IndigoVision

Maxxess Integration

Administrator's Guide

IndigoVision

THIS MANUAL WAS PUBLISHED ON THURSDAY, FEBRUARY 21, 2019.

DOCUMENT ID: IU-IM-MAN034-1

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 the Maxxess system with 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:

- Control Center Help
  Start > IndigoVision > Control Center > Control Center Help
  Located on the Control Center workstation, by default
- IndigoVision Control Center Installation Guide
  Located on the Control Center CD.
- Integration Modules http://www.indigovision.com/products/Integration
- eFusion & eAXxess Installation & Configuration Guide, Software Version 6.0.x

2 OVERVIEW

The Maxxess Integration allows alarms from a Maxxess system to integrate into IndigoVision Control Center suite. Operators can acknowledge and delete Maxxess alarms by acknowledging or clearing the corresponding zone alarm within IndigoVision Control Center. It also allows Control Center operators to remotely action Maxxess doors and outputs from within Control Center.

This document explains how to install and configure the Maxxess Integration.

Compatibility

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

System requirements

You can install Maxxess Integration 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)

If a firewall is enabled on your system, ensure that you add the Maxxess Integration executable

IndigoVision.IntegrationCore.exe to the list of exceptions.

Maxxess requirements

The Maxxess Integration is compatible and has been tested with Maxxess eFusion 6.2.4.

The Maxxess Integration license must have one MultiPort license dedicated to this integration.

You can install the Maxxess Integration on either the same machine as the Maxxess, or on a different machine. If installing on a remote machine, ensure that both are configured to use the same time zone.

If a firewall is enabled on Maxxess eFusion machine, ensure that you add an exception for TCP port 1705 for incoming connections.

Licensing

The Maxxess Integration is a licensed product, which you can install on a physical or virtual machine.

Install the license key on the same machine as the Maxxess Integration using License Manager.

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

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

Notice *The Maxxess Integration must not be run on the same server as any other licensed IndigoVision software, such as the License Server.*

3 INSTALLATION

This section describes how to install the Maxxess Integration.

Before you install the Maxxess Integration, you must first configure the Maxxess system:

1. Ensure that Maxxess eFusion Desktop is running on the Maxxess machine.
2. Create a new user, dedicated for the IndigoVision Maxxess Integration.
3. Ensure that the Maxxess MultiPort service is installed and running on the Maxxess machine:
   a. From ***Start***, navigate to ***Maxxess SMS*** and open ***Service Manager***
   b. Click on ***Service Control*** and provide administrator's credentials
   c. From the dropdown list, select ***MultiPort*** and inspect the **Status**. If the **Status** is `MultiPort is stopped`, click ***Start*** to start the service.

   If the MultiPort service is not installed, follow the Maxxess installation guide.
   ► For more information, *see "References" on page 5*

To install the Maxxess Integration:

1. Download the Maxxess 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 Maxxess Integration is installed to:

   C:\Program Files (x86)\IndigoVision\Integration\Nedap AEOS

   by default.
3. If the Microsoft .NET 4.7.2 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 Maxxess Integration using the License Manager tool.
   ► For more information, *see "License the integration" on page 9*
5. Configure the Maxxess Integration.
   ► For more information, *see "Configuration" on page 11*
6. Start the IndigoVision Maxxess Integration service using the Windows® services utility.

License the integration

You must have a valid software or hardware license that allows the IndigoVision Maxxess Integration to run on a specific machine.

You can manage the software license using the License Manager tool, which is installed as part of the Maxxess 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 license from one machine to another using the License Manager tool.

Upgrade from 1.0

When upgrading from version 1.0, the installer automatically:

- Backs up the existing system configuration file (***System.conf***)
- Moves the existing ***TolvConf*** file to the TolvConf folder (under ***C:\Program Data\IndigoVision\Integration\Maxxess***). This is still valid.

The existing ***System.conf*** file is not compatible, so you can run the Integration Configuration Tool and set up your integration module. Do not manually edit the System configuration file.

Some parameters have changed name from 1.0:

- **System Alarm Server IP** is the IP of the alarm server where the system events will be sent
- **Integration Offline**, formerly **BMOffline**
- **Integration Online**, formerly **BMOnline**
- **Maxxess Offline**, formerly **3rdPartyOffline**
- **Maxxess Online**, formerly **3rdPartyOnline**
- **Server Host**, formerly **3rdPartyAddress**
- **Server Port**, formerly **3rdPartyPort**
- **Username** and **Password** moved to an encoded file
- Logging level has been moved. It can be configured using the shortcut in the start menu.

► For more information regarding the Integration Configuration Tool, *see "Integration Configuration Tool" on page 11*

4 CONFIGURATION

To integrate Maxxess alarm events into the IndigoVision Alarm Server, perform the following steps:

1. Run the Integration Configuration Tool for Maxxess Integration – *see "Integration Configuration Tool" on page 11*.
2. Logging configuration – *see "Logging configuration" on page 25*.
3. Configure IndigoVision Control Center:
   a. Create a new external system – *see "Create a new external system" on page 16*.
   b. Create a new zone and external detector for each Maxxess event – *see "Create a new zone and external detector for Maxxess events" on page 17*

Integration Configuration Tool

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

1. Run the Integration Configuration Tool for Maxxess Integration.
   Start > All Programs > IndigoVision Maxxess Integration > Configure Maxxess Integration
2. Optionally provide the **Alarm Server IP** for **System Events**.
   - **System Events** report the status of the Maxxess Integration and its connection to Maxxess.
3. Provide the **Integration IP** address of the Maxxess Integration.
   - When the IndigoVision Maxxess 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**
   - **Maxxess Online** and **Offline**
5. Provide the details and credentials to connect to the Maxxess MultiPort service. It normally runs on the same machine as Maxxess.
   - It is recommended to leave the **Server Port** to its default value of 1705.
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 Maxxess alarms 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 of Maxxess alarms across multiple Alarm Servers.
7. Configure the event mappings for each Alarm Server. The event mapping file is known as a Maxxess events configuration file (events to IndigoVision).

- The Maxxess events configuration file for the Alarm Server opens in a new window.

► For more information, *see "Maxxess event configuration files" on page 12*

8. Optionally enable **Alarm Actions** from IndigoVision Control Center if you wish to acknowledge and delete Maxxess Integration alarms from IndigoVision Control Center.
9. Optionally enable **Relays** if you wish to remote control outputs and doors from IndigoVision Control Center.
10. Configure the relay mappings. The file opens in a new window.
11. Click ***Finish*** to close the dialog, save your settings and automatically start the Maxxess Integration.

Maxxess event configuration files

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

Maxxess event configuration files contain information for mapping each Maxxess event received from the Maxxess 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 a Maxxess event configuration file

```
# This file contains the mapping of Maxxess events to IndigoVision
# external event input numbers.
#
# Each entry consists of three comma separated elements:
#
# Input Number, Maxxess Event, Optional Description
#
# 1. The first element of each entry, InputNumber, is the positive integer
#    corresponding to the External Event input in the Alarm Server.
#
# 2. The second element, Maxxess Event, describes the details of the event
#    within Maxxess.
#
#    The Maxxess event consists of 2 parts separated by a colon:
#        - Address:State
#
#    Address: The Full Address of the point creating the event.
#       It is composed of different parts separated by periods,
#       for example "SECURITY-PC.R6.10.1" or "WIN-RBRH6710NQR.P2.1.1""
#
#    State: The message code of the event. This is typically 2 characters.
#       Configuration of the IndigoVision Maxxess Integration involves using
#       Maxxess Message Codes and Event Codes to define the type of event.
#       An up to date list of these event codes can be found in the
#       Maxxess online help. Open the eFusion Desktop Help and search for
#       "Message codes" and "Event Codes".
#
#       When using Virtual Event buttons, this will be the value configured
#       within eFusion for "Data".
```

```
#
# 3. An optional third field, separated by another comma can be added with
#    a description of the event mapping.
#
# Example:
# 10, SECURITY-PC.R6.10.1:A1
#
# Example of an event with the optional description:
# 11, SECURITY-PC.R6.10.1:A3, Front door - Request to Exit
#
# The Maxxess event cannot contain the characters '\', '{', '}', ':' or ','.
# When configuring Virtual Event buttons in Maxxess it would be recommended
# that the Data field does not use these characters. Alternatively the
# following octal escape codes can be used to represent these characters.
# Character '\': => \134
# Character '{': => \173
# Character '}': => \175
# Character ':': => \072
# Character ',': => \054
#
# Example using octal escape code for the character ':' when a Sensor has been
# configured with a Virtual Event button where a value of A:B has been
# specified for "Data".
# 12, SECURITY-PC.P2.1.1:A\072B
```

Octal escape codes are required to configure Maxxess events with special characters, such as comma and backslash.

Remote control of doors and outputs

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

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

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 actions within the
# Maxxess system.
#
# The following formats are used to define the relay outputs:
#
# OutputNumber, Target:Action:Address
# OutputNumber, Target:Action:ControllerAddress:Name
#
# The first element of each entry is a positive number corresponding to an
# external relay output in the IndigoVision Control Center system.
#
# The second element contains information about the action to perform
# in the Maxxess system.
```

```
# This can be an action on an output, output group, door or door group.
#
# Output Actions
#
# OutputNumber, OUTPUT:Action:Address
#
# To perform an action on an output, the 'OUTPUT' target must be used and the
# Address specified must be the full address of the output as displayed in
# eFusion Desktop.
# The Action must be one of:
#
# - Momentary
# - Energize
#
# When the relay in the Control Center system is activated, the mapped action
# is attempted on the output at the specified address.
# When a relay mapped to an Energize action in the Control Center system
# is deactivated,
# the output at the specified address is de-energized.
#
# Examples:
# 1, OUTPUT:Energize:SECURITY-PC.R6.10.1, Energize/De-energize output
# at address SECURITY-PC.R6.10.1
# 2, OUTPUT:Momentary:SECURITY-PC.R6.10.1, Momentarily energize output
# at address SECURITY-PC.R6.10.1
#
# Output Group Actions
#
# OutputNumber, OUTPUTGROUP:Action:ControllerAddress:Name
#
# To perform an action on an output group, the 'OUTPUTGROUP' target must be used,
# the ControllerAddress specified must be the full address of the area controller
# the output group belongs to, as displayed in eFusion Desktop, and the Name
# specified must be the name of the output group as displayed in eFusion Desktop.
# The Action must be one of:
#
# - Momentary
# - MomentaryIfEnabled
# - Energize
# - EnergizeIfEnabled
#
# When the relay in the Control Center system is activated, the mapped action
# is attempted on the output group with the specified name belonging
# to the area controller at the specified address.
# When a relay mapped to an Energize action in the Control Center system
# is deactivated, the output group is de-energized.
#
# Examples:
# 3, OUTPUTGROUP:Energize:SECURITY-PC.R:FrontDoor_output_group,
# Energize/De-energize all outputs in the output group named 'FrontDoor_output_group'
# within the SECURITY-PC.R area controller
# 4, OUTPUTGROUP:EnergizeIfEnabled:SECURITY-PC.R:FrontDoor_output_group,
# Energize all enabled outputs in the output group named 'FrontDoor_output_group'
```

```
# within the SECURITY-PC.R area controller
# 5, OUTPUTGROUP:Momentary:SECURITY-PC.R:FrontDoor_output_group,
# Momentarily energize all outputs in the output group named 'FrontDoor_output_group'
# within the SECURITY-PC.R area controller
# 6, OUTPUTGROUP:MomentaryIfEnabled:SECURITY-PC.R:FrontDoor_output_group,
# Momentarily energize all enabled outputs in the output group
# named 'FrontDoor_output_group' within the SECURITY-PC.R area controller
#
# Door Actions
#
# OutputNumber, DOOR:Action:Address
#
# To perform an action on a door, the 'DOOR' target must be used and the
# Address specified must be the full address of the door as displayed in
# eFusion Desktop.
# The Action must be one of:
#
# - Momentary
# - Unlock
# - Lockdown
#
# When the relay in the Control Center system is activated, the mapped action
# is attempted on the door at the specified address.
# When a relay mapped to an Unlock action in the Control Center system
# is deactivated, the door at the specified address is unlocked.
# When a relay mapped to a Lockdown action in the Control Center system
# is deactivated, the lockdown state on the door
# at the specified address is cleared.
#
# Examples:
# 7, DOOR:Momentary:SECURITY-PC.R6.10.1, Momentarily unlock the door
# at address SECURITY-PC.R6.10.1
# 8, DOOR:Unlock:SECURITY-PC.R6.10.1, Unlock the door
# at address SECURITY-PC.R6.10.1
# 9, DOOR:Lockdown:SECURITY-PC.R6.10.1, Lockdown the door
# at address SECURITY-PC.R6.10.1
#
# Door Group Actions
#
# OutputNumber, DOORGROUP:Action:ControllerAddress:Name
#
# To perform an action on a door group, the 'DOORGROUP' target must be used,
# the ControllerAddress specified must be the full address of the area controller
# the door group belongs to, as displayed in eFusion Desktop, and the Name specified
# must be the name of the door group as displayed in eFusion Desktop.
# The Action must be one of:
#
# - Momentary
# - MomentaryIfNotLockedDown
# - Unlock
# - UnlockIfNotLockedDown
# - Lockdown
#
```

```
# When the relay in the Control Center system is activated, the mapped action
# is attempted on the door group with the specified name within the area controller
# at the specified address.
# When a relay mapped to an Unlock action in the Control Center system
# is deactivated, the door group is locked.
# When a relay mapped to a Lockdown action in the Control Center system
# is deactivated, the lockdown state on the door group is cleared.
#
# Examples:
# 10, DOORGROUP:Momentary:SECURITY-PC.R:Hall_door_group,
# Momentarily unlock all doors in the 'Hall_door_group' group
# within the SECURITY-PC.R area controller
# 11, DOORGROUP:MomentaryIfNotLockedDown:SECURITY-PC.R:Hall_door_group,
# Momentarily unlock all doors that are not locked down in the 'Hall_door_group'
# within the SECURITY-PC.R area controller
# 12, DOORGROUP:Unlock:SECURITY-PC.R:Hall_door_group,
# Unlock all doors in the 'Hall_door_group' group
# within the SECURITY-PC.R area controller
# 13, DOORGROUP:UnlockIfNotLockedDown:SECURITY-PC.R:Hall_door_group,
# Unlock all doors that are not locked down in the 'Hall_door_group' group
# within the SECURITY-PC.R area controller
# 14, DOORGROUP:Lockdown:SECURITY-PC.R:Hall_door_group,
# Lockdown all doors int the 'Hall_door_group' group
# within the SECURITY-PC.R area controller
#
# The address or name cannot contain the characters ':', '\', '{', '}', ',' or
leading or trailing whitespaces.
# The following octal escape codes can be used to represent these characters.
# Character ':': => \072
# Character '\': => \134
# Character '{': => \173
# Character '}': => \175
# Character ' ': => \040 - for allowing leading or trailing spaces
# Character ',': => \054
#
# Example using octal escape codes for an output group
# called BackDoor:output1,output2
# 15, OUTPUTGROUP:Energize:SECURITY-PC.R:BackDoor\072output1\054output2
```

Configure IndigoVision Control Center

Zones and detectors must be created in Control Center for the configured Maxxess events. When acknowledging and deleting Maxxess alarms from IndigoVision Control Center, it is recommended that a zone with only one detector is created for each Maxxess alarm.

If the **Integration Online**, **Integration Offline**, **Maxxess Offline** or **Maxxess Online** system events have been specified, 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 Maxxess Integration. Refer to the Control Center online help about creating a new external system.

Create a new zone and external detector for Maxxess events

You must create zones and detectors for the configured Maxxess events using one of the following methods:

1. Manually create the zones and external detectors within Control Center.
   - Add a new zone for each unique alarm you want to report 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 Maxxess event configuration file of the Maxxess Integration.
   - IndigoVision recommends that you configure the zone name description in Control Center to closely match the Maxxess alarm name. This helps to ensure there is no confusion in correlating events.
2. Use the IndigoVision Import Alarm Sources tool to automatically create zones and detectors for each event within a Maxxess event configuration file.
   - After you have edited the Maxxess event configuration file, accessible through the Integration Configuration Tool, with all the supported events, configure an IndigoVision Alarm Server using the IndigoVision Import Alarm Sources tool.
   - You can download the Import Alarm Servers tool from the IndigoVision website.
   - Every time an event is added to Maxxess event configuration file, run the tool again to create new zones and detectors.

Create external relays

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

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

5 TROUBLESHOOTING

This chapter provides troubleshooting information for the Maxxess Integration.

Service does not start

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

If no `FATAL` level log messages are available:

1. Open Windows **Event Viewer**
2. Navigate to ***Windows Logs > Application***
3. Find one or more events logged at `ERROR` level and with ***Source*** `IndigoVision IntegrationCore Service`

The ***General*** field describes why the service is not starting.

Unable to connect to Maxxess

If you are unable to connect to the Maxxess MultiPort service, check the following:

1. Check the log file for `ERROR` level messages and follow the advice in the error message.
2. If the log files contain errors related to connection failures:

   ```
   [ERROR][MaxxessIntegration.Connection.ConnectionManager]: Unable to connect to Maxxess server at 192.168.1.26:1705.
   [ERROR][MaxxessIntegration.Connection.ConnectionManager]: Please check Maxxess host and port are configured correctly and the firewall on the Maxxess server is not preventing connections to the machine.
   ```

   Make sure the Server Host configured matches the Maxxess server IP or host name. In the example above, the Maxxess Integration is trying to connect to a Maxxess server with IP 192.168.1.26.
3. The Maxxess Integration uses a TCP connection to communicate to Maxxess MultiPort service. If the machine running Maxxess and the Maxxess MultiPort service has a firewall enabled, create a rule to allow TCP incoming connection on port 1705.
4. If the Server Host and Server port are correct, please make sure the MultiPort service is running on the Maxxess server:
   - From ***Start***, navigate to ***Maxxess SMS*** and open ***Service Manager***
   - Click on ***Service Control*** and provide administrator's credentials
   - From the dropdown list, select MultiPort and inspect the **Status**. If the **Status** is `MultiPort is stopped`, click ***Start*** to start the service
   - The Maxxess Integration will automatically try to connect once the MultiPort service is running
5. If the MultiPort service is running, you may see the following errors:

```
[ERROR][MaxxessIntegration.Connection.HeartbeatMonitor]: Unable to connect to the
Maxxess MultiPort service. Please verify the username and password for the Master
user are valid.
```

In this case, please verify the credentials you have entered are valid and match the Maxxess user you want to use for the Integration. Run the Integration Configuration tool and change the credentials if needed.

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 you to determine the source of the problem:

1. Verify that the Maxxess Integration is running.
2. Enable `INFO` level logging.
   ► For more information, *see "Logging configuration" on page 25*.

   This enables the Maxxess Integration to log all alarms and events received from Maxxess, not only those that are mapped in the event configuration file.
3. If the Maxxess Integration cannot contact the Alarm Server, you will see a log message similar to the following:
   ```
   [ERROR][IntegrationCore.Core.Event.BindingKit]: Failed to send ToIv event.
   ```
4. Ensure that the Alarm Server is online, and that the firewall is not blocking communication. Refer to the IndigoVision Control Center Installation Guide for more information about IndigoVision Firewall Requirements.
   ► For more information, *see "References" on page 5*.
5. Inspect the log file for messages showing that the event has been received:
   ```
   [INFO ][MaxxessIntegration.ToIv.GenericEventHandler]: Received Maxxess event 'WIN-
   RBRH6710NQR.P2.1.1:C2'.
   ```
   a. If the event is within the log file, then look for a log message confirming that the event has been sent to the Alarm Server:
      ```
      [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 '01/02/2019 11:16:23'.
      ```
      If you see the above log message, then the Integration has successfully processed the event, however it the alarm or detector may not configured correctly, in which case progress to steps 6 & 7.

      If you do not see the log message confirming that the message was sent, then the event is not correctly configured to forward this event to the IndigoVision system, in which case you will see a log message similar to the following:
      ```
      2019-02-01 10:42:08,335 [INFO ][IntegrationCore.Core.EventManager]: ToIv event
      'WIN-RBRH6710NQR.P2.1.1:C2' is not configured to send to any Alarm Server.
      ```
      The event can be configured using the Integration Configuration Tool.
      ► For more information on how to configure events, *see "Integration Configuration Tool" on page 11*
   b. If there are no messages confirming that the event has been received then it may not have been received within Maxxess, or the event is not correctly configured within Maxxess.
6. Verify that you have:
   - created corresponding zones and external detectors
   - set the zones
   - enabled external detectors in Control Center

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

a. Select the ***External Systems*** tab. Ensure that you have created an External System with the IP address of the PC running the Maxxess Integration.
b. Select the ***Zones*** tab. Ensure that you have created a zone containing an external detector with the Input Number as the external input number configured for the event.
c. Ensure that the zone belongs to the nominated Alarm Server.

   Right-click the zone, then select ***Properties*** > ***Zone***.

7. Ensure that the Alarm Server containing the zones and detectors for Maxxess events is the same Alarm Server that is configured using the Integration Configuration Tool.
8. Verify that the System user is authorized to write to the log file regardless of the current login user's authorization.

Maxxess alarms not acknowledged or deleted from Control Center

If alarm actions are not performed in Maxxess, then the following end-to-end check for a single alarm may help you to determine the source of the problem:

1. Verify that the Maxxess Integration is running.
2. Enable INFO level logging.
   ► For more information, *see "Logging configuration" on page 25*
3. Open the Integration Configuration tool and verify the feature is enabled in the page **Alarms Actions from IndigoVision Control Center**.

   If it is disabled, please enable it, and finish the wizard so the service will be restarted.
4. Make sure only one Maxxess alarm you want to acknowledge or delete from Control Center is mapped to a Control Center zone. If multiple Maxxess events are mapped to detectors belonging to the same Control Center zone, acknowledging and deleting may not work as expected.
5. Verify the Maxxess alarm is still in alarm and not already acknowledged or deleted.

   Open Maxxess Desktop, log in and go to Alarm Log and make sure there's a red symbol next to the alarm, to show the alarm is active, or a green symbol to show the alarm has been acknowledged.

   An active alarm can be acknowledged or deleted by acknowledging or clearing the corresponding zone, an acknowledged alarm cannot be acknowledged again but it can be deleted by clearing the corresponding zone.

   If the alarm is not present in Maxxess Desktop, then the alarm has already been deleted.
6. Open the log files for the Maxxess Integration by using the shortcut in the Start Menu. If you see:

   ```
   [MaxxessIntegration.FromIvActions.FromIvActionModule]: Unable to acknowledge alarm: no active alarm has been found for alarm point at address WIN-II7T4H4M9BM.R0.0.0
   ```

   This means that the Maxxess alarm has already been acknowledged or deleted, or it was triggered while the Maxxess Integration was offline.

   It is not possible to acknowledge/delete Maxxess alarms that have been triggered when the Maxxess Integration service was stopped or when there was a lack of communication with the Maxxess MultiPort service.
7. If you see any of the following:

   ```
   [MaxxessIntegration.Maxxess.DataParser]: An alarm for the alarm point at the address 'WIN-II7T4H4M9BM.R0.0.0', with alarm Key '898-267357-8', has been acknowledged on '2019-02-11 10:23:39'
   ```

or

```
[MaxxessIntegration.Maxxess.DataParser]: An alarm for the alarm point at the
address 'WIN-II7T4H4M9BM.R0.0.0', with alarm Key '898-267357-8', has been deleted
on '2019-02-11 10:23:39'
```

This highlights an issue in Maxxess Desktop or with the MultiPort service.

Please log out and log in to Maxxess Desktop again. It the issue is still present, please contact Maxxess support.

8. Verify if there was a third party offline event triggered in Control Center before you acknowledged or cleared the Control Center zone. If the Maxxess Integration cannot contact the Maxxess Multiport service, any attempt to acknowledge/delete the alarm will fail.

Maxxess outputs or doors not actioned from Control Center

If relay actions are not performed in Maxxess, then the following end-to-end check for a single action may help you to determine the source of the problem:

1. Verify that the Maxxess Integration is running.
2. Enable INFO level logging.
   ► For more information, *see "Logging configuration" on page 25*
3. Open the Integration Configuration tool and verify the feature is enabled in the page **Relay Actions from IndigoVision Control Center**.

   If it is disabled, please enable it, and finish the wizard so the service will be restarted.
4. If it is enabled, open the mapping file by clicking Configure Relay Actions and make sure the expected door or output is present and mapped to the correct Control Center relay number. Also check the full address of the mapped door or output is correct, as displayed in Maxxess Desktop.
5. Make sure you see the following log message:

   ```
   [MaxxessIntegration.FromIvRleays.Actions.OutputEnergizeAction]:
   Attempting to energize output at address 'WIN-II7T4H4M9BM.R0.0.0'
   ```

   or a similar message, depending on the action you are performing.
6. Open Maxxess Desktop and check if the door controller or the panel are online and communicating with Maxxess eFusion. If there is a communication error, the relay action will not be performed.
7. Verify the Maxxess MultiPort has received the action. Open eFusion Desktop, go to ***Status > System Logs...*** and inspect the log.
8. Verify if there was a third party offline event triggered in Control Center before you performed the relay action. If the Maxxess Integration cannot contact the Maxxess Multiport service, any attempt to perform a relay action will fail.

Maxxess Integration is slow to start

If no internet access is available, a standard security check causes the Maxxess Integration service to start slowly, 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 ***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, disable ***Check for publisher's certificate revocation*** 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 Maxxess Integration is installed on a machine that has not had Sentinel HASP software installed previously.

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

Before installing the Maxxess Integration, uninstall IndigoVision software that is licensed with a software license.

A LOGGING CONFIGURATION

Logging is configured with a separate file, which allows you to customize logging and to manage backup log files.

You need only to change this file when you require more detail on events received, or as advised by IndigoVision.

To access this file, navigate to the following location:

Start > All Programs > IndigoVision Maxxess Integration > Logging Configuration for Maxxess Integration

To adjust the logging level, modify ***level*** in the root section. You can change this 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 Maxxess Integration is functioning incorrectly and may require action.
- **ERROR**: Only capture messages where a failure has occurred and may require action.
- **FATAL**: Critical errors where the Maxxess Integration cannot continue.

For example, to increase 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 kept. Older files are removed when this limit is reached and new files are required.

IndigoVision recommends that you do not change any other settings unless advised to by IndigoVision.