SAFR Digifort Integration Guide
Documentation Version = 3.010
Publish Date = February 18, 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 Digifort Integration Guide 3
2 SAFR Digifort Operation Guide 10
1 SAFR Digifort Integration Guide

Integrated SAFR Digifort is only available on Windows.

Integrating SAFR’s facial recognition and analysis capabilities into Digifort enables you to use SAFR’s video feed information overlays within Digifort camera video feeds, thus making it much easier to quickly and accurately separate unknown people from authorized people from known threats. You’ll also have immediate access to additional information such as age, gender, sentiment, name, company, known associates, or any other configurable information you want to create.

Integrating the two systems also allows SAFR’s information about individuals to trigger Digifort alerts and other actions within the Digifort system. Digifort’s metadata within bookmarks are enriched with SAFR’s additional information, allowing you to more easily find relevant bookmarks.

1.1 Integration Overview and Requirements

A typical deployment requires the following:

- A machine running Digifort Server and Digifort Administration Client.
- A machine running the Digifort Surveillance Client at monitoring locations.
- One or more machines running the SAFR Desktop Client to process videos.
- If you’re doing a SAFR local 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 Digifort. The SAFR Desktop Client can connect to Digifort to perform analysis of the video. Depending on the number of cameras you need, one or more machines can run SAFR Desktop, each processing multiple video feeds. The Desktop Client processes the video and returns information to Digifort to generate events. The Desktop Client is also used to perform various management activities. This could be run on the same system as Digifort Server.

1.1.1 System Requirements

Digifort has the following requirements:

- Each machine running Digifort must meet the following requirements:
  - The Digifort version must be 7.2.1 or later.
  - The machine must be running Windows 10 or later.
  - .Net Framework 4.6.2 or later must be installed.
- Each camera connected to Digifort requires a Digifort license.

Note: Digifort licenses must be acquired before attempting to discover and add cameras.

SAFR has the following requirements:
• Each camera running SAFR must have a SAFR license.
• Each machine running the SAFR Desktop Client must meet the following requirements:
  • The Desktop Client must be version 1.4.162 or later.
  • The system requirements described here.
• Local SAFR deployments require at least one machine running SAFR Platform 1.4.157 or later.
• Each machine running SAFR Platform must meet the system requirements described here.

1.2 Install and Configure Digifort

Download and install Digifort by doing the following:

1. Turn off Windows Defender and Firewalls. (Digifort requires that both these features be disabled.)
2. Download the latest Digifort installer package from Digifort and install the full package.
3. Open the Digifort Administration Client and add a new server. Log in with the default username admin and set a password in the Users tab. As an administrator, you can create additional user accounts if needed.
4. To connect cameras to Digifort, do the following:
   1. Go to Recording Servers in the Digifort Administration Client.
   2. Click Camera from the Add Button.
   3. Complete the dialog shown in the following graphic to add Camera manufacturer, model, IP Address, and other information as needed.

![Digifort Administration Client](image)

Note: Digifort allows you to add mobile cameras as well as using the Digifort Mobile Camera Pro App. In the Add Camera dialog, select Digifort as the manufacturer and Mobile Camera Pro as the make.

5. You may need to update the Video Compression, Image Resolution, Frame Rate, or Image Rotation, as shown below:
6. You may need to update the *Image Rotation* or *Profile Description* on the Media Profile settings page, as shown below:
7. Navigate to **Alerts and Events > Global Events** to add events as needed. You can configure the event actions there too, when needed.
Configure the Digifort Surveillance Client by doing the following:

1. Start Digifort Serveillance Client.
2. Go to Setting > Servers > Add.
3. Restart Digifort Serveillance Client.
4. Select the IP camera from the list.
1.2.1 Connect an IP Camera

**Important**: Digifort licenses must be acquired prior to attempting to discover and add cameras.

1. Start the Digifort Surveillance Client.
2. Select the IP camera from the Cameras list.

1.3 Install and Configure SAFR

1. From the SAFR Download Portal, download and install either SAFR Platform or SAFR Desktop, depending on your deployment type. Make sure to select the Digifort VMS extension install option.
2. After installing SAFR, you’ll be prompted for the Digifort Credentials as shown in the following dialog:

   ![Provide Digifort Credentials dialog](image)

3. Enter the information for the Digifort user created previously to connect to Digifort server, and click **OK**.
Note: During the Digifort login and authentication process, you may be prompted to enter your SAFR account credentials as well as to log into any automatically detected cameras.

4. After SAFR finishes installing, open the SAFR Desktop Client.
5. From the **Tools** menu, select **Preferences**, and click the Digifort tab.

6. Enter the following information.
   - **Digifort User Id**: User created previously in Configure Digifort.
   - **Digifort User Password**: Password created for the SAFR user.
   - **Digifort Server Address**: IP address of server running Digifort.
   - **Media Gateway Port**: Set to 554 unless configured otherwise in Digifort.

7. Click **OK**.

1.4 Verify your Connection

To verify successful connection to the Digifort system, open the **Preferences > Camera** tab. Cameras connected to the Digifort system should be visible. All cameras connected to the Digifort system have a Digifort prefix in their names.
2 SAFR Digifort Operation Guide

2.1 SAFR Digifort Preferences

- **Digifort User Id**: User created previously in Configure Digifort
- **Digifort User Password**: Password created for the SAFR user
- **Digifort Server Address**: IP address of server running Digifort
- **Media Gateway Port**: Set to 554 unless configured otherwise in Digifort
- **Report Events**: Controls if events are sent to Digifort. Events are used to trigger alarms in Digifort.
- **Insert Bookmarks**: Adds bookmarks to the video stream related to events. Allows operators to search video for events or recognized person names. **Note**: Use caution when deciding what to include since many faces can cause many bookmarks to be created.
  - **Include Unrecognizable Faces**: Adds bookmarks when a face detected by SAFR does not have enough information to determine if it is a stranger or known person. This can become visually noisy and is disabled by default. Generally useful for areas where nobody should enter.
  - **Include Strangers**: Adds bookmarks when a face is determined to be a stranger. Generally useful for secured areas where only known people should be.
  - **Include Enrolled**: Adds bookmarks when a face is determined to be a known person.
  - **Include Concerns and Threats**: Adds bookmarks when a face is determined to be a known concern or threat.
  - **Include Smile Activation**: Requires smile activation to trigger recognition.
- **Advanced**: Clicking on the **Advanced** button opens the following window:
If the Digifort events are disabled (gray; no matching Digifort event), refer to Digifort documentation to create Digifort events. Once the events are created, open the Digifort Advanced Settings dialog and, from the menu for the associated SAFR event, select the Digifort event. Once the Digifort events are created and matched, the events are enabled (black). For information on creating events, refer to Digifort documentation.
This affects the titles given to bookmarks created from the respective events.

Note: Each event type is only created if enabled in the SAFR Digifort Preferences tab.

2.2 Connect and Use Cameras and Video Feeds

In the SAFR Desktop Client, view the video feed for the camera selected from the camera selection menu.
The menu shows the cameras available from the Digifort servers. To enable the row at the bottom of the screen that isolates individual faces, click View > Detection List.

2.3 Digifort Bookmarks

Digifort creates bookmarks to help locate important events. Bookmarks are populated with Person Type, ID Class, and Name. They can also provide more detailed information with even more search attributes, such as Age and Gender.

The following illustration shows how bookmarks can be used to review important events, such as the detection of a stranger tailgating behind a registered user.

To view Digifort Bookmarks, do the following:

- Click the Bookmark icon on right side panel.
- Set a date range or other criteria, and click Search.
- Click a bookmark of interest.
- To play the video, click Video.

2.4 SAFR Identities

To add people through the SAFR Desktop Client from an image or video file, do the following:

1. Open the Desktop Client.
2. Click File > Import Faces.
3. Select the image.
   - For an image, each recognized face is enclosed by a box, and you have the option to type a name.
   - For a video, each recognized person is learned automatically as long as the faces meet the minimum criteria for recognition.
4. If faces are not learned, check the settings in the Detection and Recognition tabs under Preferences to ensure faces meet minimum criteria.
   - Detection > Minimum searched face size
   - Recognition > To allow identification
**Warning:** Reducing detection and recognition settings lowers the quality of the reference face and negatively impacts recognition. It is preferable to increase the quality of your sources than to lower the criteria for learning.

**Warning:** Users added to SAFR are not synchronized with Digifort; these users exist only in SAFR. It may be desirable to edit people properties to control which events get triggered when that person is recognized. For example, setting a person’s *ID Class* to *Concern* or *Threat* triggers the respective alarms. The most important people attributes are *Name*, *Image*, *Person Type*, and *ID Class*.

*Name*, *Image*, and *Person Type* should be edited through SAFR. *Person Type* defines a person’s role (e.g. staff or visitor), while the *ID Class* defines the risk level (No-Concern, Concern, or Threat). *Person Type* and *Image* can be edited in the Desktop Client by changing the *Person Type* on the People screen.

*ID Class* and all other attributes of a person are also edited within SAFR People dialog, accessed through the SAFR Desktop Client **Tools** menu. All identities are created by default with an *ID Class* of *No Concern*. To edit a person’s *ID Class*, open the People window from the SAFR Desktop Client **Tools** menu as follows:
The Person Type and Name can be edited by clicking the respective fields on the People screen. To edit ID Class, double-click the person, and choose the desired value from the ID Class menu in the People Edit dialog as shown in the following graphic:

![Person Edit Dialog](image)

### 2.5 SAFR Events

You can use SAFR to generate events. When enabled on the Events Preferences page, events occur when a person appears in the view of a connected camera. When a person appears in the camera’s view, they’re immediately assigned an ID Class attribute, although that ID Class may change if the system successfully recognizes them and assigns them a more appropriate ID Class. The types of ID Classes are listed below.

- Unrecognizable: A face was detected but it wasn’t of sufficient quality to attempt recognition.
- Stranger: The person has been recognized, but they’re not in Genetec’s cardholder database nor in SAFR’s Person Directory.
- Registered person without a name.
- Registered person with a name.
- Registered person marked as a Concern.
- Registered person marked as a Threat.

The following table lists the available events that are SAFR makes available to Digifort.

<table>
<thead>
<tr>
<th>Event Message</th>
<th>Id Class</th>
<th>Named</th>
<th>Person Type</th>
<th>Condition</th>
<th>People Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unrecognizable face detected</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Face detected but insufficient information for recognition</td>
<td>idClass=&quot;unidentified&quot;</td>
</tr>
<tr>
<td>Event Message</td>
<td>Id Class</td>
<td>Named</td>
<td>Person Type</td>
<td>Condition</td>
<td>People Attributes</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------</td>
<td>-------</td>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Stranger detected</td>
<td>Stranger</td>
<td>N/A</td>
<td>N/A</td>
<td>Face detected but not found in registered people</td>
<td>idClass=&quot;stranger&quot;</td>
</tr>
<tr>
<td>Registered person detected</td>
<td>Normal</td>
<td>No</td>
<td>None</td>
<td>Registered person without name or person type assigned</td>
<td>idClass=&quot;noconcern&quot; &amp;&amp; person-Type=&quot;&quot; &amp;&amp; name=&quot;&quot;</td>
</tr>
<tr>
<td>without name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registered person detected</td>
<td>Normal</td>
<td>Yes</td>
<td>None</td>
<td>Registered person with name but no person type</td>
<td>idClass=&quot;noconcern&quot; &amp;&amp; person-Type=&quot;&quot; &amp;&amp; name=&lt;name&gt;</td>
</tr>
<tr>
<td>with name &lt;name&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registered person detected</td>
<td>Normal</td>
<td>No</td>
<td>Defined</td>
<td>Registered person with person type and name</td>
<td>idClass=&quot;noconcern&quot; &amp;&amp; person-Type=&lt;personType&gt; &amp;&amp; name=&lt;name&gt;</td>
</tr>
<tr>
<td>of type &lt;personType&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registered person detected</td>
<td>Concern</td>
<td>No</td>
<td>None</td>
<td>Same as above for Concern</td>
<td>idClass=&quot;concern&quot; &amp;&amp; person-Type=&quot;&quot; &amp;&amp; name=&quot;&quot;</td>
</tr>
<tr>
<td>without a name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concern</td>
<td>Concern</td>
<td>Yes</td>
<td>None</td>
<td>Same as above for Concern</td>
<td>idClass=&quot;concern&quot; &amp;&amp; person-Type=&quot;&quot; &amp;&amp; name=&lt;name&gt;</td>
</tr>
<tr>
<td>person detected with name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;name&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concern</td>
<td>Concern</td>
<td>No</td>
<td>Defined</td>
<td>Same as above for Concern</td>
<td>idClass=&quot;concern&quot; &amp;&amp; person-Type=&lt;personType&gt; &amp;&amp; name=&quot;&quot;</td>
</tr>
<tr>
<td>person detected of type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;personType&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concern</td>
<td>Concern</td>
<td>Yes</td>
<td>Defined</td>
<td>Same as above for Concern</td>
<td>idClass=&quot;concern&quot; &amp;&amp; person-Type=&lt;personType&gt; &amp;&amp; name=&lt;name&gt;</td>
</tr>
<tr>
<td>person detected of type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;personType&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Concern</td>
<td>Threat</td>
<td>No</td>
<td>None</td>
<td>Same as above for Threat</td>
<td>idClass=&quot;threat&quot; &amp;&amp; person-Type=&quot;&quot; &amp;&amp; name=&quot;&quot;</td>
</tr>
</tbody>
</table>
2.5.1 SAFR Video Processing Modes

SAFR has different video processing modes that control what events are generated. Below is a short summary of the modes most relevant to Digifort integration. For a complete description, see Connect to a Video Feed in the SAFR Documentation.

- **Secure Access**: Only triggers events when cardholders and people registered in SAFR’s Person Directory are identified with a high degree of certainty. This mode is useful when the system is being used to manage physical access. (i.e. When the system is responsible for unlocking doors for authenticated people.)
- **Secure Access with Smile**: Similar to Secure Access mode, except that registered people must smile in order to cause the system to grant them access.
- **Enrolled Monitoring**: Similar to Secure Access mode, but events are triggered at a lower recognition confidence level.
- **Enrolled and Stranger Monitoring**: Similar to Enrolled Monitoring mode, but events are also triggered for strangers.

2.5.2 Alarms and Notifications

You can also use SAFR to view recognition events. Recognition events occur when a known, unknown, or unrecognized person appears in the view of a camera. The types of recognized persons are:

- Unrecognizable: A face was detected but it wasn’t of sufficient quality to attempt recognition.
- Stranger.
- Registered person without a name.
- Registered person with a name.
- Registered person marked as a *Concern*.
- Registered person marked as a *Threat*.

There are several different combinations of these conditions that are triggered. The following graphic shows multiple events populated in the Digifort alerts panel:
2.6 Troubleshooting Tips

**Note:** When closing SAFR, use the Quit SAFR option on the **File** menu. Closing SAFR using the Window Close button will cause you to lose the SAFR state settings and connected cameras for that window.

- If detection or recognition results in few faces found or recognized, check that the Digifort video feeds are of a sufficiently large frame size.
- If Digifort cameras do not appear in the SAFR Desktop Client, make sure you have added cameras to Digifort as described in Connect Your Cameras to Digifort.
- If events are not being triggered, ensure the correct SAFR video processing mode is selected.