Last updated: September, 2021

INSTALLATION GUIDE

Milestone Alarm Notification from IRIS

Prepared by:
Mattias Johansson, R&D Group Manager, Irisity

milestone

IRISITY

Table of Content

Design 2

Requirements and Considerations 2

Installation 3

Configuration 3

Setup on the IRIS ARC 3

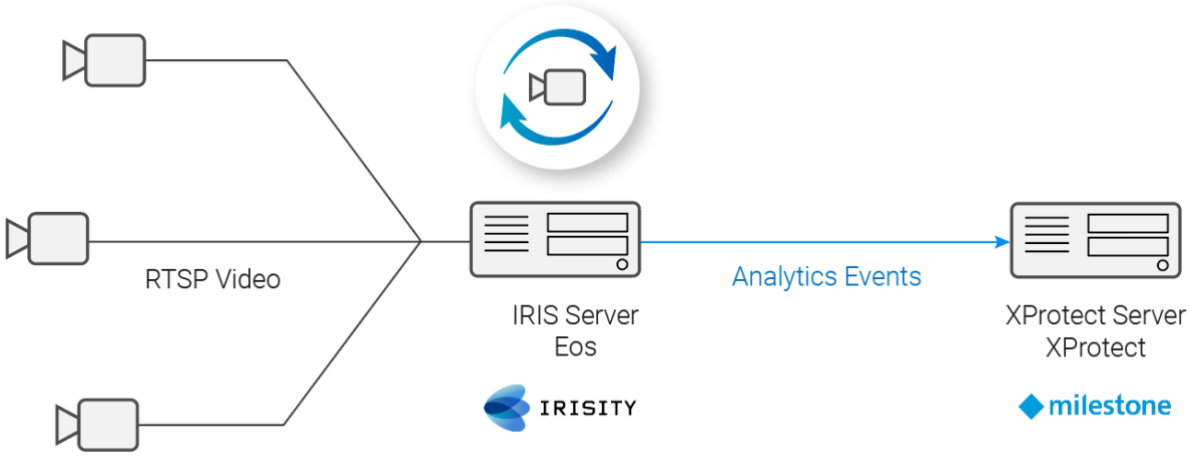
Setup on the IRIS analysis machine 3

Milestone Specific settings in IRIS 4

Alarm information reference 6

Operations, maintenance, and troubleshooting 6

Design



When an alarm has been triggered by IRIS analytics running on the IRIS Server with Eos which is continuously monitoring all Real-Time Streaming Protocol (RTSP) video streams from connected surveillance cameras, the system will trigger a notification to the Milestone system using Analytics Events. Analytics Events are a flexible solution that can be configured to trigger alarms in the Milestone system using Alarm Definitions.

Requirements and Considerations

The configuration for external alarm notification is done after successfully setting up IRIS and installing the necessary services on local machines. The setup is done locally on the machine running the IRIS analysis software (Eos) *or* on the machine running the IRIS alarm receiver (IRIS ARC). No configuration option is available in the IRIS Manage Portal.

Setting up the configuration on the IRIS analysis machine running Eos will mean that no centralized or cloud-hosted AI-based alarm filtering will be applied. This might degrade analytics performance, depending on the analysis algorithm used. Setting up the configuration on the final (“destination”) IRIS alarm receiver running IRIS ARC will not alter the alarm flow; AI-based alarm filtering will thus be applied if configured. Notice that, when setup on the IRIS analysis machine, the local settings described here applies to all sites and cameras running on the same machine. Likewise, when setup on the IRIS ARC, the settings will be applied to all received alarms.

When setup on the IRIS ARC, a notification will be generated and sent for each received alarm as soon as the alarm is received. There is no possibility to add conditions on how the alarm is classified by the operator.

Notice the connection between a camera in IRIS and in Milestone is done through the hostname/IP number of the camera. This information is taken from the *External IP* parameter field in IRIS, hence all cameras in IRIS which are expected to trigger alarms must have their *External IP* field set to the same value as in Milestone. Cameras without this field will not be successfully identified by Milestone and their alarms will not show up.

Installation

Ensure that Milestone is setup with at least one Analytics Event to which IRIS can send alarm notifications and make sure that the port for accepting Analytics Events is enabled in Milestone and that the firewall allows incoming traffic on this port.

Configuration

Setup on the IRIS ARC

Notifications to all external alarm receivers are configured via the local configuration file `%programdata%\Irisity\Configuration\AlarmCentral\APISettings.json`
This is a json file listing all external systems which should be notified when an alarm has been received. The section *AlarmNotifierSettings* defines which external systems should be notified after an alarm has been received. This section may list any number of alarm receivers, including multiple alarm receivers of the same type.

```
{
  "AlarmNotifierSettings": [
    {
      "Type": "<receiver type>",
      "IsEnabled": true,
      "<TypeSpecificSettings>":
      {
        ...
      }
    }
  ]
}
```

Notice: On the IRIS ARC, notifications are generated and sent whenever a new alarm is received from the IRIS analysis software.

Setup on the IRIS analysis machine

External alarm receivers are configured via the local configuration file `%programdata%\Irisity\Configuration\Client\AlarmSendingSettings.json`.

The section *AlarmReceivers* defines which external systems should be notified after an alarm has been triggered. This section may list any number of alarm receivers, including multiple alarm receivers of the same type.

```
{
  "AlarmReceivers": [
    {
      "Type": "<receiver type>",
      "IsEnabled": true,
      "<TypeSpecificSettings>":
      {
        ...
      }
    }
  ]
}
```

If there are no alarm receivers configured in the file `AlarmSendingSettings.json`, or this file does not exist, then the IRIS analysis software will default to sending alarms to an IRIS ARC, as configured in the Manage Portal.
However, to support the situation to only send alarms to an external alarm system, the IRIS analysis software will not automatically send alarms to an IRIS ARC when there is an external alarm receiver configured.

If alarms are to be sent both to an IRIS ARC and an external alarm system then `AlarmSendingSettings.json` must include one alarm receiver of type `IrisArc`, as in the example below. The settings for this IRIS ARC are setup in the Manage Portal.

```
{
  "AlarmReceivers": [
    {
      {
          "Type": "IrisArc",
          "IsEnabled": true,
       },
       "<TypeSpecificSettings>":
       {
         ...
       }
    }
  ]
}
```

Milestone Specific settings in IRIS

To enable alarm sending to Milestone, setup the following contents in the local configuration file:

```
{
  "Type": "Milestone",
  "MilestoneSettings":
  {
    "Hostname": "127.0.0.1",
    "Port": 9090,
    "PingPeriod": "00:01:00",
    "DefaultAnalyticsEvent": "Default Analytics Event",
```

```
    "DefaultDescription": "Tresspassing detected"
  }
}
```

Where the fields have the following significance:

Field	Description
Hostname	Mandatory Hostname or IP address of the Milestone server.
Port	Optional Port number of the Analytics Receive Port on the Milestone server. Default is 9090.
PingPeriod	Optional How often that IRIS should check that the Milestone server is still up and running. This is a string in the format "HH:MM:SS". Remove to disable ping.
DefaultAnalyticsEvent	Optional The default Analytics Event to use for all detections, unless another event is configured for a specific alarm type below. Default is *Default Analytics Event*.
RailDefenderAnalyticsEvent	Optional The Analytics Event to use for Rail Defender alarms, unless another event is configured for a more specific type of Rail Defender alarms. Default is value of DefaultAnalyticsEvent.
RailDefenderHumanAnalyticsEvent	Optional The Analytics Event to use for Rail Defender Human activity alarms. Default is value of RailDefenderAnalyticsEvent.
RailDefenderObjectAnalyticsEvent	Optional The Analytics Event to use for Rail Defender Object alarms. Default is value of RailDefenderAnalyticsEvent.
DefaultDescription	Optional Default description to use for all detections, unless another description is configured for a specific alarm type below. Default is *Trespassing detected*.

RailDefenderHumanDetectedDescription	Optional Description to use for Rail Defender Human detections. Default is value of DefaultDescription.
RailDefenderObjectDetectedDescription	Optional Description to use for Rail Defender Object detections. Default is value of DefaultDescription.

Alarm information reference

The following information is sent to Milestone:

Field	Description
ID	The ID of the alarm.
Timestamp	The time of the alarm.
Type	The type of alarm. Is one of: • *Human* • *Object* • *Unknown*
Message	Human-readable message describing the type of alarm. This information is taken from the settings.
Source Name	The hostname or IP of the camera that the alarm originates from.
Location	The name of the camera that the alarm originates from.

Operations, maintenance, and troubleshooting

The entire IRIS system, including configuration, management, monitoring, troubleshooting, and much more, can be installed on-premise or connected to the IRIS cloud-hosted platform. Both systems include all the tools needed for efficient management of thousands of cameras, potentially divided amongst thousands of surveillance sites and/or customers. Depending on the installation method, workflows for operations and maintenance will differ. Please reach out to success@irisity.com for detailed information and further assistance.

ABOUT IRISITY

Irisity is a leader in intelligent camera surveillance. We develop deep learning powered algorithms upgrading both existing and new surveillance cameras and security systems into proactive intelligent devices. IRIS™, our fully cloud-based SaaS solution, detect with high precision unwanted activity and behavior at long distances.

Staying at the forefront of technology innovation we continue developing agile algorithms providing the best possible security solutions for clients worldwide.

irisity.com

ABOUT MILESTONE

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.

www.milestonesys.com/community/marketplace

milestone

IRISITY