed</b>	Input pressed
<b>InputReleased</b>	Input released
<b>AccessPermitted2</b>	Access permitted
<b>AccessDenied3</b>	Access denied
<b>AccessDeniedLockdownInProgress</b>	Access Denied - Lockdown in progress
<b>DoorEnteredLockdownState</b>	Door responded to lockdown command and has entered lockdown state
<b>DoorExitedLockdownState</b>	Door responded to lockdown command and has exited lockdown state
<b>SetDoorOpenedTime</b>	Set Door Entry Door Opened Time
<b>AcuNotResponding</b>	ACU not responding
<b>AcuOnline</b>	ACU online
<b>CheckCommunicationsInterface</b>	Check communications interface
<b>IoBoardNotResponding</b>	IO board not responding
<b>IoBoardOnline</b>	IO board online
<b>IoBoardFirmwareUpdateSucceeded</b>	IO board firmware update succeeded
<b>IoBoardFirmwareUpdateFailed</b>	IO board firmware update failed
<b>CouldNotConnectToIoBoard</b>	Could not connect to IO board
<b>CouldNotConfigureIoBoard</b>	Could not configure IO board
<b>IoBoardSettingsUpdated</b>	IO board settings updated
<b>LoggedOnAsOemClient</b>	Logged on as OEM client
<b>LoggedOffAsOemClient</b>	Logged off as OEM client
<b>Operator</b>	Operator
<b>AlarmActioned</b>	Alarm actioned
<b>BackupSucceeded</b>	Backup succeeded
<b>BackupFailed</b>	Backup failed
<b>ArchiveSucceeded</b>	Archive succeeded
<b>ArchiveFailed</b>	Archive failed
<b>Server</b>	Server
<b>ServerError</b>	Server error
<b>AddAcu</b>	Add ACU
<b>AddAcuError</b>	Add ACU Error

---

---

<b>ServerWarning</b>	Server warning
<b>SendMessageFailed</b>	Send message failed
<b>ObjectChangedLowPriority</b>	Object Changed Without Event Showing In Event Viewer
<b>Object</b>	Object (Deprecated)
<b>ObjectChanged</b>	Object
<b>UserDetails</b>	User details
<b>Timezone</b>	Timezone
<b>AccessLevel</b>	Access level
<b>AcuConfiguration</b>	ACU configuration
<b>Area</b>	Area
<b>Report</b>	Report
<b>Antipassback</b>	Anti-passback
<b>SystemOperator</b>	System operator
<b>FirmwareUpgradeError</b>	Firmware upgrade error
<b>SiteGraphics</b>	Site graphics
<b>RequestDoorOpen</b>	Request door open
<b>OpenDoorGroup</b>	Open door group
<b>CloseDoorGroup</b>	Close door group
<b>LockdownInitiatedByUser</b>	Lockdown initiated by user instruction
<b>LockdownEndedByUser</b>	Lockdown ended by user instruction
<b>RemoteSite</b>	Remote site
<b>EventTableCorrupted</b>	Event table corrupted
<b>FlashCrcChanged</b>	Flash CRC changed
<b>EepromCrcChanged</b>	EEPROM CRC changed
<b>InvalidSession</b>	Invalid session
<b>SessionStarted</b>	Session started
<b>SessionComplete</b>	Session complete
<b>CompactStarted</b>	Compact started
<b>CompactComplete</b>	Compact complete
<b>FactoryResetStarted</b>	Factory reset started
<b>FactoryResetComplete</b>	Factory reset complete
<b>NanoDebugInformation</b>	Nano Debug information
<b>QueuedEventsLost</b>	Queued events lost
<b>NanoCannotUnlock</b>	nano cannot unlock
<b>NanoCannotLock</b>	nano cannot lock
<b>LowBattery</b>	Low battery
<b>BatteryCriticallyLow</b>	Battery critically low
<b>BatteryLevelUpdated</b>	Battery level updated

---

## Supported event sub-types

---

<b>None</b>	None, or not set.
<b>PowerOn</b>	Power on
<b>CopReset</b>	COP reset
<b>InvalidInstruction</b>	Invalid instruction
<b>ClockFail</b>	Clock fail
<b>SoftwareInterrupt</b>	Software interrupt
<b>RtcStop</b>	RTC stop
<b>RtclcError</b>	RTC IC error
<b>Initialised</b>	Initialised
<b>PublicHolidayStart</b>	Public holiday start
<b>PublicHolidayEnd</b>	Public holiday end
<b>ProximityWakeUp</b>	Proximity wake up
<b>ScheduledWakeUp</b>	Scheduled wake up
<b>AccessLevelNotValid</b>	Access level not valid
<b>IndividualPermissionsNotValid</b>	Individual permissions not valid
<b>CardDetailsNotFound</b>	Card details not found
<b>CardDataAba</b>	Card data ABA
<b>CardPaxtonUserCard</b>	Card Paxton user card
<b>CardPaxtonNonUserCard</b>	Card Paxton non user card
<b>CardThirdParty</b>	Card third party
<b>CardDataWiegand26</b>	Card data Wiegand 26
<b>CardDataError</b>	Card data error
<b>ClockIn</b>	Clock in
<b>ClockOut</b>	Clock out
<b>VehicleRegistrationNotRecognised</b>	Vehicle registration not recognised
<b>Opened</b>	Opened
<b>Closed</b>	Closed
<b>AntipassbackLogical</b>	Anti-passback (Logical)
<b>AntipassbackTimed</b>	Anti-passback (Timed)
<b>AntipassbackLogicalTimed</b>	Anti-passback (Logical + Timed)
<b>AntipassbackLostContactWithServer</b>	Anti-passback (Lost contact with server)
<b>NoAccessMade</b>	No access made
<b>GoneLow</b>	Gone low
<b>GoneHigh</b>	Gone high
<b>On</b>	ON

---

---

<b>Off</b>	OFF
<b>WithTimezone</b>	With timezone
<b>WithNetworkInstruction</b>	With network instruction
<b>WithExitButton</b>	With exit button
<b>WithNet2DoorEntry</b>	With Net2 Door Entry System
<b>NotActive</b>	Not active
<b>UserOnHoliday</b>	User on holiday
<b>CardReportedLost</b>	Card reported lost
<b>Armed</b>	Armed
<b>Disarmed</b>	Disarmed
<b>AlarmStillArmed</b>	Alarm still armed
<b>AnprAccessAttempt</b>	ANPR access attempt
<b>DuringOfflineMode</b>	During offline mode
<b>LockdownInitiatedWithToken</b>	Lockdown initiated with token at designated door
<b>LockdownEndedWithToken</b>	Lockdown ended with token at designated door
<b>LockDownStillActive</b>	Lockdown still active
<b>BreakReceived</b>	Break received
<b>Logon</b>	Logon
<b>Logoff</b>	Logoff
<b>AlarmActionedBy</b>	Alarm actioned by:
<b>InvalidDirectory</b>	Invalid directory:
<b>StartStopError</b>	Error:
<b>Started</b>	Started
<b>Stopped</b>	Stopped
<b>ClientConnected</b>	Client connected:
<b>ClientDisconnected</b>	Client disconnected:
<b>DatabaseCreated</b>	Database created
<b>SoftwareUpdated</b>	Software updated
<b>BackupRestored</b>	Backup restored:
<b>AcuAddError</b>	Error:
<b>NewAcuAddedSuccessfully</b>	New ACU added successfully
<b>TooManyDoors</b>	Too many doors
<b>ModificationError</b>	Error:
<b>Added</b>	Added:
<b>Modified</b>	Modified:
<b>Deleted</b>	Deleted:
<b>FirmwareRefresh</b>	Firmware refresh:

---

<b>Reinstated</b>	Reinstated:
<b>ModemStatus</b>	Modem status
<b>Connected</b>	Connected:
<b>Disconnected</b>	Disconnected:
<b>ConnectionFailed</b>	Connection failed:
<b>ConnectionCancelled</b>	Connection cancelled

## 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 Paxton Integration > Edit Logging Configuration File***

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 Paxton 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