IndigoVision

Software House 9000 Integration

Administrator's Guide

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

Contact address

IndigoVision Limited

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

TABLE OF CONTENTS

Administrator's Guide - v13   **3**

1   ABOUT THIS GUIDE

This guide is provided for system administrators integrating the Tyco Software House C•CURE 9000 system (C•CURE 9000) with the IndigoVision Control Center suite.

Safety notices

This guide uses the following formats for safety notices:

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

⚠ **Caution**	*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 and are referenced in this document. The paths are to the default locations where the documents can be found.

1. Control Center Help

   IndigoVision > Control Center > Control Center Help

   (located on the Control Center server)
2. Integration

   https://www.indigovision.com/products/integration
3. IndigoVision Camera Gateway Administrator's Guide
4. IndigoVision Video Stream Manager Administrator's Guide

Integration specific references

1. C•CURE 9000 Installation and Upgrade Guide on C•CURE 9000 DVD
2. C•CURE 9000 Monitoring Station Guide on C•CURE 9000 DVD

3. C•CURE 9000 Video Guide on C•CURE 9000 DVD
4. C•CURE 9000 Software Configuration Guide on C•CURE 9000 DVD

2 OVERVIEW

The Software House 9000 Integration allows video and events from IndigoVision Control Center suite to be integrated with C•CURE 9000.

The integration can also be configured to forward events from C•CURE 9000 to the Control Center suite.

This document explains how to install and configure the Software House 9000 Integration.

Compatibility

Please ensure you have properly installed, configured, and licensed the C•CURE 9000.

System requirements

The Software House 9000 Integration can be installed on the following Windows$^®$ operating systems with latest service packs applied:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows10 (64-bit)
- Windows 8.1 (64-bit)

C•CURE 9000

The Software House 9000 Integration is compatible and has been certified with C•CURE 9000 v2.80.

Supported cameras

The following IndigoVision cameras and encoders are supported:

- 9000 Range
- 11000 Range
- GX Range
- BX Range
- Ultra Range
- Ultra 5K Fixed Camera
- ONVIF, Video Stream Manager and Camera Gateway cameras supported by Control Center v16.0

Bidirectional Communication

You can synchronize the state of C•CURE 9000 events with the state of detectors in the IndigoVision Control Center suite.

- When a detector activates in Control Center, the corresponding C•CURE 9000 event is latched.

  When the detector deactivates, the C•CURE 9000 event is unlatched.
- When a C•CURE 9000 event activates, the corresponding detector activates in Control Center.

  When the C•CURE 9000 event deactivates, the detector deactivates.
- When a Control Center zone is in alarm, the corresponding C•CURE 9000 event activates.

Notice   *When a Control Center zone is cleared or acknowledged, this information is not passed to C•CURE 9000.*

Licensing

The Software House 9000 Integration is a licensed product, which can be installed on a physical or virtual machine.

Install the license key on the same machine as the Software House 9000 Integration 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 Software House 9000 Integration.

C•CURE 9000 CrossFire Server

You must obtain a valid IndigoVision integration license from Software House for the C•CURE 9000 CrossFire Server to operate the Software House 9000 Integration.

C•CURE 9000 Monitoring Stations

C•CURE 9000 Monitoring Stations do not require any additional licenses to access video from the IndigoVision Control Center system.

3 INSTALLATION

This section describes how to install the IndigoVision Software House 9000 Integration server and client components.

If only the alarm functionality is required, install only the server component.

For video support, you need to install the client component on all C•CURE 9000 workstations.

License the integration

To run the IndigoVision Software House 9000 Integration, you must have a valid license. This can be a hardware license or a software license which allows the Software House 9000 Integration to run on a specific machine.

You can manage the license using the License Manager tool, which is installed as part of the Software House 9000 Integration 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.

Server installation

1. Download the Integration components from the Support area of the IndigoVision website.
2. Double click **C-CURE_9000_Server_Integration-English.exe** and extract the software to a new folder.
3. Click **setup.exe**.

   The Software House 9000 Integration is installed by default to **C:\Program Files (x86)\IndigoVision\Integration\Software House 9000**.

   The Software House 9000 Integration server component is installed by default to: **C:\Program Files (x86)\Tyco\CrossFire\ServerComponents**.
4. After the installation has completed, open the **Server Configuration Application** and restart the following services:
   - Crossfire Framework Service
   - Crossfire Server Component Framework Service
5. Configure the Software House 9000 Integration.
   ► For more information, see "Configuration" on page 13
6. Request and install a software license for Software House 9000 Integration using the License Manager tool.

► For more information, see "License the integration" on page 9

7. In the C•CURE 9000 Server Configuration Application, open the list of Extension Services. Enable and start the IndigoVision Software House 9000 Integration.

Notice *You can only install the IndigoVision Software House 9000 Integration if a compatible version of C•CURE 9000 is already installed.*

Installing with multiple network adapters or IP addresses

When the IndigoVision Software House 9000 Integration is installed on a machine with multiple network adapters or multiple IP addresses, then the parameter `IntegrationModuleIP` in the `System` section of the System configuration file must be configured.

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

Notice *If you are upgrading from a previous release of the IndigoVision Software House 9000 Integration, you must manually add this parameter to the System configuration file.*

An example is available in the sample System configuration file, located in the IndigoVision Software House 9000 Integration installation folder.

*By default, this sample configuration file is located at **C:\Program Files x86\IndigoVision\Integration\Software House 9000\System.conf.sample**.*

Client installation

The Software House 9000 Integration Client is required for viewing video, and must be installed on each C•CURE 9000 workstation.

1. Download the Integration components from the Support area of the IndigoVision website.

2. Double click **C-CURE_9000_Client_Integration-English.exe** and extract the software to a new folder.

3. Click **setup.exe**.

   The Software House 9000 Integration Client component is installed by default to:

   C:\Program Files (x86)\Tyco\CCURE Client and **C:\Program Files (x86)\Tyco\CrossFire**.

4. After the installation has completed, open the **Server Configuration Application** and restart the following services:

   • Crossfire Framework Service

   • Crossfire Server Component Framework Service

   This is only required when installing the Software House 9000 Integration Client on the C•CURE 9000 Application Server.

Upgrading

If you are upgrading from version 3.2 and earlier, you must make the following changes to the System configuration file:

- Add a new `[System]` section.
- Optionally, add the parameter `IntegrationModuleIP`. This new parameter allows you to specify an IP for the Integration.
  - ► For more information, see "Installing with multiple network adapters or IP addresses" on page 10
- Optionally, remove the following unused parameters in the System configuration file:
  - IMServer section including parameters IP and Port
  - 3rdPartyOffline in the SystemEvents section
  - 3rdPartyOnline in the SystemEvents section
  - Log section including the parameter Level
  - ► For more information, see "System configuration file (System.conf)" on page 17

If you want to use the stateful detector and C•CURE 9000 events, you must make changes to the configuration.

- To deactivate C•CURE 9000 events for FromIv detector deactivations within the Control Center system, configure a parameter within the Events section of the System configuration file.

  Set `EnableLegacyFromIvDetectorBehaviour` to `False`.
  - ► For more information, see "System configuration file (System.conf)" on page 17
- To set the state of the detector in Control Center to mirror the state of the C•CURE 9000 event, set the To Iv configuration file(s) to have both an activation input number and deactivation input number.
  - ► For more information, see "Alarms from IV configuration file (FromIv.conf)" on page 14
- To use a deactivation event, you must recreate the detectors within the Control Center front-end application.
  - ► For more information, see "Create a new zone and external detector for ToIv events" on page 14

If you do not make any changes to the configuration files, the IndigoVision Software House 9000 Integration handles FromIv and ToIv events as before.

4 CONFIGURATION

This sections describes how to configure the IndigoVision Software House 9000 Integration components.

Integration

To integrate alarms and events between C•CURE 9000 and the IndigoVision Control Center suite, you need to configure the following:

1. The system configuration file.
   ► For more information, *see "System configuration file (System.conf)" on page 14*
2. The C•CURE 9000 events (ToIv) of interest.
   ► For more information, *see "Alarms to IV configuration file (ToIv.conf)" on page 14*
3. The IndigoVision zones and detectors (FromIv) of interest.
   ► For more information, *see "Alarms from IV configuration file (FromIv.conf)" on page 14*
4. The list of ToIv IndigoVision alarm servers that receive C•CURE 9000 events.
   ► For more information, *see "To IV Alarm Servers Configuration file (ToIvAlarmServers.conf)" on page 14*
5. The list of FromIv IndigoVision alarm servers that notify the Integration of IndigoVision zone and detector alarms.
   ► For more information, *see "From IV Alarm Servers Configuration file (FromIvAlarmServers.conf)" on page 14*
6. Define the C•CURE 9000 events and system events that are of interest within IndigoVision Control Center suite.
   ► For more information, *see "IndigoVision Control Center configuration" on page 14*

The Integration service must be manually restarted for configuration file changes to have an effect.

- If only one-way operation (toIv) is required, you do not have to configure:
  - *FromIv.conf*
  - ► For more information, *see "Alarms from IV configuration file (FromIv.conf)" on page 14*
  - *FromIvAlarmServers*
  - ► For more information, *see "From IV Alarm Servers Configuration file (FromIvAlarmServers.conf)" on page 14*.
- If only one-way operation (fromIv) is required, you do not have to configure:
  - *ToIv.conf*
  - ► For more information, *see "Alarms to IV configuration file (ToIv.conf)" on page 14*
  - *ToIvAlarmServers.conf*

► For more information, *see "To IV Alarm Servers Configuration file (ToIvAlarmServers.conf)" on page 14.*

System configuration file (System.conf)

This file contains all the system configuration parameters.

► For more information, *see "System configuration file (System.conf)" on page 17*

Alarms to IV configuration file (ToIv.conf)

This file contains the mapping between the C•CURE 9000 alarm event name and the IndigoVision external event ID. It contains the data that will map the alarm event received from C•CURE 9000 to the IndigoVision Control Center suite.

► For more information, *see "Alarms to IndigoVision configuration file(s) " on page 18*

Alarms from IV configuration file (FromIv.conf)

This file contains the mapping between the IndigoVision zone and detector alarms and the alarm name that will be sent to C•CURE 9000. It contains the data that will map the alarm received from the IndigoVision Control Center suite to the alarm sent to C•CURE 9000.

► For more information, *see "Alarms from IndigoVision Configuration File(s) " on page 20*

To IV Alarm Servers Configuration file (ToIvAlarmServers.conf)

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

► For more information and an example file, *see "To IV Alarm Servers configuration file (ToIvAlarmServers.conf)" on page 22*

From IV Alarm Servers Configuration file (FromIvAlarmServers.conf)

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

► For more information, *see "From IV Alarm Servers configuration file (FromIvAlarmServers.conf)" on page 22*

IndigoVision Control Center configuration

All the C•CURE 9000 events of interest and the IMOnline and IMOffline alarm IDs as defined in the system configuration file must be configured in Control Center.

► For more information, *see "References" on page 5*

Create a new external system for ToIv events

The IP address entered is the IP address of the host running the Integration.

Create a new zone and external detector for ToIv 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. Specify the Input Number as the Activation Input Number configured for the event in the ToIv file of the Integration.

To set the state of the detector to reflect whether the event in C•CURE 9000 is active or inactive, create the detector with a Deactivation Event of type External, and a Deactivation Input Number configured for the C•CURE 9000 event in the ToIv event configuration file.

► For more information, see "Alarms from IndigoVision Configuration File(s) " on page 20

To make sure that there is no confusion in correlating events, choose zone and detector names in Control Center which closely match the C•CURE 9000 event name.

Integration Server Component

To configure the Integration Server Component that interacts with the C•CURE 9000 system:

1. Check the Windows Event Logger settings and update if necessary.
2. Use the C•CURE 9000 Server Configuration Application to manually restart the Integration Server Component. This is necessary for the configuration file changes to take effect.
   a. On the *Services* tab, under *Extension Services*, identify the Software House 9000 Integration.
   b. Select *Stop*.
   c. After the server component has stopped, select *Start*.
   ► For more information, see the C•CURE 9000 documentation

Notice	*You can alternatively restart the C•CURE 9000 Server Component Framework service.*

Redundant setups

If you are using redundancy extensions supported by C•CURE 9000, change the parameters within the Server Component configuration.

1. Navigate to the folder in which the Server Component is installed.
   By default the Server Component is installed in the C•CURE 9000's Server Component directory at *C:\Program Files (x86)\Tyco\CrossFire\ServerComponents*.
2. Open *IndigoVision.NextGenConnectedProgram.Video.Server.exe.config* using Notepad.
3. Replace any instance of `localhost` with one of the following:
   • the redundant IP address.
   • the hostName for the C•CURE 9000 server configured within the redundancy extension.
4. Restart the Server Component using Server Application Configuration.

5 SYSTEM CONFIGURATION FILES

This section contains examples of the configuration files required by the Software House 9000 Integration.

System configuration file (System.conf)

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

The comments in the sample configuration file below explain how to use the parameters listed.

Figure 1: Example of a System Configuration file

```
[AlarmServer]
#
# MANDATORY: The IP address of the Alarm Server (NVR-AS) must be specified
#
# Note: If no system events are configured in the [SystemEvents] section
# then this property is not mandatory.
#
# 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
[Events]
#
# The direction of forwarding of events that the
# Integration Module should support
#
# The default events direction is "toIv", whereby events are forwarded from
# Software House C-CURE 9000 system to the IndigoVision system
#
# Change to "fromIv", whereby events are forwarded from
# the IndigoVision system to Software House C-CURE 9000 system.
#
# Change to "both" to forward events in both directions.
# That is whereby events are forwarded from a third party system to the
# IndigoVision system
# AND
# events are forwarded from the IndigoVision system to a third party system
```

```
#
# Direction=toIv
#
# OPTIONAL: Control whether to use legacy behaviour for FromIv detector events.
#
# Set to True for C-CURE 9000 events to automatically deactivate after one hour.
# Set to False for C-CURE 9000 events to deactivate when the Control Center
# detector is deactivated.
# If the parameter is not provided then the legacy behaviour will be enabled.
#
# This parameter only applies when the Direction is set to "fromIv" or "both".
# This is not the default setting for Direction, see above.
#
EnableLegacyFromIvDetectorBehaviour=False
[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 system input number of an alarm source
# in Control Center.
#
#
# If IMOffline is defined, an event with this number will be sent
# to the NVR/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 when the USB license dongle is removed or expires
# (trial dongles only).
#
# IMOffline=1
#
# If IMOnline is defined, an event with this number will be sent
# to the NVR/Alarm Server whenever the Integration Module has
# successfully started up.
#
# IMOnline=2
```

Alarms to IndigoVision configuration file(s)

During installation one default Alarms to IndigoVision configuration file (ToIv.conf) is provided in the ToIv folder.

There is one mapping entry per line in the 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 C-CURE 9000 events to IndigoVision
# external event input numbers.
#
# Each mapping entry consists of two (optionally three) comma separated fields.
```

```
#
# InputNumber, CCURE9000Event, OptionalDescription
#
# 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 representing the C-CURE 9000 event name.
# Examples of basic event configuration:
# 10, CCURE9000Event10
# 11, MotionDetection
# An optional third field, separated by another comma can be added with
# a description of the event mapping.
# Examples of an event with the optional description:
# 12, CCURE9000Event12, Event activate in C-CURE 9000.
# Events can also be configured as stateful so that the state of the detector in
# the Control Center system mirrors the state of the C-CURE 9000 event. It is
# recommended that events are configured as stateful.
#
# To configure a stateful event a pair of input numbers should be provided for
# the InputNumber field separated by a ':'.
#
# ActivationInputNumber:DeactivationInputNumber, CCURE9000Event, OptionalDescription
#
# The External Detector in the Alarm Server should be created using the
# ActivationInputNumber as the activation event and the DeactivationInputNumber
# as the deactivation event.
# Example of stateful events:
# 13:14, Perimeter Break
# 15:16, Face Detection Alert
# The CCURE9000Event field 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 "Motion: Gate, Front":
# 17:18, Motion\072 Gate\054 Front
# Unicode characters are supported by the Software House 9000 Integration.
# Event mapping example:
# 19:20, インジゴビジョン
```

Each entry consists of first and second elements:

- The first element of each entry corresponds to the input number(s) associated with the External Detector in the IndigoVision Control Center suite.
  This can be one of the following:
    - one positive integer which is the activation source
    - two positive integers separated by a colon (:) where the first corresponds to the activation source and the second to the deactivation source.

  Configuring both the activation and deactivation input numbers sets the state of the Control Center detector to reflect the state of the C•CURE 9000 event when active and inactive.

► For more information about configuring the External Detector in the IndigoVision Control Center suite, see "Create a new zone and external detector for ToIv events" on page 14

• The second element of each entry is a string equal to the C•CURE 9000 event name.

► For information about Software House 9000 system configuration, *see "References" on page 5*

The C•CURE 9000 event name within the mapping cannot use the following restricted characters: {, }, \, :, and ,.

To configure events that use these characters within C•CURE 9000, replace the characters with octal escape codes.

For example, in order to produce the following mapping:

```
13, CCure\Event,13
```

The following mapping should be entered:

```
13,CCure\134Event\05413
```

To further aid identification of C•CURE 9000 events of interest and their names, you can set the Software House 9000 Integration to *Info level logging* in the logging configuration file.

► For more information on configuring logging, see "Logging Configuration " on page 23

Notice   *The IMOnline and IMOffline alarms must be unique if configured. No alarm with these alarm IDs should be configured in ToIv.conf. If these alarms are not configured or are configured to 0, then these alarms will be disabled.*

Alarms to IV configuration file names cannot include leading or trailing whitespace. As such, filenames cannot be mapped in the ToIV Alarm Servers Configuration file.

Alarms from IndigoVision Configuration File(s)

During installation one default Alarms from IndigoVision configuration file (FromIv.conf) is provided in the FromIv folder.

► For more information on using more than one Alarms to IndigoVision configuration file, *see "From IV Alarm Servers configuration file (FromIvAlarmServers.conf)" on page 22*

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

Figure 3: Example of an Alarms from IndigoVision Configuration file

```
# This file contains the FromIv mapping of IndigoVision zone and detector events
# to C-CURE 9000 events.
# Each mapping entry consists of two (optionally three) comma separated fields
# IndigoEvent, CCURE9000Event, OptionalDescription
# The first field is the IndigoVision event type, which defines whether to use a
# Zone or Detector as the activation source.
# For zone events, the only extra information required is the zone name.
# Zone definition example:
# ZONE:IvZone100
# For detector events, the zone containing the detector needs to be specified,
# along with the detector name.
# Detector definition example:
# DETECTOR:IvZone100:FrontDoor
# Assuming the Alarm Server is configured with unique zone names and
```

```
# detector names are unique within each zone, these parameters together form a
# single unit that uniquely describes the IndigoVision detector.
# This is separated from the C-CURE 9000 event name by a ','
#
# An optional third field, separated by another comma can be added
# with a description of the event mapping.
# Event mapping example:
# ZONE:IvZone,CCUREEvent
# ZONE:Lobby,CCURELobby
# DETECTOR:IvZone:IvDetector,CCURE9000Event
# DETECTOR:Lobby:Front Door,Lobby Front Door
# The IndigoEvent and CCURE9000Event names cannot contain the characters ':',
# '\', '{', '}' or ','.
# Also, any unescaped leading or trailing whitespace will be stripped.
#
# The following octal escape codes can be used to represent these characters.
# Character ':': => \072
# Character '\': => \134
# Character '{': => \173
# Character '}': => \175
# Character ',': => \054
# Character ' ': => \040 (for leading or trailing white space)
# Event mapping examples:
# ZONE:Darwin House\072 1st Floor,Darwin House\072 1st Floor
# DETECTOR:Lobby:Camera102\072 Motion,Lobby\134Camera102\072 Motion
# DETECTOR:Lobby:Camera102\072 Fault\054 Video,Lobby\134Camera102\072 VideoFault
# Unicode characters are supported by the Software House 9000 Integration.
# Event mapping example:
# DETECTOR:Rear Entrance:α door,Alpha Door
```

The first element of each entry uniquely identifies the IndigoVision alarm based on the event type (ZONE) and the zone name. The second element is a string equal to the C•CURE 9000event name.

The zone, detector, and C•CURE 9000 event names within the mapping cannot use the following restricted characters: {, }, \, :, and ,.

To configure mapping when the zone, detector, or C•CURE 9000 event names use these characters, replace the characters with octal escape codes.

For example, in order to produce the mapping of the following:

```
Zone of  "IvZone:102" to CCure 9000 event of "CCure\Event,102"
Zone of  "IvZone 103 " to CCure 9000 event of "CCureEvent103"
```

The following mappings should be entered:

```
ZONE:IvZone\072102,CCure\134Event\054102
ZONE:IvZone 103\040,CCureEvent103
```

Notice   *Alarms from IV configuration file names cannot include leading or trailing whitespace. As such, filenames cannot be mapped in the FromIV Alarm Servers Configuration file.*

To IV Alarm Servers configuration file (ToIvAlarmServers.conf)

This file contains a list of IndigoVision ToIv alarm server IP addresses that receive C•CURE 9000 events. Each Alarm Server IP address is associated with an Alarms To IndigoVision configuration file.

Figure 4: Example of a To IV Alarm Servers Configuration file

```
# List of each ToIv Alarm Server (NVR-AS)
# and its ToIv file (without .conf extension)
#
# Each mapping entry consists of two (optionally three) comma separated fields
#
# The first field is the IP address of the Alarm Server
#
# The second field is the Alarms ToIV configuration file excluding file
# extension of ".conf". All Alarms ToIV configuration files are located in
# the "ToIv" folder. For example an entry of "ToIv" indicates that the
# Alarms ToIv 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 From Iv configuration file by entering "ToIv" as the second field
# for all entries.
# IP address, ToIv file, Description (optional)
# Example:
#
# 0.0.0.0, ToIv, Default ToIv\ToIv.conf
```

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

From IV Alarm Servers configuration file (FromIvAlarmServers.conf)

This file contains a list of IndigoVision alarm server IP addresses that receive IndigoVision alarms. Each Alarm Server IP address is associated with an Alarms From IndigoVision configuration file.

Figure 5: Example of a From IV Alarm Servers Configuration file

```
#
# List of each FromIv Alarm Server (NVR-AS)
# and its FromIv file (without .conf extension)
#
# Each mapping entry consists of two (optionally three) comma separated fields
#
# The first field is the IP address of the Alarm Server
#
# The second field is the Alarms From IV configuration file excluding file
# extension of ".conf". All Alarms From IV configuration files are located in
# the "FromIv" folder. For example an entry of "FromIv" indicates that the
```

```
# Alarms From Iv configuration file is .\FromIv\FromIv.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 From Iv configuration file by entering "FromIv" as the second field
# for all entries.
# IP address, FromIv file, Description (optional)
# Example:
#
# 0.0.0.0, FromIv, Default FromIv/FromIv.conf
```

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

Logging Configuration

You can customize logging or manage backup log files in the logging configuration file.

To access the logging configuration file, navigate to the following location:

Start > All Programs > IndigoVision Software House 9000 Integration > Logging Configuration for Software House 9000 Integration

To set the category of incident which will initiate a log entry, modify `level` in the root section.

You can enter one of the following values:

- **DEBUG**

  The system records verbose logs with comprehensive details on operations.
- **INFO**

  The system records details of successful events and behavior as well as all warnings and errors.
- **WARN**

  The system records warning or error messages.

  These indicate that the Software House 9000 Integration may not be functioning correctly and may require action.
- **ERROR**

  The system records messages where a failure has occurred and action may be required.
- **FATAL**

  The system records critical errors where the integration cannot continue.

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

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

To manage how the system stores log files, set 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.

IndigoVision does not recommend changing any other settings.

6 VIDEO INTEGRATION

This sections describes how to configure and use the IndigoVision Software House 9000 Integration video integration.

Configure video

Video configuration of IndigoVision products in the C•CURE 9000 is done through the C•CURE 9000 Administration Workstation.

Use the Administration Workstation to create an IndigoVision Server. This associates an NVR with a group of cameras. You can then create and configure IndigoVision Video Cameras for each camera that is recording on the NVR.

Create an IndigoVision Video Server

1. Open the C•CURE 9000 Administration Workstation.
2. In the navigation pane, click *Video* to open the **Video** pane.
3. Select a folder, or create and name a new video folder
   ► For more information, refer to the C•CURE 9000 Video Guide
4. Right-click the video folder, select *IndigoVision Video Server*, and click *New*.
5. Enter the following details for the IndigoVision NVR:
   - **Name** – The name to give this Video Server
   - **Description** – A short description of the Video Server
   - **Time Zone** – The time zone that the server/cameras are based in
   - **IP** – The IP address of the IndigoVision NVR
   - **Default Username & Password** – ONVIF and Video Stream Manager cameras use these unless they are overridden by the camera
     ► For more information, *see "Create an IndigoVision Video Camera" on page 25*
6. Click *Save & Close*.

Create an IndigoVision Video Camera

1. Open the C•CURE 9000 Administration Workstation.
2. In the navigation pane, click *Video* to open the **Video** pane.
3. Right-click an IndigoVision Video Server you have previously created, select *IndigoVision Video Camera*, and click *New* .
4. Enter the following details for your device:
   - **Name** – The name of the camera
   - **Description** – A short description of the camera
5. Click *Configure…*.

---

6. Select whether the camera uses the IndigoVision, ONVIF, Camera Gateway or Video Stream Manager (VSM) protocol and enter the camera IP address.

7. Click **OK**.

    If you are adding a Camera Gateway or Video Stream Manager device, a dialog is shown containing a list of all available cameras on the Camera Gateway or Virtual Stream Manager at the IP address specified in step 6.

8. Select the required camera and click **OK**.

Notice   *To add Camera Gateway and Video Stream Manager devices, multicast traffic must be enabled on the network.*

---

9. Enter the details for your device. The required details vary based on protocol:
    *   IndigoVision cameras:

        Camera Type – Fixed: Select for non-PTZ cameras | Dome: Select to enable PTZ controls

        Video Profile – The video profile to use for streaming

        Audio Profile – The audio profile to use for streaming

        Connection Type – The type of connection to the camera. Best Effort/Reliable/MultiCast/Firewall-Friendly

    *   IndigoVision PTZ cameras:

        All of the above details, plus:

        PTZ Priority – The priority to use when connecting to camera PTZ control. Values are 1 to 10 (1 highest priority, 10 lowest). The default is 5.

        PTZ Protocol – The file to use for the camera PTZ control

    *   ONVIF and Video Stream Manager cameras:

        Camera Type – Fixed: Select for non-PTZ cameras | Dome: Select to enable PTZ controls

        Profile – Optional. The ONVIF profile to use for streaming both video & audio. Leave this field empty to automatically select a profile.

        Connection Type – The type of connection to the camera. Best Effort/Reliable/MultiCast/Firewall-Friendly

        Use Server Access Credentials – Tick this to enable overriding the server username & password

        Username – The username to use when accessing the camera

        Password – The password to use when accessing the camera

    *   Camera Gateway cameras:

        Camera Type – Fixed: Select for non-PTZ cameras | Dome: Select to enable PTZ controls

        Profile – Optional. The ONVIF profile to use for streaming both video & audio. Leave this field empty to automatically select a profile.

        Connection Type – The type of connection to the camera. Best Effort/Reliable/MultiCast/Firewall-Friendly

10. Click **Save & Close**.

Configure an IndigoVision Four Channel Encoder - BX Range

The Four Channel Encoder is an ONVIF encoder that supports up to four analogue devices at once. Each profile on the device represents a separate analogue device.

The Four Channel Encoder is represented in Control Center as one device with three clones. Each clone has a separate Service ID to enable video recording from each device. Therefore, to view recordings from these devices in C•CURE 9000 the Service ID must be edited to match that of the Control Center clone.

1. Create an IndigoVision Video Camera and select the correct profile for the Four Channel Encoder Clone.
   ► For more information, *see "Create an IndigoVision Video Camera" on page 25*

2. Copy the Service ID from the IndigoVision Control Center clone.

3. Right click the IndigoVision Video Camera you have created and select *Edit*.

4. Click *Edit…* beneath the Service ID.

5. Replace the Service ID with the one you copied from the Control Center clone.

6. Click *OK*.

7. Click *Save & close*.

Create templates

Templates can be created for both IndigoVision Video Servers and Cameras. Templates are used to help you quickly create similar devices.

Templates are particularly useful for configuring Four Channel Encoders because all camera details are the same except for the profile and service ID.

► For more information about templates, refer to the C•CURE 9000 Video Guide

View video

The IndigoVision Camera Viewer enables you to view live video and recorded video from cameras and NVRs, as well as control PTZ cameras.

To open the Camera Viewer, right-click the camera in the video pane, and select one of the following options:

• *View* – Display the video in a dynamic view
• *Popup View* – Display the video in a popup window
• *View in Current Tab* – Display the video in the current tab in the content area

Video viewer controls

The Camera Viewer controls change depending on whether you are watching live video or recorded video.
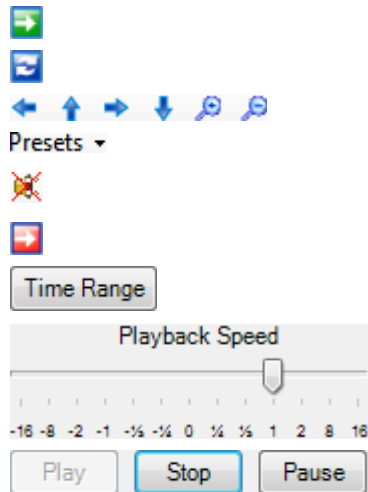
	Retrieve recorded video	Switches to the Playback view
	Reconnect	Attempts to reconnect to the camera
← ↑ → ↓ 🔍 🔍	**PTZ controls**	Control a PTZ camera - Pan/Tilt/Zoom
Presets ▾	**Presets**	Move a PTZ camera to a preset position
🔇	**Toggle audio**	Enables or disables the audio from the camera
	Go to live video	Switches to the Live view
Time Range	**Time Range**	Select the start and end dates & times for the playback duration
Playback Speed -16 -8 -2 -1 -⅓ -¼ 0 ¼ ⅓ 1 2 8 16	**Playback Speed**	Controls the playback speed of the recorded footage
Play Stop Pause	**Playback controls**	Start, stop, or pause the recoded footage

7 TROUBLESHOOTING

Server installation fails

If the following error is experienced during the server installation:

```
The server installation fails (46139) error: Error 25541. Failed to open XML file
C:\Program Files (x86)\Tyco\CrossFire.
```

Then confirm the following:

- Software House C•CURE 9000 is installed on the machine.
- The installation folder specified during the installation of the IndigoVision Software House 9000 Integration matches the Software House C•CURE 9000 installation folder on the machine.

Server installation fails due to SQL errors

If the following error is experienced during the installation of the Integration:

```
An error occurred while connecting to 'ACVSCore' database on SQL server
'localhost\SQLEXPRESS'
```

The Alarm and Events integration will work. The Video Integration will not work, as expected.

To resolve the issue, follow these steps after the installation has completed:

1. Open Microsoft SQL Server Management Studio.
2. Connect to the Software House ACVSCore database using an SQL user who can connect, create tables and alter tables.
3. Locate the script *IndigoVisionTables.sql* in the Integration installation directory, typically *C:\Program Files (x86)\IndigoVision\Integration\Software House 9000*.
4. Run the script, or press F5 to run the script.
5. Ensure the command has completed successfully.
6. Open an Administrator command prompt.
7. Navigate to *Tyco\Crossfire\Tools*, where C-CURE has been installed, typically *C:\Program Files (x86)*.
8. Type:
```
insertlicenseoption /U /S:localhost\SQLExpress /N:"Indigo Vision Integration"
/A:"IndigoVision" /G:819f7d8a-0c50-4633-9a94-6e934c6b51b1 /C:0 /P:89
/ObjectType:"IndigoVision.NextGenConnectedProgram.Video.Objects.IndigoVisionVideo
Server"
```

Notice	*Replace **localhost\SQLExpress** in step 8 with the SQL server name and instance, for example* `localhost` *for Microsoft SQL Server Full on the local PC.*

9. Ensure the command returns the following:

```
Option Indigo Vision Integration with GUID:819f7d8a-0c50-4633-9a94-6e934c6b51b1
updated in the database...
```

Error when creating an IndigoVision camera

If either of the following errors are experienced when creating an IndigoVision camera within
C-CURE 9000 Administration Workstation:

```
Invalid Object name: ACVSCore.DBO.IndigoVisionVideoCamera
A Database error occurred processing the current request.
```

Then follow the steps outlined in the server installation failure process.

► For more information, *see "Server installation fails due to SQL errors" on page 29*

IndigoVision Video Server not available in Administration Workstation

If it is not possible to add an IndigoVision Video Server in the **Video** section of the C•CURE
Administration Workstation, then confirm the following:

- The entry `IndigoVision.NextGenConnectedProgram.Video.Objects` is
  listed in the **Database** tab of the C•CURE Server Configuration Application.
- An IndigoVision license is correctly installed for the IndigoVision Software House 9000
  Integration. Open the Tyco License Manager, and navigate to the **C•CURE 9000** tab.
  The entry `Indigo Vision Integration` must be present.
- The installation folder of the IndigoVision Software House 9000 Integration, specified
  during the installation of the Client Integration (by default **C:\Program Files
  x86\Tyco**), matches the installation folder on the machine.
- Open the **Server Configuration Application** and restart the following services:
  - Crossfire Framework Service
  - Crossfire Server Component Framework Service
- If the issue is still present, follow the steps in the server installation failure process.
  - ► For more information, *see "Server installation fails due to SQL errors" on page 29*

Error: Section System not found in the system configuration file.

If you see an error in the log file `Section System not found in the system
configuration file.` and you are upgrading from v.3.2 or earlier of the Software House
9000 Integration, you need to manually configure the configuration file.

► For more information, see "Installing with multiple network adapters or IP addresses" on
page 10

Integration cannot start

If the PC running the IndigoVision Software House 9000 Integration has multiple IP
addresses, then you must provide an IP address in the System configuration file. This is the
IP address configured as the **External System IP address** within Control Center.

If the IndigoVision Software House 9000 Integration does not start properly from C•CURE
9000 Server Configuration Application or Windows Services, do one of the following:

- Open **Windows Event Viewer** and navigate to **Windows Logs > Application**.

  Find one or more events logged at `Error` level and with Source IndigoVision IntegrationCore Service.

  In the General field, you can see a description of the problem which prevents the service from starting.

- Open the most recent log file and look at the latest 2 messages marked as FATAL.

  If the message described a configuration error, follow the guidance in the message and configuration file.

  If a FromIv or ToIv event configuration file is wrongly configured, then an error message will be provided for each issue.

The following log message indicates a license failure:

```
2016-07-15 10:11:32,175 [FATAL][IntegrationCore.Core.IntegrationCoreManager]: License
check has failed. Ensure that the correct license dongle is attached.
```

Ensure that the license dongle is attached if applicable, and that the software license is applied.

If an IP address is not configured, the Integration fails to start with the following error message:

```
2015-06-24 16:58:05,123 [FATAL] [IntegrationCore.Core.EventManager]: Parameter
IntegrationModuleIP in section System is mandatory since the machine has multiple IPs
configured.
```

► For more information about setting the Integration IP address, see "System Configuration Files" on page 17

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 23

2. Verify that the Integration is sending events to the nominated Alarm Server by opening the most recent Integration log file and check for messages stating that the alarm has been sent e.g.
   ```
   2016-06-24 15:21:56,345 [INFO ] [IntegrationCore.Core.IntegrationCoreManager]:
   ToIv stateless event sent to Alarm Server '10.1.219.11' with external input
   number '20' from IP '10.1.219.40'. The UTC time of the event was '24/06/2016
   14:21:56'.
   ```
   If the alarm is generated as expected go to step 3.

   If step 2 does not identify that an alarm has been sent for the C•CURE 9000 event of interest then look to see if the Integration is receiving the event but has not been configured, for example:
   ```
   2016-02-16 13:38:18,536 [INFO ] [IntegrationCore.Core.EventManager]: ToIv
   event 'Example Event' is not configured to send to any Alarm Server.
   ```
   If the event is not seen in the log file then refer to C•CURE 9000 documentation on how to set up and configure the C•CURE 9000.

   If the event is seen in the log file then the Alarms To IV configuration file (**ToIv.conf**) is not correctly configured to forward this event to the Control Center suite.

3. Verify that the corresponding zones and external detectors have been created and that the zones have been set and the external detectors have been enabled in Control Center. In the **Site Setup** mode select the relevant **Site** on **Alarms** explorer then:

a. Click on the ***External Systems*** tab. Ensure that an External System with the IP address of the PC running the Software House 9000 Integration has been created.

If the PC running the Software House 9000 Integration has multiple IP addresses, ensure that the `IntegrationModuleIP` parameter has been configured to the IP address that you wish to use within Control Center.

b. Click on the ***Zones*** tab. Ensure that a zone has been created containing an external detector with Input Number being the event number identified from step 2 above. Also ensure that the external system is correct. The external detector must be enabled and the zone must be set.

c. Ensure that the zone belongs to the nominated Alarm Server. Right-click on the zone, select ***Properties*** then on the ***Zone*** tab ensure that the Alarm Server is the same as that configured in the ToIV Alarm Servers configuration (***ToIvAlarmServers.conf***) file for the Software House 9000 Integration.

Deactivating an event in C•CURE 9000 does not deactivate the detector in Control Center

If a detector is active in Control Center, and it does not deactivate when a configured event in C•CURE 9000 is deactivated, do the following:

1. Check the Alarms to IndigoVision configuration file (ToIv).

   Ensure that a deactivation input number has been configured for the C•CURE 9000 event.

   ► For more information, see "Alarms to IndigoVision configuration file(s) " on page 18

2. Enable Info level logging.

   ► For more information about configuring logging, see "Logging Configuration " on page 23

3. Check that the Integration is sending deactivation events to the Alarm Server.

   • If you can see log messages similar to the following:

   ```
   2016-06-24 15:21:56,345 [INFO ] [IntegrationCore.Core.IntegrationCoreManager]:
   ToIv stateless event sent to Alarm Server '10.1.219.11' with external input
   number '20' from IP '10.1.219.40'. The UTC time of the event was '24/06/2016
   14:21:56'.
   ```

   where the external input number is the deactivation input number configured for the C•CURE 9000 event, proceed to the next step.

   • If you can see log messages similar to the following:

   ```
   2016-06-24 15:21:56,345 [INFO ] [IntegrationCore.Core.EventManager]: ToIv
   event 'Example Event' is not a configured stateful event
   ```

   then the event has not been configured with a deactivation input number within the Alarms to IndigoVision configuration file.

   ► For more information, see "Alarms from IndigoVision Configuration File(s) " on page 20

4. Check that an external detector has been created with a deactivation event that uses the deactivation input number configured within the Alarms to IndigoVision configuration file.

   ► For more information on creating detectors with deactivation events, see "Create a new zone and external detector for ToIv events" on page 14

Notice	*If an event has an associated activate or deactivate manual action, this may override the manual actions performed by the integration.*
	When you migrate from legacy to recommended FromIv detector behavior, any previously active events may have an associated activate manual action, which expires within one hour.

Notice	*You should not manually activate or deactivate FromIv events within C•CURE 9000. You can view the manual action associations with an event in C•CURE 9000 through the C•CURE 9000 software.*

Alarms not appearing in C•CURE 9000

If alarms are not appearing in C•CURE 9000 then the following end-to-end check for a single alarm may help to determine the source of the problem.

1. Check that the Integration has been configured to send alarms to C•CURE 9000 in the system configuration file.

2. Enable debug level logging.

   Do this by setting Level=debug in the [Log] section of the system configuration file, then restart the 'IndigoVision Software House 9000 Integration' service. This will allow the to log all alarms and events received from the Alarm Server, not just those that have been mapped in the Alarms From IV configuration file.

3. Verify that the Integration is sending alarms or events to C•CURE 9000 by opening the most recent Integration log file and check for messages stating that the alarm has been sent, for example;

   ```
   2016-06-24 15:21:56,345 [INFO ]
   [IndigoVision.NextGenConnectedProgram.Video.Server.FromIv.FromIvModule]:
   FromIv event 'ExampleEvent' successfully activated in C-CURE 9000.
   ```

   If step 3 identifies that the alarm is sent to C•CURE 9000 then go to step 4.

   If step 3 does not identify that an alarm has been sent for the IndigoVision alarm of interest then look to see if the Integration is receiving the event but has not been configured, for example:

   ```
   2016-02-16 13:38:18,536 [INFO ][IntegrationCore.Core.EventManager]:
   DETECTOR:MyZone:MyDetector from 10.1.219.1 has changed state to Triggered,
   however it is not configured in the FromIv configuration files.
   ```

   If the alarm is seen in the log file as not being configured then the Alarms From IV configuration file and/or Alarms Server configuration file is not correctly configured to forward this event to the C•CURE 9000.

4. On the C•CURE 9000 server, verify that the C•CURE 9000 services are running. An easy way to check this (and start the services if necessary) is to use the C•CURE 9000 Server Configuration Application available as a shortcut via ***Start > All Programs > Tyco > Server Configuration***.

5. If the services are running then check the Application Event Log on the C•CURE 9000 Server machine for any errors related to IndigoVision or C•CURE 9000 and take action as necessary. If no errors refer to C•CURE 9000 documentation.

C•CURE 9000 events remain active for one hour before deactivating

To set FromIv detector deactivations within the Control Center system to deactivate C•CURE 9000 events, open the System Configuration File, and set the parameter `EnableLegacyFromIvDetectorBehaviour` to `False`.

If the parameter is not set, then the following message is displayed in the log file when the logging level is set to Info:

```
2016-06-24 15:21:56,345 [INFO ]
[IndigoVision.NextGenConnectedProgram.Video.Server.FromIv.FromIvModule]:
Ignoring deactivation for event FromIvExampleEvent as legacy behaviour is
enabled.
```

► For more information, see "System configuration file (System.conf)" on page 17

FromIv zone events always remain active for one hour before deactivating.

IndigoVision recommends that you configure FromIv detector events to have a synchronized system.

Unable to discover Camera Gateway or Video Stream Manager devices

If you are unable to find Camera Gateway devices:

1. Verify that the IP address for the Camera Gateway machine has been provided, not the IP address of the camera.
2. Ensure that multicast networking is enabled. The Camera Gateway only supports multicast discovery.
3. Use the Service Configuration Tool on the Camera Gateway machine to ensure that the correct IP address has been configured.
4. Use Camera Gateway Administrator to check the online status of the cameras.
5. Check that the IndigoVision Camera Gateway Interface and Camera Gateway Core services are running on the Camera Gateway machine.

► For more information about configuring the Camera Gateway, refer to the IndigoVision Camera Gateway Admin Guide

If you are unable to find Video Stream Manager devices:

1. Verify that the IP address for the Video Stream Manager machine has been provided, not the IP address of the camera.
2. Ensure that multicast networking is enabled. The Video Stream Manager is only supported using multicast discovery.
3. Use the VSM Service Configuration Tool on the Video Stream Manager machine to ensure that the correct IP address has been configured.
4. Use VSM Administrator to check the online status of the cameras.
5. Check that the IndigoVision Video Stream Manager service is running on the VSM machine.

► For more information about configuring the Video Stream Manager, refer to the IndigoVision Video Stream Manager Admin Guide

Software House 9000 Integration is slow to start

If the Software House 9000 Integration cannot access the internet, then a standard security check may cause the Software House 9000 Integration service to take up to a minute to start.

To resolve this, disable **Check for publisher's certificate revocation** for the Local System user in the registry key.

1. Start the Windows Registry Editor.
2. Navigate to **HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\TrustProviders\Software Publishing.**
3. Select **State**.
4. Set **Value data** to 23e00 for **Base: hexadecimal** or 146944 for **Base: decimal**.
5. Click **OK**.
6. Close Registry Editor.

   Check for publisher's certificate revocation is no longer enabled.