IndigoVision

Microsoft SQL Server Integration

Administrator's Guide

This manual was published on Tuesday, November 6, 2018.

Document ID: IU-IM-MAN030-3

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

Contact address

IndigoVision Limited

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

TABLE OF CONTENTS

1 ABOUT THIS GUIDE

This guide is provided for system administrators integrating a Microsoft SQL Server database with IndigoVision Control Center.

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

- Control Center Help

   Start > IndigoVision > Control Center > Control Center Help

   Located on the Control Center server.
- IndigoVision Integrations

   http://www.indigovision.com/products/integration
- IndigoVision Control Center Installation Guide

   Located on the Control Center CD.

Integration-specific references

1. Microsoft SQL Server documentation[1]

   https://msdn.microsoft.com/en-us/library/mt590198.aspx

2. SQL Server Management Studio

   https://msdn.microsoft.com/en-us/library/mt238290.aspx

---

[1]Documentation for all supported versions of Microsoft SQL Server can be found here.

---

2 OVERVIEW

The IndigoVision Microsoft SQL Server Integration allows integration with a Microsoft SQL Server database to send events to the IndigoVision Control Center suite.

The Microsoft SQL Server Integration can be used to integrate events from any system that uses a Microsoft SQL Server database through the use of triggers on tables.

This document explains how to install and configure the Microsoft SQL Server Integration.

Compatibility

Please ensure you have properly installed, configured, and licensed the Microsoft SQL Server.

System requirements

The Microsoft SQL Server Integration can be installed on the following Windows® operating systems with latest service packs applied:

- Windows® Server 2016
- 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)

Licensing

The Microsoft SQL Server 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 Microsoft SQL Server 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 Microsoft SQL Server Integration.

► For more information about troubleshooting the USB license, *see "License issues" on page 21*

Notice   *The Microsoft SQL Server Integration must not be run on the same server as any other licensed IndigoVision software.*

Microsoft SQL Server licenses

No specific licenses are required by Microsoft to integrate Microsoft SQL Server with the IndigoVision Microsoft SQL Server Integration.

The IndigoVision Microsoft SQL Server Integration is compatible with Microsoft SQL Server Express, the free edition of Microsoft SQL Server.

The following versions of Microsoft SQL Server are supported:

- Microsoft SQL Server 2008
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017

Notice   *The IndigoVision Microsoft SQL Server Integration should not be run on the same server as any other licensed IndigoVision software.*

---

3 INSTALLATION

This section describes how to install the Microsoft SQL Server Integration.

If you have an IndigoVision Microsoft SQL Server Integration USB license dongle, ensure it is inserted into the machine that you are installing the software on before beginning the installation.

To install the Microsoft SQL Server Integration, follow these steps:

1. Download the Microsoft SQL Server Integration from the support section of the IndigoVision Website.

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

2. Run the *setup.exe* file and follow the on-screen instructions. The Microsoft SQL Server Integration is installed to:

   C:\Program Files (x86)\IndigoVision\Integration\Microsoft SQL Server Integration by default.

3. If the Microsoft .NET 4.7.1 Framework or later is not installed, then you are prompted to install it.

4. Once the installation is complete, request and install a software license for the Microsoft SQL Server Integration using the License Manager tool.

   ► For more information, *see "License the integration" on page 10*

5. Configure the Microsoft SQL Server Integration.

   ► For more information, *see "Configuration" on page 11*

6. Start the IndigoVision Microsoft SQL Server Integration service using the Windows® services utility.

Upgrading

This section describes the actions necessary to upgrade from version 1.0.1 and earlier.

Database and Table

The IndigoVision Microsoft SQL Server Integration is compatible with database and the `IV_LOG` table configured in version 1.0.1 or earlier. No modifications are required.

It is recommended that Query Notifications are enabled to receive events in a more efficient manner. Additionally the date and time of the original event can be used by adding the `EVENT_DATE` field.

► For more information on the recommended table structure, *see "Configuration" on page 11*

Configuration

When upgrading from version 1.0.1 or earlier, the system configuration will be ignored and will need to be reset. Your existing configuration will be stored in the following directory:

C:\ProgramData\IndigoVision\Integration\MS-Sql.

The values set in your *system.conf* file should be entered into the relevant pages on the Configuration tool. Additionally, the events entered into the *Tolv.conf* file should be entered into the **Configure Alarm Servers for Receiving Events** page.

► For more information, *see "Configuration" on page 11*

Specify Service User

Specify the user details for the IndigoVision Microsoft SQL Server Integration to connect to the Microsoft SQL Server using Windows authentication. This is achieved by configuring the service to log on as a specific Windows user account.

During installation you are prompted to provide the username and password for the Windows user account. Include the domain name in the username, for example `CompanyDomain\SqlWindowsUser` or `MachineName\SqlWindowsUser`.

For configurations using SQL Server authentication, or when the `Local System` account has permissions on the database (for example, as is standard with SQL Server Express), specifying the service user is not required.

► For more information on using SQL Server authentication, *see "Configure SQL login for SQL Server authentication" on page 15*

Alternatively, configure the service user from the Windows® services.

Notice *For a Windows user account to be used to run a service it must be listed in the **Log on as a service** policy within the **Local Policies > User Rights Assignments** section of **Local Security Policy**.*

License the integration

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

You can manage the license using the License Manager tool, which is installed as part of the Microsoft SQL Server 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.

4 CONFIGURATION

To integrate Microsoft SQL Server events into the IndigoVision Alarm Server, perform the following steps:

1. Run the Integration Configuration tool for Microsoft SQL Server Integration – *see "Integration Configuration tool" on page 11*.

2. If you are using SQL Server authentication rather than Windows authentication, you will need to configure the credentials for the Integration to connect – see "Configure SQL login for SQL Server authentication" on page 15.

3. Create the `IV_LOG` table in the Microsoft SQL Server database – *see "Create the event table" on page 14*.

4. Optionally, create a trigger to automatically insert records from a table into the `IV_LOG` Table – *see "Create a trigger" on page 14*.

5. IndigoVision Control Center configuration:

   a. Create a new external system – *see "Create a new external system" on page 13*.

   b. Create a new zone and external detector for SQL Server events – *see "Create a new zone and external detector for Microsoft SQL Server events" on page 14*.

6. Logging configuration – *see "Logging configuration" on page 16*.

7. Enable the service broker on the Microsoft SQL Server database to use query notifications.

   This allows events to be forwarded to Control Center in a quicker and more efficient manner. If the service broker cannot be enabled on the database, then the Integration will poll the table for new events every 5 seconds – *see "Using query notifications" on page 15*.

Integration Configuration tool

The Integration Configuration tool can be used to configure the events and system settings for the Microsoft SQL Server Integration:

1. Run the Integration Configuration tool for Microsoft SQL Server Integration.

   Start > All Programs > IndigoVision Microsoft SQL Server Integration > Configure Microsoft SQL Server Integration

2. Optionally provide the ***Alarm Server IP*** for **System Events**.

   System Events report the status of the Microsoft SQL Server Integration and its connection to the Microsoft SQL Server.

3. Provide the IP address of the Microsoft SQL Server Integration.

   - When the IndigoVision Microsoft SQL Server 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 ***Alarm Server IP*** for **System Events** was provided, configure **System Events**.

---

5. Provide the *Microsoft SQL Server Database Host*.
   - Typically, this will be the host name of the machine running the Microsoft SQL Server.
   - This setting can be omitted if the Microsoft SQL Server Integration is installed on the same machine as the Microsoft SQL Server.
6. Provide the *Microsoft SQL Server Database Instance* to which the Integration should connect.
   - This is required if the *Database Host* was omitted in the previous step and can be left blank otherwise.
7. Provide the *Database Name*.
   - This is the name of the database where the *IV_LOG* table is located.
8. Specify whether SQL authentication should be used.
   - If this is disabled, the current Windows user will be used by the Integration to connect to the Microsoft SQL Server Instance.
   - If this is enabled, the Integration will use SQL authentication. The login credentials should be specified using the Configure SQL login for Microsoft SQL Server Integration tool – *see "Configure SQL login for SQL Server authentication" on page 15*.
9. 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 detectors to be configured, or the Alarm Server has detectors for other sources configured (such as Advanced Analytics or Digital Input detectors), then you can split the configuration across multiple Alarm Servers.
10. Configure the event mappings for each Alarm Server. The event mapping file is known as a ToIv configuration file (events to IndigoVision) – see "Configure ToIv configuration file" on page 14.
    - The ToIv configuration file for the Alarm Server will open in a new window.
11. Click *Finish* to close the dialog and save your settings.
    - You have the option to restart the service at this point, or to manually restart later.
    - Any changes made will not take effect until the service restarts.

Configure Microsoft SQL Server custom events

Custom events can be created from the **Configure Microsoft Server Events** page of the Configuration tool. One mapping entry is created per line and each entry is a comma-separated pair.

Figure 1: An example alarms to IndigoVision configuration file(s)

```
# This file contains the ToIv mapping of Microsoft SQL Server alarms to
# IndigoVision external event input numbers.
#
# Each mapping entry consists of two ( optionally three ) comma separated
# fields.
#
# InputNumber, EventName, Optional Description
#
# 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 event name, which mapped to
# the IV_ALARM_STRING field in the IV_LOG table on the database.
```

```
#
# The EventName can be a numeric or text value (such as char, varchar & nchar).
# Examples of an event without the optional description:
# 10, Main Door Opened
# 11, 1234
# 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, PN12-EV6, Panel 12 (Staff Room) Door opened
# Unicode characters are supported by the IndigoVision Microsoft SQL Server
# Integration. In order to receive Unicode EventName values, the
# IV_ALARM_STRING field in the IV_LOG table must be a type that supports
# Unicode, for example nvarchar.
# Example of EventName with Unicode characters:
# 13, δ Lab Door Forced
# The EventName received from the database will be trimmed with any leading or
# trailing white space removed. This allows for use of fixed length field types
# like char or nchar where spaces are appended by SQL Server.
# The EventName cannot contain the characters ':', '\', '{', '}' or ','.
# The following octal escape codes can be used to represent these characters.
# Character ':': => \072
# Character '\': => \134
# Character '{': => \173
# Character '}': => \175
# Character ',': => \054
# Example using octal escape codes for the EventName "Access: Door, Main":
# 14, Access\072 Door\054 Main
```

The first element of each entry is the positive integer associated with the IndigoVision external event ID corresponding to the event. The second element is a string that is equal to the name of the event. The source of this name is the IV_ALARM_STRING field for new entries in the IV_LOG table.

► For more information about the IV_LOG table, *see "Create the event table" on page 14*

To further aid identification of events of interest and their 3rd Party Event names, the Alarms to IV configuration file names cannot include leading or trailing whitespace. Therefore filenames can not be mapped in the ToIv Alarm Servers Configuration file.

Notice   *The IMOffline and IMOnline 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.*

Configure IndigoVision Control Center

If the Integration Online, Integration Offline, Third Party Offline or Third Party Online system events have been configured, then they must be configured in Control Center.

Create a new external system

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

Create a new zone and external detector for Microsoft SQL Server events

Create zones and detectors for the configured Microsoft SQL Server events using one of the following methods:

- Manually create the zones and external detectors within Control Center.
    a. Add a new zone for each unique alarm you want to report in Control Center.
    b. 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 configuration file of the Microsoft SQL Server Integration.

Notice　　*IndigoVision recommends that you configure the zone name description in Control Center to closely match the Microsoft SQL Server event name. This will help to ensure there is no confusion in correlating events.*

- Or use the IndigoVision Import Alarm Sources tool to automatically create zones and detectors for each event within a ToIv configuration file.
    a. Edit the ToIv configuration file, accessible through the Integration Configuration tool, with all the supported events.
    b. Configure an IndigoVision Alarm Server using the IndigoVision Import Alarm Sources tool.
    c. You can download the Import Alarm Servers tool from the IndigoVision website.
    d. Every time an event is added to ToIv configuration file, run the tool again to create new zones and detectors.

Microsoft SQL Server configuration

Create the event table

Create a table called `IV_LOG` in the database. The IndigoVision Microsoft SQL Server Integration monitors this table for new events.

The following outlines the fields that are read by the IndigoVision Microsoft SQL Server Integration. Any additional fields in the table will be ignored.

Table 1:　　　`IV_LOG` Table

Column name	Type	Mandatory	NULLs allowed	Description
IV_ALARM_STRING	nvarchar	Yes	No	The event name. The type can be an alternate char type or numeric.
EVENT_DATE	datetime	No	Yes	The date & time that the event occurred. If not provided then the date and time that the event is received by the Integration will be used. The time must be specified as UTC time.

An example SQL script showing how to create the table with the recommended structure is provided in the *SQL Scripts* folder. This is found using the shortcut in the *Start* menu.

Create a trigger

The IndigoVision Microsoft SQL Server Integration is used to integrate events from any system that uses a Microsoft SQL Server database through the use of triggers on tables. This allows automatic insertion of rows into the `IV_LOG` table.

An example SQL script showing how to create a trigger is available in the *SQL Scripts* folder. This is found using the shortcut in the *Start* menu.

Configure SQL login for SQL Server authentication

The IndigoVision Microsoft SQL Server Integration supports using either Windows authentication or SQL Server authentication to connect to the Microsoft SQL Server database.

If SQL Server authentication is enabled then you must specify the SQL Server login details using the Configure SQL Login tool.

1. Run the tool from *Start > IndigoVision Microsoft SQL Server Integration*
2. Enter the *LoginName* and *Password* for a valid SQL Server login
3. Click *Save*
4. Click *Yes* to restart the service using the new credentials

   Alternatively, click *No* and then manually restart the service later using the **Service Control Manager** under *Administrative Tools* in the Windows Control Panel.

The recommended method of authenticating with the Microsoft SQL Server is using Windows authentication.

► For information on configuring Windows authentication, *see "Specify Service User" on page 10*

Using query notifications

Query notifications is a feature of Microsoft SQL Server that allows for efficient retrieval of events by providing a notification when new records have been added.

This feature is supported by the IndigoVision Microsoft SQL Server Integration. Using query notifications ensures that the event is forwarded to Control Center immediately after it has been added to the table. In systems with only periodic events this also reduces the database load by performing fewer database transactions.

To use query notifications, you must enable the Service Broker, which can be performed using Microsoft SQL Server Management Studio. The following instructions apply to Microsoft SQL Server Management Studio version 10.0.1600.22:

1. Stop any services using the database, such as the Integration.
2. Connect to the Microsoft SQL Server using Microsoft SQL Server Management Studio
3. Right-click on the database and select *Properties*
4. Select *Options*
5. Under the *Service Broker* section, change *Broker Enabled* to `true`
6. Click *OK*

Alternatively, the following SQL query can be performed:

```
ALTER DATABASE MyDatabaseName SET ENABLE_BROKER;
```

► For more information on enabling query notifications, *see "Integration-specific references" on page 6*

If the service broker is not enabled on the Microsoft SQL Server database, or if the SQL user does not have permission to use them, then the IndigoVision Microsoft SQL Server Integration will check the table for new events every 5 seconds.

Logging configuration

Logging is configured with a separate file, allowing customization of the logging and the management of backup log files. To access this file, navigate to the following location:

Start > All Programs > IndigoVision Microsoft SQL Server 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 behaviour as well as all warnings and errors.
- **WARN**: All messages logged are warning or error messages that indicate that the Microsoft SQL Server Integration 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 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.

5 TROUBLESHOOTING

This chapter provides troubleshooting information for the Microsoft SQL Server Integration.

Service 'IndigoVision Microsoft SQL Server Integration' (SQLServerIM) could not be installed

The installer has been unable to install and configure the service. This may be due to the following reasons:

1. The Windows® services control panel is open. Ensure that it is closed along with any properties windows then click *Retry*.

2. During installation the logon details for a Windows account have been provided but the Windows account does not have permission to run as a service.

   For a Windows user account to be used to run a service it must be listed in the *Log on as a service* policy within the *Local Policies > User Rights Assignments* section of *Local Security Policy*.

3. During installation the logon details for a Windows account has been provided but the Windows account name is incorrect.

   Ensure that the Username includes the domain, which for a local account is the name of the machine, for example, when configuring the Windows account SqlUserAccount on a PC with the hostname Server3 the Username would be `Server3\SqlUserAccount`.

► For more information about configuring the Windows account, *see "Specify Service User" on page 10*

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 about configuring logging, *see "Logging configuration" on page 16*

   This allows the Integration to log all alarms and events received from the Microsoft SQL Server, not just those that have been mapped in the Alarms To IV configuration file.

   For more detailed information, including advanced errors reported by Microsoft SQL Server and the connection string used to connect. This provides the most verbose level of log messages and is intended for advanced use. It is not recommended that `DEBUG` level logging is used in normal operation.

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.

For example,

```
2016-02-16 13:38:23,537 [INFO ]
[MicrosoftSqlServerIntegration.Database.DatabaseTransactionHa
ndler]: Event 'Event1' received 16/02/2016 13:38:22.
2016-02-16 13:38:23,550 [INFO ]
[IntegrationCore.Core.Event.BindingKit]: ToIv stateless event
sent to Alarm Server '10.1.219.11' with external input number
'12' from IP '10.1.219.1'. UTC time of the event was
'16/02/2016 13:38:22'.
```

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 Microsoft SQL Server database 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 stateless event
'Example Alarm' is not configured to send to any Alarm
Server.
```

If the event is seen in the log file, then the Alarms to IV configuration is not correctly set to forward this event to the Control Center suite. This can be amended by running the Configure Microsoft SQL Server Integration tool.

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 follow these steps:

a. Click on the **External Systems** tab. Ensure that an External System with the IP address of the PC running the Microsoft SQL Server Integration has been created.

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. This can be confirmed using the Configure Microsoft SQL Server Integration tool.

Service does not start

If the IndigoVision Microsoft SQL Server Integration does not start properly from Windows Services, then :

1. Open Windows **Event Viewer**

2. Navigate to *Windows Logs > Application*

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

In the *General* field, a description of the problem which prevents the service from starting is shown.

Alternatively, open the most recent log file and look at the latest 2 messages marked as `FATAL`.

If you receive the following error, then the user account configured for the service does not have permission to log on as a service:

`Error 1069: The service did not start due to a logon failure`

To resolve this, either use an alternate user account or add the user account to the list of users who can log on as a service:

1. From the *Start* menu, run `secpol.msc`
   The **Local Security Policy** window is shown.
2. Navigate to *Local Policies > User Right Assignments* in the *Security Settings* tree
3. Double click *Log on as a service* in the *Policy* list
4. Click *Add User or Group...*
   The **Select Users or Groups** window is shown.
5. Enter or select the user account intended for use with the IndigoVision Microsoft SQL Server Integration, and click *OK*
6. Click *OK* to confirm and close the **Log on as a service Properties** dialog
7. Close the **Local Security Policy** window
8. Start the Integration from Windows® Services

Notice *The user account configured for the IndigoVision Microsoft SQL Server Integration to log on as is used for Windows authentication with the Microsoft SQL Server.*

► For more information about setting up the Windows user account for Windows authentication, *see "Specify Service User" on page 10*

Unable to connect to the Microsoft SQL Server

If you are unable to connect to the Microsoft SQL Server, check the following:

1. Ensure that the service is configured to log on with a Windows user account that has permissions to access the database on the specified Microsoft SQL Server.
   If using SQL Server authentication, verify that connecting using SQL Server authentication has been enabled in the System configuration file and the SQL login details have been provided using the Configure SQL Login tool.
2. Verify that the `DatabaseHost`, `DatabaseName` and if required, `DatabaseInstance`, have all been correctly provided and that the specified database exists.
   Using Microsoft SQL Server Management Studio, attempt to log in to the server and verify that you can access the database. Specify the *Server name* as either the `DatabaseHost` if using the default instance, or `DatabaseHost\DatabaseInstance` to specify a named instance.

Events take several seconds to be triggered within IndigoVision Control Center

The IndigoVision Microsoft SQL Server Integration supports query notifications to forward events to IndigoVision Control Center suite when inserted into the database. If query notifications are not enabled on the database, then the IndigoVision Microsoft SQL Server Integration retrieves events every 5 seconds.

If query notification could not be enabled you will see the following error in the log files:

```
2016-02-16 12:34:56,789 [WARN ][MicrosoftSqlServerIntegration.Database.Database
Manager]: Query notifications could not be enabled. Events will be retrieved via
polling.
```

► For more information about configuring query notifications, *see "Using query notifications" on page 15*

Detector activation times are incorrect in IndigoVision Control Center

The EVENT_DATE field in the IV_LOG table requires the datetime value to be in UTC time. If the third party system uses local time then the time for detector activations will be incorrect within Control Center.

If the third party system cannot be configured to provide UTC times then update the trigger to not provide a value for the EVENT_DATE field. If no value is provided then the default behavior is to use the current UTC time.

Also ensure that time for the PCs for the SQL Server and Integration are also synchronised through NTP as well as the Alarm Server.

► For more information on configuring the NTP, refer to the IndigoVision Control Center Install Guide.

Microsoft SQL Server Integration is slow to start

If no internet access is available then a standard security check may cause the Microsoft SQL Server Integration service to be slow to start, taking up one minute.

This is resolved by disabling 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\Trust Providers\Software Publishing.
3. Double-click the *Value* called *State*.
4. Set the *Value* data to 23e00 for hexadecimal or 146944 in decimal.
5. Click *OK*.
6. Quit **Registry Editor**.

Optionally, perform the same steps for the default registry key:

```
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust
Providers\Software Publishing.
```

Notice   *If you have configured a different user to run the service (see "Specify Service User" on page 10) then* `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.

License issues

You should not encounter license issues if the Microsoft SQL Server Integration 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 Microsoft SQL Server Integration, 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, then 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**, then expand the list.
5. Check that the following are listed:
   - SafeNet Inc. Sentinel HL Key
   - SafeNet Inc. HASP Key
   - SafeNet Inc. USB Key