



SAFR Video Insight Integration Guide

Documentation Version = 3.017

Publish Date = April 11, 2021

Copyright © 2021 RealNetworks, Inc. All rights reserved.

SAFR® is a trademark of RealNetworks, Inc. Patents pending.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

Contents

1	SAFR Video Insight Integration Guide	3
2	SAFR Video Insight Operation Guide	7

1 SAFR Video Insight Integration Guide

Integrated SAFR Video Insight is only available on Windows.

Integrating SAFR's facial recognition and analysis capabilities into Video Insight allows SAFR to trigger camera flashes and/or pop-up alert messages on Video Insight camera windows when specified types of people are seen by cameras. This makes it much easier to quickly and accurately separate unknown people from authorized people from known threats.

1.1 Integration Overview

A typical deployment requires the following:

- A machine running VI Health MonitorPlus.
- One or more machines running the SAFR Desktop Client to process videos.
- If you're doing a SAFR on-premise deployment, you'll also need a machine running SAFR Server. SAFR Server can run on the same machine as one of the Desktop Clients, provided the host machine meets the system requirements.

Cameras are connected to the VI Health MonitorPlus. The SAFR Desktop Client can then connect to the MonitorPlus to perform analysis of the video feeds and trigger Video Insight camera view color flashes and/or pop-up alert messages. Depending on the number of cameras you need, one or more machines may be required to run the SAFR Desktop Client(s), each processing multiple video feeds. The Desktop Client is also used to perform various management activities.

1.1.1 System Requirements

Video Insight has the following system requirements:

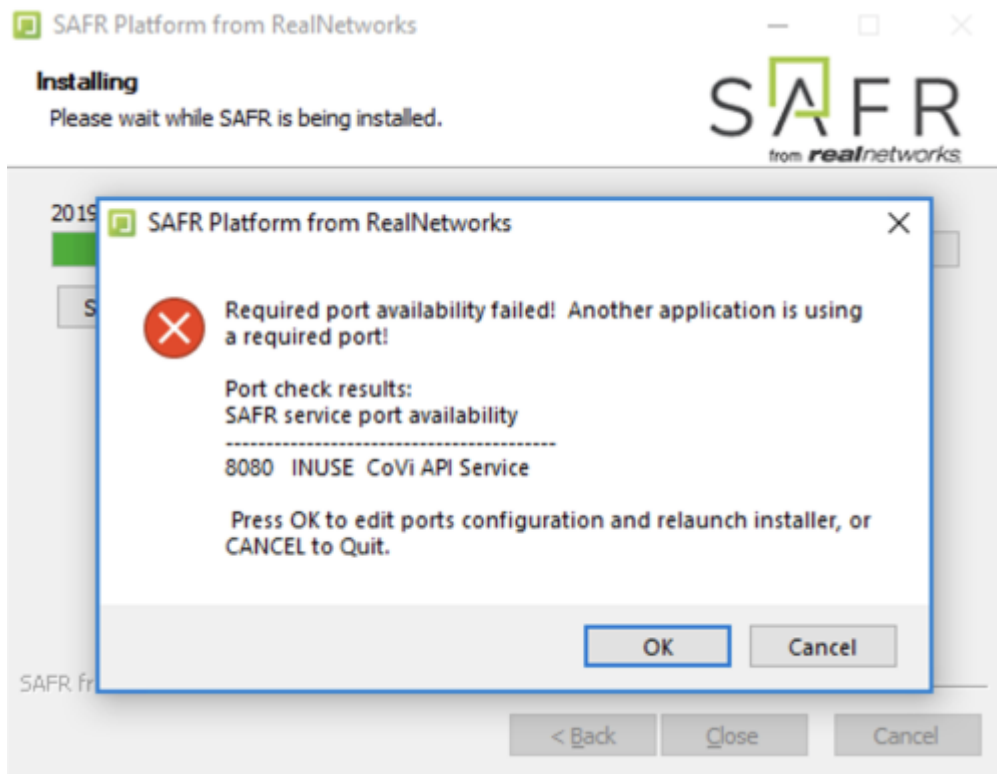
- A machine running VI Health MonitorPlus.
- Each machine running a Video Insight product must meet the following system requirements:
 - Dual 2.4 GHz Quad CPU
 - 8GB RAM
 - 1 GB/s network interface
 - Windows Server 2012 R2

SAFR has the following system requirements:

- Each machine running the SAFR Desktop Client must meet the following requirements:
 - Windows 10.
 - The Desktop Client must be version 3.2.141 or later.
 - Additional system requirements as described on the SAFR system requirements page.
- On-premise SAFR deployments require at least one machine running SAFR Platform 3.2.139 or later.
- Each machine running SAFR Server must meet the following requirements:
 - Windows 10.
 - Additional system requirements as described on the SAFR system requirements page.

1.2 Install and Configure SAFR

1. Go to the SAFR Download Portal.
2. If you're doing a cloud deployment, download and install Windows SAFR Desktop. Make sure to select the Video Insight install option.
3. If you're doing an on-premise deployment, download and install Windows SAFR Platform. Make sure to select the Video Insight install option.
 - When installing the SAFR Platform, the default SAFR port assignments sometimes conflict with other software port assignments. If a port conflict occurs, the error message shown below will pop up in the middle of your installation.



If this happens, do the following:

1. Click **OK** to edit port configurations.
2. **Notepad** will open, displaying the *safrports.conf* file.
3. Edit any conflicting ports to new values. (e.g. CoviHTTP=18080)
4. Save and exit **Notepad**.

The Platform installer will then restart and the new port values will be used. You can find the modified *safrports.conf* file at `C:\Program Files\RealNetworks\SAFR\`.

After the installation finishes, two icons will appear on your desktop: one labeled *SAFRActions* and another labeled *SAFR*. *SAFRActions* launches SAFR Actions, while *SAFR* launches the Desktop Client. The SAFR Server (when installed as part of a local deployment) automatically runs as a collection of background services.

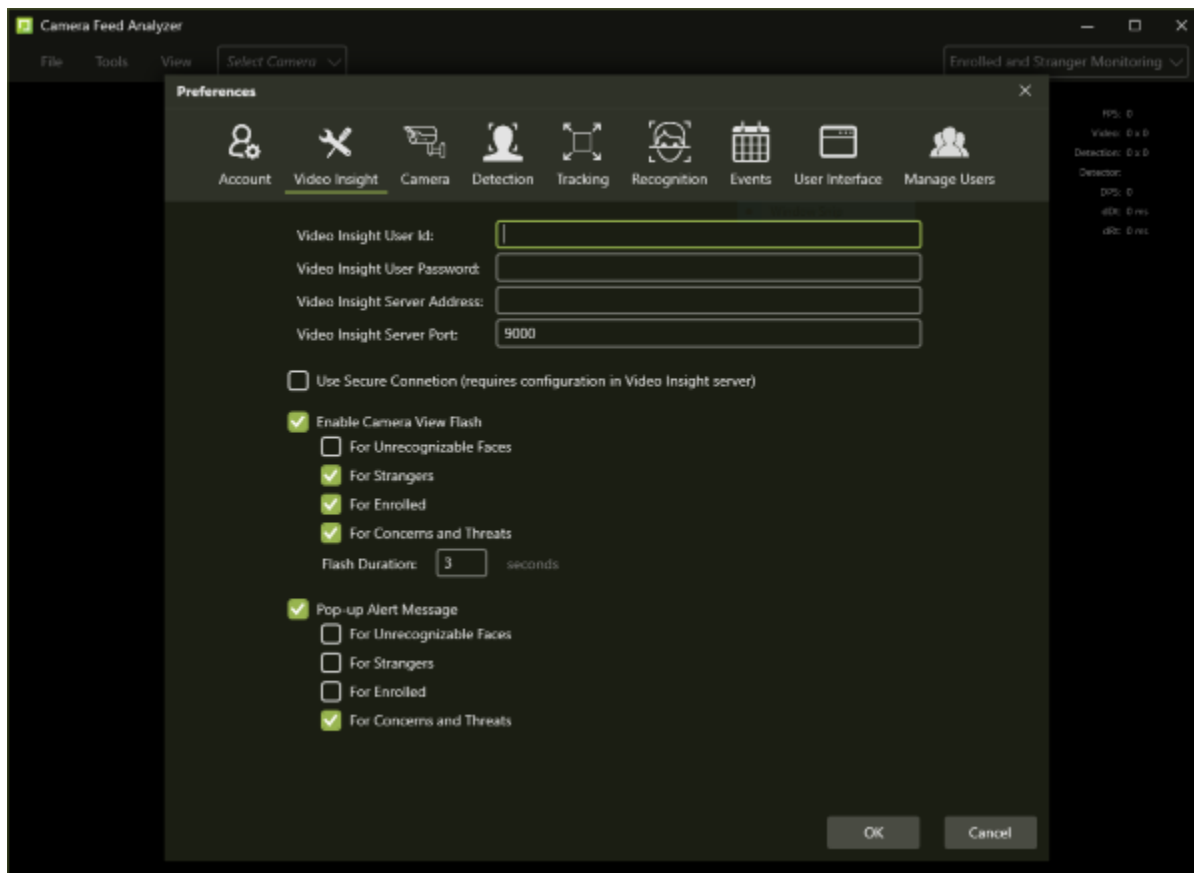
Immediately following installation, the installer opens the Desktop Client and prompts you to log in with your SAFR Account credentials. Make sure to log in; it's important in acquiring the SAFR license.

1.2.1 Connect SAFR to Video Insight

To connect SAFR to Video Insight, do the following:

1. Within your SAFR Desktop Client, select **Tools->Preferences->Video Insight**.
2. Enter information for the first four settings on the SAFR Video Insight Preferences menu: *Video Insight User Id*, *Video Insight User Password*, *Video Insight Server Address*, and *Video Insight Server Port*. See below for information about the available SAFR Video Insight preference settings.

1.2.1.1 SAFR Video Insight Preferences You can configure several settings specific to Video Insight by opening the SAFR Desktop Client and clicking on **Tools -> Preferences -> Video Insight**.



- **Video Insight User Id:** User Id of a Video Insight user with the necessary permissions to connect SAFR to Video Insight.
- **Video Insight User Password:** Password of a Video Insight user with the necessary permissions to connect SAFR to Video Insight.
- **Video Insight Server Address:** IP Address of the Video Insight server.
- **Video Insight Server Port:** Port number of the Video Insight server.
- **Use Secure Connection:** Enables the use of an https connection between Video Insight and SAFR.
- **Enable Camera View Flash:** When enabled, the camera views within the Video Insight VMS system will flash when the specified person types are seen by Video Insight cameras. For more information, see the Camera View Flash section of the SAFR Video Insight Operation Guide.
 - **For Unrecognizable Faces:** Enables camera view flashes when unrecognizable faces are seen.
 - **For Strangers:** Enables camera view flashes when people who aren't enrolled in SAFR are seen.
 - **For Enrolled:** Enables camera view flashes when people who are enrolled in SAFR and who aren't flagged as persons of concern or threats are seen.
 - **For Concerns and Threats:** Enables camera view flashes when people who are enrolled in SAFR and who are flagged as persons of concern or threats are seen.
 - **Flash Duration:** Specifies how long the triggered camera view flashes should last.
- **Pop-up Alert Message:** When enabled, the camera views within the Video Insight VMS system will display pop-up alert messages when the specified person types are seen by Video Insight cameras. For more information, see the Pop-Up Alert Messages section of the SAFR Video Insight Operation Guide.
 - **For Unrecognizable Faces:** Enables pop-up alert messages when unrecognizable faces are seen.
 - **For Strangers:** Enables pop-up alert messages when people who aren't enrolled in SAFR are seen.
 - **For Enrolled:** Enables pop-up alert messages when people who are enrolled in SAFR and who aren't flagged as persons of concern or threats are seen.
 - **For Concerns and Threats:** Enables pop-up alert messages when people who are enrolled in

SAFR and who are flagged as persons of concern or threats are seen.

1.2.2 Verify the Connection to Video Insight

To verify that your SAFR system successfully connected to the Video Insight system, do the following:

1. Open the Camera Feed Analyzer in the SAFR Desktop Client.
2. Click on the camera selection drop-down menu at the top of the *Camera Feed Analyzer*.
3. You should see the cameras connected to Video Insight among the available camera. (All Video Insight cameras have the camera's IP address or hostname appended to the beginning of the camera name.)
 - If you don't see any Video Insight cameras listed, try shutting down and then restarting your SAFR Desktop Client.

2 SAFR Video Insight Operation Guide

2.1 Camera View Flash

When enabled, faces that are seen by Video Insight cameras cause the Video Insight camera view to flash a color. Which color is flashed depends on what type of person is seen.

The camera view flash will only occur when the viewing camera is running a SAFR Video Processing Mode that supports generating events based on the person type viewed. For example, a camera running the *Enrolled and Stranger Monitoring* mode will generate a camera view flash whenever anybody is viewed, whereas cameras running the *Recognition* mode will never generate a camera view flash.

Person Type	Color
Unrecognizable face	White
Stranger (i.e. Person who isn't enrolled in SAFR)	Purple
Enrolled person without a name who isn't flagged as "Concern" or "Threat"	Blue
Enrolled person with a name who isn't flagged as "Concern" or "Threat"	Green
Enrolled person flagged as "Concern" (with or without a name)	Orange
Enrolled person flagged as "Threat" (with or without a name)	Red

2.2 Pop-Up Alert Messages

When enabled, people that are seen by Video Insight cameras cause pop-up alert messages to appear on Video Insight camera views. These messages can be generated when either a face is detected (if face detection is enabled in SAFR's Detection Preferences), a person's body is detected (if person detection is enabled in SAFR's Detection Preferences), or both.

Pop-up alert messages are only generated when the camera viewing the person is running a SAFR Video Processing Mode that supports generating events based on the person type viewed. For example, a camera running the *Enrolled and Stranger Monitoring* mode can generate any of the pop-up alert messages, whereas cameras running the *Recognition* mode can't generate any messages.

Below are all the pop-up alert messages that can be generated.

Event Message	Id Class	Named	Person Type	Condition	People Attributes
Unrecognizable person detected.	N/A	N/A	N/A	Face detected but insufficient information for recognition	idClass="unidentified"
Stranger detected	Stranger	N/A	N/A	Face detected but not found in registered people	idClass="stranger"

Event Message	Id Class	Named	Person Type	Condition	People Attributes
Enrolled person detected without name. 98.2% match.	Normal	No	None	Enrolled person without name or person type assigned	idClass="noconcern" && personType="" && name=""
Enrolled person detected with name <name>. 98.2% match.	Normal	Yes	None	Enrolled person with name but no person type	idClass="noconcern" && personType="" && name=<name>
Enrolled person detected of type <personType>. 98.2% match.	Normal	No	Defined	Enrolled person with person type but no name	idClass="noconcern" && personType=<personType> && name=""
Enrolled person detected of type <personType> with name <name>. 98.2% match.	Normal	Yes	Defined	Enrolled person with person type and name	idClass="noconcern" && personType=<personType> && name=<name>
Smile activation by enrolled person of type <personType> without a name. 98.2% match.	Normal	No	Defined	Smile activation by an enrolled person with person type but no name	personType=<personType> && name=""
Smile activation by enrolled person of type <personType> with name <name>. 98.2% match.	Normal	Yes	Defined	Smile activation by an enrolled person with person type and name	personType=<personType> && name=<name>
Concern person detected without a name. 98.2% match.	Concern	No	None	Same as above for Concern	idClass="concern" && personType="" && name=""

Event Message	Id Class	Named	Person Type	Condition	People Attributes
Concern person detected with name <name>. 98.2% match.	Concern	Yes	None	Same as above for Concern	idClass="concern" && personType="" && name=<name>
Concern person detected of type <personType>. 98.2% match.	Concern	No	Defined	Same as above for Concern	idClass="concern" && personType=<personType> && name=""
Concern person detected of type <personType> with name <name>. 98.2% match.	Concern	Yes	Defined	Same as above for Concern	idClass="concern" && personType=<personType> && name=<name>
Threat person detected without a name. 98.2% match.	Threat	No	None	Same as above for Threat	idClass="threat" && personType="" && name=""
Threat person detected with name <name>. 98.2% match.	Threat	Yes	None	Same as above for Threat	idClass="threat" && personType="" && name=<name>
Threat person detected of type <personType>. 98.2% match.	Threat	No	Defined	Same as above for Threat	idClass="threat" && personType=<personType> && name=""
Threat person detected of type <personType> with name <name>. 98.2% match.	Threat	Yes	Defined	Same as above for Threat	idClass="threat" && personType=<personType> && name=<name>