# Windows SAFR® Documentation

Documentation Version = 2.007

Publish Date = April 12, 2020

# Contents

# 1 What's New

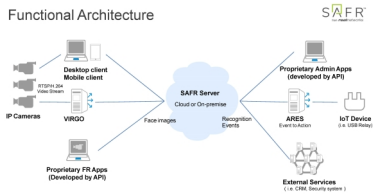
The following features are new in the May 2020 SAFR release:

- **Added Mask Detection integration**. Only available on Windows. An enhanced mask recognition model has been implemented that greatly increases SAFR's ability to recognize people even when they're wearing a mask. Only standard blue or white surgical masks are currently supported; SAFR is unable to use the enhanced mask recognition model with masks of different colors or with masks that have customized patterns. Mask detection can be configured on the Recognition Preferences tab of the Windows Desktop client.
- **Added Intel RealSense camera support**. Only available on Windows.
- **Added 3D Liveness Detection**. (Beta Feature) Only available on Windows. 3D liveness is a special feature of Intel RealSense cameras that allows them to distinguish flat images from 3 dimensional ones, thus allowing SAFR to tell the difference between a real face and a photo. This feature only works with Intel RealSense cameras; if you don't have any cameras of this type connected to SAFR, then this feature will not work. 3D Liveness Detection can be configured on the Recognition Preferences tab of the Windows Desktop client.

# 2 SAFR Overview

SAFR is a facial recognition system that integrates cameras, door locks, and alert systems with face recognition technology to enhance access control and security. It runs on a variety of operating systems, including Windows, macOS, Linux, iOS, and Android.

## 2.1 SAFR Components




SAFR primarily consists of the following components:

- **SAFR Server**: Available for Windows, macOS, and Linux. The SAFR Server installation contains the recognition engine, event server, several databases, and the Web Console. The databases contain stored enrolled face images, the identity information for the stored faces, and recognition events that have been generated by the SAFR system.
  The SAFR Server runs as several background services that automatically start on system reboot and are kept active by the operating system. They must be running at all times for the system to be operational. All other SAFR components must connect to a SAFR Server, although if you're doing a cloud deployment you'll be connecting to a SAFR Server in the cloud that RealNetworks maintains.
- **Desktop client**: Available for Windows and macOS. The Desktop client is one of the primary ways that administrators and operators can interact with the SAFR system. As such, the client can be used to enable camera connectivity, monitor video camera feeds, register users, view recognition events, and more.
- **Mobile client**: Available for Android and iOS. The Mobile client converts a mobile device into a registration kiosk or a recognition panel. Registration kiosks allow people to self-register their face into the Identity Database so they can be approved for access or granted other privileges. Recognition panels enable the mobile device to scan the faces of people that walk by and to compare those faces against faces in the Identity Database. Mobile devices set up as recognition panels can also provide visual or audio feedback to the person viewing the mobile device based on actions that a SAFR administrator has configured.
- **VIRGO**: Available as a standalone download for macOS and Linux. It's also available as part of the SAFR Desktop, SAFR Edge, and SAFR Platform download packages for Windows, macOS, and Linux. The Video Recognition Gateway (VIRGO) is a daemon system which receives video feeds from one or more cameras and recognizes and tracks faces in those video streams in real time. It generates tracking events and sends those events to an event server. The VIRGO daemon can be controlled either by the command line tool or through the Video Recognition Gateway Administration (VIRGA) command & control server.
- **Web Console**: Available on all platforms. The Web Console provides administrators and operators web-based access to the SAFR system. As such, the Web Console can be used to generate analytical reports, monitor video camera feeds, register users, view recognition events, and more.
- **ARES**: Available as a standalone download for all platforms. Actions Relay Event Service (ARES) is a cross-platform Java application that acts as the event listener that dispatches configured actions in response to events. ARES can provide replies on any event handled by the client that originates an event and is normally installed as a service when either SAFR Platform or SAFR Edge are installed. It is constantly active and is automatically started by the operating system on power-up.
- **SAFR Actions**: SAFR Actions is a GUI that facilitates configuring SAFRActions.config. SAFRActions.config is the file that defines all the defined actions for your SAFR System, as well as a couple fields that are used to connect ARES (and SAFR Actions) to your primary SAFR Server, whether that server is local or in the cloud. See Actions for more information about actions in SAFR.

In addition to the SAFR components listed above, SAFR also relies on a couple additional non-SAFR components:

- **IP Cameras**: As you might expect, Internet Protocol (IP) cameras are absolutely integral to SAFR. Both the Desktop client and VIRGO automatically detect integrated, USB, and Open Network Video Interface Forum (ONVIF) IP cameras. If an IP camera does not support ONVIF or doesn't have ONVIF enabled, you can still manually add it to the SAFR system as described here.
- **Physical access control devices**: Door locks, electronic gates, etc. can all be used by SAFR to grant or deny access to people, depending on whether or not they're identified as having the proper authorization.
- **Notification systems**: Email can be used to discretely notify specified people of various events, while general alarms can be used to alert everybody in the vicinity when unauthorized people attempt to force entry.
- **Additional external peripherals**: Any device that can be controlled by a computer language or protocol can be incorporated into the SAFR system.

## 2.2 Available Download Packages

The following download packages are available on the SAFR Download Portal:

- **SAFR Platform:** Available on Windows, macOS, and Linux. The SAFR Platform installs everything you need to set up a local deployment of SAFR. This downlaod package enables a locally deployed system to be easily deployed on a single computer and afterwards expanded to additional computers as needed. See Getting Started with SAFR Platform on Windows or macOS for more information.
- **SAFR Desktop:** Available on Windows and macOS. Installs the Desktop client and one of the VMS extensions. Windows has an additional download variant called SAFR Desktop Lite which has fewer features and lower system requirements.
- **SAFR Edge:** Available on Windows and macOS. SAFR Edge installs the Desktop client as well as SAFR Actions, a programmable interface to create and manage responses to event triggers. For example, you can unlock a door, turn on a light, send an alert, and so on. See Getting Started with SAFR Edge with a Cloud Account for more information.
- **SAFR Mobile:** Available on Android and iOS. Installs the Mobile client. When you download SAFR Mobile for Android, you're also offered the SAFR Beam download. SAFR Beam allows you to enable the more secure Lock Task Mode on your Android device. If you don't install SAFR Beam, then Android devices can only enable the less secure Screen Pinning Mode. See Configure Devices into Locked Mode for more information.
- **Actions Relay Event Service (ARES):** Available on all platforms. Installs ARES.
- **Video Recognition Gateway (VIRGO):** Available on Linux and macOS. Installs VIRGO.

## 2.3 Deployment Types

There are two types of SAFR deployment: cloud and local. Each deployment type requires its own account type; a cloud deployment requires a SAFR Cloud Account, while a local deployment requires a SAFR Local Account. Contact your SAFR Account Manager to obtain either type of account.

### 2.3.1 Cloud Deployment

When SAFR is deployed as a cloud deployment, all your SAFR components are deployed locally except for the SAFR Server. Your components will connect to a SAFR Server located in the cloud which is operated by RealNetworks, Inc. Using the cloud SAFR Server greatly simplifies deployment and maintenance, but it requires a network connection to the cloud at all times in order to be operational.

A single installation of the Desktop client can handle about 16 connected cameras, assuming the hosting machine meets the recommended system requirements listed here. Expanding your SAFR system beyond this limitation is fairly easy; simply install additional Desktop clients onto additional machines.

### 2.3.2 Local Deployment

When SAFR is deployed as a local deployment, all of the SAFR components (including SAFR Server) are installed locally. During installation a connection is made to a SAFR License Server in the cloud to obtain a licence, but after a license has been obtained, local deployments do not require a connection to the cloud.

A single installation of the SAFR Server can handle about 25 viewed faces at one time, assuming the hosting machine meets the recommended system requirements listed here. Note that for the purposes of server capacity, “25 viewed faces” can mean “25 cameras with 1 face in each camera view” or “1 cameras with 25 faces in its camera view”, or anything in between. If you want to expand your SAFR system beyond this limitation please see Large Scale Deployments.

# 3 SAFR System Requirements

## 3.1 Windows Requirements

| Product | Description | Minimum Requirements | Recommended Requirements |
|---|---|---|---|
| Desktop client | One of the adminstration consoles for SAFR. Use the Desktop client to connect to a camera, video feed, detect faces, and submit images to the SAFR Server for recognition. | • Windows Server 2016 or Windows 8.1<br>• .NET Framework 4.6.2 or later<br>• Intel Core i5-8259U or AMD Ryzen 7 2700X<br>• NVIDIA GT 1030 2GB<br>• 1GB RAM per connected camera<br>• 1.5GB available storage<br>• Supports 2-3 4K cameras[1]<br>• Supports 4+ 1080p cameras[1] | • Windows Server 2016 or Windows 10<br>• .NET Framework 4.6.2 or later<br>• Intel Core i9-7980XE or AMD Ryzen 7 2700X<br>• NVIDIA GTX 1050Ti 4GB<br>• NVIDIA driver 418.96+ for GPU-enhanced performance<br>• 1GB RAM per connected camera<br>• 1.5GB available storage<br>• Supports up to eight 4K cameras[1]<br>• Supports 9+ 1080p cameras[1] |
| Desktop Lite | A version of the Desktop client with fewer features and lower system requirements. | • Windows Server 2016 or Windows 8.1<br>• .NET Framework 4.6.2 or later<br>• Intel Core i5-7260U<br>• NVIDIA GT 1030 2GB<br>• 0.2GB RAM per connected camera<br>• 0.5GB available storage | • Windows Server 2016 or Windows 10<br>• .NET Framework 4.6.2 or later<br>• Intel Core i7-8750H<br>• NVIDIA GTX 1050Ti 4GB<br>• 0.2GB RAM per connected camera<br>• 0.5GB available storage |
| SAFR Actions | Actions allow you to create and manage responses to event triggers; deploy them to unlock a door, turn on a light, send an alert, record data for reporting, or any security response to fit the use case. | • Windows Server 2016 or Windows 8.1<br>• Intel Core i5-7260U or AMD Ryzen 7 2700X<br>• 1GB RAM<br>• 1GB available storage | • Windows Server 2016 or Windows 10<br>• Intel Core i5-8259U or AMD Ryzen 7 2700X<br>• 1GB RAM<br>• 1GB available storage |

| Product | Description | Minimum Requirements | Recommended Requirements |
|---|---|---|---|
| SAFR Server[2] | The trusted engine of SAFR solutions, the SAFR Server includes: the facial recognition server, identity database, recognition event server, event archive, report server, and remote video feed administration servers. | • Windows Server 2016 or Windows 8.1<br>• .NET Framework 4.6.2 or later<br>• Intel Core i9-7980XE or AMD Ryzen TR 1950X<br>• NVIDIA GTX 1050Ti 4GB<br>• NVIDIA driver 418.96+ for GPU-enhanced performance<br>• 16GB RAM<br>• 1TB available storage | • Windows Server 2016 or Windows 10<br>• .NET Framework 4.6.2 or later<br>• Intel Core i9-7980XE or AMD Ryzen TR 1950X<br>• NVIDIA GTX 1050Ti 4GB<br>• NVIDIA driver 418.96+ for GPU-enhanced performance<br>• 32GB RAM<br>• 1TB available storage |

1 = Number of cameras is based on an average of five visible faces in a 4K resolution camera view, running at 15 frames per second. Using fewer faces per camera and lower resolution will enable support for more cameras.

2 = Installed as part of the SAFR Platform installer.

## 3.2 Jetson Requirements

| Product | Description | Minimum Requirements | Recommended Requirements |
|---|---|---|---|
| Desktop client | Not available on Jetson. | N/A | N/A |
| SAFR Actions | Not available on Jetson. | N/A | N/A |
| SAFR Server[1] | The trusted engine of SAFR solutions, SAFR Server includes: the facial recognition server, identity database, recognition event server, event archive, report server, and remote video feed administration servers. | • Linux Ubuntu 18.04<br>• 6GB RAM<br>• 5.5GB available storage<br>• Jetson TX2<br>• Jetson Xavier | • Linux Ubuntu 18.04<br>• 6GB RAM<br>• 5.5GB available storage<br>• Jetson TX2<br>• Jetson Xavier |

1 = Installed as part of the SAFR Platform installer.

## 3.3 Mobile Requirements

| Product | Description | Minimum Requirements | Recommended Requirements |
|---|---|---|---|
| Mobile client for iOS | Set up a registration kiosk, perform facial recognition, and add users — all from a mobile device. | • iOS 11.0<br>• iPad Pro or iPhone 6/7/8/X | • iOS 11.0<br>• iPad Pro or iPhone 6/7/8/X |
| Mobile client for Android | Set up a registration kiosk, perform facial recognition, and add users — all from a mobile device. | • Android 5.0 with Google Play Services 13.2.74 or later<br>• Quad-core Snapdragon 802 2.5GHz<br>• 2GB RAM<br>• 13MB available storage | • Android 6.0<br>• Quad-core Snapdragon 802 2.5GHz<br>• Samsung Galaxy Tab S4<br>• Samsung Galaxy S8<br>• Google Pixel 2 XL<br>• 2GB RAM<br>• 13MB available storage |
| SAFR Beam for Android | This SAFR utility allows you to configure Android mobile devices for secure SAFR operation. | • Android 6.0<br>• Near-Field Communication (NFC) support required<br>• 1MB RAM<br>• 8MB available storage | • Android 6.0<br>• Near-Field Communication (NFC) support required<br>• 1MB RAM<br>• 8MB available storage |

## 3.4 SDK Requirements

| Product | Description | Minimum Requirements | Recommended Requirements |
|---|---|---|---|
| Windows SAFR SDK, Lite Edition | Create a Windows app that can be used to locate and track faces and/or badges in a video file or live video stream. The Lite Edition lacks GPU acceleration, but it has a smaller footprint. | • Windows 8.1 64-bit<br>• C# 7.0<br>• 1GB RAM per 4k video stream<br>• 60MB available storage | • Windows 10 64-bit<br>• Microsoft Visual C++ (MSVC) 2017 or newer is strongly recommended<br>• C# 7.0<br>• 1GB RAM per 4k video stream<br>• 60MB available storage |

| Product | Description | Minimum Requirements | Recommended Requirements |
|---|---|---|---|
| Windows SAFR SDK, Standard Edition | Create a Windows app that can be used to locate and track faces and/or badges in a video file or live video stream. The Standard Edition has GPU acceleration. | • Windows 8.1 64-bit<br>• C# 7.0<br>• 1GB RAM per 4k video stream<br>• 0.5GB available storage<br>• NVIDIA GTX 1030 or better<br>• NVIDIA driver 418.96 or later | • Windows 10 64-bit<br>• Microsoft Visual C++ (MSVC) 2017 or newer is strongly recommended<br>• C# 7.0<br>• 1GB RAM per 4k video stream<br>• 0.5GB available storage<br>• NVIDIA GTX 1080 Ti<br>• NVIDIA driver 418.96 or later |
| Linux SAFR SDK, Lite Edition | Create a Linux app that can be used to locate and track faces and/or badges in a video file or live video stream. The Lite Edition lacks GPU acceleration, but it has a smaller footprint than the Standard Edition. | • Ubuntu 16 or 18<br>• If Ubuntu 18 is used, you may need to downgrade the OpenSSL installation to version 3.<br>• 1GB RAM per 4k video stream<br>• 60MB available storage<br>**Install the following additional software components to allow VIRGO to run successfully:**<br>• libcurl3<br>• libgomp1<br>• libatomic1<br>• libbsd0<br>• libv4l-0 | • Ubuntu 16 or 18<br>• If Ubuntu 18 is used, you may need to downgrade the OpenSSL installation to version 3.<br>• 1GB RAM per 4k video stream<br>• 60MB available storage<br>**Install the following additional software components to allow VIRGO to run successfully:**<br>• libcurl3<br>• libgomp1<br>• libatomic1<br>• libbsd0<br>• libv4l-0 |

| Product | Description | Minimum Requirements | Recommended Requirements |
|---|---|---|---|
| Linux SAFR SDK, Standard Edition | Create a Linux app that can be used to locate and track faces and/or badges in a video file or live video stream. The Standard Edition has GPU acceleration. | • Ubuntu 16 or 18<br>• If Ubuntu 18 is used, you may need to downgrade the OpenSSL installation to version 3.<br>• 1GB RAM per 4k video stream<br>• 0.5GB available storage<br>• NVIDIA GTX 1080 Ti<br>• NVIDIA driver 418.96 or later<br>**Install the following additional software components to allow VIRGO to run successfully:**<br>• libcurl3<br>• libgomp1<br>• libatomic1<br>• libbsd0<br>• libv4l-0 | • Ubuntu 16 or 18<br>• If Ubuntu 18 is used, you may need to downgrade the OpenSSL installation to version 3.<br>• 1GB RAM per 4k video stream<br>• 0.5GB available storage<br>• NVIDIA GTX 1080 Ti<br>• NVIDIA driver 418.96 or later<br>**Install the following additional software components to allow VIRGO to run successfully:**<br>• libcurl3<br>• libgomp1<br>• libatomic1<br>• libbsd0<br>• libv4l-0 |
| macOS SAFR SDK | Create a macOS app that can be used to locate and track faces in a video file or live video stream. | • macOS 10.12<br>• 1GB RAM per 4K video stream<br>• 215MB available storage | • macOS 10.14<br>• 1GB RAM per 4K video stream<br>• 215MB available storage |
| iOS SAFR SDK | Create an iOS app that can be used to locate and track faces in a video file or live video stream. | • iOS 11 or higher<br>• iPhone 6<br>• Swift 5<br>• 92MB available storage | • iOS 12<br>• iPhone X or iPad Pro<br>• Swift 5<br>• 92MB available storage |
| Android SAFR SDK | Create an Android app that can be used to locate and track faces in a video file or live video stream. | • Android 6.0<br>• 1GB RAM<br>• 0.5GB available storage | • Android 6.0<br>• 1GB RAM<br>• 0.5GB available storage |

## 3.5 Embedded SDK Requirements

| Product | Description | Minimum Requirements | Recommended Requirements |
|---|---|---|---|
| Android SAFR Embedded SDK | Build a facial recognition app on an Android device with limited resources (RAM, CPU, or memory). | • Android 6.0<br>• ARM Architecture<br>• 200MB RAM<br>• 150MB available storage | • Android 6.0<br>• ARM Architecture<br>• 200MB RAM<br>• 150MB available storage |
| Windows SAFR Embedded SDK, Lite Edition | Build a facial recognition app on a Windows device with limited resources (RAM, CPU, or memory). The Lite Edition lacks GPU acceleration, but it has a smaller footprint than the Standard Edition. | • Windows 8.1 64-bit<br>• 200MB RAM<br>• 60MB available storage | • Windows 10 64-bit<br>• 200MB RAM<br>• 60MB available storage |
| Windows SAFR Embedded SDK, Standard Edition | Build a facial recognition app on a Windows device with limited resources (RAM, CPU, or memory). The Standard Edition has GPU acceleration. | • Windows 8.1 64-bit<br>• 200MB RAM<br>• 0.5GB available storage<br>• NVIDIA GTX 1030 or better<br>• NVIDIA driver 418.96 or later | • Windows 10 64-bit<br>• 200MB RAM<br>• 0.5GB available storage<br>• NVIDIA GTX 1080 Ti<br>• NVIDIA driver 418.96 or later |
| Linux x86 SAFR Embedded SDK, Lite Edition | Build a facial recognition app on a Linux x86 device with limited resources (i.e. RAM, CPU, or memory). The Lite Edition lacks GPU acceleration, but it has a smaller footprint than the Standard Edition. | • Ubuntu 16.04 or later<br>• 500 MB RAM | • Ubuntu 16.04 or later<br>• 500 MB RAM |
| Linux x86 SAFR Embedded SDK, Standard Edition | Build a facial recognition app on a Linux x86 device with limited resources (RAM, CPU, or memory). The Standard Edition has GPU acceleration. | • Ubuntu 16.04 or later<br>• 1500 MB RAM<br>• Nvidia GPU GTX10xx or later | • Ubuntu 16.04 or later<br>• 1500 MB RAM<br>• Nvidia GPU GTX10xx or later |
| Linux ARM SAFR Embedded SDK | Build a facial recognition app on a Linux ARM device with limited resources (RAM, CPU, or memory). | • Ubuntu 18.04 or later<br>• 64bit ARMv8 CPU<br>• 200 MB RAM | • Ubuntu 18.04 or later<br>• 64bit ARMv8 CPU<br>• 200 MB RAM |

| Product | Description | Minimum Requirements | Recommended Requirements |
|---|---|---|---|
| Jetson SAFR Embedded SDK | Build a facial recognition app on a Jetson device with limited resources (RAM, CPU, or memory). | The following Jetson devices are supported:<br>• Nvidia Jetson TX2<br>• Nvidia Jetson Xavier<br>• Nvidia Jetson Nano | The following Jetson devices are supported:<br>• Nvidia Jetson TX2<br>• Nvidia Jetson Xavier<br>• Nvidia Jetson Nano |

# 4 Licensing

SAFR systems require a license to operate.

## 4.1 License Limit Metrics

SAFR licenses limit usage according to the following metrics:

- **Expiration date**: The date when the SAFR license expires. After this date, SAFR software discontinues operation.
- **Max Feeds per Hour**: Maximum number of video feeds that can be used at one time by the SAFR system. If you attempt to connect more video feeds than your license allows, the excess video feed connection attempts will all fail. Existing video feeds must be disconnected for a period of 1 hour before new video feeds are allowed to re-use the license.
  **Note**: If a single camera is providing video feeds to 2 different Desktop client instances, that counts as 2 video feeds for licensing purposes.
- **Max Faces**: Maximum number of people that can be registered with the SAFR system's Person Directory. Attempting to add people above this limit results in an error.
- **Max Days Between Reports**: The maximum elapsed time that can pass before the SAFR system can report its status to a SAFR License Server. SAFR Server discontinues operation if it is unable to reach the SAFR License Server after the specified time has elapsed. If you need to operate your SAFR system on a private network that isn't connected to the Internet, contact your SAFR account manager to acquire a special offline license.
  **Note**: This metric is only applicable for local deployments.

License limit metrics for your SAFR license can be found on the Status page of the Web Console. Note that *Max Days Between Reports* won't appear on your Web Console if you have a cloud deployment.

## 4.2 Licensing for Local Deployments

In local deployments, SAFR licenses are attached to your SAFR system's primary server. The following describes how the SAFR license is managed:

- License Acquisition - Your SAFR Server attempts to acquire a license from the SAFR license server when it's first run. If your SAFR system doesn't have Internet connectivity, see the Offline Licensing section below to see how to obtain a SAFR license.
- Licenses are bound to the primary SAFR Server. If you install one or more secondary servers for the purpose of load balancing or redundancy, the secondary servers acquire their licenses through the primary server.
- If you want to move your primary server to a machine with a different IP address, you must wait 24 hours between uninstalling the server and reinstalling it on the new machine. If you try to reinstall the SAFR Server before 24 hours has elapsed, you will get an unauthorized access error when the SAFR Server unsuccessfully attempts to get a valid licence from the SAFR License Server. After 24 hours has elapsed, however, a reinstalled SAFR Server will automatically (and successfully) reacquire a SAFR license.
  - Note that the previous behavior only applies to SAFR servers that are **uninstalled**. If, on the other hand, the IP address of your SAFR Server changes or changes to a hostname while the server remains installed, there is no problem; your server simply informs the SAFR License Server of its new IP address or hostname the next time it checks in with the SAFR License Server.

## 4.3 Offline Licensing

If your SAFR system doesn't have Internet connectivity, do the following to get a SAFR license:

1. Obtain a license request file for the machine on which SAFR Platform is installed.
   1. On the machine that has SAFR Platform installed, run get-license-request.py.
      - For Windows: `C:\Program Files\RealNetworks\SAFR\bin\get-license-request.py`

    2. When prompted, enter the SAFR account name and password.
    3. The script will attempt to read *safrports.conf* to communicate with CoVi. If *safrports.conf* can't be found, then the script will use the default port, 8080.
    4. The script can be copied and run from any system that has Python 3 installed. If you run the script on a machine other than the one hosting SAFR Platform, use the -n parameter to provide the hostname of the machine hosting SAFR Platform.
    5. Running the script generates a file called *safr_license_request.json* in the same working directory as the script. Make sure to run the script in a directory that you have write access to.
2. Retrieve the license by sending the license request to SAFR Cloud.
    1. Copy the newly generated *safr_license_request.json* file and the script get-license.py to a machine that has Internet access and has Python 3 installed. get-license.py can be found at the following locations:
        - For Windows: `C:\Program Files\RealNetworks\SAFR\bin\get-license.py`
    2. When prompted, enter the SAFR account name and password.
    3. You can use the -p parameter to tell the script where *safr_license_request.json* is located.
    4. You can use the -e parameter to set the environment value. (i.e. *prod*, *int2*, or *dev*) The default is *prod*.
    5. Running the script generates a file called *safr_license.json* in the same working directory as the script. Make sure to run the script in a directory that you have write access to.
3. Install the retrieved license onto your installed SAFR Platform.
    1. Copy *safr_license.json* to the machine running your SAFR Platform.
    2. Run insert-license.py to install the license onto your SAFR installation.
        - For Windows: `C:\Program Files\RealNetworks\SAFR\bin\insert-license.py`
    3. When prompted, enter the SAFR account name and password.
    4. The script will attempt to read *safrports.conf* to communicate with CoVi. If *safrports.conf* can't be found, then the script will use the default port, 8080.

# 5 Getting Started with SAFR Platform on Windows or macOS

The computer used for the first installation of SAFR Platform acts as the primary server for the entire SAFR system. The primary server acquires a SAFR license that is then restricted to that machine. (See Licensing for details.) Any additional instances of SAFR Server you install under the same SAFR Local Account must be configured as secondary servers for the purposes of load balancing or redundancy and are linked to the primary server as described in Large Scale Deployments.

## 5.1 SAFR Platform Contents

The Windows SAFR Platform installation includes the following:

- **SAFR Server**: Includes the recognition engine, event server, several databases, and the Web Console. The databases contain stored enrolled face images, the identity information for the stored faces, and recognition events that have been generated by the SAFR system.
- **Desktop client**: One of the primary ways that administrators and operators can interact with the SAFR system. As such, the client can be used to enable camera connectivity, monitor video camera feeds, register users, view recognition events, and more.
- **Web Console**: Provides web-based access to the SAFR system. As such, the Web Console can be used to generate analytical reports, monitor video camera feeds, register users, view recognition events, and more.
- **SAFR Actions**: SAFR Actions is a GUI that facilitates configuring SAFRActions.config. SAFRActions.config is the file that defines all the defined actions for your SAFR System, as well as a couple fields that are used to connect ARES (and SAFR Actions) to your primary SAFR Server, whether that server is local or in the cloud. See Actions for more information about actions in SAFR.
- **ARES**: Actions Relay Event Service (ARES) is a cross-platform Java application that acts as the event listener that dispatches configured actions in response to events. ARES can provide replies on any event handled by the client that originates an event and is normally installed as a service when either SAFR Platform or SAFR Edge are installed. It is constantly active and is automatically started by the operating system on power-up.
- **0 or 1 of the VMS extensions**
- **VIRGO for Windows**: A version of VIRGO with fewer features than the normal VIRGO product. It allows Windows machines to monitor video feeds with a daemon process so that the Desktop client no longer needs to remain open for feeds to be monitored.

## 5.2 Prerequisites

Before you begin the installation, ensure that you have the following prerequisites:

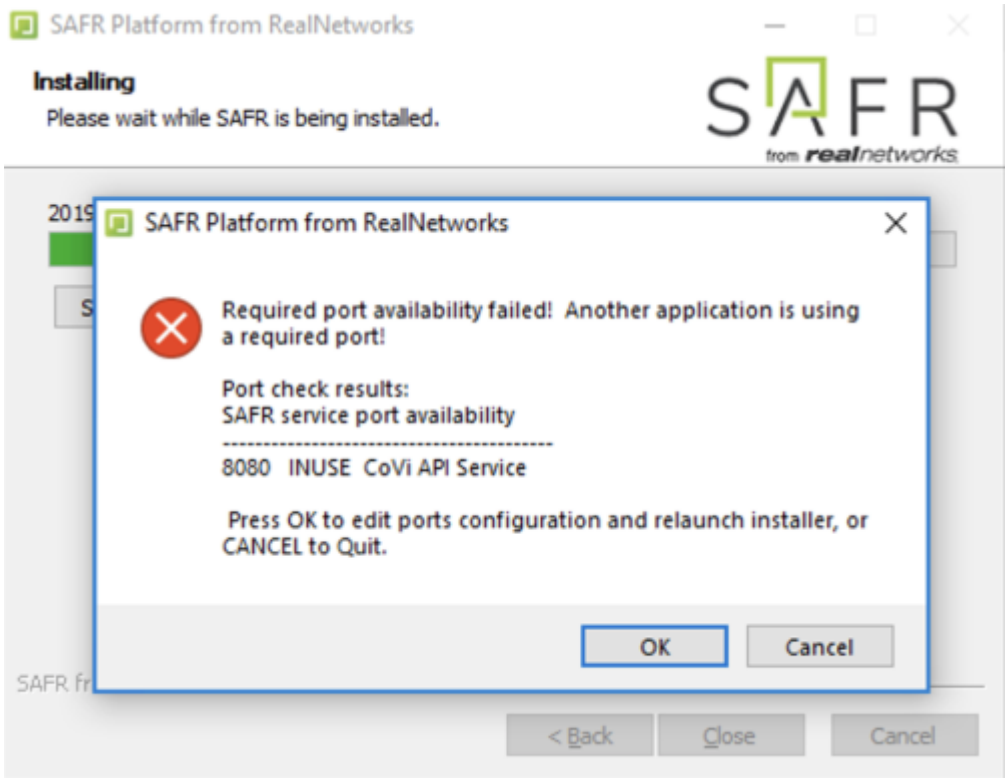
- **SAFR Local Account**: If you're not sure which account type you have, go to the SAFR Download Portal. If SAFR Platform is listed among the downloads, then you have a SAFR Local Account.
- **System requirements**: Ensure that your system meets the minimum system requirements listed here.
- **An up-to-date SAFR License**: See Licensing for information about SAFR Licenses.
- **SSL certificate**: SSL certificates are required if you want your SAFR Server to support HTTPS connections. If you don't care if HTTPS connections are supported, this prerequisite may be skipped. See SSL Certificate Installation for information about how to get an SSL Certificate.
  **Note:** There are 2 situations where SAFR requires that your server supports HTTPS connections:
  1. **iOS Devices**: The iOS Mobile client can only connect to the SAFR Server over HTTPS, so you must obtain an SSL certificate if you want to run the Mobile client on any iOS devices.
  2. **Additional SAFR Servers**: SAFR Servers can only connect to each other over HTTPS, so you must obtain an SSL certificate if you want to install additional SAFR servers. Additional SAFR Servers are used when you want to scale your SAFR system beyond the procesing capacity of a single machine. See Large Scale Deployments for additional information.

## 5.3 Download and Install SAFR Platform

To download and install SAFR Platform using, do the following:

1. On the computer where you want to install SAFR Server, open a web browser and go to the SAFR Download Portal.
2. Sign in with your SAFR Local Account's credentials.
3. Once signed in, select your operating system from the menu and download the appropriate SAFR Platform installer.
4. After the download is complete, start the installation.
5. The Platform installer displays a *Choose Components* window where you can choose the features you want to install, such as:
    - SAFR Face Attribute Recognition
        - Age
        - Gender
        - Occlusion
        - Sentiment
        - Optimize GPU models
    - SAFR Peripheral Sub-systems
        - SAFR Actions (If you choose to install SAFR Actions, ARES will automatically also be installed.)
        - SAFR Reports
        - SAFR Logs
        - SAFR Web Console
        - SAFR Video Recognition Gateway (VIRGO)
        - SAFR Video Recognition Gateway Administrator (VIRGA)
    - VMS Extensions
        - Digifort
        - Genetec Security Center
        - Genetec Security Center with FaceRec
        - Milestone XProtect
    - Camera Extensions
        - Ximea
    - GPU Support
        - NVIDIA Accelerated Detection
        - NVIDIA Accelerated Recognition
    - SAFR Application (This refers to the Desktop client)

    You may uncheck the boxes for any features you do not want to install. We recommend installing all the components except the VMS extensions the first time you install SAFR Platform.
    In addition to whatever components you selected, SAFR Platform also always installs SAFR Server.
6. Follow the installer prompts as they guide you through the rest of the installation process. The final phase of the installation may take a few minutes to complete as it installs dependencies and runs the configuration scripts. Allow it to continue without interruption.
7. On Windows 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 automatically runs as a collection of background services.

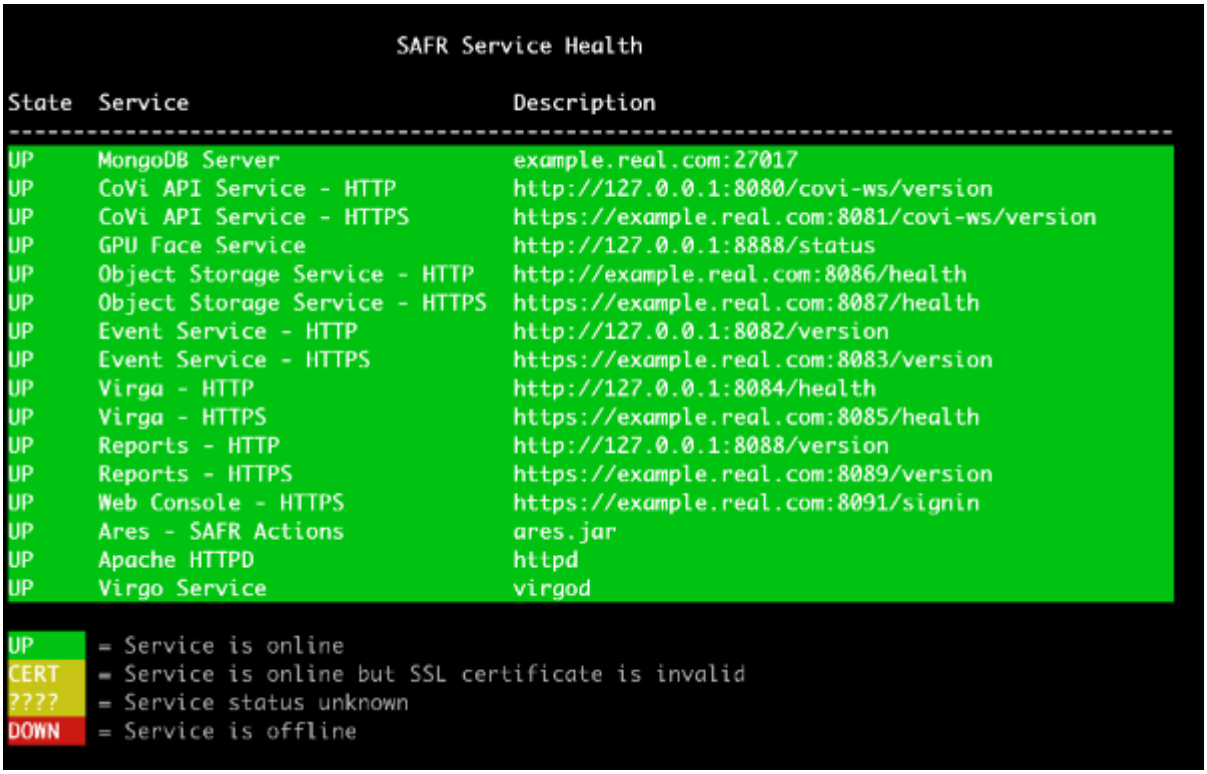
Immediately following installation, the Platform installer opens the Desktop client and prompts you to log in with your SAFR Local Account. Make sure to log in; it's important in acquiring the SAFR license.

## 5.4 Check Server Status

To check the status of your SAFR Server, use the *check* script. See the table below for the location of the script.

| Platform | Script Name | File Location |
|---|---|---|
| Windows | check.bat | `C:\Program Files\RealNetworks\SAFR\bin` |

The *check* script displays the status of all SAFR services. The following screenshot shows a server installation with healthy statuses for all its services:




## 5.5 Connect Desktop Clients

A Desktop client that is installed on the same machine as the primary server is automatically connected with your primary server; no additional actions need to be taken.

Desktop clients that are installed on machines other than the primary server, however, need to be configured so they can connect with the primary server. Clients that aren't connected to a server are nearly useless and have very limited functionality.

To connect a remote Desktop client, do the following:

1. On the remote machine download and install either SAFR Desktop or SAFR Edge for your OS from the SAFR Download Portal.
2. Start the Desktop client. If prompted, cancel the camera login screen. Also cancel the SAFR Account login if it is displayed.
3. Click **Tools > Preferences**. On the **Account** tab, enter your user identifier and password for your SAFR Local Account.
4. Select *SAFR Custom* from the drop down menu of the *Environment* setting. Do one of the following: **Note**: If you customized ports when installing SAFR Server, use the customized port values instead of the values listed below.
   - If you are running the server without an SSL certificate, enter the following in the associated fields, substituting the server IP Address for **localhost**:
     - CoVi Server: http://localhost:8080/covi-ws
     - Event Server: http://localhost:8082
     - Object Server: http://localhost:8086
     - VIRGA Server: http://localhost:8084
   - If you are running the server with an SSL certificate, enter the following in the associated fields, substituting your server's hostname for **localhost**:
     - CoVi Server: https://localhost:8081/covi-ws
     - Event Server: https://localhost:8083

- Object Server: https://localhost:8087
- VIRGA Server: https://localhost:8085

5. Click **OK** to save the preference changes.

# 6 Getting Started with SAFR Edge with a Cloud Account

SAFR Edge installs the Desktop client as well as SAFR Actions, a programmable interface to create and manage responses to event triggers.

## 6.1 SAFR Edge Contents

The Windows SAFR Edge installation includes the following:

- **Desktop client**: One of the primary ways that administrators and operators can interact with the SAFR system. As such, the client can be used to enable camera connectivity, monitor video camera feeds, register users, view recognition events, and more.
- **SAFR Actions**: SAFR Actions is a GUI that facilitates configuring SAFRActions.config. SAFRActions.config is the file that defines all the defined actions for your SAFR System, as well as a couple fields that are used to connect ARES (and SAFR Actions) to your primary SAFR Server, whether that server is local or in the cloud. See Actions for more information about actions in SAFR.
- **ARES**: Actions Relay Event Service (ARES) is a cross-platform Java application that acts as the event listener that dispatches configured actions in response to events. ARES can provide replies on any event handled by the client that originates an event and is normally installed as a service when either SAFR Platform or SAFR Edge are installed. It is constantly active and is automatically started by the operating system on power-up.
- **0 or 1 of the VMS extensions**
- **VIRGO for Windows**: A version of VIRGO with fewer features than the normal VIRGO product. It allows Windows machines to monitor video feeds with a daemon process so that the Desktop client no longer needs to remain open for feeds to be monitored.

## 6.2 Prerequisites

Before you begin the installation, ensure that you have the following prerequisites:

- **SAFR Cloud Account**: If you're not sure which account type you have, go to the Download Portal. If SAFR Cloud is listed among the downloads, then you have a SAFR Cloud Account.
- **System requirements**: Ensure that your system meets the minimum system requirements listed here.
- **An up-to-date SAFR License**: See Licensing for information about SAFR Licenses.
- **An Internet connection**: Cloud deployments must maintain a network connection with the SAFR Server maintained by RealNetworks in the cloud at all times. Any components that lose their connection to the cloud will immediately lose almost all their functionality.

## 6.3 Download and Install SAFR Edge

To download and install SAFR Edge, do the following:

1. On the computer where you want to install SAFR Edge, open a web browser and go to the Download Portal.
2. Sign in with your SAFR Cloud Account's credentials.
3. Once signed in, select your operating system from the menu and download the appropriate SAFR Edge installer.
4. After the download is complete, start the installation.
5. The Edge installer displays a *Choose Components* window where you can choose the features you want to install, such as:
    - SAFR Actions (If you choose to install SAFR Actions, ARES will automatically also be installed.)
    - SAFR Video Recognition Gateway Administration (VIRGO)
    - VMS Extensions
        - Digifort
        - Genetec Security Center
        - Genetec Security Center with FaceRec

    - Milestone XProtect
- GPU Support
    - NVIDIA Accelerated Detection

      You may uncheck the boxes for any features you do not want to install. We recommend installing all the components except the VMS extensions the first time you install SAFR Edge.

6. Follow the installer prompts as they guide you through the rest of the installation process. The final phase of the installation may take a few minutes to complete as it installs dependencies and runs the configuration scripts. Allow it to continue without interruption.

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.

# 7 Recommendations for Camera Placement and Use

The best placement for cameras is at choke points where subjects tend to be looking straight ahead and traffic is going in one direction. Doorways are a common example of such a choke point. Doorways are also ideal in that they channel all subjects to a narrow access point where the pixel density of even a low resolution camera can be concentrated for the highest possible pixel density, resulting in higher quality recognition.

The top of an esccalator is another ideal spot for camera placement. Escalators have the added advantage that subjects tend to be looking up, which negates some of the problems introduced by headwear such as baseball caps. Just like doorways, escalators also allow the camera pixels to be concentrated on an very narrow region.

The one major challenge with placing cameras in doorways is the backlight. Strong backlight can result in either very dark or poor contrast on a person's face, thus diminishing recognition capability. See the Backlighting Considerations section below for a discussion about how to overcome backlight difficulties.

In the most common use cases, cameras are positioned either inside the building pointed at external doors or mounted just outside external entrances pointed at approaching subjects. The major challenge here is the lighting. You can face the following challenges:

- Very high contrast - The subjects might be incredibly dark with a very bright background.
- Highly variable lighting conditions - Opening doors can change lighting conditions right at the moment the subject is walking past; the camera is still trying to adjust to the lighting conditions. This is especially true with automatic doors that open wide and remain open for a period of time.
- Daily light variations - The amount and quality of the light varies greatly between direct sunlight, indirect sunlight, daylight when it's cloudy, and nighttime.

Camera recognition accuracy should be tested under the following conditions:

- Bright sunny daytime conditions.
- Cloudy daytime conditions.
- Nighttime conditions.

## 7.1 Camera Positioning

We recommend that you obey the following guidelines whenever possible:

- If inside a building, place camera 20-30 feet in front of the door and about 10-12 feet high.
- The subject should be facing the camera nearly straight on.
- Camera resolution should be such that subjects' faces are at least 80 pixels high (120 is optimal) when at the door, larger if possible.
- When attempting to learn subjects, pixel density should be 180 or higher. (220 is optimzal.)

## 7.2 Backlighting Considerations

There are three basic strategies to overcome backlight:

1. Use cameras with good dynamic range control. These are often abbreviated WDR (wide dynamic range) or HDR (high dynamic range). These cameras allow for dark regions to appear brighter and very bright regions not to get over saturated with light.
2. Use cameras that have good shutter control. In some cases this might mean the ability to define the aperture (the degree to which the lense opsn) and in other cases it means good exposure (the duration of time in which a shutter opens). A shutter that opens wide can let in more light while a camera that holds the lense open longer lets in more light. Both techniques can be used to allow more light onto the region of the face but they both have the effect of oversaturating the bright regions.
3. A combination of strategies 1 and 2.

Given the choice, it's better to have good dynamic range than to use shutter controls to manage backlight. If you are using shutter conrol, however, some basic steps you can take are as follows:

- Place the bound on the slowest shutter speed allowed. As people are moving through the field of view (FOV), maintaining high shutter speed is important to obtain blur-free images.
  - Set the slowest shutter speed to at least 1/90 second.
  - In some cameras, if the shutter speed's lower bound is not settable for auto mode, you may need to use Shutter Priority mode.
- If faces are still dark, adjust the exposure compensation to brighten the faces. The background becomes overexposed, but that works for facial recognition.
- If there are specular reflections or faces that are still too dark, turn on Highlight Compensation.

The previous approach is appropriate for the situation where varying outdoor conditions also vary the amount of light reflected from the face. Light intensity is simply boosted above what the cameras would choose automatically and enhancing the image to reduce exposer variance.

In cases where outdoor conditions only generate backlight (light from behind the subject's face) and there is minimal variation in lighting from inside (e.g. there are few windows so indoor illumination on the face is mostly constant), it is more appropriate to place the camera in fully manual mode and set Shutter Speed, Iris, and Gain values manually to properly expose the face while allowing the background to be overexposed. In this mode, the camera makes no auto-adjustments and is not thrown off by momentary bursts of light due to a door opening or other momentary reflections. To do this:

- Set shutter speed to 1/90 or higher.
- Open the iris, increasing the f-stop for the iris (aperture) until the face is bright enough.
- Focus the camera on the sweet spot or optimal point of recognition where people are most likely to face the camera.

Increasing the iris reduces the depth of field (distance during which the face is in focus). Increasing the iris increases the quality of the image but reduces the amount of time the image is in focus and viability for recognition. In either case, focus the camera on the optimal point of recognition where people are most likely to face toward the camera.

## 7.3 General Lighting Considerations

Success with recognition indoors or outdoors depends on lighting conditions.

- Should have a light source that hits the front of the face.
- Outdoors:
  - Typically always has more light during daytime unless there is an awning blocking the light from above and front as the subject approaches.
  - At nighttime, a light source is required behind the camera to illuminate the front of the subject's face.
  - Avoid a direct line between the sun and the camera lens.
  - The camera lens should have sun/rain shade for effective operation.
- Indoors:
  - Need to contend with the backlight illumination.
  - There should be ample ambient lighting conditions and relatively uniform light on the subject's face for the best results.

## 7.4 Additional Information

- Anyone setting up cameras for facial recognition should be fully familiar with digital photography concepts described in the following 15 minute video:
  - https://www.youtube.com/watch?v=F8T94sdiNjc&app=desktop
- The following video covers some specifics on backlight compensation:
  - https://www.dpmag.com/how-to/tip-of-the-week/combat-backlighting-with-exposure-compensation/

# 8 Set up ONVIF IP Cameras

A camera must be correctly configured for authentication via the ONVIF protocol to work.

## 8.1 Enable ONVIF

Make sure that ONVIF is enabled in the camera settings. The precise procedure for how this is done depends on the make and model of the camera.

## 8.2 Configure the Date and Time

The canmera's configured date & time must not differ by more than +/- 5 seconds from the machine you're connecting the camera to. Follow these steps to ensure that the camera date & time are configured correctly:

1. Set the camera Time Zone to the local time zone. (e.g. GMT-8 if you're in Seattle)
2. Disable daylight savings time (DST) adjustments. The Network Time Protocol (NTP) will take care of this automatically.
3. Set the NTP server to `time.google.com` and port `123`.
4. Synchronize the camera time to the time on your computer. The web interface usually has a button that allows you to do this.
5. Enable the NTP service.

The end result should be that the camera's date and time are up-to-date and that the NTP service is enabled to keep it up-to-date.

Some camera web UIs will show an incorrect/strange/nonsensical time after you've set the time zone to your local time zone. Do not change the time zone away from your local time zone! It must be set to the local time zone for ONVIF authentication to work.

## 8.3 Configure the Camera's ONVIF User

Many cameras maintain two sets of users: one set of web users and a second (and independent) set of ONVIF users. These cameras with 2 sets of users do not automatically create an ONVIF user even when a new web user is created.

Be sure that your camera has at least one ONVIF user with administration privileges. If there aren't any ONVIF with administration privileges, ONVIF authentication will not work.

# 9 Connect Cameras to SAFR

SAFR supports USB and integrated cameras, which are always auto-detected. SAFR also supports the standard Open Network Video Interface Forum (ONVIF) camera auto-discovery protocol used by most IP cameras. When ONVIF discovery is enabled, IP cameras are also auto-detected. To connect an auto-detected camera, simply click on the **Select Camera** menu on *Camera* window.

In some cases, however, ONVIF discovery is disabled by default. (ONVIF is sometimes disabled by default for security reasons.) This makes the camera effectively invisible to SAFR and SAFR is unable to discover or communicate with the camera automatically. See the Manually Add and Configure IP Cameras section to see how to manually add such cameras.

## 9.1 Manually Add and Configure Cameras

1. On the Desktop client, click **Tools** > **Preferences**, then select the **Camera** tab.
2. In the lower left corner, click +.
3. In the **Name** field, enter a descriptive name for the camera.
4. In the **URL** field, enter the RTSP (Real Time Streaming Protocol) URL to the live video feed of the camera or an RTSP server. For information on how to find the RTSP URL for your camera, see the **Determine the IP Address and Streaming URL for the Camera** section below.


After a camera is successfully connected, you can configure it. See camera preferences for more information on available options and how to use them.

## 9.2 Determine the IP Address and Streaming URL for the Camera

The IP addresses of many security cameras can't be auto-discovered because their ONVIF has been disabled for security reasons. This makes the camera effectively invisible to SAFR and thus SAFR is unable to find and communicate with the camera automatically. For SAFR to discover and connect to a camera automatically, you must enable ONVIF.

If you already know the IP address for the camera, do the following:

1. Connect to the camera from a web browser by typing the URL of the camera'S IP address (e.g. *http://10.124.13.34*).
2. Find its streaming URL (starting with rtsp://). You need the streaming URL to enter when you add the camera to SAFR. The rtsp:// URL you enter into SAFR most likely includes the camera user ID and password.

The streaming URLs, while different for different camera manufacturers, tend to follow the same format for different camera models of the same manufacturer. The following table includes a few examples of camera streaming URLs for different camera manufacturers. To use them for your camera, match your camera make to an example listed in the table and enter the SAFR provided streaming URL while replacing example values with actual values for your camera. Replace username, password, and IP address (for example, 10.124.13.32) with actual ones configured for your camera. Even if your camera model is not the same as the one listed,

there is a good chance the streaming URL provided in the table works if your camera manufacturer is the same.

| Camera Make | Camera Model | Example rtsp:// URL |
|---|---|---|
| Avigilon | 5.0-H3-DO1-IR | rtsp://username:password@10.124.13.32/defaultPrim |
| Axis | Q6128-E | rtsp://username:password@10.124.13.32/axis-media/media.amp |
| Dahua | HFW5421E-Z | rtsp://username:password@10.124.13.32/cam/realmo |
| HikVision | DS-2CD4185F-IZ | rtsp://username:password@10.124.13.32/h264 |
| Mobotix | M26 | rtsp://username:password@10.124.13.32/mobotix.h2 |
| Panasonic | WV-SFV781L | rtsp://username:password@10.124.13.32/MediaInput |
| Samsung | SND-L6013R | rtsp://username:password@10.124.13.32/onvif/profil |
| Sony | SNC-VM772R | rtsp://username:password@10.124.13.32/video1 |

If you are unable to find your camera's RTSP address, do the following:

1. Determine the make, model, and manufacturer for the camera.
2. Contact your system administrator or the camera manufacturer. They should be able to provide you with instructions for configuring the camera, determining its IP address, enabling it to be discovered by IP address, and/or finding the camera rtsp:// URL.

## 9.3 Save your camera configuration

After you complete your manual camera connection, we recommend that you export and save the created camera connection configurations. Although your configurations are automatically stored in the Desktop client, they cannot be shared with other SAFR components that are installed on different computers unless you export the camera configurations. Exporting your camera connection configurations makes your setup work shareable to other SAFR components and preserves it in case the Desktop client is re-installed later on different hardware.

To export your camera configurations, do the following:

1. In the Desktop client menu, click **Tools > Preferences** and select the **Camera** tab.
2. In the lower left corner, click the gear icon.
3. Click **Export Configurations**.
4. Specify the file name and location where the configurations are to be saved.

**Note:** Your camera connection configurations are saved in a file with an .acc extension. This file may contain your camera access credentials, so save it in secure location.

To import camera configurations, do the following:

1. In the Desktop client menu, click **Tools > Preferences** and select the **Camera** tab.
2. In the lower left corner, click the gear icon.
3. Click **Import Configurations**.
4. Specify the file name and location where the configurations are located.

## 9.4 Interaction of Auto-detected and Manually Configured Cameras

Auto-detected camera configurations and manually entered camera configurations may exist for the same camera. This situation does not cause a conflict. Each configuration can be separately selected; you can choose a method of connection when selecting a camera from the feed window.

Your exported camera connection configurations include only manually configured cameras. Auto-detected camera configurations are dynamic and are discovered by the SAFR client at start and when *Camera Preferences* are opened. Because auto-discovered cameras are dynamically discovered, they may not appear

for a few seconds after the application starts, so make sure to wait several seconds to give the discovery process time to complete.

## 9.5 Delete a Camera Configuration

To delete a camera configuration, do the following:

1. In the Desktop client menu, click **Tools > Preferences** and select the **Camera** tab.
2. In the left hand field select the camera you want to delete.
3. In the lower left corner, click **-**.

**Note:** Auto-detected camera configurations cannot be deleted. They are dynamically discovered.

# 10 Connect to a Video Feed

The Desktop client requires a video feed window to be open for each camera feed (or video file) it is monitoring. The video feed window not only facilities SAFR monitoring of the video but can also present additional information overlaid on top of the video to assist staff in interpreting the scene in the video. For more information on the additional overlaid information, see Interpret Video Feed Overlays.

The Desktop client automatically detects integrated, USB, and Open Network Video Interface Forum (ONVIF) compatible IP cameras. While you're becoming familiar with SAFR, we recommended that you plug in a single USB camera (aka a web cam). Only after you've spent some time learning SAFR should you attempt to connect to additional IP cameras.

The instructions on this page assume you have at least one camera detectable from the computer where SAFR is installed. See Connect Cameras to SAFR for information about how to connect a camera.

## 10.1 Connect to a Camera Video Feed with the Desktop Client

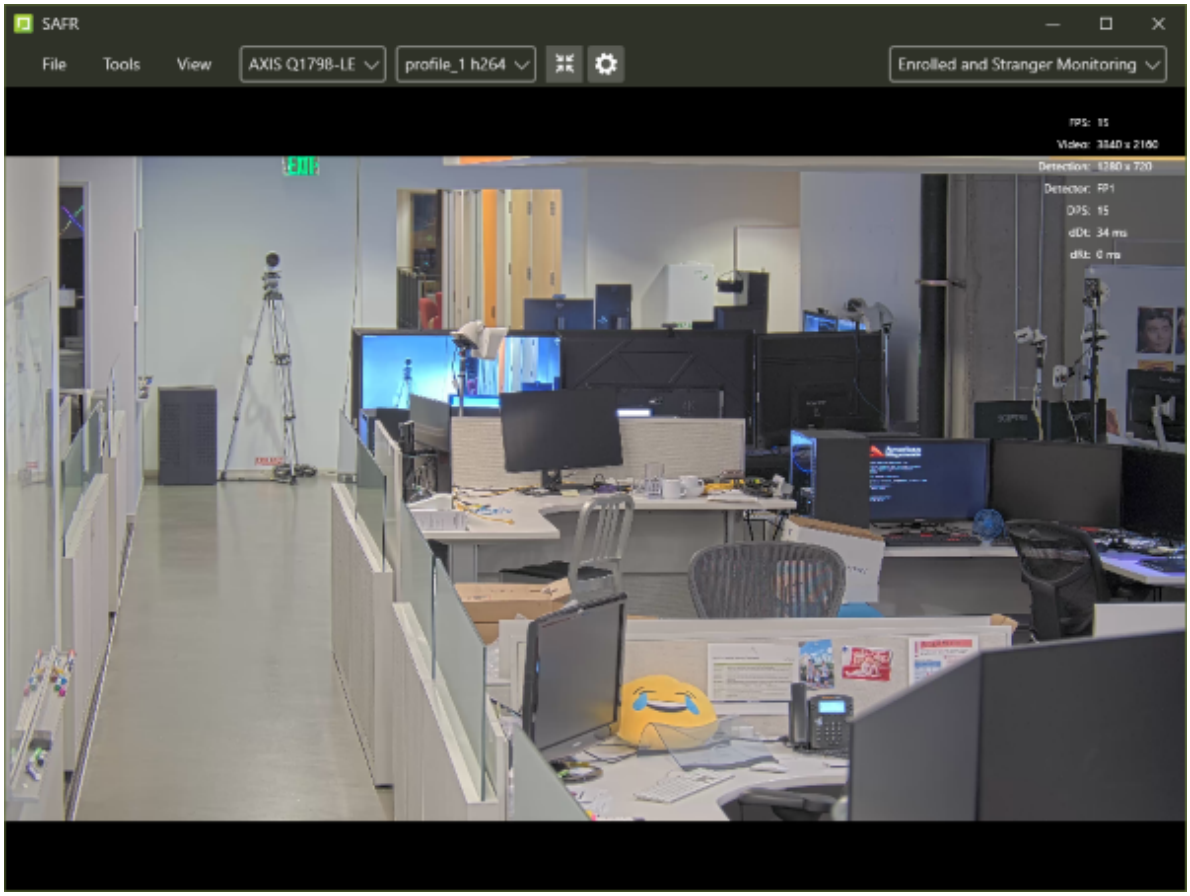
If you have a local deployment, you must first install and configure SAFR Platform before connecting to a live video feed. For information on how to do this, see Getting Started with SAFR Platform on Windows or macOS or Getting Started with SAFR Platform on Linux.

If you have a cloud deployment, your Desktop client should automatically be configured to connect to your SAFR Server in the cloud when you install it.

To connect to a video feed, do the following:

1. From the Desktop client menu, click **File > New** to open a new *Camera* window. **Note**: It's possible that your client will default to the *Camera* window when you first start it. If this happens, there's no need to open a new *Camera* window.

   Below is an example *Camera* window.




2. Along the top of the *Camera* window, select a camera from the **Camera Selector** drop-down menu. The menu displays all detected cameras.

3. Set the camera frame rate and resolution in the **Video Feed Profile Selector** to the right of the **Camera Selector** menu. Frame rate and resolution selection are only configurable for USB and IP cameras auto-discovered via ONVIF. For IP ONVIF cameras, only configured ONVIF media profiles are able to be selected. The higher the frame rate (i.e. frames per second) and resolution for a video feed, the more processing power is required to monitor and collect data from the video feed.

Once you complete this procedure, SAFR receives, monitors, and processes the video feed from the camera. The Desktop client *Camera* window must remain open for SAFR to continue to monitor the video feed. If the window is closed, SAFR no longer receives the video feed and no longer monitors it. The *Camera* window can be minimized without affecting the monitoring of the feed.

## 10.2 Select a Video Processing Mode

A variety of different video processing modes are supported to accommodate different monitoring and security needs, as described in the table below. Each mode can be customized through the Detection, Tracking, Recognition, Events, and User Interface tabs of the **Preferences Window**.

| SAFR Video Processing Mode | Description |
|---|---|
| Recognition | • This is the default mode typically used for set-up, validation, and experimentation.<br>• Only reports enrolled individuals.<br>• No events are generated or recorded. |

| SAFR Video Processing Mode | Description |
|---|---|
| Import | • Any face that can be clearly seen but is unidentified will be automatically registered.<br>• Faces that are already registered are only recognized and do not create additional entries in the Person Directory.<br>• Additional different face images (e.g. from different expressions) may be added to the existing faces in the Person Directory if they improve the recognition of the person.<br>• No events are recorded. |
| Learn and Monitor | • Monitors all person events within view. If a person is not registered in the system, they are added as long as the image meets the specified image quality metric criteria.<br>• Allows for automatic saving of recognized persons to the server. |
| Secure Access | • Secure access uses strict criteria for confirming the identity of the face in the view of the camera.<br>• Records events and images for recognized faces.<br>• Listens for event replies and displays them on the screen.<br>• Typically used for door access control.<br>• Events and images are not recorded for unrecognized faces. |
| Secure Access with Smile | • Uses strict criteria for confirming the identity of the face in the view of the camera. It also looks for transitions in the facial expression (e.g. non-smiling to smiling).<br>• Records events and images for recognized individuals.<br>• Listens for event replies and displays them on the screen.<br>• Typically used for door access control where it is necessary to guard against identity impersonation via photo.<br>• Includes all functionality of *Secure Access* mode and can be used to allow access on first sight recognition for a certain time (e.g. when security staff are on duty) and can change to a higher degree of security (e.g. recognition with smile expression change) at set times (e.g. when security staff is off duty).<br>• Events and images are not recorded for unrecognized faces. |

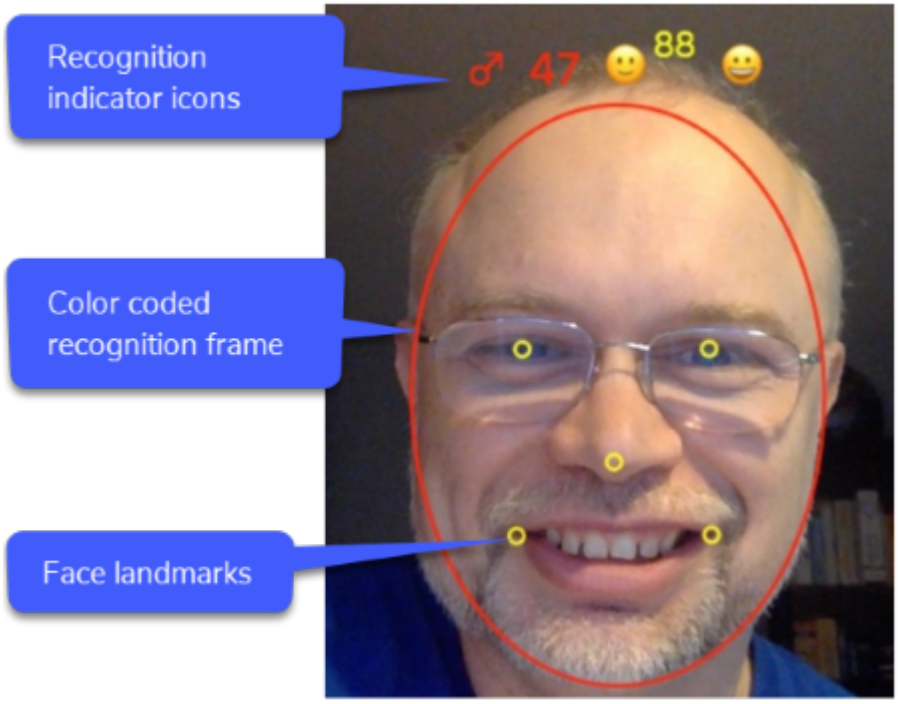
| SAFR Video Processing Mode | Description |
|---|---|
| Secure Access with Liveness | • Secure access uses strict criteria for confirming the identity of the face in the view of the camera.<br>• Records events and images for recognized individuals.<br>• Listens for event replies and displays them on the screen.<br>• Typically used for door access control where you want to use liveness detection to guard against face spoofing.<br>• See Pose Liveness Detection for information about liveness detection. |
| Enrolled Monitoring | • Facial recognition, events, and images are only recorded for registered/recognized faces.<br>• Images and events are not recorded for unrecognized faces. |
| Anonymous Traffic Monitoring | • Only gender and age information is detected and recorded anonymously for faces viewed by cameras.<br>• Images and biometric information are not recorded. |
| Enrolled and Anonymous Traffic Monitoring | • Recognition events are recorded for registered individuals.<br>• Anonymous age and gender information is also recorded for unknown/unrecognized faces.<br>• No images are recorded for recognized or unrecognized faces. |
| Enrolled and Unique Traffic Monitoring | • Events are recorded for registered and unknown individuals.<br>• Any faces that can be clearly seen but are currently unknown are automatically registered.<br>• Age and gender information is recorded for all clearly seen faces.<br>• Images are recorded for all faces. |
| Enrolled and Stranger Monitoring | • Events are recorded for registered and unknown individuals.<br>• Faces that are clearly seen but aren't currently registered are reported as strangers.<br>• Faces that can't be seen clearly enough to attempt recognition are reported as unrecognizable.<br>• Images are recorded for all faces. |

## 10.3 Recommendations for the Best Video Experience

- Use the highest resolution available (4K) if you need to monitor an area of 5 meters or wider.
- To monitor a narrow area of approximately 2-3 meters, 1080p video is sufficient.
- For up close door access applications, 720p video offers adequate quality.
- For resolutions of 1080p or higher, we recommend 15 frames per second.
- For cameras used in *Secure Access With Smile* mode, we recommend 30 frames per second at 720p resolution.
- Generally, one computer can support one 4K camera (or 2 HD cameras) for every 2 CPU cores depending on the camera make and model.

# 11 Interpret Video Feed Overlays

Video feed overlays are available in the video feed window. Depending on the View menu options you choose, various supplemental information is displayed in real time in the form of overlays and readouts to help monitor the video feed.




## 11.1 Color Codes for the SAFR Recognition Frame

The following colors are used to indicate the level of recognition for a face:

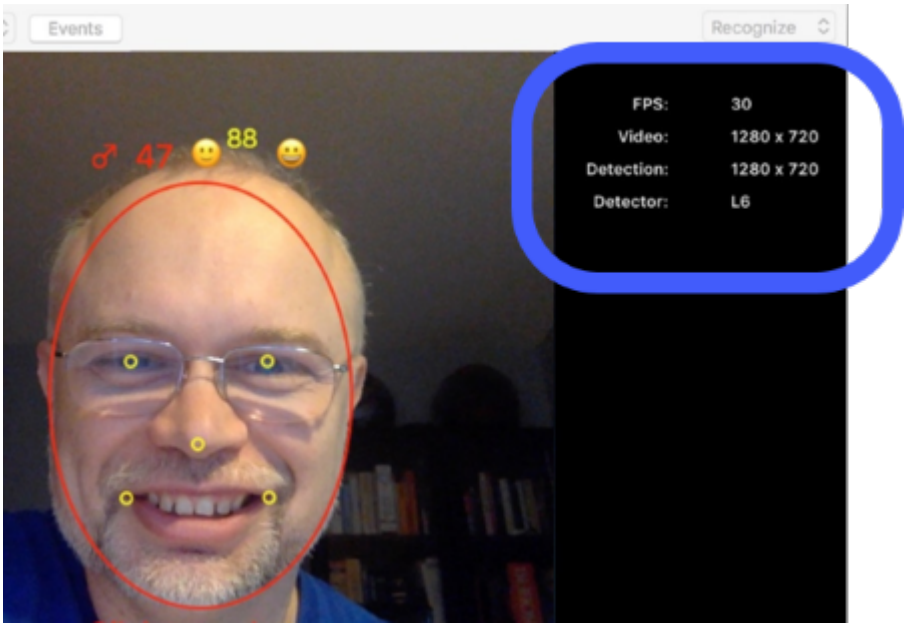
- **Gray**: Unrecognizable. Either the face does not meet minimum quality values to be recognized or the response from the attempted recognition has not yet arrived.
- **Purple**: Stranger. The face met sufficient quality for recognition but was not recognized and did not meet minimum quality to be registered.
- **Cyan**: Identified as a close match to recognized user but not 100% identification.
- **Blue**: Registered person without a name. The face was recognized as matching one already in the Person Directory.
- **Green**: Registered person with a name. The face was recognized as matching one already in the Person Directory.
- **Yellow**: Concern. The registered face has been tagged as a concern.
- **Red**: Threat. The registered face has been tagged as a threat.

## 11.2 Recognition Indicator Icons

The indicator icons indicate the following:

- Gender
- Age
- Sentiment
- Sentiment score
- Smile

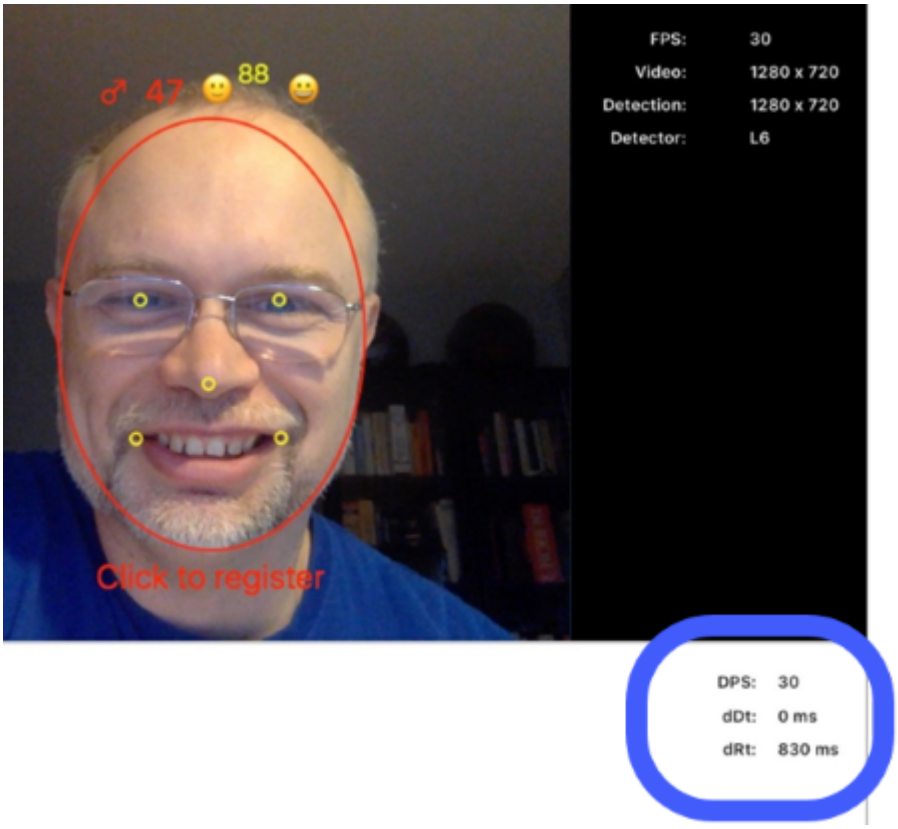
## 11.3 General Video Information




The following information is provided in the Desktop client video display:

- **FPS**: The number of frames per second being captured by the camera.
- **Video**: Video resolution. (e.g. 1280x720)
- **Detection**: Face detection resolution.
- **Detector**: The detector CPU capacity level. It's based on the number of CPU processing cores.

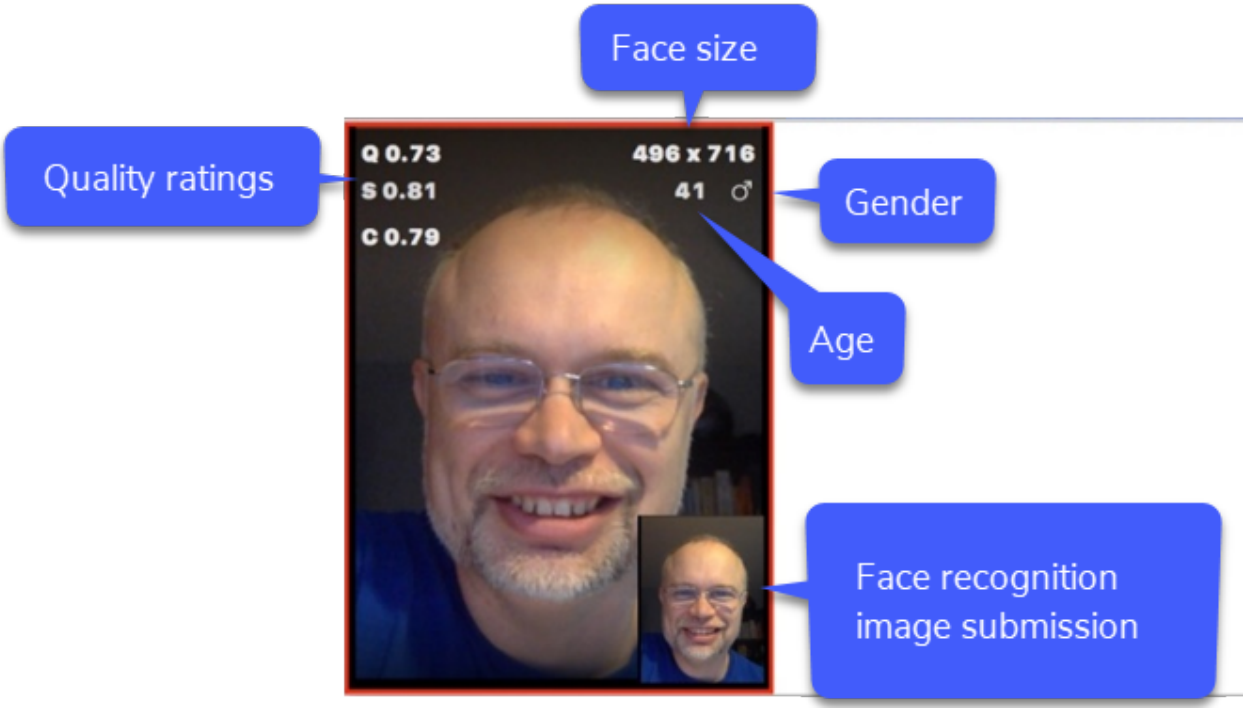
## 11.4 Video Processing Latency Information




- **DPS**: Frame detections per second.
- **dDt**: Detection time. For example, how long it is taking to detect a face.
  - This time should normally be in 20-50ms range.
- **dRt**: Recognition time. For example, how long it is taking to recognize a face.
  - This time should normally be in the 60 - 250 ms range for only identity recognition.
  - If age, gender, and sentiment are also being recognized, the time can be expected to be up to 450 ms.

If your processing times are longer than indicated here, it may be an indication your system is overloaded. You should look to offload some of your video feed processing to other computers.

## 11.5 Face Detection Information




There are 3 main image quality metrics:

- **Q**: Center pose. Represents how directly the face is looking at the camera. A face looking directly at the camera would receive a score of 1. The more the face looks up, down, left, or right of the camera, the more this metric is reduced.
- **S**: Face sharpness. Represents how clear the image is. A score of 1 represents a perfectly clear image. while 0 represents an extremely blurry image.
- **C**: Face contrast. Represents the color contrast within the image. A score of 1 represents an image with very high contrast, while 0 represents very low contrast.

For guidance on these 3 metrics, see Image Quality Metrics Guidance. These metrics can be configured in the recognition preferences.

- **Face size**: Face size is the resolution of the image with a 25% margin. It can be used to ignore background (smaller) faces or to require an up-close high resolution image to be presented before the face is learned by the SAFR system. See detection preferences and recognition preferences for information on how to customize SAFR behavior based on the detected face size.
- **Gender**: Displayed as an icon if gender recognition is enabled.
- **Age**: Age of user if age recognition is enabled.
- **Face recognition image submission**: The thumbnail in the lower right corner is the image submitted for facial recognition. This is only displayed if you select *Recognition Candidates* (for macOS) or *Detection List and Recognition Details* (for Windows) from the View menu.

# 12 View Video Feeds Status

Video feeds status provides real-time monitoring of the Desktop client, the Mobile client, and the VIRGO client within an account. While VIRGO clients support both remote monitoring and configuration, the Desktop and Mobile clients only support remote monitoring and must be configured locally in their GUI.

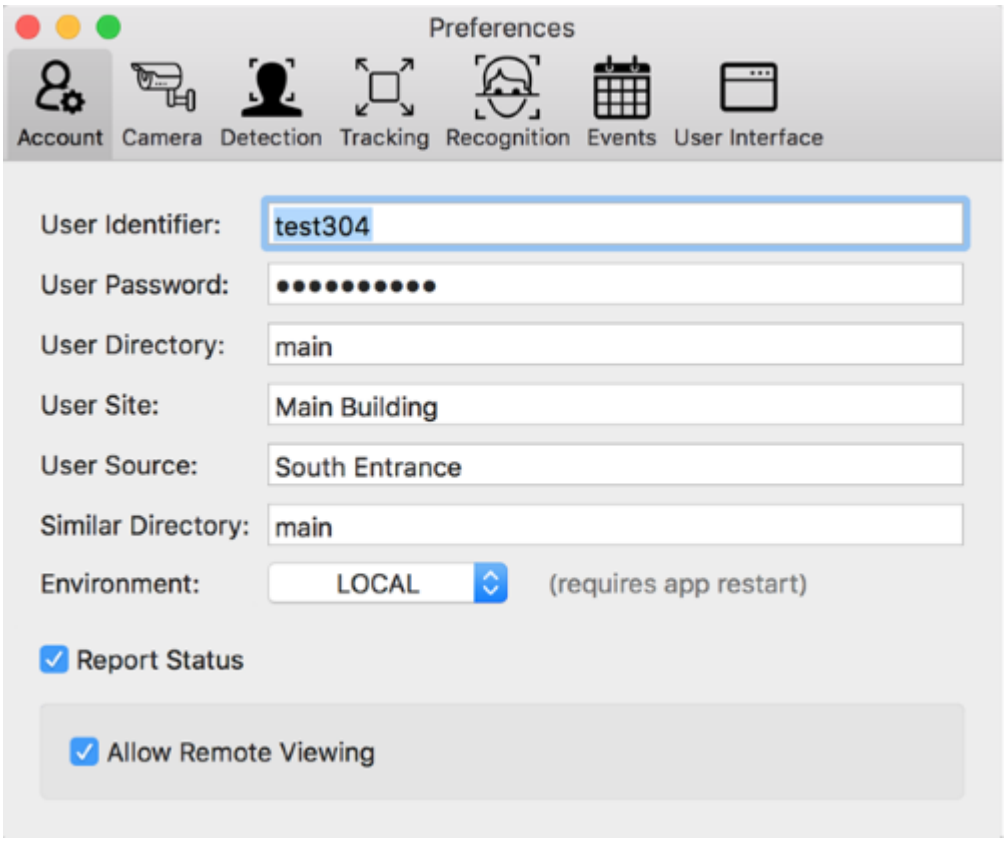
**Note:** This feature is available with the Web Console or on macOS Desktop client installations.

## 12.1 Enable the Desktop or Mobile Clients for Remote Monitoring

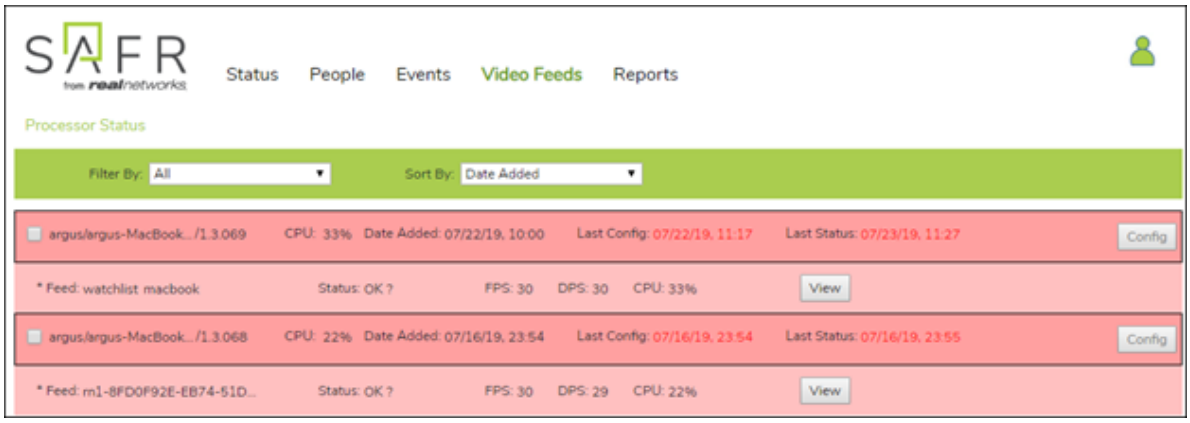
Both the Desktop and Mobile clients can be enabled for remote status monitoring and remote viewing.

To enable those clients for remote monitoring:

- For macOS, click the **SAFR** > **Preferences** > **Account** tab, and select the **Report Status** and **Allow Remote Viewing** check boxes.

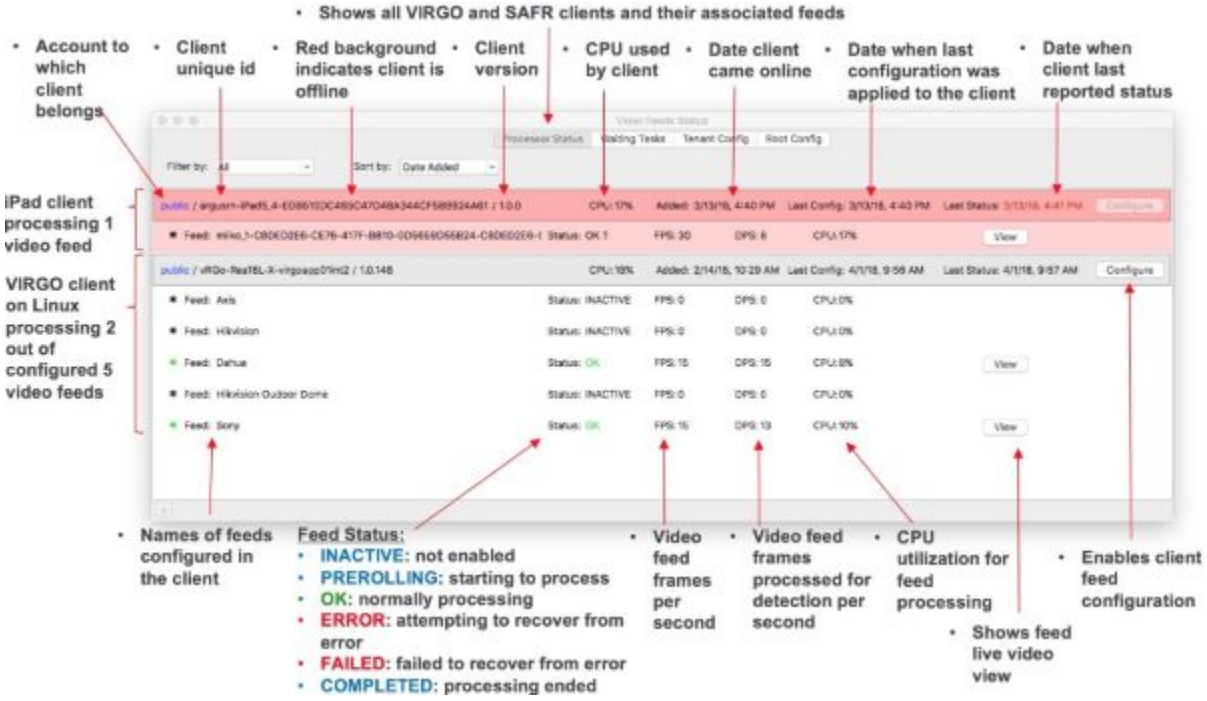



- In the Web Console, click **Video Feeds** > **Processor Status**.

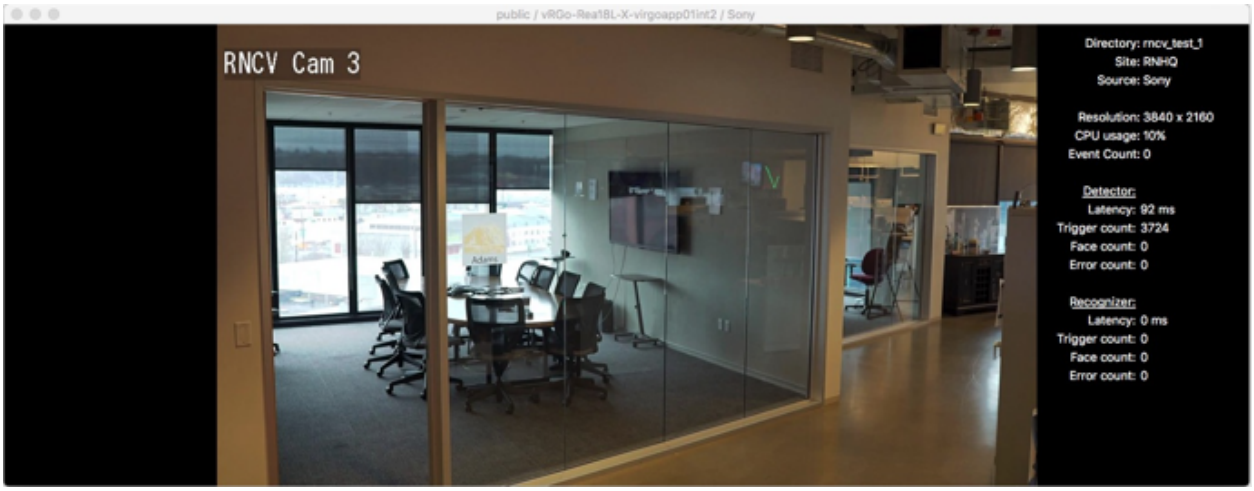



## 12.2 The Video Feeds Status Window (aka Processor Status Window)

The Video Feeds Status (or Processor Status) window can be accessed from the **SAFR** menu of the Desktop client for macOS and from the Web Console Video Feeds page. It displays real-time status of all VIRGO, Desktop, and Mobile clients enabled for status reporting.



## 12.3 The Live Status Video View




The **Live Status Video** view can be accessed by clicking the **View** button next to an active feed in the **Video Feeds Status** window. You can display the **Live Status Video** view for all active VIRGO clients and for all Desktop and Mobile clients for which you have enabled **Allow Remote Viewing**.

You can simultaneously view live status video of as many feeds as you like from a single remote viewer. Only one viewer of the status video is allowed at any given time, however.

The **Live Status Video** view is displayed at low frame rates (~1 frame per second) and is intended for cursory inspection or monitoring. Full fidelity live video view, including recognition overlays, is available only in the video feeds window of the Desktop and Mobile clients to which the camera is connected.

The top of the status video view displays the *Account*, *Client ID*, and the *Name* of the video feed.

On the right-hand side of the view, overlaid text displays additional information about the feed.

- **Directory**: Face Directory used for face recognition in the video feed, as specified in Account Preferences.
- **Source**: Source label for the video feed, as specified in Camera Preferences.
- **Site**: Site label for the video feed.
- **Source**:Source label for the video feed.
- **Resolution**: Video feed resolution.
- **CPU Usage**: CPU percent used for video feed processing.
- **Event Count**: Number of events reported since start of video feed processing.

Detector:

- **Latency**: Face detector latency in the last second of operation.
- **Trigger count**: Number of times face detector was triggered.
- **Face count**: Number of faces detected since the start of the video feed.
- **Error count**: Number of face detector errors since video processing started.

Recognizer:

- **Latency**: Face recognition latency in the last second of operation.
- **Trigger count**: Number of times face recognition was triggered since the start of the video feed.
- **Face count**: Number of faces recognized since video processing started.
- **Error count**: Number of face recognition errors since video processing started.

# 13 Manage People in the Person Directory

The Person Directory contains a list of all people stored in the user directory location specified under Account Preferences. To open the directory from the Desktop client:

- For Windows, click **Tools > People**.

By default, the list is displayed in chronological order with the most recently added displayed first. You can also search and filter identities by *Name*, *Person Type*, *ID Class*, and *Home Location*. All 4 of those properties can be changed by clicking the available fields to the right of the identity's picture.

- Metadata applied to identity groups is applied to all identities within the group. Changing these properties for any identity within a group will cause the change to be applied to all identities within that group.
- Groups are alternative identities belonging to a single person. While rare, a person may require such grouping to fully cover all different face modalities by which he or she can be recognized.

Double click the identity entry to view or edit even more information associated with the identity.

- The *Id Class* field is important and can be used to define a person as a *Concern* or *Threat*.
- *Moniker* is an advanced feature used to realize two factor authentication with visual badges.

You can also perform the following actions on identities in the People Directory:

- **Regroup**: Removes selected face from their existing groups (if any) and forms a new group of faces to represent a new identity. Root identity is always the earliest one added to the directory.
- **Delete**: Deletes selected identities and all information associated with the identity from the directory. All information associated with the identity is removed.
- **Export**: Exports a face image into an image (.jpg) file on the local drive.
- **Refresh**": Reloads the people directory page making sure up-to-date information is displayed.

## 13.1 Add a Person Type or Home Location

In the Person Directory, click **Add Person Type**, and then type the *Person Type* you want to assign (for example, Staff, Guest, or Maintenance). Likewise, you can click **Add Home Location** and type text representing a person's home location.

**Best Practice:** You can create and customize as many *Person Types* and *Home Locations* as you like, but we recommend keeping the list short (less than a dozen or so) because short lists are easier to maintain. As *Person Types* are entered for a few registered individuals, *Person Types* that are already entered become available for selection once **Add Person Type** is clicked, which makes designation easier for new registration. The same is the case for *Home Location*. The system knows of all previously entered *Home Locations* and offers them in the menu when **Add Home Location** is clicked.

# 14 Importing and Registering People

There are three main ways to register people to SAFR's Person Directory: cameras, photos, and recorded video. Imported people are registered to the Person Directory and stored in the directory specified in the User Directory setting of your Account preferences.

## 14.1 Register People Using a Camera Connected to the Desktop Client

1. Select the connected camera you want to use by clicking on **File > New** to open the Desktop client's *Camera* window, then select a camera from the **Select Camera** menu.
2. Set your **video feed processing mode** (located in the upper right hand corner) to one of the following modes: *Recognition*, *Import*, or *Learn and Monitor*. *Recognition* is considered the default mode for set-up validation and experimentation.
3. All the faces in view of the camera will initially have a grey overlay, which indicates one of two things:
    1. Your client or console hasn't received a response from its attempted recognition from the SAFR Server yet, or
    2. The face does not meet minimum image quality metric values and recognition cannot be successful. If the grey overlay persists, then the problem is the image quality. Try cleaning your camera lens or adjusting your camera placement to fix the problem.
4. When the overlay turns purple, the face has sufficient image quality for recognition by SAFR but it isn't recognized by SAFR because it hasn't been registered yet. To register the face, double click the face and the *Register* dialog will open.
5. You can choose to enter a name for the face if you want, but it's not required. Click **Register** to complete the registration.
6. The color of the face's overlay will change to either green (if you named the face) or blue (if you didn't name the face). Both of those colors mean that SAFR recognizes the face. For more information on overlays, see Interpret Video Feed Overlays.

## 14.2 Register People Using the Mobile Client

Another way to register faces is by using a Mobile client installed on an iOS or Android device. For more information, see Connect a Registration Kiosk.

## 14.3 Register People by Importing Faces from Picture Files

To import faces from picture files, do the following:

1. Open either the Desktop client (by clicking on the **SAFR** icon on your desktop) or the Web Console. (See Access the Web Console for information on how to do this.)
2. On the Desktop client, click **File > Open** and select an image file. On the Web Console, click on the **People** tab, click on the up arrow symbol in the upper right hand corner, select **Pick File** in the dialog window that pops up, and select an image file.
3. Image files are usually .jpg, .jpeg, or .png files. If the file you selected has multiple faces on it, then SAFR will import all the faces on the image.
4. On Windows, you're able to select multiple image files at the same time to import all of them at one time. We recommend that you select no more than 20 images at a time. If you select more than ~20 images at a time, you're likely to experience a degradation of system performance.
5. When you import facial images, you may be prompted to resolve any duplicate and/or low-quality image conflicts that may have arisen.

### 14.3.1 Resolve Duplicate Images

To resolve conflicts resulting from people that already exist in the Person Directory, do the following:

1. Click on the **Fix conflicts** link in the notification bar.
2. Duplicates are displayed side by side in the *Report Dialog*.

3. Click on **Replace** to replace the existing image with the new image, or click **Keep** to not replace the existing image.
4. Repeat the previous step for all duplicates.

**Note**: At the top of the *Report Dialog*, there is an option to accept the default recommendations. SAFR defaults to accept whichever of the duplicate images is higher quality based on internal image quality metrics.

### 14.3.2 Resolve Low-Quality Images

To resolve conflicts resulting from low-image quality images, do the following:

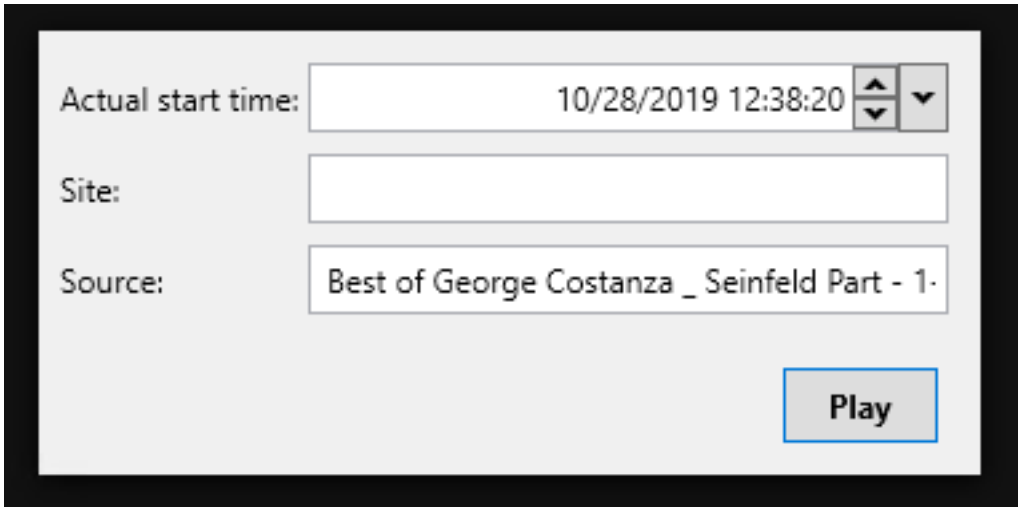
1. Click on the **Fix conflicts** link in the notification bar.
2. Low-quality images are displayed in the *Report Dialog*. Note that a warning symbol appears next to the image quality metric(s) that are problematic. See Image Quality Metrics Guidance for information and guidance on the metrics.
3. Click on **Import anyway** to import the low-quality image, or click **Skip Import** to not import the image.
4. Repeat the previous step for all low-quality images.

**Note**: Clicking on **X** in the Notification bar or at the top of the *Report Dialog* cancels the import operation for all remaining low quality image conflicts.

## 14.4 Register People from a Video File

You can open a saved video file to recognize and extract facial recognition data. To do so, do the following:

1. Open the Desktop client.
2. Click **File > Open**, and then browse to any saved .mp4 file to open it.
3. If you're on a Windows machine and you have event reporting enabled for the currently selected video processing mode, (located on the Events Preferences tab) the dialog below will open. (If you don't meet both of these conditions, then the video will simply open.)




- **Actual start time**: The timestamp that the video will acquire when you press **Play**. (e.g. In the example above, the played video's timestamp would start at 12:38,10/28/2019) The input box starts 'live' and keeps up-to-date with the local time. When you interact with the time or set the focus, the input box stops being live.
  **Note**: Deleting the timestamp and leaving the field blank is valid, despite the red outline that the field acquires. Of course, if you do leave the field blank, the video won't have a timestamp, as expected.

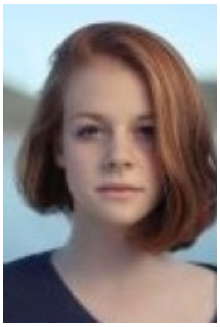
- **Site**: The *Site* label that will be applied to all events generated by the video. This field is auto-populated with your *User Site* preference located in the Account Preferences.
- **Source**: The *Source* label that will be applied to all events generated by the video. This field is auto-populated with the name of the video.

4. Set the video file's video feed processing mode to *Recognition*.
5. SAFR will proceed to register any unregistered faces that appear in the video.

# 15 Image Quality Metrics Guidance

Choosing to import images that have been flagged as "low-quality" will cause more false positives to occur as SAFR incorrectly identifies newly scanned faces as identical to the low-quality facial image. Greater discrepancies between the recommended metric value and the actual metric value will result in more false positives. Similarly, having more than one metric value be poor or very poor will also result in more false positives.

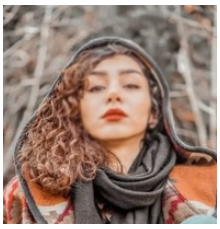
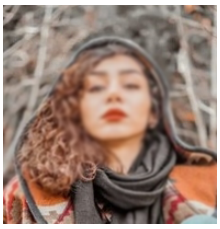
## 15.1 Center Pose

| | | | | |
|---|---|---|---|---|
|  |  |  |  |  |
| Center Pose = .89 | Center Pose = .76 | Center Pose = .54 | Center Pose = .34 | Center Pose = .21 |

Center pose represents how directly the face is looking at the camera. The more the face looks up, down, left, or right of the camera, the more this metric value is reduced from 1. Similarly, if the face is tilted in any way (e.g. the person's chin is pointing at a corner of the image) this metric value is reduced. The default recommended minimum value for this metric is .59. You can adjust the recommended minimum value by going to **Tools** âĘŠ **Preferences**, clicking on the **Recognition** tab, then adjusting the **For merging** slider in the **Minimum required center pose quality** section.

| Quality Label | Metric Range | Description |
|---|---|---|
| Excellent | 0.7 - 1.0 | Full recognition accuracy can be expected under all conditions. |
| Good | 0.6 - 0.7 | Very good recognition accuracy can be expected in general but may confuse closely related family members. |
| Marginal | 0.45 - 0.6 | Good recognition but may result in occasional failures. |
| Poor | 0.3 - 0.45 | Recognitions can be performed to significant extent but may produce false recognitions. |
| Very Poor | 0.0 - 0.3 | Recognitions can still be performed but with significant possibility of confusing similar faces. |

## 15.2 Sharpness

| | | | | |
|---|---|---|---|---|
|  |  |  |  |  |
| Sharpness = .79 | Sharpness = .62 | Sharpness = .58 | Sharpness = .35 | Sharpness = .22 |

Sharpness represents how clear the facial image is. The more blurry the face is, the more this metric value is reduced from 1. The default recommended minimum value for this metric is .45. You can adjust the recommended minimum value by going to **Tools** âĘŠ **Preferences**, clicking on the **Recognition** tab, then adjusting the **For merging** slider in the **Minimum required face sharpness** quality section.

| Quality Label | Metric Range | Description |
|---|---|---|
| Excellent | 0.7 - 1.0 | Full recognition accuracy can be expected under all conditions. |
| Good | 0.6 - 0.7 | Very good recognition accuracy can be expected in general but may confuse closely related family members. |
| Marginal | 0.45 - 0.6 | Good recognition but may result in occasional failures. |
| Poor | 0.3 - 0.45 | Recognitions can be performed to significant extent but may produce false recognitions. |
| Very Poor | 0.0 - 0.3 | Recognitions can still be performed but with significant possibility of confusing similar faces. |

## 15.3 Contrast

| | | | | | |
|---|---|---|---|---|---|
|  |  |  |  |  |  |
| Contrast = 1 | Contrast = .87 | Contrast = .63 | Contrast = .47 | Contrast = .40 | Contrast = .20 |

Contrast represents the color contrast within the facial image. The less color contrast a face has, the more this metric value approaches 0. The default recommended minimum value for this metric is .45. You can adjust the recommended minimum value by going to **Tools** âĘŠ **Preferences**, clicking on the **Recognition** tab, then adjusting the **For merging** slider in the **Minimum required face contrast quality** section.

| Quality Label | Metric Range | Description |
|---|---|---|
| Excellent | 0.7 - 1.0 | Full recognition accuracy can be expected under all conditions. |
| Good | 0.6 - 0.7 | Very good recognition accuracy can be expected in general but may confuse closely related family members. |
| Marginal | 0.45 - 0.6 | Good recognition but may result in occasional failures. |
| Poor | 0.3 - 0.45 | Recognitions can be performed to significant extent but may produce false recognitions. |
| Very Poor | 0.0 - 0.3 | Recognitions can still be performed but with significant possibility of confusing similar faces. |

## 15.4 Face Size

Face size defines the minimum required face size in pixels. The metric also includes a margin around the face. The margin is required when learning a face. The face itself (without the margin) includes the area ranging from the top of the forehead to the bottom of the chin and across the full width of the face excluding ears.

The recommended minimum value for this metric is 220 pixels. You can adjust the recommended minimum value by going to **Tools** âĘŠ **Preferences**, clicking on the **Recognition** tab, then adjusting the **For learning / strangers** slider in the **Minimum Required Face Size** section.

Note that only the shortest side of the image is used for the purpose of determining the metric value. For example, a facial image that is 200 x 300 (including the margin) would be classified as *Marginal*, since the shortest side (200) falls in the *Marginal* range.

| Quality Label | Metric Value | Description |
|---|---|---|
| Excellent | 260 px and greater | Full recognition accuracy can be expected under all conditions. |
| Good | 210 px - 260 px | Very good recognition accuracy can be expected in general but may confuse closely related family members. |
| Marginal | 160 px - 210 px | Good recognition but may result in occasional failures. |
| Poor | 110 px - 160 px | Recognitions can be performed to significant extent but may produce false recognitions of blurry or otherwise not clearly visible faces. |
| Very Poor | 60 px - 110 px | Recognitions can still be performed but with significant possibility of confusing similar faces. |

## 15.5 Occlusion

Occlusion represents how much of the face is occluded. Faces can be occluded by masks, baseball caps, or even the person's hands held between the face and the camera. The default recommended maximum value for this metric is .5. You can adjust the recommended maximum value by going to **Tools** âĘŠ **Preferences**, clicking on the **Recognition** tab, then adjusting the **For learning / strangers** slider in the **Maximum allowed occlusion** section.

| Quality Label | Metric Range | Description |
|---|---|---|
| Occluded | 0.5 - 1.0 | At least one of the facial features is not clearly visible thus potentially preventing full recognition accuracy.<br>Recognition based on occluded features will not be possible and incorrect recognition of similar faces occluded in similar manner is possible.<br>Recognition is generally possible as long as two out of three key features (eyes, nose, mouth) are visible. |
| Not Occluded | 0.0 - 0.5 | All facial features are clearly visible and full recognition accuracy can be achieved. |

## 15.6 Sentiment

Sentiment represents how happy (a positive sentiment score) or angry (a negative sentiment score) a face is. 0 sentiment (a neutral or serious expression) yields the most accurate facial recognition.

# 16 Actions Overview

In SAFR an action is essentially a script/macro that communicatesa desired action in a language/protocol the receiving device or system understands. It can be written in any language supported by the computer where ARES is installed. It only needs to be invocable as an executable directly or through the use of another executable (usually a script interpreter such as Python).

## 16.1 Actions Components

These are the principle components involved with actions:

- **Actions Relay Event Service (ARES)**: ARES is a cross-platform Java application that acts as an event listener that dispatches configured actions in response to events, as defined in the SAFRActions.config file. ARES can provide replies on any event to be handled by the client originating the event and is normally installed as a service by either the SAFR Platform or SAFR Edge installers. It is constantly active and is automatically started by the operating system on power-up.
- **SAFRActions.config**: The SAFRActions.config file defines which events will trigger specified actions. It also can specify additional condition constraints before the action(s) will trigger.
- **SAFR Actions**: SAFR Actions is a GUI tool that makes editing the SAFRActions.config file much easier. It presents the JSON information of the config file in a visual and easy to understand manner, offers drop-down menus when appropriate so you can quickly and easily what values are available and valid, makes the JSON element heirarchies easy to understand, and ensures that your changes will validate against the SAFRActions.config JSON schema.

## 16.2 SAFRActions.config Overview

```
<name: value connection attributes>
rules: [
  {
    event: {  },
    triggers: [
        <time of day and week properties>
        actions: [  ],
        reply: {  },
        conditionalReply: {  },
    ],
    excludeDates: [  ]
  }
]
noTriggerReply: {  }
nFactorDef: [ {  }, { }, ... ]
emailDef: [  {  }, {  }, ... ]
smsDef: [  {  }, {  }, ... ]
```

- **rules**:
  - 1 or more rules can be defined.
  - When an event occurs each rule is checked to see if any of its events match.
  - A rule's event matches an occurring event when:
    - All attributes rules[i].events match the event.
  - Each rule has 1 or more triggers.
    - Each Trigger inside a matching rule is fired as long as time of day conditions match. **Exception**: If 2 *triggerId*s are identical only the first trigger is fired.
  - Each trigger has one or more actions.
    - Actions are either:
      - A shell command or a batch/shell script to be executed.

        - A send email command that has the syntax of: `@emailSend <value of emailDef.label>`
      - All actions are run asynchronously unless a *conditionalReply* is specified in which case the first rule is run synchronously (and the return code of that rule is used for the conditionalReply) and all other rules are run asynchronously.
- *noTriggerReply* is used to perform a reply if none of the triggers are fired.
- *nFactorDef* can define 2 or more conditions that must occur within the specified time window.
- *emailDef* defines one or more email message attributes (subject, from, message, etc).
- *smsDef* defines one or more Short Message Service (SMS) messages.

**Examples**:

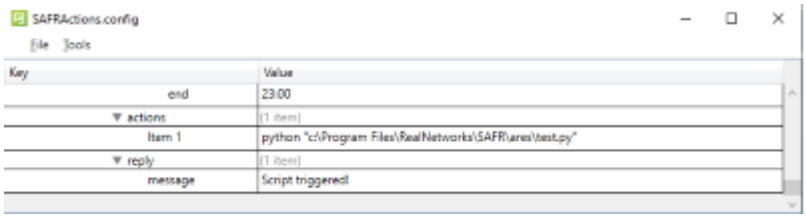
- Send email when visitor arrives during work hours
  - rules
    - Rule 1
      - event (hasPersonId=false)
      - trigger (day/hours: 8-5, M-F)
        - action: @emailSend visitorEmail
  - emailDef
    - label=visitorEmail
    - subject="Visitor Arrived"
    - message="A visitor has arrived at #I - #S.
    - ...
- Log all events to a CSV and send one type of email for a known person event and another for a threat event.
  - rules
    - Rule1 (known person email)
      - event ( hasPersonId=true, idClass=No-Concern )
      - trigger
        - action: @emailSend knownEmail
    - Rule 2 (threat email)
      - event (hasPersonId=true, idClass=[Threat, Concern])
      - trigger
        - action: @emailSend threatEmail
    - Rule 3 (log)
      - trigger
        - action: ".\scripts\log_event.bat "#D" "#N" "#F" ..."
          - If editing config file, escape backslash or quotes with another backslash. (In SAFR Actions no escaping is needed.)
          - The file 'log_event.bat' should be placed in `C:\Program Files\RealNetworks\SAFR\ares\scripts` (for Windows) or `/Library/RealNetworks/SAFR/ares/scripts` (for macOS).
  - emailDef
    - 1 (label=knownEmail, subject, message, etc)
    - 2 (label=threatEmail, subject, message, etc)

### 16.2.1 Long File Names

- When using long file names for actions they need to be escaped correctly:

```
"actions": [
            "python \"c:\\Program
               Files\\RealNetworks\\SAFR\\ares\\test.py\""
          ]
```

- Within the SAFR Actions GUI the same entry appears as follows:


SAFRActions.config
File Tools
Key
Value
end
23:00
actions
(1 item)
Item 1
python "c:\Program Files\RealNetworks\SAFR\ares\test.py"
reply
(1 item)
message
Script triggered!

# 17 Actions Relay Event Service (ARES)

ARES is a cross-platform Java application that acts as SAFR Platform event listener that dispatches configured actions (macros) in response to events. The recommended Java version is 9.0.4 or later. ARES can provide replies on any event to be handled by the client originating the event and is normally installed as a service by either SAFR Platform or SAFR Edge installers. It is constantly active and is automatically started by the operating system on power-up.

## 17.1 ARES Installation Locations

- For Windows: C:Files

## 17.2 Command Line Start

```
java -jar Ares.jar
```

Command line supports the following options:

```
-u <UserId>        - provides RealCV account User Id
-p <Password>      - provides RealCV account password
-q                 - turns on quiet mode which suppress most console output
```

Command line UserId/Password override those configured in SAFRActions.config.

## 17.3 Re-configuration

- ARES dynamically applies any changes to config file without restarting:
  - ARES monitors config file for any changes.
    - ARES examines config file for modifications every 2 seconds
- When a change is noticed, ARES reads and reconfigure atomically (event polling is to suspend briefly and then promptly resumed after reconfiguartion).
- Reconfiguration action is indicated in the log:

  ```
  --- RECONFIGURED at <date>
  ```

## 17.4 Console Output

- At start, ARES displays any errors or warning based on contents of the config file.
- ARES displays all received events, triggered actions, and replies issued unless it was given -q (quiet) option at start.

**Tip**: In the Mac terminal or in the Windows Cygwin shell, the `tail -f ares.log` command is a convenient way to monitor the SAFR Action service in real time.

# 18 SAFRActions.config

The SAFRActions.config file defines which events will trigger specified actions. You can also specify additional condition constraints before the action(s) will trigger. It also contains basic configuration information so that ARES can communicate with other SAFR components, such as the Event Archive.

## 18.1 SAFRActions.config JSON Schema

```
{
   environment : "string",
                 <optional,
                 - values: "LOCAL", "DEV", "INT2", "PROD", "Custom"
                 - if not specified assumed PROD >
   eventServer : "string",
                 <optional,
                 - required in case of Custom environment
                 - only affects Custom environment>
   replyServer : "string",
                 <optional,
                 - only affects Custom environment>
   coviServer : "string",
                 <optional,
                 - only affects Custom environment>
   reportServer : "string",
                 <optional,
                 - only affects Custom environment>
   configServer : "string",
                 <optional, "https://cvos.int2.real.com" for
                                          partner cloud environment
                            "https:\/\/cvos.real.com" for
                                          cloud environment
                 - if specified config is retrieved from the cloud using
                    the
                  following address: <configServer>/obj/ares/<aresId> >
   userId :      "string", <optional>
   userPwd :     "string", <optional>

   directory :   "string", <required>
   site :        "string", <optional>
   source :      "string", <optional>

   aresId :      "string", <optional>

   maxEventLatency: <long>,  <optional, in milliseconds, default = 8000>

   rules: [
      {
        event : {
          type: [ "string", ... , "string" ],
                 <optional, values=(person, badge, action or object),
                    default = all>
          personType: [ "string", ... , "string" ],
                 <optional, default = all, "" = no personType>
          personTags: [
```

```
        [ "string", ... , "string" ],
        ...
        [ "string", ... , "string" ]
]
        <optional, default = all>
tagType: [ "string", ... , "string" ]
        <optional, values=(april), default = all, "" = no
           tagType>
tagId: [ "string", ... , "string" ],
        <optional, values=(Ids of tagType) default = all, "" =
           no tagId>
actionType: [ "string", ... , "string" ],
        <optional, values=(smileToActivate) default = all, "" =
           no actionType>
actionId: [ "string", ... , "string" ],
        <optional, default = all, "" = no actionId>
name: [ "string", ... , "string" ],
        <optional, default = all, "" = no name>
company: [ "string", ... , "string" ],
        <optional, default = all, "" = no company>
moniker: [ "string", ... , "string" ],
        <optional, default = all, "" = no moniker>
personId: [ "string", ... , "string" ],
        <optional, default = all, "" = no personId>
hasPersonId: <boolean>,
        <optional, default = all>
hasName: <boolean>,
        <optional, default = all>
hasMoniker: <boolean>,
        <optional, default = all>
hasRootEventId: <boolean>,
        <optional, default = all>
gender: [ "string", ... , "string" ],
        <optional, default = all>
age: [
        <optional, default = all>
   {
      min: <float>,
      max: <float>
   },
   ...
],
smile: <boolean>,
        <optional, default = all>
avgSentiment: [
        <optional, default = all>
   {
      min: <float>,
      max: <float>
   },
   ...
],
liveness: {
        <optional, default = all>
```

```
            min: <float>,
            max: <float>
         },
         livenessConfirmed: <boolean>,
                <optional, default = all>
         mask: <boolean>,
                <optional, default = all>
         similarityScore: {
                <optional, default = all>
            min: <float>,
            max: <float>
         },
         occlusion: {
                <optional, default = all>
            min: <float>,
            max: <float>
         },
         site: "string",
                <optional if specified at the root>
         source: "string",
                <optional if specified at the root>
         idClass: [ "string", ... , "string" ],
                <optional, default = all, "" = no idClass>
         directGazeDuration: {
                <optional, default = all>
            min: <long>,
            max: <long>
         }
         objectType: [ "string", ... , "string" ]
                <optional, default = all, "" = no objectType>
         objectId: [ "string", ... , "string" ],
                <optional, default = all, "" = no objectId>
      }
      triggers : [
         {
            triggerId : "string",
                <optional>
            daysOfWeek: ["Mon","Tue","Wed","Thu","Fri","Sat","Sun"],
                <optional, default = all>
            timesOfDay: [
                <optional, default = all>
               {
                  start: "11:00",                  <required>
                  end: "17:00"                     <required>
               },
               ...
            ],
            actions: [
                <required - can be empty (no actions)>
               "string",
               ...
            ],
            reply: {
                <optional, default = no reply>
```

```
            "replyDelay": long,
                 <optional, in milliseconds, default = 0>
            "message": "string",
                 <optional, default = no message>
            "disposition": double,
                 <optional, range [-1 .. 1], default = 1>
            "tags": [ "tag1", ... "tagN" ]
                 <optional, default = no tags>
         },
         conditionalReply: [
             <optional, default = no conditional reply>
             {
                  "actionResponse": [ integer, ..., integer ],
                       <required>
                  "replyDelay": long,
                       <optional, in milliseconds, default = 0>
                  "message": "string",
                       <optional, default = no message>
                  "disposition": double,
                       <optional, range [-1 .. 1], default = 1>
                  "tags": [ "tag1", ... "tagN" ]
                       <optional, default = no tags>
             }
             ...
         ],
      },
      ...
   ],
   excludeDates : [
             <optional, default = none>
            "7/4",
            "12/25",
            "4/10/2017",
            ...
   ]
  }
  ...
],
noTriggerReply: {
             <optional, default = no reply>
  "replyDelay": long,
             <optional, in milliseconds, default = 0>
  "message": "string",
             <optional, default = no message>
  "disposition": double,
             <optional, range [-1 .. 1], default = -1>
  "tags": [ "tag1", ... "tagN" ]
             <optional, default = no tags>
},
nFactorDef: [
  {
     "name": string,
        <required>
     "failOnMismatch": string,
```

```
            <optional: "delayed"/"immediate"/"none", default = "delayed">
         "maxDelay": <milliseconds>,
            <optional, default = 60000 (1min)>
         "factors": [
            "<factor_name>|<factor_value>",
            ...
         ],
         "actions": [
            "<action_command>",
            ...
         ]
      },
      ...
   ],
   emailDef: [
      {
         "label": string,
            <required>
         "recipients": [ "recipient1", ... "recipientN" ],
            <required, escape sequences can be used>
         "subject": string,
            <required, escape sequences can be used>
         "cc": [ "cc1", ... "ccN" ],
            <optional, escape sequences can be used>
         "bcc": [ "bcc1", ... "bccN" ],
            <optional, escape sequences can be used>
         "message": string,
            <optional, escape sequences can be used>
         "attachments": [ "attachment1", ... "attachmentN" ],
            <optional, escape sequences can be used
             http://, https://, cvos:// url schemes are supported>
      },
      ...
   ]
   smsDef: [
      {
         "label": string,
            <required>
         "recipients": [ "recipient1", ... "recipientN" ],
            <required, escape sequences can be used, phone numbers using
               the the E.164 format required>
         "maxPrice": string,
            <optional>
         "message": string,
            <optional, escape sequences can be used>
      },
      ...
   ],
}
```

- Events that are older than maxEventLatency will be ignored. Event time is defined as the difference between the time the event was generated - as measured by the SAFR Cloud (or machine Platform is running) and the time the event is processed – as measured on the machine the SAFR Actions app is running.

## 18.2 rules

### 18.2.1 event

- For rules.events that allow arrays, the new event must contain all the specified array elements to match. For example, if a config file specified rules.events.personType as follows:

```
personType: [
    "staff",
    "admin",
    "guest"
],
```

  Then the new event's personTags array would have to have all 3 specified personTypes for it to match the rule.

- personTags: all elements in one of sub-arrays need to exist in event's personTags array to match the rule.

### 18.2.2 trigger

- Event (id) can trigger actions only once (albeit multiple triggers can be activated simultaneusly).
- Event (id) can trigger replies only once per reply context (triggered, notTriggered). Multiply replies can be triggered simultaneously (one reply per triggered action).
- triggerId - ID Unique within the triggers array used in rare case where you want only 1 trigger to fire. If triggerId is same on 2 or more, only 1st of all matching get triggered.
- Useful if date filters are overlapping and during overlap times only wish to actions from single trigger.

### 18.2.3 conditionalReply and reply

- disposition refers to how the reply should be perceived by the recipient:
  - Replies with disposition in range [-1 .. 0 > are interpreted as negative replies and can thus be expected to be presented (color, sound, voice) in manner consistent with rejection.
    - Value of 0 is a neutral reply and can thus be expected to be presented in a neutral manner (color, sound, voice).
    - Replies with disposition in range <0 .. 1 ] are interpreted as positive replies and can thus be expected to be presented (color, sound, voice) in manner consistent with acceptance.
- When conditional reply is specified, non-conditional reply is used only as catch-all if none of the action response codes match.
- When conditional reply is specified, execution of the FIRST action in trigger will occur in blocking manner to enable retrieval of the response code from that FIRST action.
  - If any other actions are specified, they will be performed in non-blocking manner and their response codes will not be retrieved or used.
- When conditional reply is not specified, execution of all actions will occur in non-blocking manner.
- A reply is generated as follows:
  - One or more matching conditionalReply entries are sent
  - In addition, either the reply or noTriggerReply is sent
- URL used to post the reply: `<replyServer>/stream/reply.<Base64(event Id)>`
  - By default the reply is posted to the CVOS server (replyServer)
  - POST is a file of the following format.
  - The reply object (JSON file) can be obtained by querying the CVOS server after some delay after the event was fired

#### 18.2.4 actions

- Each action is a command string that will be executed.
- Commands are executed asynchronously unless conditionalReply is set
- If conditionalReply is set, the first command is executed synchronously.
- Some Windows programs (particular Windows programs that do not have a message pump) may not run in background and block until the command returns.
- If multiple actions are defined, each action is executed in sequence.
- For information on the syntax for emails, see Email Actions below.
- For information on the syntax for SMS notifications, see SMS Actions below.

## 18.3 Action and Reply Message Escape Sequences

```
#N - name
#F - first name (name prefix up to first white-space)
#U - surname (name postfix: staring after first white-space sequence to
   the end of name string)
#T - person type
#S - source
#I - site
#D - person id
#R - root person id
#E - person external id
#G - gender
#A - age       (###)
#M - sentiment (#.##)
#L - smile     (true/false)
#V - event type
#v - event id
#B - tag type
#C - action type
#b - tag id
#c - action id
#k - direction id
#s - event start time (milliseconds since epoch)
#r - event start date/time (local time)
#p - validation phone
#e - validation email
#H - home location
#t - personTags (comma separate list of personTags)
#O - company
#m - moniker
#<d>m - moniker substring (delimited by white-space)
        indexed by single decimal digit 0-9 .  E.g.:  #0m or #3m
#l - similarityScore (#.####)
#a - idClass
#Z - directGazeDuration
#o - objectType
#d - objectId
#u - occlusion (#.##)
#i - liveness (#.##)
#n - livenessConfirmed (true/false)
#z - mask (true/false)
```

## 18.4 N-factor Actions

- nFactor actions are started via internal @nFactorStart action within standard trigger actions array:

```
{
   triggerId : "string",
   ...
   actions: [
      "@nFactorStart <name>",
      ...
   ],
   reply: {
      ...
   },
   conditionalReply: [
      ...
   ]
}
```

At the time of starting, the following occurs:

- @nFactorStart action just as any other action is first resolved for escape sequences
- factors (names and values) defined in corresponding nFactorDef are also resolved for escape sequences
- actions defined in corresponding nFactorDef are also resolved for escape sequences
- eventStartTime is retrieved from the triggering event

Response codes for nFactorStart action:

- 0 = nFactor monitoring for action started successfully

nFactorStart-ed action are resolved via nFactorResolve commands. When all factors needed for the actions are resolved, actions are executed:

```
{
   triggerId : "string",
   ...
   actions: [
      "@nFactorResolve <name> <factor_name>|<factor_value>",
      ...
   ],
   reply: {
      ...
   },
   conditionalReply: [
      ...
   ]
}
```

- At the time of resolving the following occurs:
  - @nFactorResolve action just as any other action is first resolved for escape sequences.
  - Each factor can resolved at most one not yet resolved factor requirement.
- Response codes for nFactorResolve action:
  - 0 = resolved last unresolved factor
    - Executed action response supersedes
  - >=1 resolved other than last unresolved factor
  - -1 = no matching <Site>/<Source>/<name>

- -2 = <mismatched factor - ignored since failOnMismatch = none>
- -3 = <matches but already resolved>
- -4 = <matches but too late to resolve>
- -5 = <mismatched factor - error since failOnMismatched = delayed/immediate>
- -6 = unknown (not defined in nFactorDef) factor_name.

- @nFactorStartOrResolve combines starting and resolving into one action. Usually used for generating pseudo events from monikers.

```
{
   triggerId : "string",
   ...
   actions: [
      "@nFactorStartOrResolve <name> <factor_name>|<factor_value>",
      ...
   ],
   reply: {
      ...
   },
   conditionalReply: [
      ...
   ]
}
```

@personEventFromMoniker action generates a pseudo person event from moniker created by combining all the resolved factor values (separated by space) in order listed in factors array. The generated event is of type person which is populated with meta-data of person with moniker matching the assembled moniker value.

```
{
   nFactorDef : [ {
      factors : [
            "moniker|**",
            "moniker|1**",
            "moniker|2**",
            "moniker|3**"
      ],


      actions : [
            "@personEventFromMoniker"
      ]
      }
   ]
}
```

## 18.5 Email Actions

To send emails using actions, you must do the following:

1. Obtain an SMTP server account that you can use to send emails.
2. Configure SAFR so that it's ready to use your SMTP server account to send emails. You can do this from the Status page of the Web Console. On Windows machines, you can also do this via **Tools -> Configure Email Server** in SAFR Actions.
3. Configure the emailDef section of the SAFRActions.config, as described below. Note that your emailDef section can define multiple emails, each one being identified by the `label` field.

```
emailDef: [
    {
        "label": string,
            <required>
        "recipients": [ "recipient1", ... "recipientN" ],
            <required, escape sequences can be used>
        "subject": string,
            <required, escape sequences can be used>
        "cc": [ "cc1", ... "ccN" ],
            <optional, escape sequences can be used>
        "bcc": [ "bcc1", ... "bccN" ],
            <optional, escape sequences can be used>
        "message": string,
            <optional, escape sequences can be used>
        "attachments": [ "attachment1", ... "attachmentN" ],
            <optional, escape sequences can be used
                http://, https://, cvos:// url schemes are supported>
    },
]
```

- **label**: The label used to identify this particular email.
- **recipients**: One or more email addresses where the email will be sent.
- **subject**: The text that will appear in the email's subject line.
- **cc**: List of email addresses that will be cc'ed on the email.
- **bcc**: List of email addresses that will be bcc'ed on the email.
- **message**: The text that will be the body of the email.
- **attachments**: The location of any attachments you want to attach to the email.

4. In the `actions` field of SAFRActions.config, enter a string with the following syntax: "@emailSend <label>", where <label> = the label of whichever email within your SAFRActions.config that you want to use.

## 18.6 SMS Actions

To use Short Message Service (SMS) notifications within actions, you must do the following:

1. Obtain an AWS account which is configured for your region so it can send SMS messages.
2. Configure SAFR so that it's ready to use your AWS account to send SMS notifications. You can do this from the Status page of the Web Console. On Windows machines, you can also do this via **Tools -> Configure SMS Sender** in SAFR Actions.
3. Configure the smsDef section of the SAFRActions.config, as described below. Note that your smsDef section can define multiple SMS messages, each one being identified by the `label` field.

```
smsDef: [
   {
      "label": string,
         <required>
      "recipients": [ "recipient1", ... "recipientN" ],
         <required, escape sequences can be used, phone numbers using the
            the E.164 format required>
      "maxPrice": string,
         <optional>
      "message": string,
         <optional, escape sequences can be used>
   },
```

```
]
```

- **label**: The label used to identify this particular SMS message.
- **recipients**: The list of recipients to receive the SMS message, formatted using the E.164 format. (e.g. +2065551313)
- **maxPrice**: The maximum amount in USD that you are willing to spend to send the SMS message. Amazon SNS will not send the message if it determines that doing so would incur a cost that exceeds the maximum price. See the description of the `AWS.SNS.SMS.MaxPrice` attribute here for more information about this field.
- **message**: The text message to be sent.

4. In the `actions` field of SAFRActions.config, enter a string with the following syntax: "@smsSend <label>", where <label> = the label of whichever SNS message within your SAFRActions.config that you want to use.

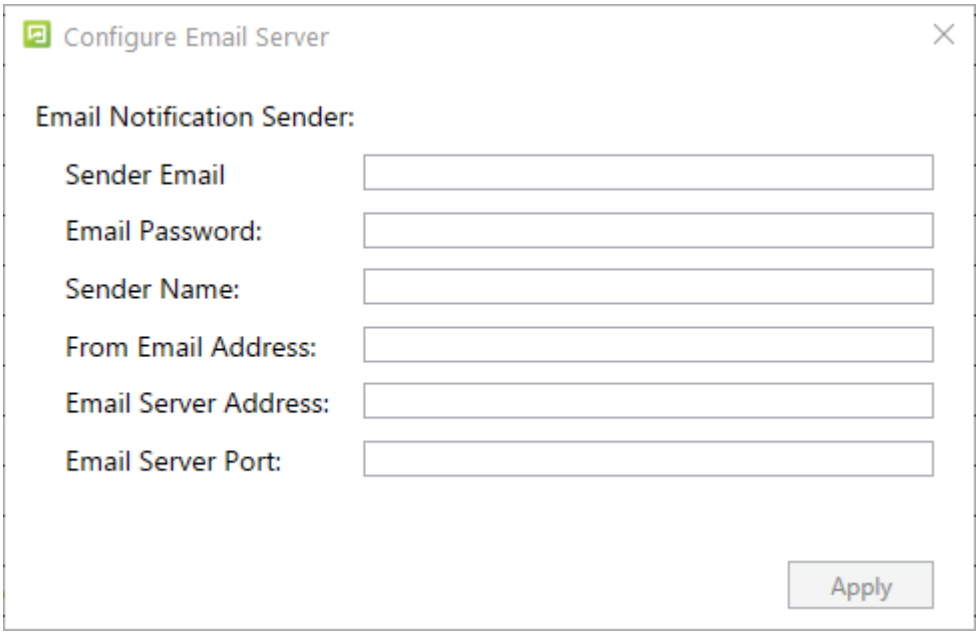
# 19 SAFR Actions

SAFR Actions is a GUI tool to aid users to edit the SAFRActions.config configuration file. It comes already installed with SAFR Platform and SAFR Edge.

SAFR Actions is generally very light in terms of system resource usage but can be burdensome if the rate of events requiring handling is high (for example, hundreds per second) and actions scripts are computationally or I/O intensive. However, this is not a common occurrence.

## 19.1 Configure Email Server

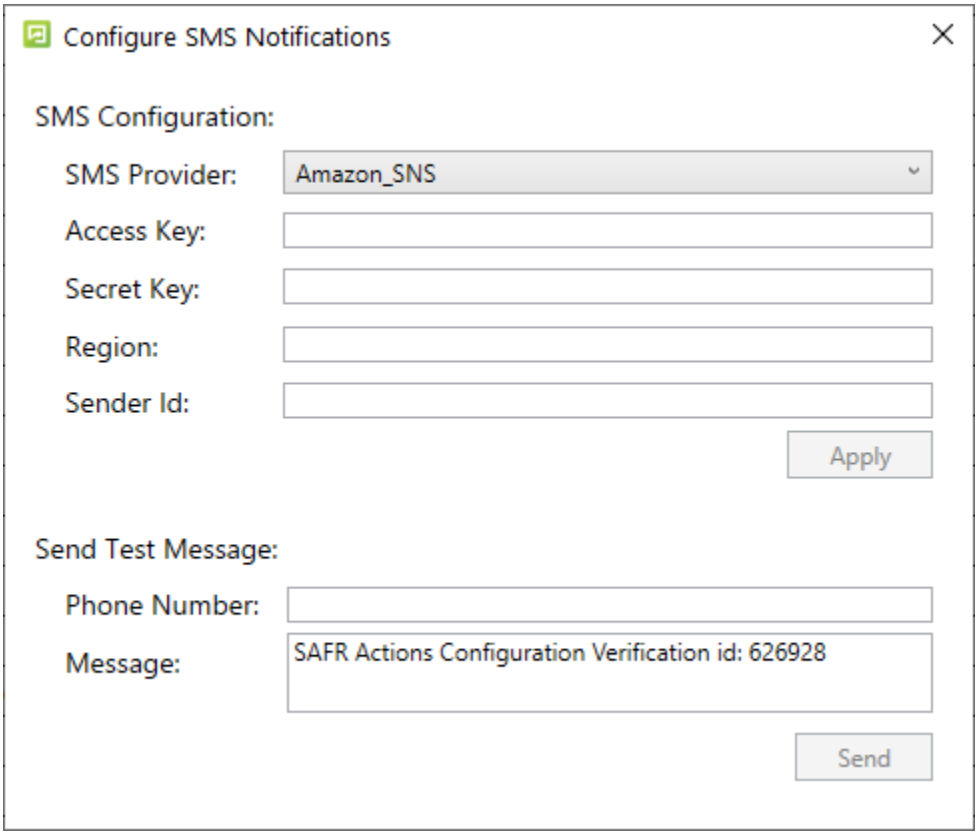
Enables SAFR's actions to send emails. Before you can configure SAFR to send emails, make sure you obtain an SMTP server account that you can use to send emails.




- **Sender Email**: The email username of the SMTP account. (e.g. me@gmail.com)
- **Email Password**: The password for the SMTP account.
- **Sender Name**: The email username of the SMTP account. (e.g. me@gmail.com)
- **From Email Address**: The email address that will appear on the "From" line. This feature isn't supported by all email servers; if this field isn't used then the *Sender Email* value is used for the "From" line.
- **Email Server Address**: The address of the SMTP email server.
- **Server Port**: The email server port. The default port for SMTP is 587.

## 19.2 Configure SMS Sender

Enables SAFR's actions to send short message service (SMS) messages. Before you can set up SMS, you must first set up an AWS account which is configured for your region so it can send SMS messages.




- **SMS Provider**: The SMS provider that you're using. This value will always be `Amazon SNS`.
- **Access Key**: Your Amazon SNS Access Key.
- **Secret Key**: Your Amazon SNS Secret Key.
- **Region**: The region of your Amazon SNS.
- **Sender Id**: The name that will be used to send the SMS notifications.
- **Send Test Message**: Configure the test message that will be sent after you finish setting up SMS.
  - **Phone Number**: The phone number to which the test message will be sent.
  - **Message**: The text message that will be sent to the phone number specified above.

# 20 Large Scale Deployments

At some point, your SAFR system's capacity and/or performance may become limited by your SAFR Server; your server's load is primarily limited by the number of *face recognitions* occurring per second and the number of people in your Person Directory. You can install additional SAFR Servers on other machines in order to achieve higher capacity, improve performance, and improve resiliency. The first SAFR Server you install is your primary server, while all additional servers are secondary servers.

In order to install additional servers, you must first install an SSL certificate on your primary server. See SSL Certificate Installation for information about how to do this.

**Note**: You can change which machine is the primary server by uninstalling the primary server, waiting 24 hours, and then re-installing the SAFR Server on a different machine. If you want to preserve existing data, you should create a backup prior to the change.

There are three different load balancing configurations you can choose from.

- **Prescribed Configuration**: Cameras are connected to Desktop clients or VIRGO daemons running on the same machines that are hosting your SAFR Servers. This gives you tight control over how your face recognition load is distributed, since the video feeds' face recognition requests are processed on the same machine where the video feeds are connected.
- **Software-Based Load Balancing Configuration**: In this configuration the machines hosting SAFR Servers do not also have cameras connected to them. All face recognition requests are initially sent to the primary server. The primary server acts as the load balancer for the server cluster.
- **External Load Balancing Configuration**: All recognition requests are directed at one or more external load balancer(s), which handle load balancing duties for the SAFR system.

## 20.1 Understand When to Scale

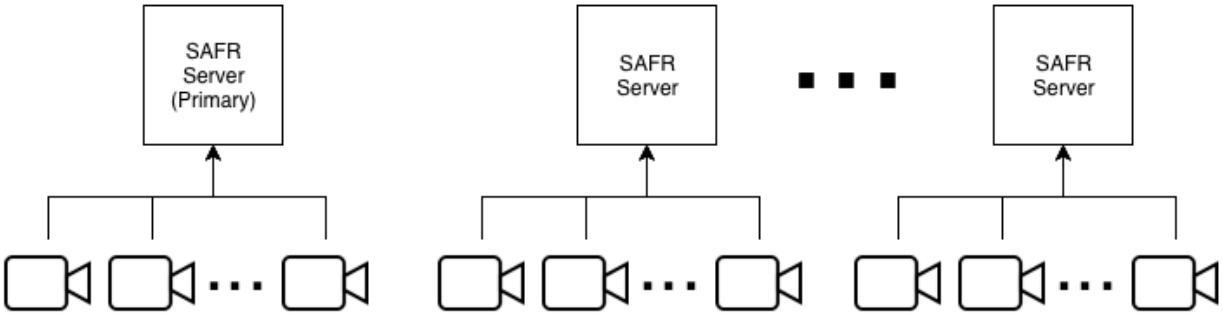
A single SAFR Server that's also running a Desktop client can handle up to 16 cameras, (assuming each camera view contains just a single face), as long as the host machine meets the recommended hardware requirements If the machine running the server doesn't have any cameras directly connected to it, then the server's capacity increases to 25 cameras, each camera view containing a single face. A higher number of faces per camera or a higher number of cameras requires either vertical scaling of a single server (i.e. more or faster CPUs) or horizontal scaling by installing more SAFR Servers.

For prescribed deployments, the system requirements of the Desktop client need to be combined with those of SAFR Server. A single Desktop client typically handles up to 16 cameras as long as it is equipped with a GPU card (see SAFR System Requirements). In this way, running SAFR Server and the Desktop client on the same machine using the recommended configuration can host up to 16 cameras, each camera with a single face.

## 20.2 Prescribed Configuration

In the prescribed configuration, you run multiple SAFR Servers by connecting cameras to Desktop clients or VIRGO daemons running on the same machines that are hosting SAFR Servers. In this way, you have tight control over which servers take the video feed load. This is also a useful configuration for very small stream count loads where running a Desktop client on a separate machine from the SAFR Server would take more resources than are required for the given use case.

The following illustration demonstrates this setup:

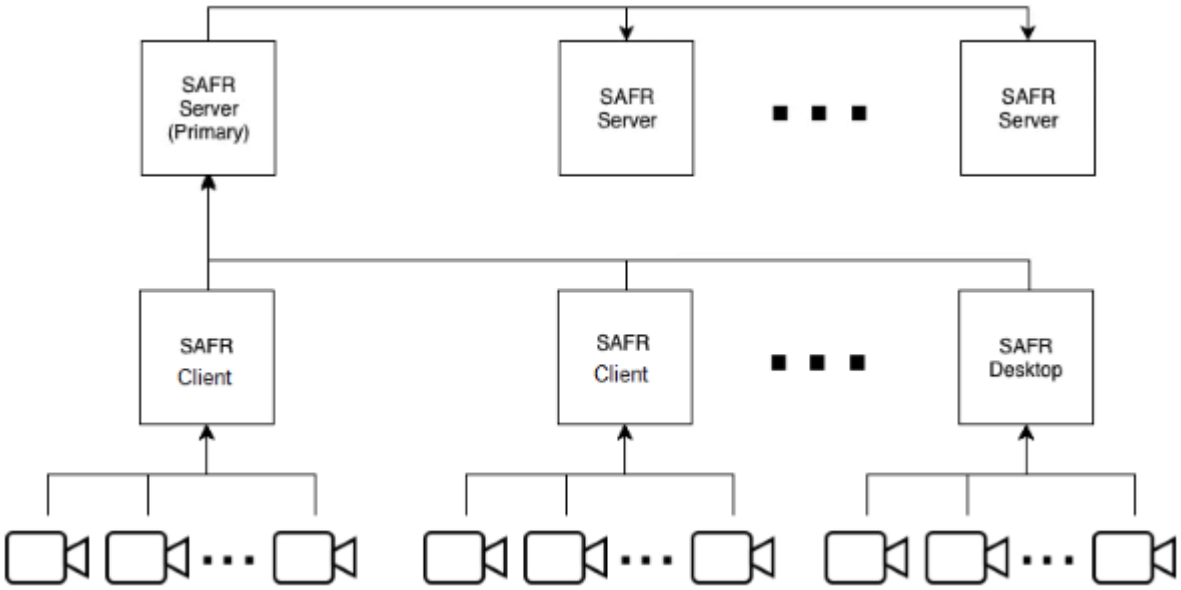



Most services (e.g. face service, events, and reports) are performed on the server where recognition requests are sent.

See Add a Secondary Server for information about how to add secondary servers.

## 20.3 Software-Based Load Balancing Configuration

In the software-based load balancing configuration, cameras aren't connected to machines running SAFR Servers. When newly installed secondary servers are configured, they check in with the primary server and announce that they're ready to receive load-balanced traffic. All recognition requests go through the primary server. which balances the load among itself and all other servers in the SAFR system. The following illustration demonstrates this setup:




See Add a Secondary Server for information about how to add secondary servers.

### 20.3.1 Secondary SAFR Server Health Checks

- At startup each server, both primary and secondary, registers itself by posting its status to the database on the primary server.
- The primary server directs requests to all secondary servers in a *least connection method* that keeps the load evenly balanced among all secondary servers.
- As long as a secondary server remains healthy, the primary server keeps the secondary server in its load balance rotation.

- Status information about all secondary servers is stored in the primary server database. In this way, it is not lost on restart of the primary server.
- Every minute the secondary servers and the primary server send a status update to the database on the primary server.
- Every five seconds, the SAFR load balancer process on the primary server calls a heath check API on each secondary and the primary server.
- If the health check fails for 15 seconds, the server is pulled out of rotation and is no longer sent requests. If the health check succeeds for that server for ten seconds, the server is returned to accepting requests.
- If a server's status has not been reported for over five minutes, it is removed from the load balancer configuration. In this case, it is no longer sent requests or health check requests.
- If a secondary server has been pulled out of rotation for not responding to health checks, or is removed from the load balancer config for not reporting status for more than five minutes, it can still be put back in rotation through any of the following:
  - If a network interruption prevents the secondary server from sending a request, the secondary server continues to send a status update at its regularly scheduled interval after it goes back online and its status is updated in the primary server.
  - If the secondary server is restarted, it sends a status update after all services are started and ready.
  - If the secondary server IP address is changed, the server must be manually restarted to force it to send a status update to the primary server with the new IP address.

### 20.3.2 Manually Configure Load Balancing

SAFR Servers can be manually enabled or disabled to accept load balancing traffic.
**Note**: If the server you want to disable is the only one configured to take traffic, you receive a warning and prompt to continue. In this case, should you proceed, your system will most likely go offline.

**Disable Load Balancer Traffic**

To stop receiving traffic on a server, log in to a shell on the server and run the appropriate command for your server's OS:

| OS | Command |
|---|---|
| Windows | `"C:\Program Files\RealNetworks\SAFR\bin\server-status.py" --disable` |

It may take up to one minute for the desired traffic state to change.

**Enable Load Balancer Traffic**

To stop receiving traffic on a server, log in to a shell on the server and run the appropriate command for your server's OS:

| OS | Command |
|---|---|
| Windows | `"C:\Program Files\RealNetworks\SAFR\bin\server-status.py" --enable` |

It may take up to one minute for the desired traffic state to change.

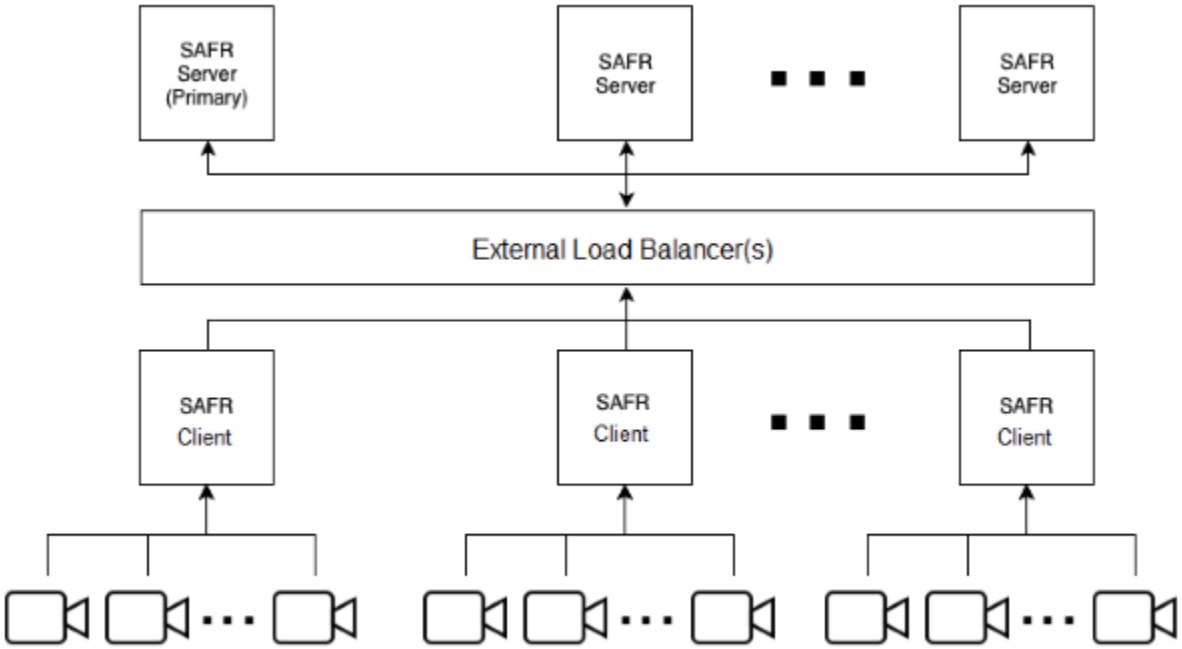
## 20.4 External Load Balancing Configuration

The software-based load balancing for SAFR is limited by the primary server being a single point of failure. All traffic must be routed through the primary server to reach the rest of the servers. If the primary server is down, all traffic will stop.

External load balancing may be used to provide a more robust setup that can better deal with server failure than software load balancing.

When using external load balancing solutions, you can route traffic to one or more load balancer(s), have HTTPS/SSL terminate there, and then proxy requests to the backend servers over either HTTP or HTTPS. HTTP would be OK in situations where network traffic is isolated to a trusted network, or when network sniffing by non-target hosts is impossible.

If HTTPS is used to proxy traffic to SAFR servers, you should manually disable load balancing on all secondary servers as described above so that the primary server isn't double load balancing traffic to them. A valid (i.e. non self-signed) SSL certificate would still need to be installed and configured on the primary server. Secondary servers should be fine with the default (i.e. self-signed) certificate, if your load balancer allows it.




See Add a Secondary Server for information about how to add secondary servers.

## 20.5 Troubleshooting Tips

- The network throughput of the primary server is a possible performance bottleneck. Monitor the primary server network throughput during maximum concurrency times to make sure the network is not over-saturated.

# 21 Database Redundancy

The first SAFR Server you install will automatically become the primary server. All subsequent servers you install will be secondary servers. There are two types of secondary servers:

- **Simple**: Does not replicate the database data.
- **Redundant**: Replicates database data from the primary server. If there are at least two redundant secondary servers (three servers total), fail-over functionality is enabled, which means that if the primary server is offline, the secondary servers will continue to function.
  **Note**: Only Windows and Linux SAFR Servers can become redundant secondary servers.

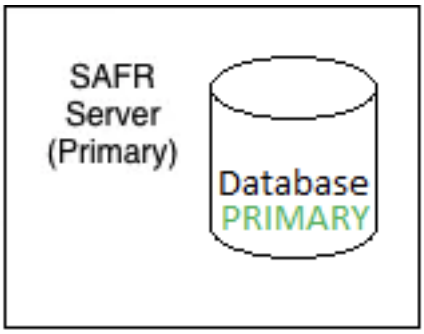
With both types of secondary servers the traffic for the CoVi and Event API services are load-balanced across all servers. Other services, such as VIRGA (feed management), Reports, and the Web Console are not load-balanced and are always served from the primary server.

## 21.1 Multiple Server Installations

### 21.1.1 1 Server

Install a single SAFR Server. The database runs on the primary (and only) server.

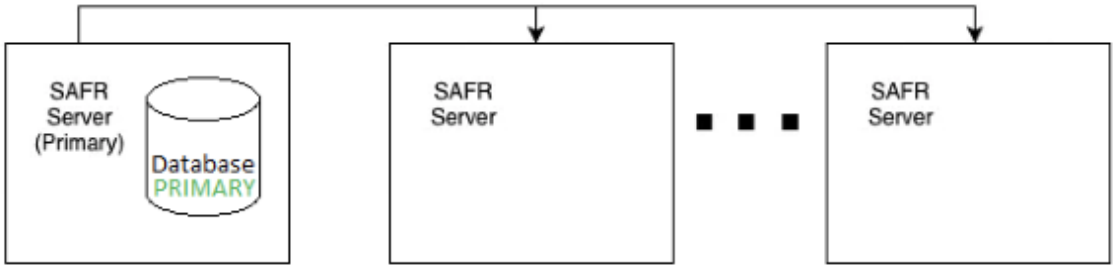
- This configuration provides no redundancy if the primary server is offline.

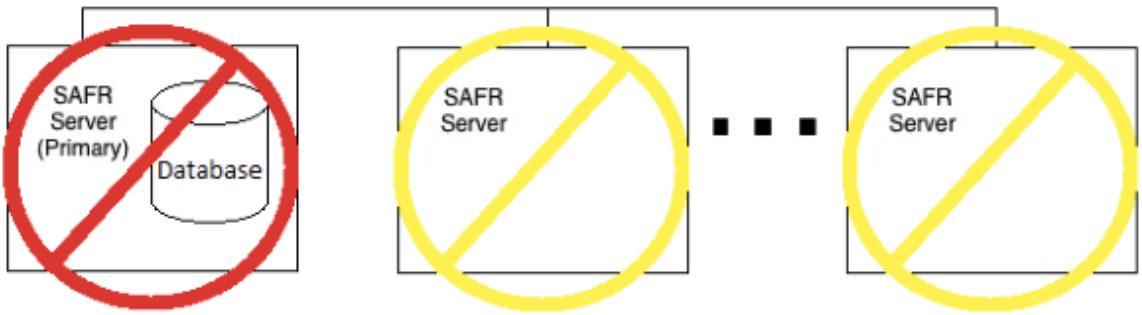



### 21.1.2 2+ Servers (Simple)

Install a primary server and one or more simple secondary servers. The database runs on the primary server only.

- This configuration provides no redundancy if the primary server is offline.
- The secondary servers can be offline without impacting functionality, although performance may suffer.

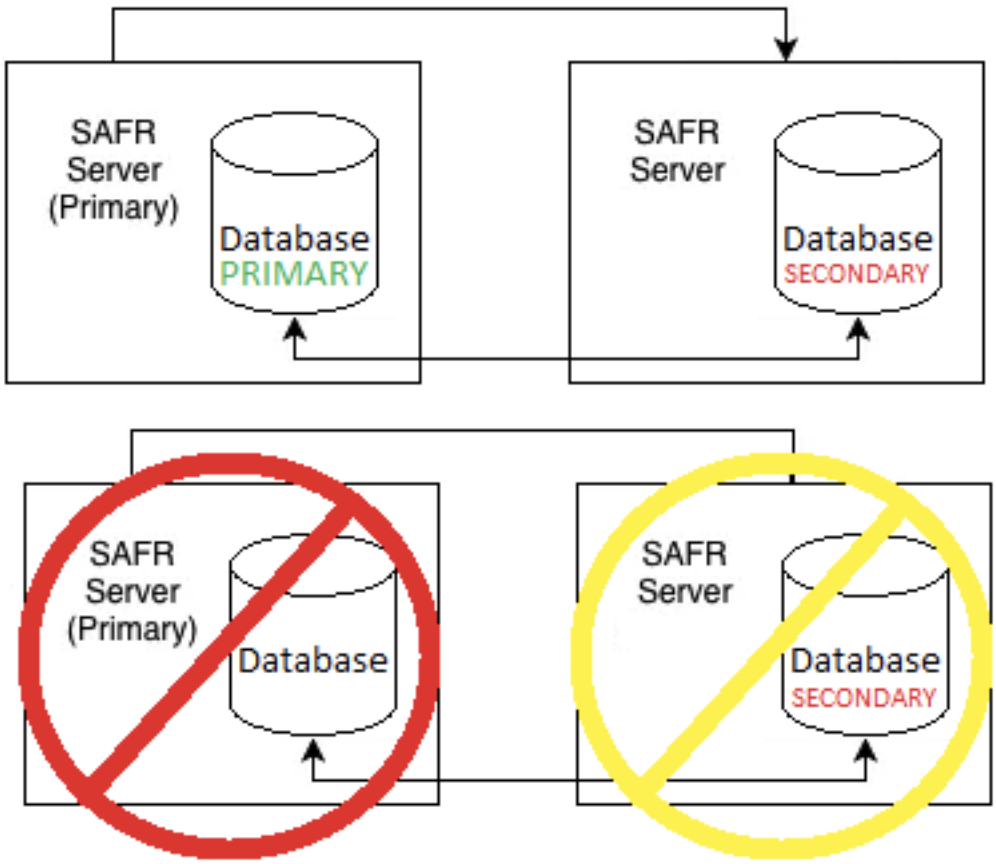





### 21.1.3 2 Servers (Redundant)

Install a primary server and a redundant secondary server. The database runs on both the primary and secondary servers.

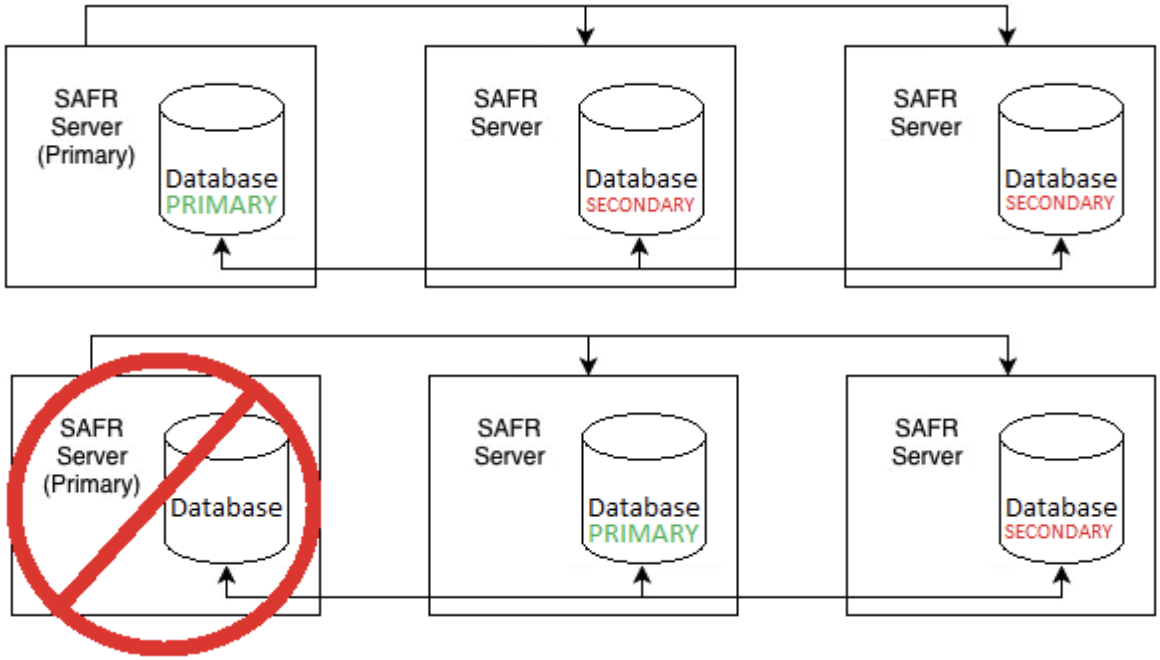
- This configuration provides no redundancy if the primary server is offline.
- The secondary server can be offline without impacting functionality, although performance may suffer.
- Database content is replicated to the secondary server, which provides another copy of the data. This can act as a backup in case of emergencies, but the backup & restore scripts should be used for proper and complete backups.



### 21.1.4 3 Servers (Redundant)

Install a primary server and 2 redundant secondary servers. The database runs on both the primary and both secondary servers.

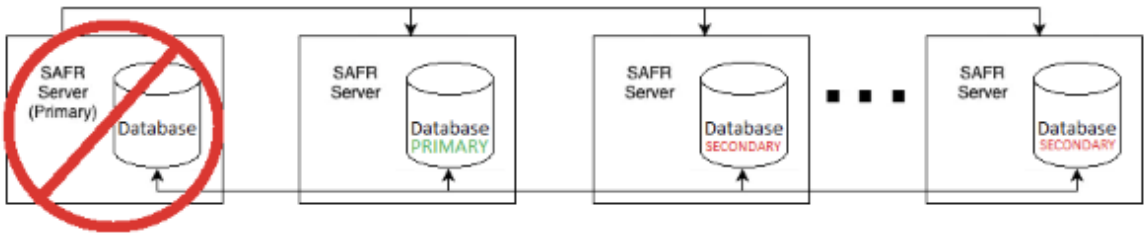
- This configuration provides redundancy if the primary server is offline.
- A single server can be offline without impacting functionality. If the primary and one secondary, or both secondary servers go offline, the whole cluster will go offline. A majority of the servers are required to be online for your SAFR system to function.




### 21.1.5 4+ Servers (Redundant)

Install a primary server and 3 or more redundant secondary servers. The database runs on both the primary server as well as all the secondary servers. Only the first two secondary servers that were added can act as the primary database host, though. Additional secondary servers will continue to replicate database data but cannot become the primary database host and do not count towards the "majority" count required for a primary database host to be elected.

- This configuration provides redundancy if the primary server is offline.
- A single server can be offline without impacting functionality. If the primary and one of the first two secondary, or both of the first two secondary servers go offline, the database cannot have a primary member, and the whole cluster will go offline. A majority of the first three installed servers is required to be online for SAFR to function. Additional secondary servers past the first two can be offline without any impact to functionality.




### 21.1.6 Add a Secondary Server While Connected to the Internet

If your system is connected to the Internet, do the following to add a secondary server to your existing primary server:

1. Download and install SAFR Platform on the additional machine.
2. To start the SAFR auto-discovery process:
   - Connect the Desktop client to the primary server as described here .
3. During auto-discovery, the following automatically happens:
   1. The secondary server contacts a SAFR Licensing Server in the cloud to acquire a license.
   2. The SAFR Licensing Server authenticates the SAFR account credentials.
   3. The SAFR Licensing Server identifies the license and deployment type.
   4. A suitable license is returned to the secondary server and information about the primary server is returned to the secondary server, including the hostname.
4. If your new secondary server is on a Windows or Linux machine, you will be prompted to choose which kind of secondary server you want: simple or redundant. If your new secondary server is on a macOS machine no prompt will occur; macOS secondary servers are always simple.
5. Auto-discovery will now continue, with the following automatically occurring:
   1. The secondary server re-configures itself to reference the primary server.
   2. The secondary server registers itself with the primary server.
   3. The primary server updates its local database and adds the new secondary server to its load balancer configuration.
   4. From this point on, the primary server uses the secondary server as an additional node in its cluster.

### 21.1.7 Add a Secondary SAFR Server While Offline

If you are not connected to the Internet, you can still connect to the primary SAFR Server, but the auto-discovery process is not available. You must instead manually configure the newly installed secondary server to locate the primary server. When manually configuring the new secondary server, Windows and Linux users will need to choose if they want the server to be a simple secondary server or a redundant secondary server.

1. Download and install SAFR Platform on the second machine.
2. Run the `safr-worker` script on your secondary server by doing the following:
   1. On the primary server record the contents of `C:\Program Files\RealNetworks\SAFR\mongo\.adminpass` and `C:\Program Files\RealNetworks\SAFR\mongo\mongod.keyfile`
   2. On the new secondary server, open a command prompt by right-clicking on the **Start** menu, select **Run**, and enter `cmd`.
   3. If you want it to be a simple secondary server, in the new command prompt run the following command, substituting the password from Step 1 for PASSWORD and the primary server hostname for HOSTNAME:
      - `"C:\Program Files\RealNetworks\SAFR\bin\safr-worker.py" -p PASSWORD HOSTNAME`

      OR

4. If you want it to be a redundant secondary server, in the new command prompt run the following command, substituting the `mongod.keyfile` contents from Step 1 for KEYFILE, the password from Step 1 for PASSWORD, and the primary server hostname for HOSTNAME:

   - `"C:\Program Files\RealNetworks\SAFR\bin\safr-worker.py" -s KEYFILE -p PASSWORD HOSTNAME`

### 21.1.8 Error Messages

When attempting to join a new secondary server, you might encounter the following error messages:

| Error Message | Description |
|---|---|
| System is offline | Network or system connectivity issue. Attempt to access the system at a later time. |
| SAFR master host is not reachable | Ensure all servers are connected to the same network and try again. |
| Improperly configured SSL certificate | SSL certificates are required to set up multiple servers. See the SSL Certificate Installation page for information about how to install an SSL certificate. |
| Secure connection error. Check server for valid SSL certificate | SSL certificates are required to set up multiple servers. See the SSL Certificate Installation page for information about how to install an SSL certificate. |
| Incomplete server connection | Attempt to join again; a persistent issue may require either uninstalling and reinstalling SAFR Platform on your servers or contacting your SAFR support representative. |

# 22 Object Storage Service Redundancy (CVOS)

The Object Storage Service is used for storing objects, such as profile and event images, as well as ephemeral data, such as event reply messages.

The service can operate in a redundant configuration when you have multiple SAFR servers running. All redundant secondary servers are load-balanced by the primary server for all Object Storage Service requests it receives.

## 22.1 Local Object Storage vs Shared Object Storage

### 22.1.1 Local Object Storage

By default all redundant servers will save objects locally, and ask other Object Storage Servers for objects it does not have locally.

When you're using local object storage, you will lose access to all objects that are only stored by an offline Object Storage Server until the server becomes healthy again. If that server's objects are lost, and you do not have backups, they will be unrecoverable.

Backups must be run on every redundant server that has Object Storage enabled.

### 22.1.2 Shared Object Storage

Using network storage (NFS, SMB, etc) provides a shared location for each server to save and retrieve objects from. This provides each Object Storage Server with access to all of the objects, rather than just objects saved to its local storage.

Shared storage also provides an easier backup process, as you only have to run it from the primary server.

## 22.2 Simple vs. Redundant Secondary Server Behavior

### 22.2.1 Simple Secondary Servers

On simple secondary servers, the Object Storage Service will operate in proxy mode.

Object Storage Servers operating in proxy mode will not attempt to use their own storage for objects, but will instead proxy the request to Object Storage Services that are running on either the primary server or on a redundant secondary server. If the redundant server it contacts doesn't have the object, the contacted redundant server will ask all other redundant servers for the object.

The list of servers that run the Object Storage Service is stored in the database and updated every minute. If a host does not respond within a timeout, it is de-prioritized.

### 22.2.2 Redundant Secondary Servers (and the Primary Server)

On both the primary server and on redundant secondary servers the Object Storage Service stores new objects in storage.

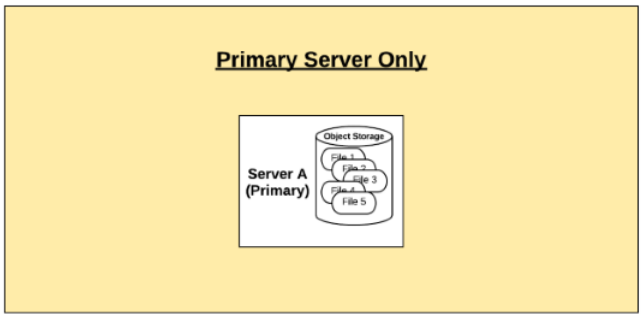
When a server receives a request for a file it does not find in its storage, it will request the object from other Object Storage Servers via HTTPS, and return the object if found. (The same applies for DELETEs.) This allows multiple Object Storage Servers to operate without using shared network storage, with each server saving a subset of the total objects, and relaying requests for other objects to its neighbors.

Even when using shared network storage, sometimes a request will come in for a new object before it is visible to all systems on the shared storage. The Object Storage Service will ask all the other Object Storage Servers for the object until it finds one that has the object.

## 22.3 CVOS Redundancy Configurations

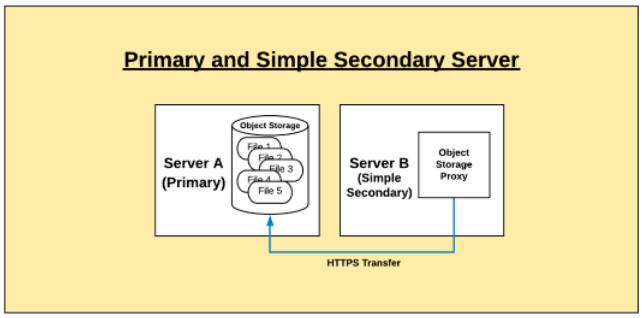
### 22.3.1 Single Server, Local Storage

All objects are stored on a single server, and no proxying requests occur.



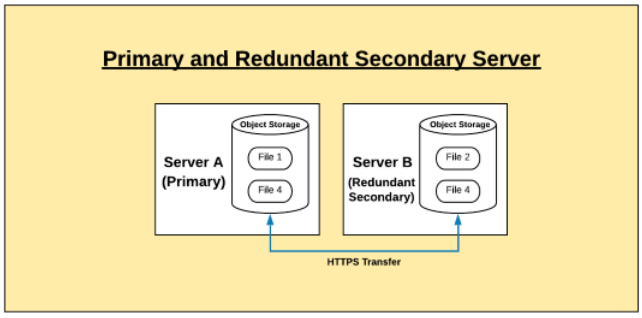

### 22.3.2 Primary and Simple Secondary Servers, Local Storage

All objects are stored on a primary server. Any object requests sent to the secondary server are proxied back to the primary server.




### 22.3.3 Primary and Redundant Secondary Servers, Local Storage

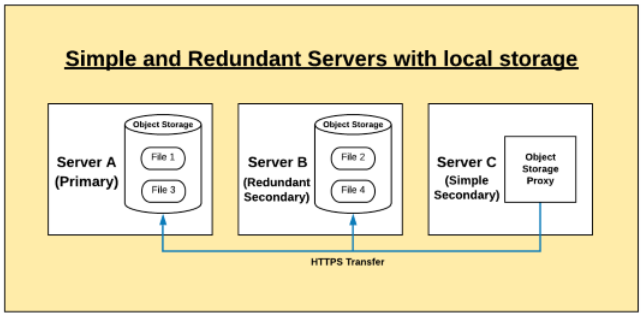
Objects are saved to whichever server receives the POST request. Objects requested in GET requests are facilitated from either system object storage, if found, or requested from other Object Storage Servers if not.




### 22.3.4 Primary, Redundant, and Simple Secondary Servers, Local Storage

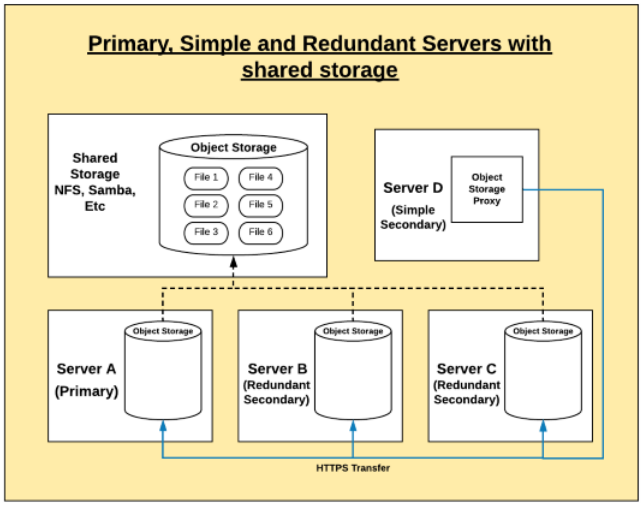
Objects are saved locally on the host that services the POST request. GET requests are served from local storage if found, or requested from other Object Storage Servers if not. All requests to server C are proxied

to servers A and B.




### 22.3.5 Primary, Redundant, and Simple Secondary Servers, Shared Storage

Objects are saved to shared storage on the host that services the POST request. GET requests are served from local storage if found, or requested from other Object Storage Servers if not. All requests to server C are proxied to servers A and B.




## 22.4 Migrating from Local to Shared Storage

If you start with local storage but later decide to move to shared storage, you will need to consolidate all of your objects to the new shared storage solution, delete the local copies, and then mount the shared storage to the right location. To do this, do the following:

1. Back up both the primary and redundant secondary servers to ensure you have a full backup of all SAFR content.
   - **On Windows**:
     - **Primary**: `python "C:\Program Files\RealNetworks\SAFR\bin\backup.py"`
     - **Redundant Secondaries**: `python "C:\Program Files\RealNetworks\SAFR\bin\backup.py" -o`
2. Stop all primary and redundant secondary servers by using the **stop** command. This can be done by doing the following on each server:
   - `"C:\Program Files\RealNetworks\SAFR\bin\stop.bat"`
3. Mount the new shared storage to a temporary location on primary and redundant secondary servers.

4. Copy all files from the primary server and every redundant secondary server(s) to the temporary location of the shared storage. from within the following paths:
   - `C:\ProgramData\RealNetworks\SAFR\cv-storage`
5. Delete or move the contents of the CV Storage folder on each primary and redundant secondary server as specified below.
   - `C:\ProgramData\RealNetworks\SAFR\cv-storage`
6. Unmount the temporary location of the new shared storage.
7. Mount the shared storage to the correct CV Storage location, or create a symlink to the shared storage location.
8. Start the primary and redundant secondary servers by using the **start** command. On each server, do the following:
   - `"C:\Program Files\RealNetworks\SAFR\bin\start.bat"`
9. Disable any automatic backups on redundant secondary servers.
   - Now that you're using shared storage, only the primary server needs to be backed up. If you have any automatic backups configured on secondary servers, disable them.

## 22.5 Backup and Restore with Local Storage

The SAFR backup and restore process when using shared network storage is straightforward - you just need to back up the primary server. This will back up all configs, database content, and Object Storage objects.

When using local storage, the objects are distributed to multiple servers, so the backup must be run on the primary server as well as any redundantly secondary servers.

The primary server should run a regular backup, while the redundant secondary servers run an '*objects only*' backup. The difference is just the addition of the "**-o**" flag to the backup script.

When restoring multiple backups, you can restore them all to the primary server, or you can restore the '*object only*' backups back to the same servers that they were backed up from.

### 22.5.1 Backup

- **On Windows**
  - **Primary**: `python "C:\Program Files\RealNetworks\SAFR\bin\backup.py"`
  - **Redundant Secondaries**: `python "C:\Program Files\RealNetworks\SAFR\bin\backup.py" -o`

### 22.5.2 Restore

- **On Windows**
  - **Primary**: `python "C:\Program Files\RealNetworks\SAFR\bin\restore.py" BACKUPFILENAME`
  - **Redundant Secondaries**: `python "C:\Program Files\RealNetworks\SAFR\bin\restore.py" -o BACKUPFILENAME`

## 22.6 Example Shared Storage Configuration

Windows cannot mount a shared storage location directly to the `C:\ProgramData\RealNetworks\SAFR\cv-storage` location. Instead it must create a symbolic link from that location to the shared storage location (either mapped network drive or SMB share).

1. Stop SAFR.
   - `"C:\Program Files\RealNetworks\SAFR\bin\stop.bat"`
2. Create NFS or some other shared storage location.
3. Delete the existing `C:\ProgramData\RealNetworks\SAFR\cv-storage` by running `rmdir /q /s C:\ProgramData\RealNetworks\SAFR\cv-storage` in an administrative command prompt. Deleting the existing cv-storage allows you to create a symbolic link from the 'cv-storage' location to your shared storage location. **Note**: Be sure you are either doing this on a new system without any data, or that

you've followed the migration steps above to consolidate your objects onto the new shared storage location.

4. Create the symbolic link from the `cv-storage` location to your shared storage location. To do this, run one of the following commands in an administrative command prompt:
   - If you're using a mapped network drive, run `mklink /d C:\ProgramData\RealNetworks\SAFR\cv-storage Z:\`
   - If you're using an SMB share, run `mklink /d C:\ProgramData\RealNetworks\SAFR\cv-storage \\servername\share`
5. Start SAFR.
   - `"C:\Program Files\RealNetworks\SAFR\bin\start.bat"`

# 23 SSL Certificate Installation

A properly installed secure sockets layer (SSL) certificate is critical to the secure operation of your SAFR Server. SAFR uses SSL certificates to establish secure network connections and data transfers. (i.e. https connections) SAFR requires https connections between SAFR Servers and between SAFR Servers and iOS Mobile clients. None of the other SAFR components require https connections.

Before you can install an SSL certificate on your SAFR Server, you must first configure a Domain Name System (DNS) hostname for your server within your network domain, as described below.

## 23.1 DNS Hostnames

If you do not currently have a domain, you need to first obtain a domain name registered and configured with an accredited domain registrar.

### 23.1.1 How to Obtain a Domain Name

In order to set up a DNS, you need a domain within which you can register hostnames. ICANN maintains a list of accredited registrars from which to choose.

The following is a list of common registrars:

- GoDaddy
- Google Domains
- AWS
- HostGator

Follow the processes on these websites to find, purchase, and configure your domain name. Most registrars offer the ability to host your DNS for you and most also give you a web interface for managing it.

The following links lead to instructions on how to modify DNS entries:

- GoDaddy
- Google Domains
- AWS
- HostGator

After you have your domain, you can create a DNS hostname entry for your SAFR Server.

### 23.1.2 What a DNS Hostname Entry Does

DNS is a system that translates a hostname to a network IP address. For example, when a user types `www.example.com` into their browser, DNS servers resolve it to the IP address where the website is hosted.

To provide this translation, DNS requires an entry for each hostname. This entry typically takes the form of an *A record* (the A stands for "Address") which defines the hostname to IP address translation in DNS. An *A record* is the most basic type of syntax used in DNS records.

The following is an example of an *A record*:

```
safr.example.com     A    12.34.56.78
```

### 23.1.3 Set Up a DNS Hostname Entry for your Primary Server

DNS can be managed in numerous ways. This might be a text file or a web interface for configuring the DNS entries. If you are not sure, contact the person managing the domain name for your network.

#### 23.1.4 What Type of IP Address Should I Use?

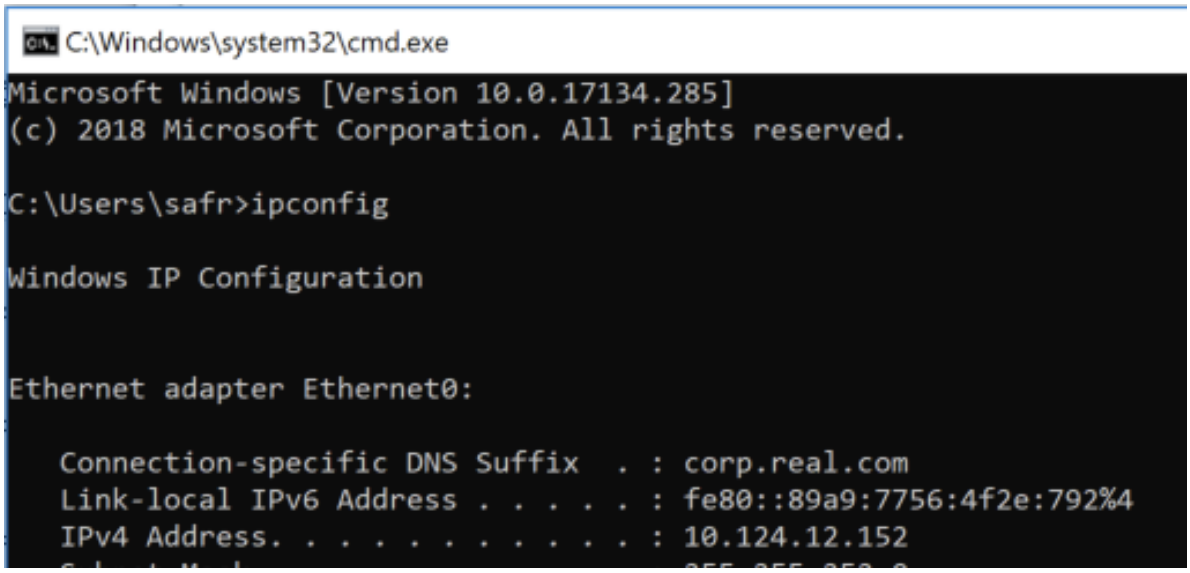
You should use a static IP address. If you instead choose to use DHCP to get a dynamically assigned IP address, and your IP address happens to change, your DNS hostname entry will stop working until you update the entry.

##### 23.1.4.1 Configure a Static IP

1. Obtain a static IP from your network administrator. The information should include the following:
   - Static IP address
   - Subnet mask
   - Default gateway
2. Configure your system as described below:
   - For Windows, see https://www.howtogeek.com/howto/19249/how-to-assign-a-static-ip-address-in-xp-vista-or-windows-7/.

The IP address should be the internal IP address of the computer running the SAFR Server. This should not be your public IP address because the public IP address usually points at your router, modem, or similar device. The internal IP address is the IP used locally by the computer. It can be determined by doing the following:

1. Open a command prompt (cmd.exe).
2. Run ipconfig.
3. The IP address is listed as the IPv4 Address.




### 23.2 SSL Certificates

After you have configured a DNS hostname for your primary server, you can now install an SSL certificate.

#### 23.2.1 What an SSL Certificate Does

SSL certificates are small data files that digitally bind a cryptographic key to an organization's information. When installed on a server, an SSL certificate allows secure connections from the server to a browser or other program and protects sensitive information.

A common use for SSL certificates is to enable a web server to provide a secure connection with a web browser (i.e. an https:// connection instead of an http:// connection).

### 23.2.2 Obtain an SSL Certificate

SSL certificates need to be issued from either a trusted certificate authority or from an accredited domain registrar.

Browsers, operating systems, and mobile devices maintain lists of trusted certificate authority root certificates, which must be present on a computer for it to trust the certificate.

The following is a list of popular certificate authorities from which you can obtain an SSL certificate:

- Comodo
- IdenTrust
- GoDaddy
- GlobalSign
- Digicert
- Certum
- Entrust

Go to ICANN for a complete list of accredited domain registrars.

Because SAFR uses Apache as its web server, request SSL certificate files for Apache web server. You will receive the following three files SAFR uses to configure the Apache web server:

- **Key**: This is your key file and should not be shared publicly.
- **Certificate**: The SSL certificate for your domain.
- **Ca_bundle**: Signer root/intermediate certificate. This file is optional; it's not always provided by the SSL certificate provider.

**Note:** Self-signed certificates do not work.

### 23.2.3 Provision SSL Certificates for your Primary Server

Do the following to configure Apache to serve the request over HTTPS:

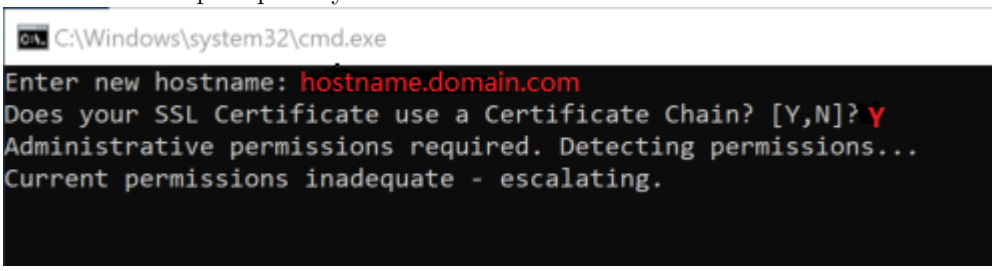
1. Log in to your primary server.
2. It is recommended that you make a backup of the default SSL files and save them in case you need to perform a rollback to the earlier version.
    - On Windows, back up the following files:
        - `C:\Program Files\RealNetworks\SAFR\httpd\conf\ssl\SAFR.key`
        - `C:\Program Files\RealNetworks\SAFR\httpd\conf\ssl\SAFR.crt`
3. Upload the certificate-related files to the SSL certificate folder:
    - SSLCertificateFile – Certificate CRT
    - SSLCertificateKeyFile – `Private.a` key file
4. Change the names of the following files:
    - Rename *_certificate.crt to SAFR.crt
    - Rename *_private.key to SAFR.key
5. If your certificate authority provided an intermediate certificate chain, do the following:
    1. Save your SSL intermediate certificate chain file to the following location:
        - **On Windows**:
            - `C:\Program Files\RealNetworks\SAFR\httpd\conf\ssl\SAFR-ca.crt`
    2. Check the `SAFR-ssl-cert.inc` file to connect your SSL certificate to the certificate chain.
        - **On Windows**:
            - `C:\Program Files\RealNetworks\SAFR\httpd\conf\ssl\SAFR-ca.crt`
            - `#Define ssl_certificate_chain_file "conf/ssl/SAFR-ca.crt"`

- Certificate file mappings

| Certificate file | Certificate file in SAFR |
|---|---|
| *.domainname.key | SAFR.key |
| .domainname_chain.crt | SAFR-ca.crt |
| .domainname_public.crt | SAFR.crt |

6. Run the SAFR **reconfigure** script, as described below.

   - **On Windows**:
     - Enter this command: `"C:\Program Files\RealNetworks\SAFR\bin\reconfigure.bat"`
     - Enter the hostname and click **Yes** when prompted if your SSL certificate uses a certificate chain.
     - Click **Yes** when prompted by *User Account Control*.




   See SAFR Support Tools and Scripts for more information about this script.

7. Verify that your services are running and your SSL certificate is properly installed by opening a browser and opening `https://hostname.domain.com:8085/health`. (Replace hostname.domain.com with your hostname and domain.)

   You should receive the following message:

```
{ "status" : "up" }
```

## 23.3 Troubleshoot

**Database Service Down**

**Problem**: You receive an error report saying Database (MongoDB) Service Down when you run the **check** command after you install SSL.

**Solution**: The cause may be that the DNS hostname IP is different from the IP when you installed SAFR without SSL installed.

Use the following workaround:

Add the following line to your primary server /etc/hosts file: `127.0.0.1 hostname.domain.com`

# 24 SAFR Support Tools and Scripts

The SAFR Platform installation includes several scripts to manage and monitor your server. They are located in the bin folder under the SAFR Platform installation location.

- On Windows: `C:\Program Files\RealNetworks\SAFR\bin`

**Note**: Some of the scripts below may not work if you're accessing the SAFR Platform through the NVIDIA Metropolis Application Framework (MAF).

## 24.1 Tools

### 24.1.1 check

Use the **check** command to check the status of SAFR Server services.

- On Windows, run `"C:\Program Files\RealNetworks\SAFR\bin\check.bat"`

### 24.1.2 configure-ports

Use the **configure-ports** command to customize the ports SAFR services listen on. This is typically done only if there is a conflict with existing software on the same server.

If port conflicts are detected during SAFR Platform installation, the following occurs:

1. The ports in conflict are reported.
2. Notepad is launched to edit safrports.conf
3. The SAFR Platform installer is automatically relaunched after new non-conflicting ports are chosen.

This command is executed as part of the installation when appropriate, so it does not need to be executed manually unless you are changing the port settings after installation.

This command takes no arguments but relies on the safrports.conf file to determine what ports are to be used.

safrports.conf is located at the following locations:

- On Windows: `C:\Program Files\RealNetworks\SAFR\safrports.conf`

### 24.1.3 reconfigure

Use the **reconfigure** command to configure the hostname used by the SAFR Server. Run this command when configuring the server to use a DNS hostname with an SSL certificate.

This command can be run with arguments specifying the hostname and whether an SSL certificate chain is used by your SSL certificate. If no arguments are passed, you will be prompted for those values.

This command requires administrator privileges. It automatically asks for admin privileges on Windows and requires `sudo` on macOS and Linux.

- On Windows, run `"C:\Program Files\RealNetworks\SAFR\bin\reconfigure.bat"`

*Examples:*

**Windows:**

- `"C:\Program Files\RealNetworks\SAFR\bin\reconfigure.bat"`
- `"C:\Program Files\RealNetworks\SAFR\bin\reconfigure.bat" safr.example.com y`

### 24.1.4 start

Use the **start** command to start up the SAFR Server. It starts all server services on the current machine.

- On Windows, run `"C:\Program Files\RealNetworks\SAFR\bin\start.bat"`

### 24.1.5 stop

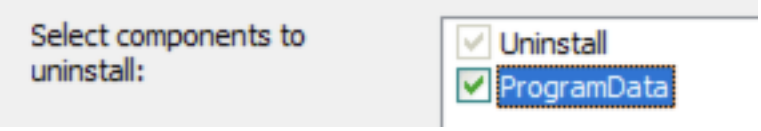
Use the **stop** command to shut down the SAFR Server. It stops all server services on the current machine.

- On Windows, run `"C:\Program Files\RealNetworks\SAFR\bin\stop.bat"`

### 24.1.6 uninstall

Use the **uninstall** command to remove the SAFR Platform entirely. This closes all SAFR applications, stops all SAFR services, and then removes all SAFR services and data.

On Windows, you must select the optional ProgramData component to remove the config files, logs, and database files.




- On Windows, run `"C:\Program Files\RealNetworks\SAFR\bin\uninstall.exe"`

# 25 SAFR Server Backup and Restore

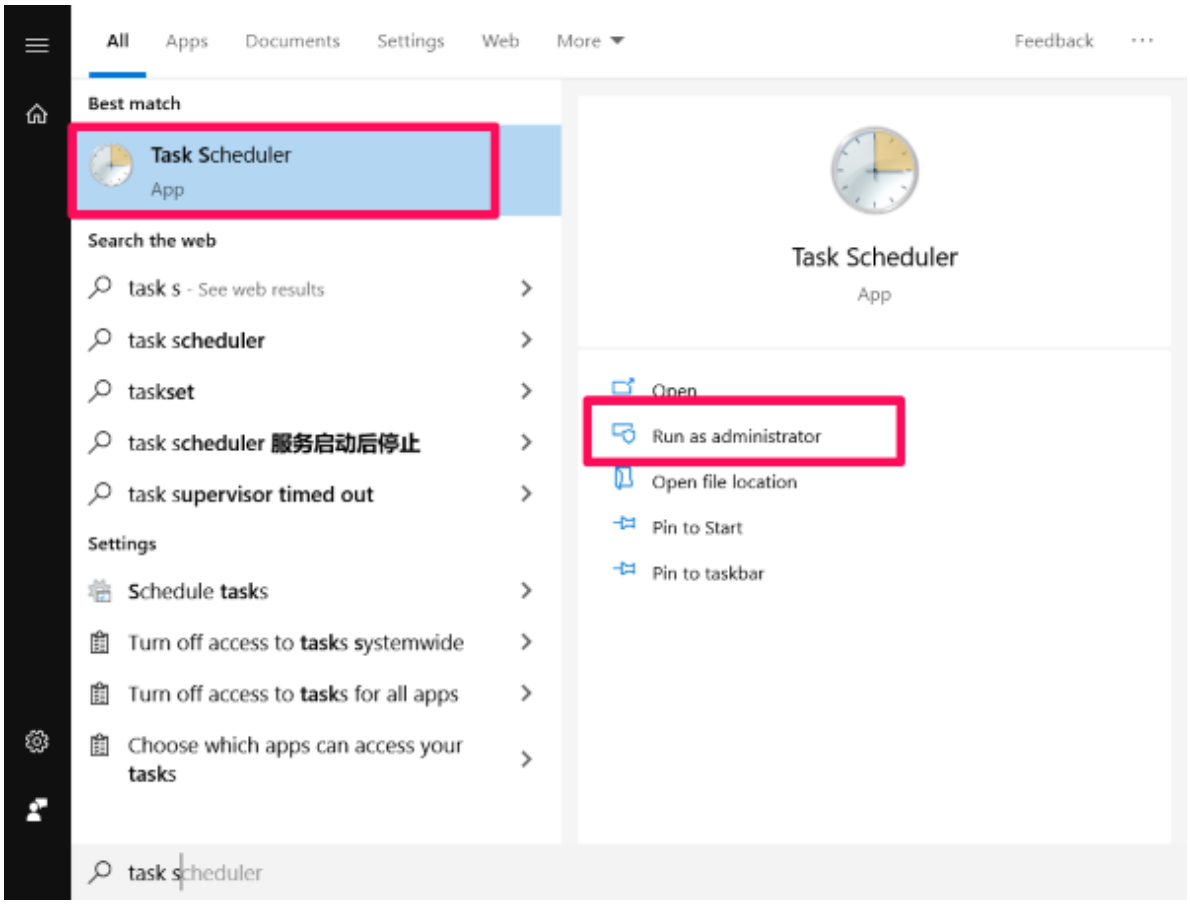
The backup process backs up and restores the entire SAFR Server, including the various databases, configuration files, images, and objects.

## 25.1 On Windows

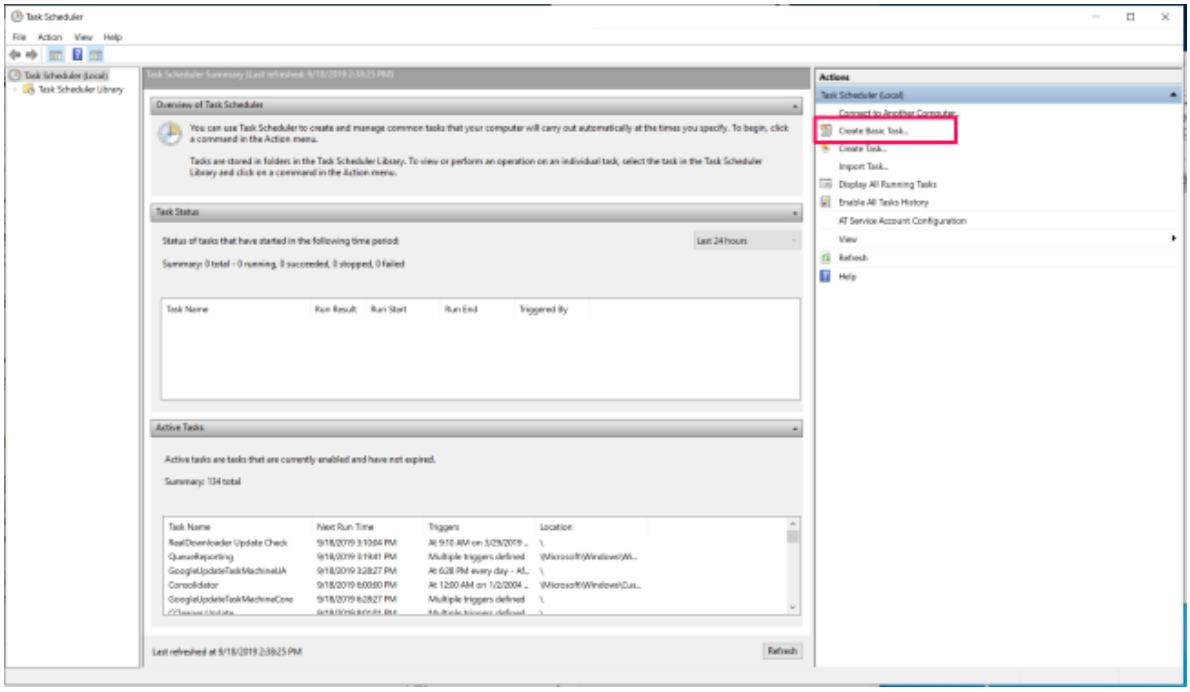
### 25.1.1 Backup

To use the *Windows Task Scheduler* to create a daily database backup, do the following:

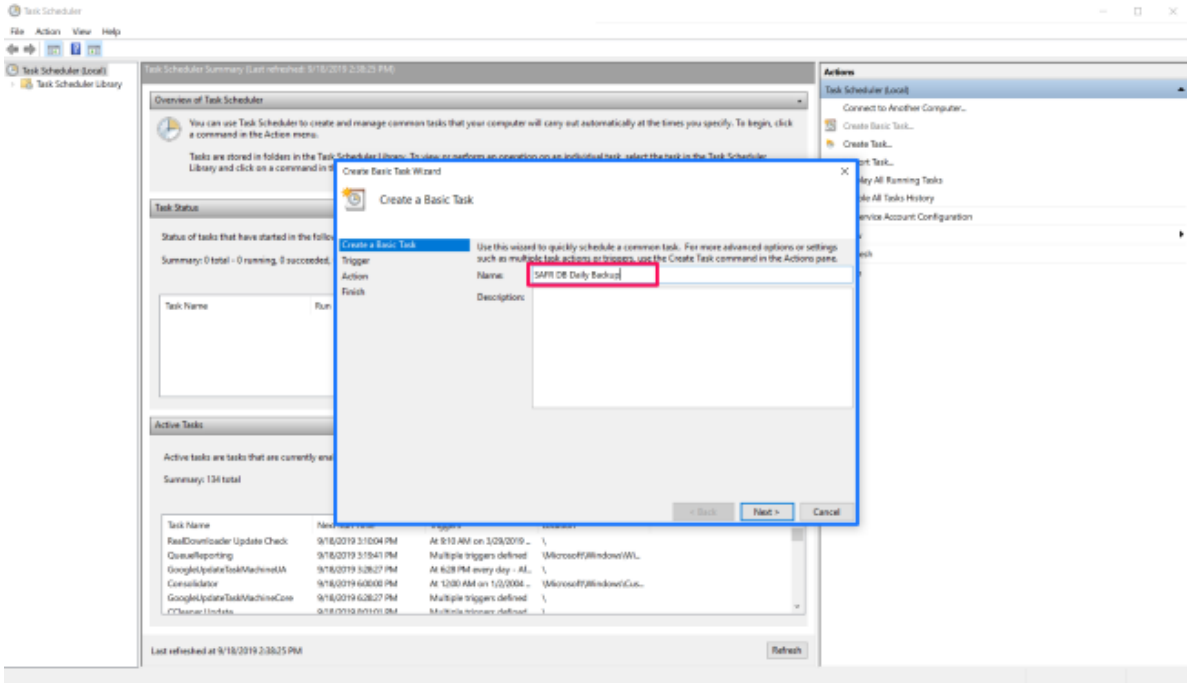
1. Run the *Windows Task Scheduler* as an administrator. The *Task Scheduler* window will be displayed.



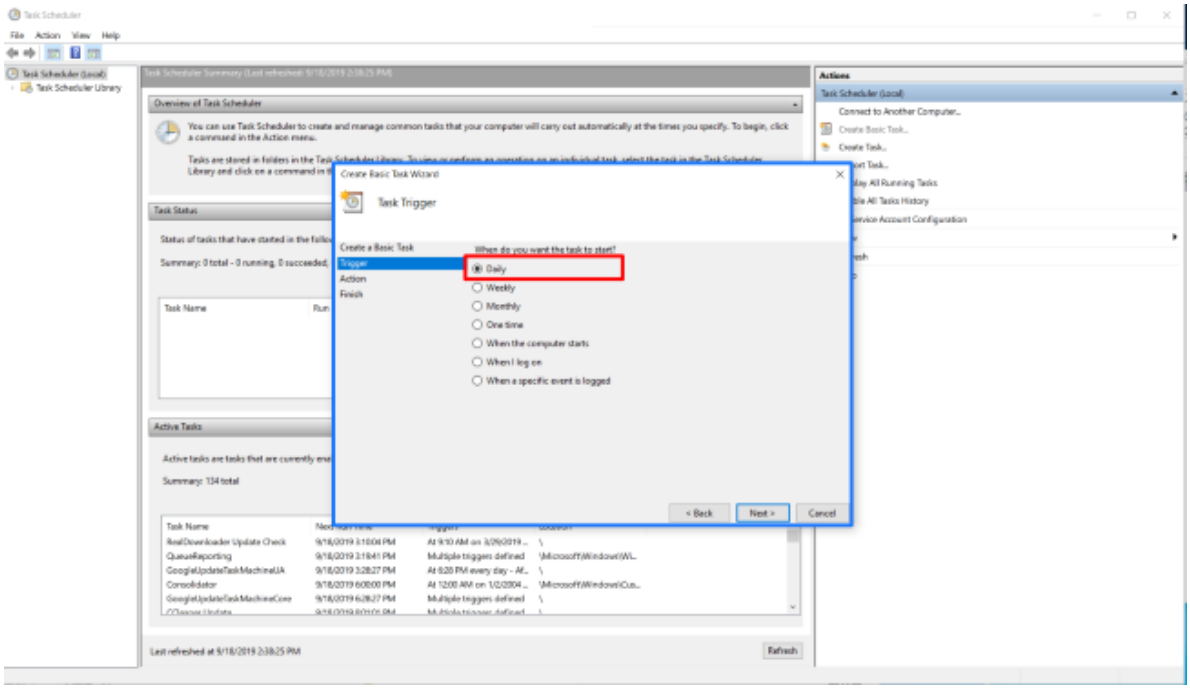

2. In the **Actions** pane, click **Create Basic Task**.



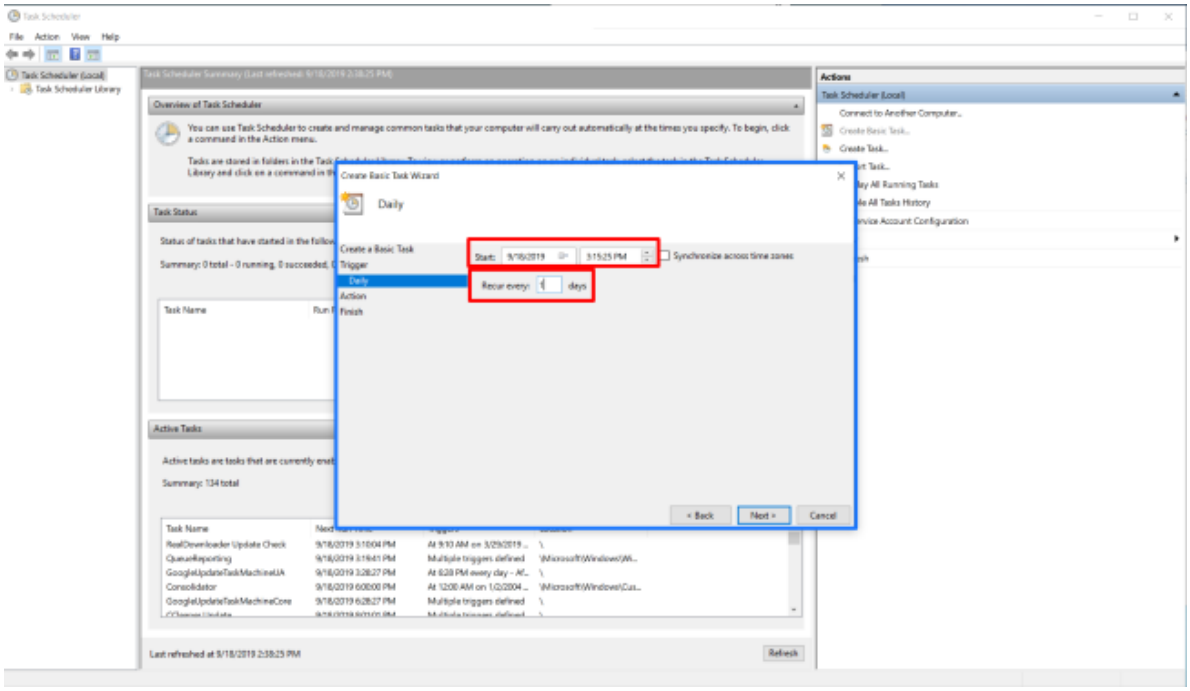
3. In the wizard's **Name** field, provide a name for the task. (e.g. *SAFR DB Daily Backup*) Click **Next**.



4. Under **Task Trigger**, select the **Daily** option, and click **Next**.



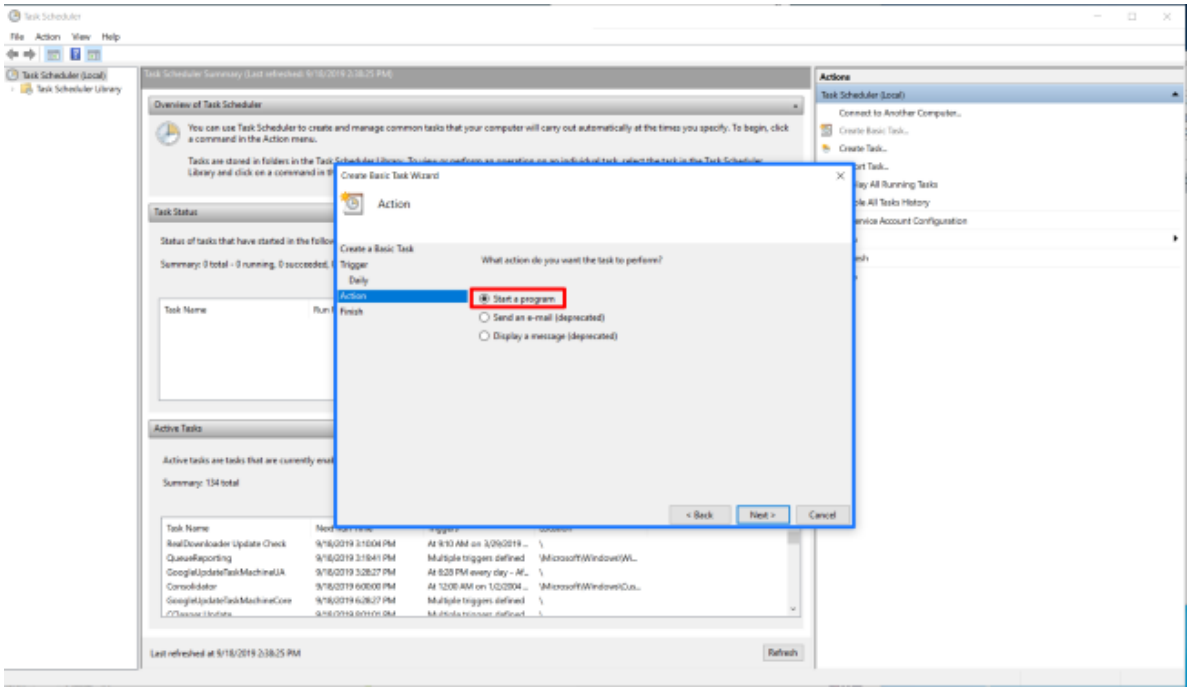

5. Set the date and time for when you want the task to run, and enter 1 in the **Recur** field. Click **Next**.



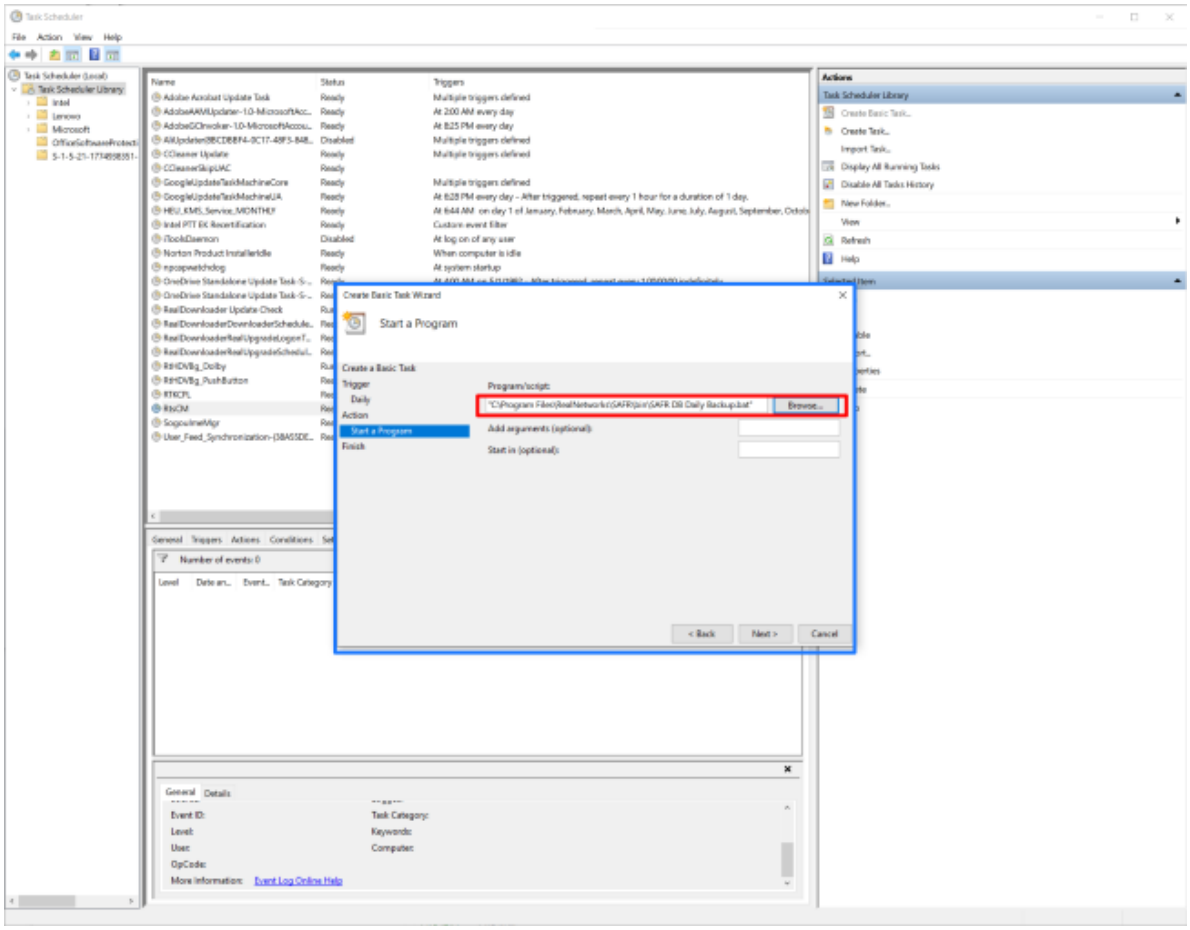

6. Using a text editor, create a .bat file called *SAFR DB Daily Backup*. Edit the .bat file, add the following commands, and thensave the file.

```
@echo off
cd C:\Program Files\RealNetworks\SAFR\bin
start python backup.py
```

7. Under **Action**, select the **Start a Program** option, and click **Next**.

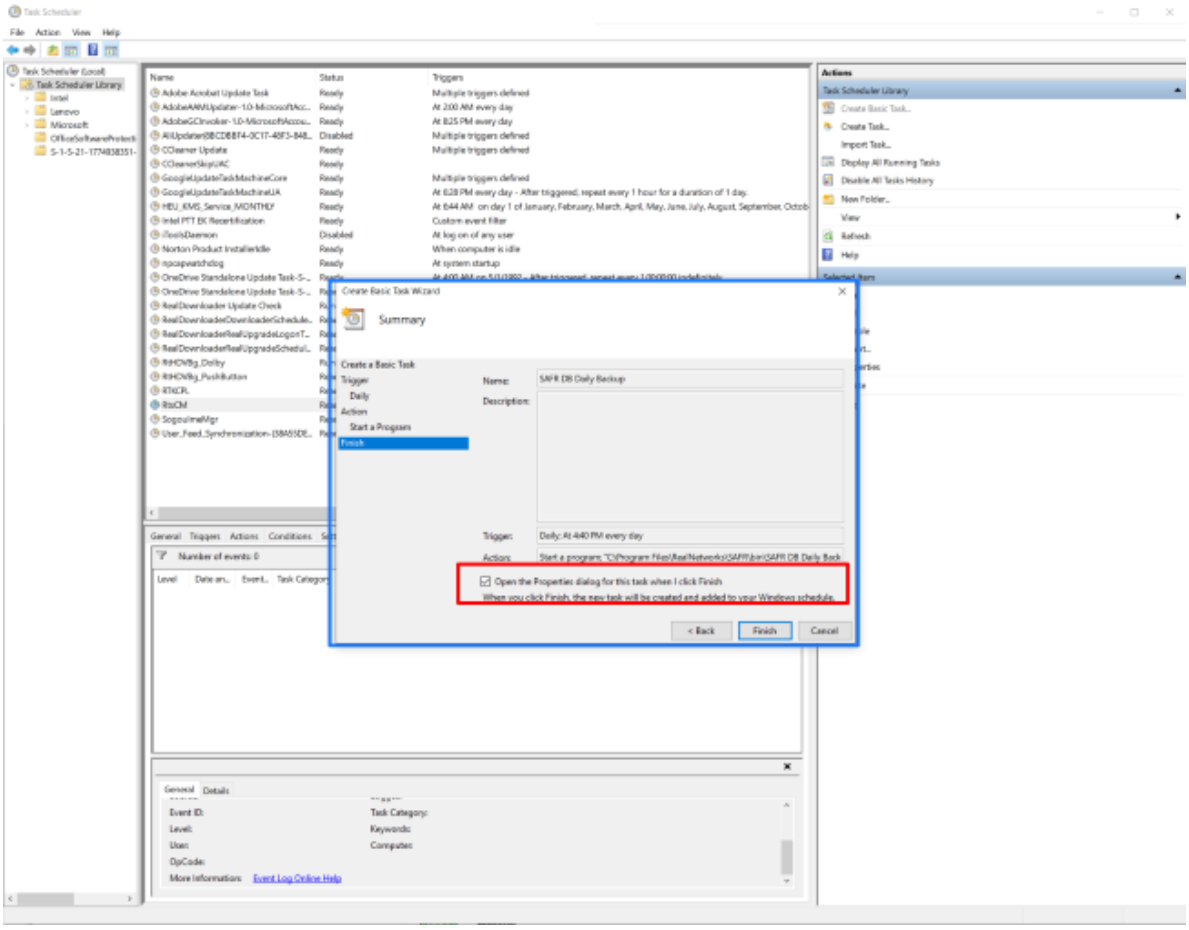



8. Click **Browse** and select the *SAFR DB Daily Backup.bat* file you created in Step 6. Click **Next**.

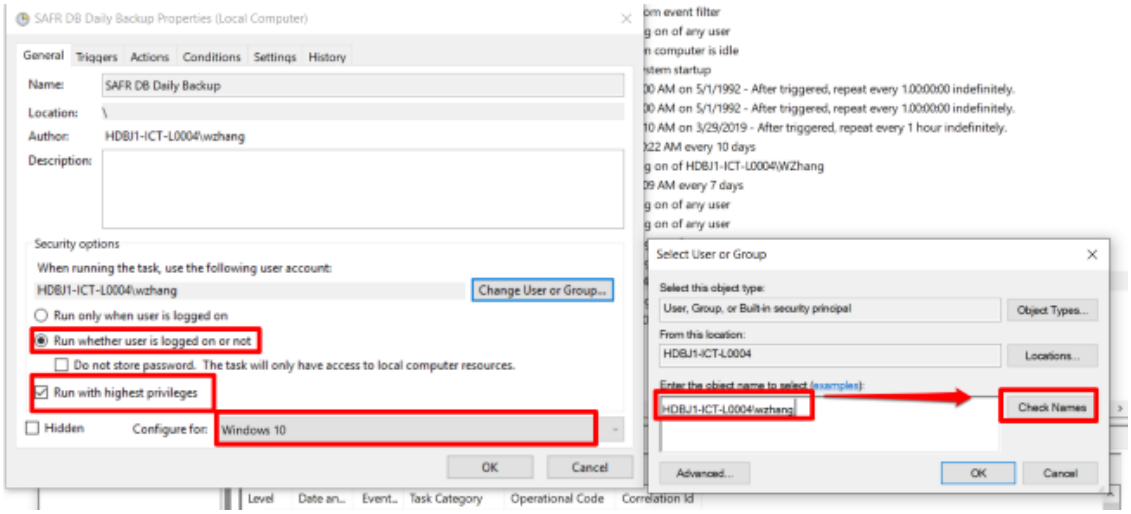



9. Under **Summary**, select **Open the Properties dialog for this task when I click Finish**, and

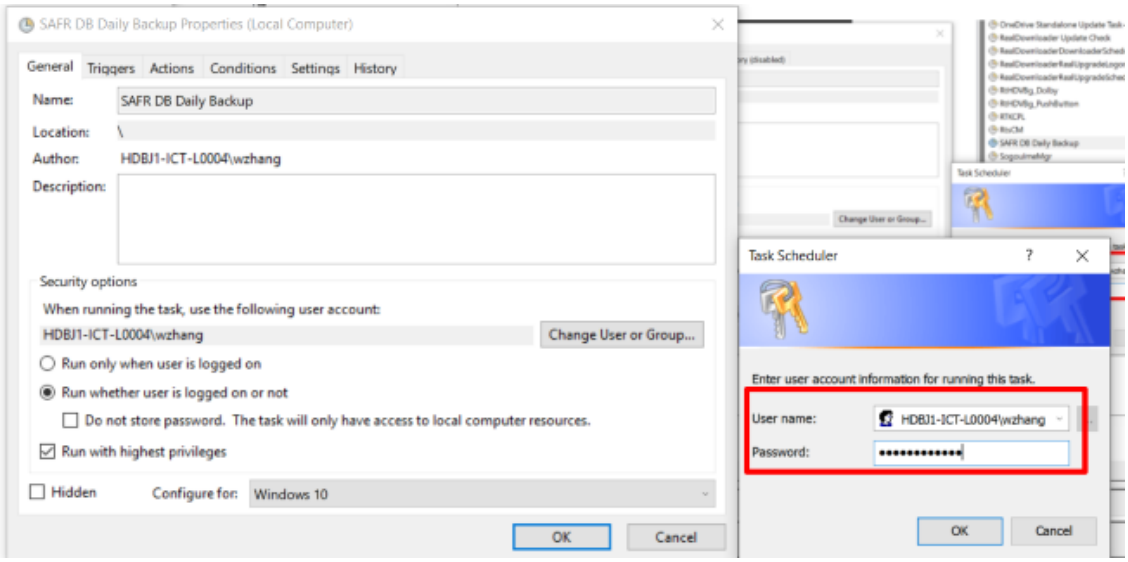
click **Finish**.




10. In **Properties**, do the following:
    1. Select the **Run whether user is logged on or not** option.
    2. Select the **Run with highest privileges** option.
    3. Click **Change User or Groups**.
    4. Enter the object name to select in the field. (e.g. DB-USERMACHINE-T/username) Click **Check Name** and click **OK**.




5. Enter your username and password and click **OK**.




Once this procedure is completed, you can find the task in the *Task Scheduler Library*. Check **History** to view the task events. You can find the daily backup file in the path shown in the *SAFR DB Daily Backup.bat* file.

### 25.1.2 Restore

**command path:** `C:\Program Files\RealNetworks\SAFR\bin`

**run command:** `python restore.py BACKUPFILENAME`

- Example: `python restore.py "C:\Program Files\RealNetworks\SAFR\backups\SAFR-backup-20190814-003342.`

Press Y when asked, "Are you sure? (Yy/Nn)"

You'll receive the following message when the restore is complete:

- `SAFR Restore Complete.`

# 26 SAFR Platform Command Line Install Options

Silent installation of the SAFR Platform on Windows can be achieved by invoking the SAFR Platform installer via the command line and using the `/S` switch.

**Example**:

```
SAFRPlatform_win_1_8_302_08_13_19.exe /S
```

The Windows SAFR Platform installer provides several options for configuring the component selection during install. Each component can be disabled or enabled by using the following syntax:

- `SAFRPlatform_win_1_8_302_08_13_19.exe /S /COMPONENT=YES`
- `SAFRPlatform_win_1_8_302_08_13_19.exe /S /COMPONENT=NO`

**Examples**:

```
SAFRPlatform_win_1_8_302_08_13_19.exe /S /VIRGO=YES /Actions=NO

SAFRPlatform_win_1_8_302_08_13_19.exe /Age=YES /Gender=YES /Sentiment=YES
```

## 26.1 Command Line Install Options

| Feature Type | Component | Flag | Default | Notes |
|---|---|---|---|---|
| Silent Install | Silent Install | /S | Disabled | |
| Component | SAFR Actions | /Actions | Enabled | |
| Component | Desktop Client | /Application | Enabled | |
| Component | Web Console | /Console | Enabled | |
| Component | SAFR Reports | /Reports | Enabled | |
| Component | SAFR Logs | /Logs | Enabled | |
| Component | VIRGA | /VIRGA | Enabled | |
| Component | VIRGO | /VIRGO | Enabled | |
| Component | GPU Accelerated Recognition (HTFS) | /GPUFaceService | Enabled | Only enabled by default if NVIDIA Drivers greater than 418.67 are detected. |
| Face Service Model | Age Model | /Age | Enabled | |
| Face Service Model | Gender Model | /Gender | Enabled | |
| Face Service Model | Sentiment Model | /Sentiment | Enabled | |
| Face Service Model | Occlusion Model | /Occlusion | Enabled | |
| Face Service Model | Optimize GPU Models during installation | /OptimizeModels | Enabled | |
| VMS Integration Plugin | Avigilon Plugin | /Avigilon | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |

| Feature Type | Component | Flag | Default | Notes |
|---|---|---|---|---|
| VMS Integration Plugin | Digifort Plugin | /Digifort | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |
| VMS Integration Plugin | Genetec Plugin | /Genetec | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |
| VMS Integration Plugin | GenetecFR Plugin | /GenetecFR | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |
| VMS Integration Plugin | Milestone Plugin | /Milestone | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |
| Camera Extension | Ximea Camera Extension | /Ximea | Disabled | |
| Installation Location | Installation Location | /D | `C:\Program Files\RealNetworks\SAFR` | Must be the last command line argument. Do not use quotes. |

# 27 Video Recognition Gateway (VIRGO)

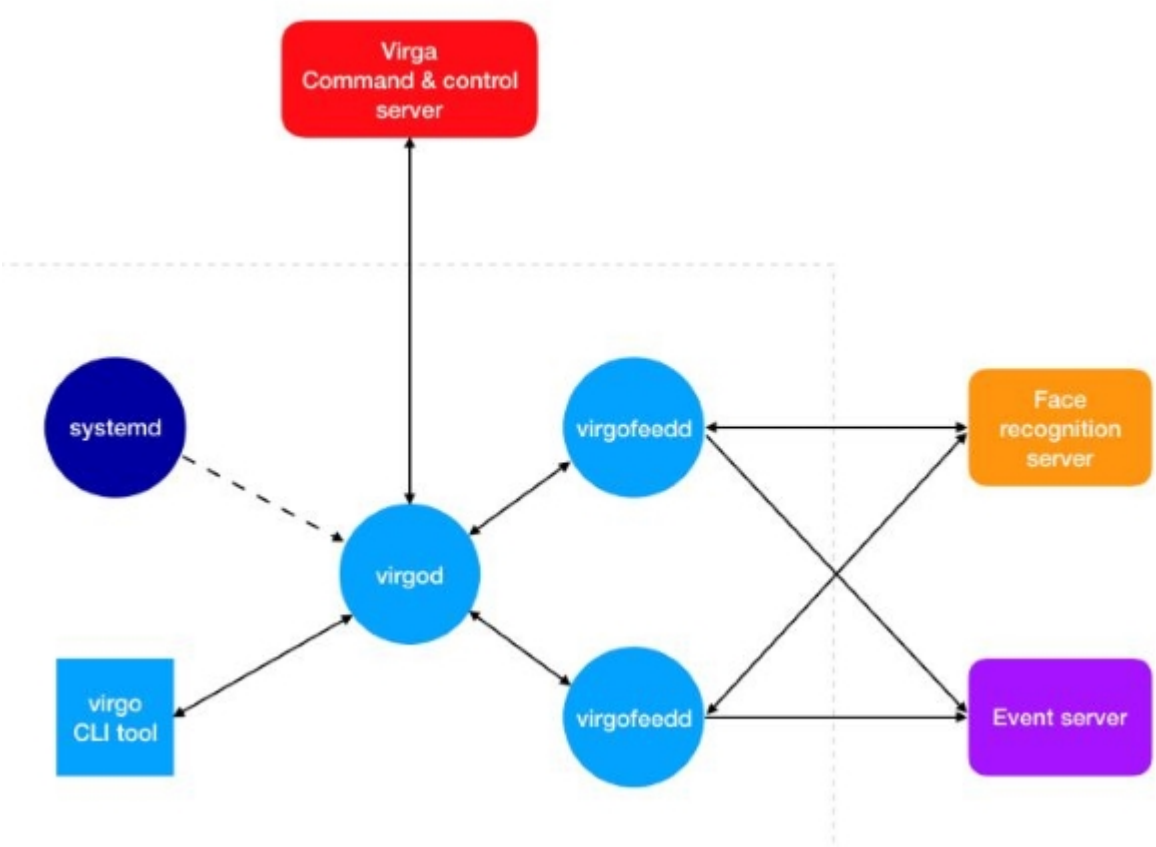
VIRGO (Video Recognition Gateway) is a daemon system which runs on a POSIX compatible system. It receives video feeds from one or more cameras and recognizes and tracks faces in those video streams in realtime. It generates tracking events and sends those events to an event server. The VIRGO daemon can be controlled either by the command line tool or through the VIRGA command & control server.

## 27.1 Architecture

A single VIRGO installation consists of the following components:

- **virgod**: The VIRGO control daemon. One such daemon is spawned and maintained per VIRGO hardware.
- **virgofeedd**: A *virgod* child process which handles a single video feed.
- **virgo**: The locally available VIRGO command line tool which acts as a Command Line Interface (CLI)-based user interface to the VIRGO daemon.

This diagram shows how those components fit together:




**virgod**:

- Spawned by the operating system systemd/launchd service. The daemon is automatically restarted by the OS if the hardware power cycles or virgod terminates for some unexpected reason.
- Runs as its own user. The VIRGO user is limited to read/write access to the "virgo" home directory.
- The VIRGO user home directory contains just the ~/Library directory which is the place where libFoundation (used in the implementation of VIRGO) stores the daemon settings.
- Is responsible for spawning the per-video-feed child processes: virgofeedd.

- *virgod* monitors each *virgofeedd* child process that it has spawned and it automatically restarts a *virgofeedd* if it unexpectedly terminates for some reason. (e.g. it ran out of memory)
- Is responsible for caring out all the necessary steps for an update to the VIRGO daemon system.
- Is the only process on the machine which talks to the VIRGA command & control server.
- carries out any command sent by VIRGO to *virgod*.
- regularly informs VIRGA about the current status of *virgod*.

**virgofeedd**:

- Spawned by *virgod*.
- Runs as the same user as *virgod*.
- Receives a video stream. Detects and recognizes faces in that video stream, generates events and reports them to the event server.
- Receives commands from *virgod*.

**virgoupdaterd**:

- Spawned by *virgod* after it has received an update request.
- Runs as the same user as *virgod*.
- Downloads the update archive, extracts it, installs the update bundle, and saves the current persistent *virgod* state.
- Restarts *virgod*. (*virgod* takes care of data migration.)
- Monitors *virgod* after restart and rolls back to the previous *virgod* version if the new *virgod* fails to startup or fails to check back in with a commit message in less than a couple seconds.
- Once the update has finished, the updater exits.

**virgo**:

- Implements the local (CLI-based) user interface to *virgod*.
- Offers commands to show the current status, select the cloud environment, get a screen capture from a feed, etc.

## 27.2 VIRGO Bundle (File System Layout)

VIRGO ships as a bundle which supports multiple versions of the VIRGO daemon. The VIRGO bundle directory contains a "versions" directory which in turn contains one sub-directory per installed VIRGO version. The name of a version sub-directory is the semantic version number of the VIRGO installation. The "versions" directory also contains a symlink named "current". This symlink points to the version sub-directory which is currently active.

The version sub-directory stores all necessary executable, library, and data files for the VIRGO version.

VIRGO bundle layout:

```
virgo/
   versions/
      1.0.0/
         virgo
         virgod
         virgofeedd
         virgoupdaterd
         lib/
            <shared libraries>
         model/
            <tensor flow model files>
         virgo-factory.config
      current -> ./1.0.0
   virgo -> ./versions/current/virgo
```

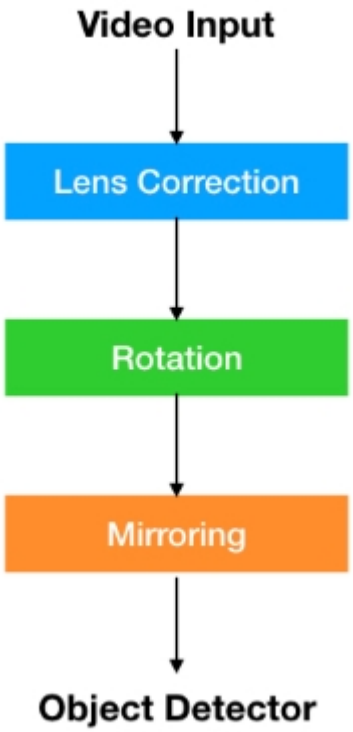
## 27.3 VIRGO Feeds

A single *virgod* instance manages a set of feeds. Each feed represents a video stream from a camera, a file, or some other video source. Each feed is associated with a set of configuration information which is stored persistently by VIRGO. The configuration information for the feeds is either provided by the VIRGO server through the COP-HTTP protocol or through the VIRGO command line tool and the COP-DTP protocol.

Each feed has a name which is unique among the set of feeds of a single *virgod* instance. These names are used as a simple and convenient way to refer to a feed and its configuration. Each feed is managed by a separate *virgofeedd* instance which is started and monitored by *virgod*. *Virgod* will automatically restart a *virgofeedd* instance if it dies for some unexpected reason.

A feed may be enabled or disabled. Only enabled feeds are associated with a *virgofeedd* instance. The enabled state of a feed may be changed through the VIRGO command line tool by issuing a **feed start** or a **feed stop** command. A feed may also be enabled or disabled through the COP-HTTP protocol by changing the **enabled** setting in the feed configuration dictionary. This allows the system to reclaim resources like memory and network bandwidth if a feed is temporarily not needed. Feeds which are no longer needed at all should be removed altogether.

A feed has an input which connects the feed to a video stream. The only type of input currently supported is "stream". A stream input is specified by a URL which may point to a publicly accessible RTSP, HTTP, or FILE video stream. Each video frame from the input is first sent through a video post-processing pipeline before it is fed into the object detector and recognizer sub-systems:




First a lens correction algorithm is applied to an incoming video frame. This step removes distortions that may be introduced by the optical system of a camera. After that the image will be rotated to compensate for any undesired rotation that may have been introduced by the physical orientation of the camera. Finally the image may be mirrored to ensure that a camera that is facing a user will produce an image that aligns with what a user expects to see.

# 28 VIRGO for Windows

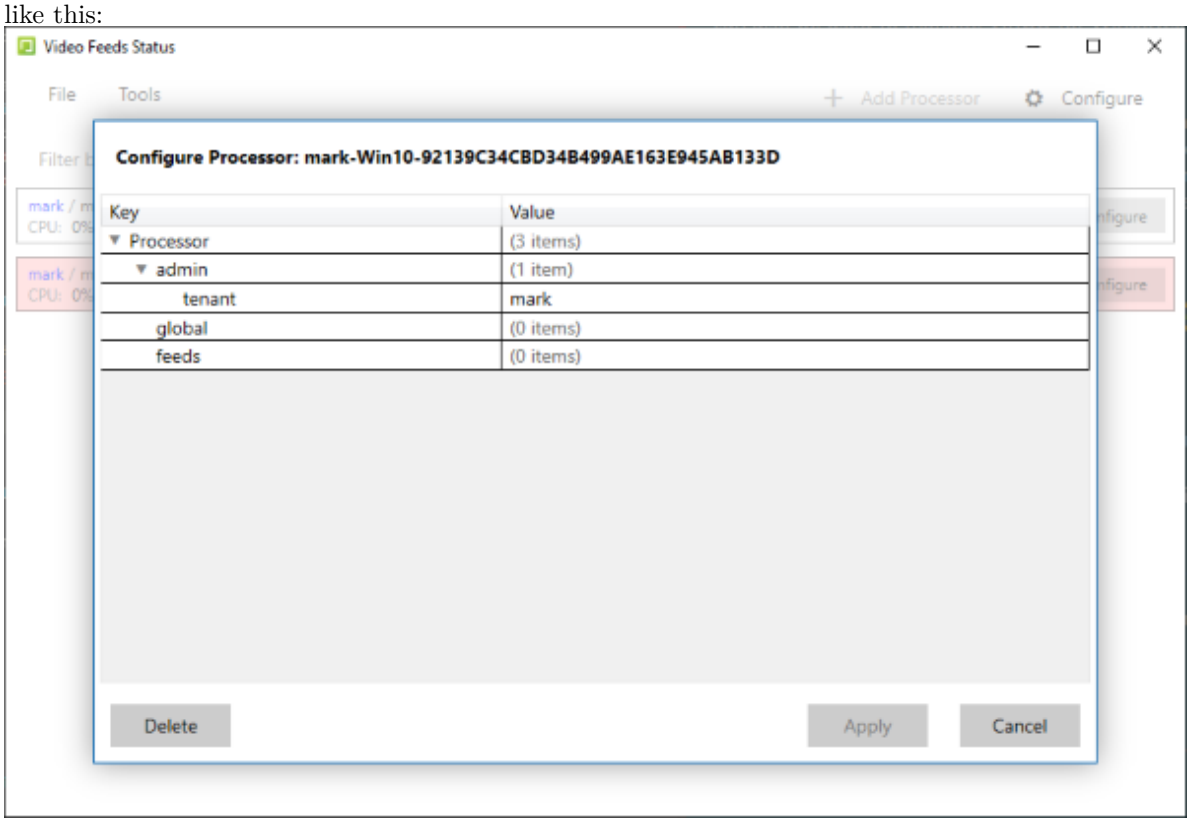
A modified version of VIRGO has been implemented for use with Windows machines. VIRGO for Windows has been designed to be managed by the Windows Desktop client, although the Web Console can also be used to manage VIRGO for Windows. Unlike regular VIRGO, VIRGO for Windows can't be managed by VIRGA, as VIRGA doesn't run on Windows.

Using VIRGO for Windows, a VIRGO daemon can be created and attached to any camera feed currently connected to the Windows Desktop client. Attaching a VIRGO daemon allows you to monitor the video feed even if the Desktop client is closed. (If you don't create and attach a VIRGO daemon to the camera feed, then the camera feed stops being monitored when the Desktop client is shut down.) Note that using the VIRGO daemon to monitor the video feed uses slightly more resources than using the Desktop client to monitor it.

## 28.1 Create a VIRGO Daemon

To create a VIRGO daemon, do the following:

1. Connect a camera to your SAFR system, then connect a video feed to your Desktop client, as described here.
2. Within the Desktop client, go to **Tools** -> **Video Feeds Status**.
3. Click the **Configure** button on the video feed you just connected. You'll be shown a screen that looks like this:




4. When you hover your mouse over the **feeds** entry, you'll see a + button and a **-** button. Click the + button to create a VIRGO daemon. You'll be prompted for the following information:
   - **Feed Name**: Enter any name for the video feed you wish.
   - **Camera**: Select the camera from the drop-down menu that is providing the video feed.
   - **Mode**: Select the video processing mode from the drop-down menu that you want the VIRGO daemon to operate in. For a description of the video processing modes, see here.
   - **Apply Mode Customizations from Preferences**: Enable if you want the Desktop client

preferences applied to the new VIRGO daemon.

5. After you press the **Add** button, the VIRGO daemon will be created. **Note**: At this point, the VIRGO daemon exists independently of both the Desktop client and the video feed that you cloned to create the daemon.

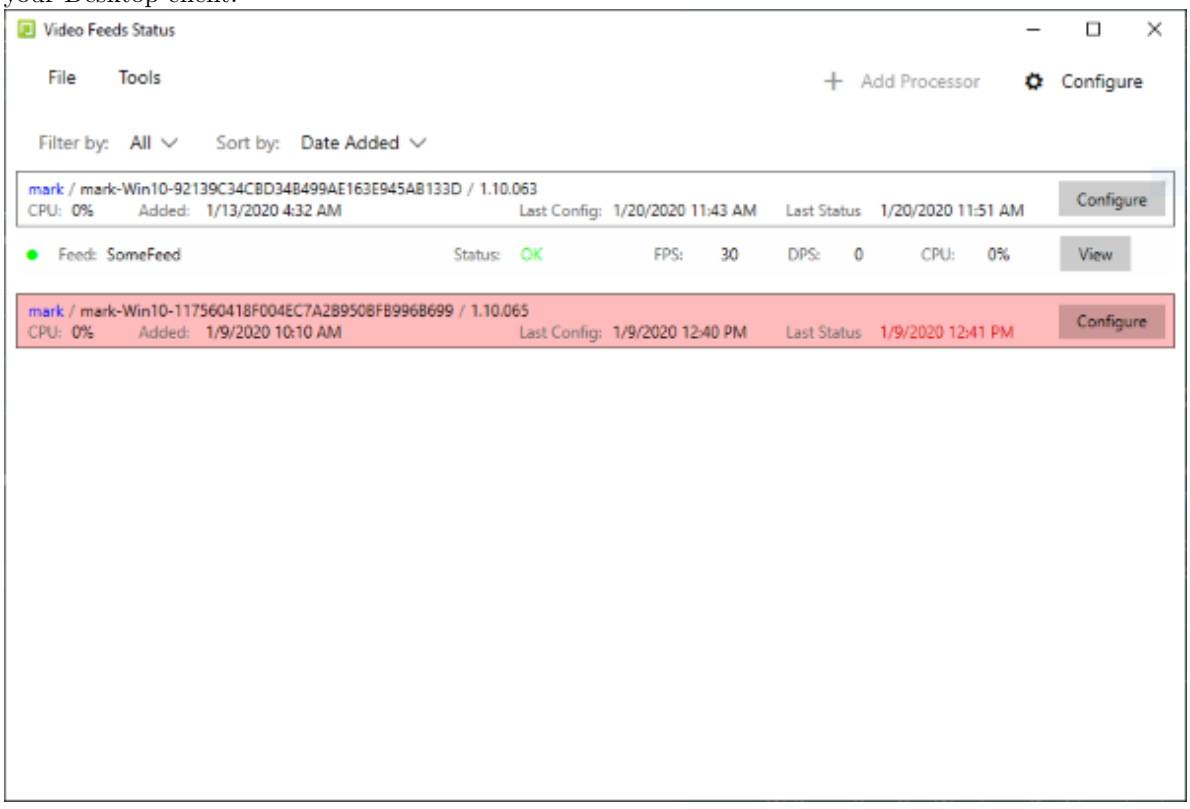
## 28.2 Manage the VIRGO Daemon

The created VIRGO daemon behaves similarly to VIRGO daemons created on macOS and Linux machines. Specifically, the following behavior patterns are true for VIRGO for Windows VIRGO daemons:

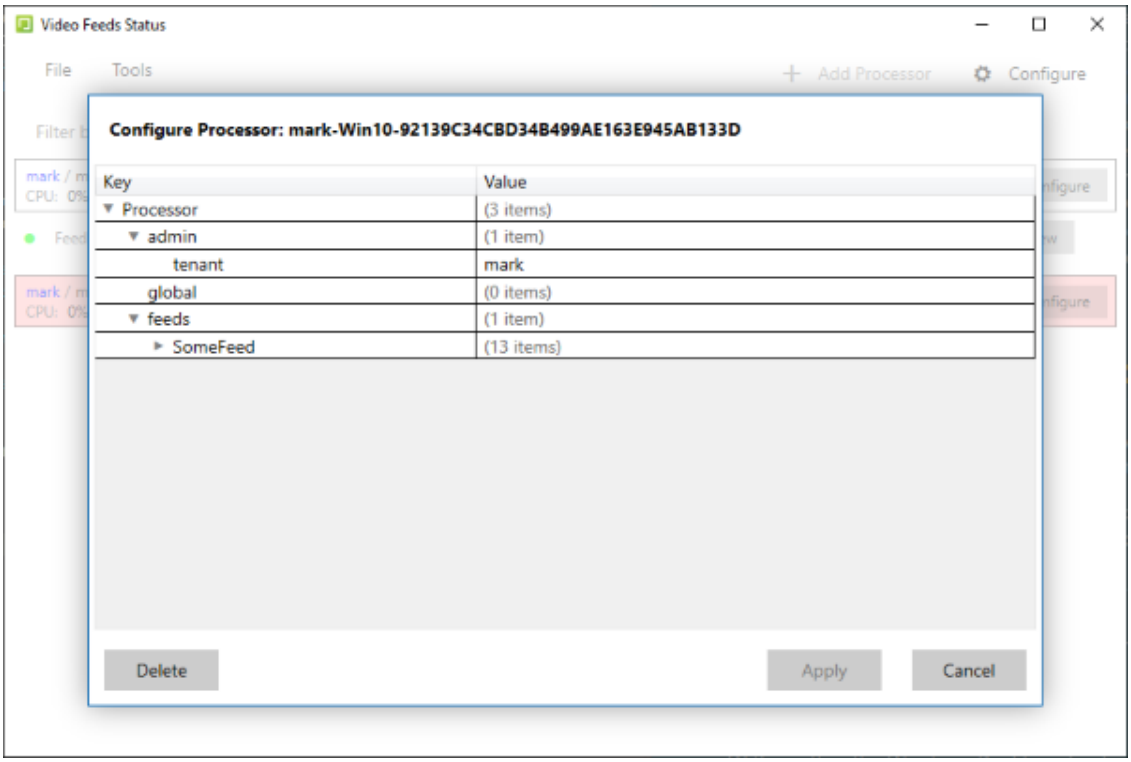
- The daemon is not affected by subsequent changes to preferences made within the Desktop client. If you change a preference within your Desktop client, that change is not cloned to the existing VIRGO daemon(s).
- Daemons continue running and processing their video feeds regardless of whether or not the Desktop client is running or not.
- If you shut down your machine, the daemon will try to restart itself whenever your machine is turned on again.

To manage the VIRGO daemon, do the following:

1. Within either the Windows Desktop client or within the Web Console, open the *Video Feeds Status* window. If you named your VIRGO daemon *SomeFeed*, you'll see a screen such as the following within your Desktop client:




2. You can view the video feed that the daemon is processing by clicking the **View** button.
3. To terminate the daemon, do the following:
    1. Click the **Configure** button. You'll see a screen that looks like this:



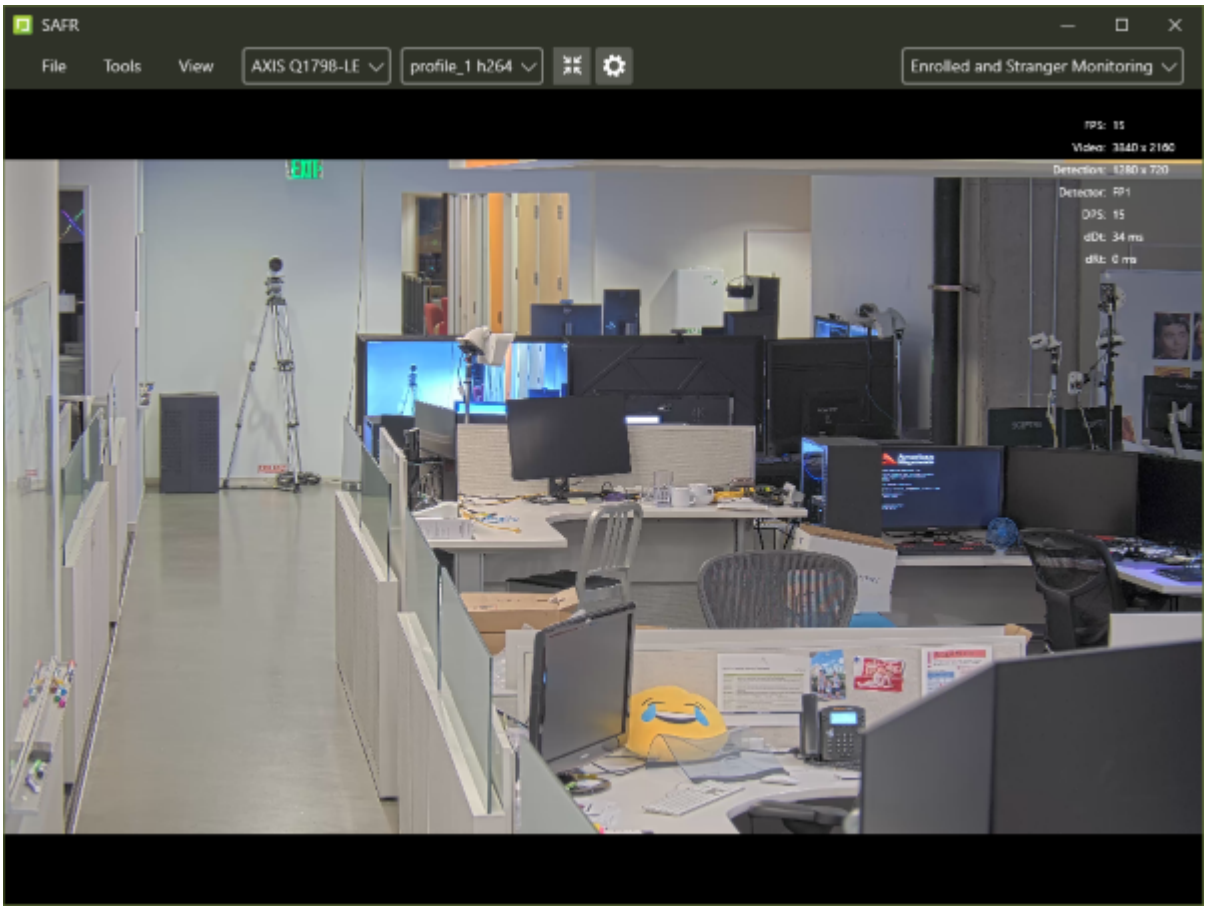

2. When you hover your mouse over the **feeds** entry, you'll see a + button and a **-** button. Click the **-** button.
3. Click the **Apply** button. At this point, the daemon will be terminated. **Note**: If you click the **Cancel** button, the daemon termination is undone and the daemon will continue operating.

# 29 Desktop Client

The Desktop client is used to add and configure cameras, monitor feeds, get alerts, and view activity. It is also used to update and manage the Identity Database. The Desktop client can be installed on additional laptops or desktops to allow administration and monitoring.

# 30 Camera Feed Analyzer

This window enables you to easily view and configure the live feeds from the cameras connected to this client. You can select any of the cameras connected to this Desktop client from the drop-down menu at the top of the window.

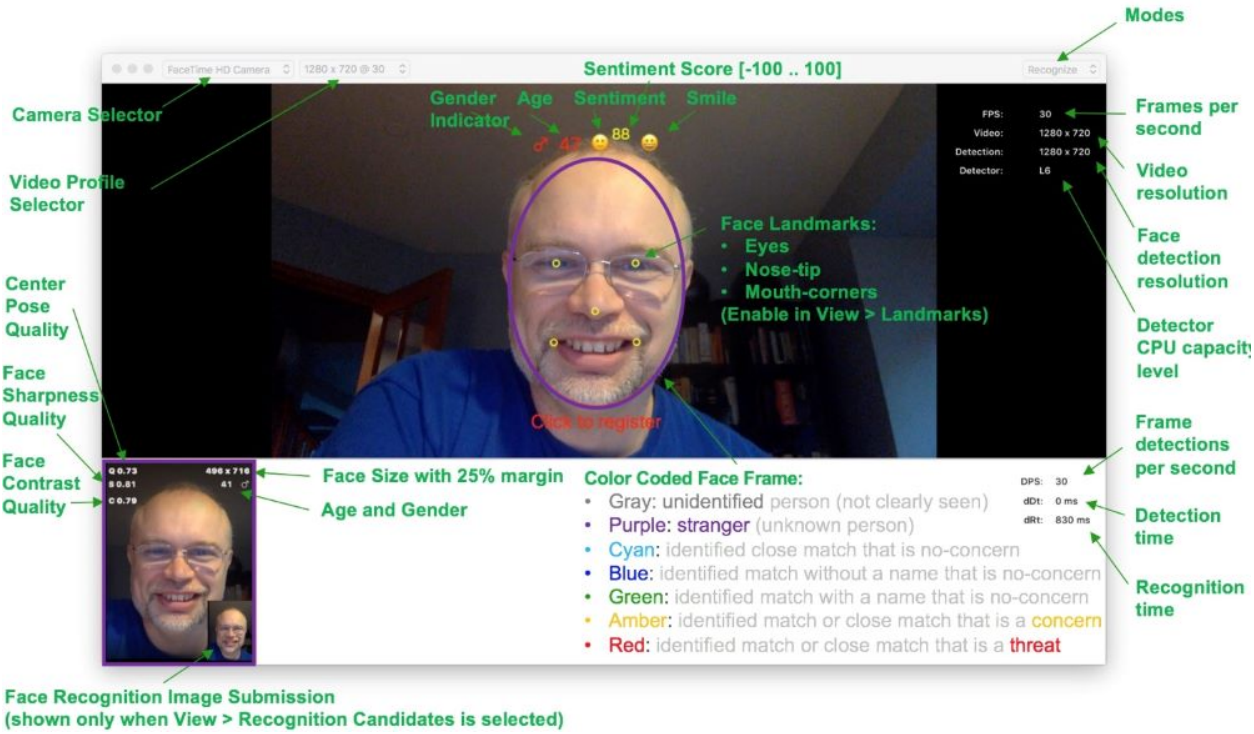


# 31 View Menu Options

You can customize the information displayed in the Desktop client's Camera Feed Analyzer by clicking on the **View** menu option when the client has the *Camera Feed Analyzer* open. The following options are available:

- **Tracking Frames:** Enables colored indicator frames overlaid around detected faces and objects. See the color codes section here for a description of what each color indicates.
- **Attributes**: Enables the the selected attributes located in the *Detect* section of the Recognition preferences tab to be displayed above the faces seen in the *Camera* window's video feed.
- **Names**: Displays the name (if known) of recognized people below their faces.
- **Full-Screen Names**: Flashes recognized people's names or badge IDs (if known) over the entire video.
- **Detection List**: Displays a row at the bottom of the screen showing detected faces. Recognition details for each face also appear.
- **Recognition Details**: Displays image quality metric values on the facial image(s) along the bottom of the *Camera* window. See Image Quality Metrics Guidance for more information about image quality metrics.
  On Windows selecting this option will automatically select the *Detection List* option (described above) as well.
- **Video**: Disables the video, causing only the overlay elements to show.
- **Performance Metrics**: Displays feed window metrics, including frames per second, video and face detection resolution, and CPU capacity level.
- **Pose Liveness State Data**: Displays pose liveness data. For more information, see Pose Liveness Detection
- **Enter full-screen**: Enables full screen mode. Ctrl-F exits full screen mode.
- **Enter lock-screen**: Enables locked mode. While in locked mode all interactive controls are disabled, except those aplicable for the current video processing mode. A lock icon is added when in full screen which can be rapidly tapped 3 times to exit locked mode. Ctrl-L exits lock screen mode.

The following depicts various information that is displayed in the feed view, whether it is live from the camera or recorded video:



# 32 Operator Console

The Operator Console window gives SAFR operators a unified UI with which to manage cameras, monitor events and activity, and view identity information.

In the screenshot below, the major panels of the console are outlined in green, while special buttons are highlighted in red. The various buttons are described in the relevant panel sections below.


## 32.1 Recent Activity Panel (Center Panel)

This panel, located in the center of the Operator Console window, displays thumbnail images of the events that your SAFR system has recently recorded. You can select which events will be displayed by selecting one of the 3 values at the upper right corner of the panel:

- **All**: All events will be displayed.
- **Recognized**: Only events triggered by people who are registered in the Person Directory will be displayed.
- **Unknown**: Only events triggered by people who aren't registered in the Person Directory will be displayed.

Hovering over an event thumbnail causes the thumbnail to be outlined. See Interpret Video Feed Overlays for information about what the different colors mean. **Note**: *Threats* and *Concerns* are always outlined in red and yellow, respectively.

Hovering over an event thumbnail usually also causes a button to appear. Clicking on the button causes one or two menu items to appear:

- **View scene**: Brings up a dialogue with a still image of the event. This item is only offered if saving scene images has been enabled for the *Person Type* that triggered the event.
- **View matched events**: Brings up a dialogue that allows you to see information about the people that triggered the event. You can also compare thumbnails to decide which image is clearer. This item

is only offered for people that are registered in your Identity Database.

## 32.2 Video Sources Panel (Left Panel)

This panel, located along the left side of the Operator Console window, displays all the video sources that are defined for your SAFR system. If a video source is associated with a VIRGO daemon, double clicking it will cause its live video feed to play in the Live Video Panel on the right of the Operator Console window.

Inactive sources are greyed out, while all the sources whose events are included in the Recent Activity Panel have a checkmark next to them. Note that you can check and uncheck sources on this window, but you must configure whether they're active or inactive elsewhere.

Sources with a yellow exclamation mark next to them are experiencing errors with at least one of the video feeds associated with it. (Although each source usually has only one video feed associated with it, it's possible to associate multiple feeds with a single source.) To troubleshoot video feed errors, do the following:

1. Hover over the source with an exclamation mark.
2. Note which video feed is experiencing the error.
3. Go to the Video Feeds Status window to get more information.

The Video Sources panel can be collapsed and expanded by clicking on the *Toggle panel* hamburger icon in the upper left corner of the Operator Console. The eye icon in the upper right of the panel expands and closes the live video panel on the far left of the Operator Console.

## 32.3 Live Video Panel (Right Panel)

This panel, located along the right side of the Operator Console Window, displays live video feeds.

**Note**: Live video feeds are only available for feeds associated with a VIRGO daemon. You can create VIRGO daemons in the Video Feeds Status Window.

You can right click on a live video to enable or disable tracking frames. Tracking frames are colored indicator frames overlaid around detected faces and objects. See the color codes section here for a description of what each color indicates.

This panel can be collapsed and expanded by clicking on the eye icon in the upper right-hand corner of the Video Sources Panel. You can view the live video feeds in their own dedicated window by clicking on the Context menu in the upper right corner of the panel, and selecting **Open panel in new window**.

## 32.4 Match Notifications (Bottom Panel)

This panel, located along the bottom of the Operator Console window, displays notifications of all the events that meet the specified levels of threat specified by the panel's Context menu in the upper right corner of the panel. By default, **Show all Threat** and **Show all Concern** are selected, while **Show all No-Concern** isn't.

The events are aggregated based on the person that triggered the event. Whenever a new event is triggered that meets the threat level criteria, that event is added to the Match Notification panel and the panel is automatically expanded. You can manually collapse or expand the panel by clicking on the panel's header bar.

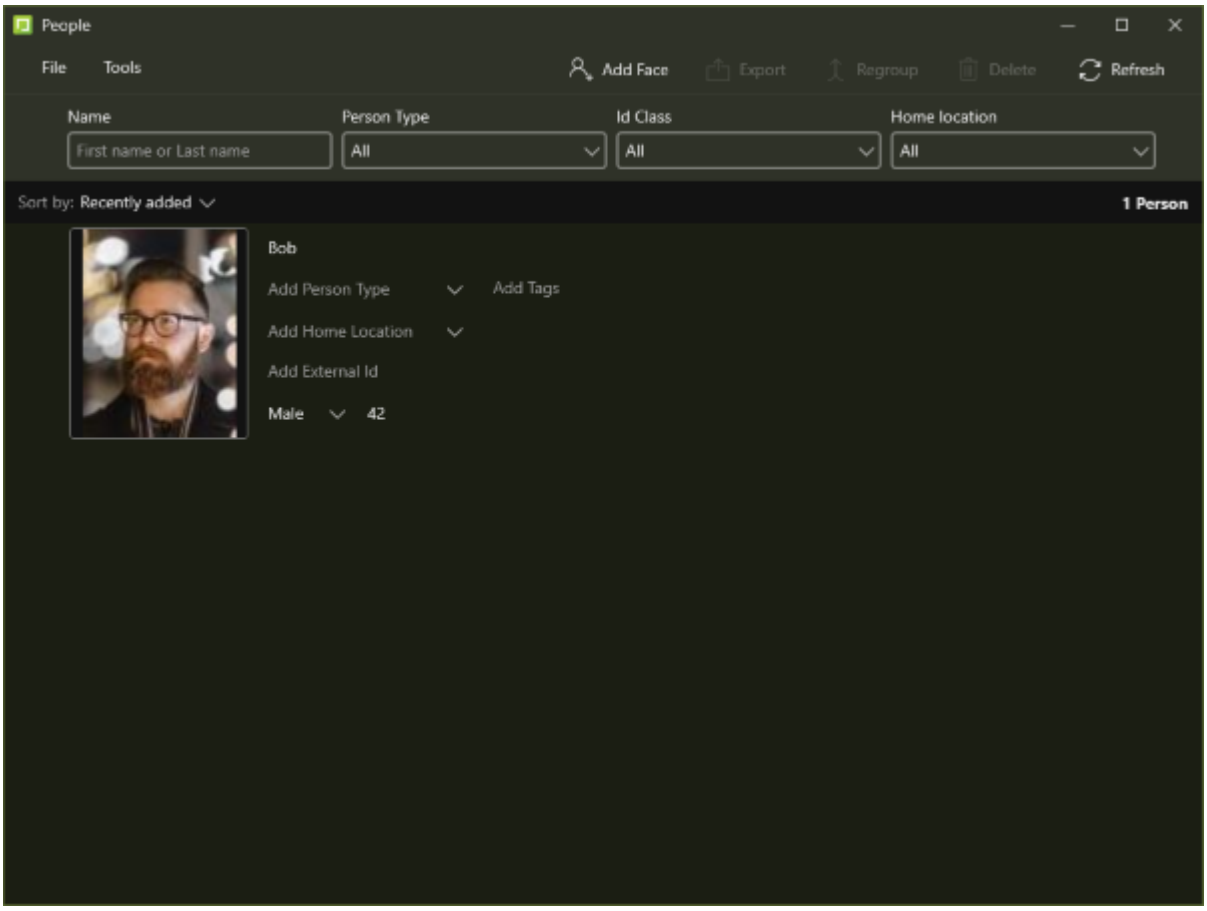
All new events are marked with a red circle in the upper left corner, so you can easily identify newly generated events. To clear the red circles, collapse the Match Notification panel.

# 33 People Window

This window allows you to view and manage registered people. Clicking on the **Add Face** button at the top of the window allows you to use saved image files (e.g. photos) to register people, while clicking on the **Export** button allows you to export the selected faces to image files.

The **Regroup** button allows you to tell SAFR that two different listings in the Identity Database are actually the same person, and they should be merged together. Merging two separate listings together greatly improve, as that particular person will have two reference images that the SAFR system will be able to use to better identify him or her.

Conversely, the **Regroup** button can be used to separate an Identity Database listing that had been previously erroneously merged from two separate listings.




## 33.1 People Filters

You can choose which people are listed in the bottom half of the window by specifying any of the following filters:

- **Name**: Filter based on the people's names.
- **Person Type**: Filter based on the people's `Person Types`.
- **Id Class**: Filter based on the people's `Id Classes` (i.e. their threat level).
- **Home location**: Filter basad on the people's `Home locations`.

## 33.2 Identity Database

All the people in the Identity Database that match your specified filters will be listed in the bottom half of the window. Any people that have an `Id Class` of "Threat" will be outlined in red, while any people with an `Id Class` of "Concern" will be outlined in yellow.

All listed people will display the reference image for that person in the Identity Directory, (if available) information about the event, and an image from the event along the right (if available).

You can sort the people based on the following criteria:

- **Recently added**: Sort the people based on when they were registered to the Identity Database, with the latest registrants at the top.
- **First added**: Sort the people based on when they were registered to the Identity Database, with the earliest registrants at the top.
- **Last name A-Z**: Sort the people alphabetically based on their last names, with last names beginning with "A" at the top.
- **Last name Z-A**: Sort the people alphabetically based on their last names, with last names beginning with "Z" at the top.

### 33.2.1 Identity Attributes

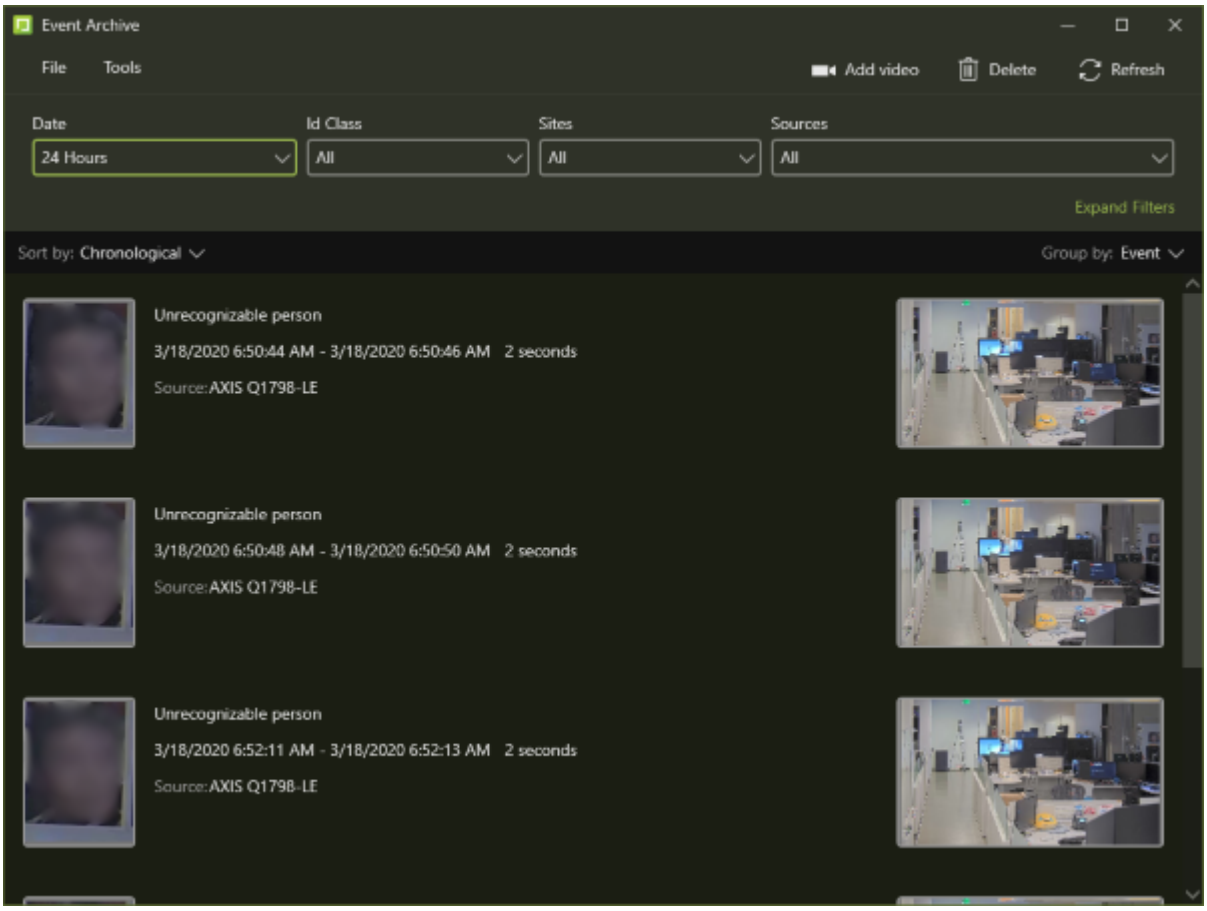
Some of the identity attributes are exposed in the default view of the Person Window, but if you double click on people's faces, you can view and configure all the identity attributes. Note that most of their identity attributes will be empty until manually enter the information.

- **Name**: The person's name.
- **Identifier**: The person's unique identifier within SAFR. This value is automatically assigned to them when they're registered, and cannot be changed.
- **Enrolled Since**: The date when the person was registered.
- **Gender**: The person's gender.
- **Age**: The person's age.
- **Company**: The company the person works for.
- **Moniker**: Used to realize two-factor authentication with visual badges.
- **Validation Phone**: The person's validation phone number.
- **Validation Email**: The person's validation email address.
- **Enrollment Expiration**: The expiration date of the person's enrollment.
- **Id Class**: The person's threat level. (i.e. Threat, Concern, or No-Concern)
- **Person Type**: The person's `Person Type`. `Person Types` are groupings that you define to differentiate the people registered in your Identity Database. (e.g. "student", "teacher", and "staff")
- **External Id**: If the person has been imported from another database, this value can be used to track the identity in both databases.
- **Home Location**: The person's Home Location. Home Locations, much like Person Types, are labels that you define to help differentiate the people registered in your Identity Database.
- **Tags**: Any custom tags that you have defined. People can have multiple tags assigned to them.

**Note**: When you double click on a person, there will be a View person activity button just below their face if they have been active recently.

# 34 Events Window

This window allows you to view and manage recorded events. By clicking on the **Add video** button at the top of the window you can also use saved video files to generate events and register people.




## 34.1 Event Filters

You can filter the events based on the following criteria. The first 4 filters are always visible, while the others become visible when you click on the **Expand Filters** button.

- **Date**: The date when the event was recorded.
- **Id Class**: The threat level of the person that triggered the event.
- **Sites**: The camera or set of cameras that recorded the event. **Note**: Usually `Sites` are set to multiple cameras.
- **Sources**: The camera or set of cameras that recorded the event. **Note**: Usually `Sources` are set to single cameras.
- **Name**: The name of the person that triggered the event.
- **Person Type**: The `Person Type` of the person that triggered the event.
- **Gender**: The gender of the person that triggered the recording of the event.
- **Tenure**: The date when the identity that triggered the event was registered to the Identity Database.
- **Shortest Gap**: If a person is viewed by one or more cameras multiple times within this time period, all those appearances are considered the same event.
- **Shortest Duration**: The minimum event duration, in milliseconds, to include in your search.
- **Disparate Sources**: If a person is viewed by multiple cameras at the same time, all those appearances are considered the same event when this filter is enabled.

## 34.2 Event Archive

All the events that match your specified filters will be listed in the bottom half of the window. All listed events will display an image of the person who triggered the event on the far left of the listing, the reference image for that person in the Identity Directory, (if available) information about the event, and an image from the event along the right (if available).

**Note**: For all events triggered by people registered to your Identity Directory, there will be a `View person activity` button just below the event information that will take you to the Person Activity Window.

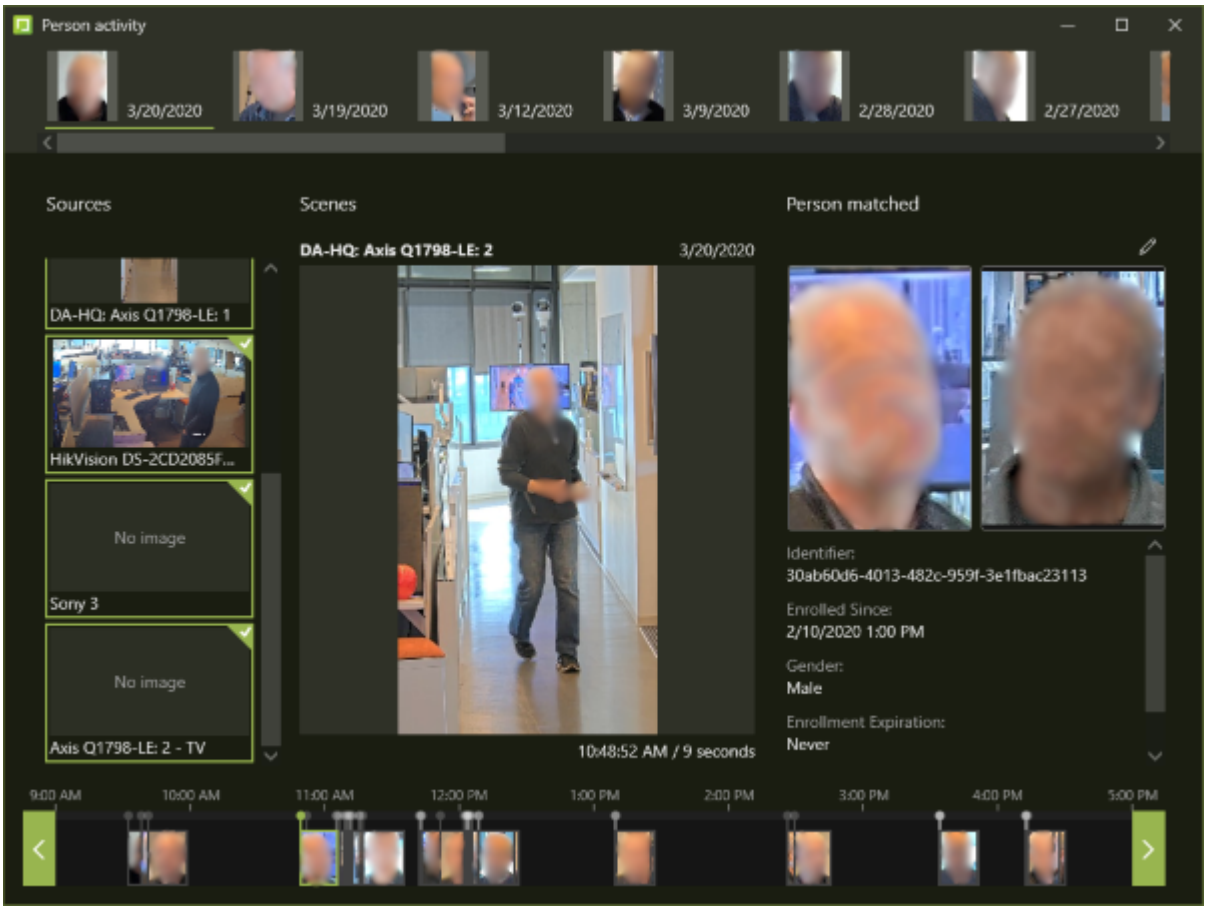
You can sort events by the following criteria:

- **Chronological**: Sort the events based on when they were recorded.
- **Duration**: Sort the events based on how long they last.
- **Name**: Sort the events based on the name of the person that triggered the event, if known.

You also have the option to group events by the person that triggered the event by selecting **Group by: Person** on the right side of the window. If you instead select **Group by: Event**, then the events aren't grouped by person and will instead only be sorted based on the sorting criteria that you have selected.

# 35 Person Activity Window

This window allows you to view the activity over time of a particular person.




## 35.1 Person Activity Panel (Top Panel)

The Person Activity Panel shows the dates when the person triggered one or more events. Click on any event to populate the Activity Timeline Panel with all the events of that date.

## 35.2 Sources Panel (Left Panel)

Shows all the cameras associated with the event(s) that you've selected in the Person Activity Panel and/or the Activity Timeline Panel.

## 35.3 Scenes Panel (Center Panel)

Shows event scenes from the event you selected in the Activity Timeline Panel if available.

## 35.4 Person Matched Panel (Right Panel)

Shows the person whose activity is being described by this window.

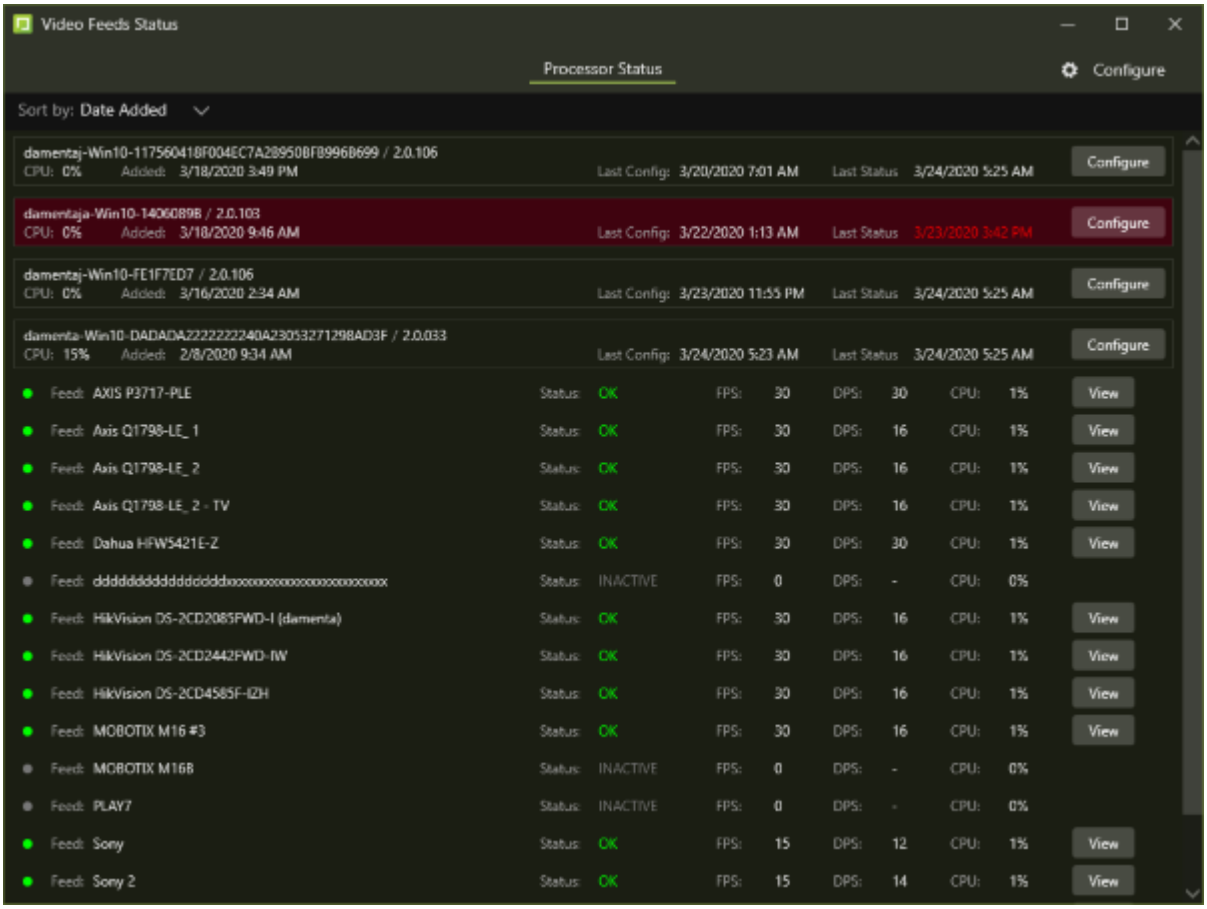
## 35.5 Activity Timeline Panel (Bottom Panel)

Shows the times of day when events were triggered on the date specified by the event you selected in the Person Activity Panel. Selecting the events on this timeline populates the Scenes Panel with event scenes, if

available.

# 36 Video Feeds Status Window

This window allows you to view and configure your video feeds. Any feed that's highlighted in red is currently inactive.




The video feeds can be sorted by one of the following criteria:

- **Date Added**: Sort the feeds based on the date when they were added.
- **Status Date**: Sort the feeds based on the date when the feeds' status last changed.
- **Client Id**: Sort the feeds based on the Id's of the clients to which the feeds are connected.
- **Tenant**: Sort the feeds based on the feeds' tenants.
- **Version**: Sort the feeds based on the feeds' version.

You can click on the **Configure** button to the right of a feed to configure it. Similarly, you can click on the **View** button the right of a camera to see a live video view of the camera.

## 36.1 Add a VIRGO Daemon

To add a VIRGO daemon, there must be at least one active video feed connected to this Desktop client. See Connect Cameras to SAFR for information about how to connect cameras to the client.

**Note**: You can't add a VIRGO daemon to a video feed that is currently being displayed by the Camera Feed Analyzer. To add a VIRGO daemon, do the following:

1. Click the **Configure** button on the active video feed that you want to associate the VIRGO daemon with.
2. Hover your mouse over the **feeds** entry. You'll see a + button and a **-** button. Click the + button. You'll be prompted for the following information:

- **Feed Name**: Enter any name for the video feed you wish.
- **Camera**: Select the camera that is providing the video feed.
- **Mode**: Select the video processing mode that you want the VIRGO daemon to operate in. For a description of the video processing modes, see here.
- **Apply Mode Customizations from Preferences**: Enable if you want the Desktop client preferences applied to the new VIRGO daemon.

3. Press the **Add** button. The VIRGO daemon has been created. **Note**: At this point, the VIRGO daemon exists independently of both the Desktop client and the video feed that you cloned to create the daemon.

# 37 Account Preferences

The Account Preferences tab allows you to configure the user account currently logged into the Desktop client. You can change which user is logged in entirely by clicking on the `Logout` button next to the *User Identifier*.

- **User Identifier**: The username of the logged-in user.
- **User Directory**: The user directory to use. (The default *user directory* is `main`.)
- **Default Site**: The default *Site* label to use for events generated by cameras connected to this Desktop client. This field is optional.
- **Server Location**: The server associated with the user's account.

# 38 Camera Preferences

The Camera Preferences tab allows you to add, remove, or configure cameras connected to this Desktop client. Cameras that have already been automatically discovered are displayed here.

SAFR normally auto-detects all integrated (built-in) cameras, USB-connected cameras, and IP (internet protocol) cameras that support the ONVIF (Open Network Video Interface Forum) protocol as long as they are present on the same network to which the Desktop client is connected. For more about ONVIF and the ONVIF specification, see the ONVIF home page.

## 38.1 ONVIF Cameras

- Each camera discovered via ONVIF must have a username and password.
- Be sure that the camera has at least one ONVIF user with administrative privileges, or ONVIF authentication will not work.
- ONVIF video profiles configured on the camera will be available to select in the live video recognition view.
- The date and time configured on the camera must be within five seconds of the system time SAFR is running on.

## 38.2 Camera Preferences

To configure a camera, select any of the connected cameras in the left panel. If you need to add a camera, see Connect Cameras to SAFR. When a camera is selected, a set of preferences will appear on the right of the window. Which preferences are exposed depends on what kind of camera is selected.

### 38.2.1 USB Camera Preferences

USB cameras have the following preference settings.

- **Source**: Use this field to override the default source label for the camera. For example, you might want to change a default source label to West Hall or a more meaningful label for your specific environment. Multiple cameras can have the same source label. For example, you could have several cameras labeled as South Exit, or you could label each camera differently ("South Exit 1", "South Exit 2", or other labels that make sense for you and your SAFR environment).
- **Contrast Enhancement**: When selected, enhances low-light images and videos by enhancing the contrast.
  - **Low Light Threshold**: Determines the level of light when the exposure boost will be applied. If an image or video has more light than the threshold allows for, then the exposure boost will not be applied.
  - **Exposure Boost**: Determines how much to boost the contrast.
- **Front facing**: Indicates if the camera is front facing.
- **Rotate Image**: Use the dropdown menu to set a value that rotates to correct for camera orientation. Typically, this correction can be done directly by the camera, but if not, you can adjust it here. Recognition does not work properly unless the camera's image is properly oriented.
- **Enforce Low Latency**: This option is only available for integrated and USB cameras. *Enforce Low Latency* optimizes display and processing by allowing the video frame rate to drop if CPU resources are low.
  This may be needed for some 4K webcam models or any cameras that support particularly high frame rates.
- **Unauthorized movement detection for person**: When any of the 4 settings below are enabled, the Desktop client will generate an unauthorized movement event when a person's face travels further than the specified percentage within the camera view field. For example, if `Left travel distance` were set to 50 then an unauthorized movement event would be generated if somebody's face entered the camera view field from the right edge of the frame, and moved more than halfway across the camera field

view. Note that you can configure multiple settings at the same time, and an unauthorized movement event would be triggered if the condition specified by any of the configured settings were met.

- **Left travel distance**: Generate an unauthorized movement event when a face enters from the right edge of the camera view field and travels more than the specified percentage across the field towards the left edge.
- **Right travel distance**: Gnerate an unauthorized movement event when a face enters from the left edge of the camera view field and travels more than the specified percentage across the field towards the right edge.
- **Up/Away travel distance**: Generate an unauthorized movement event when a face enters from the bottom edge of the camera view field and travels more than the specified percentage across the field towards the top edge.
- **Down/Towards travel distance**: Generate an unauthorized movement event when a face enters from the top edge of the camera view field and travels more than the specified percentage across the field towards the bottom edge.

### 38.2.2 Xenia Camera Preferences

**Note**: Xenia cameras can connect to SAFR only if you selected the Ximea camera extension when you installed SAFR.

Xenia cameras have the following preference settings.

- **Source**: Use this field to override the default source label for the camera. For example, you might want to change a default source label to West Hall or a more meaningful label for your specific environment. Multiple cameras can have the same source label. For example, you could have several cameras labeled as South Exit, or you could label each camera differently ("South Exit 1", "South Exit 2", or other labels that make sense for you and your SAFR environment).
- **Front facing**: Indicates if the camera is front facing.
- **Rotate image**: Use the dropdown menu to set a value that rotates to correct for camera orientation. Typically, this correction can be done directly by the camera, but if not, you can adjust it here. Recognition does not work properly unless the camera's image is properly oriented.
- **Max frame rate**: Select a value from the dropdown menu to set the max frame rate for the Xenia camera.
- **Contrast Enhancement**: When selected, enhances low-light images and videos by enhancing the contrast.
  - **Low Light Threshold**: Determines the level of light when the exposure boost will be applied. If an image or video has more light than the threshold allows for, then the exposure boost will not be applied.
  - **Exposure Boost**: Determines how much to boost the contrast.
- **Unauthorized movement detection for person**: When any of the 4 settings below are enabled, the Desktop client will generate an unauthorized movement event when a person's face travels further than the specified percentage within the camera view field. For example, if `Left travel distance` were set to 50 then an unauthorized movement event would be generated if somebody's face entered the camera view field from the right edge of the frame, and moved more than halfway across the camera field view. Note that you can configure multiple settings at the same time, and an unauthorized movement event would be triggered if the condition specified by any of the configured settings were met.
  - **Left travel distance**: Generate an unauthorized movement event when a face enters from the right edge of the camera view field and travels more than the specified percentage across the field towards the left edge.
  - **Right travel distance**: Gnerate an unauthorized movement event when a face enters from the left edge of the camera view field and travels more than the specified percentage across the field towards the right edge.
  - **Up/Away travel distance**: Generate an unauthorized movement event when a face enters from the bottom edge of the camera view field and travels more than the specified percentage across the field towards the top edge.

- **Down/Towards travel distance**: Generate an unauthorized movement event when a face enters from the top edge of the camera view field and travels more than the specified percentage across the field towards the bottom edge.

### 38.2.3 IP Camera Preferences

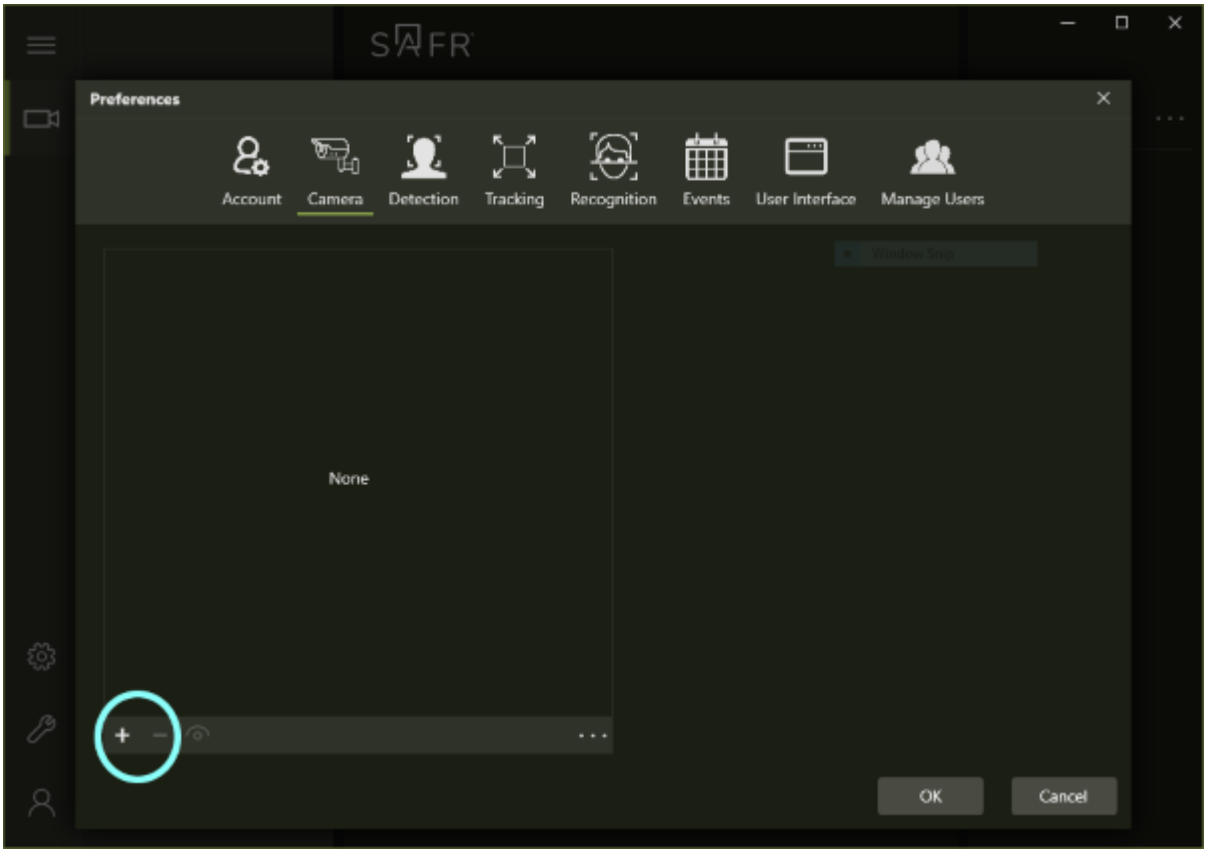
IP cameras have the following preference settings.

- **Source**: Use this field to override the default source label for the camera. For example, you might want to change a default source label to West Hall or a more meaningful label for your specific environment. Multiple cameras can have the same source label. For example, you could have several cameras labeled as South Exit, or you could label each camera differently ("South Exit 1", "South Exit 2", or other labels that make sense for you and your SAFR environment).
- **URL**: URL of the camera.
- **RTSP Transport Protocol:** For the lowest latency, select UDP (User Datagram Protocol). If network packet loss is an issue, select TCP (Transmission Control Protocol).
  Generally, UDP is a faster best effort communication system, whereas TCP is more reliable but slower. For example, if network connectivity is a concern for a particular camera, you might want to change this to TCP. Otherwise, UDP should be adequate in most situations.
- **Contrast Enhancement**: When selected, enhances low-light images and videos by enhancing the contrast.
  - **Low Light Threshold**: Determines the level of light when the exposure boost will be applied. If an image or video has more light than the threshold allows for, then the exposure boost will not be applied.
  - **Exposure Boost**: Determines how much to boost the contrast.
- **Lens Correction**: Enable lens correction to help correct the fisheye effect for very wide-angle lenses. This also improves recognition accuracy although is not needed in most cases.
  - **Coefficient K1**: The "K1" lens correction factor.
  - **Coefficient K2**: The "K2" lens correction factor.
- **Enforce timing for video frames**: When enabled, playback frame syncing to the video clock is enforced.
- **Front facing**: Indicates if the camera is front facing.
- **Rotate Image**: Use the dropdown menu to set a value that rotates to correct for camera orientation. Typically, this correction can be done directly by the camera, but if not, you can adjust it here. Recognition does not work properly unless the camera's image is properly oriented.
- **Back Channel**: When the connected camera is a Mobotix camera, you can set this field to *Mobotix MX* in order to have SAFR report *STRANGER* and *RECOGNIZED* event types to the camera. This feature is necessary if you want to make use of the Mobotix app.
  When the connected camera isn't a Mobotix camera, this setting doesn't have any effect.
  - **Cash Point**: This value must match the configured *cash point* within the Mobotix app. If this *Cash Point* setting doesn't match the cash point within the Mobotix app, the back channel won't work.
- **Frame buffer size**: Sets the size of the camera's frame buffer for buffering network streams.
- **Unauthorized movement detection for person**: When any of the 4 settings below are enabled, the Desktop client will generate an unauthorized movement event when a person's face travels further than the specified percentage within the camera view field. For example, if `Left travel distance` were set to 50 then an unauthorized movement event would be generated if somebody's face entered the camera view field from the right edge of the frame, and moved more than halfway across the camera field view. Note that you can configure multiple settings at the same time, and an unauthorized movement event would be triggered if the condition specified by any of the configured settings were met.
  - **Left travel distance**: Generate an unauthorized movement event when a face enters from the right edge of the camera view field and travels more than the specified percentage across the field towards the left edge.
  - **Right travel distance**: Gnerate an unauthorized movement event when a face enters from the left edge of the camera view field and travels more than the specified percentage across the field

towards the right edge.

- **Up/Away travel distance**: Generate an unauthorized movement event when a face enters from the bottom edge of the camera view field and travels more than the specified percentage across the field towards the top edge.
- **Down/Towards travel distance**: Generate an unauthorized movement event when a face enters from the top edge of the camera view field and travels more than the specified percentage across the field towards the bottom edge.

## 38.3 Use Additional Options




Click + to manually add an IP camera.

Click **-** to delete the configuration for manually added cameras. This option is not available for auto-discovered cameras.

Exporting enables you to create a copy of a camera configuration. Exporting saves a camera configuration to an .acc file in JSON format.

Importing enables you to import a copy of a camera configuration. Use this feature to copy a camera configuration from one SAFR system to another.

# 39 Detection Preferences

The Detection Preferences tab allows you to configure facial, badge, and person detection characteristics.

Note that if both face detection and person detection are enabled, face objects can be associated with the appropriate person objects, thus enabling SAFR to continue tracking people even when they turn their faces away from the camera. See the Face Detection-Person Detection Tie-In topic for more information about this feature.

- **For Mode**: Specifies which video processing mode is affected by the current settings on this page. See here for information about the different modes.

## 39.1 Enable Face Detector

The **Enable face detector** check box must be selected to enable face recognition.

- **Reduce vertical input image size to**: Represents the vertical size in pixels to which the image scanned by the camera is scaled in order perform face detection. Scaling down reduces CPU usage. 720-pixel resolution is usually sufficient for high-quality face detection without slowing down the CPU. Vertical size can be reduced to 640-pixels and even 480 to greatly reduce CPU usage for face detection, but this reduces the ability to detect and recognize smaller faces.(e.g. faces farther away from the camera)
- **Minimum searched face size**: Defines the minimum face size that can be detected. A searched size of 80, for example, can still manage to detect faces as small as 60x60, but with lower certainty. Lowering this number enables SAFR to detect much smaller faces but also greatly increases CPU usage.
- **Minimum required face size**: Defines the minimum required size for a face to be detected. Any face smaller than the height or width is ignored.
  This is typically set when face detection needs to be limited only to large faces, which indicates a face being closer to the camera. It may not be desirable, for example, to cause a lot of detection events for faces that are too far from a camera to be considered necessary for attention by SAFR.
- **Consecutive confirmations required**: This setting adds consecutive confirmations to the SAFR facial recognition to create more reliable detections. Increase this setting for more reliable but slower facial detection.
- **Generate recognizer hint for detected faces**: Optimizes facial recognition. This setting should usually be enabled, it can be disabled to improve performance if detection is being performed at very low resolutions. Note that if this setting is disabled, recognition accuracy will be reduced.
- **Use custom detection thresholds**: Allows you to customize the detection threshold. When this setting is checked, you can click on the *Configure* button to do the customization.
  - **Initial candidate selection threshold**: Initial face candidate threshold that is used during face detection.
  - **Middle candidate selection threshold**: Middle face candidate threshold that is used during face detection.
  - **Final candidate selection threshold**: Final face candidate threshold that is used during face detection.
- **Frame buffer size**: Sets the size of the frame buffer.
- **Maximum detectors per feed**: Specifies the maximum number of detectors that can run concurrently on the same feed.

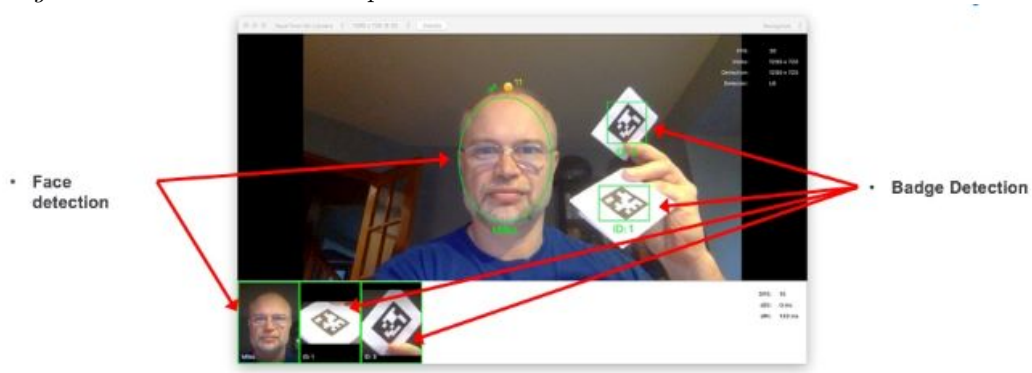
## 39.2 Enable Badge Detector

The **Enable badge detector** check box must be selected to enable badge detection. Badges are visual representations of users that are quicker and easier to detect than faces. Compared to faces, they are easier to detect and recognize when rotated and when used in low light conditions.

- **Reduce vertical input image size to**: Represents the vertical size a scanned image (badge) is scaled to in order to detect the badge. Scaling down the image reduces CPU usage.

If your badges are very small, we do not recommend using this setting.

- **Minimum searched badge size**: Defines the minimum badge size that can be detected. Lowering this value enables SAFR to detect very small badges (down to 15x15 pixels) at the cost of increasing the CPU usage. Conversely, increasing this value reduces CPU usage but requires larger badges for successful detection.
- **Minimum required badge size**: Use this setting to require a minimum badge size in pixels. Any badge smaller than this value in either height or width is ignored. This setting is mainly used when badge detection is only expected to occur when the badges are close to the camera. (When cameras are close to the camera, the badge sizes are guaranteed to be larger.) If this value is set too small, SAFR could create many detection events for badges that are far from the camera and therefore not of interest.
- **Consecutive confirmations required**: This setting adds consecutive confirmations to the SAFR detection to create more reliable detections. Increase this setting for more reliable but slower badge detection. Decrease it for faster but slightly less reliable detection.
- **Detection service**: Specifies which badge detection method will be used. Depending on the capabilities of your cameras, lighting conditions, and other variables, certain options may work better with your environment than others.
  You can choose from the following options:
  - **apriltags**: Basic badge detection.
  - **rhinotagsLite**: The fastest badge detector, but it has a lower tolerance for motion blur. It requires cameras with a fast shutter speed.
  - **rhinotagsTeam**: Faster badge detector, but it has little resilience to motion blur.
  - **rhinotagsFlex**: Fast badge detector with moderate resilience to motion blur.
  - **rhinotagsFull**: Badge detector with robust handling under various conditions and a strong resilience to motion blur.
    *rhinotagsFull* is the recommended option.




- Sample Badges (can be printed for experimentation – 2"x2" intended size):

A full set of badge images supported by SAFR is available at https://github.com/anqixu/apriltag/tree/master/tag36h11.

- It is recommended these images be re-sized to at least 2" x 2" size using the nearest neighbor algorithm (to maintain sharp edges) before use with SAFR.
- Although a single badge of displayed format can express only 587 different IDs, multiple badges can be combined to increase the number of expressible IDs into the billions. For example, using 6 badges providesover 827 billion expressible IDs.

- **Frame buffer size**: Sets the size of the frame buffer.
- **Maximum detectors per feed**: Specifies the maximum number of detectors that can run concurrently on the same feed.

## 39.3 Enable Person Detector

The **Enable person detector** check box must be selected to enable person detection.

**Note**: Person detection is not available on the Lite Desktop client.

- **Minimum required person to screen proportion**: Specifies the ratio of the person to the screen height. This can be between 0 - 1 and allows for decimal precision. For example, if you don't want the person to show up unless they are greater than 25% of the image height, specify a value of 0.25.
- **Consecutive confirmation required**: Number of consecutive detections that are required before reporting that the person (based on object id) was actually detected. This setting can be used to filter out false positives.
- **Detect persons every**: This can be used to avoid running person detection on every frame. Since person detection requires a lot of GPU processing if the hardware is not powerful enough this value can be changed so that you only attempt to detect people every Nth frame to save processing power to keep up with real-time detection.
- **Person detection threshold**: Detection threshold to use when matching persons. The higher the threshold the more strict the matching will be and the higher the confidence will be that the actual person matches.
- **Person separation threshold**: Threshold controlling the person separation when the persons are overlapping. This determines how much overlap is needed before no longer detecting the object with the weaker footprint.
- **Detection service**: This setting may have one of 3 values:
  - *Maximum accuracy*: Uses a larger model for the best accuracy, but the speed will be the slowest of the 3 options.
  - *Maximum speed*: Uses a smaller model for the fastest speed, but the accuracy will be the lowest of the 3 options.
  - *Balanced*: Uses a medium-sized model to have average precision and speed.
- **Input size**: Sets the person detector input size. This setting allows you to manage the trade-off between accuracy vs. speed. There are 3 possible values:
  - *Normal*: This is the standard against which the other 2 possible values are measured.
  - *Small*: This value has decreased accuracy but increased speed.
  - *Large*: This value has increased accuracy but decreased speed.
- **Frame buffer size**: Sets the size of the frame buffer.
- **Maximum detectors per feed**: Specifies the maximum number of detectors that can run concurrently on the same feed.

# 40 Tracking Preferences

The Tracking Preferences tab allows you to configure settings for tracking detected people.

- **For Mode**: Specifies which video processing mode is affected by the current settings on this page. See here for information about the different modes.
- **Maximum change relative to face size**
  - **Position**: The maximum position change, specified in percentage relative to the object size, to continue tracking.
  - **Size**: The maximum size change, specified in percentage relative to the object size, to continue tracking.
- **Stop tracking a face after it has lingered for**: Specifies how many additional frames SAFR will continue to keep a tracked face around after SAFR has failed to detect the face in the most recent frame.
- **Minimum recognitions to lock on to identity**: Minimum number of consecutive recognition attempts that must produce the same identity before SAFR locks onto the identity.
- **Minimum recognitions to learn identity**: Minimum number of consecutive face recognitions required to register a face into the Identity Database. This setting also affects the quality of the reference face signature recorded for an identity.
  Increasing this value increases the minimum quality of the face signature stored for a newly registered identity, but it decreases how quickly SAFR registers new identities.
- **Initial recognition attempts**: Number of initial recognition attempts to make on an unrecognized face as quickly as possible.
- **Failed recognition back-off interval**: After making the initial recognition attempts as quickly as possible, back up the amount specified by this setting for each subsequent recognition to slow down. This goes on until the retry interval is reached.
- **Retry failed recognition after every**: The interval in which to run recognition requests if the face has not been recognized.
- **Reconfirm identity after every**: Specifies how often a face's identity is reconfirmed, in milliseconds. If you set this value to zero, SAFR continues to re-confirm a face's identity at its normal rate. Increasing this value increases the confirmation rate and improves SAFR tracking subjects in crowded settings at the cost of increased CPU and network usage.
- **Update identity every**: Updates the identity when the currently saved identity is older than the updated identity.
- **Minimum failed recognitions to stop tracking identity**: When a face is being tracked recognitions are continually confirming the identity. The identity is also being verified if it is transferred from a person object. In these cases, if the recognition or verification consecutively fails this number of times then the identity will be reset and no longer associated with the face because we are no longer sure it is the same identity.
- **Update identity with better image**: Updates the identity only when the currently saved identity is older than the updated identity.
- **Enable correlation of faces by size**: Enables face correlation of tracked faces, which compares detected faces looking for a change in area.
  In most situations this setting should be enabled, but disabling it may help performance when there is only a single face to track and head movements are very fast.
- **Enable motion prediction**: Enables face motion prediction, which predicts which direction the face is moving in order to maintain tracking.
  In most situations this setting should be enabled, but disabling it may improve performance when tracked faces are moving in highly irregular motion patterns.
- **Stop tracking on failed recognition**: Enabling this option causes identity tracking to stop when SAFR doubts a confirmation of face tracking failures. SAFR is then forced to obtain a new identity lock. Enabling it may produce more discontinuity in recognition events and provide additional protection against mistaken tracking.
  This setting rarely needs to be enabled.
- **Reconfirm identity in video after each Key Frame**: When a key frame is encountered in a video

file all the faces that are being tracked are marked as unconfirmed so that their identities are reconfirmed to make sure they are the same person. This setting only applies to video files; it can't be used with live video. If a video file does not represent recorded live video then this can typically be set to true for better tracking during scene changes.

# 41 Recognition Preferences

The Recognition Preferences tab allows you to configure a variety of settings that affect how SAFR detects, tracks, and recognizes faces and identities.

## 41.1 Understand Facial Recognition

There are three key elements of SAFR facial recognition, each of which consists of a variety of settings that can be changed to help you fine-tune SAFR's performance:

- Detection: When a face is detected by a SAFR camera, as well as various settings that can affect how a face is recognized; minimum size, and resolution for a face to be detected, and more.
- Recognition: When a face is recognized it is compared against the SAFR database of recognized faces so it can be identified. Over time, SAFR collects and compares more images of an individual's face to help it build a catalog of variations to enable it to better recognize someone's face under different lighting conditions, angles, and with differing characteristics, such as a beard or different colored hair.
- Tracking: When a face is tracked, how long it is tracked, and other characteristics such as how tolerant the tracking is of motion and when to stop tracking.

## 41.2 Understand Occlusion Detection

SAFR can detect occluded faces. Occlusion constitutes any obstruction of the key facial features by, for example, a scarf, a hand, glasses, a mask, or hair draping over the face. Occlusion detection can be used to:

- Filter out highly occluded faces while learning them in the wild and preventing the storing of ambiguous face references in the Identity Database. For example, occlusion detection might be used when attempting to register players sitting at a table to prevent registering them with an occlusion feature, such as wineglass in front of their faces that may later create recognition inaccuracies.
- Update the occurrence event record with better face images without the occlusion to increase the value of the image stored with the event for presentation and investigation purposes.

### 41.2.1 Occlusion Detection Related to Events

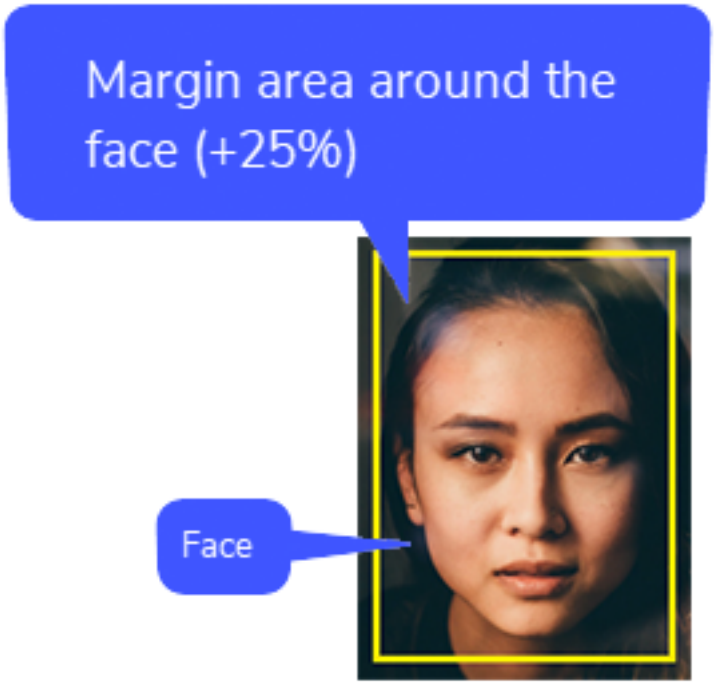
When the server returns an occlusion threshold in a recognition response, the most recent value is passed to the posted event under the following circumstances:

- When the event image is posted or updated.
- When the event `idClass` is set or updated.

The effect is the occlusion value in the event reflects occlusion of either the most recent event image update or an idClass change, whichever occurs last.

## 41.3 Recognition Preference Options

- **For Mode**: Specifies which video processing mode is affected by the current settings on this page. See here for information about the different modes.
- **Minimum required face size**




  - **For recognition**: Defines the minimum required face size in pixels to attempt recognition. It includes a 25% margin around the face.
    The minimum face size (with +25% percent margin) for maximum recognition accuracy is 240 pixels. Faces smaller than 240 pixels may have slightly reduced recognition accuracy.
    This setting can be as low as 60 pixels if other image characteristics are favorable.
  - **For merging**: Defines the minimum required face size (+25% margin) to attempt merging a captured face with the existing reference image for an already registered identity.
    When in *Learn and Monitor* video processing mode, SAFR may merge reference images for an identity to improve its understanding of different face characteristics for that identity. Consider this as a catalog of variations for a face. See Select a Video Processing Mode for more information about modes.
  - **For learning/strangers**: Defines the minimum required face size (+25% margin) to enable SAFR to store a reference image for a new identity.
  - **For full accuracy**: Establishes the point below which face size is considered when determining image quality. Once the face size goes above this setting, face size is no longer used to determine the quality of the image. This setting should be changed only in very special circumstances.
- **Minimum required center pose quality**
  - **For recognition**: Defines the minimum required quality for a face posed directly in front of the camera (center posed) to attempt recognition. Center pose quality (CPQ) ranges from one to zero. A score of 1 is given to a face looking straight into the camera. Any deviation from this position diminishes center pose quality. Center pose quality of a face in full profile position is given a score of zero. Recognition from any pose is possible, but accuracy is reduced for faces that are in extreme profile positions.
  - **For merging**: Defines the minimum required face center pose quality to attempt merging with existing reference images for a recognized identity.
  - **For learning/strangers**: Defines the minimum required face center pose quality to enable SAFR to store a reference image for a new identity.
  - **For direct gaze detection**: Events include a directGazeDuration property describing how long the person was looking at the camera. The directGazeDuration value is controlled by this For Direct Gaze Detection threshold in the settings. If the CPQ value is above this threshold, the face is determined to be looking at the camera, but if the value is below this threshold, the face is

determined to be turned away. The longer the value is above this threshold, the longer the direct gaze duration is.
    - **Use advanced settings for learning/strangers**: Enable if you want to modify the advanced learning setting below.
        - **Max Yaw**: Indicates minimum required yaw value to attempt registering somebody into the Person Directory. Yaw measures how much a face is turned to the left or right; a value of 0 indicates that the face is looking straight ahead.
        - **Max Pitch**: Indicates minimum required pitch value to attempt registering somebody into the Person Directory. Pitch measures how much a face is tilted up or down; a value of 0 indicates that the face is looking straight ahead and isn't tilted at all.
        - **Max Roll**: Indicates minimum required roll value to attempt registering somebody into the Person Directory. Roll measures how much a face is tilted to one side or the other; (i.e. the person's ear is moved closer to their shoulder) a value of 0 indicates that the face isn't tilted to either side.
- **Minimum required face sharpness quality**
    - **For recognition**: Indicates minimum required face sharpness quality to attempt recognition.
    - **For merging**: Indicates minimum required face sharpness quality to attempt recognition.
    - **For learning/strangers**: Indicates minimum required face sharpness quality to store as a reference for a new identity.
- **Minimum required face contrast quality**
  Contrast quality defines the difference between the color of a subject's face and the background.
    - **For recognition**: This setting indicates the minimum amount of contrast quality (lower or higher contrast) for SAFR to attempt a recognition.
    - **For merging**: Defines the minimum required face contrast quality to attempt merging a captured face with its existing references in the SAFR system.
    - **For learning/strangers**: Indicates the minimum required face contrast quality to store as a reference for a new identity.
- **Maximum allowed occlusion**
    - **For learning/strangers**: Indicates the maximum occlusion value allowed for a face to be registered to the Person Directory. When this setting is set to 1, no occlusion filtering is applied, and the default configuration is ignored.
    - **Learn occluded faces**: Select to have the system learn the faces. The check box is cleared by default.
- **Clipping tolerances**
  Clipping occurs when a face is only partially captured by a camera.
    - **For recognition**: This value defines the maximum amount of clipping tolerance (as a percentage of width or height) to attempt recognition. Faces not fully in the field of view are not recognized unless within this clipping tolerance threshold.
    - **For learning**: Indicates maximum allowed face clipping tolerance (as percent of width or percent height) to store as a reference for a new identity.
- **Identity recognition threshold**: Determines the strictness of the face recognition when declaring identity matches between a face and stored identity image. You can independently set the Identity Recognition Thresholds for the following:
    - **Camera**: Sets the threshold for images. (e.g. photos)
    - **Video**: Sets the threshold for video feeds and saved videos.
- **Proximity threshold allowance**: A boost value that is added to the Identity Recognition Threshold. For detailed information about how Identity Recognition Threshold and Proximity threshold Allowance work, see the Identity Recognition Thresholds topic.
- **Maximum recognizers per feed**: Specifies the maximum number of recognizers that can run concurrently on the same feed.

## 41.4 Detect

Select the check box to enable the detection of the following characteristics:

- **Identity**: The identity of the user in the SAFR system, such as their name.
- **Occlusion**: Obstructing the full view of the face by using, for example, a mask, glasses, or using a hand to block a part of the face.
  Note that if you disable this setting, then the *Mask* setting below will automatically be deselected as well.
- **Mask**: When enabled, SAFR will evaluate all occluded faces to see if they're covered by a mask. If they are, then SAFR will use the mask enhanced model to attempt to recognize the face behind the mask. If the occluded face isn't covered by a mask, then the normal occluded model will be used instead. Only standard blue or white surgical masks are currently supported; SAFR is unable to use the enhanced mask recognition model with masks of different colors or with masks that have customized patterns Enabling this setting will greatly increase SAFR's ability to recognize faces covered by masks, but it will needlessly slow down the system if there aren't any masks.
  Note that the *Occlusion* setting above will automatically be enabled if this setting is enabled.
- **Gender**: Enables the detection of gender information.
- **Age**: Enables the detection of age information.
- **Sentiment**: Enables the detection of sentiment information.
- **Smile action**: Enables the smile action recognizer.
  - **Pre-smile delay**: The amount of time, in milliseconds, that there should be no smile.
  - **Smile duration**: The amount of time, in milliseconds, that the smile should last.
  - **Identity recognition threshold boost**: The smile threshold to boost temporarily during the smile action.
- **Pose liveness action**: Enables the pose liveness action recognizer. See Pose Liveness Detection for more information.
  - **Center pose quality**: Minimum center pose quality to use when detecting the initial center pose.
  - **Profile pose quality**: The maximum center pose quality to use when detecting the final profile pose.
  - **Max profile confidence at start**: Maximum profile pose confidence to allow during the initial center pose detection phase.
  - **Min profile confidence at end**: Minimum profile pose confidence to allow during the final profile pose detection phase.
  - **Min profile pose yaw**: The minimum profile pose yaw value that is required during the final profile pose detection phase.
  - **Center pose consecutive confirmations required**: Number of consecutive center pose confirmations required to enter the initial center pose detection phase
  - **Profile pose consecutive confirmations required**: Number of consecutive profile pose confirmations required to enter the initial center pose detection phase.
  - **Min profile similarity**: Minimum similarity score required when verifying the final profile pose.
  - **Min Detections Per Second**: Minimum number of frames per second required during the process.
  - **Min transition poses**: Minimum number of required center pose samples during the transition from center to profile pose.
  - **Max CPQ jump in continuous tracking**: Maximum change between samples while the pose is changing from center to profile.
  - **Max CPQ jump after tracking loss**: Maximum change between samples while the pose is changing from center to profile if lingering.
  - **Max profile pose roll**: The maximum roll threshold in either direction in which the face can rotate when determining whether the face is in profile pose.
- **3D Liveness**: Enables 3D liveness. 3D liveness is a special feature of Intel RealSense cameras that allows them to distinguish flat images from 3 dimensional ones, thus allowing SAFR to tell the difference between a real face and a photo. This feature only works with Intel RealSense cameras; if you don't have any cameras of this type connected to SAFR, then this feature will not work.

- **Liveness Threshold**: Specifies the liveness threshold.

# 42 Events Preferences

The Events Preferences tab allows you to enable and configure event reporting and event replies. Every reported event contains start and end times as well as information about where it occurred and who or what triggered it. The location of the event is indicated by the site and source labels, which can be defined for each camera. Events are stored in the Event Archive and can be easily retrieved in real time or on demand for search and analytics. Events are reported promptly as they occur and when they end. Events are updated as a better understanding of what they represent becomes available.

- **For Mode**: Specifies which video processing mode is affected by the current settings on this page. See here for information about the different modes.

## 42.1 Report Events

Enables event reporting. Event reporting enables SAFR to log and track events over time and gain additional insight into your SAFR system and usage patterns.

- **Include Unrecognizable Events from Camera**: Enable this option to report the appearance of unrecognized people captured by camera feeds. Unrecognized people are people that the SAFR system can't see well enough to compare it to its People Directory.
- **Include Unrecognizable Events from Video**: Enable this option to report the appearance of unidentified individuals captured in video files imported into SAFR. Unrecognized people are people that the SAFR system can't see well enough to compare it to its People Directory.
- **Include Stranger Events**: Enable this option to report when cameras see strangers. Strangers are people who the SAFR system can see well enough to compare him/her to individuals stored in its People Directory, and there isn't a match.
  - **Min Age**: The minimum age of strangers that will trigger stranger events. If a stranger younger than the specified minimum age is detected, no stranger event is generated.
  - **Max Age**: The maximum age of strangers that will trigger stranger events. If a stranger older than the specified maximum age is detected, no stranger event is generated.
  - **Only if occluded**: When enabled stranger events are only reported when the stranger is occluded. This can be useful if you want to catch people who are attempting to bypass your security system by intentionally occluding their faces.
- **Include Speculated Identity Events**: Enables reporting events for speculated people. A "Speculated Identity" is a face that isn't a 100% match with a face in the Person Directory, but is close.
- **Include Secondary Events**: When enabled, face events that are tied to a person event will be included. Enabling secondary events often produces undesired "noise", so it is turned off by default. See Face Detection-Person Detection Tie-In for information about secondary events.
- **Preserve Event Face Image**: Select this check box if you want the images that trigger an event to be saved with the event report.
  - **Max Image Size**: The maximum size of the event face images, in pixels.
  - **Image Margin**: Specifies how much extra space around the face to include in the event face image.
- **Preserve Event Scene Thumbnail Image**: Select this option if you want a thumbnail of the scene image in which the event occurred to be saved with the event report.
  - **Max Image Size**: The maximum size of the event scene thumbnail images, in pixels.
- **Include Unrecognizable Event Images**: Specifies if event images should be stored for events triggered by unrecognizable people.
- **Include Stranger Event Images**: Specifies if event images should be stored for events triggered by people who aren't registered in your Identity Database.
- **Reporting delay**: The number of seconds an event report is delayed in order to properly assess the nature of the event. For example, a person who may at first seem unknown may become known after a second observation.
- **Min Identified Event Duration**: The minimum duration required for an event representing a known person to be recorded as an event.

This setting helps filter out noise or brief appearances that may not be worth reporting as a system event.
If this setting and *Reporting Delay* have different settings, the greater number is used.

- **Min Unrecognizable Event Duration**: The minimum duration of an event representing an unrecognizeable person to be recorded as an event.
  If this setting and *Reporting Delay* have different settings, the greater number is used.
- **Min Stranger Event Duration**: The minimum duration of an event representing a stranger to be recorded as an event.
  If this setting and *Reporting Delay* have different settings, the greater number is used.
- **Update in-progress event attributes**: If this is enabled then any event properties that change will be updated at the specified interval. Many properties do change periodically, such as images or other averages that are continually computed.
  - **Update interval**: Specifies the interval time in which to update event properties that change.
  - **Include qualified images with updates**: When enabled, SAFR will include qualified images with in-progress event attribute updates. These qualified images will be included even if they're lower quality than earlier images.
- **Update with higher quality image**: Update the thumbnail images with higher quality images during the course of the event if possible.

## 42.2 Listen for Event Replies

- **Display Reply Message**: Enables SAFR to display reply messages on the screen.
- **Display until end of event**: When enabled, the event reply is continuously displayed until the event ends. When this isn't enabled, the event reply is only shown for a couple seconds.
- **Positive Reply**: Allows you to configure positive replies.
  - **Sound**: Specifies which sound, if any, is played when a positive event occurs.
  - **Voice**: Specifies which voice, if any, will be used.
  - **Overlay image**: The image to be displayed while a positive reply is being displayed. If no image has been uploaded, then the live view of the video feed will be shown.
  - **Text Color**: Specifies the text color of the reply.
- **Neutral Reply**: Allows you to configure neutral replies.
  - **Sound**: Specifies which sound, if any, is played when a neutral event occurs.
  - **Voice**: Specifies which voice, if any, will be used.
  - **Overlay image**: The image to be displayed while a neutral reply is being displayed. If no image has been uploaded, then the live view of the video feed will be shown.
  - **Text Color**: Specifies the text color of the reply.
- **Negative Reply**: Allows you to configure negative replies.
  - **Sound**: Specifies which sound, if any, is played when a negative event occurs.
  - **Voice**: Specifies which voice, if any, will be used.
  - **Overlay image**: The image to be displayed while a negative reply is being displayed. If no image has been uploaded, then the live view of the video feed will be shown.
  - **Text Color**: Specifies the text color of the reply.
- **Reaction Delay**: Delays the event reporting to the server by this amount in seconds.

## 42.3 Remove events

Enables removing of events according to the preferences selected within this section.

- **Remove events**: It's *Enabled* if either anonymous or non-anonymous events are configured to be removed. Click the **Change...** button to configure the event removal.
  - **Remove Anonymous Events after**: Determines how many days to wait before removing events triggered by people without a *name* attribute in the Person Directory. If this value is set to zero, then anonymous events won't be automatically removed.
  - **Remove Known Identity Events after**: Determines how many days to wait before removing non-anonymous events. If this value is set to zero, then non-anonymous events won't be

automatically removed.

- **Remove identities**: It's *Enabled* if either anonymous or non-anonymous events are configured to be removed. Click the **Change...** button to configure the event removal.
  - **Target Directory**: Determines the directory whose identities are to be automatically removed.
  - **Remove Anonymous Identities after**: Determines how many days to wait before identities that don't have a *name* attribute. If this value is set to zero, then anonymous identities won't be automatically removed.
  - **Remove Identities of person type**: Select the *Person Type* of the identities you'd like removed. If you don't modify this field, then identities of all *Person Types* will be removed.
  - **after**: Determines how many days to wait before removing identities of the specified *Person Type*. If this value is set to zero, then identities with *Person Types* won't be automatically removed.

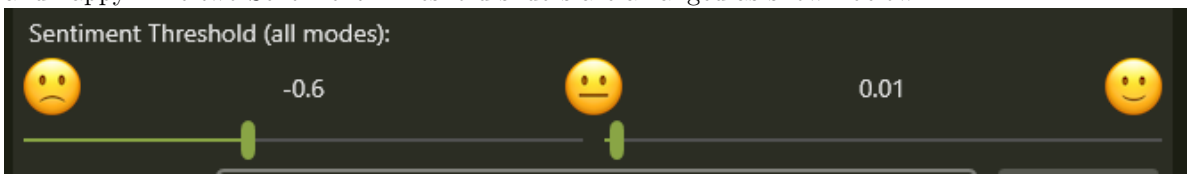
# 43 User Interface Preferences

The User Interface tab allows you to customize your Desktop client's user interface.

- **For Mode**: Specifies which video processing mode is affected by the current settings on this page. See here for information about the different modes.
- **Default Window**: Chooses the window that the Desktop client will default to when it starts.
- **Operator Console is the primary application window**: Sets the Operator Console as the primary application window. If this setting is not selected, then the Camera Window is the primary application window. Setting a window to be the primary application window means the Desktop client will shut down when the window is closed.
- **Language**: The language the Desktop client uses.

## 43.1 Video

- **Accelerated Video Decoding**: When enabled, the GPU will be used for video decoding.
- **Accelerated Video Rendering**: When enabled, the GPU will be used for video rendering.
- **Loop playback**: Enable this to loop playback of a video file. This is primarily useful for looping video demos.
- **Display time**: Use the slider to set the number of seconds a newly recognized person's name is flashed on the screen.
- **Minimum name refresh time**: This setting defines how long (in seconds) a recognized person must be out of camera view before their name is flashed again should they reappear in the camera view.
- **Highlight border thickness**: Use the slider to set the thickness (in pixels) of the frame displayed around faces and badges.
- **Custom highlight colors**: Allows you to customize the colors for the video feed overlays.
- **Overlay text size**: Specifies the size of the text in the video feed overlay.
- **Name display message (#N = Full name, #F = First name, #U = Last name)**: Use this option to display a custom message to registered and recognized entrants.
  Use #N as a placeholder for the name of any recognized person. For example, Welcome, #N would display "Welcome, <recognized person's name>." The message is only displayed to registered persons.
- **Speak name display message**: When enabled, the *Name display message* will be spoken aloud.
- **Average Age and Gender**: During its normal operation, SAFR estimates the age and gender of people in every frame of a video stream independently. Thus, a person's displayed age can fluctuate by 10 years frame to frame. When this setting is enabled, ages and gender for a detected person are averaged over time, which creates a much smoother and more accurate experience. This setting has no effect on recognized people whose age or gender are specified within the Identity Database; SAFR will always display the stored values.
- **Sentiment Thresholds**: Specifies what range of sentiment values are classified as unhappy, neutral, and happy. The two Sentiment Threshold sliders are arranged as shown below.




- **Overlay image**: Default background image that shows all the time. It can change based on events. If this is left blank, the video feed is shown.
- **Enable Registration**: Enable this to allow unknown users to register their faces.
- **Start automatically after signing into Windows**: Causes the Desktop client to automatically start when you sign in to Windows. This setting does nothing when kiosk mode is on.
  - **Configure Windows automatic sign-in**: Enables configuration of the credentials used when the Desktop client automatically starts. If no credentials are entered, then SAFR won't be able to automatically start.
- **Kiosk mode**: Enables kiosk mode for the Desktop client. In Kiosk mode, the Windows taskbar

won't be visible and the Desktop client will be the only program that runs after signing into the account. Elevation is used to change the setting, and the current user SID is passed through such that a low-privilege kiosk user and a high-privilege admin user account may be configured on the machine. If the Desktop client crashes for any reason while in kiosk mode, it will immediately and automatically restart.

When you enable kiosk mode, a dialogue box will pop up with the following 2 settings you can enable:

  - **Also prevent this PC from going to sleep or activating the screen saver**
  - **Also prevent Windows Update automatic updates (manual update check required)**

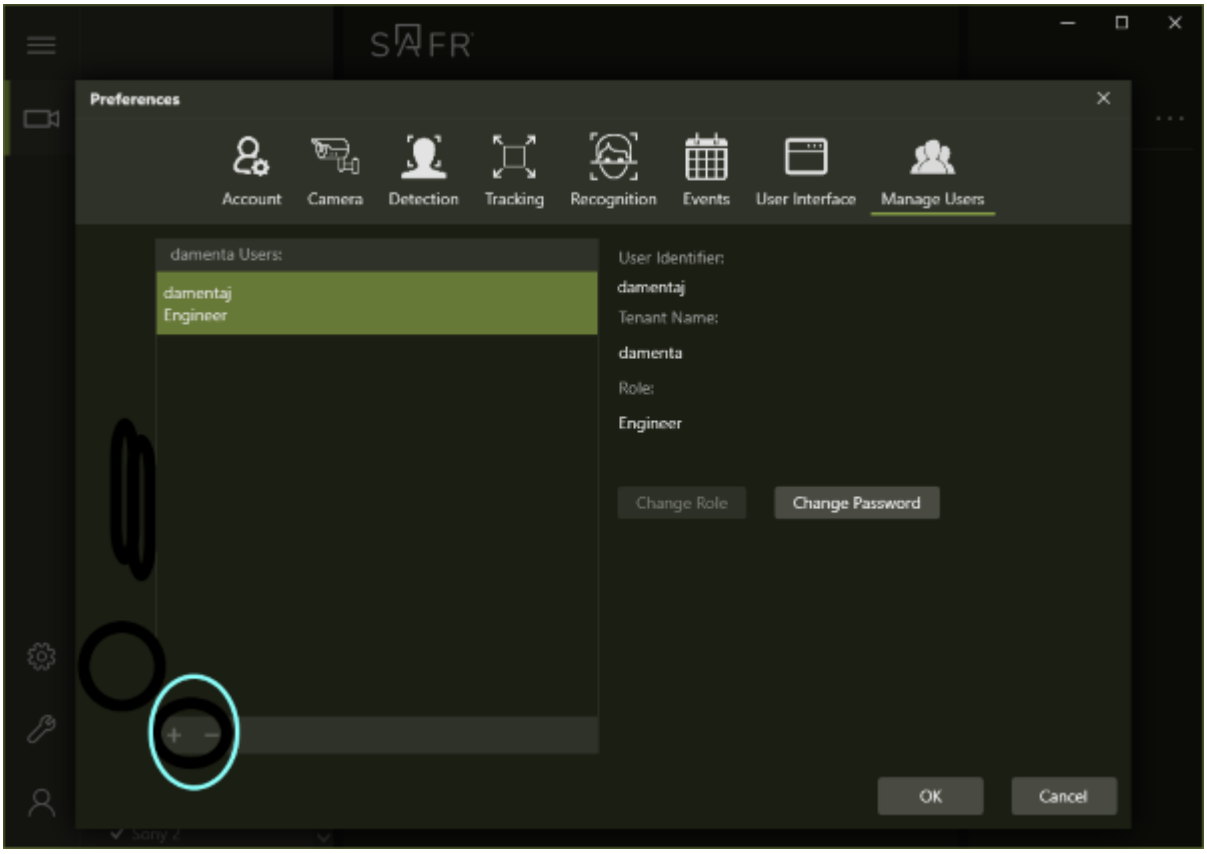
- **Require sign-in every time SAFR Desktop starts**: When enabled, users will be prompted to sign in every time the Desktop client starts.

# 44 Manage Users Preferences

The Manage Users Preferences tab allows you to change your password, add or remove users, and edit users' access levels.

All users can change their own password by clicking on the **Change Password** button. Administrators can also use this button to change the passwords of other users in their tenant, while super administrators can change the passwords of any other user. This can be useful when a password reset is needed.

Administrators can change other users' roles within their tenant by clicking on the **Change Role** button, while super administrators can change any user's role.




Administrators and super administrators can click the + button to add a new user. Similarly, administrators can click the - button to delete a user in their tenant, while super administrators can click - to delete any user.

## 44.1 User Roles

Every user account has a user role assigned to it, which determines the access priveleges granted to the user. The following user roles are defined:

- **Super Administrator**: Super administrators can manage all users and data across all tenants. This role is only available to local deployments; in cloud deployments SAFR administrators adopt the role of super administrators, by design, since the SAFR engineering team is responsible for managing the SAFR Servers for cloud deployments. Super sdministrators have the following access rights:
  - READ_PRIVILEGE
  - WRITE_PRIVILEGE
  - DELETE_PRIVILEGE
  - CONFIG_PRIVILEGE

    - ACCOUNT_PRIVILEGE
    - ACCESS_PRIVILEGE
    - READ_EVENT_PRIVILEGE
    - WRITE_EVENT_PRIVILEGE
    - SUPER_READ_PRIVILEGE
    - SUPER_WRITE_PRIVILEGE
    - SUPER_DELETE_PRIVILEGE
    - SUPER_CONFIG_PRIVILEGE
    - SUPER_ACCESS_PRIVILEGE
    - SUPER_READ_EVENT_PRIVILEGE
    - SUPER_WRITE_EVENT_PRIVILEGE
    - LICENSE_RETRIEVAL_PRIVILEGE
- **Administrator**: Administrators can manage all users and data within their tenants. Administrators have the following access rights:
    - READ_PRIVILEGE
    - WRITE_PRIVILEGE
    - DELETE_PRIVILEGE
    - CONFIG_PRIVILEGE
    - ACCOUNT_PRIVILEGE
    - ACCESS_PRIVILEGE
    - READ_EVENT_PRIVILEGE
    - WRITE_EVENT_PRIVILEGE
- **Engineer**: Engineers can manage all data stored in their tenants. Engineers have the following access rights:
    - READ_PRIVILEGE
    - WRITE_PRIVILEGE
    - DELETE_PRIVILEGE
    - CONFIG_PRIVILEGE
    - ACCOUNT_PRIVILEGE
    - READ_EVENT_PRIVILEGE
    - WRITE_EVENT_PRIVILEGE
- **Editor**: Editors can read and write all all identity and event data stored in their tenants. They can also delete person data in their tenants. Editors have the following access rights:
    - READ_PRIVILEGE
    - WRITE_PRIVILEGE
    - DELETE_PRIVILEGE
    - ACCOUNT_PRIVILEGE
    - READ_EVENT_PRIVILEGE
    - WRITE_EVENT_PRIVILEGE
- **User**: Users can read and write all person and event data stored in their tenants. Users have the following access rights:
    - READ_PRIVILEGE
    - WRITE_PRIVILEGE
    - ACCOUNT_PRIVILEGE
    - READ_EVENT_PRIVILEGE
    - WRITE_EVENT_PRIVILEGE
- **Editor Proxy**: Editor proxies are identical to editors with the exception that they can't change their own passwords.
    - READ_PRIVILEGE
    - WRITE_PRIVILEGE
    - DELETE_PRIVILEGE
    - CONFIG_PRIVILEGE
    - READ_EVENT_PRIVILEGE
    - WRITE_EVENT_PRIVILEGE

- **User Proxy**: User proxies are identical to users with the exception that they can't change their own passwords.
  - READ_PRIVILEGE
  - WRITE_PRIVILEGE
  - CONFIG_PRIVILEGE
  - READ_EVENT_PRIVILEGE
  - WRITE_EVENT_PRIVILEGE
- **Monitor**: Monitors can read identity and event data stored in their tenants.
  - READ_PRIVILEGE
  - ACCOUNT_PRIVILEGE
  - WRITE_EVENT_PRIVILEGE
- **Analyst**: Analysts can read event data stored in their tenants.
  - ACCOUNT_PRIVILEGE
  - READ_EVENT_PRIVILEGE
- **Founder**: Internal use only.

## 44.2 Privilege Types

The following privilege types determine what access priveleges have been granted to users:

- **READ_PRIVILEGE**: Allows the user to read identity data in their own tenant.
- **WRITE_PRIVILEGE**: Allows the user to write identity data in their own tenant.
- **DELETE_PRIVILEGE**: Allows the user to delete identity data in their own tenant.
- **CONFIG_PRIVILEGE**: Allows the user to add, remove, or edit any of the configuration values on the Video Feeds Status Window except for the root configuration.
- **ACCOUNT_PRIVILEGE**: Allows the user to change their own password.
- **ACCESS_PRIVILEGE**: Allows the user to add or remove user accounts in their own tenant. The user can also modify other users' roles in their own tenant.
- **READ_EVENT_PRIVILEGE**: Allows the user to read event data in their own tenant.
- **WRITE_EVENT_PRIVILEGE**: Allows the user to write event data in their own tenant.
- **SUPER_READ_PRIVILEGE**: Allows the user to read identity data in any tenant.
- **SUPER_WRITE_PRIVILEGE**: Allows the user to write identity data in any tenant.
- **SUPER_DELETE_PRIVILEGE**: Allows the user to delete identity data in any tenant.
- **SUPER_CONFIG_PRIVILEGE**: Allows the user to add, remove, or edit any of the configuration values on the Video Feeds Status Window.
- **SUPER_ACCESS_PRIVILEGE**: Allows the user to add or remove user accounts in any tenant. The user can also modify other users' roles in any tenant.
- **SUPER_READ_EVENT_PRIVILEGE**: Allows the user to read event data in any tenant.
- **SUPER_WRITE_EVENT_PRIVILEGE**: Allows the user to write event data in any tenant.
- **LICENSE_RETRIEVAL_PRIVILEGE**: Allows the user to retrieve and edit SAFR license information. See Licensing for information about SAFR licenses.

# 45 SAFR Edge Command Line Install Options

Silent installation of SAFR Edge on Windows can be achieved by invoking the SAFR Edge installer via the command line and using the `/S` switch.

**Example**:

```
SAFREdge_win_1_8_442_10_18_19.exe /S
```

The Windows SAFR Edge installer provides several options for configuring the component selection during install. Each component can be disabled or enabled by using the following syntax:

- `SAFREdge_win_1_8_442_10_18_19.exe /S /COMPONENT=YES`
- `SAFREdge_win_1_8_442_10_18_19.exe /S /COMPONENT=NO`

**Examples**:

```
SAFREdge_win_1_8_442_10_18_19.exe /S /VIRGO=YES /Actions=NO

SAFREdge_win_1_8_442_10_18_19.exe /Actions=YES /Digifort=YES
```

## 45.1 Command Line Install Options

| Feature Type | Component | Flag | Default | Notes |
|---|---|---|---|---|
| Silent Install | Silent Install | /S | Disabled | |
| Component | SAFR Actions and ARES | /Actions | Enabled | |
| Component | Desktop Client | /Application | Enabled | |
| Component | VIRGO | /VIRGO | Enabled | |
| VMS Integration Plugin | Avigilon Plugin | /Avigilon | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |
| VMS Integration Plugin | Digifort Plugin | /Digifort | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |
| VMS Integration Plugin | Genetec Plugin | /Genetec | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |
| VMS Integration Plugin | GenetecFR Plugin | /GenetecFR | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |
| VMS Integration Plugin | Milestone Plugin | /Milestone | Disabled | Only one VMS Plugin allowed. The first specified plugin will be used. |
| Camera Extension | Ximea Camera Extension | /Ximea | Disabled | |

| Feature Type | Component | Flag | Default | Notes |
|---|---|---|---|---|
| Installation Location | Installation Location | /D | `C:\Program Files\RealNetworks\SAFR` | Must be the last command line argument. Do not use quotes. |

# 46 SAFR Desktop Command Line Install Options

## 46.1 Command Line Feature Controls

If you launch the Desktop client installer via command line, you can specify which features will be installed. The syntax for the command line options is:

```
msiexec -i /quiet <installer.msi> ADDLOCAL=Feature1,Feature2
```

where:

- **msiexec**: The default Windows installer. It's included by default in all Windows installations, and you can call it from any console command window.
- **/quiet**: When this command line option is used, the installation is executed quietly (i.e. without any user interaction).
- **<installer.msi>**: Placeholder representing the msi installer that you download when you choose to download SAFR Desktop. The actual msi installer will look something like this:

  ```
  SAFRDesktop_win_1_8_442_10_18_19.msi
  ```

- **ADDLOCAL**: Whichever features you add here will be installed during the Desktop client installation.

The command line options listed below control which features are turned on in the feature selection tree during installation.

- VIRGO - VIRGO for Windows
- Milestone - SAFR-Milestone VMS integration
- Genetec - SAFR-Genetec VMS integration
- GenetecFR - SAFR-Genetec FaceReq VMS integration
- Digifort - SAFR-Digifort VMS integration
- Avigilon - SAFR-Avigilon VMS integration
- Ximea - Ximea camera extension

**Note:** Only one VMS (Milestone, Genetec, GenetecFR, Digifort, or Avigilon) may be selected during installation. If more than one VMS is selected, an error is generated and the installation fails.

The default features are: VIRGO, no VMS, and no Ximea camera extension.

Defaults are cleared when any features are specified on the command line. If you set any features on the command line, then you must set all the features you want. In other words, even though VIRGO is enabled by default, you must still specify VIRGO on the command line if you specify any other features.

**Examples:**

| Action | Sample Commands |
|---|---|
| Milestone VMS integration, VIRGO for Windows, quiet install | `msiexec -i /quiet SAFRDesktop_win_1_8_442_10_18_19.msi ADDLOCAL=Milestone,VIRGO` |
| VIRGO for Windows without VMS | `msiexec -i SAFRDesktop_win_1_8_442_10_18_19.msi` |
| Genetec VMS integration without VIRGO for Windows | `msiexec -i SAFRDesktop_win_1_8_442_10_18_19.msi ADDLOCAL=Genetec` |

## 46.2 Custom Properties

You're also able to configure the following properties:

- **SAFR_ENVIRONMENT**

  Updates the Argus.exe.config 'Environment' setting.

  Typical environment values are:

  - LOCAL
  - PROD

  **Example:**

  ```
  msiexec -x installer.msi SAFR_ENVIRONMENT=PROD
  ```

- **SAFR_USERID**

  Updates the Argus.exe.config 'UserId' setting.

  **Example:**

  ```
  msiexec -x installer.msi SAFR_USERID=argusrn
  ```

- **SAFR_USERPASSWORD**

  Updates the Argus.exe.config 'UserPassword' setting.

  **Example:**

  ```
  msiexec -x installer.msi SAFR_USERPASSWORD=OpenSesame
  ```

- **SAFR_USERDIRECTORY**

  Updates the Argus.exe.config 'UserDirectory' setting.

  **Example:**

  ```
  msiexec -x installer.msi SAFR_USERDIRECTORY=main
  ```

- **REMOVEAPPLICATIONSETTINGS**

  Determines if the Desktop client's setting folder is removed.

  The default is to not remove the settings folder.

  Application settings are stored in the `C:\Users\user\AppData\Local\RealNetworks` folder.

  Set this property to "1" to override the default behavior and delete the Local AppData folder during uninstall.

  **Example:**

  ```
  msiexec -x installer.msi REMOVEAPPLICATIONSETTINGS="1"
  ```

- **REMOVESAFRPLUGIN**

  Determines if the third party SAFRPlugin.dll is removed during uninstall.

  The default is to not remove SAFRPlugin.dll

  Set this property to "1" to override the default behavior and delete SAFRPlugin.dll during uninstall.

  **Example:**

  ```
  msiexec -x installer.msi REMOVESAFRPLUGIN="1"
  ```

## 46.3 Logging

To install logging, run the following command:

```
msiexec /i installer.msi /l*v installLog.txt
```

To uninstall logging, run the following command:

```
msiexec /x installer.msi /l*v uninstallLog.txt
```

For a list of error codes, see https://cloudywindows.io/windowsinstallererrorcodes/

# 47 Connect a Face Recognition Panel

A face recognition panel is a mobile device running the Mobile client placed in **Secure Access** or **Secure Access With Smile** video processing mode. It is used at the door (usually placed behind safety glass on the inner side of a door) as part of the SAFR Secure Access setup. A face recognition panel provides an event to SAFR Server that is then picked up by SAFR Actions, which in turn triggers the door unlock action.

## 47.1 Download and Install the Mobile Client

To install the Mobile client, simply go to the SAFR Download portal, download the Mobile client specfic to your mobile device's OS, and then run the installer.

iOS devices have additional potential download locations:

- Go to the *Apple App Store* and search for *SAFR Recognition*.
- Using your browser, navigate to *itunes.apple.com/app/id1376830890*.

**Note**: In local deployments, iOS devices require that the primary SAFR Server have an SSL certificate. See SSL Certificate Installation for instructions on how to do this.

## 47.2 Connect the Mobile Client to a SAFR Server

To connect your Mobile client to a SAFR Server, do the following:

1. Make sure your mobile device is connected to the internet and that it can make a network connection either to the SAFR Cloud (for cloud deployments) or to your SAFR Server (for local deployments).
2. Start the Mobile client.
3. Sign in using your credentials.
    - If you have been issued an account for the Cloud environment, enter your user ID and password in the sign-in dialog that appears on the screen.
      **Note:** Make sure the front facing camera of your mobile device has a view of your face when signing in. Your face is not recorded, but it must be detected for sign-in to be offered.
    - If you instead have an account for the Partner Cloud environment:
        1. Cancel the sign-in dialog.
        2. Open the Mobile client settings by tapping the gear icon in bottom left.
        3. In the Account tab of the Mobile client settings, change the environment to SAFR Partner Cloud.
        4. Close the settings.
        5. Make sure the front facing camera of your mobile device has a view of your face. Your face is not recorded, but it must be detected for sign-in to be offered.
    - Tap the **Sign In** button that appears at the top of the screen.
    - Enter your credentials, select the agreement to terms of service check box, and tap **Sign In**.

If successful, the **Sign In** button disappears and a purple frame is displayed around your face with **Tap to Register** displayed underneath.

## 47.3 Configure the Mobile Client as a Face Recognition Panel

To configure the Mobile client as a face recognition panel, do the following:

1. Start the Mobile client.
2. Open the settings menu by tapping the gear icon in bottom left corner of the screen.
3. Tap the video processing mode selector at the top center of the screen, and select either **Secure Access** or **Secure Access With Smile**.
    - **Secure Access** mode generates an event when a person is recognized.

- **Secure Access with Smile** mode generates an event when a recognized person is observed changing expression from non-smiling to smiling.

  **Note:** When in **Secure Access** or **Secure Access With Smile** mode, video is turned off by default. If you want to show the video, you can override this behavior from the settings menu (gear icon) in the **User Interface** tab.

4. Complete the **User Site** and **User Source** fields.
   - The **User Site** labels the site (e.g. My-Office) at which you are deploying SAFR Secure Access.
   - The **User Source** labels the entrance location (e.g. Front-Door) at which the mobile device is placed.

     **Note:** *Site* and *Source* labels are associated with every registration as well as with every other event and are crucial in making the source of registrations as well as other events traceable.

5. (Optional) Configure the mobile device into Locked Mode to lock in the Mobile client as the exclusive application for the device.

   **Note**: Locking your mobile device locks the phone to your Mobile client and prevents any disruption in the registration kiosk operation due to operating system updates or unauthorized user interference. It isn't necessary to lock your mobile device if you merely want to try out the Mobile client as a registration kiosk. However, you should lock the device before deploying the registration kiosk in a production environment.

# 48 Connect a Registration Kiosk

A SAFR registration kiosk is a mobile device running a Mobile client that has been placed in Registration Kiosk mode. It is used to take pictures of users and enable them to register their faces and identity information with the SAFR system.

## 48.1 Download and Install the Mobile Client

To install the Mobile client, simply go to the SAFR Download portal, download the Mobile client specfic to your mobile device's OS, and then run the installer.

iOS devices have additional potential download locations:

- Go to the *Apple App Store* and search for *SAFR Recognition*.
- Using your browser, navigate to *itunes.apple.com/app/id1376830890*.

**Note**: In local deployments, iOS devices require that the primary SAFR Server have an SSL certificate. See SSL Certificate Installation for instructions on how to do this.

## 48.2 Connect the Mobile Client to a SAFR Server

To connect your Mobile client to a SAFR Server, do the following:

1. Make sure your mobile device is connected to the internet and that it can make a network connection either to the SAFR Cloud (for cloud deployments) or to your SAFR Server (for local deployments).
2. Start the Mobile client.
3. Sign in using your credentials.
    - If you have been issued an account for the Cloud environment, enter your user ID and password in the sign-in dialog that appears on the screen.
      **Note:** Make sure the front facing camera of your mobile device has a view of your face when signing in. Your face is not recorded, but it must be detected for sign-in to be offered.
    - If you instead have an account for the Partner Cloud environment:
        1. Cancel the sign-in dialog.
        2. Open the Mobile client settings by tapping the gear icon in bottom left.
        3. In the Account tab of the Mobile client settings, change the environment to SAFR Partner Cloud.
        4. Close the settings.
        5. Make sure the front facing camera of your mobile device has a view of your face. Your face is not recorded, but it must be detected for sign-in to be offered.
    - Tap the **Sign In** button that appears at the top of the screen.
    - Enter your credentials, select the agreement to terms of service check box, and tap **Sign In**.

If successful, the **Sign In** button disappears and a purple frame is displayed around your face with **Tap to Register** displayed underneath.

## 48.3 Configure the Mobile Client as a Registration Kiosk

Do the following:

1. Start the Mobile client.
2. Open the settings menu by tapping the gear icon in bottom left corner of the screen.
3. Tap the mode selector at the top center of the screen, and select **Registration Kiosk**.
4. Complete the **User Site** and **User Source** fields.
    - The **User Site** identifies the site (e.g. My-Office) at which you are deploying the SAFR System.

- The **User Source** identifies the registration kiosk (e.g. Registration-Kiosk) as the source of registrations. **Note:** *Site* and *Source* labels are associated with every registration as well as with every other event and are crucial in making the source of registrations as well as other events traceable.

5. (Optional) Configure the mobile device into Locked Mode to lock in the Mobile client as the exclusive application for the device.

   **Note**: Locking your mobile device locks the phone to your Mobile client and prevents any disruption in the registration kiosk operation due to operating system updates or unauthorized user interference. It isn't necessary to lock your mobile device if you merely want to try out the Mobile client as a registration kiosk. However, you should lock the device before deploying the registration kiosk in a production environment.

## 48.4 Register and Organize SAFR Users in your System

Although users can self-register their face at a registration kiosk, they are not automatically registered and approved in the system or granted access privileges. SAFR administrators can classify and control access to resources by using the Person Directory to assign various categories and tags to registrants. For more information on searching, viewing, and organizing registrants, see Manage People in the Person Directory.

For example, you can require every registrant to be assigned a **Person Type** property and base access to certain resources on that property. Think of **Person Type** as a category for your users, such as Staff, Maintenance, Administrator, or anything else you might like to define. The **Home Location** and **Person Type** properties associated with registrants can be adapted to different needs for different organizational purposes. You can also use the **Home Location** and **Person Type** properties to filter information. For example, in a school setting you might use **Home Location** to denote the grade of a student, and **Person Type** might be defined as *student*.

Click **Add Home Location** or **Add Person Type** to add new options or choose from the existing ones. Existing options appear as options in the menu.

### 48.4.1 Best Practices for Organizing your SAFR Registrants

- You can create and customize as many **Person Types** and **Home Location** as you like, but we recommend keeping the number of defined values to less than a dozen or so for each property, for ease of maintainence.

# 49 Customize a Registration Kiosk

Each registration kiosk can be customized to prompt for additional required or optional information from the registrant. You can also customize:

- The registration prompt.
- Registration completion message.
- The default **Person Type** or **Home Location** for the registrant.
- A minimum age requirement for registrants (estimated based on the registrant's face).

## 49.1 Customize the Registration Prompt

To customize the registration prompt, do the following:

1. In the Mobile client, tap the gear icon (settings) > **User Interface**.
2. Enter a new text next to **Prompt**.

## 49.2 Assign Default Person Type or Home Location Values

It may be desirable to assign a default **Person Type** or **Home Location** value to all registrants who complete registration at a particular registration kiosk. For example, if a registration kiosk is located in the admissions office, anyone registered there could be assigned the **Person Type** of *Student* or perhaps *Employee*. Anyone registered at the registration kiosk placed at a specific location could be given a default **Home location** corresponding to the town in which the registration kiosk is located. This can save administrative time. Both **Person Type** and **Home Location** can be changed by the administrator after the registration when needed.

To configure the default **Person Type** or **Home Location**:

1. In the Mobile client, tap the gear icon (settings) > **User Interface**.
2. Enter a value for **Person Type** if desired. By default, **Person Type** is not assigned.
3. Enter a different value for **Home Location**. By default, **Home Location** is set the same as the *Site* label specified in the **Account** settings.

The **Home Location** field associated with every person registered can be used for various purposes. For example, in a school settings, it could be used by the administrator to enter the building name in which a student's home classroom is located. **Home Location** and **Person Type** fields offer filtering based on labels used for these fields and can become important organizational tools. They are named generically to allow labels to be created on the fly by simply entering them. You should decide how to use these labels and then use them consistently to get the most value from them.

**Note:** As a best practice, neither of these fields should have more than two dozen labels for ease of use.

## 49.3 Restricting Registration to a Minimum Age

It may be desirable to prevent registration of people below a certain age. The Mobile client can be configured to asses a person's age and not offer registration to people below a specified minimum age.

To configure the minimum registration age:

1. In the Mobile client, tap the gear icon (settings) > **User Interface**.
2. Enter the desired value for **Min Age**.
3. (Optional) Change **Show Attributes** to *Off*.

   **Tip:** Switching **Show Attributes** to *Off* prevents displaying the assessed age to the registrant. Because some people may be sensitive to this feedback, it is recommended that age not be shown.
4. On the **Recognition** tab, change **Detect Age** to *On*. With age detection set to *On*, the restriction is now active.

## 49.4 Customize the Registration Form

To customize the message your kiosk displays to registrants:

1. In the Mobile client, tap the gear icon (settings) > **User Interface > Form: Customize**.
2. For any fields you want to add to your form, change the *Hidden* indicator to either *Required* or *Optional*. Any field that is marked as *Required* needs to be filled out by the registrant before registration is allowed to be complete.
    - The *Name*, *Company*, *Mobile*, and *Email* fields have fixed meanings. While you can customize prompt names for these fields, information entered for these fields is registered under the prescribed meaning. If you do not want to have this information gathered during registration, keep these fields hidden. Do not re-label them to a different meaning.
      **Note:** *Name* cannot be hidden and must be entered by the registrant.
    - If you need to gather information in addition to these prescribed fields, use the generic fields labeled by default as *Field*. These form entries have no prescribed meaning. Any information provided through these fields appears as tags in the registered person's record. If you want to give the entered information a tag name, complete the *Tag* field for each entry. If *Tag* is completed, information the registrant fills out for this field is prefixed with "Tag=" when appearing in person's record (e.g. Car Make=Ford). If the tag is not filled out, the information provided by the registrant appears on its own in the list of tags associated with the registered person.
3. Enter the names for the fields and add any information placeholder text. (e.g."Type Your Name Here")
4. Change the labels for the actions buttons if desired.
5. Enter the completion message displayed once the registration process is successfully completed.

# 50 Configure a Mobile Device into Locked Mode

Single App Mode for iOS, or Lock Task Kiosk Mode for Android, allow you to lock an iOS or Android device into a single application. When enabled, the mobile device is restricted to running only one application even if it is rebooted. This mode allows the device to be fully locked from any unauthorized access, and it will remain locked until Single App or Lock Task Mode is explicitly disabled.

You can control how users interact with devices using Single App and Lock Task Modes by enabling or disabling any of the following features:

- Screen auto-lock
- Touch input
- Screen rotation
- Volume control
- Sleep/wake button
- Side switch

**Warning**: Putting an iOS device in Supervised Mode wipes all the information on the device and resets it. Likewise, when using an Android device, you must return the target device to factory settings which causes all information to be wiped from the device resets it.

## 50.1 Requirements

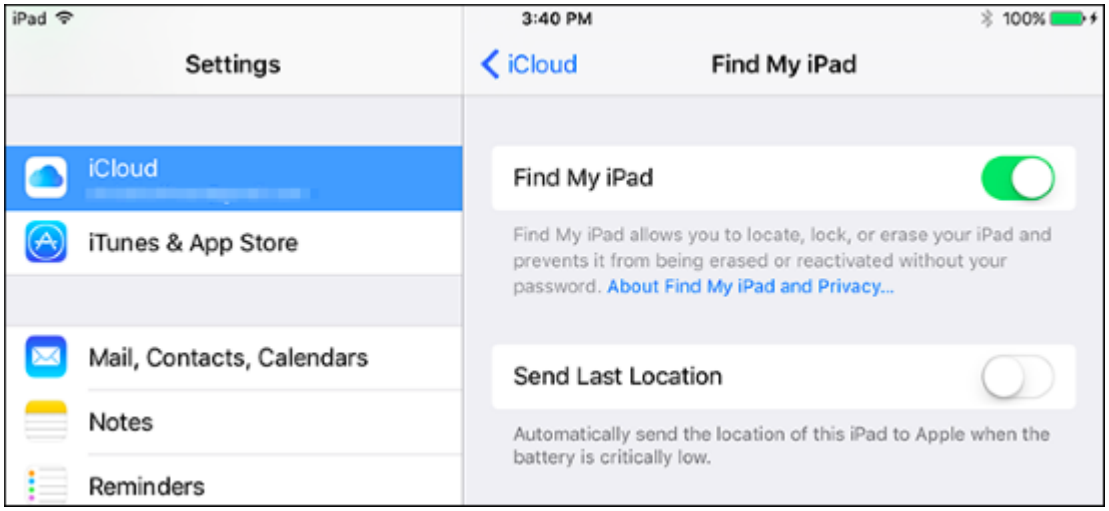
- For macOS, you'll need a Macintosh computer running 10.14 Mojave or later.
- For Android, you'll need 2 Android devices to set up the most secure mode, Lock Task Mode. If you only have a single Android device, then you can only set up the less secure Screen Pinning Mode.

## 50.2 Put an iOS Device into Supervised Mode

While the procedure described here manually puts a mobile device into Supervised Mode, there are other ways to do this via mobile device management (MDM).

To put an iOS device into Single App Mode, the device must first be put into Supervised Mode. To do this, do the following:

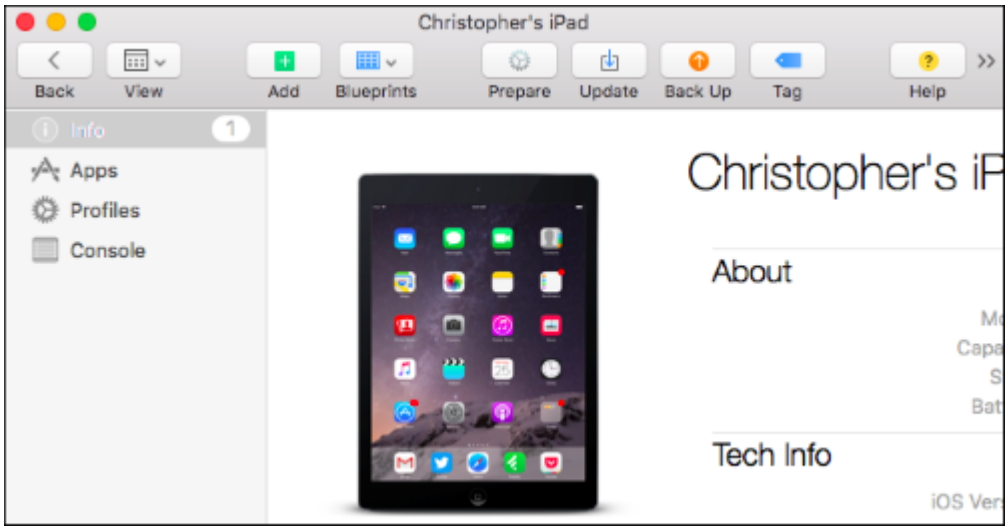
1. Go to **Settings** > **(User)** > **iCloud** > **Find My iPad/iPhone**. Disable the **Find My iPad/iPhone** switch by entering the password.



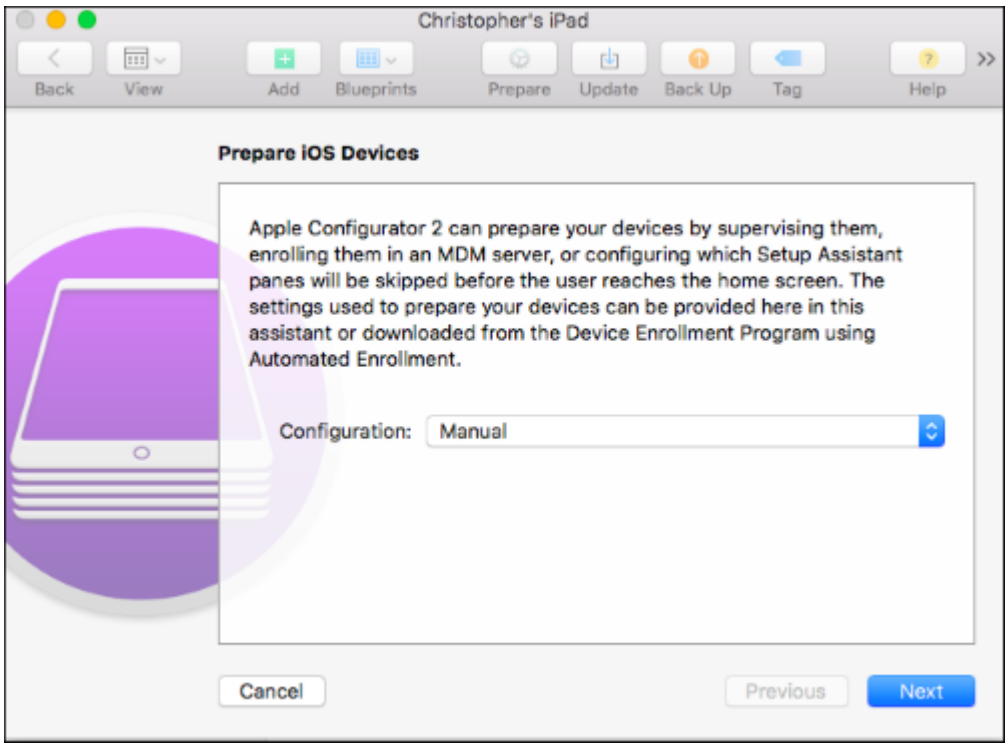

2. On your Mac, launch the **App Store** application and search for **Apple Configurator 2**. Download and install this application on the computer.

3. Plug in your iOS device to your Mac.
4. Launch **Apple Configurator 2**. You should see something that looks like the image below.

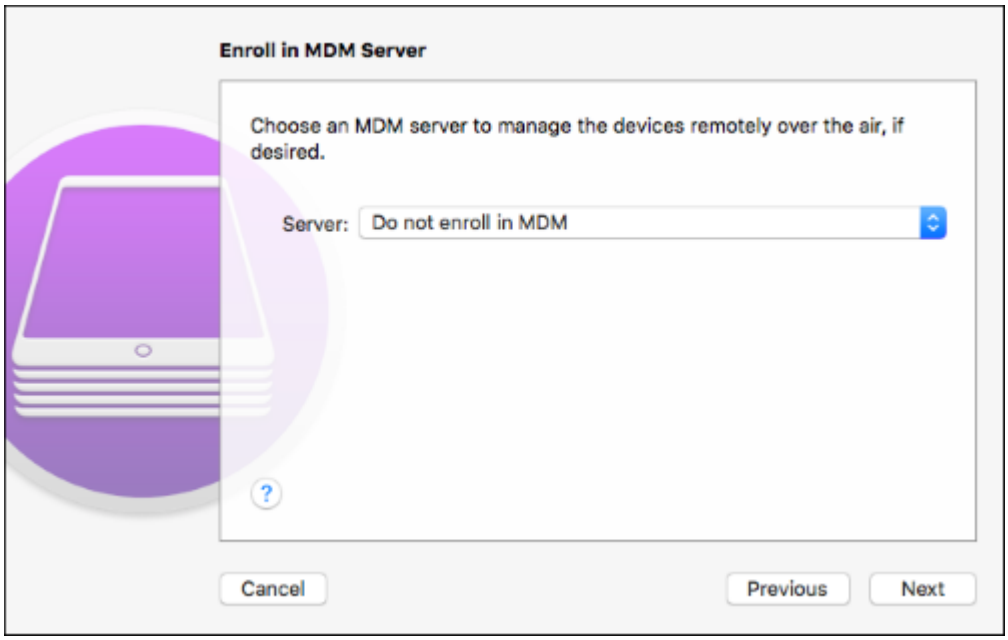

5. Double-click the device.
6. On the **Details** screen about the device, click the **Prepare** button.



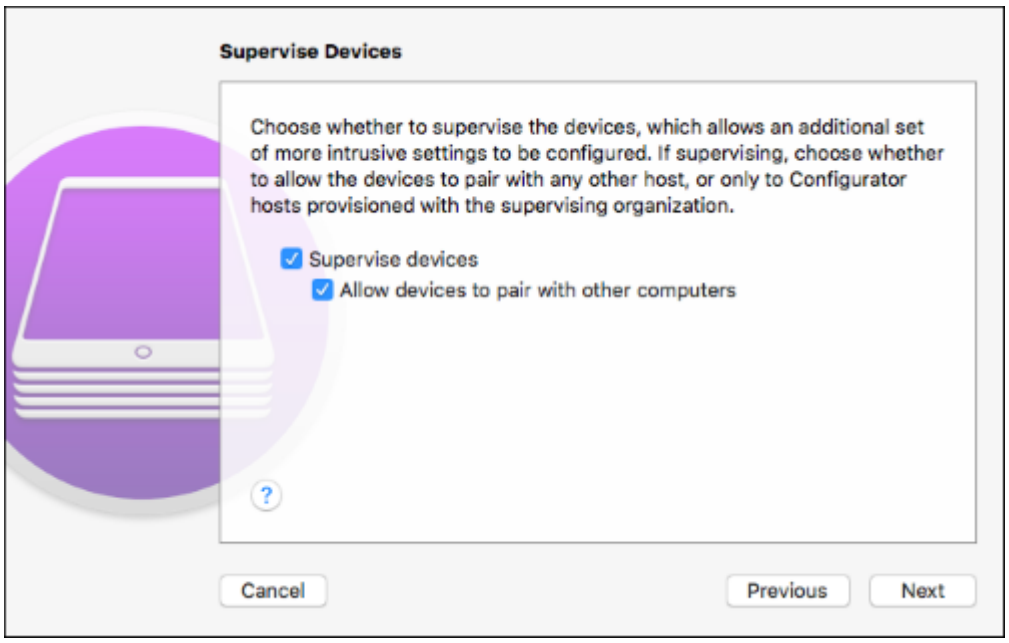

7. From the **Configuration** menu, select **Manual**.



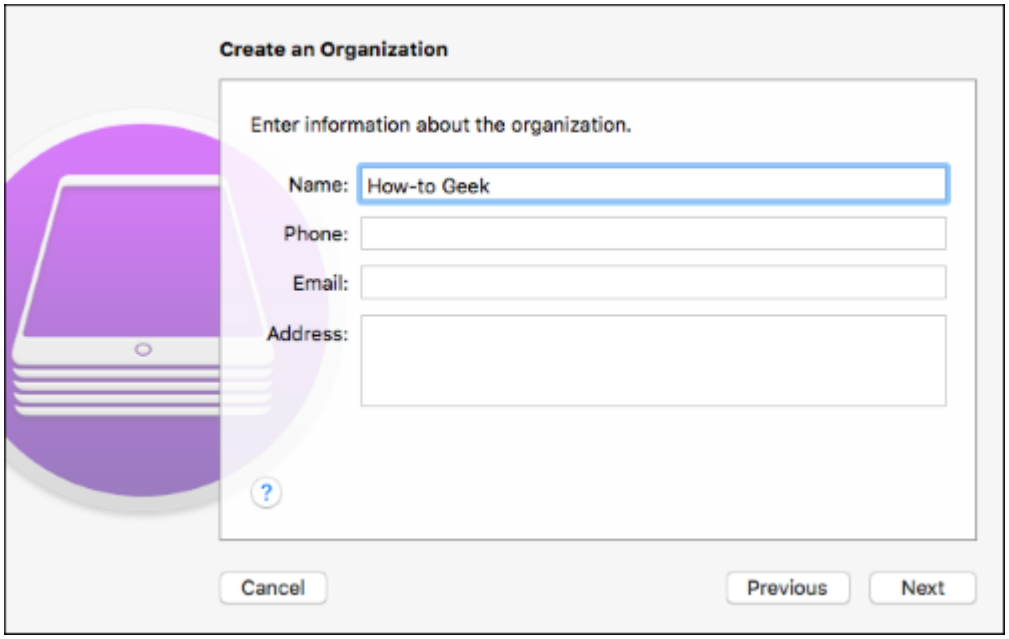

8. From the **Server** menu, select **Do Not Enroll in MDM** unless you have an MDM server you want to use and enroll your device to.



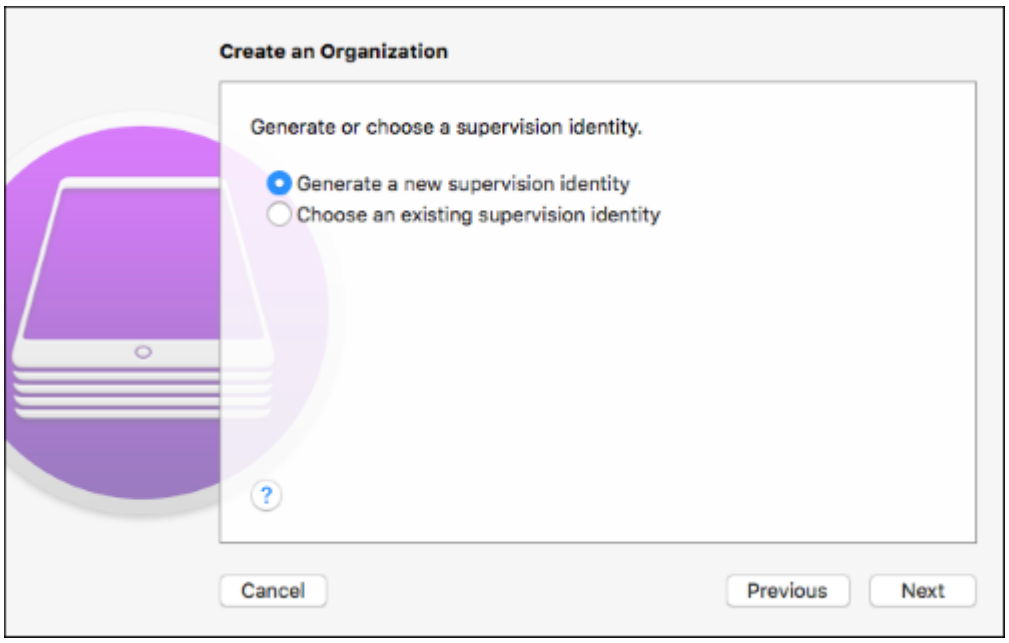

9. If you selected **Do Not Enroll**, you must now plug the mobile device into your Mac to configure it.
10. Click the **Supervise Devices** check box. If you want the device to be configured on multiple computers leave the default **Allow Device to Pair with Other Computers** selected.




11. Enter your organization information.

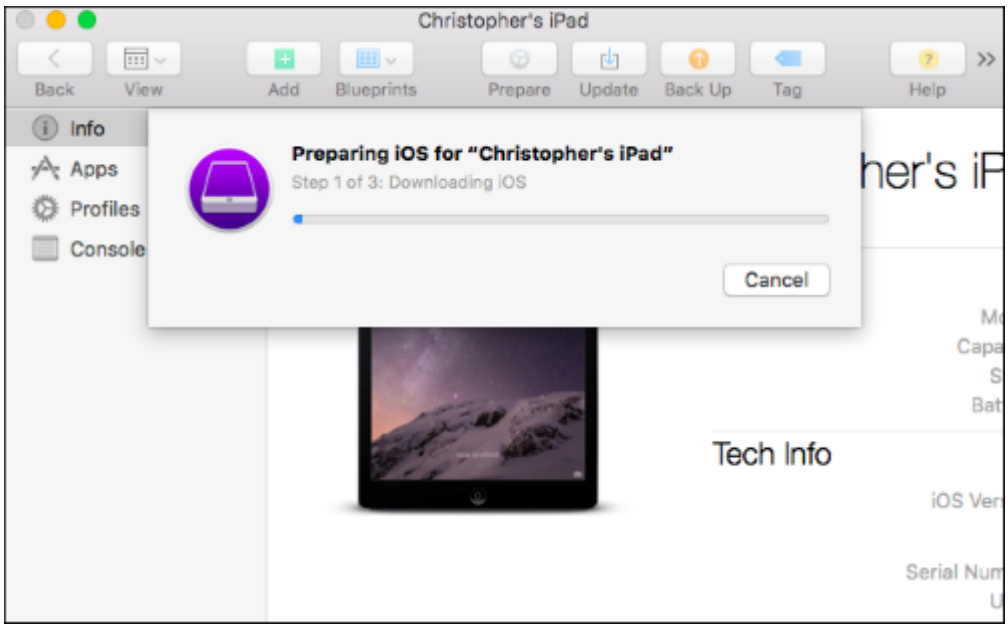



12. If you've previously generated a supervision identity at some point, select **Choose an Existing Supervision Identity**. Otherwise, you'll need to generate one by selecting **Generate a New Supervision Identity**.




13. Select the options you want the device to run after it is reset. The default options are generally sufficient.


14. Click **Prepare**. A status bar will be displayed as ithe iOS device is configured in supervised mode. **WARNING:** Clicking the **Prepare** button wipes all information on the device and resets it.




After the device is wiped and rebooted it will be running in supervised mode.

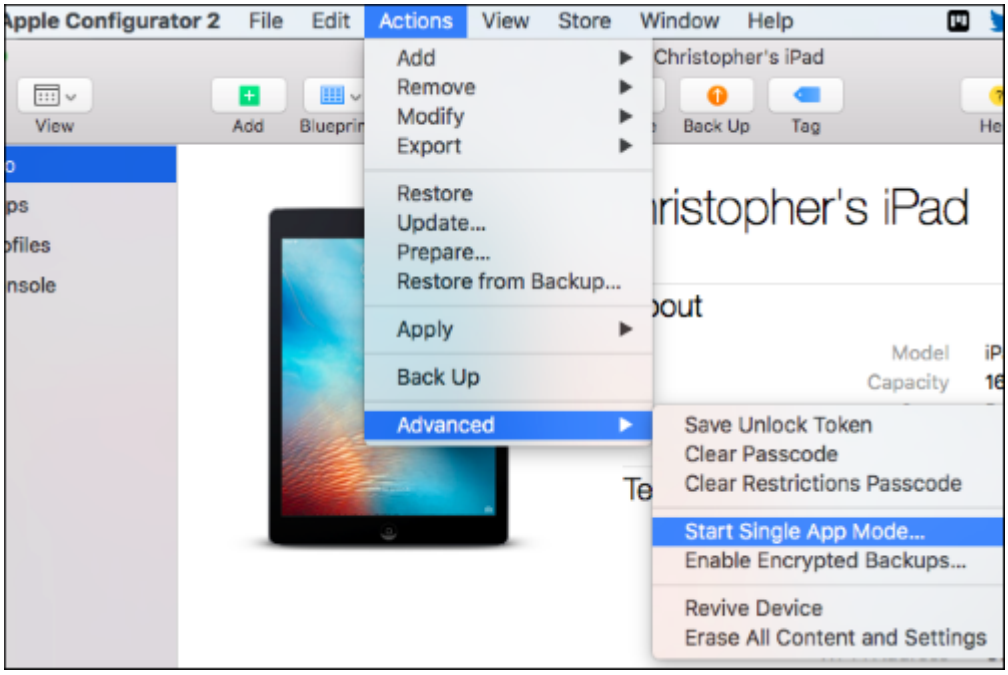
### 50.2.1 Enable Single App Mode

**Note**: To continue from this point, the iOS device should be in supervised mode. If the iOS device is not in supervised mode, repeat the instructions from the prior section first to put it in supervised mode.

To enable or disable Single App Mode, do the following:

1. On your Mac running 10.14 or greater Mojave, launch the *App Store* application and search for *Apple Configurator 2*.
2. Download and install *Apple Configurator 2* to your Mac.
3. Plug in your iOS device to your Mac computer.
4. Launch *Apple Configurator 2*. You should see something that looks like the image below. Double-click the device.

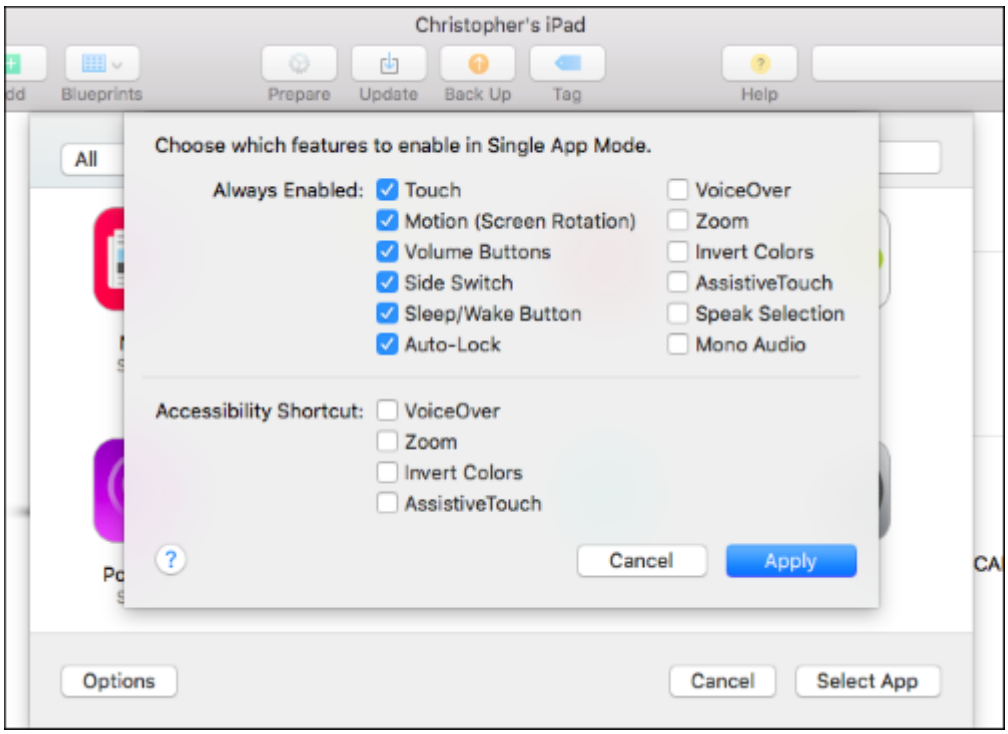

5. On the **Device Details** screen, from the **Actions** menu, click **Advanced > Start Single App Mode**.



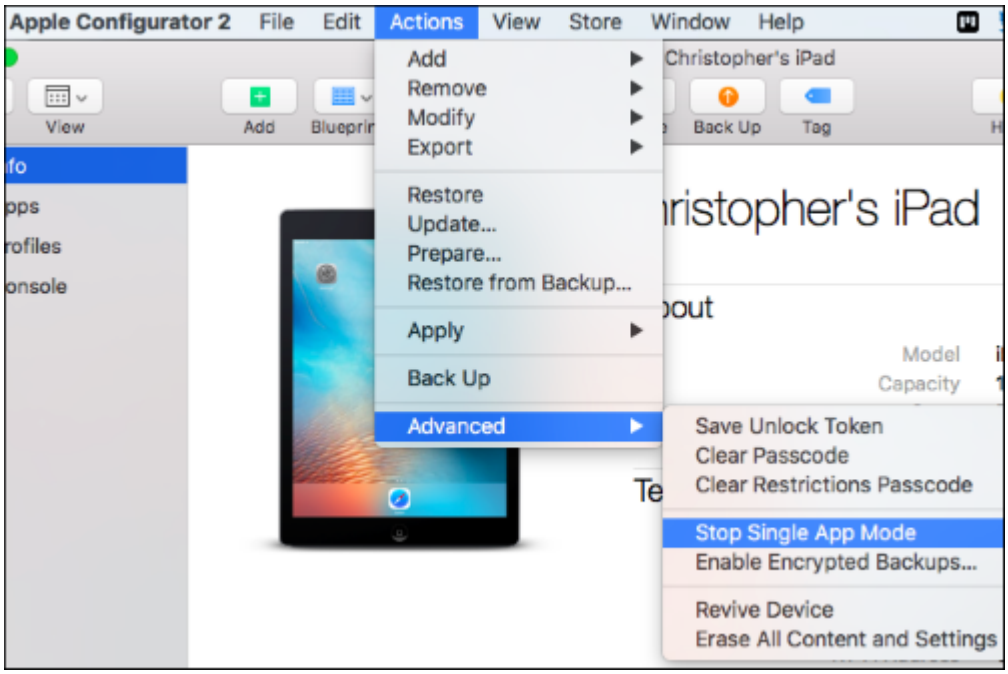

6. Select SAFR from the list of applications.

7. Click the **Select App** button when you're ready to launch SAFR. The iOS device is now locked in Single App Mode.


8. OPTIONAL: If you want to configure advanced options, click **Options**. From the dialog, select the options you want enabled, and click **Apply**. However, usually the defaults are sufficient.




9. When you return to the applications screen, click the SAFR application and click Select **App**.
10. To disable Single App Mode, plug the iOS device into the computer. In the **Actions** menu, click **Advanced > Stop Single App Mode**.




## 50.3 Enable Kiosk Mode for Android

There are two kiosk modes available in the Android Mobile client:

- Lock Task mode (LTM): A robust kiosk mode where only administrators are able to alter the configu-

ration or access the data on the device. The device is locked into one application until the mode is explicitly disabled. You must install the Mobile client using SAFR Beam to use this mode.
- Screen Pinning mode (SPM): A less secure kiosk mode without device administrator registration. When using the device you can exit the mode at any time. Available for any Android device with the Mobile client installed.

**Note**: While this procedure explains how to manually set up a device using SAFR Beam, you can also use the Android Debug Bridge (ADB) command line tool.

To set up and enable Lock Task mode:

1. Go to the SAFR download portal and from the menu, select Android.
2. Install SAFR Beam on your primary device.
3. Set your target device in factory reset prior to use.
4. Follow the instructions on the primary device for installing the Mobile client on a target device.
5. Once the Mobile client is installed on the target machine, click the lock icon next to the settings gear icon. Follow the instructions for setting the device up for Lock Task mode.
   **Note**: In this mode, the client has full control over the device and only the client can request exiting the mode.
6. Exiting can be done by tapping the screen three times (3-taps gesture) which displays the system's security dialog. (assuming that one has been configured) In the dialog, you are prompted to confirm your identity by entering the device's credentials (PIN, gesture, or fingerprint). If the device does not have security settings in place or your identity is confirmed, the Mobile client restarts in an unlocked state.

**Important**: You should configure device security either with a PIN, a gesture, or a fingerprint. That way, if a device is turned off while the Mobile client is locked (either by the power button or as the result of drained battery), only a credible user is able to start the device and re-run the Mobile client. When re-run, the Mobile client enters the mode it was in prior to turning off the device.

**Note**: If you install the Mobile client apart from SAFR Beam, you can still set up security by clicking the lock icon. However, because the Mobile client has not been registered as a device administrator, its security is not as strong as the Lock Task mode.

The following scenarios occur when using the kiosk modes when the Mobile client is or is not registered as a device manager:

| Scenario | Action |
|---|---|
| No device security configured (not registered); you confirm to enter SPM on the security dialog | Exits via 3-taps gesture, or by holding the Recents and Back keys at the same time; the Mobile client is restarted in unlocked state (Screen Pinning mode) |
| No device security configured (not registered); you deny entering SPM on the security dialog | The Mobile client is in locked state but is restarted in unlocked state after approximately ten (10) seconds; a timer is triggered that queries for locked state and corrects it if needed |
| PIN device security configured (registered); you confirm to enter SPM on the security dialog | Exit by 3-taps gesture or by holding the Recents and Back keys at the same time; SAFR prompts you to confirm your identity by entering PIN and if successful, it is restarted in unlocked state |

**Note**: On some devices, SPM can be explicitly enabled in system's setting with an option to ask for a PIN upon unlocking/PIN device security configured. If you confirm to enter SPM on the system dialog by exiting by holding the Recents and Back keys at the same time, you are prompted to confirm your identity by entering PIN. If successful, the device home screen is displayed. The next time, SAFR restarts in an unlocked state.

# 51 Install SAFR Beam

Install the SAFR Beam for Android utility onto one device and use this primary device to install the Mobile client in a Lock Task kiosk mode on a second target device. Using SAFR Beam provides added security to the target device, locking it down in cases where added security is required. For example, using the device camera to identify employees and open secured door to them. For more information, see Configure Devices into Locked Mode section.

## 51.1 To Install and Use SAFR Beam

1. Secure two Android devices capable of running SAFR. One device serves as the primary and the other as the target. For more information, see SAFR System Requirements.
2. Log into the SAFR download portal and install SAFR Beam on the primary device.
3. On the primary device, turn on Near Field Communication (NFC). Make sure the target device has NFC capabilities.
4. Reset the target to its factory settings.
5. Place the target device back to back with the primary device.
6. Once the target device is detected, tap the screen on the primary device to start the beam.
7. Follow the instructions on the target device to complete the installation.
8. Although not required, we highly recommend that you set up security access on the target device. (e.g. a PIN or gesture)
9. Run the Mobile client on the target device. If prompted, set SAFR as the default launcher app.

# 52 Mobile Account Preferences

The Account preferences tab is where you configure your organization's SAFR accounts and related information, such as the directory for your facial recognition database.

- **Environment**: Determines which operating environment your client contacts. The possible values for this field are as follows:
  - *SAFR Developer Cloud*: Internal use only.
  - *SAFR Partner Cloud*: Internal use only.
  - *SAFR Cloud*: Used for cloud deployments. This is a general availability SAFR Server in the cloud maintained by RealNetworks. It is a stable, high availability environment intended for production use.
  - *SAFR Custom*: Used for local deployments. If you select *SAFR Custom*, you will be asked to provide the URLs for the primary SAFR Server services.
- **User Identifier**: The account can have multiple user identifiers with different access privileges.
- **User Password**: The password for the user entered in the *User Identifier* field.
- **User Directory**: The directory in the account where the data used for facial recognition is stored.
- **User Source**: The *User Source* label for this mobile device. All SAFR event data is tagged by site and source labels. These labels are used to help filter and analyze collected recognition events, such as where a face was recognized.
- **User Site**: The *User Site* label for this mobile device. All SAFR event data is tagged by site and source labels. These labels are used to help filter and analyze collected recognition events, such as where a face was recognized.
- **Enable Active Camera Connect**: Only available on Android devices. When enabled, the mobile device's connected rtsp:// camera will continue to be processed even when the Mobile client is in the background or when the mobile device is asleep.
- **Report Status**: Enables a preview of the video stream in the video feed status window. The feed view is a simple low frame-rate stream (1 frame per second). It is only intended for inspecting camera orientation and lighting conditions. It is not intended for actively monitoring feeds for security purposes.
  - **Allow Remote Viewing**: Enables remote monitoring for your mobile device's video feed.

# 53 Mobile Detection Preferences

Use detection preferences to enable and configure facial detection characteristics.

- **Enable Face Detection**: The check box must be selected to enable face detection.
- **Min Searched Face Size**: Defines the minimum face size that can be detected. A searched size of 80, for example, can still manage to detect faces as small as 60x60, but with lower certainty. Lowering this number enables SAFR to detect much smaller faces but also greatly increases CPU usage.
  **Note**: This setting does not impact face recognition accuracy.
- **Min Required Face Size**: Defines the minimum required size for a face to be detected. Any face smaller than the height or width is ignored.
- **Generate Recognizer Hint**: Optimizes facial recognition. It should be turned on for most cases. If it is turned off, recognition accuracy may be reduced if detection is performed at very low resolutions.

# 54 Mobile Recognition Preferences

Use Recognition preferences to adjust the range for a variety of settings that determine whether or not SAFR detects, tracks, and recognizes faces and identities.

- **Detect Identity**: Select to enable identity detection.
- **Detect Gender**: Select to enable gender detection.
- **Detect Age**: Select to enable age detection.
- **Detect Sentiment**: Select to enable sentiment detection.
- **Detect Smile Action**: Select to enable smile detection.
- **Pre-smile Delay (seconds)**: The amount of time that there should be no smile.
- **Smile Duration (seconds)**: The amount of time that the smile should last.
- **Identity Threshold Boost**: The smile threshold to boost temporarily during the smile action.
- **Minimum Recognition Face Size (pixels)**: Defines the minimum required face size in pixels to attempt recognition. It includes a 25% margin around the face.
- **Minimum Learning Face Size (pixels)**: Defines the minimum required face size in pixels to enable SAFR to store a reference image for a new identity. It includes a 25% margin around the face.

# 55 Mobile Events Preferences

Use the Events preferences tab to configure event reporting as well as how your client listens for event replies.

- **Report Events**: Enables event reporting. Event reporting enables SAFR to log and track events over time and gain additional insight into your SAFR system and usage patterns.
- **Include Unrecognizable Events**: Enable to report the appearance of unrecognizable people captured by camera feeds. Unrecognized people are people that the SAFR system can't see well enough to compare it to its Person Directory.
- **Include Stranger Events**: Enable this option to report when the appearance ofstrangers. Strangers are people that the SAFR system can see well enough to compare to individuals stored in the People Directory, but for whom there isn't a match.
  - **Min Age**: The minimum age of strangers that will trigger stranger events. If a stranger younger than the specified minimum age is detected, no stranger event is generated.
  - **Max Age**: The maximum age of strangers that will trigger stranger events. If a stranger older than the specified maximum age is detected, no stranger event is generated.
- **Include Speculated Identity Events**: Enables reporting events for speculated people. A "Speculated Identity" is a face that isn't a 100% match with a face in the Person Directory, but is close.
- **Preserve Event Face Image**: Enable if you want the images that trigger an event to be saved with the event report.
- **Preserve Event Scene Thumbnail Image**: Enable if you want a thumbnail of the scene image in which the event occurred to be saved with the event report.
- **Reporting Delay**: The number of seconds an event report is delayed in order to properly assess the nature of the event. For example, a person who may at first seem unknown may become known after a second observation.
- **Min Identified Event Duration**: The minimum duration required for an event representing a known person to be recorded as an event.
  This setting helps filter out noise or brief appearances that may not be worth reporting as a system event.
  If this setting and *Reporting Delay* have different settings, the greater number is used.
- **Min Unrecognizable/Stranger Event Duration**: The minimum duration of an event representing an unrecognizeable person to be recorded as an event.
  If this setting and *Reporting Delay* have different settings, the greater number is used.
- **Min Stranger Event Duration**: The minimum duration of an event representing a stranger to be recorded as an event.
  If this setting and *Reporting Delay* have different settings, the greater number is used.
- **Listen For Event Replies**: Select to enable listening for event replies. Listening for event replies enables the client to display reply messages on the screen.
- **Display Reply Message**: Select to enable the display of reply messages on the screen.
- **Reaction Delay**: Delays the event reporting to the server by the specified number of seconds.

# 56 Mobile User Interface Preferences

The User Interface preferences tab is where you can customize your user interface.

- **Enable Registration**: Select to enable unknown users to register their faces.
- **Min Age**: The minimum age for unknown users to register their own faces.
- **Highlight Border Thickness**: Use the slider to set the thickness (in pixels) of the frame displayed around faces.
- **Overlay Text Size**: Specifies the size of the text in the video feed overlay.

# 57 Web Console

The Web Console provides administrators and operators web-based access to the SAFR system. It allows you to make changes to your account, manage the Person Directory, view events in the Events Archive, manage video feeds, and generate reports.

## 57.1 Access the Web Console with a Cloud Deployment

To access the Web Console with a cloud deployment, do the following:

1. Go to the **Products** tab of the SAFR Download Portal.
2. Click on the **System Console** link located under the first listed product, **SAFR Cloud**.
3. Log in using your SAFR Cloud Account credentials.

It's also possible to go straight to the Web Console login page located at https://safr.real.com/console.

## 57.2 Access the Web Console with a Local Deployment

To access the Web Console with a local deployment, do the following:

If you're on the same machine as your primary SAFR Server:

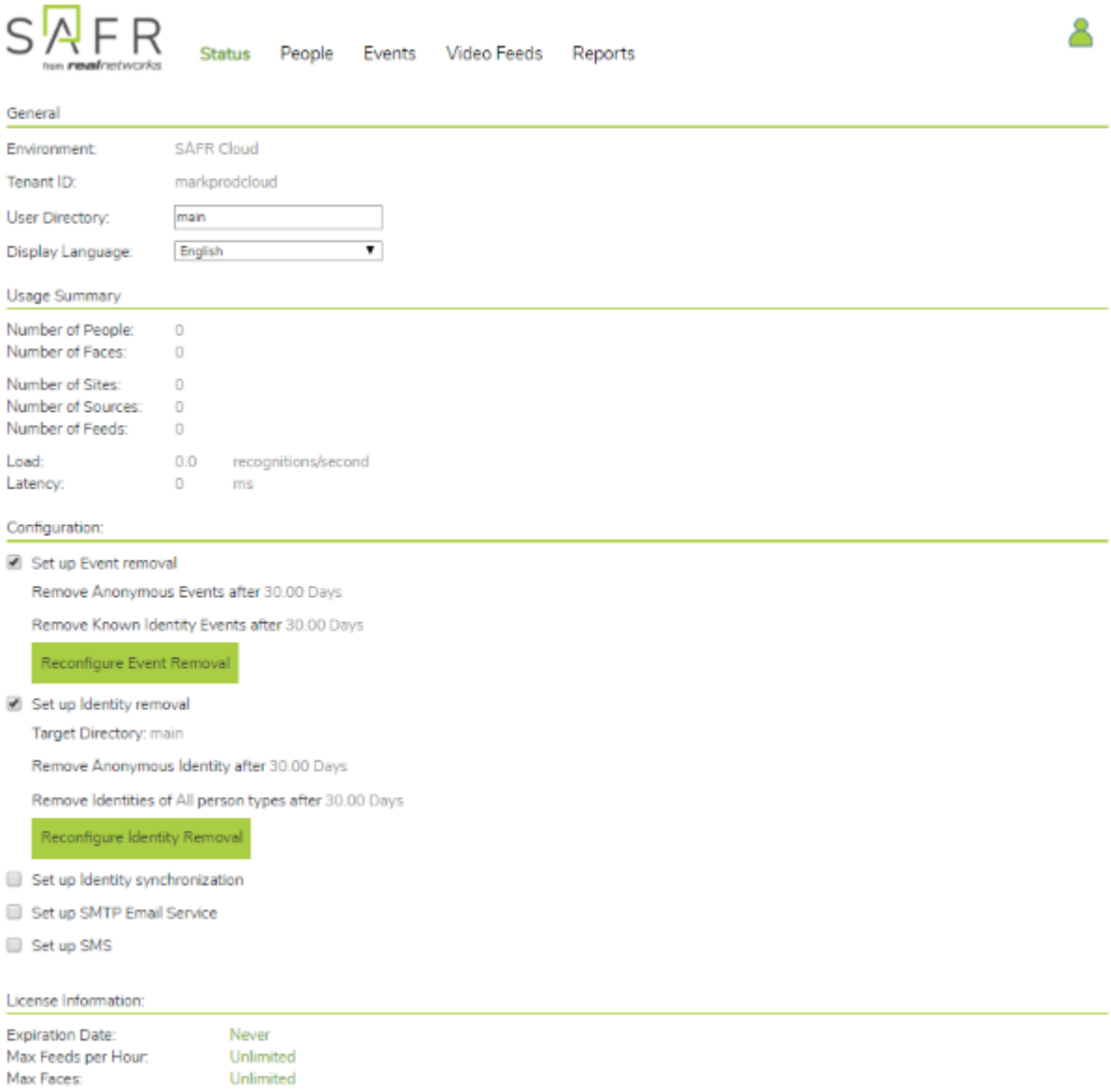
1. Open a web browser.
2. Go to either http://localhost:8090/ or http://localhost:8091/.
3. Sign in using your SAFR Local Account credentials.

If you're on any machine other than your primary SAFR Server:

1. Open a web browser.
2. Go to either `http://<ServerIP>:8090` or `http://<ServerIP>:8091`, where `<ServerIP>` = the IP address of your primary SAFR Server.
3. Sign in using your SAFR Local Account credentials.

# 58 Status Page

The Status page includes general system, directory, and licensing information. It also allows you to set a deadline for event removal and to set the system's display language.




## 58.1 General

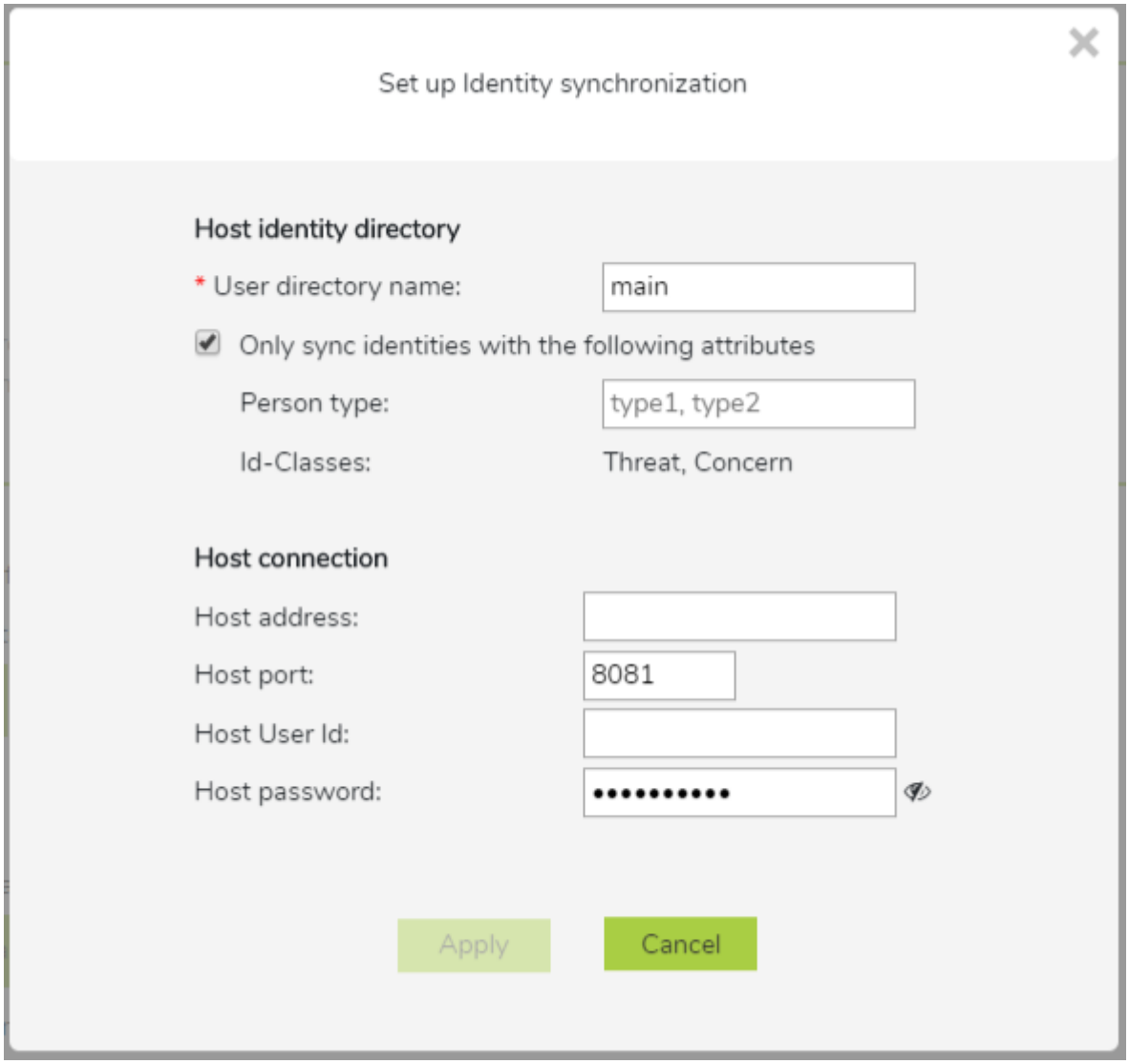
- **Environment**: Environment associated with the user's account. There are two possible values for this field:
  - *SAFR Cloud*: A SAFR Server in the cloud maintained by RealNetworks. Cloud deployments use this environment.
  - *SAFR Local*: A locally installed SAFR Server that the user maintains. Local deployments use this environment.
- **Tenant ID**: The name of the person currently logged in.
- **User Directory**: User directory where the user's data is stored. The default value for this is `main`.
- **Display Language**: Language used by SAFR.

## 58.2 Usage Summary

- **Number of People**: Number of people currently registered.
- **Number of Faces**: Number of faces currently stored in SAFR's database.
- **Number of Sites**: Number of defined sites. A site can consist of one or more cameras, although usually it consists of multiple cameras.
- **Number of Sources**: Number of defined sources. A source can consist of one or more cameras, although usually it consists of a single camera.
- **Number of Feeds**: Number of feeds currently running across the SAFR system.
- **Load**: Number of recognition attempts every second across all video feeds that are currently active in your SAFR system.
- **Latency**: Number of milliseconds it takes for your SAFR Server to generate a response after it receives a recognition request from a client.

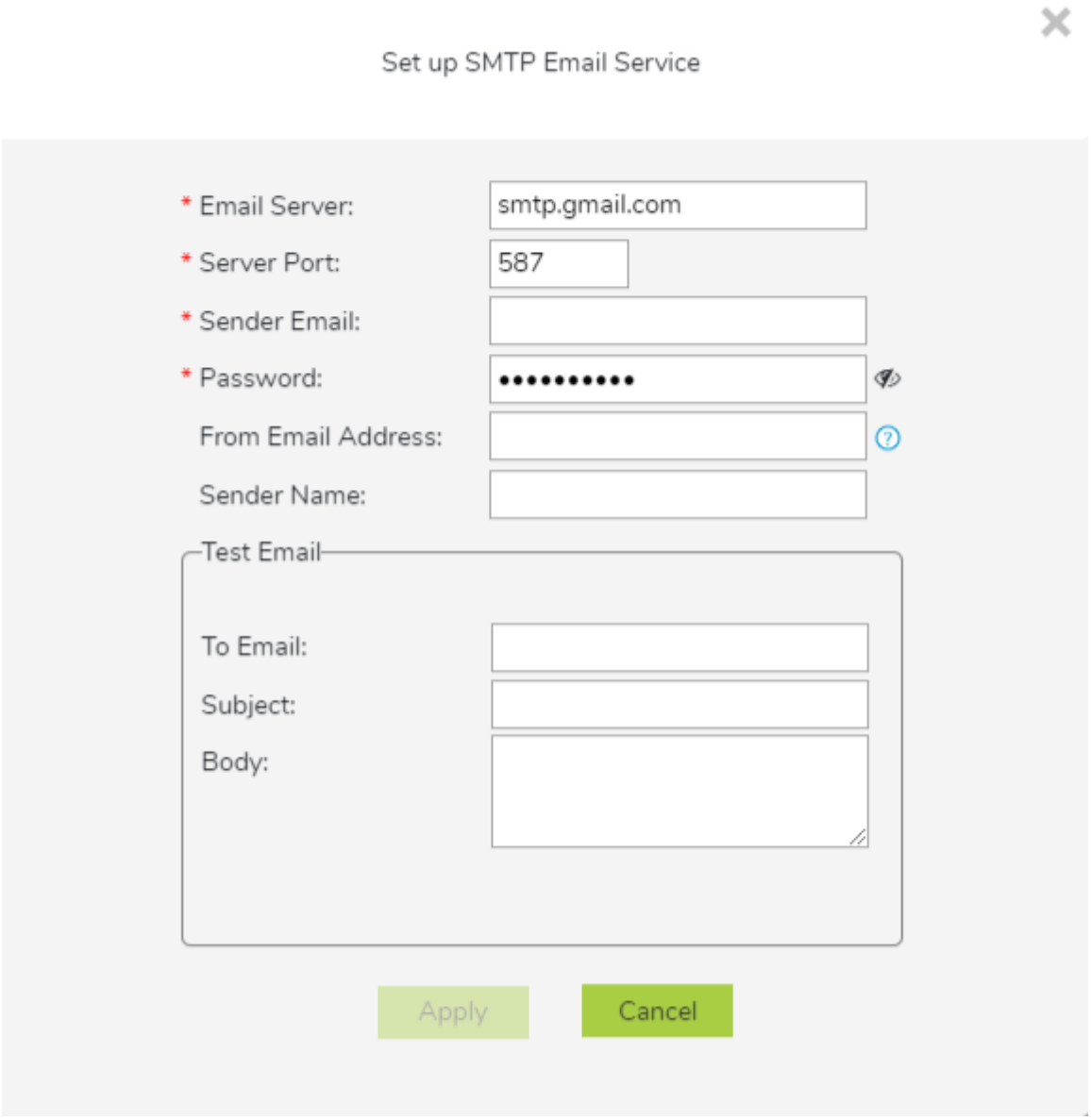
## 58.3 Configuration

- **Set up Event removal**: Enables the automatic removal of events after the specified time interval.
  - **Remove Anonymous Events after**: Determines how many days to wait before removing events triggered by people without a *name* attribute. Floating point numbers are valid. If this value is set to zero, then anonymous events won't be automatically removed.
  - **Remove Known Identity Events after**: Determines how many days to wait before removing non-anonymous events. Floating point numbers are valid. If this value is set to zero, then non-anonymous events won't be automatically removed.
- **Set up Identity removal**: Enables the automatic removal of identities after the specified time interval.
  - **Target Directory**: Determines the directory whose identities are to be automatically removed.
  - **Remove Anonymous Identity after**: Determines how many days to wait before removing identities that don't have a *name* attribute. Floating point numbers are valid. If this value is set to zero, then anonymous identities won't be automatically removed.
  - **Remove Identities of person type**: Select the *Person Type* of the identities you'd like removed. If you don't modify this field, then identities of all *Person Types* will be removed.
  - **after**: Determines how many days to wait before removing identities of the specified *Person Type*. Floating point numbers are valid. If this value is set to zero, then identities with *Person Types* won't be automatically removed.
- **Set up Identity synchronization**: Enables the identity synchronization feature. When enabled and configured correctly, your Person Directory will sync with another Person Directory. The Person Directory that you're syncing with can belong to another SAFR system, or it can belong to a different user directory within your own SAFR system. Selecting the *Set up Identity synchronization* box causes the following dialogue to appear:



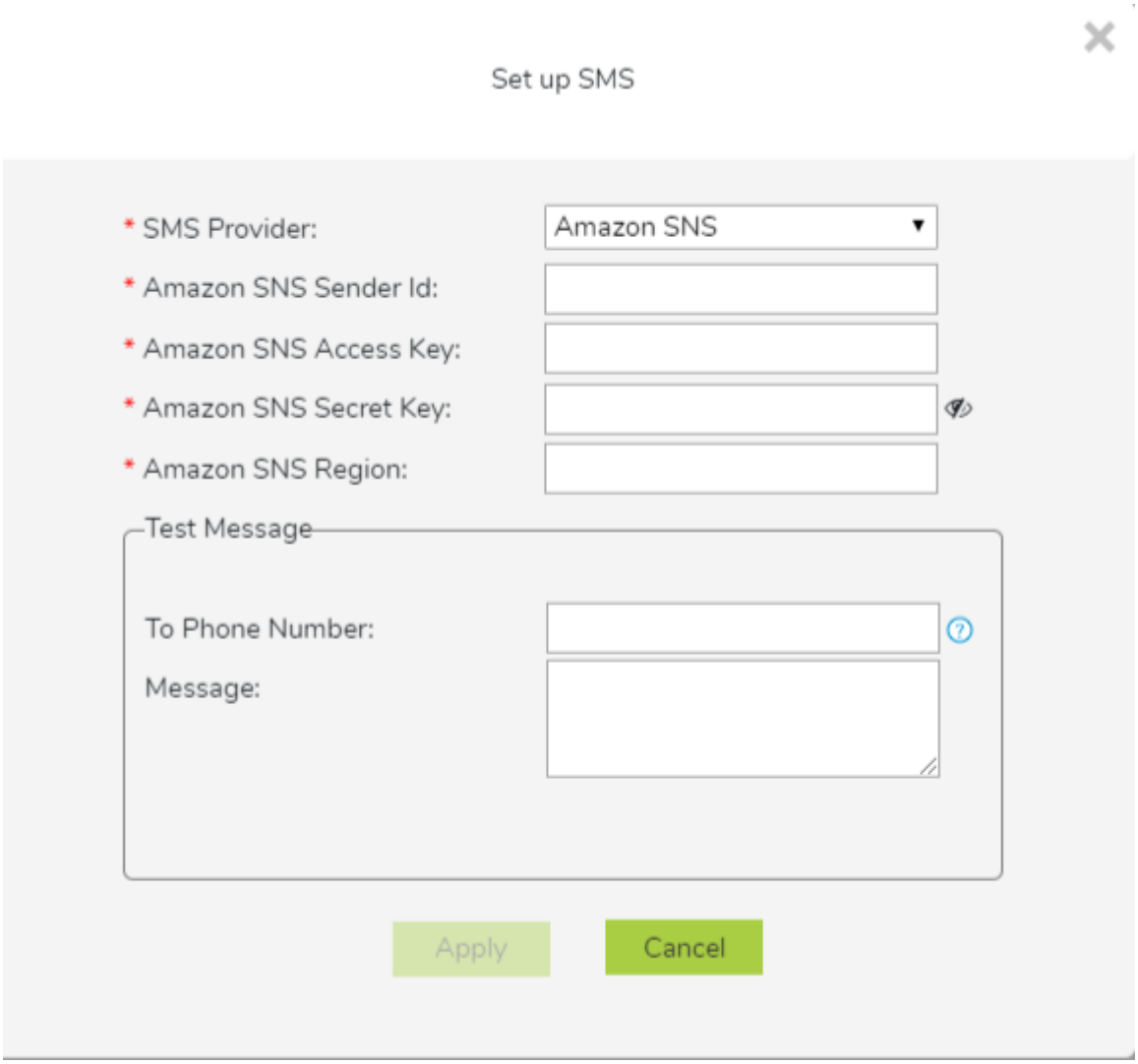

- **User directory name**: The name of the user directory that you're trying to sync identities with.
- **Only sync identities with the following attributes**: When selected, it causes only identities with the specified attributes to be synced.
  - **Person type**: The *Person types* that identities must have to be synced.
  - **Id-Classes**: The *Id Classes* that identities must have to be synced.
- **Host address**: The IP address or the hostname of the target host machine.
- **Host port**: The port number that the target machine's CoVi server listens on.
- **Host User Id**: The *User Id* of somebody who has the credentials to log into the host machine.
- **Host password**: The *Password* of somebody who has the credentials to log into the host machine.

- **Set up SMTP Email Service**: Enables SAFR's actions to send emails. Before you can configure SAFR to send emails, make sure you obtain an SMTP server account that you can use to send emails. When you click on *Set up SMTP Email Service*, a dialogue will pop up requesting configuration information.




- **Email Server**: The address of the SMTP email server.
- **Server Port**: The email server port. The default port for SMTP is 587.
- **Sender Email**: The email username of the SMTP account. (e.g. me@gmail.com)
- **Password**: The password for the SMTP account.
- **From Email Address**: The email address that will appear on the "From" line. This feature isn't supported by all email servers; if this field isn't used then the *Sender Email* value is used for the "From" line.
- **Test Email**: Configure the test email that will be sent after you finish setting up the SMTP email service.
  - **To Email**: The email address to which the test email will be sent.
  - **Subject**: The test email's subject.
  - **Body**: The test email's body.

- **Set up SMS**: Enables SAFR's actions to send short message service (SMS) messages. Before you can set up SMS, you must first set up an AWS account which is configured for your region so it can send SMS messages.
  When you click on *Set up SMS*, a dialogue will pop up requesting configuration information.




- **SMS Provider**: The SMS provider that you're using. This value will always be `Amazon SNS`.
- **Amazon SNS Sender Id**: The name that will be used to send the SMS notifications.
- **Amazon SNS Access Key**: Your Amazon SNS Access Key.
- **Amazon SNS Secret Key**: Your Amazon SNS Secret Key.
- **Amazon SNS Region**: The region of your Amazon SNS.
- **Test Message**: Configure the test message that will be sent after you finish setting up SMS.
  - **To Phone Number**: The phone number to which the test message will be sent.
  - **Message**: The text message that will be sent to the phone number specified above.

## 58.4 License Information

Shows the operating limits of your SAFR license. See Licensing for additional information about SAFR licenses.

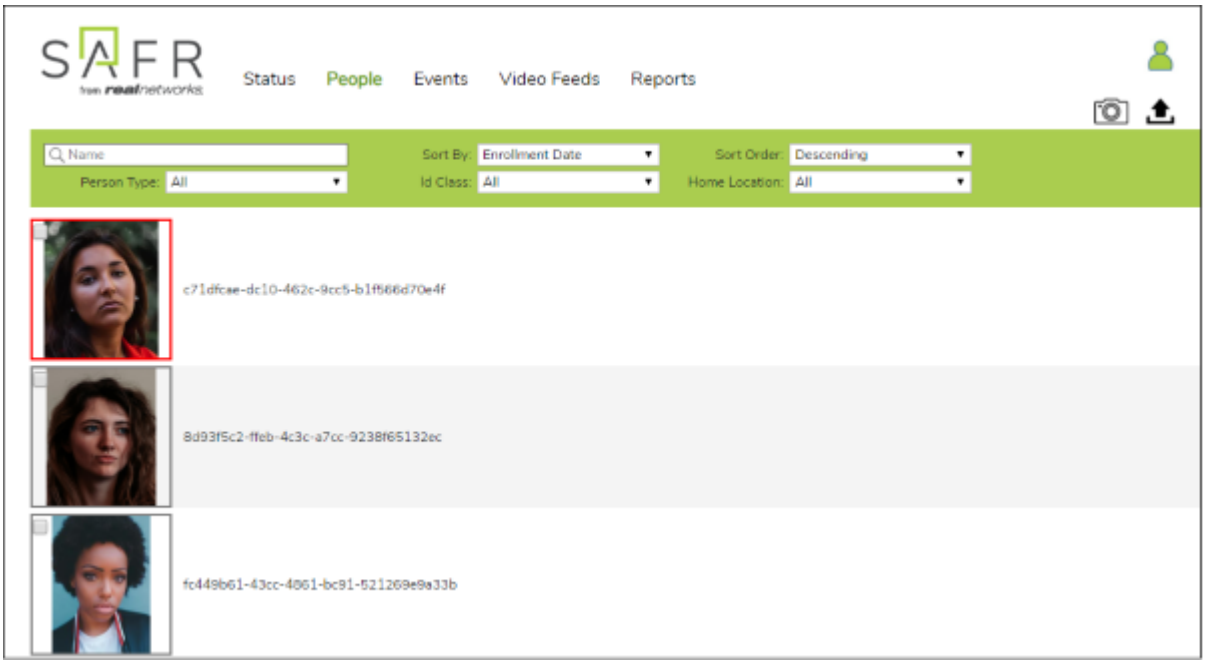
- **Expiration date**: The date when the SAFR license expires. After this date, SAFR software discontinues operation.
- **Max Feeds per Hour**: Maximum number of video feeds that can be used at one time by the SAFR system. If you attempt to connect more video feeds than your license allows, the excess video feed connection attempts will all fail. Existing video feeds must be disconnected for a period of 1 hour before new video feeds are allowed to re-use the license.
  **Note**: If a single camera is providing video feeds to 2 different Desktop client instances, that counts as

2 video feeds for licensing purposes.

- **Max Faces**: Maximum number of faces that can be stored in SAFR's database. Attempting to save more faces than this limit allows results in an error.
- **Max Days Between Reports**: The maximum elapsed time that can pass before the SAFR system can report its status to a SAFR License Server. SAFR Server discontinues operation if it is unable to reach the SAFR License Server after the specified time has elapsed. If you need to operate your SAFR system on a private network that isn't connected to the Internet, contact your SAFR account manager to acquire a special offline license.
  **Note**: This metric is only applicable for local deployments, and won't appear on the Web Consoles of cloud deployments.

# 59 People Page

The People page provides the ability to view and edit information about all the registered people in the Person Directory. For more information, see Manage People in the Person Directory.



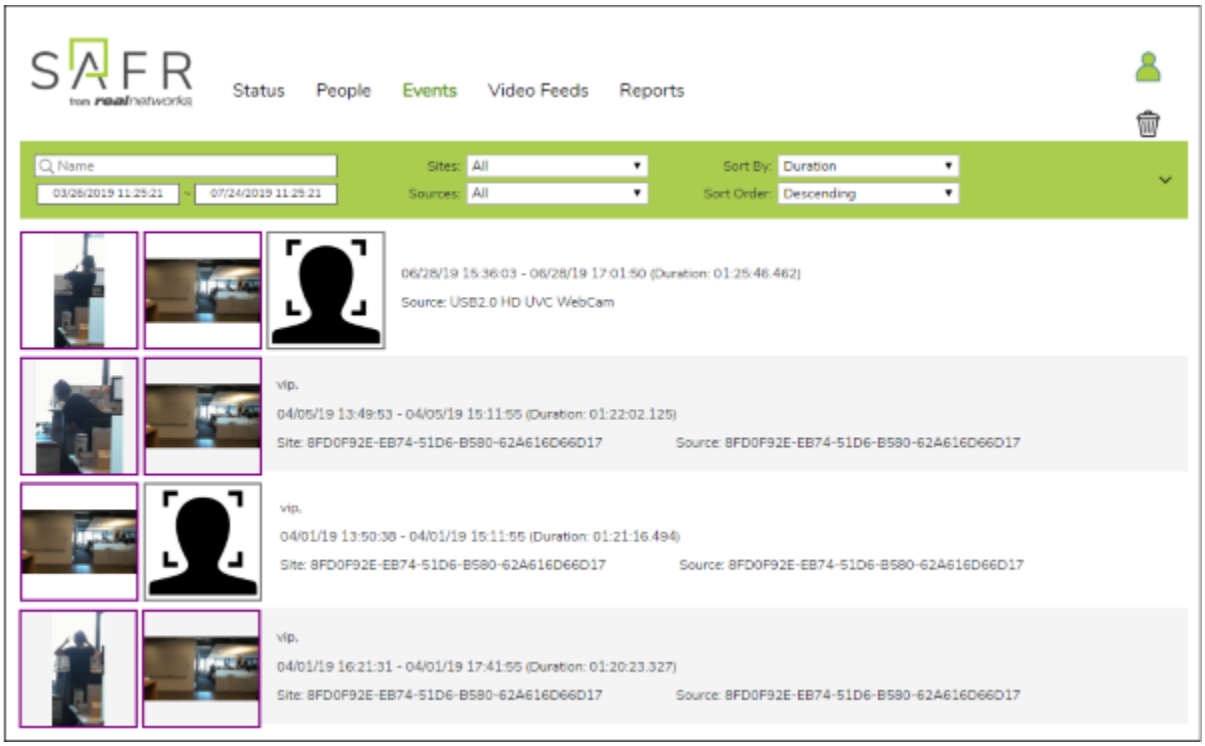

In addition, you can:

- Click the camera icon to take pictures of faces using your integrated camera to register people to the Person Directory.
- Click the upload icon to import images from files. Click the setting icon to adjust the acceptable lower limits of the center pose, contrast, and sharpness image quality metrics.

See Importing and Registering People for more information.

# 60 Events Page

The Events page lists all reported events stored in your Event Archive.



# 61 Video Feeds Pages

The Video Feeds pages provide processor status and tenant configuration capabilities for all your connected video feeds. Root Config provides a list of all SAFR global default processor and feed properties.

The system is organized as follows:

- Tenants can have directories.
- Users and user IDs are security principals. They have privileges and map to a tenant. They have access to all directories within the tenant.
- If you have super privileges, you're also able to read, write, or config other tenants' properties for APIs that allow for those changes.
- A user ID can be restricted to particular directories within a tenant using white-listing.

**Note**: For cloud deployments, the Root Config properties are read-only. For local deployments, the Root Config property defaults can be changed by users with super config privileges. However, you are advised to make Root Config changes only when necessary.

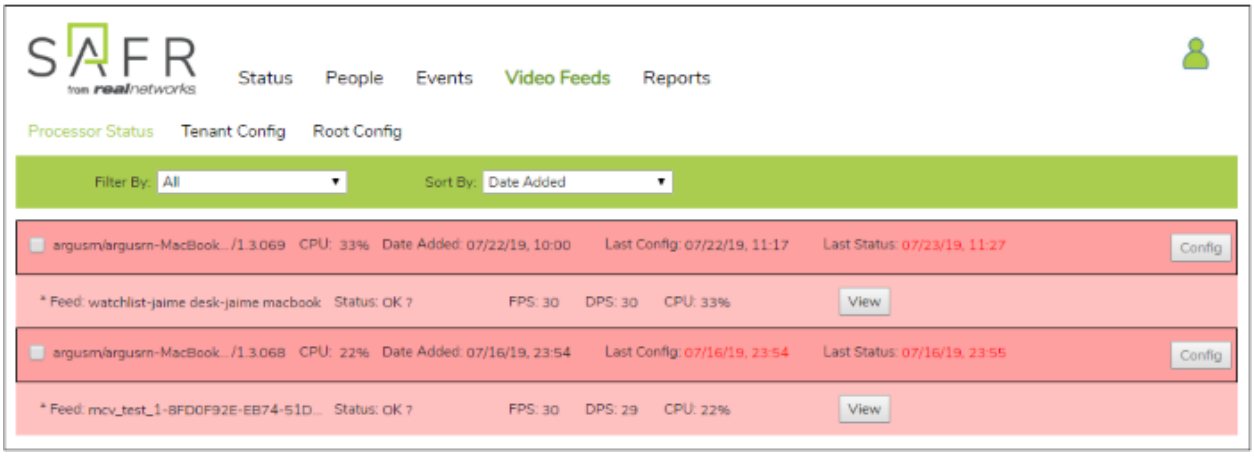
The Root and Tenant configs and modes are set on the tabs. Worker config is set by clicking the **Config** button on the **Processor Status** page.

- Tenant Config properties override Root Config properties or Feed properties for your account.
- Root mode overrides settings set on the Root and Tenant Config pages. Tenant mode overrides settings on other pages.
- Like the source URL, the Worker Config sets instance properties, although you can override any settings. This is useful to override settings for an individual device if, for example, there are unique lighting conditions for one feed.

## 61.1 Processor Status Page

This page provides a list of Desktop client instances and video feeds associated with the account. Each row represents a separate computer running the Desktop client that has a video feed associated with it. Inactive video feeds are identified by a red date-time status. Feeds are made inactive by either having status reporting disabled or shutting down the associated Desktop client.

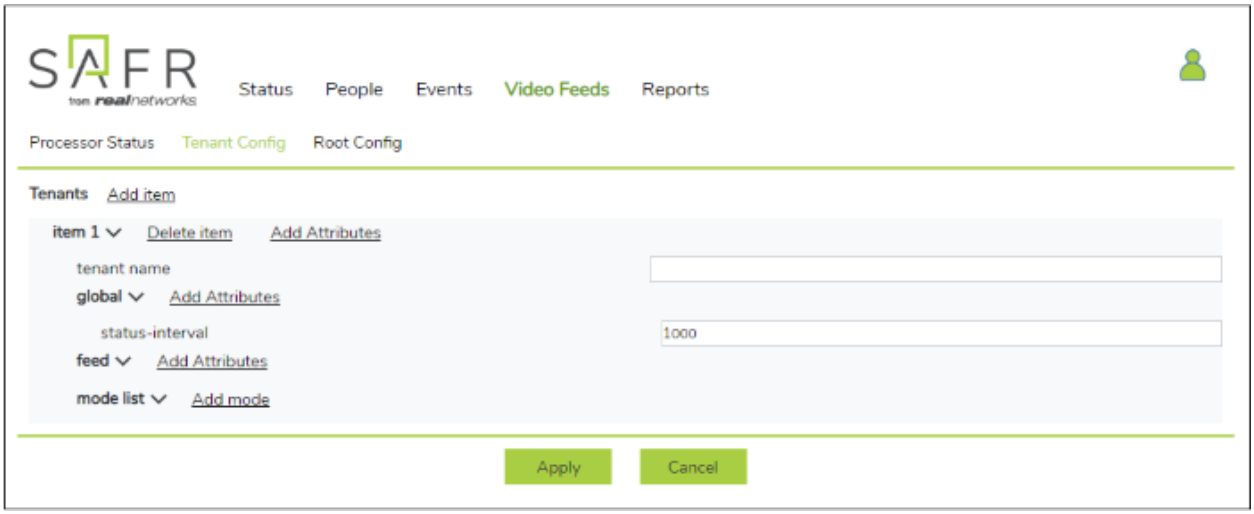
If the video feed is active, click **View** to access a streaming video window. Depending on your privileges, click **Config** to view, edit, or add attributes to override Root and Tenant global configuration settings for a single video feed. To make changes to global account settings, go to the Tenant Config page.




## 61.2 Tenant Config Page

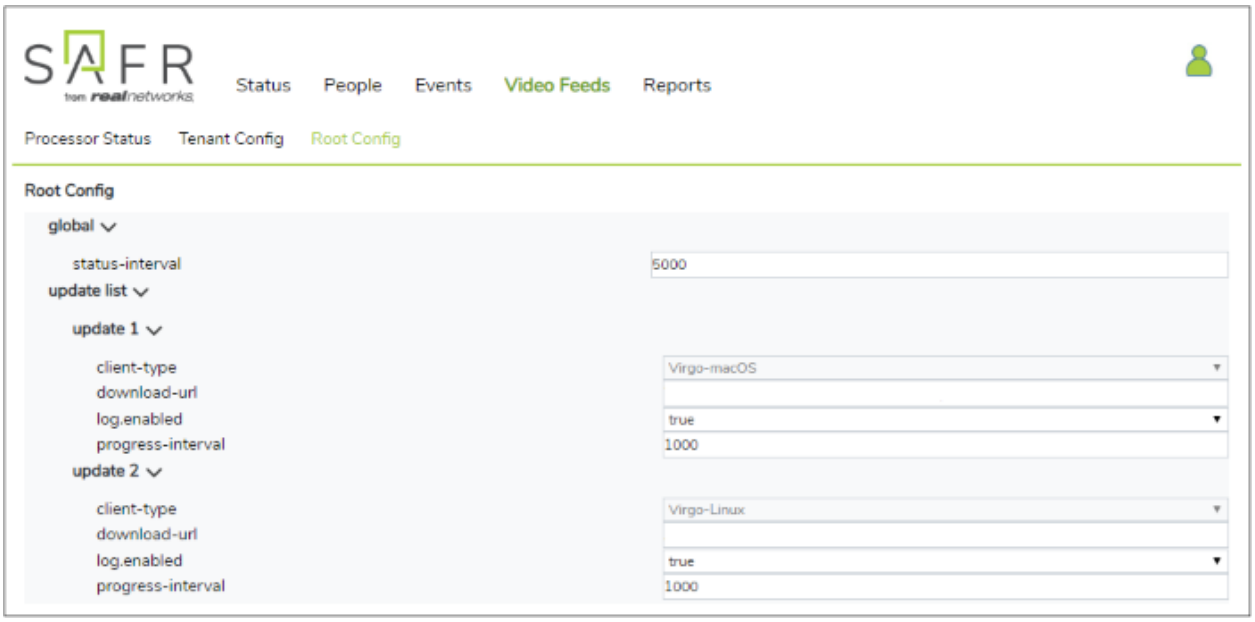
The Tenant is the primary account. Use this page to add and edit attributes of global settings at the account level to override the Root configurations. Directories can be added at this level by clicking the **Add Item**

link. To make changes to individual video feeds, go to the Processor Status page.



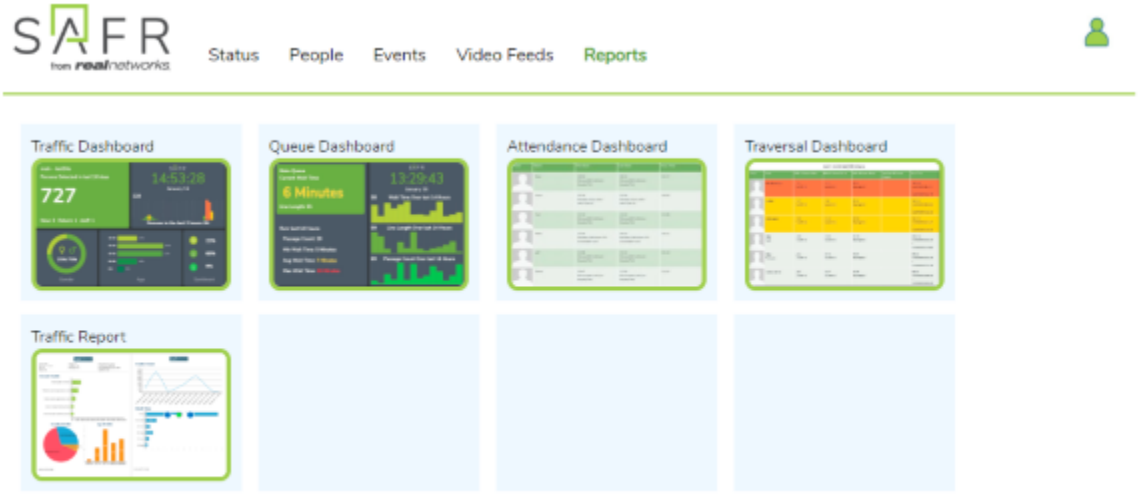

## 61.3 Root Config Page

The Root Config page displays all the properties set in VIRGO by RealNetworks. These global settings are read-only for cloud deployments, but they can be changed for local deploymentts. To override these settings for your deployment, go to the Tenant Config and Processor Status pages.



# 62 Reports Page

Click on the report that you're interested in to set the report's parameters and generate the report.




## 62.1 Save and Share Reports

The URLs of the generated reports contain all of the report's parameters, so you can save reports by bookmarking them and revisiting them at a later date.

Similarly, you can share reports with other people by emailing them reports' URLs. Note, however, that the link recipient will need to meet the following criteria to access the reports:

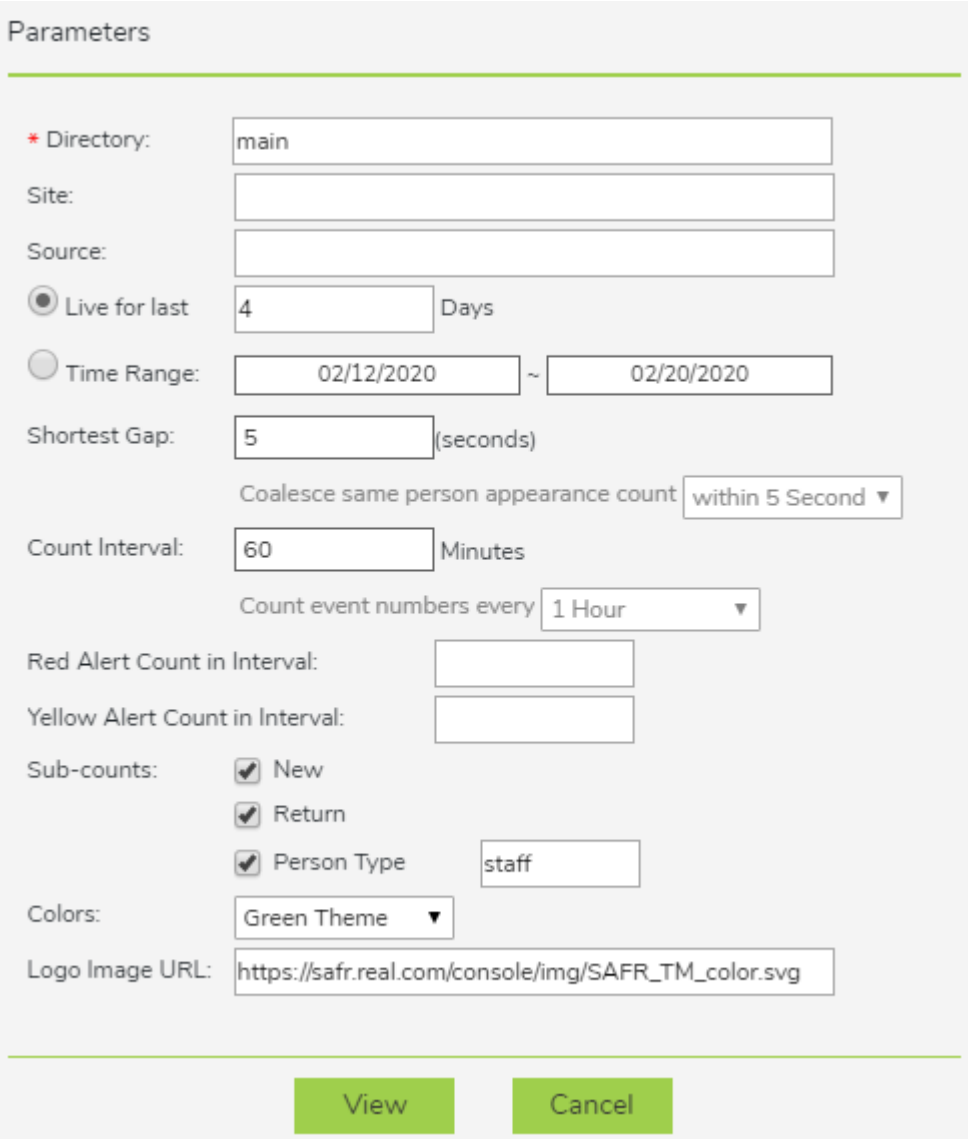
- They must have valid credentials for your SAFR system.
- They must have a user role other than Analyst. (i.e. Analysts are unable to view reports, but all other roles can view them.)

# 63 Traffic Dashboard

The traffic dashboard provides in-depth information about recognized and unrecognized people at your site, including:

- Total number of people viewed.
- Percentage of male and female faces.
- Age and sentiment percentages.
- Sentiment scores.

## 63.1 Input Parameters




- **Directory**: User directory from which to run the dashboard.
- **Site**: Filter that allows you to limit the report to cameras with the specified site value. Site values can be set using the Account Preferences tab within the Desktop client.
- **Source**: Filter that allows you to limit the report to a single source. A source is typically a camera but may also be the source ID assigned when processing video from a file or making REST API calls. Source values can be set using the Camera Preferences tab within the Desktop client.

- **Live for last**: Number of previous days to include in the dashboard. When this parameter is used, the Traffic Dashboard is dynamically re-generated every 30 seconds using the most recent time frame. For example, if you were to set this parameter to "2" and then leave the dashboard open for a week, it would always display data from the most recent two days. This parameter is mutually exclusive with *Time Range* below.
- **Time Range**: Dates to include in the dashboard. This parameter is mutually exclusive with *Life for last* above.
- **Shortest Gap**: If a person is viewed by a camera (thus triggering an event), leaves the field of view of the camera, and is then seen by the camera again (thus triggering another event), the two events will be merged into a single event if the time between them is equal to or less than the number of seconds specified by the *Shortest Gap* parameter.
    - **Coalesce same person appearance count**: This is a field to help you calculate the *Shortest Gap* parameter. You can select a value from the drop-down menu, and the correct number of seconds will be calculated and entered into the *Shortest Gap* field.
- **Count Interval**: Defines the time interval included in each data bar of the trend chart.
    - **Count event numbers every**: This is a field to help you calculate the *Count Interval* parameter. You can select a value from the drop-down menu, and the correct number of minutes will be calculated and entered into the *Count Interval* field.
- **Red Alert Count in Interval**: When the count within a count interval is greater than this number, the trend chart bar is shown in red. Set this value to zero if you don't want any bars shown in red.
- **Yellow Alert Count in Interval**: When the count within a count interval is greater than this number, the trend chart bar is shown in yellow. Set this value to zero if you don't want any bars shown in yellow.
- **Sub-counts**: Specifies which sub-counts, if any, you want displayed on your dashboard. You can choose one or more of the following sub-counts:
    - **New**: Number of unique registered people that appear.
    - **Return**: Total number of registered people that appear. Note that multiple appearances by the same number are counted multiple times for the purpose of this sub-count.
    - **Person Type**: Number of people who appeared with the specified *Person Type*.
- **Colors**: Specifies which color scheme will be used for the dashboard. There are two options: *Blue Theme* and *Green Theme*.
- **Logo Image URL**: Use this to use a custom logo in place of the SAFR logo at the top of the trend chart.

## 63.2 Generated Dashboard

Below is a sample traffic dashboard.

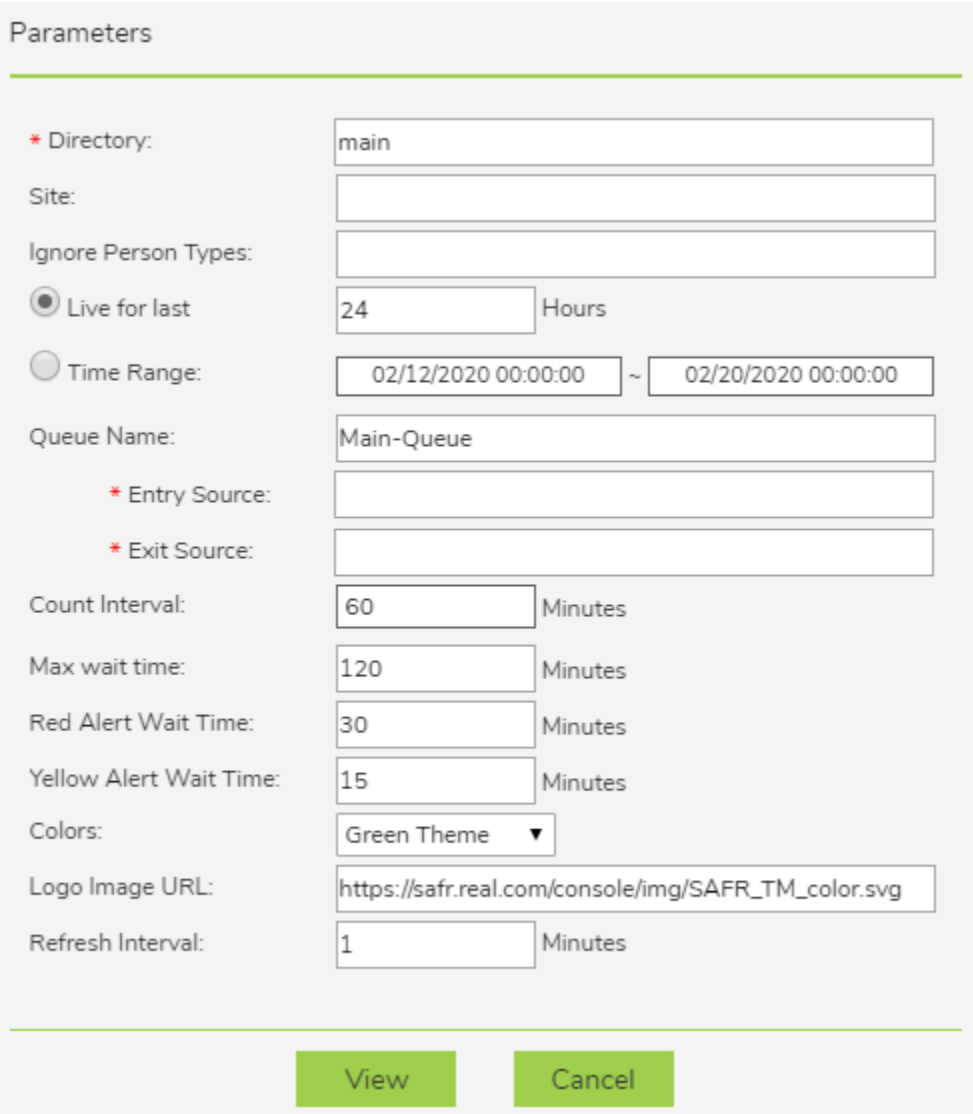

The trend chart is the chart in the upper right corner of the dashboard.

Note that the dashboard can have “Unknown” entries for both gender and age if some of your video feeds didn’t have gender and/or age detection enabled during the time frame in question. Both gender and age detection can be enabled or disabled on the Recognition Preferences tab in the Desktop client.

# 64 Queue Dashboard

The Queue Dashboard is used to monitor wait times in a queue. In order to use the Queue Dashboard you'll need 2 cameras: one for the entrance, and one for the exit.

## 64.1 Input Parameters

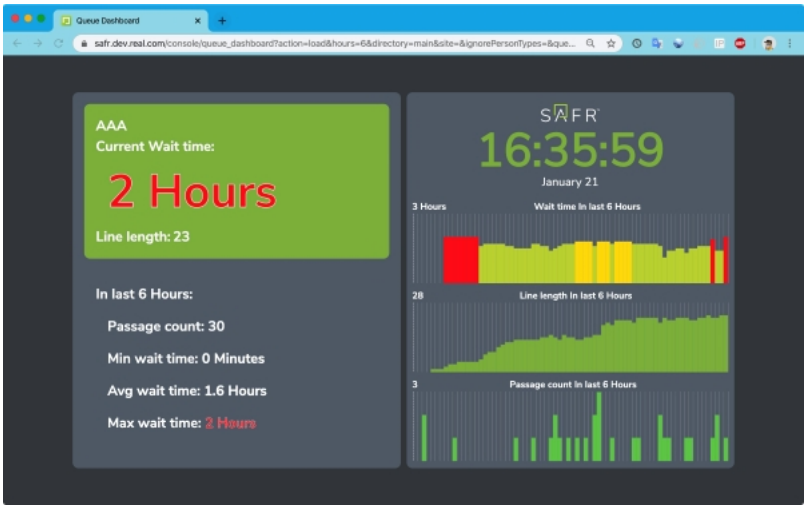



- **Directory**: User directory from which to run the dashboard.
- **Site**: Specifies the camera(s) to use. Cameras' site values can be set using the Account Preferences tab within the Desktop client.
- **Ignore Person Types**: The Person Types that should not be included in the dashboard, if any.
- **Live for last**: Number of previous hours to include in the dashboard. Every time the dashboard refreshes, the most recent *Live for last* hours are used to re-generate the Queue Dashboard. The dashboard's refresh rate is defined by the *Refresh Interval* parameter below. This parameter is mutually exclusive with *Time Range* below.
- **Time Range**: Time range to include in the dashboard. This parameter is mutually exclusive with *Live for last* above.
- **Queue Name**: Title of the queue that appears at the top of the dashboard.
  - **Entry Source**: The camera at the beginning of the queue.

    - **Exit Source**: The camera at the exit of the queue.
- **Count Interval**: The amount of time each bar on the wait time chart in the Queue Dashboard represents.
- **Max wait time**: Any individual whose wait time exceeds this value is assumed to be a false data point and is discarded. It's assumed that the person left the queue without waiting within it to get to the end.
- **Red Alert Wait Time**: When the wait for somebody is greater than this number, the bar in the wait time chart is shown in red. Set this parameter to zero if you don't want any bars shown in red.
- **Yellow Alert Wait Time**: When the wait for somebody is greater than this number, the bar in the wait time chart is shown in yellow. Set this parameter to zero if you don't want any bars shown in yellow.
- **Colors**: Specifies which color scheme will be used for the dashboard. There are two options: *Blue Theme* and *Green Theme*.
- **Logo Image URL**: Use this to use a custom logo in place of the SAFR logo at the top of the wait time chart.
- **Refresh Interval**: Specifies how frequently the data on the dashboard is refreshed. If "0" is entered, the dashboard won't work. If you want a very quick refresh time, enter a very small non-zero number such as 0.1.

## 64.2 Generated Dashboard

Below is a sample queue dashboard.



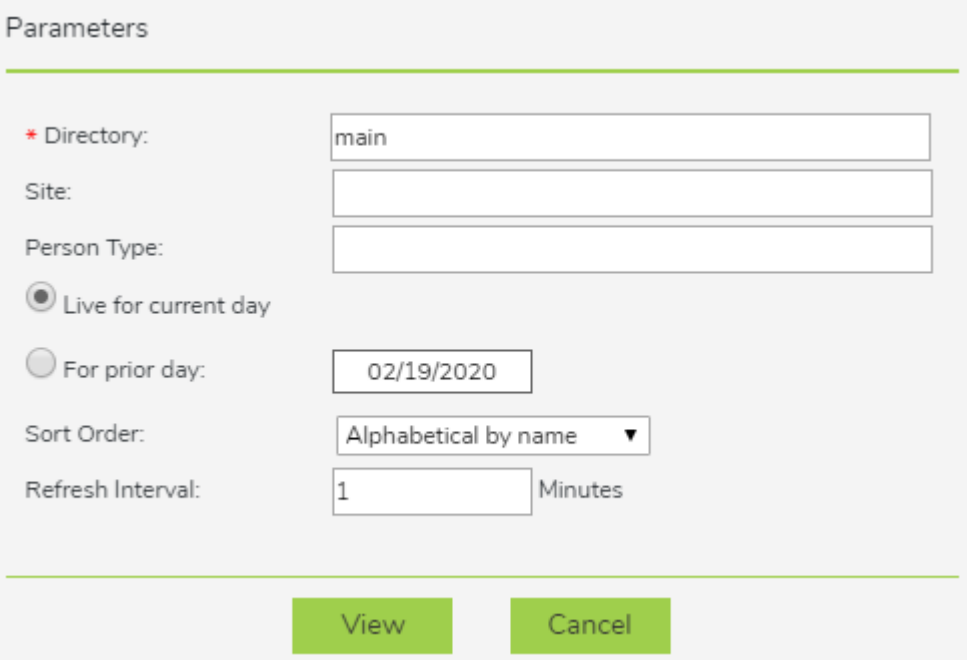
# 65 Attendance Dashboard

This report allows you to monitor the attendance record of a group of people (e.g. employees or students) on a given day. Although somebody might be seen multiple time in a day, this dashboard only reports the first time in a day they're seen and the last time in day they're seen, which allows the report to calculate how long a person was at the location. Note that this dashboard doesn't recognize periods in the middle of the day where the person might leave and then later come back to the location. (e.g. during lunch hour)

This report enables the following use case:

- **Time clock** - Have employees "punch in" and "punch out" daily at a tablet or other device. Employees must simply go to the tablet and ensure they are recognized by awaiting having their name flashed on the screen. Response messages can be customized so that at different times of day they may say "Checked in" or "Checked out", or you can just have it say "Confirmed". The person may appear any number of times but the tool will report based on only the first and last occurrence of a person.

## 65.1 Input Parameters



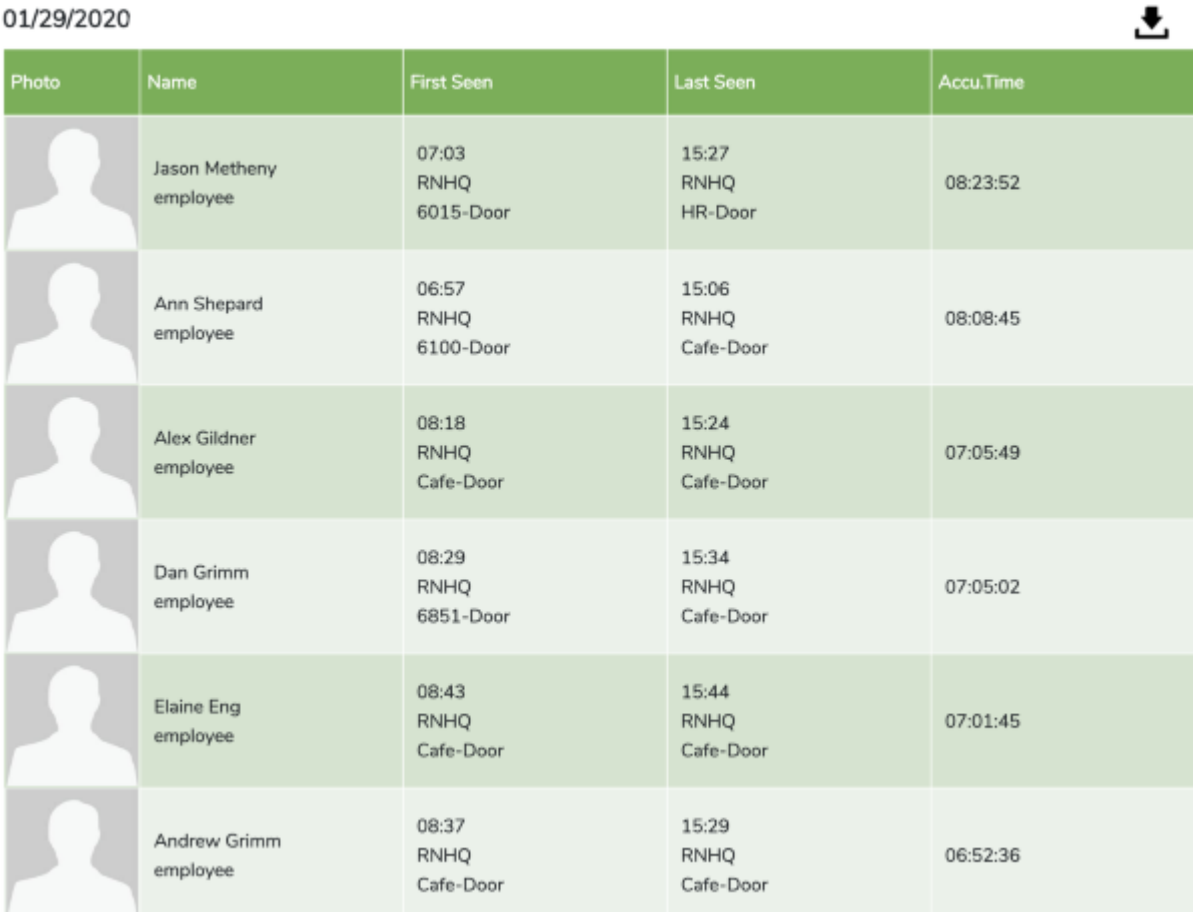

- **Directory**: User directory from which to run the dashboard.
- **Site**: Specifies the camera(s) to use. Cameras' site values can be set using the Account Preferences tab within the Desktop client.
- **Person Type**: The Person Type(s) to be included in the dashboard. If this parameter is left blank, then all Person Types are included.
- **Live for current day**: Causes the current day to be used for the dashboard. Selecting this parameter is mutually exclusive with the *For prior day* parameter below.
- **For prior day**: The day which you want to appear in the dashboard. Selecting this parameter is mutually exclusive with the *Live for current day* parameter above.
- **Sort Order**: Specifies the criteria by which the people are sorted. There are 4 options:
  - Alphabetical by name - Sorts based on the alphabetical order of their names.
  - In order of arrival - Sorts based on the order of people's arrival times, with people who arrived first being displayed first.
  - Shortest attendance first - Sorts based on how long each person has attended, with the shortest attendances appearing first.

- Longest attendance first - Sorts based on how long each person has attended, with the longest attendances appearing first.

- **Refresh Interval**: Specifies how frequently the data on the dashboard is refreshed. If "0" is entered, the dashboard won't work. If you want a very quick refresh time, enter a very small non-zero number such as 0.1.

## 65.2 Generated Dashboard

Below is a sample attendance dashboard. Note that you can download the dashboard as an *.xslx file by clicking on the download symbol in the upper right corner.



01/29/2020

| Photo | Name | First Seen | Last Seen | Accu.Time |
|---|---|---|---|---|
| | Jason Metheny<br>employee | 07:03<br>RNHQ<br>6015-Door | 15:27<br>RNHQ<br>HR-Door | 08:23:52 |
| | Ann Shepard<br>employee | 06:57<br>RNHQ<br>6100-Door | 15:06<br>RNHQ<br>Cafe-Door | 08:08:45 |
| | Alex Gildner<br>employee | 08:18<br>RNHQ<br>Cafe-Door | 15:24<br>RNHQ<br>Cafe-Door | 07:05:49 |
| | Dan Grimm<br>employee | 08:29<br>RNHQ<br>6851-Door | 15:34<br>RNHQ<br>Cafe-Door | 07:05:02 |
| | Elaine Eng<br>employee | 08:43<br>RNHQ<br>Cafe-Door | 15:44<br>RNHQ<br>Cafe-Door | 07:01:45 |
| | Andrew Grimm<br>employee | 08:37<br>RNHQ<br>Cafe-Door | 15:29<br>RNHQ<br>Cafe-Door | 06:52:36 |

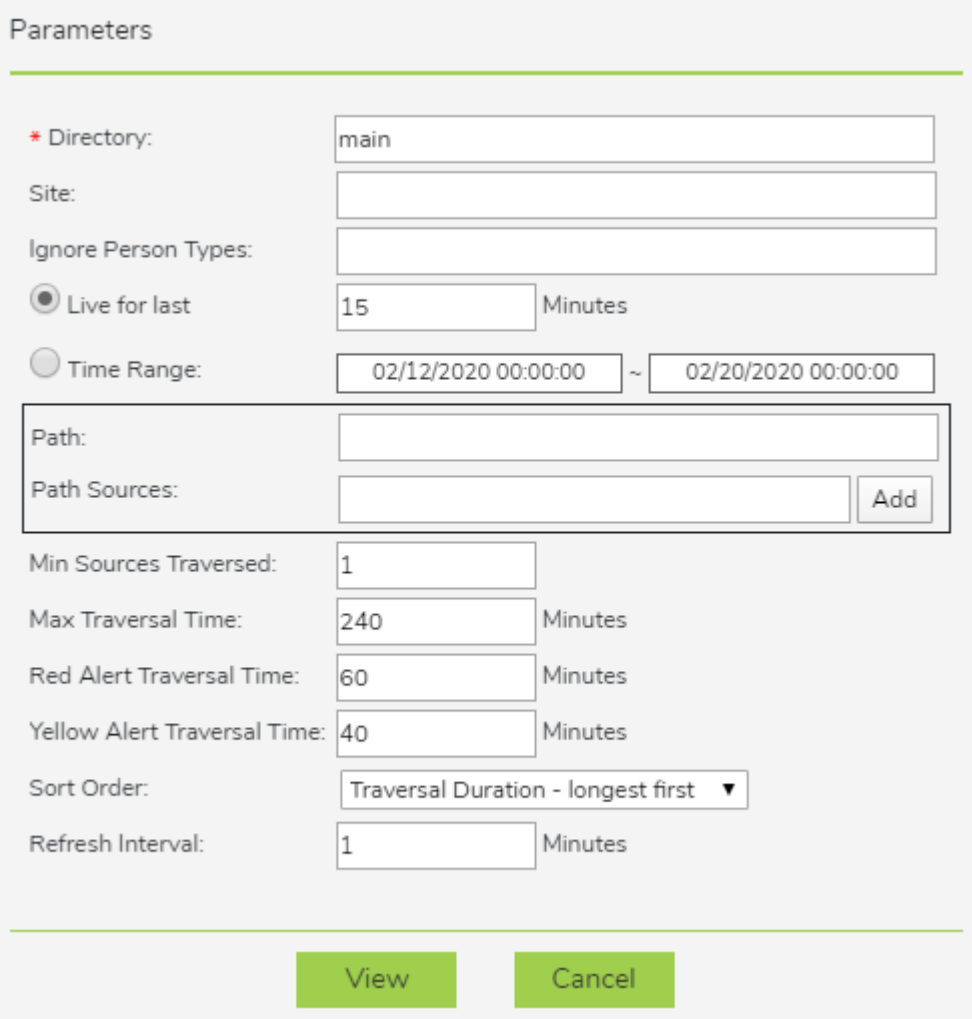
# 66 Traversal Dashboard

Displays traversal durations of individuals along a defined set of cameras. This dashboard highlights individuals exceeding expected traversal times and can be used to identify suspicious activity or general slow-downs (i.e. congestion) in real-time or time-frames in the past.

To use this report, you will either define a path when you input parameters or you can use an already defined path. A path is a list of 2 or more cameras. Thus, a path might consist of a set of cameras monitoring a causeway or a set of cameras monitoring all the entrances to a warehouse.

The report requires that either SAFR is set to auto-register people or that viewed people are already registered in the database. Auto-registration is typically done by setting cameras to the `Learn and Monitor` video processing mode in the Camera Feed Analyzer window in the Desktop client. In order for auto-registration to be sucessful, the facial images should be high quality and at least 220 pixels wide. This can be achieved by using high resolution cameras with sufficient zoom to capture faces.

## 66.1 Input Parameters




- **Directory**: User directory from which to run the dashboard.
- **Site**: Specifies the camera(s) to use. Cameras' site values can be set using the Account Preferences tab within the Desktop client.
- **Ignore Person Types**: The Person Types the dashboard should ignore, if any.

- **Live for last**: Number of previous minutes to include in the dashboard. Every time the dashboard refreshes, the most recent *Live for last* hours are used to re-generate the Traversal Dashboard. The dashboard's refresh rate is defined by the *Refresh Interval* parameter below. This parameter is mutually exclusive with *Time Range* below.
- **Time Range**: Dates to include in the dashboard. This parameter is mutually exclusive with *Live for last* above.
- **Path**: The path that you want to use for this Traversal Dashboard. **Note**: If you have already defined one or more paths, then you have the option to use one of them by selecting an already defined path from a drop-down menu that this field will offer you.
- **Path Sources**: All the cameras that make up this traversal route. **Note**: The order you add cameras to this field doesn't matter.
- **Min Sources Traversed**: The minimum number of cameras that a person must pass in front of before the traversal dashboard will include them in its data.
- **Max Traversal Time**: Any individual whose traversal time exceeds this value is assumed to be a false data point and is discarded. It's assumed that the person left the traversal area without completing the path.
- **Red Alert Traversal Time**: When a person's traversal time exceeds this value, their data is shown in red on the Traversal Dashboard. Set this value to zero if you don't want any data shown in red.
- **Yellow Alert Traversal Time**: When a person's traversal time exceeds this value, their data is shown in yellow on the Traversal Dashboard. Set this value to zero if you don't want any data shown in yellow. The *Red Alert Traversal Time* parameter takes precedence over this parameter.
- **Sort Order**: Specifies the criteria by which the people are sorted. There are three values you can choose from:
  - Traversal Duration - longest first
  - Traversal Start - in order of arrival
  - Traversal Start - most recent first
- **Refresh Interval**: Specifies how frequently the data on the dashboard is refreshed. If "0" is entered, the dashboard won't work. If you want a very quick refresh time, enter a very small non-zero number such as 0.1.

## 66.2 Generated Dashboard

Below is a sample traversal dashboard. Note that you can download the dashboard as an *.xslx file by clicking on the download symbol in the upper right corner.

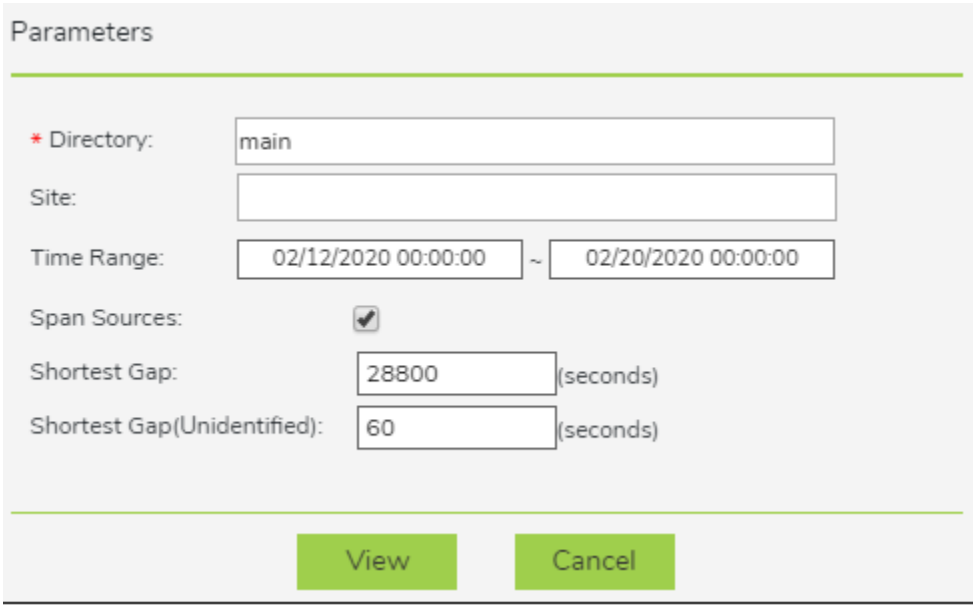

safr.real.com/console/traversal_dashboard?action=load&directory=main&site=&minutes=120&ignorePersonTypes=&pathS...
Board Arrival - Live for last 120 minutes
Photo
Name
6015-Door
6851-Door
HR-Door
Accu.Time
James Walker
admin
13:38 03/11
13:57 03/11
1:37:29
13:38 03/11 - 15:16 03/11
Garri Sarkisov
IT
13:12 03/11
14:04 03/11
14:37 03/11
1:25:20
13:12 03/11 - 14:38 03/11
Michael
Parham
exec
15:12 03/11
14:27 03/11
0:48:15
14:27 03/11 - 15:16 03/11
Dan Grimm
employee
14:22 03/11
0:16:5
14:22 03/11 - 14:38 03/11
Timothy Lloyd
IT
14:06 03/11
0:13:14
14:06 03/11 - 14:19 03/11
Gary Lewis
employee
13:36 03/11
0:0:4
13:36 03/11 - 13:36 03/11

# 67 Traffic Report

Provides in-depth information about recognized and unrecognized people at your site, including:

- Total number of events.
- Counts for unknown and known persons.
- Gender and age profiles.
- Traffic trends per day.
- Dwell time: The amount of time a person remains on camera per event.

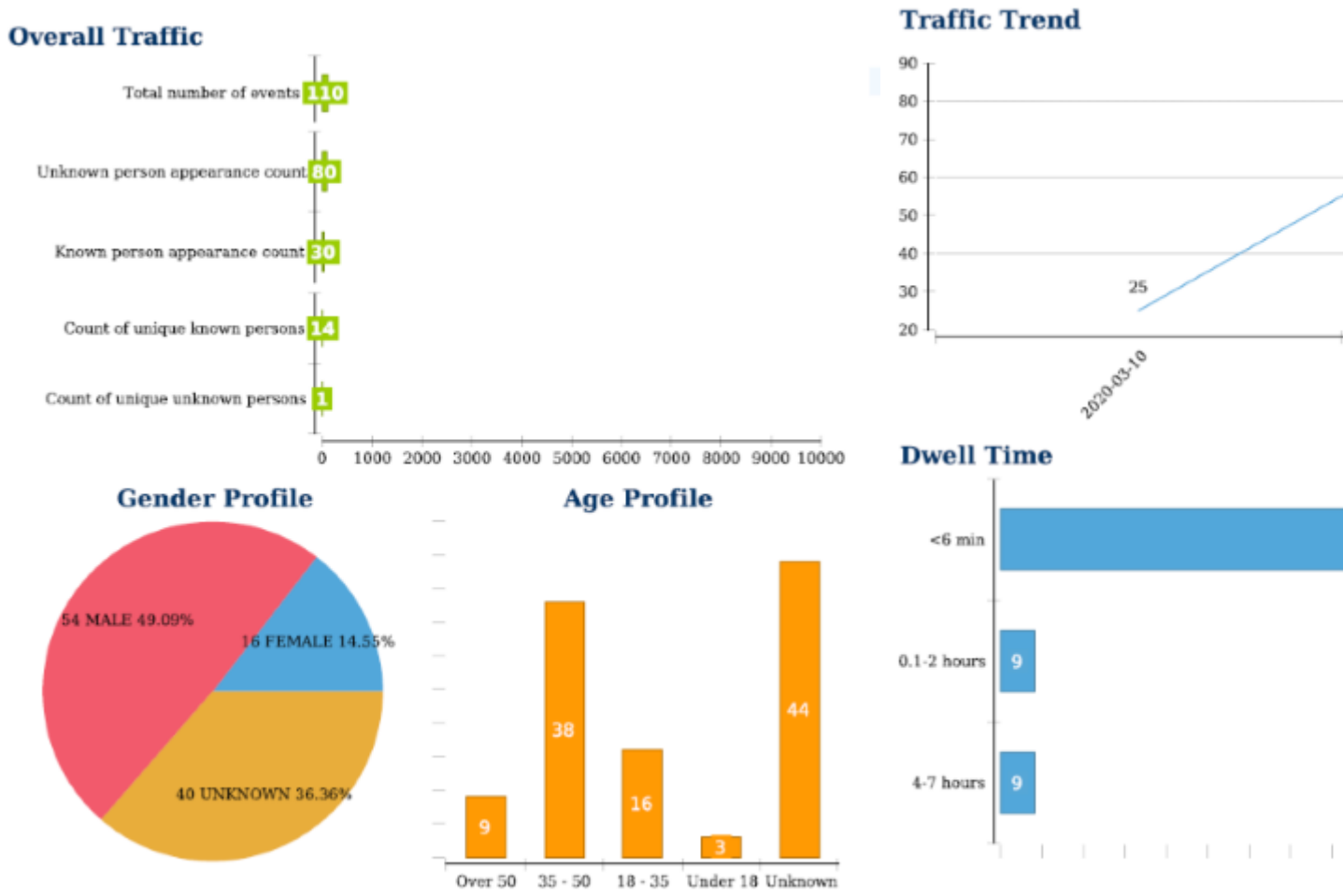
## 67.1 Input Parameters




- **Directory**: User directory from which to run the report.
- **Site**: Specifies the camera(s) to use. Cameras' site values can be set using the Account Preferences tab within the Desktop client.
- **Time Range**: Dates and times to include in the report.
- **Span Sources**: Specifies whether or not events triggered in multiple cameras at the same time (plus or minus the shortest gap time) by the same person should be combined into a single event.
- **Shortest Gap**: If an identified person is viewed (thus triggering an event), leaves the field of view of the camera, and is then seen by the camera again (thus triggering another event) the two events will be merged into a single event if the time between them is equal to or less than the number of seconds specified by the *Shortest Gap* field.
- **Shortest Gap(Unidentified)**: If an unidentified person is viewed (thus triggering an event), leaves the field of view of the camera, and is then seen by the camera again (thus triggering another event) the two events will be merged into a single event if the time between them is equal to or less than the number of seconds specified by the *Shortest Gap(Unidentified)* field.

## 67.2 Generated Report

Below are screenshots from a sample traffic report:




The Overall Traffic graph exposes the following data:

- **Total number of events**: Total number of events generated over the time period covered by the report.
- **Unknown person appearance count**: Number of apppearances of registered people who don't have a name assigned to them in the Identity Database.
- **Known person appearance count**: The number of apppearances of named registered people.
- **Count of unique known persons**: Number of named registered people who were seen. Note that if a person was seen multiple times, they're only counted once for the purpose of this value.
- **Count of unique unknown persons**: Number of registered people who don't have a name assigned to them in the Identity Database who were seen. Note that if a person was seen multiple times, they're only counted once for the purpose of this value.

Both the gender and age profiles can have "Unknown" entries if some of your video feeds didn't have gender and/or age detection enabled during the time frame covered by the report. Both gender and age detection can be enabled or disabled on the Recognition Preferences tab in the Desktop client.

Dwell time is the amount of time a person remains on camera per event.

You can download the sample traffic report here.

# 68 Face Detection-Person Detection Tie-In

When face detection and person detection are enabled at the same time, face objects will be associated with the appropriate person objects. This allows SAFR to continue tracking people even if they turn their faces away from the camera. In addition, face recognition metadata will be used to automatically enhance the metadata of the associated person object. Each face object can be associated with at most one person object. Similarly, each person object can be associated with at most one face object.

When a face object and person object have become associated with each other, events that are generated by the person object are called "parent events" or "root events", while events generated by the face object are called "children events" or "secondary events". You can choose if secondary events are included in the Event Archive by enabling or disabling the **Include Secondary Events** setting on the Events Preferences tab in the Desktop client. SAFR's default behavior is to not include secondary events, as they can create too much useless "noise" in the Event Archive.

Face detection and person detection can be enabled and configured on the Detection Preferences tab.

## 68.1 Shared Event Attributes

When a face object and a person object become associated, they will share the following event attributes:

- age
- avgSentiment
- company
- directGazeDuration
- expDate
- externalId
- gender
- homeLocation
- idClass
- imageTime
- maxSentiment
- minSentiment
- moniker
- name
- newId
- occlusion
- personId
- personTags
- personType
- region
- rootPersonAddDate
- similarityScore
- smileDuration
- tagId
- tagType
- validationEmail
- validationPhone

Whenever a face event is updated with any of the above properties, the associated person event will be updated as well.

Secondary events (i.e. associated face events) have their **rootEventId** attribute set to the eventId of their parent event. (i.e. the person event it's associated with) This enables all secondary events to be gathered and appropriately presented. Each secondary event has only one **rootEventId**.

Conversely, root events (i.e. associated person events) have their **hasSubEvents** attribute set to `true`.

Root events aren't ended until all their child events are ended.

# 69 Identity Recognition Thresholds

SAFR measures the difference between a face image and the stored identity image by a difference measure known as "Identity Recognition". The value of Identity Recognition can range from 0 to about 1.3. Values of 0.54 or lower represent are interpreted as certain matches, while values above 1.0 are interpreted as different faces.

SAFR has 2 configurable settings that define the acceptable difference between a reference image and the event face image. These are defined as follows:

- **Identity Recognition Threshold** - The largest difference between a face image and a stored identity image at which SAFR will report a 100% confidence match. As noted above, a value of 0.54 or lower represents a certain match. This is the default value for SAFR and usually shouldn't be changed.
- **Proximity Threshold Allowance** - A boost value that is added to the Identity Recognition Threshold. The sum of Identity Recognition Threshold and Proximity Threshold Allowance is used as the largest difference between a face image and a stored identity image at which SAFR will report a reduced confidence match.

SAFR uses Proximity Threshold Allowance to report possible matches. It does this by reporting a match with a percentage confidence. Any value that is between the Identity Recognition Threshold (e.g. 0.54) and the Proximity Threshold Allowance-boosted value (e.g. 0.92) will be reported as a probable match using a percentage scale as follows:

**Proximity Threshold Allowance Boost Confidence Table**

| Identity Recognition Threshold | Proximity Threshold Allowance | Combined Value | Confidence | Interpretation |
|---|---|---|---|---|
| 0.54 | 0 | 0.54 or less | 100% | Certain match (values > 100% are possible indicating even greater certainty). |
| 0.54 | 0.14 | 0.68 | 93% | Close match but not certain enough to unlock the door in Secure Access scenarios. |
| 0.54 | 0.3 | 0.84 | 86% | Possible match with low confidence. |
| 0.54 | 0.38 | 0.92 | 82% | Similar face with no confidence of match. |
| 0.54 | 0.51 | 1.05 | 79% or less | Different faces. |

The confidence match is overlaid on the videos or images just below the face (alongside the name) and is also reported in the SAFR Events returned through REST APIs in the `confidence` field.

## 69.1 Typical Uses of Proximity Threshold Allowance

Proximity Threshold Allowance is frequently used in the following scenarios:

- Watchlist monitoring - If you wish to have confidence reported in the user interface, it's generally recommended you set the Proximity Threshold Allowance to 0.38. With this value SAFR will begin

to report faces that are 82% confidence or greater. You can adjust the value of Proximity Threshold Allowance to limit matches to higher or lower confidences, as desired. This is typical for a watchlist scenario where you wish to see possible matches. Operators should be educated so they understand the **Proximity Threshold Allowance Boost Confidence Table** above and can use that information accordingly with possible matched individuals.

- Secure Access - If you do not wish to have confidence reported, then set Proximity Threshold Allowance to 0. In this case only certain matches are reported. This is typically used in Secure Access video processing mode where only certain matches are desired.
- User verification - In some cases, you may wish to validate a user based on a document they present such as a photo ID. While a 100% confidence is desired, this may not always be possible because of the poor condition of the photo ID or because of the age difference between the photo ID and the subject. In these cases, it may be acceptable to use the confidence value returned by SAFR to gauge a close match. For example, a value of 93% confidence could be considered sufficiently close to authorize registration.

## 69.2 See Also

- Recognition Preferences
- Face Detection-Person Detection Tie-In
- Pose Liveness Detection

# 70 Pose Liveness Detection

Liveness detection is the process whereby facial recognition software attempts to differentiate between genuine live faces and spoofed fake faces. (such as from a photo of a face) SAFR uses a face's center pose quality to attempt to detect liveness.

Pose liveness detection operates as follows:

1. State A: An unrecognized face needs to be recognized.
2. State B: Proof of liveness will pursued as follows:
    1. The recognized face is tracked at the rate of at least 25 frames per second.
    2. Any loss of tracking (occurrence of lingering for more than 1 frame) or a detection gap > 40 ms in frame capture time results in the need to re-recognize the face and thus a return to State A.
    3. Pose quality must maintain a score of 0.5 or higher for 3 consecutive frames and at least one of the samples must have a profile pose confidence of 35% or less to trigger the transition to the next state, State C.
3. State C: A smooth transition to profile pose will be pursued as follows:
    1. The face is tracked at the rate of at least 25 detections per second.
    2. Any loss of tracking (occurrence of lingering for more than 10 frames) or a detection gap > 40ms in frame capture time results in the need for re-recognition and thus return to State A.
    3. A momentary loss of tracking (recovered in less than 10 frames) will require a center pose quality difference from the prior frame of no less than 0.15.
    4. If change in identity is detected as part of prescribed re-recognition, State B will restarted.
    5. Pose quality must be observed to transition to score of 0.26 or lower for at least 3 consecutive frames and with 66% of at least 3 images but no more than 30 images immediately proceeding with scores observed > 0.26 and < 0.5 and in decreasing sequence to trigger transition to State D.
        - For example: `0.45, 0.37, 0.23, 0.12, 0.24`
        - This algorithm can interpreted as requiring presence of descending strand of samples being at least 66% of the number of samples with min number being specified in preferences and max number being 30 (~1 second).
4. State D: After the profile pose state has changed, a verification call is issued to obtain a similarity score to the identity obtained in State A.
    1. The verification call must indicate at least a 86% match.
    2. A response from recognition must also indicate that the face is in profile pose, based on profile pose confidence returned and threshold set.
    3. If both of above are met, liveness detection will conclude.
    4. If both aren't true, re-recognition will continue immediately for as long as the pose quality score remains at 0.26 or lower until successful confirmation of pose and 86% identity match is confirmed.
    5. If pose score exceeds value of 0.26 for 3 consecutive frames, transition back to state B will occur.
    6. Any loss of tracking (occurrence of lingering) will result in need for re-recognition and thus return to State A.

# 71 SAFR-Digifort Integration Guide

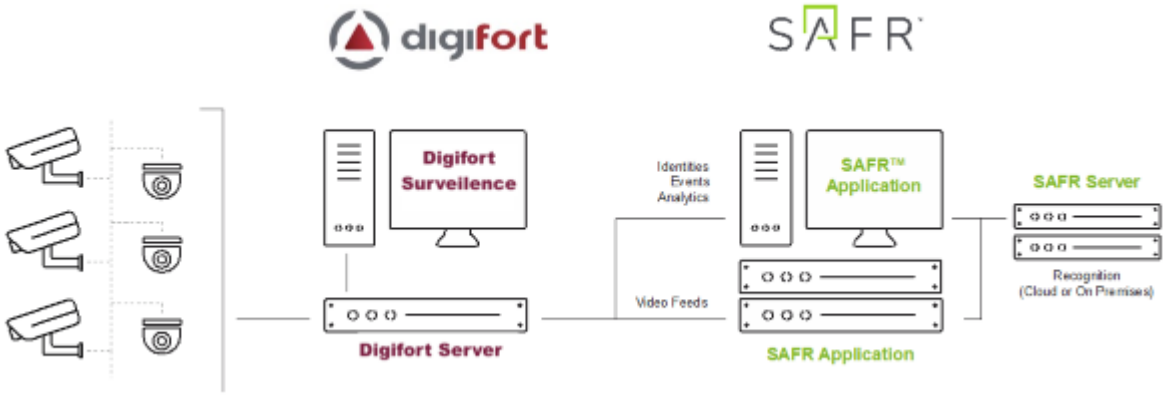
Integrating SAFR's facial recognition and analysis capabilities into Digifort enables you to use SAFR's video feed information overlays within Digifort camera video feeds, thus making it much easier to quickly and accurately separate unknown people from authorized people from known threats. You'll also have immediate access to additional infomation 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.

## 71.1 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.

### 71.1.1 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:

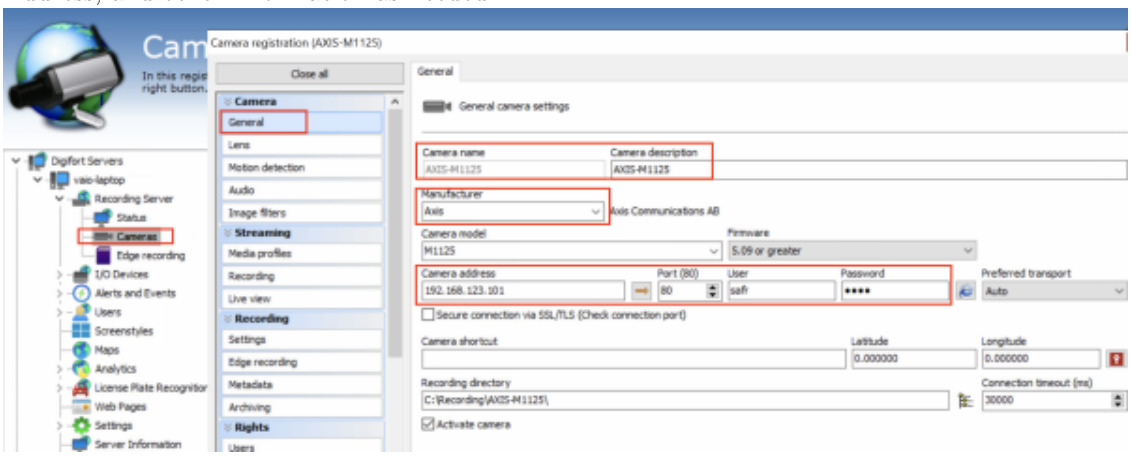
- Each camera running SAFR must have a SAFR license.

- 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.

## 71.2 Install and Configure Digifort

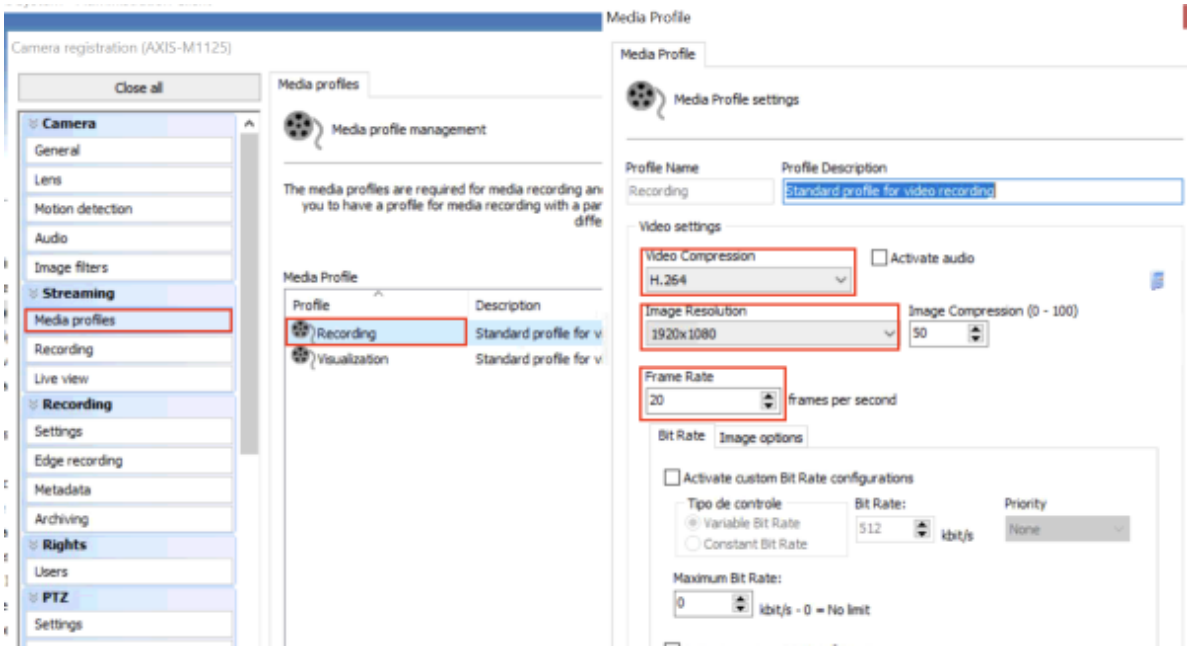
Download and install Digifort by doing the following:

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.

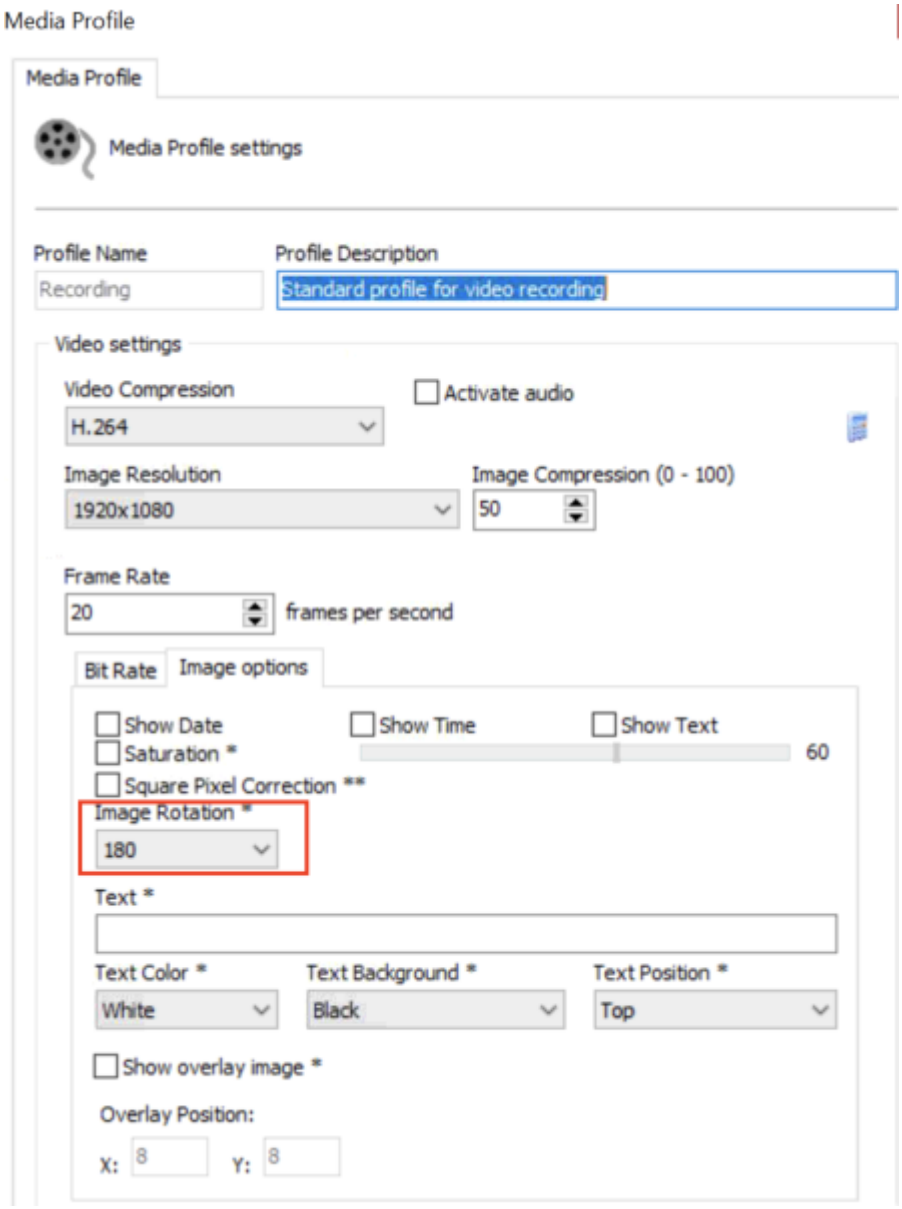



**Note**: Digifort allows you to add mobile cameras as well as using the Digifort Mobile Camera Pro App. In the Add Camera dialog, select **Digifort** as the manufacturer and **Mobile Camera Pro** as the make.

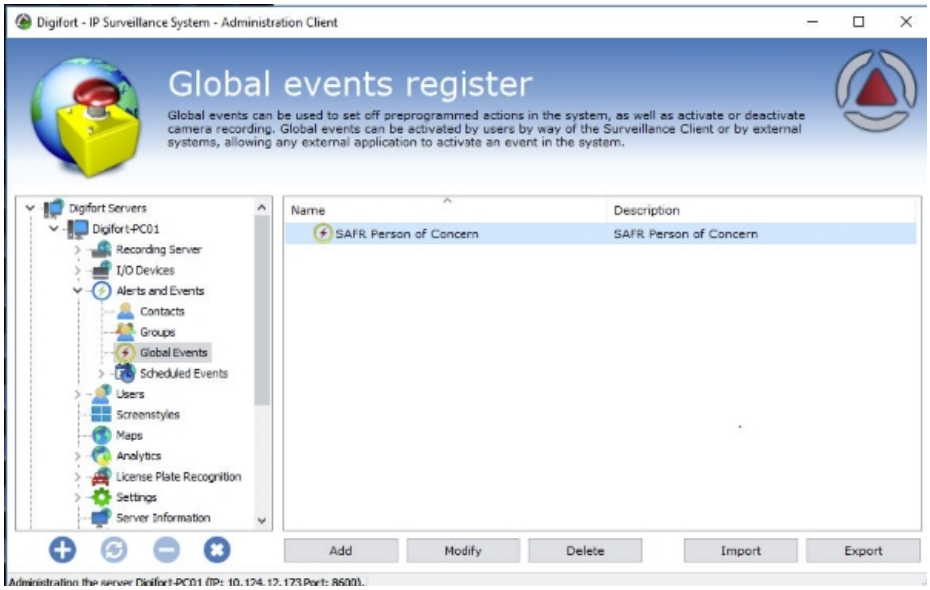
5. You may need to update the *Video Compression*, *Image Resolution*, *Frame Rate*, or *Image Rotation*, as shown below:




6. You may need to update the *Image Rotation* or *Profile Description* on the Media Profile settings page, as shown below:

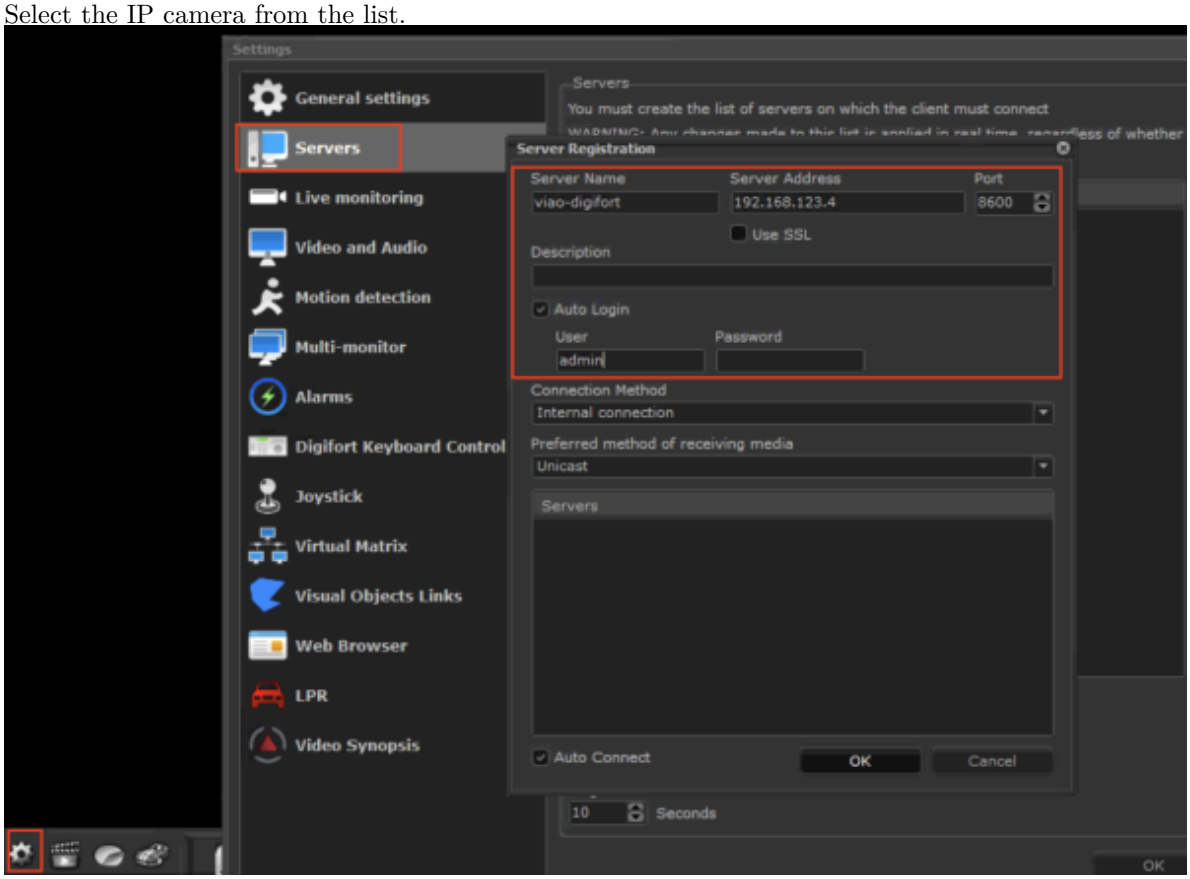



7. Navigate to **Alerts and Events > Global Events** to add events as needed. You can configure the event actions there too, when needed.




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.



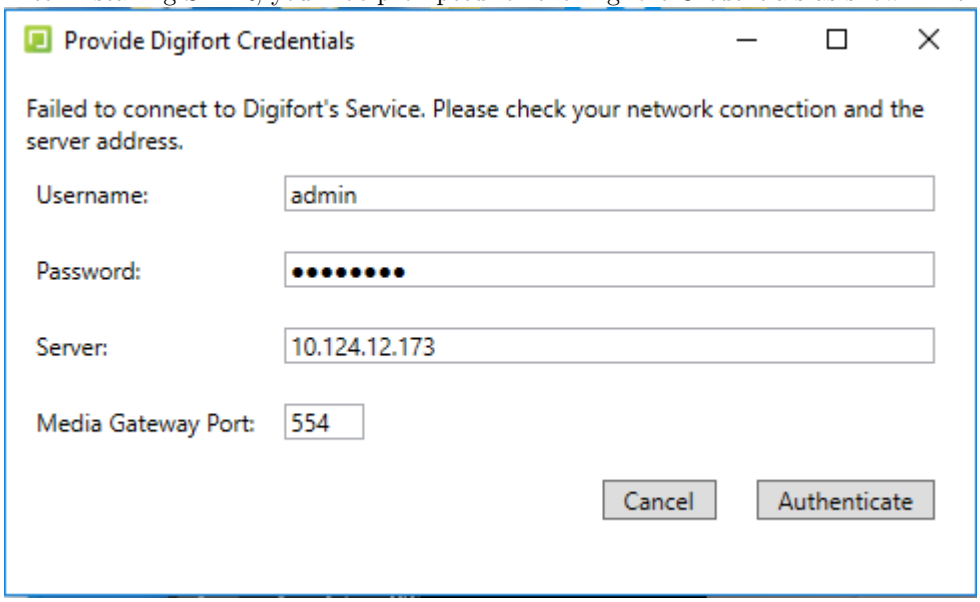
## 71.3 Connect an IP Camera

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

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


## 71.4 Install and Configure SAFR

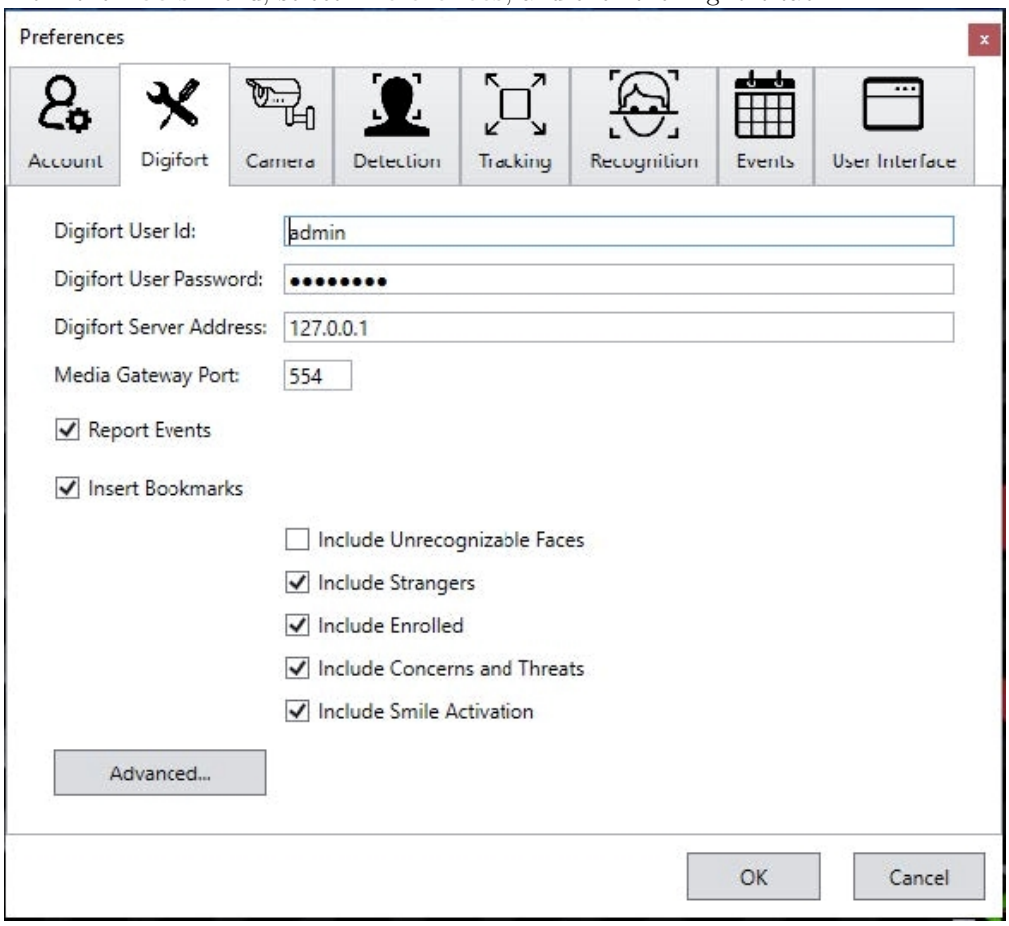
1. From the SAFR Download Portal, download and install either SAFR Platform or SAFR Edge, depending on your deployment type. Make sure to select the Digifort VMS extension install option.
2. After installing SAFR, you'll be prompted for the Digifort Credentials as shown in the following dialog:




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**.

## 71.5 Verify your Connection

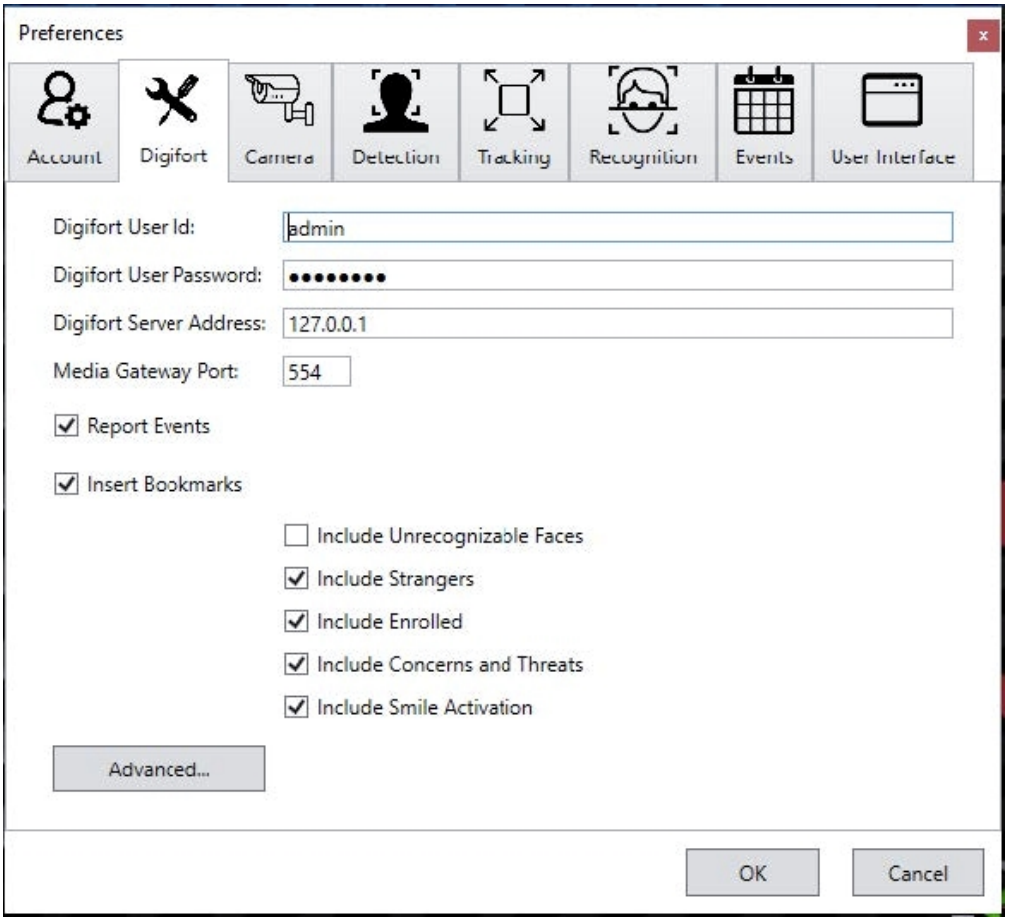
To verify successful connection to the Digifort system, open the **Preferences > Camera** tab. Cameras connected to the Digifort system should be visible. All cameras connected to the Digifort system have a Digifort prefix in their names.

# 72 SAFR-Digifort Operation Guide

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 infomation 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.

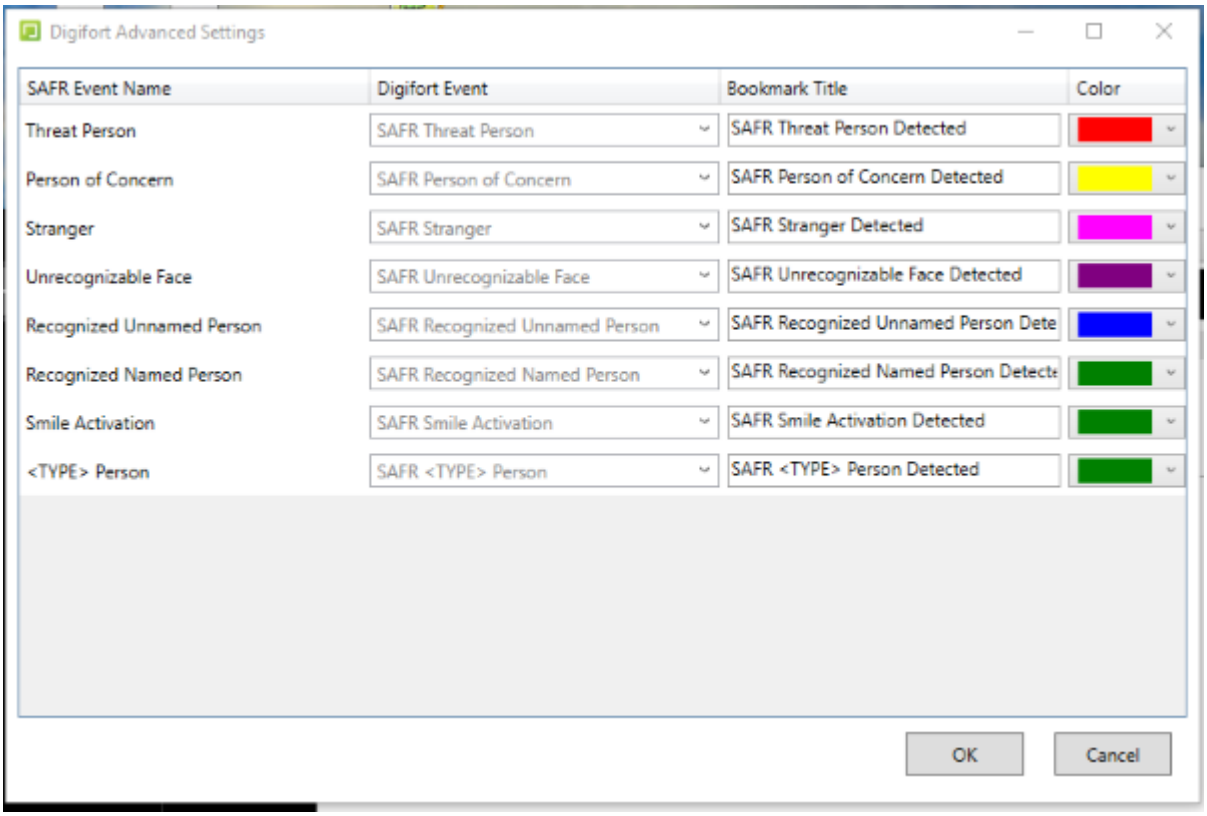
## 72.1 SAFR Digifort Preferences



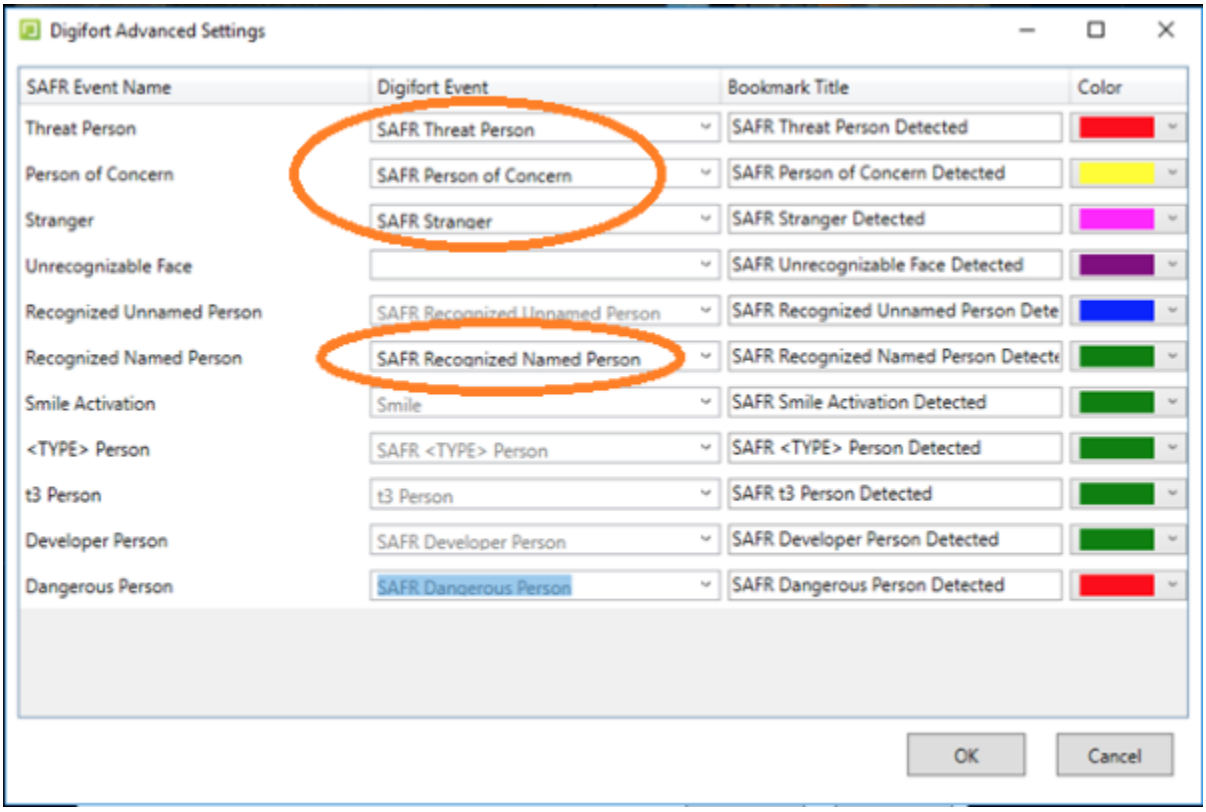

- **Digifort User Id**: User created previously in Configure Digifort
- **Digifort User Password**: Password created for the SAFR user
- **Digifort Server Address**: IP address of server running Digifort
- **Media Gateway Port**: Set to 554 unless configured otherwise in Digifort
- **Report Events**: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



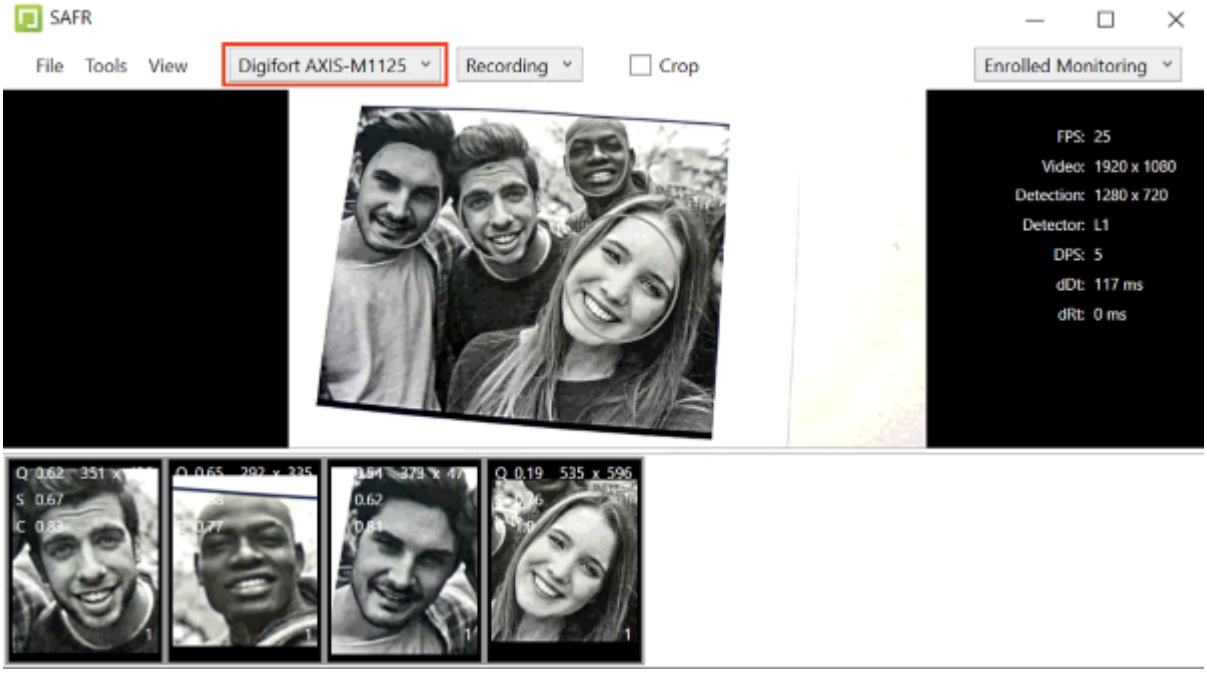

If the Digifort events are disabled (gray; no matching Digifort event), refer to Digifort documentation to create Digifort events. Once the events are created, open the Digifort Advanced Settings dialog and, from the menu for the associated SAFR event, select the Digifort event. Once the Digifort events 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.

## 72.2 Connect and Use Cameras and Video Feeds



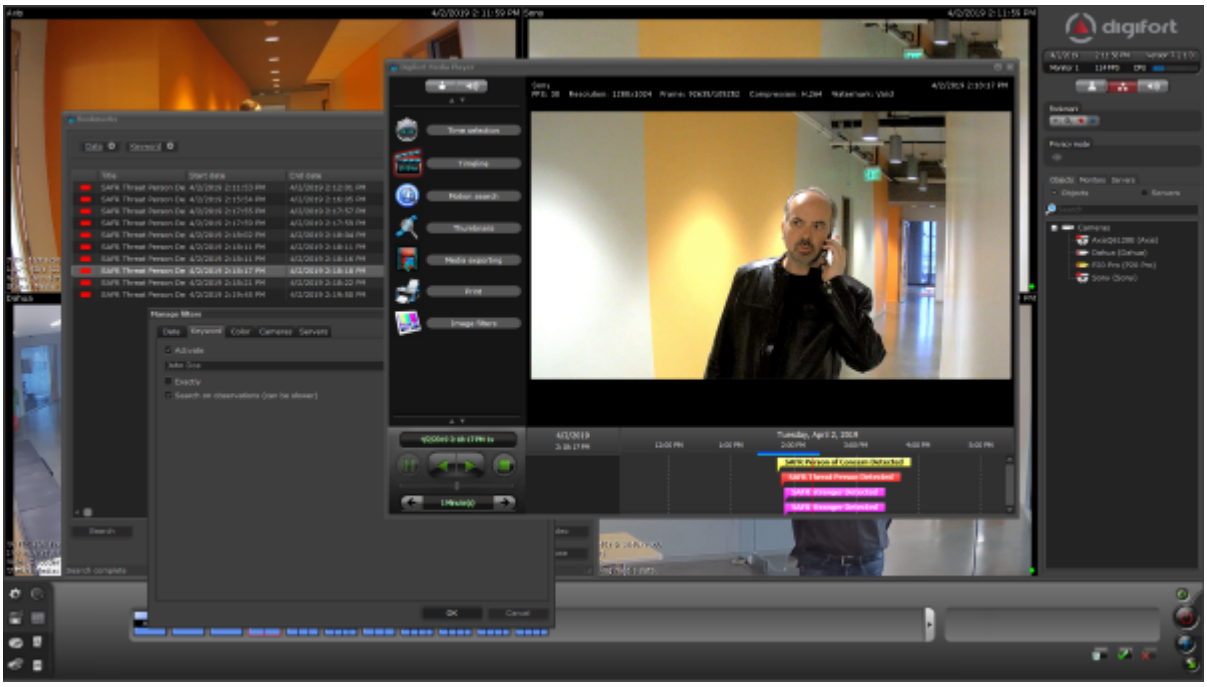

In the SAFR Desktop client, view the video feed for the camera selected from the camera selection menu.

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**.

## 72.3 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**.

## 72.4 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

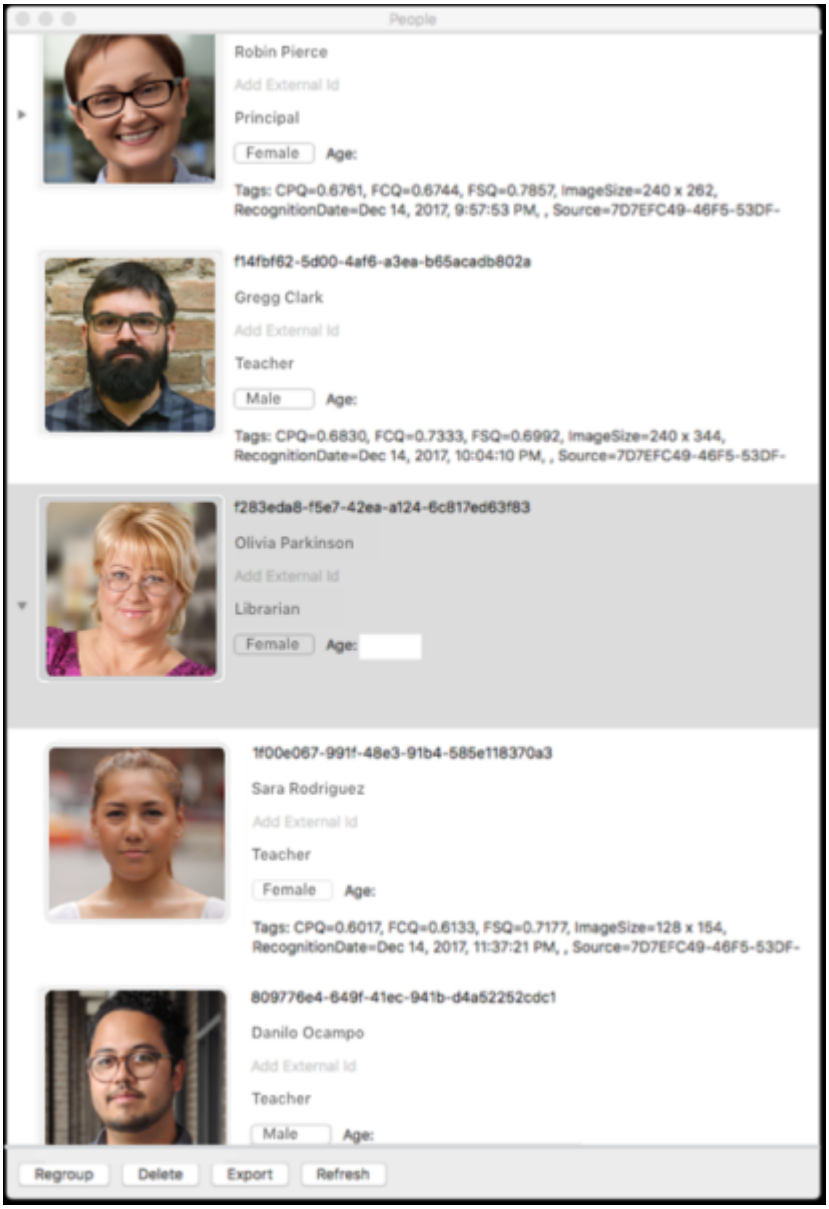
**Warning**: Reducing detection and recognition settings lowers the quality of the reference face and negatively impacts recognition. It is preferable to increase the quality of your sources than to lower the criteria for learning.

**Warning**: Users added to SAFR are not synchronized with Digifort; these users exist only in SAFR.

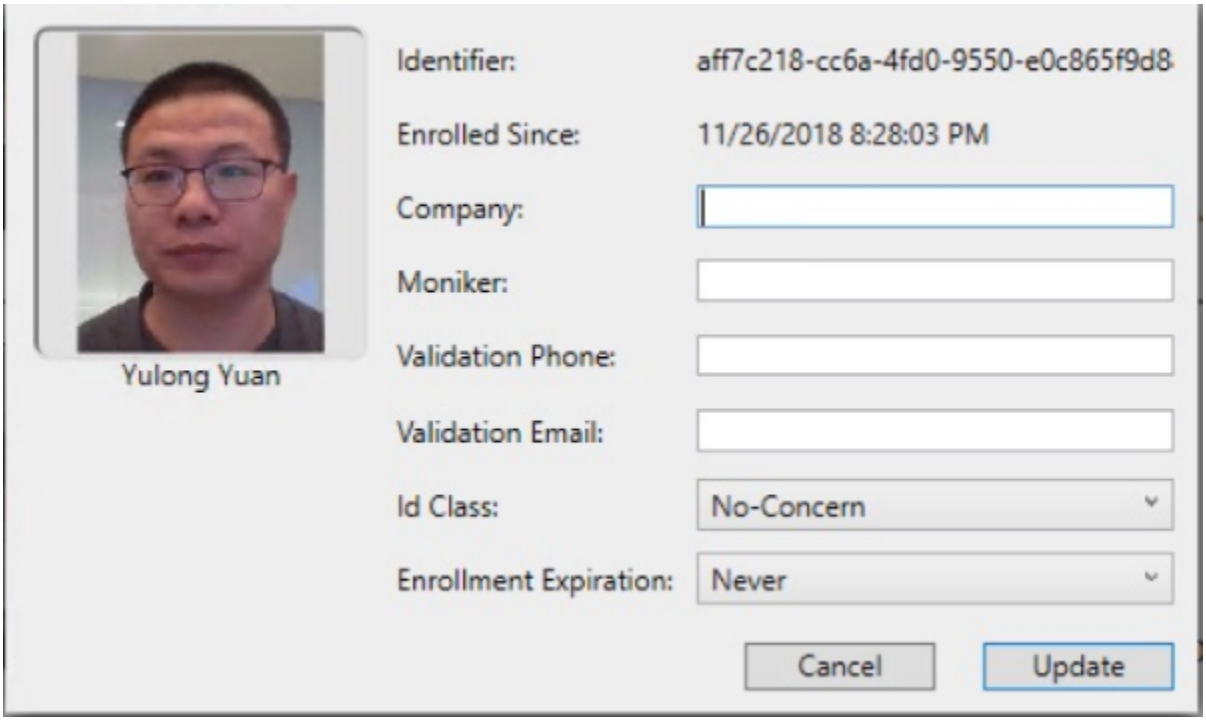
It may be desirable to edit people properties to control which events get triggered when that person is recognized. For example, setting a person's *ID Class* to *Concern* or *Threat* triggers the respective alarms. The most important people attributes are *Name*, *Image*, *Person Type*, and *ID Class*.

*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:




## 72.5 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.

| Event Message | Id Class | Named | Person Type | Condition | People Attributes |
|---|---|---|---|---|---|
| Unrecognizable face detected | N/A | N/A | N/A | Face detected but insufficient information for recognition | idClass="unidentified" |

| Event Message | Id Class | Named | Person Type | Condition | People Attributes |
|---|---|---|---|---|---|
| Stranger detected | Stranger | N/A | N/A | Face detected but not found in registered people | idClass=“stranger” |
| Registered person detected without name | Normal | No | None | Registered person without name or person type assigned | idClass=“noconcern” && personType="" && name="" |
| Registered person detected with name <name> | Normal | Yes | None | Registered person with name but no person type | idClass=“noconcern” && personType="" && name=<name> |
| Registered person detected of type <personType> | Normal | No | Defined | Registered person with person type but no name | idClass=“noconcern” && personType=<personType> && name="" |
| Registered person detected of type <personType> with name <name> | Normal | Yes | Defined | Registered person with person type and name | idClass=“noconcern” && personType=<personType> && name=<name> |
| Concern person detected without a name | Concern | No | None | Same as above for Concern | idClass=“concern” && personType="" && name="" |
| Concern person detected with name <name> | Concern | Yes | None | Same as above for Concern | idClass=“concern” && personType="" && name=<name> |
| Concern person detected detected of type <personType> | Concern | No | Defined | Same as above for Concern | idClass=“concern” && personType="" && name="" |
| Concern person detected of type <personType> with name <name> | Concern | Yes | Defined | Same as above for Concern | Registered person marked as concern detected with name assigned. |

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

### 72.5.1 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.

### 72.5.2 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:


## 72.6 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.

# 73 SAFR-Genetec SDK Integration Guide

Integrating SAFR's facial recognition and analysis capabilities into Genetec enables you to use SAFR's video feed information overlays within Genetec 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 infomation such as age, gender, sentiment, name, company, known associates, or any other configurable information you want to create.

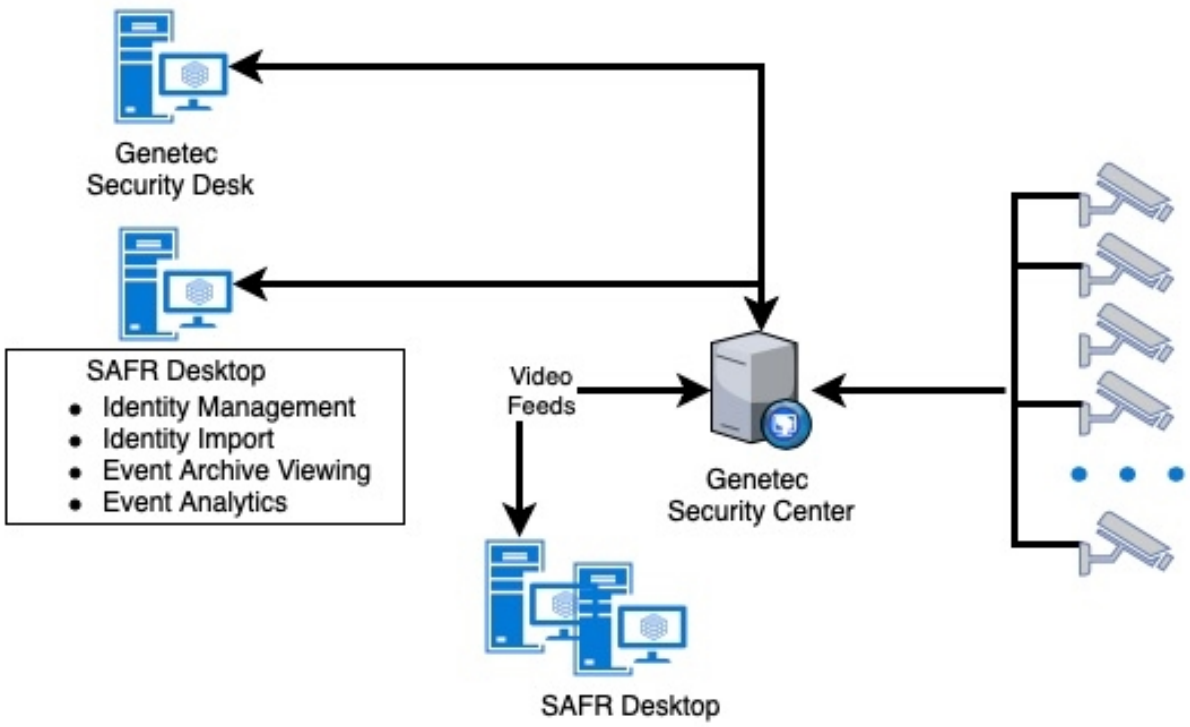
**Note**: SAFR has the native capability to detect age, gender, and sentiment, while other information needs to be manually entered by an operator.

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

## 73.1 Integration Overview and Requirements

A typical deployment requires the following:

- A machine running Genetec Security Center.
- A machine running Genetec Security Desk and Genetec Config Tool.
- 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 the Genetec Security Center. The SAFR Desktop client(s) can then connect to the Genetec Security Center to perform analysis of the video and add overlays. Depending on the number of cameras you need, one or more machines may be required to run the SAFR Desktop client, each processing multiple video feeds. The Desktop client processes the video and returns information to Genetic to overlay the video feeds and generate events. The Desktop is also used to perform various management activities.

### 73.1.1 System Requirements

Genetec has the following system requirements:

- One machine running Genetec Security Center Version 5.7 or later.
- One machine running Genetec Security Desk and Genetec Config Tool.
- Each machine running a Genetec product must meet the following system requirements:
  - Windows 10.
  - Additional system requirements as described here.

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 1.3.228 or later.
  - Genetec Security Center SDK for your version of Genetec Security Center must be installed.
  - Additional system requirements as described here.
- Local SAFR deployments require at least one machine running SAFR Platform 1.3 or later.
- Each machine running SAFR Server must meet the following requirements:
  - Windows 10.
  - Additional system requirements as described here.

### 73.1.2 Licensing and the Genetec Part Number

An accompanying Genetec part number must be added to your Genetec connection license. Do the following to discover and add the Genetec part number:

1. Go to the Genetec Portal and sign in using your Genetec credentials.
2. In the applications section, search for *SAFR*. From the results, click *SAFR Facial Recognition*.
3. On the **SAFR Facial Recognition Solution Details** page, in the right column, the *Genetec Part Number* is displayed.
4. Contact Genetec and have them add the part number to your license. You need a quantity of the part number equal to the number of cameras SAFR will be processing plus one additional license for the metadata channel SAFR creates. In other words, if SAFR will be processing cameras, then you need quantity of the part number added to your license.

You'll need the following licenses: each Genetec camera where SAFR face detection and recognition is used, you'll need:

- A Genetec connection license with the accompanying Genetec part number is required for each connected Genetec camera.
- One additional Genetec connection license for the metadata channel SAFR creates.
- A SAFR license for each camera is required

For example, if you have 300 cameras but only need face detection on 30 cameras at a time, then you would obtain a 31 connection license from Genetec and a 30 camera license from RealNetworks. Having a 31 connection Genetec license does not mean you are limited to face detection on a fixed set of 30 cameras. At any time, you can choose to connect the SAFR Desktop client to a different camera. You may have cameras in your parking garage that you were not previously monitoring with SAFR recognition. You can use a few of your licenses that are connected to other cameras to connect to garage cameras instead.

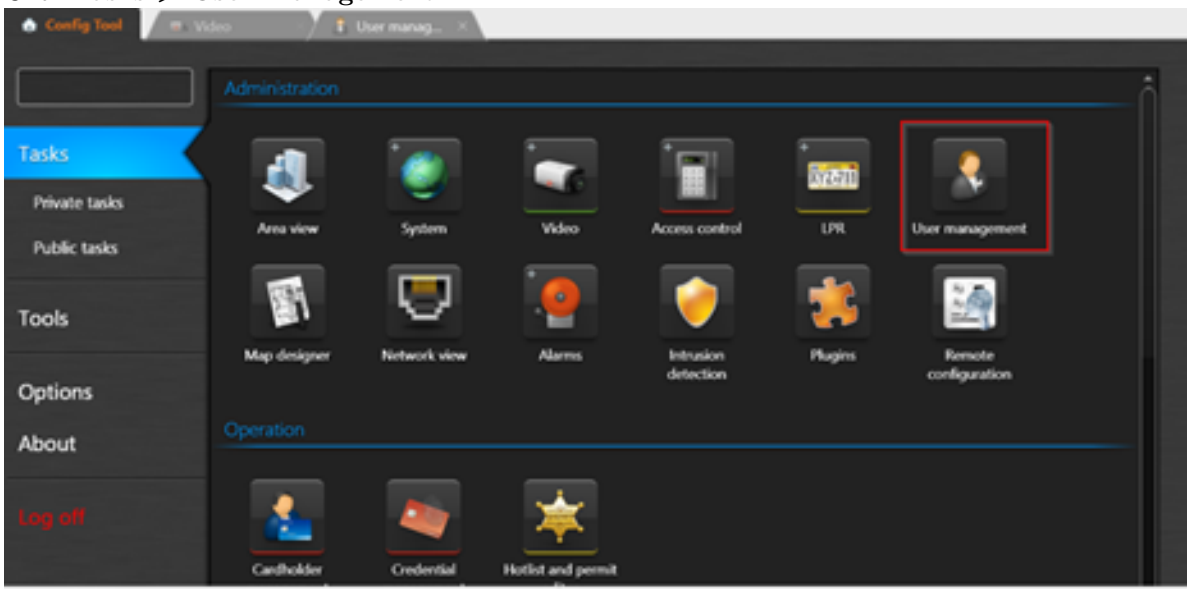
## 73.2 Install and Configure the Genetec Security Center

1. Download the latest version of Genetec Security Center from the Genetec Portal.
2. Run the installer. For details about which install options to select, see the Security Center Installation and Upgrade Guide.

### 73.2.1 Create a SAFR User

To create a user with the permissions that SAFR will require, do the following:

1. Open the Genetec Config Tool.
2. Click **Tasks > User Management**.




3. Create a new user (with a username of, for example, *SAFR*) with the following permissions:

   **All privileges**

   - Application privileges
     - Log on using the SDK

   **Administrative privileges**

   - Physical entities
     - View camera properties

   **Access control management**

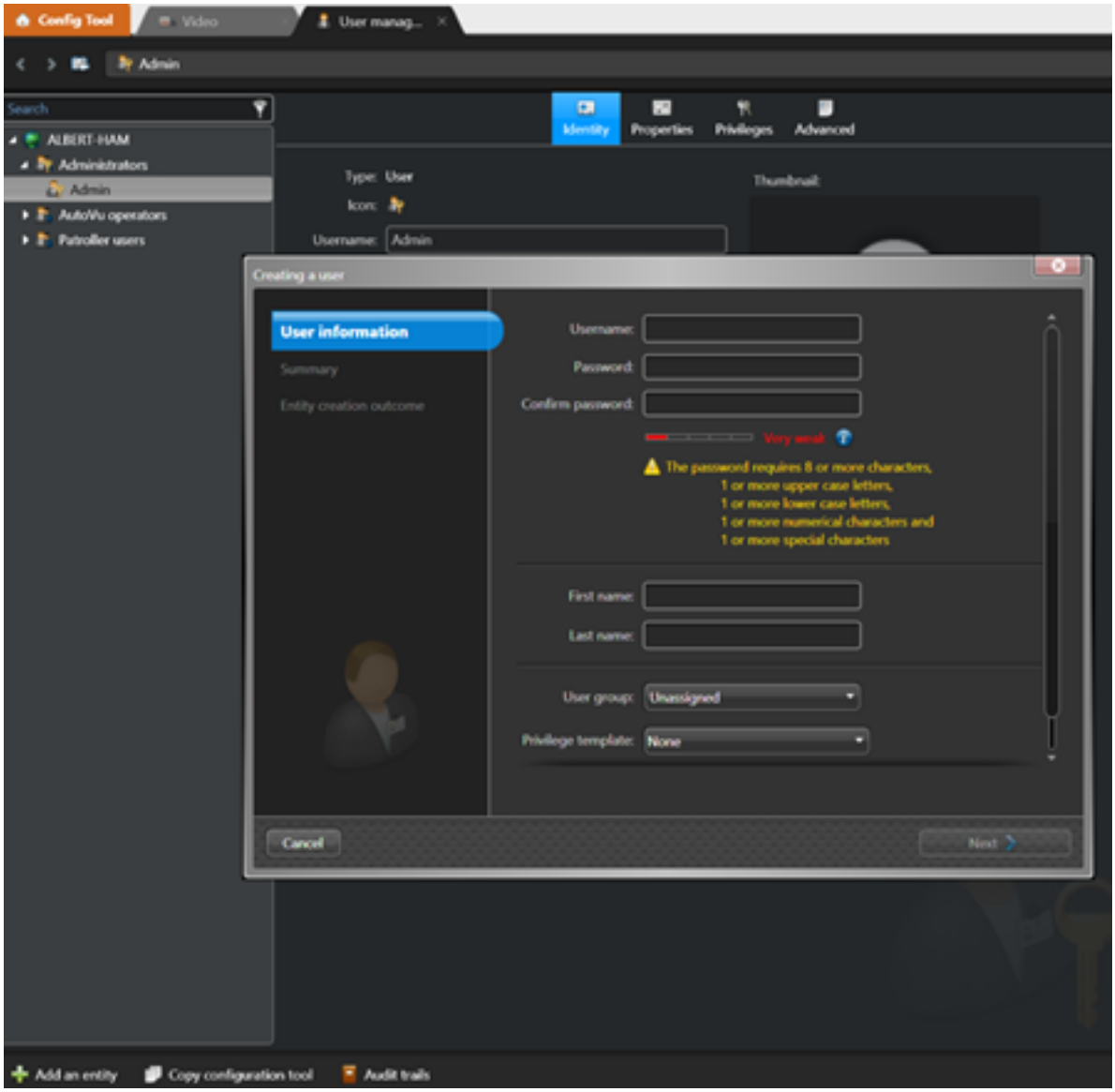
   - View cardholder group properties
   - View cardholder properties
   - View visitor properties

   **System management**

   - View general settings
     - Modify custom events

   **Action Privileges**

   - Cameras
     - View live video
     - Add bookmarks




### 73.2.2 Add Permissions for Event-to-Archive Actions

In order to create Event-to-Actions in the Genetec Config Tool, one or more of the following Action permissions must also be added to the SAFR user created in the previous section. Only those actions you want to trigger with SAFR events are needed:

**All privileges**

- Action privileges
  - Set threat level
  - Cameras
    - Protect video from deletion
    - Save/modify/print snapshots
  - Access control
    - Doors
      - Explicitly unlock doors
      - Override unlock schedules
    - Elevators

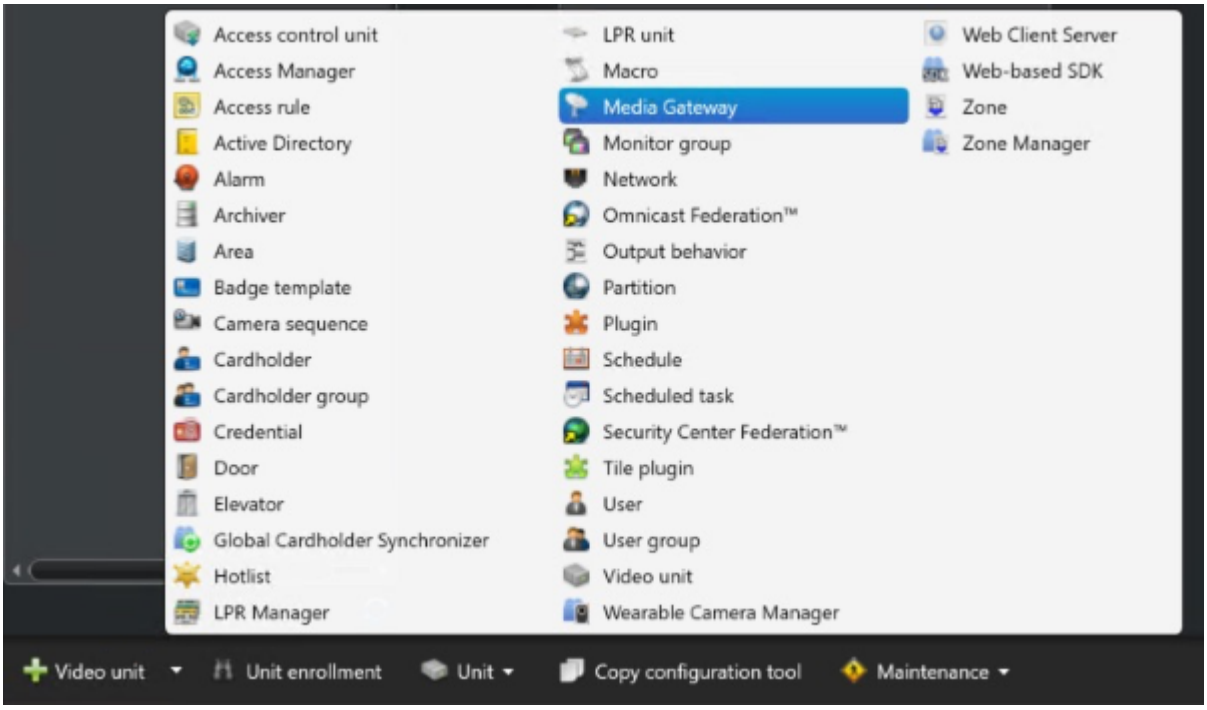
        - Override elevator schedules
    - Alarms
        - Trigger alarms
    - Users
        - Send a message
        - Send an email
        - Send/clear task
    - Macros
        - Execute macros
    - Zones
        - Arm/disarm zones
    - Areas
        - Modify people count

### 73.2.3 Set Minimum Cardholder Image Size

Do the following:

1. Open the Genetec Config Tool.
2. Open **Tasks > Administration > Access Control > General Settings**.
3. Set *Maximum Picture File Size* to 128k or larger.

### 73.2.4 Configure the Media Gateway



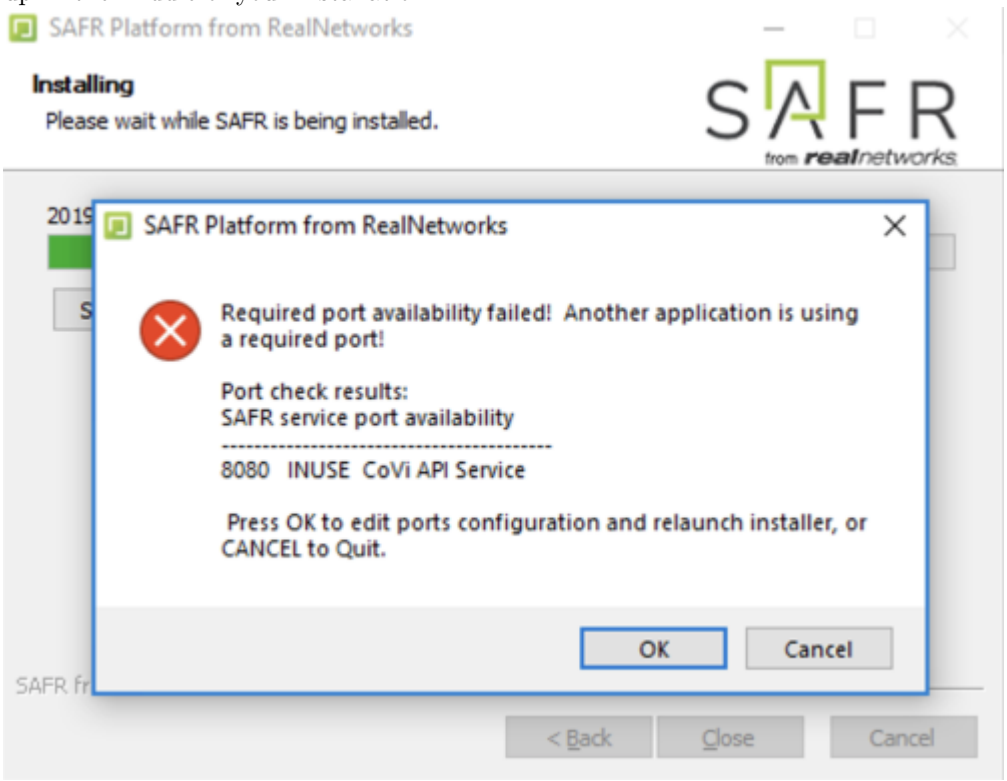

Do the following:

1. Open the Genetec Config Tool.
2. Open **Tasks > Administration > Video**.
3. Click the arrow next to the Video Unit button in the bottom left corner, and select **Media Gateway**.
4. Click **Next**, and in the *Create Media Gateway* wizard, click **Create**. Accept the default values; no changes are needed.
5. Select **Media Gateway**, and click the **Properties** task.
    - This adds a *Media Gateway* entry in the list on left side.

6. Determine the user to be granted access to the media gateway.
    - This can be the SAFR user or a different user; we recommend using the same SAFR user unless you already have one configured to use the Media Gateway.
    - This user does not need to have specific permissions. The permissions for media gateway are granted to this user in the next step.
7. To add this user to the **Accessible To** section, click the + icon. In the bottom right, click **Apply** to save the changes.
8. When prompted, enter a password for the user you are adding.
    - This password can be the same as the user's normal password or it can be different.
9. Save the *username* and *password*.
    - This is the password that must be used in the Media Gateway credentials fields in the SAFR preferences window.

## 73.3 Install and Configure SAFR

1. On the machine(s) where you plan to install the SAFR Desktop client, install the Genetec SDK from the Genetec Portal.
2. Go to the SAFR Download Portal.
3. If you're doing a cloud deployment, download and install Windows SAFR Edge. Make sure to select the Genetec SDK install option.
4. If you're doing a local deployment, download and install Windows SAFR Platform. Make sure to select the Genetec SDK 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.

### 73.3.1 Connect SAFR to Genetec

1. Within your SAFR Desktop client, select **Tools->Preferences->Genetec**.
   **Note**: If the Genetec preference tab is not showing, it means that the Genetec SDK was not properly installed on your machine.


2. Enter the following information in the Genetec preferences tab.
   - **Username**: Enter the SAFR user you created earlier.
   - **Password**: Enter the *Password* you created for the SAFR user.
   - **Directory**: IP address of the server running the Genetec Security Center server.
   - **Media Gateway**: Used for acquiring video streams.
     - **Username**: Enter the SAFR user you created earlier.
     - **Password**: Enter the *Password* you created for the SAFR user.
     - **Port**: Enter the port on which to connect to the Media Gateway. You can use the default value of `654` unless that would create a port conflict.

This should cause your SAFR system to establish a connection with the Genetec system.

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

1. On the SAFR Desktop client, open **Tools -> Preferences -> Camera**.
2. Cameras connected to Genetec system should be visible.
3. All cameras connected to Genetec have the *Genetec* prefix in their names.

## 73.4 Troubleshooting

### 73.4.1 How do I Resolve a Certificate Registration Error when Logging in from SAFR to Genetec?

This error is caused by a mismatch between the SAFR Genetec certificate and the Genetec Security Center license. SAFR builds have either a Genetec production certificate or a development certificate. The production certificate can be used only with Security Center installations that use a production or demonstration license. The development certificate can be used only with Security Center installations that use a development license.

Here are some steps you can take to try to diagnose the issue:

1. Use the Genetec Config Tool to connect to the Genetec Security Center server.
2. Click **About** on the left side.
3. Click the **Certificates** tab.
4. If you see a line that says, "Generic certificate for developers" then the Security Center server is using a developer license. You must use a SAFR build that uses a developer certificate. Builds with developer certificate are available only from SAFR build farm and should be used only by developers.
5. If that line is not present, then Security Center is using a production or demonstration license. You must use a SAFR build that uses a production certificate. Download SAFR build with production certificate from the SAFR Download Portal.
   - Click on the **Purchase Order** tab. Production or demonstration licenses must also have a license for SAFR attached to it. There should be a line with `Part #GSC-1SDK-RealN- FaceRec`. The quantity must be equal to or greater than the number of cameras that SAFR will be processing.

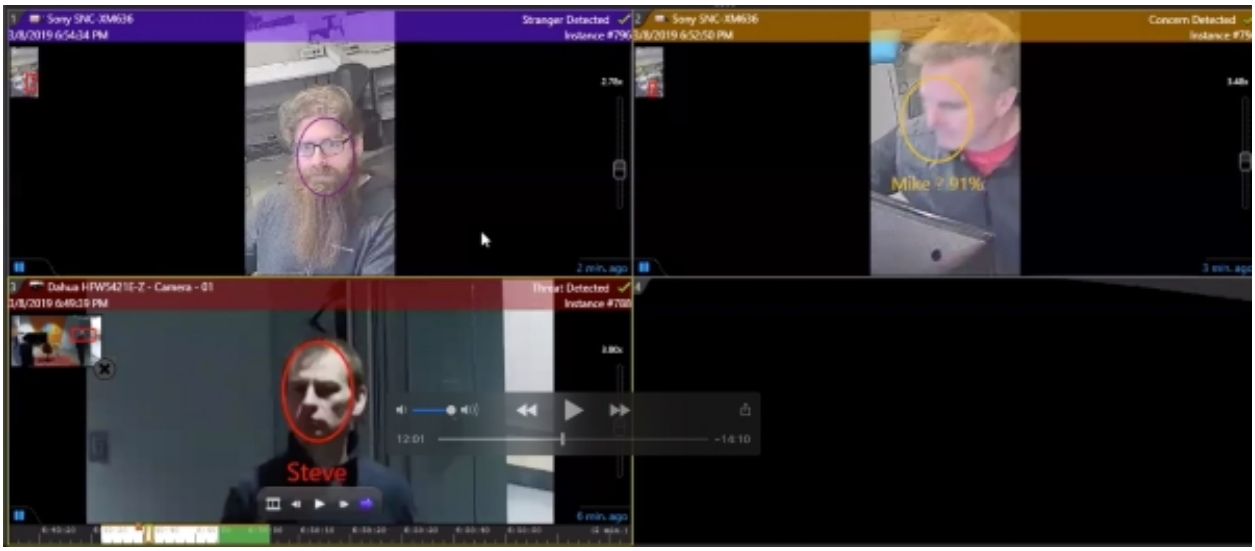
### 73.4.2 How do I Resolve a Connection Error when Logging in from SAFR to Genetec?

There can be many different causes for a Connection Timeout error from SAFR. However, if you are in a situation where this consistently happens and no cameras are connecting, then doing the following will most likely resolve the error:

1. Connect to the Security Center server using the Genetec Config Tool.
2. Go to the **Video** task.
3. In the left pane, right-click on the **Media Gateway** role.
4. Select the **Maintenance->Deactivate** role.
5. After the role turns gray, right-click on it again.
6. Select the **Maintenance->Activate** role.
7. The Media Gateway will go through a startup routine. It will turn red, yellow, and eventually white.
8. After it turns white, try connecting again.

# 74 SAFR-Genetec SDK Operation Guide

Integrating SAFR's facial recognition and analysis capabilities into Genetec enables you to use SAFR's video feed information overlays within Genetec 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 infomation such as age, gender, sentiment, name, company, known associates, or any other configurable information you want to create. Below is an example of what you might see when you integrate SAFR with Genetec's video feeds:

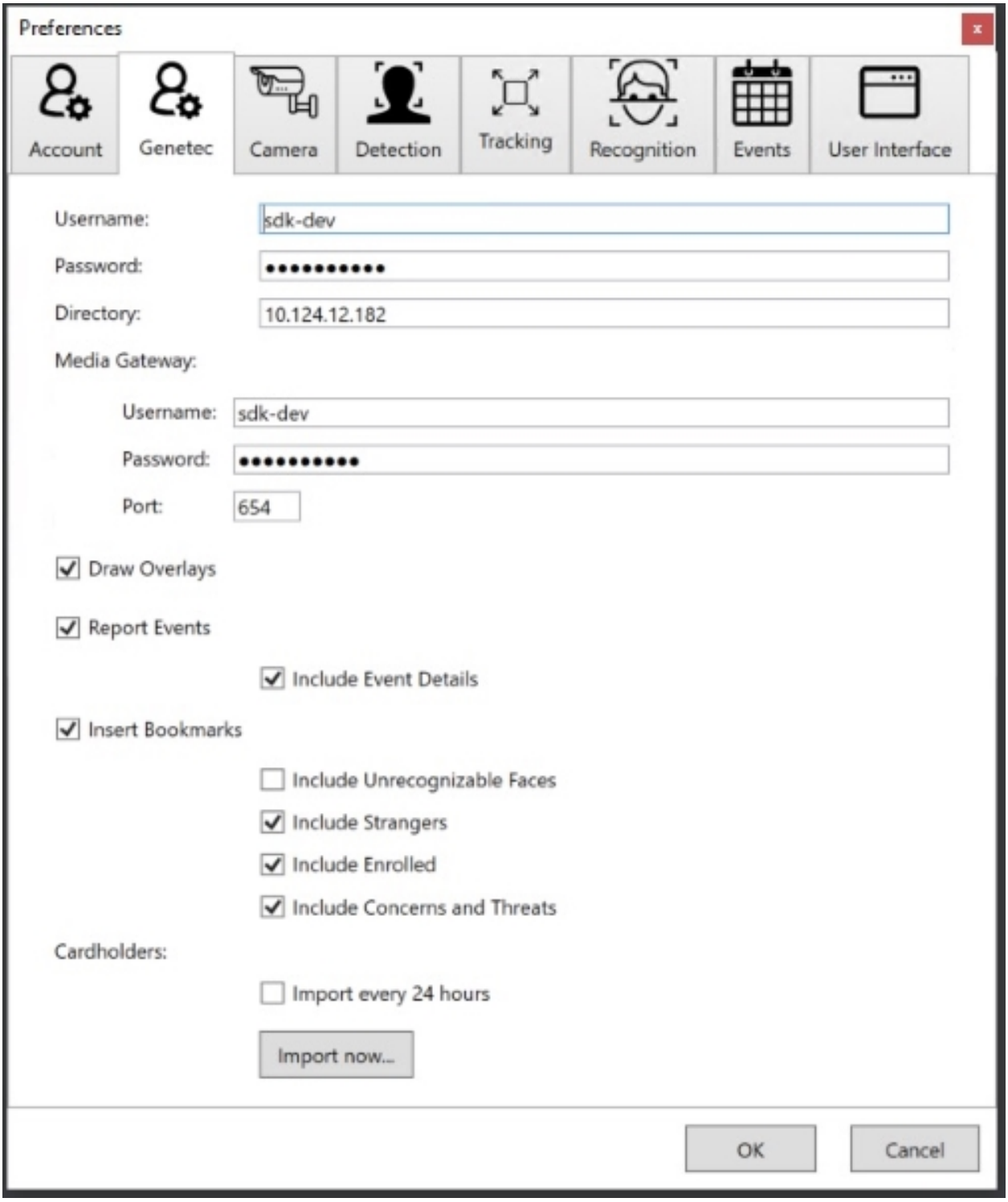



The person in the top left is a stranger, the person in the top right is has been flagged as a person of concern, and the person in the bottom left is a known threat. The information is conveyed by the color of their overlays. For more information on what the overlay colors mean, see Interpret Video Feed Overlays.

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

## 74.1 SAFR Genetec Preferences

You can set several Genetec-specific preferences by opening the SAFR Desktop client and clicking on **Tools -> Preferences -> Genetec**.




- **Username**: Person with the credentials to connect the SAFR system to the Genetec Security Center Server.
- **Password**: Password of a person with credentials to connect the SAFR system to a Genetec Security Center Server.
- **Directory**: IP address or hostname of the Genetec server.
- **Media Gateway**: Used for acquiring video streams.
  - **Username**: Person with the credentials to connect the SAFR system to a Genetec Security Center

Server.
    - **Password**: Password of a person with credentials to connect the SAFR system to a Genetec Security Center Server.
    - **Port**: The port at which SAFR will connect to the Genetec Security Center Server. The default is 654.
- **Draw Overlays**: Enables the drawing of ovals, names, and other details within Genetec camera video stream. The overlays match what would be shown in the SAFR Desktop client, so SAFR settings affecting SAFR overlays also affect what is drawn in Genetec.
- **Report Events**: Enables reporting SAFR events to Genetec. If this setting isn't checked, *Include Event Details* is automatically greyed out.
    - **Include Event Details**: When enabled, all of the technical details of the event are attached to events. This option is especially useful if an operator uses macros to handle events for decision making.
- **Insert Bookmarks**: When enabled, bookmarks are added to camera video streams events. This allows operators to search videos for events or recognized people names. Care should be taken as to what to include since encountering many faces can cause numerous bookmarks to be created. When this box isn't checked, the 4 children settings below are all greyed out.
    - **Include Unrecognizable Faces**: When enabled, adds bookmarks when a face is detected but SAFR does not have enough information to determine if they are a stranger or a known person. This can result in an overwhelming number of bookmarks, so it's disabled by default. However, this setting can be useful when monitoring areas with very few people.
    - **Include Strangers**: When enabled, adds bookmarks when a face is recognized and determined to be a stranger. This option is generally useful for secured areas where only known people should be.
    - **Include Enrolled**: When enabled, adds bookmarks when a face is recognized and determined to be a known person.
    - **Include Concerns and Threats**: When enabled, adds bookmarks when a face is recognized and determined to be a known concern or threat.
- **Cardholders**
    - **Import Every 24 Hours**: When enabled, all the Genetec cardholders not already in SAFR's Person Directory are imported and registered to SAFR every 24 hours.
    - **Import now...**: Clicking this causes all the Genetec cardholders not already in SAFR's Person Directory to be imported and registered to SAFR.

## 74.2 Connect and Use Cameras and Video Feeds

1. To connect cameras to Genetec, you need to add the cameras to the Genetec Video Archiver using the Genetec Config Tool. For details, please see the Genetec Security Center Administrator Guide.
2. After a camera has been added to the Video Archiver, it should be displayed as a Genetec camera in SAFR. If it's not, try closing and re-opening the SAFR Desktop client.
   To get SAFR video feed overlays to be displayed on Genetec camera feeds, do the following:
    1. Open the SAFR Desktop client.
    2. Select the Genetec version of the camera from the menu in the main windows (upper left). The word "Genetec" will be the first part of the camera name.
    3. After the client has successfully connected to the Genetec camera, video from the Genetec camera is displayed in the SAFR Desktop client video feed window.
    4. Open the Genetec Security Desk.
    5. Go to the **Monitoring** Task.
    6. Drag and drop a camera from the left side into one of the tiles in the middle.
    7. The camera feed should appear and show the same video feed overlays that are in SAFR.

To connect additional cameras:

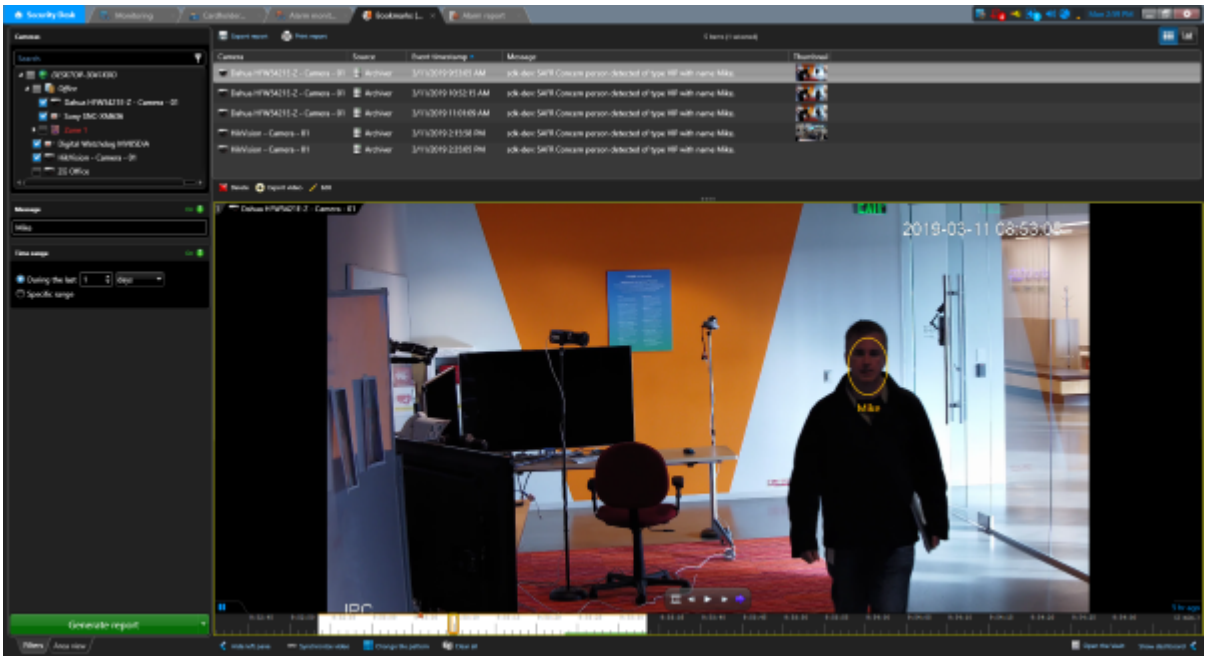
1. Open another instance of the Desktop client by selecting **File > New** on the client.
2. Repeat steps 2-6 above.

3. You can keep repeat this procedure to add overlays to as many video feeds as desired.
   **Note**: Most machines can only support up to 16 video feeds. If you want to connect more feeds than that, you'll need to install the SAFR Desktop client on additional machines.

By default, the SAFR Desktop client operates in the *Enrolled Monitoring* video processing mode and generates events and bookmarks into the Genetec system for every registered person. If you want a different mode for a given camera, choose a different mode from that camera's *Camera* window **Mode Selector** menu.

### 74.2.1 Bookmarks

SAFR enhances Genetec's bookmarks so that they provide readily accessible additional information, making the bookmarks much more useful. Bookmarked video contains the video feed overlays and enhanced people-related data described above. In addition, the bookmarks themselves are populated with the attributes for each person in the camera view so that searching bookmarks is more fruitful. All bookmarks automatically contain the *Person Type*, *ID Class*, and *Name* of each recognized person, and additional attributes such as *Age* and *Gender* will be included within the bookmarks, if such additional attributes are known. The image below shows how bookmarks can be used to review important events. The yellow overlay indicates that the person is a concern.



## 74.3 Genetec Cardholders and SAFR Identities

Genetec cardholders can be registered to SAFR by doing the following:

1. Increase the Genetec Security Center setting for thumbnail size to make sure SAFR has access to high quality images to use for face recognition.
2. On the SAFR Desktop client, click **Tools > Preferences > Genetec**.
3. In the Cardholders section click **Import Now...**. Pressing this button causes the following to occur:
   - Each imported cardholder is given a *Person Type* based on their assigned group.
   - If a cardholder has multiple group memberships, the cardholder group with the highest access privilege is used to define the group.
   - After import, SAFR updates the events in Genetec to make sure Genetec has one event for each *Person Type*.
4. You can configure SAFR to import new cardholders every 24 hours by selecting the **Import Every 24 Hours** check box.

You can also register people to SAFR by using SAFR's native functionality. For more information, see Importing and Registering People. Although people registered with SAFR are never synchronized to Genetec, you may want to register people to SAFR anyways when you want to add threats, concerns, or other registered people who may not be suitable as Genetec cardholders.

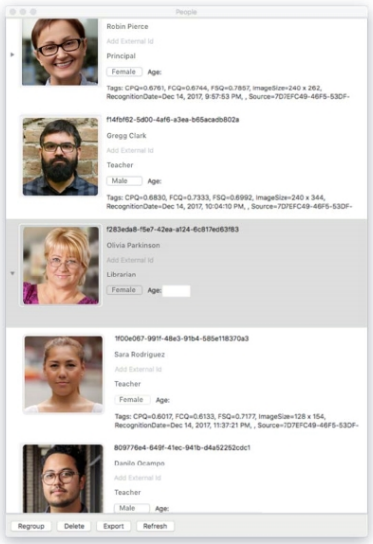
### 74.3.1 Edit Cardholder Data

You may want to edit people's properties to better manage which events get triggered when that person is recognized, For example, setting a person's *ID Class* to *Concern* or *Threat* triggers the corresponding alarms, while changing a cardholder group can allow you to trigger a VIP alert for specific cardholder groups. The most important people attributes are the *Name*, *Image*, *Person Type*, and *ID Class*.

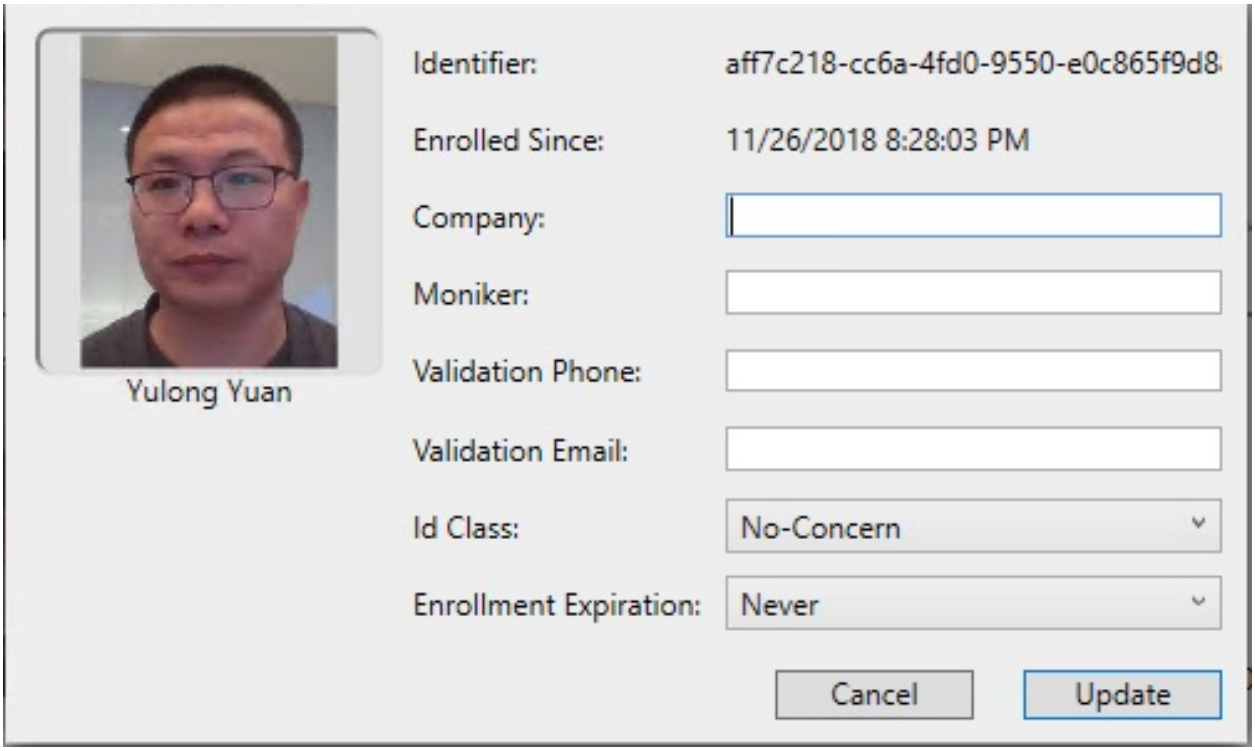
Attributes should be edited through Genetec Security Center whenever possible. *Person Type* defines a person's role (for example, staff or visitor) while the *ID Class* defines the risk level (No-Concern, Stranger, Concern, or Threat). *Person Type* and *Image* can be edited in Security Center by changing the cardholder group a person belongs to.

To edit these attributes, open Cardholder Management in Genetec Config Tool and update the desired users. After making changes, make sure to either manually synchronize users or set automatic synchronization as described previously in the "Register Cardholders".

*ID Class* and any other attributes of a person must be edited in SAFR's People dialog accessed through the Desktop client > Tools menu. All cardholders imported from Genetec Security Center are assigned an *ID Class* of *Normal*. To edit the *ID Class* of a person, click **Tools > People** in the Desktop client. The following window is displayed:




The *Person Type* and *Name* attributes can be edited by clicking their respective fields in the People window. To edit *ID Class*, in the **People Edit** dialog, double-click the user and choose the desired value from the *ID Class* menu as shown in the following image:

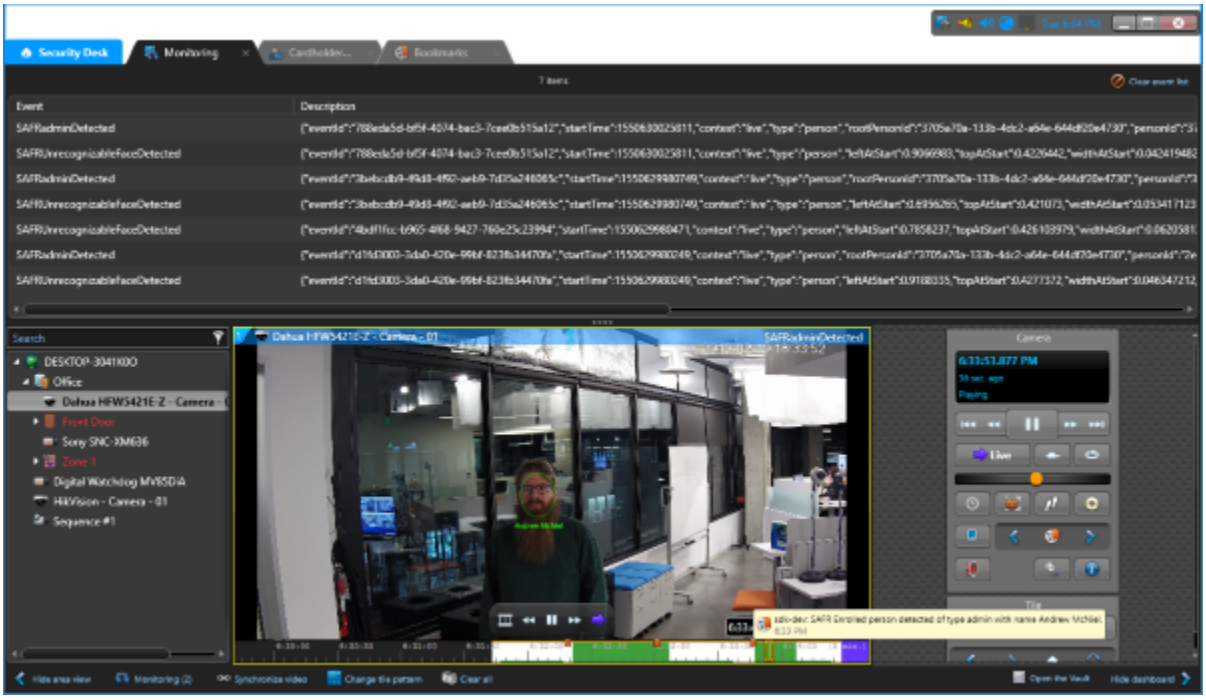



## 74.4 SAFR Events

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*.

There are several different combinations of the conditions that are triggered. The following image shows multiple events populated in the Genetec alerts panel. Clicking any of the events allows the video from that event to be replayed:



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

| Event Message | Id Class | Named | Person Type | Condition | People Attributes |
|---|---|---|---|---|---|
| Unrecognizable face 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" |
| Registered person detected without name | Normal | No | None | Registered person without name or person type assigned | idClass="noconcern" && personType="" && name="" |
| Registered person detected with name <name> | Normal | Yes | None | Registered person with name but no person type | idClass="noconcern" && personType="" && name=<name> |
| Registered person detected of type <personType> | Normal | No | Defined | Registered person with person type but no name | idClass="noconcern" && personType=<personType> && name="" |

| Event Message | Id Class | Named | Person Type | Condition | People Attributes |
|---|---|---|---|---|---|
| Registered person detected of type <personType> with name <name> | Normal | Yes | Defined | Registered person with person type and name | idClass="noconcern" && personType=<personType> && name=<name> |
| Concern person detected without a name | Concern | No | None | Same as above for Concern | idClass="concern" && personType="" && name="" |
| Concern person detected with name <name> | Concern | Yes | None | Same as above for Concern | idClass="concern" && personType="" && name=<name> |
| Concern person detected detected of type <personType> | Concern | No | Defined | Same as above for Concern | idClass="concern" && personType="" && name="" |
| Concern person detected of type <personType> with name <name> | Concern | Yes | Defined | Same as above for Concern | Registered person marked as concern detected with name assigned. |
| Threat person detected without a name | Threat | No | None | Same as above for Threat | idClass="threat" && personType="" && name="" |
| Threat person detected with name <name> | Threat | Yes | None | Same as above for Threat | idClass="threat" && personType="" && name=<name> |
| Threat person detected of type <personType> | Threat | No | Defined | Same as above for Threat | idClass="threat" && personType=<personType> && name="" |
| Threat person detected of type <personType> with name <name> | Threat | Yes | Defined | Same as above for Threat | idClass="threat" && personType=<personType> && name=<name> |

### 74.4.1 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 Genetec Security Center integration. For a complete description, see Connect to a Video Feed in the *SAFR Documentation*.

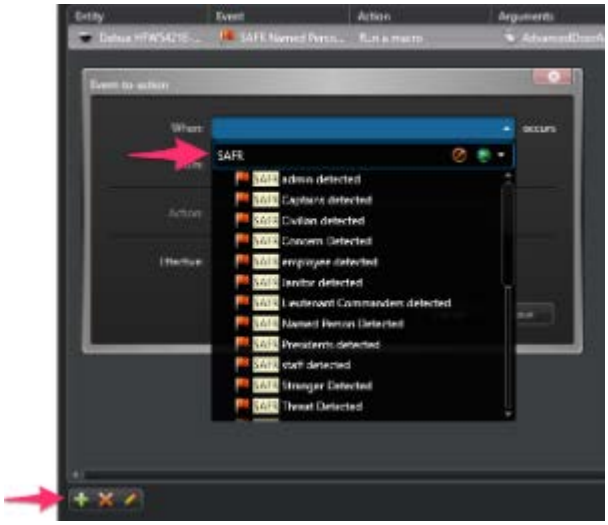
- **Secure Access**: Only triggers events when cardholders and people registered in SAFR's Person Directory are identified with a high degree of certainty. This mode is useful when the system is being used to manage physical access. (i.e. When the system is responsible for unlocking doors for authenticated 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.

### 74.4.2 Add and Configure Alerts

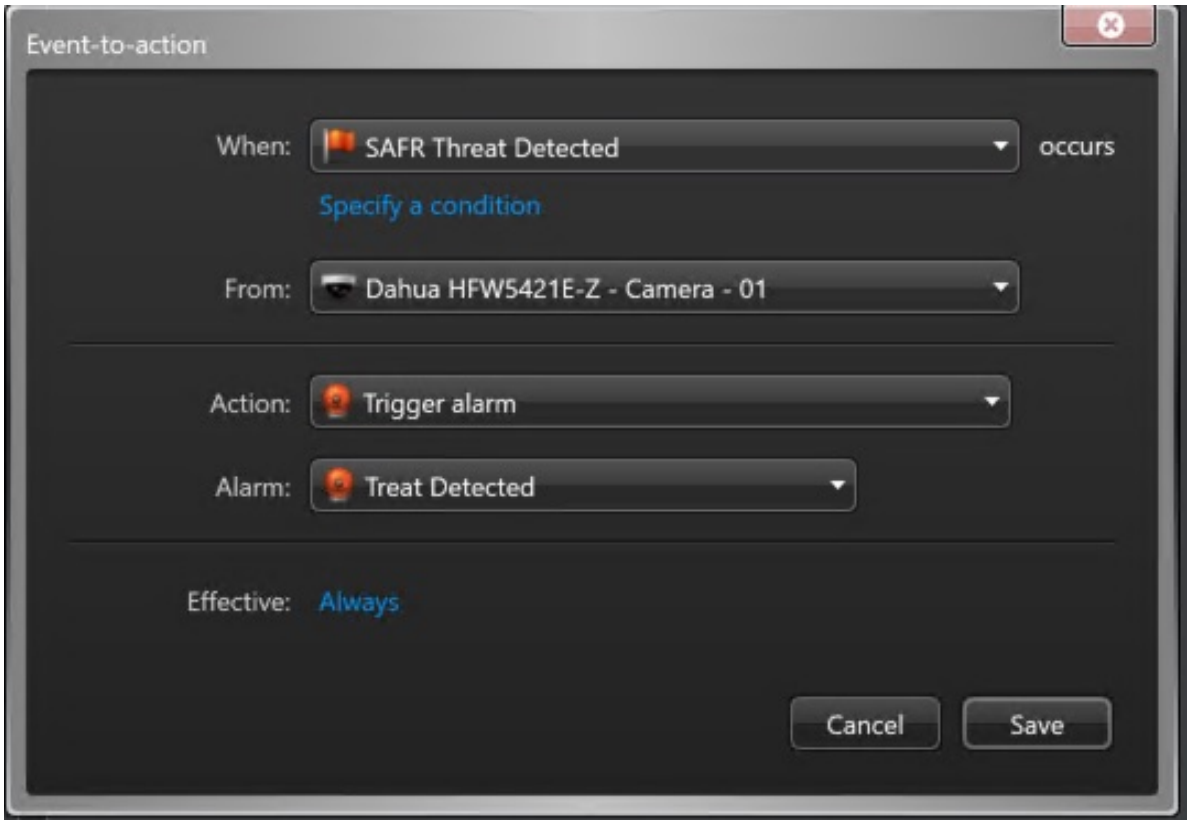
To trigger the alert as a result of a SAFR-generated event, do the following:

1. Open the Genetec Config Tool, and go to the System Panel.


2. Click the + icon to add a new alarm, and click the When menu. Type *SAFR* and press **Enter** to see the list of SAFR-enabled alarms.



3. Choose the desired entry from the list.
4. Under **From**, choose the camera you want to use to trigger the event. Under **Action**, choose a desired action. (e.g. Trigger Alarm)




5. Click **Save** when done.

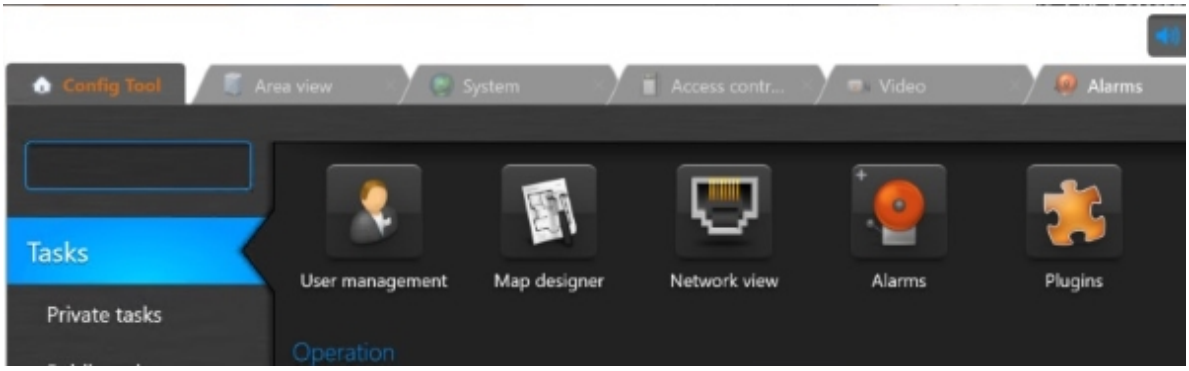
SAFR Events can be tied to Actions which can then trigger an Alarm. Initially create an alarm you want to trigger, and then use Genetec Event-to-Action dialog to tie SAFR Events to any action that can be defined in the Genetec system (for example, Trigger Alarm).

### 74.4.3 Add an Alarm

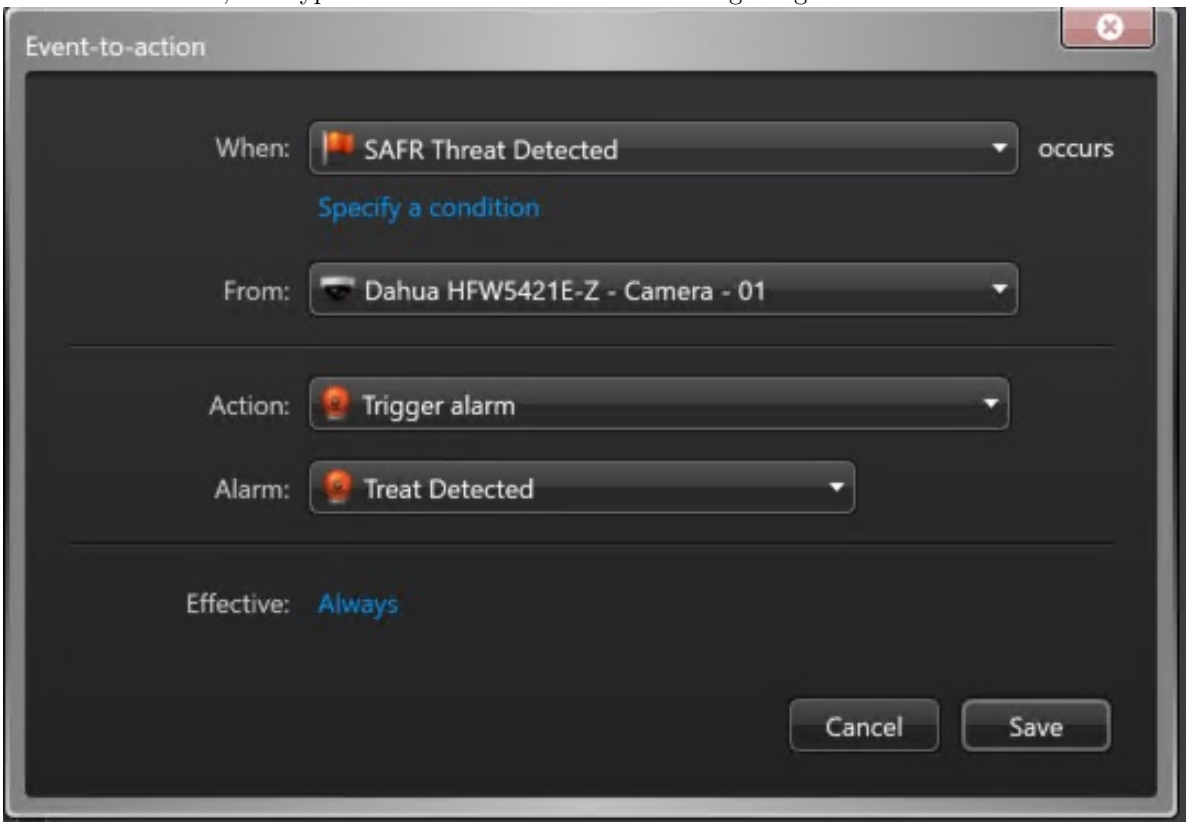
An alarm can be used to make sure an important event is noticed. In this example, we show how to create an alarm that is triggered when someone who has been marked as a threat is recognized on one of the cameras. For more information on triggering events, refer to Genetec support documentation.

To create an alarm, do the following:

1. Open the Genetec Config Tool, and open the Alarms screen.




2. Click **Add Alarm**, and type a *Name* as shown in the following image:




3. Click **Save** to save the alarm.

### 74.4.4 Recommended Settings for Alarms

| | |
|---|---|
| Properties task | Choose priorities based on circumstances and your organization guidelines (1=high, 255=low)<br>• Stranger: 100 (If infrequent, set high)<br>• Concern: 50<br>• Threat: 10<br>Video display option<br>Set to Live to see the live view when alarm loads video<br>Playback may be useful for short events where the subject may have walked off the screen by the time the video loads<br>• If playback mode, set to at least 4 seconds to avoid buffering |
| Advanced task | Auto-Acknowledge: Good for stranger events; enter the number of seconds to stay in the view before returning to the view you were on prior to the event<br>Choose color to match the SAFR colors (add ref to section in manual that describes colors)<br>Reactivate threshold: Suppresses additional alarm if another similar alarm triggered within this time<br>• Adjust as needed for use case. |

#### 74.4.5 Trigger Macros

When SAFR is configured to *Include Event Details* in reported events, highly customized actions can be programmed using macros in the Genetec system. Event details include all information associated with the detected face (e.g. *Name*, *Person Type*, *Age*, *Gender*, *Sentiment*, etc.). For more information on macros, refer to the Genetec support documentation.

### 74.5 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 is poor (not many faces found or recognized), make sure the Genetec video feeds are set for a sufficiently large frame size.
- If events are not being triggered, check the following:
  - Permissions are set correctly on Event-to-Actions.
  - Make sure the applicable SAFR Video Processing Mode is selected.

# 75 SAFR-Genetec FR Framework Integration Guide

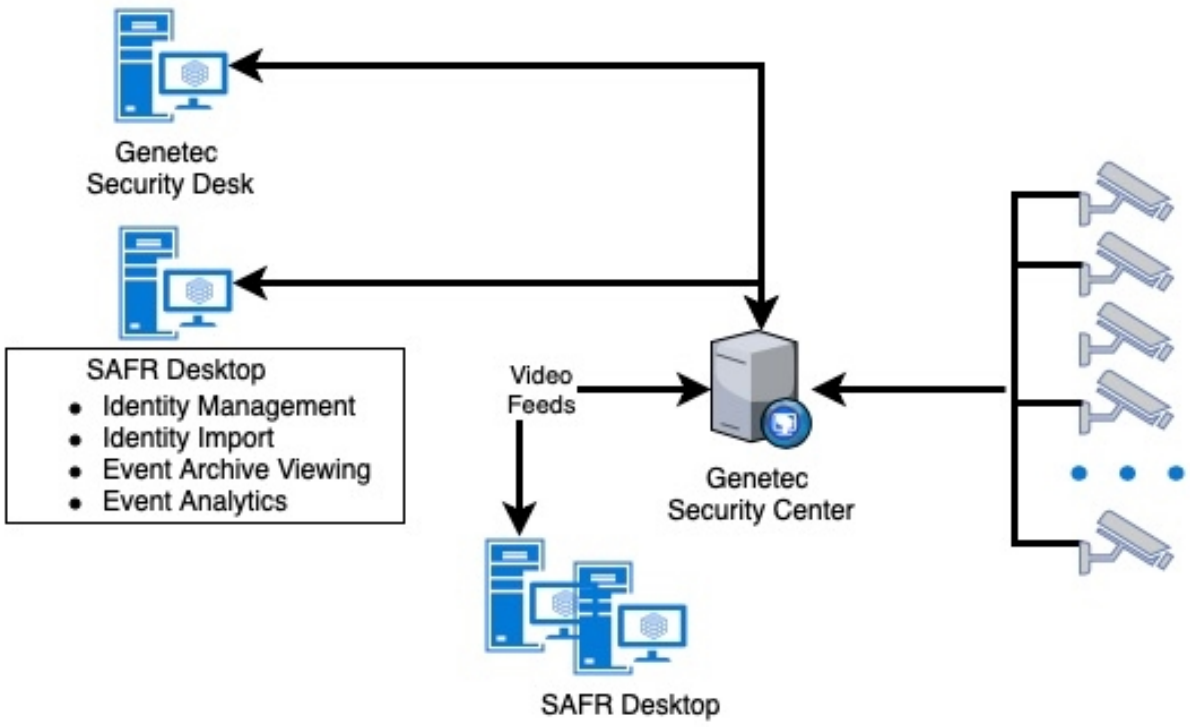
Integrating SAFR's facial recognition and analysis capabilities into Genetec enables you to use SAFR's video feed information overlays within Genetec camera video feeds, thus making it much easier to quickly and accurately separate unknown people from authorized people from known threats. You'll also have immediate access to additional infomation 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 Genetec alerts and other actions within the Genetec system.

## 75.1 Integration Overview and Requirements

A typical deployment requires the following:

- A machine running Genetec Security Center.
- A machine running Genetec Security Desk and Genetec Config Tool.
- 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 the Genetec Security Center. The SAFR Desktop client(s) can then connect to the Genetec Security Center to perform analysis of the video and add overlays. Depending on the number of cameras you need, one or more machines may be required to run the SAFR Desktop client, each processing multiple video feeds. The Desktop client processes the video and returns information to Genetic to overlay the video feeds and generate events. The Desktop is also used to perform various management activities.

### 75.1.1 System Requirements

Genetec has the following system requirements:

- One machine running Genetec Security Center Version 5.7 or later.

- One machine running Genetec Security Desk and Genetec Config Tool.
- Each machine running a Genetec product must meet the following system requirements:
  - Windows 10.
  - Additional system requirements as described here.
  - Genetec FaceReq plugin. **Note**: The installation of this plugin is performed when you install SAFR. See the Install and Configure SAFR section below for details.

SAFR has the following system requirements:

- One or more machines running Windows SAFR Desktop client 1.3.228 or later.
- Each machine running the SAFR Desktop client must meet the following requirements:
  - Windows 10.
  - Additional system requirements as described here.
- Local SAFR deployments require at least one machine running SAFR Platform 1.3 or later.
- Each machine running SAFR Server must meet the following requirements:
  - Windows 10.
  - Additional system requirements as described here.

### 75.1.2 Licensing and the Genetec Part Number

An accompanying Genetec part number must be added to your Genetec connection license. Do the following to discover and add the Genetec part number:

1. Go to the Genetec Portal and sign in using your Genetec credentials.
2. In the applications section, search for *SAFR*. From the results, click *SAFR Facial Recognition*.
3. On the **SAFR Facial Recognition Solution Details** page, in the right column, the *Genetec Part Number* is displayed.
4. Contact Genetec and have them add the part number to your license. You need a quantity of the part number equal to the number of cameras SAFR will be processing plus one additional license for the metadata channel SAFR creates. In other words, if SAFR will be processing cameras, then you need quantity of the part number added to your license.

You'll need the following licenses: each Genetec camera where SAFR face detection and recognition is used, you'll need:

- A Genetec connection license with the accompanying Genetec part number is required for each connected Genetec camera.
- One additional Genetec connection license for the metadata channel SAFR creates.
- A SAFR license for each camera is required.

For example, if you have 300 cameras but only need face detection on 30 cameras at a time, then you would obtain a 31 connection license from Genetec and a 30 camera license from RealNetworks. Having a 31 connection Genetec license does not mean you are limited to face detection on a fixed set of 30 cameras. At any time, you can choose to connect the SAFR Desktop client to a different camera. You may have cameras in your parking garage that you were not previously monitoring with SAFR recognition. You can use a few of your licenses that are connected to other cameras to connect to garage cameras instead.

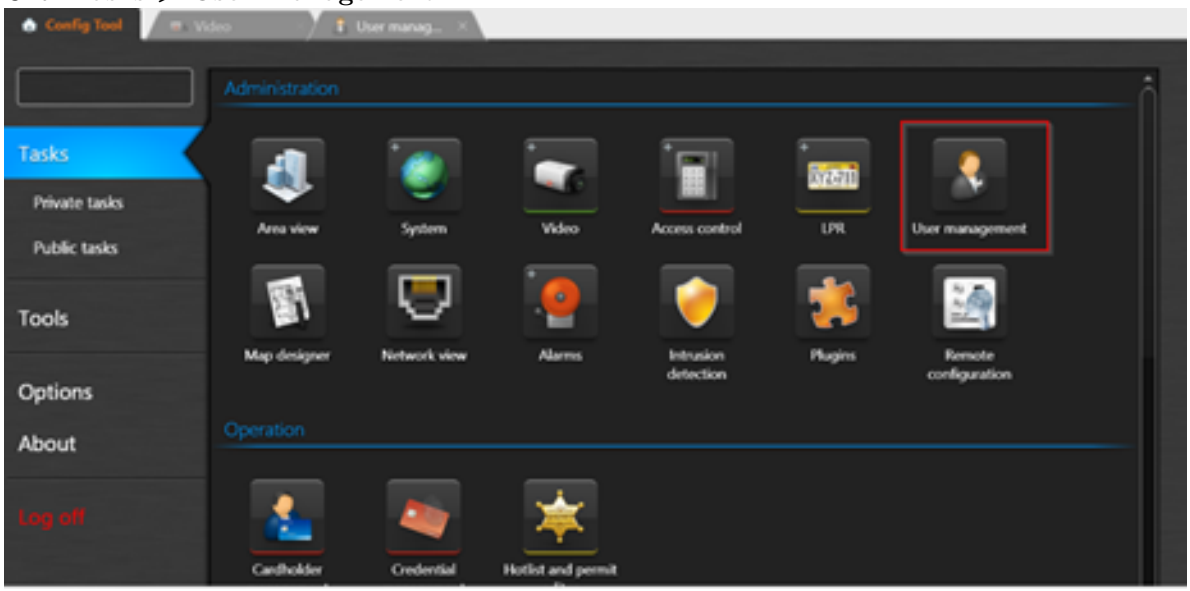
## 75.2 Install and Configure Genetec Products Security Center

1. Download the latest version of Genetec Security Center from the Genetec Portal.
2. Run the installer. For details about which install options to select, see the Security Center Installation and Upgrade Guide.
3. Download and install the latest Genetec SDK package.

### 75.2.1 Create a SAFR User

To create a user with the permissions that SAFR will require:

1. Open the Genetec Config Tool.
2. Click **Tasks > User Management**.




3. Create a new user (with a username of, for example, *SAFR*) with the following permissions:

   **All privileges**

   - Application privileges
     - Log on using the SDK

   **Administrative privileges**

   - Physical entities
     - View camera properties

   **Access control management**

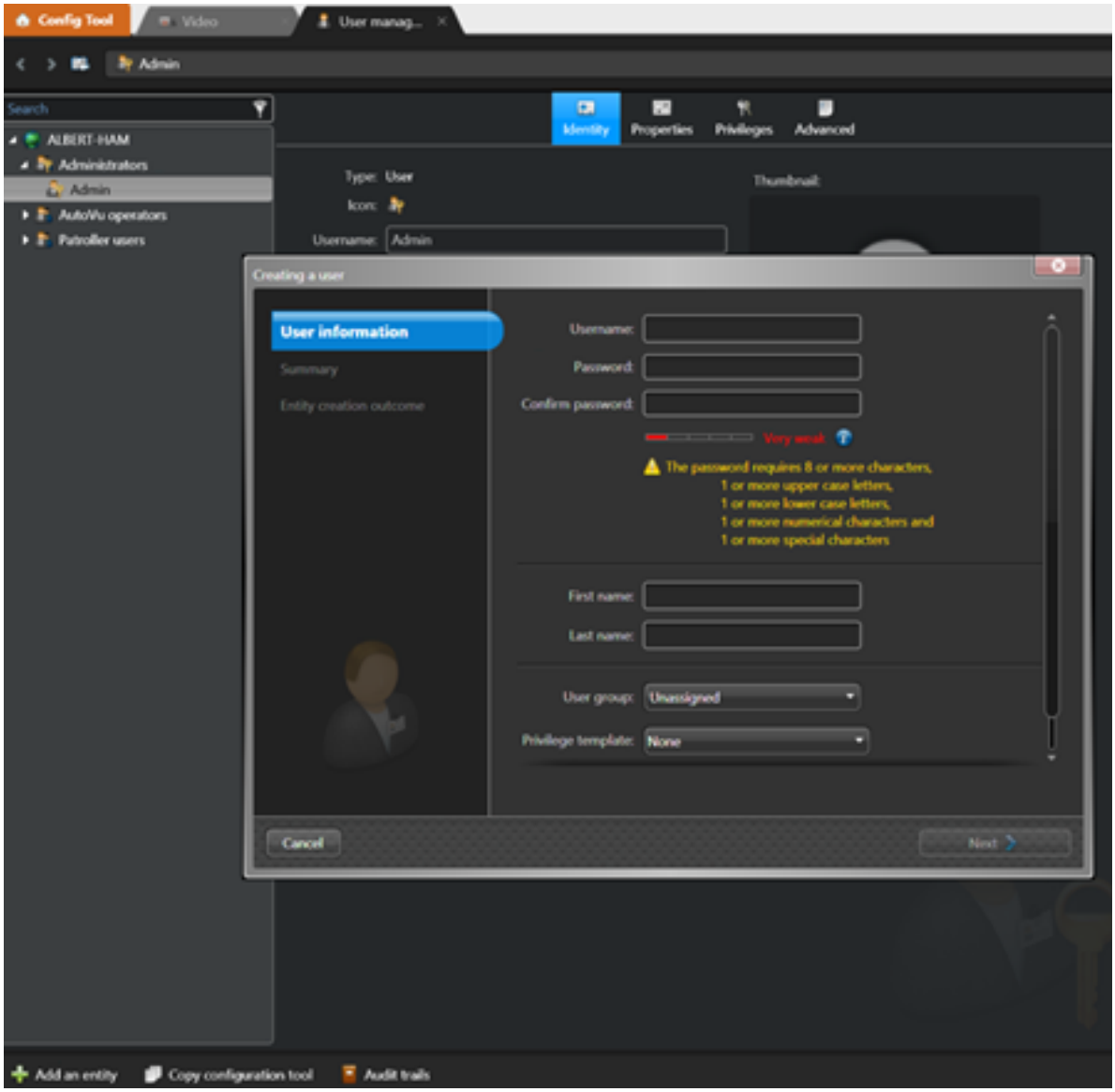
   - View cardholder group properties
   - View cardholder properties
   - View visitor properties

   **System management**

   - View general settings
     - Modify custom events

   **Action Privileges**

   - Cameras
     - View live video




### 75.2.2 Add Permissions for Event-to-Archive Actions

In order to create Event-to-Actions in the Genetec Config Tool, one or more of the following Action permissions must also be added to the SAFR user created in the previous section. Only those actions you want to trigger with SAFR events are needed:

**All privileges**

- Action privileges
  - Set threat level
  - Cameras
    - Protect video from deletion
    - Save/modify/print snapshots
  - Access control
    - Doors
      - Explicitly unlock doors
      - Override unlock schedules
    - Elevators

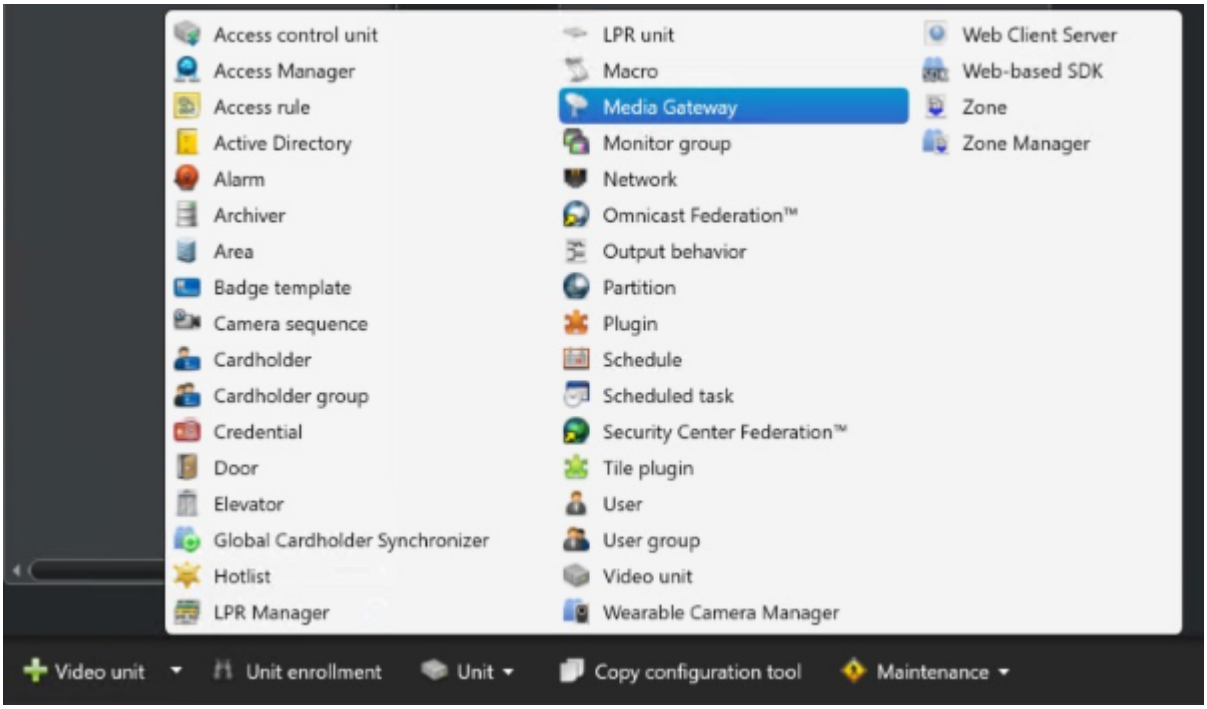
        - Override elevator schedules
    - Alarms
        - Trigger alarms
    - Users
        - Send a message
        - Send an email
        - Send/clear task
    - Macros
        - Execute macros
    - Zones
        - Arm/disarm zones
    - Areas
        - Modify people count

### 75.2.3 Set Minimum Cardholder Image Size

Do the following:

1. Open the Genetec Config Tool.
2. Open **Tasks > Administration > Access Control > General Settings**.
3. Set *Maximum Picture File Size* to 128k or larger.

### 75.2.4 Configure the Media Gateway



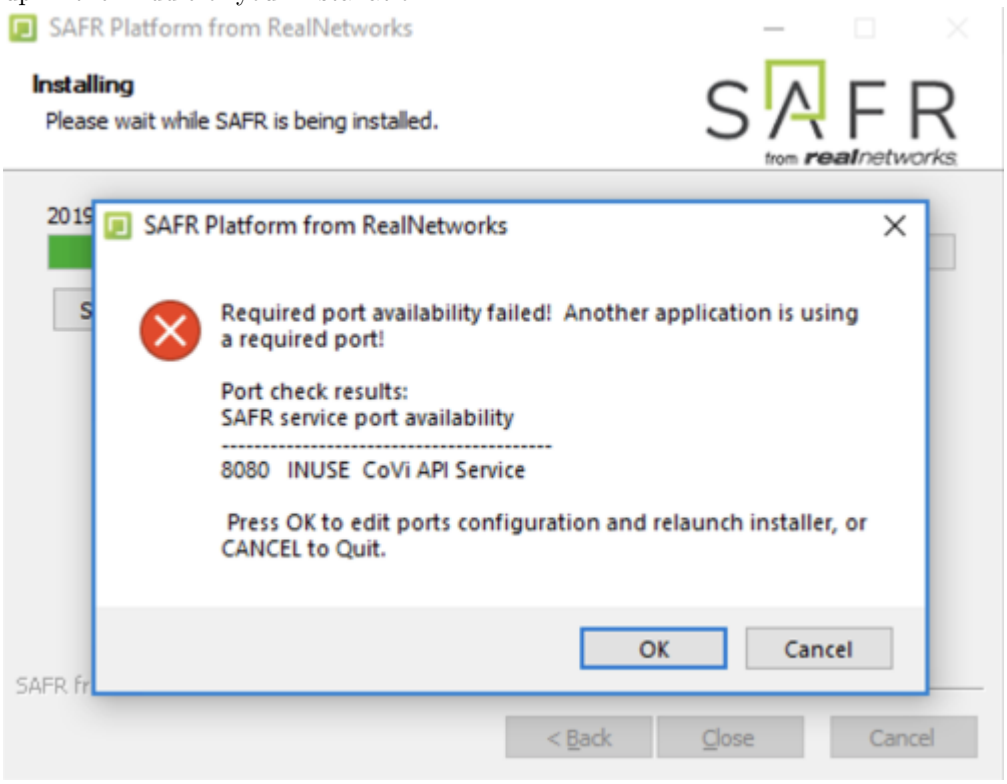

Do the following:

1. Open the Genetec Config Tool.
2. Open **Tasks > Administration > Video**.
3. Click the arrow next to the Video Unit button in the bottom left corner, and select **Media Gateway**.
4. Click **Next**, and in the *Create Media Gateway* wizard, click **Create**. Accept the default values; no changes are needed.
5. Select **Media Gateway**, and click the **Properties** task.
    - This adds a *Media Gateway* entry in the list on left side.

6. Determine the user to be granted access to the media gateway.
    - This can be the SAFR user or a different user; we recommend using the same SAFR user unless you already have one configured to use the Media Gateway.
    - This user does not need to have specific permissions. The permissions for media gateway are granted to this user in the next step.
7. To add this user to the **Accessible To** section, click the + icon. In the bottom right, click **Apply** to save the changes.
8. When prompted, enter a password for the user you are adding.
    - This password can be the same as the user's normal password or it can be different.
9. Save the *username* and *password*.
    - This is the password that must be used in the Media Gateway credentials fields in the SAFR preferences window.

## 75.3 Install and Configure SAFR

1. On the machine(s) where you plan to install the SAFR Desktop client, install the Genetec SDK from the Genetec Portal.
2. Go to the SAFR Download Portal.
3. If you're doing a cloud deployment, download and install Windows SAFR Edge. Make sure to select the Genetec FR Framework install option.
4. If you're doing a local deployment, download and install Windows SAFR Platform. Make sure to select the Genetec FR Framework 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\`.

5. After the installation finishes, a message will appear saying where you can locate the Genetec FaceReq plugin installer on your machine. Make a note of the installer location.
6. 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.
7. Go to the location specified in Step #5. Copy the installer (FaceRecSetup621.exe) to every machine running Genetec Security Center, and then run the installer on each of those machines.

Two icons will have appeared on your desktop: one labeled "SAFRActions" and another labeled "SAFR". *SAFRActions* launches SAFR Actions, while *SAFR* launches the Desktop client. If you did a local deployment, SAFR Server will be automatically running as a collection of background services.

### 75.3.1 Connect SAFR to Genetec

1. Within your SAFR Desktop client, select **Tools->Preferences->Genetec**.
   **Note**: If the Genetec preference tab is not showing, it means that the Genetec SDK was not properly installed on your machine.

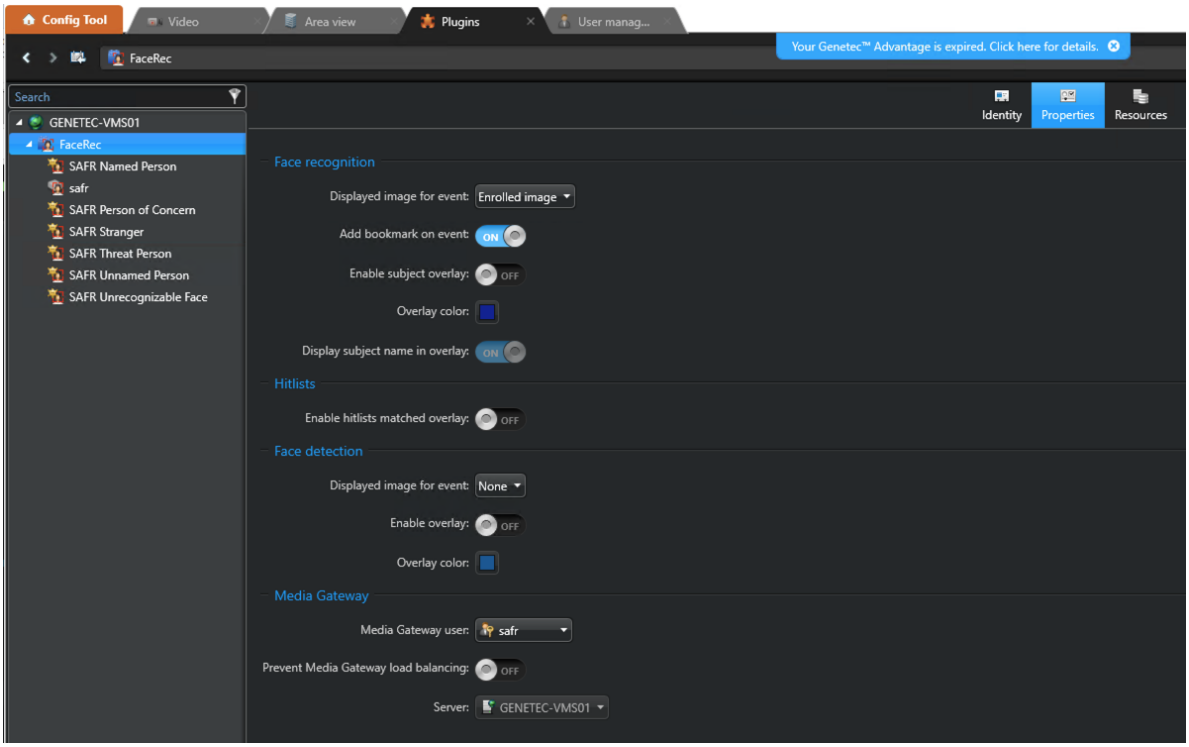
2. Enter the following information in the Genetec preferences tab.
   - **Username**: Enter the SAFR user you created earlier.
   - **Password**: Enter the *Password* you created for the SAFR user.
   - **Directory**: IP address of the server running the Genetec Security Center server.
   - **Media Gateway**: Used for acquiring video streams.
     - **Username**: Enter the SAFR user you created earlier.
     - **Password**: Enter the *Password* you created for the SAFR user.
     - **Port**: Enter the port on which to connect to the Media Gateway. You can use the default value of `654` unless that would create a port conflict.
       This should cause your SAFR system to establish a connection with the Genetec system.

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

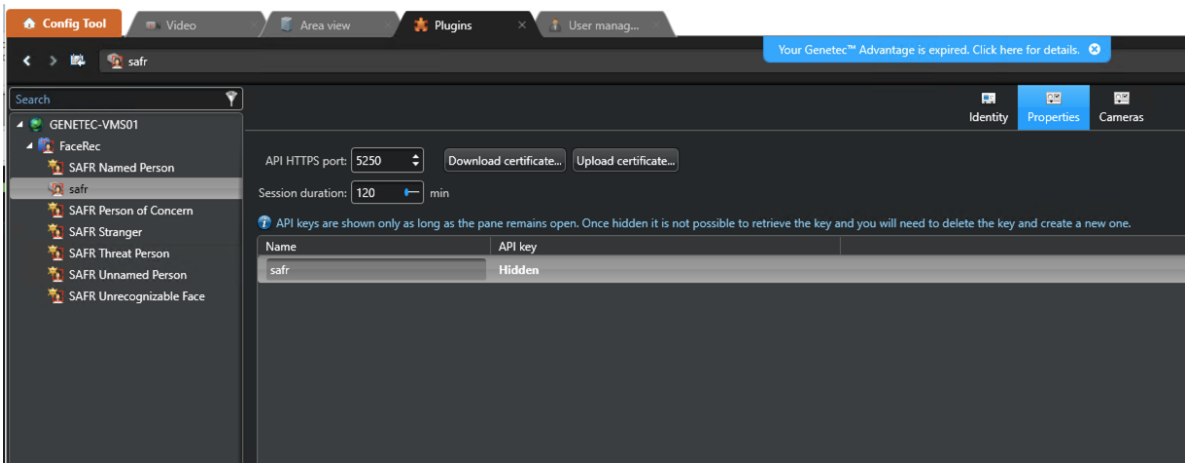
1. On the SAFR Desktop client, open **Tools -> Preferences -> Camera**.
2. Cameras connected to Genetec system should be visible.
3. All cameras connected to Genetec have the *Genetec* prefix in their names.

## 75.4 Configure the Genetec FaceReq Plugin

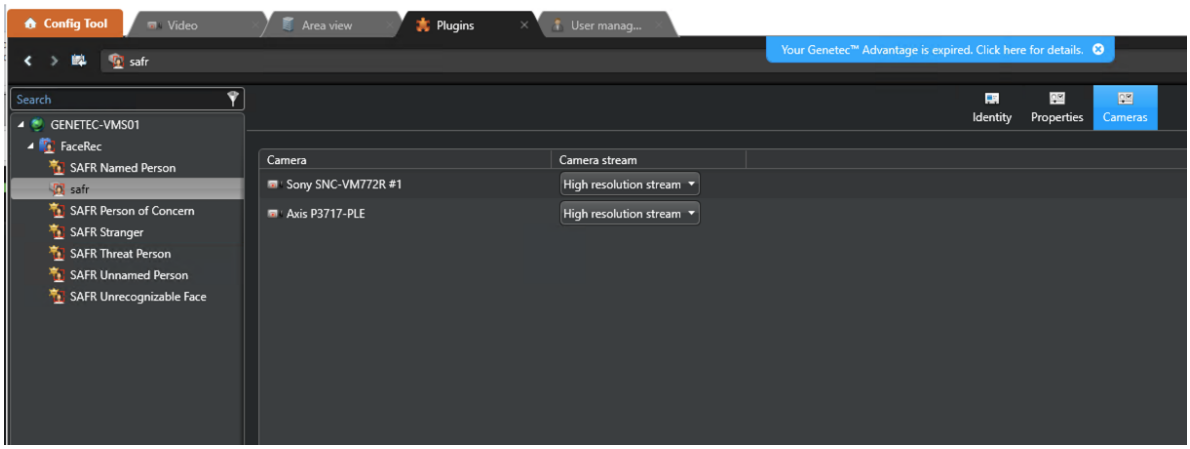
- Click Add an entry and choose Plugin and choose FaceRec
- Click Next, Next and Create to create the new unit
- Select FaceRec entity, click Add an entry and choose FaceRec Unit.
  - Enter "safr" as the same and click Save
  - Select Properties
    - Set the following features to OFF
      - Face recognition: Enable subject overlay
      - Hitlists: Enable hitlists matched overlay
      - Face detection: Enable overlay




- Select safr unit
  - Select Properties
    - In the API dialog area click the + button to add a new API Key entry
    - Name it “safr” and make a note of the API Key value (Value is only available once).
    - NOTE: API Key is used later when configuring SAFR Desktop
    - Click Apply




- Select Cameras
  - Click the + button and add all relevant cameras which require face recognition




## 75.5 Troubleshooting

### 75.5.1 How do I Resolve a Certificate Registration Error when Logging in from SAFR to Genetec?

This error is caused by a mismatch between the SAFR Genetec certificate and the Genetec Security Center license. SAFR builds have either a Genetec production certificate or a development certificate. The production certificate can be used only with Security Center installations that use a production or demonstration license. The development certificate can be used only with Security Center installations that use a development license.

Here are some steps you can take to try to diagnose the issue:

1. Use the Genetec Config Tool to connect to the Genetec Security Center server.
2. Click **About** on the left side.
3. Click the **Certificates** tab.
4. If you see a line that says, "Generic certificate for developers" then the Security Center server is using a developer license. You must use a SAFR build that uses a developer certificate. Builds with developer certificate are available only from SAFR build farm and should be used only by developers.
5. If that line is not present, then Security Center is using a production or demonstration license. You must use a SAFR build that uses a production certificate. Download SAFR build with production certificate from the SAFR Download Portal.
    - Click on the **Purchase Order** tab. Production or demonstration licenses must also have a license for SAFR attached to it. There should be a line with `Part #GSC-1SDK-RealN- FaceRec`. The quantity must be equal to or greater than the number of cameras that SAFR will be processing.

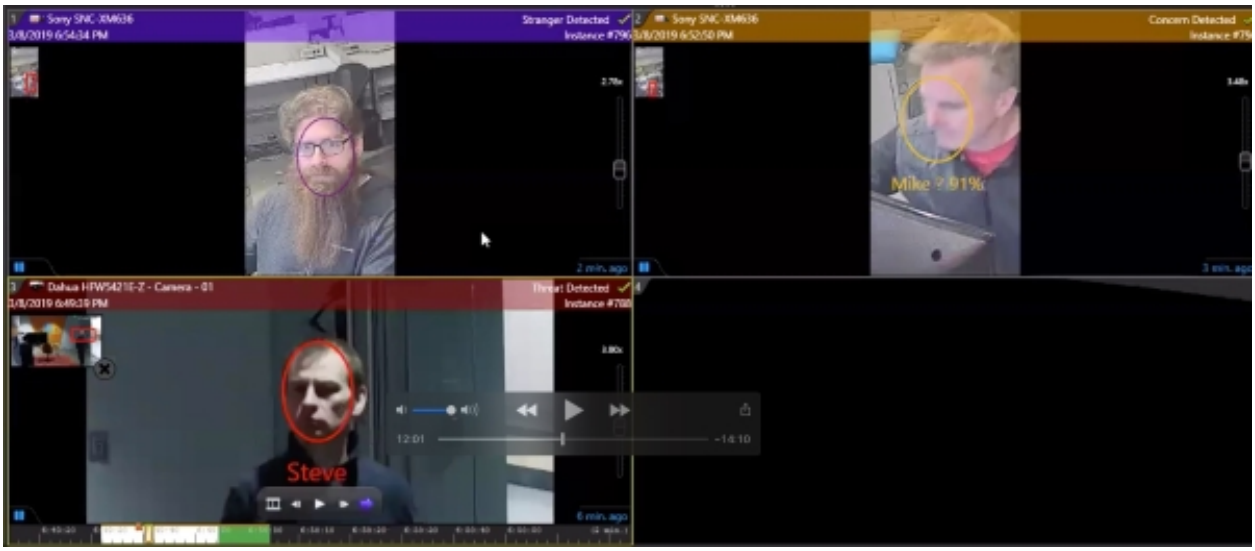
### 75.5.2 How do I Resolve a Connection Error when Logging in from SAFR to Genetec?

There can be many different causes for a Connection Timeout error from SAFR. However, if you are in a situation where this consistently happens and no cameras are connecting, then doing the following will most likely resolve the error:

1. Connect to the Security Center server using the Genetec Config Tool.
2. Go to the **Video** task.
3. In the left pane, right-click on the **Media Gateway** role.
4. Select the **Maintenance->Deactivate** role.
5. After the role turns gray, right-click on it again.
6. Select the **Maintenance->Activate** role.
7. The Media Gateway will go through a startup routine. It will turn red, yellow, and eventually white.
8. After it turns white, try connecting again.

# 76 SAFR-Genetec FR Framework Operation Guide

Integrating SAFR's facial recognition and analysis capabilities into Genetec enables you to use SAFR's video feed information overlays within Genetec 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 infomation such as age, gender, sentiment, name, company, known associates, or any other configurable information you want to create. Below is an example of what you might see when you integrate SAFR with Genetec's video feeds:

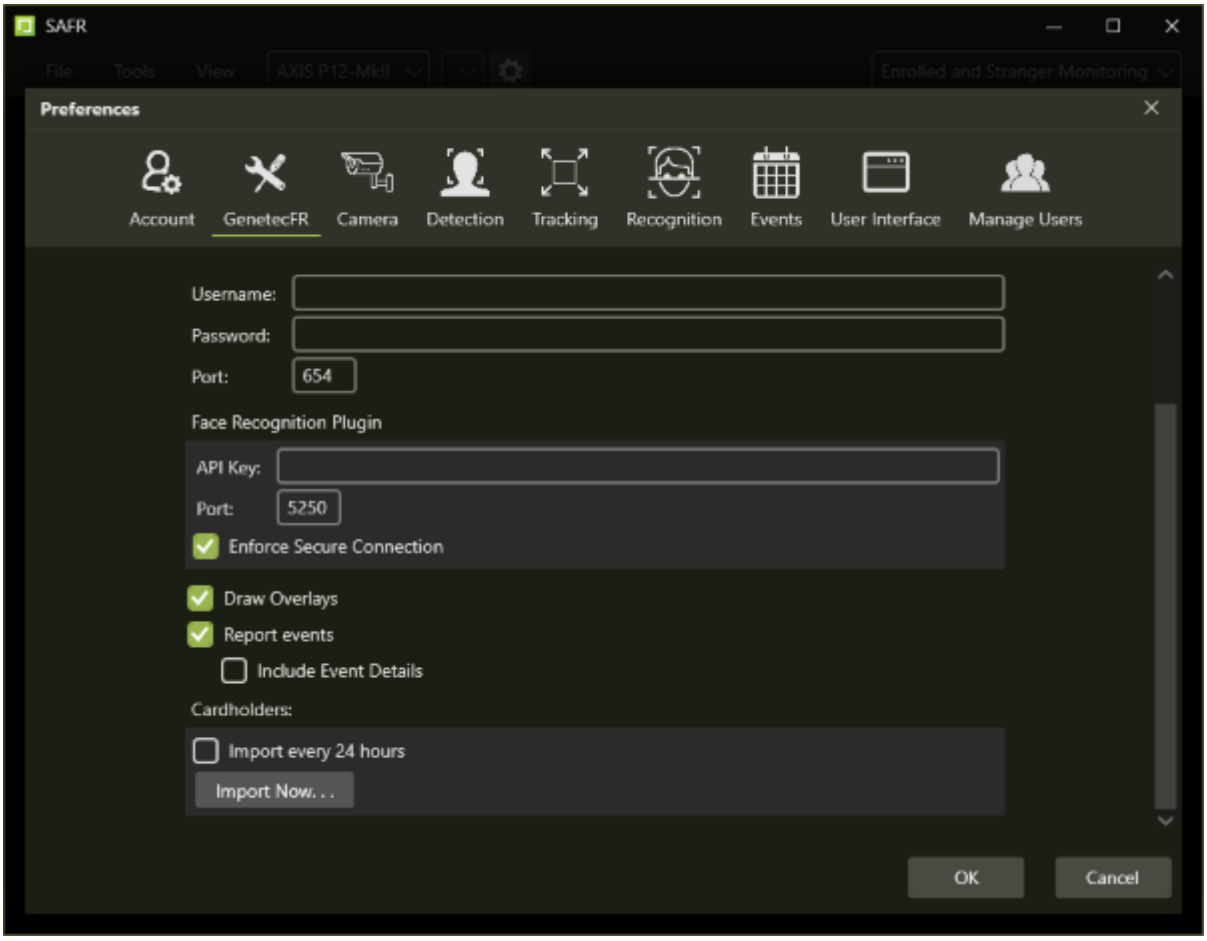



The person in the top left is a stranger, the person in the top right is has been flagged as a person of concern, and the person in the bottom left is a known threat. The information is conveyed by the color of their overlays. For more information on what the overlay colors mean, see Interpret Video Feed Overlays.

Integrating the two systems also allows SAFR's information about individuals to trigger Genetec alerts and other actions within the Genetec system.

## 76.1 SAFR Genetec Preferences

You can set several Genetec-specific preferences by opening the SAFR Desktop client and clicking on **Tools -> Preferences -> Genetec**.




- **Username**: Person with the credentials to connect the SAFR system to the Genetec Security Center Server.
- **Password**: Password of a person with credentials to connect the SAFR system to a Genetec Security Center Server.
- **Directory**: IP address or hostname of the Genetec server.
- **Media Gateway**: Used for acquiring video streams.
  - **Username**: Person with the credentials to connect the SAFR system to a Genetec Security Center Server.
  - **Password**: Password of a person with credentials to connect the SAFR system to a Genetec Security Center Server.
  - **Port**: The port at which SAFR will connect to the Genetec Security Center Server. The default is 654.
- **Face Recognition Plugin**:
  - **API key**: The API key set within the *Face Recognition Activities* section of the Genetec Security Desk.
  - **Port**: The port value used by the *API key* specified within the Genetec Security Desk.
- **Enforce Secure Connection**: When enabled, it requires that a TSL/SSL connection be established with the FaceReq server. Although this setting is enabled by default, it is automatically disabled if the user chooses "Switch to Insecure Connection" during an error dialogue that pops up if the client failes to establish a secure connection with the FaceReq server.
- **Draw Overlays**: Enables the drawing of ovals, names, and other details within Genetec camera video stream. The overlays match what would be shown in the SAFR Desktop client, so SAFR settings affecting SAFR overlays also affect what is drawn in Genetec.
  **Note**: If you enable SAFR's overlays, you should disable Genetec's overlays. You can do this by

opening the Genetec Security Desk, then going to **Options->Visual**, and then disabling the **Display overlay video controls** option.

- **Report Events**: Enables reporting SAFR events to Genetec. If this setting isn't checked, *Include Event Details* is automatically greyed out.
  - **Include Event Details**: When enabled, all of the technical details of the event are attached to events. This option is especially useful if an operator uses macros to handle events for decision making.
- **Cardholders**
  - **Import Every 24 Hours**: When enabled, all the Genetec cardholders not already in SAFR's Person Directory are imported and registered to SAFR every 24 hours.
  - **Import now...**: Clicking this causes all the Genetec cardholders not already in SAFR's Person Directory to be imported and registered to SAFR.

## 76.2 Connect and Use Cameras and Video Feeds

1. To connect cameras to Genetec, you need to add the cameras to the Genetec Video Archiver using the Genetec Config Tool. For details, please see the Genetec Security Center Administrator Guide.
2. After a camera has been added to the Video Archiver, it should be displayed as a Genetec camera in SAFR. If it's not, try closing and re-opening the SAFR Desktop client.
   To get SAFR video feed overlays to be displayed on Genetec camera feeds, do the following:
   1. Open the SAFR Desktop client.
   2. Select the Genetec version of the camera from the menu in the main windows (upper left). The word "Genetec" will be the first part of the camera name.
   3. After the client has successfully connected to the Genetec camera, video from the Genetec camera is displayed in the SAFR Desktop client video feed window.
   4. Open the Genetec Security Desk.
   5. Go to the **Monitoring** Task.
   6. Drag and drop a camera from the left side into one of the tiles in the middle.
   7. The camera feed should appear and show the same video feed overlays that are in SAFR.

To connect additional cameras:

1. Open another instance of the Desktop client by selecting **File > New** on the client.
2. Repeat steps 2-6 above.
3. You can keep repeat this procedure to add overlays to as many video feeds as desired.
   **Note**: Most machines can only support up to 16 video feeds. If you want to connect more feeds than that, you'll need to install the SAFR Desktop client on additional machines.

By default, the SAFR Desktop client operates in the *Enrolled Monitoring* video processing mode and generates events and bookmarks into the Genetec system for every registered person. If you want a different mode for a given camera, choose a different mode from that camera's *Camera* window **Mode Selector** menu.

## 76.3 Genetec Cardholders and SAFR People

Genetec cardholders can be registered to SAFR by doing the following:

1. Increase the Genetec Security Center setting for thumbnail size to make sure SAFR has access to high quality images to use for face recognition.
2. On the SAFR Desktop client, click **Tools > Preferences > Genetec**.
3. In the Cardholders section click **Import Now...**. Pressing this button causes the following to occur:
   - Each imported cardholder is given a *Person Type* based on their assigned group.
   - If a cardholder has multiple group memberships, the cardholder group with the highest access privilege is used to define the group.
   - After import, SAFR updates the events in Genetec to make sure Genetec has one event for each *Person Type*.

4. You can configure SAFR to import new cardholders every 24 hours by selecting the **Import Every 24 Hours** check box.

You can also register people to SAFR by using SAFR's native functionality. For more information, see Importing and Registering People. Although people registered with SAFR are never synchronized to Genetec, you may want to register people to SAFR anyways when you want to add threats, concerns, or other registered people who may not be suitable as Genetec cardholders.

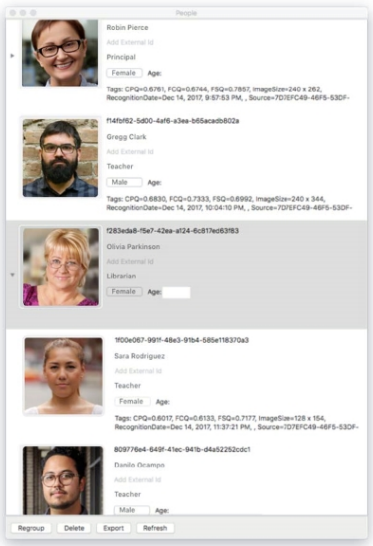
### 76.3.1 Edit Cardholder Data

You may want to edit people's properties to better manage which events get triggered when that person is recognized, For example, setting a person's *ID Class* to *Concern* or *Threat* triggers the corresponding alarms, while changing a cardholder group can allow you to trigger a VIP alert for specific cardholder groups. The most important people attributes are the *Name*, *Image*, *Person Type*, and *ID Class*.

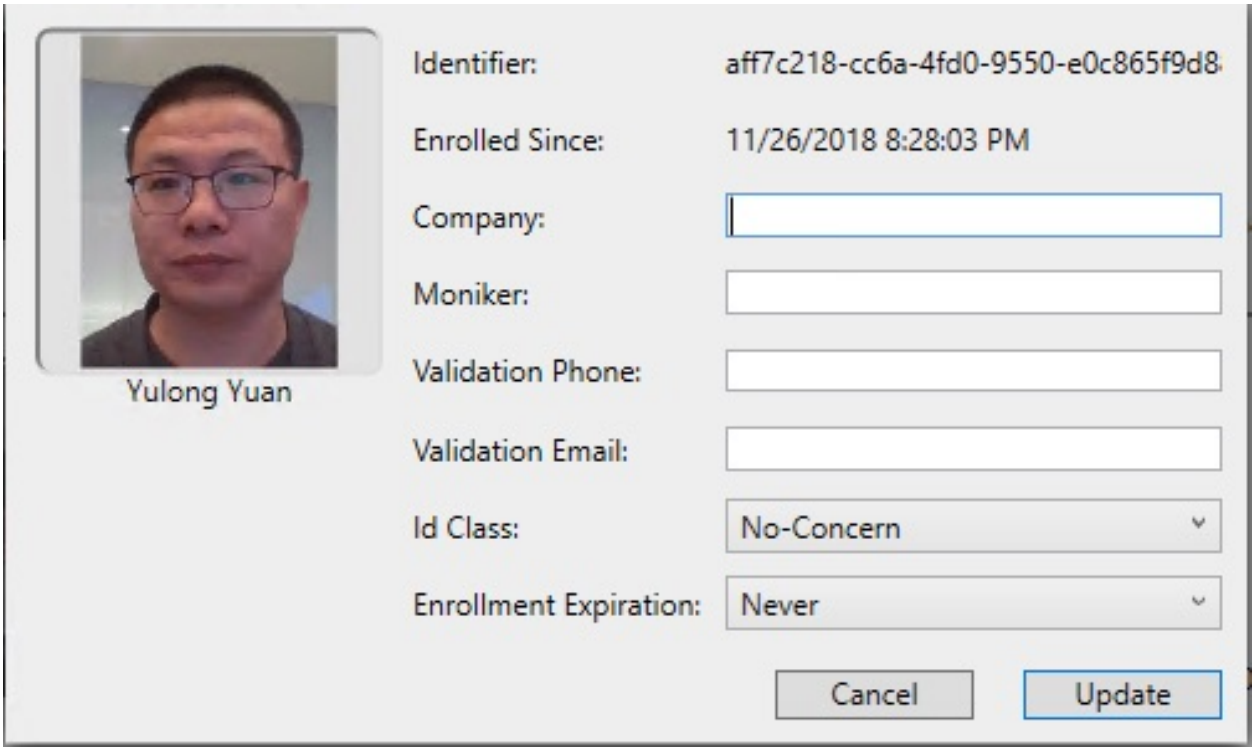
Attributes should be edited through Genetec Security Center whenever possible. *Person Type* defines a person's role (for example, staff or visitor) while the *ID Class* defines the risk level (No-Concern, Stranger, Concern, or Threat). *Person Type* and *Image* can be edited in Security Center by changing the cardholder group a person belongs to.

To edit these attributes, open Cardholder Management in Genetec Config Tool and update the desired users. After making changes, make sure to either manually synchronize users or set automatic synchronization as described previously in the "Register Cardholders".

*ID Class* and any other attributes of a person must be edited in SAFR's People dialog accessed through the Desktop client > Tools menu. All cardholders imported from Genetec Security Center are assigned an *ID Class* of *Normal*. To edit the *ID Class* of a person, click **Tools > People** in the Desktop client. The following window is displayed:




The *Person Type* and *Name* attributes can be edited by clicking their respective fields in the People window. To edit *ID Class*, in the **People Edit** dialog, double-click the user and choose the desired value from the *ID Class* menu as shown in the following image:

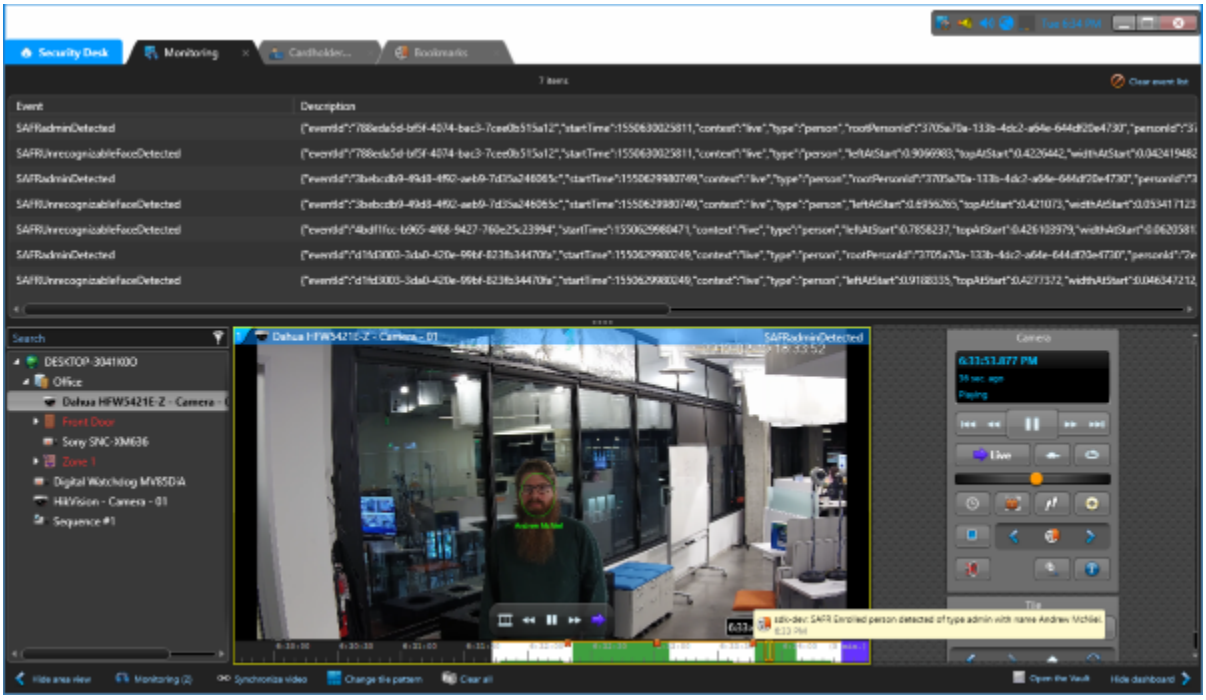



## 76.4 SAFR Events

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*.

There are several different combinations of the conditions that are triggered. The following image shows multiple events populated in the Genetec alerts panel. Clicking any of the events allows the video from that event to be replayed:



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

| Event Message | Id Class | Named | Person Type | Condition | People Attributes |
|---|---|---|---|---|---|
| Unrecognizable face 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" |
| Registered person detected without name | Normal | No | None | Registered person without name or person type assigned | idClass="noconcern" && personType="" && name="" |
| Registered person detected with name <name> | Normal | Yes | None | Registered person with name but no person type | idClass="noconcern" && personType="" && name=<name> |
| Registered person detected of type <personType> | Normal | No | Defined | Registered person with person type but no name | idClass="noconcern" && personType=<personType> && name="" |

| Event Message | Id Class | Named | Person Type | Condition | People Attributes |
|---|---|---|---|---|---|
| Registered person detected of type <personType> with name <name> | Normal | Yes | Defined | Registered person with person type and name | idClass="noconcern" && personType=<personType> && name=<name> |
| Concern person detected without a name | Concern | No | None | Same as above for Concern | idClass="concern" && personType="" && name="" |
| Concern person detected with name <name> | Concern | Yes | None | Same as above for Concern | idClass="concern" && personType="" && name=<name> |
| Concern person detected detected of type <personType> | Concern | No | Defined | Same as above for Concern | idClass="concern" && personType="" && name="" |
| Concern person detected of type <personType> with name <name> | Concern | Yes | Defined | Same as above for Concern | Registered person marked as concern detected with name assigned. |
| Threat person detected without a name | Threat | No | None | Same as above for Threat | idClass="threat" && personType="" && name="" |
| Threat person detected with name <name> | Threat | Yes | None | Same as above for Threat | idClass="threat" && personType="" && name=<name> |
| Threat person detected of type <personType> | Threat | No | Defined | Same as above for Threat | idClass="threat" && personType=<personType> && name="" |
| Threat person detected of type <personType> with name <name> | Threat | Yes | Defined | Same as above for Threat | idClass="threat" && personType=<personType> && name=<name> |

### 76.4.1 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 Genetec Security Center integration. For a complete description, see Connect to a Video Feed in the *SAFR Documentation*.

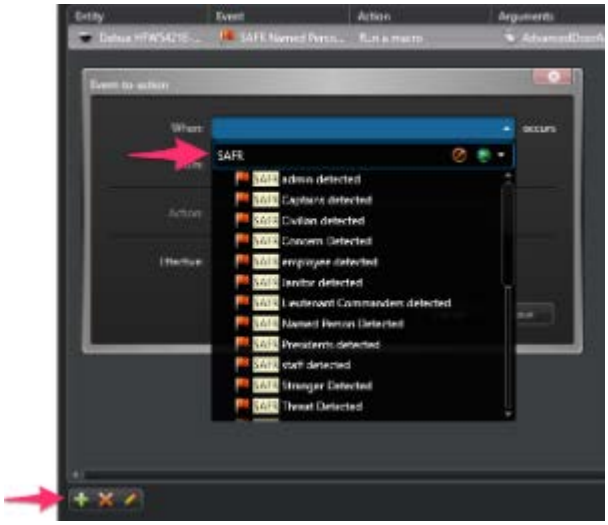
- **Secure Access**: Only triggers events when cardholders and people registered in SAFR's Person Directory are identified with a high degree of certainty. This mode is useful when the system is being used to manage physical access. (i.e. When the system is responsible for unlocking doors for authenticated 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.

### 76.4.2 Add and Configure Alerts

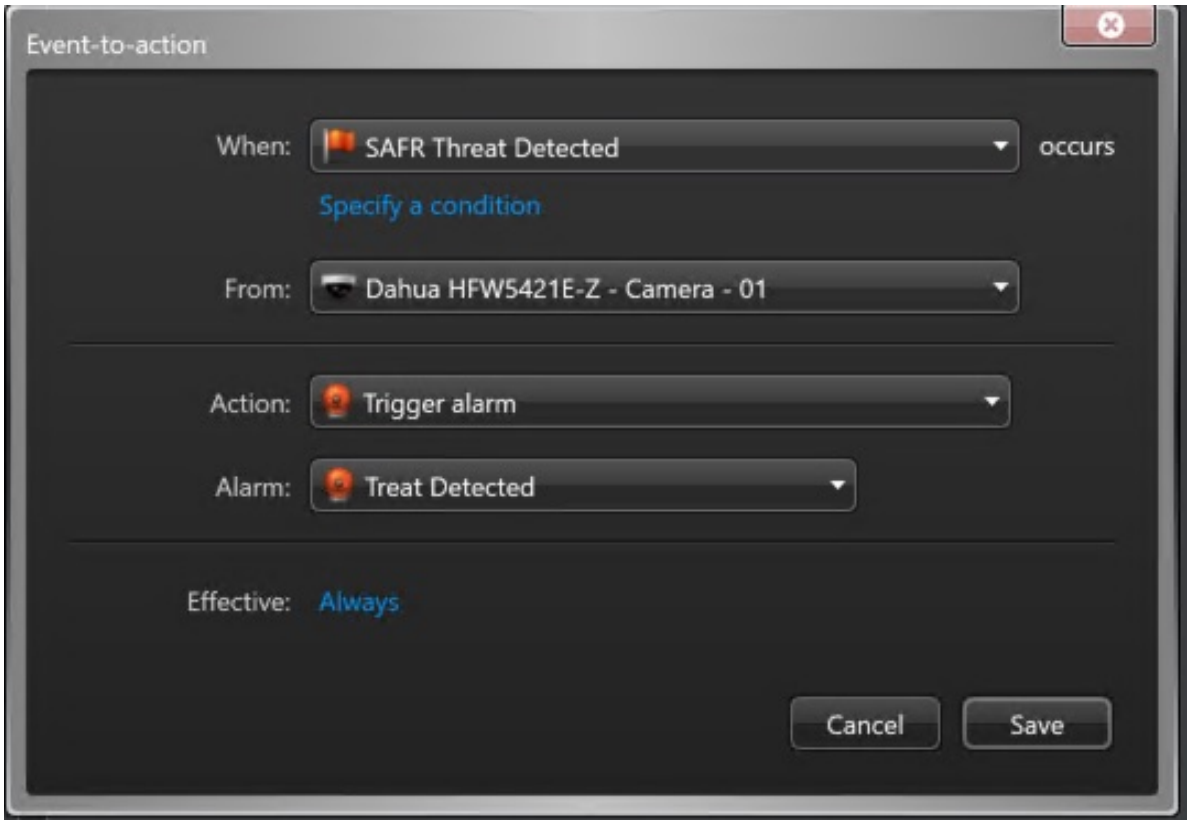
To trigger the alert as a result of a SAFR-generated event, do the following:

1. Open the Genetec Config Tool, and go to the System Panel.


2. Click the + icon to add a new alarm, and click the When menu. Type *SAFR* and press **Enter** to see the list of SAFR-enabled alarms.



3. Choose the desired entry from the list.
4. Under **From**, choose the camera you want to use to trigger the event. Under **Action**, choose a desired action. (e.g. Trigger Alarm)




5. Click **Save** when done.

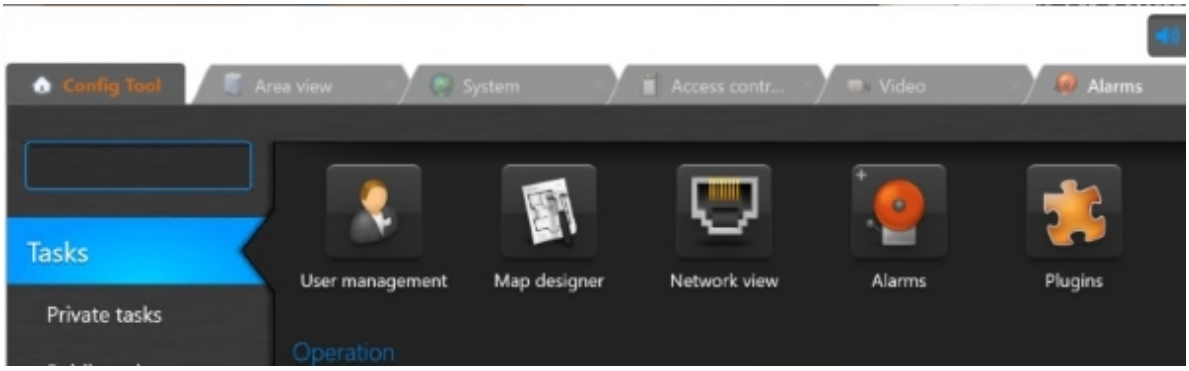
SAFR Events can be tied to Actions which can then trigger an Alarm. Initially create an alarm you want to trigger, and then use Genetec Event-to-Action dialog to tie SAFR Events to any action that can be defined in the Genetec system (for example, Trigger Alarm).

### 76.4.3 Add an Alarm

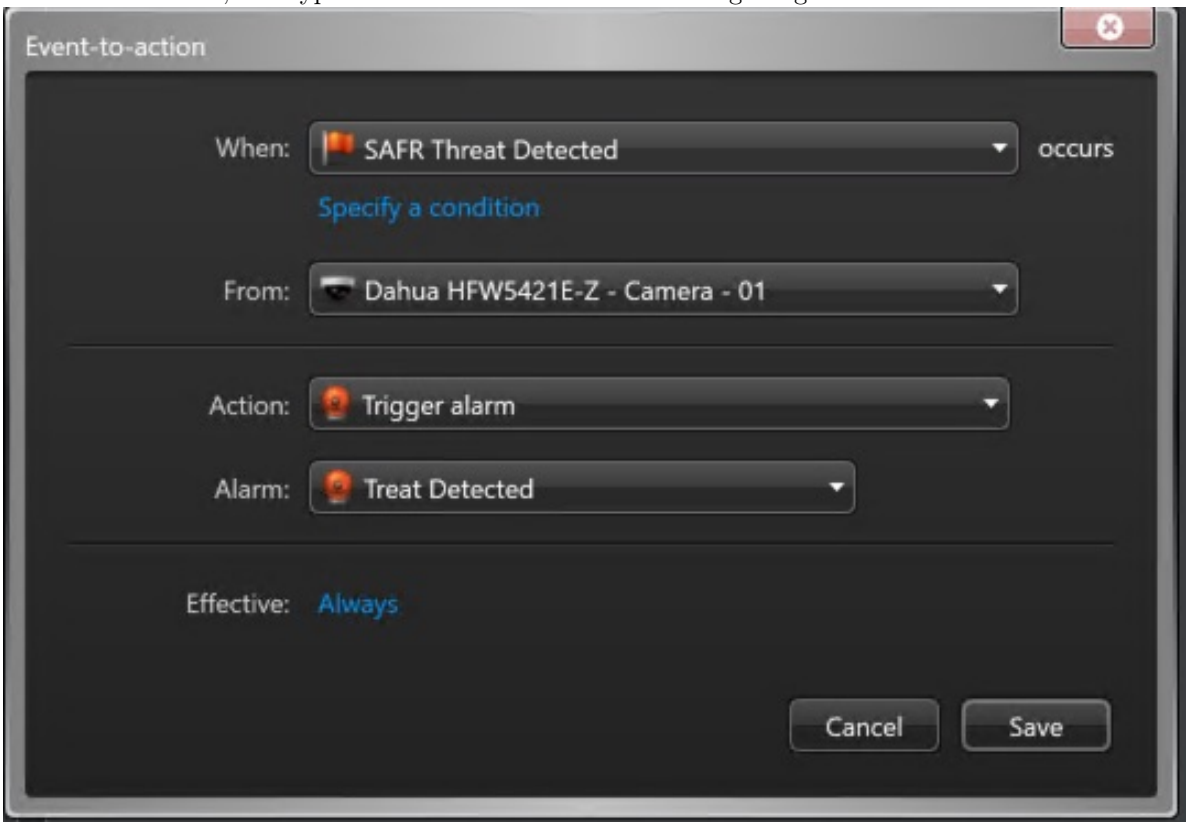
An alarm can be used to make sure an important event is noticed. In this example, we show how to create an alarm that is triggered when someone who has been marked as a threat is recognized on one of the cameras. For more information on triggering events, refer to Genetec support documentation.

To create an alarm, do the following:

1. Open the Genetec Config Tool, and open the Alarms screen.




2. Click **Add Alarm**, and type a *Name* as shown in the following image:




3. Click **Save** to save the alarm.

### 76.4.4 Recommended Settings for Alarms

| | |
|---|---|
| Properties task | Choose priorities based on circumstances and your organization guidelines (1=high, 255=low)<br>• Stranger: 100 (If infrequent, set high)<br>• Concern: 50<br>• Threat: 10<br>Video display option<br>Set to Live to see the live view when alarm loads video<br>Playback may be useful for short events where the subject may have walked off the screen by the time the video loads<br>• If playback mode, set to at least 4 seconds to avoid buffering |
| Advanced task | Auto-Acknowledge: Good for stranger events; enter the number of seconds to stay in the view before returning to the view you were on prior to the event<br>Choose color to match the SAFR colors (add ref to section in manual that describes colors)<br>Reactivate threshold: Suppresses additional alarm if another similar alarm triggered within this time<br>• Adjust as needed for use case. |

### 76.4.5 Trigger Macros

When SAFR is configured to *Include Event Details* in reported events, highly customized actions can be programmed using macros in the Genetec system. Event details include all information associated with the detected face (e.g. *Name*, *Person Type*, *Age*, *Gender*, *Sentiment*, etc.). For more information on macros, refer to the Genetec support documentation.

## 76.5 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 is poor (not many faces found or recognized), make sure the Genetec video feeds are set for a sufficiently large frame size.
- If events are not being triggered, check the following:
  - Permissions are set correctly on Event-to-Actions.
  - Make sure the applicable SAFR Video Processing Mode is selected.

# 77 SAFR-Milestone Integration Guide

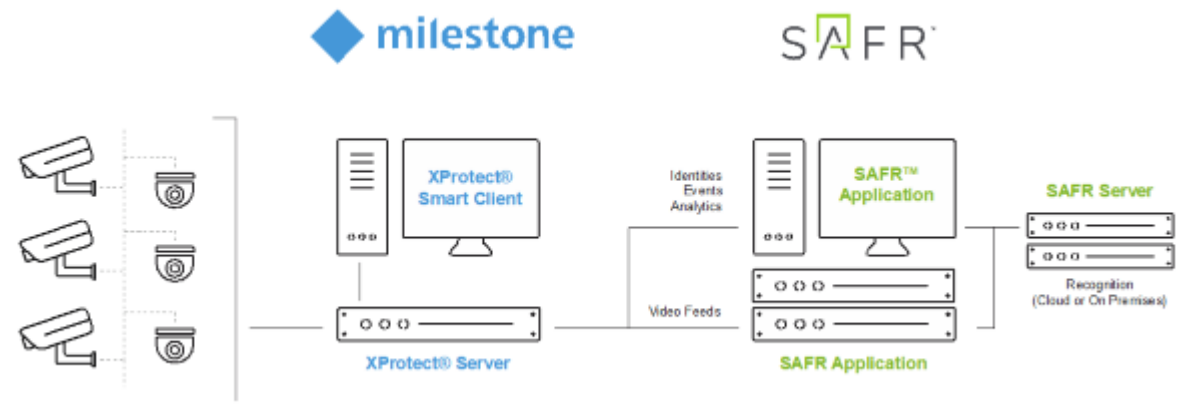
Integrating SAFR's facial recognition and analysis capabilities into Milestone enables you to use SAFR's video feed information overlays within Milestone camera video feeds, thus making it much easier to quickly and accurately separate unknown people from authorized people from known threats. You'll also have immediate access to additional infomation 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 Milestone alerts and other actions within the Milestone system. Milestone's metadata within bookmarks are enriched with SAFR's additional information, allowing you to more easily find relevant bookmarks.

## 77.1 Integration Overview and Requirements

A typical deployment requires the following:

- A machine running Milestone XProtect. (Bookmarks are only supported on XProtect Expert and Corporate.)
- Machines running Milestone XProtect Smart Client and Milestone Admin Tool for monitoring and administration of Milestone.
- 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 Milestone XProtect. SAFR can then connect to Milestone XProtect to perform analysis of the video and add overlays. Depending on the number of cameras you need, one or more machines can run the SAFR Desktop client, with each client processing multiple video feeds. SAFR processes the video and returns information to Milestone to overlay the video feeds and generate events. The SAFR Desktop client is also used to perform various management activities.

### 77.1.1 System Requirements

Milestone has the following requirements:

- Milestone XProtect 2019 R1 or later must be installed.
- Each camera connected to Milestone requires a Milestone license.
- For each camera connected to Milestone on which you want to run SAFR overlays, you'll need a second Milestone license. Thus, each Milestone camera running SAFR overlays requires 2 Milestone licenses total.

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 1.4.142 or later.
  - The system requirements described here.
- Local SAFR deployments require at least one machine running SAFR Platform 1.4.140 or later.
- Each machine running SAFR Platform must meet the system requirements described here.

## 77.2 Install and Configure Milestone XProtect

Download and install the latest Milestone installer package from the Milestone Download Portal.

To create a SAFR user in Milestone and set its permissions, do the following:

1. Add a SAFR user (e.g. `safr-roles`) in the Milestone XProtect Management Client by going to the Site Navigation pane and selecting **Security > Roles**.
2. Highlight **Administrator** in the **Roles** pane.
3. At the bottom of the GUI click **Users and Gr** and then **Add**. (Select **Basic** to add the `safr-roles`.)
4. After `safr-roles` is created, add the required SAFR camera permissions to the role in the Milestone XProtect Management Client by going to the Site Navigation pane and selecting **Security > Roles**.
5. Select **Operators** in the **Roles** pane at the bottom of the GUI **Overall Security**.
6. From **Role Settings > Camera**, check-off **Allow** for the following check boxes:
   - Read
   - View Live
   - Create bookmarks (only available on XProtect Expert and Corporate)
   - Read bookmarks (only available on XProtect Expert and Corporate)
   - Edit bookmarks (only available on XProtect Expert and Corporate)
7. Click **Save** to save the changes.

### 77.2.1 Update Milestone XProtect Operator Permissions

To enable the Milestone operators to view SAFR created overlays, update the *Operator* role (or the role you are using to log into the Milestone XProtect Smart Client) to allow display of live metadata.

- Set *Operator* role permissions in the Milestone XProtect Management Client > Site Navigation pane > Security > Roles. Click Operator > Overall Security. From Role Settings > Metadata, edit by selecting **Allow** for the *Live* check box.
- **Save** the changes.

**Note**: Overlays are not visible if the live permission is not added to the Operator role.

## 77.3 Install and Configure SAFR

1. From the SAFR Download Portal, download and install either SAFR Platform or SAFR Edge, depending on your deployment type. Make sure to select the Milestone VMS extension install option.
2. Start the Desktop client and go to **Tools > Preferences**.
3. Click the **Milestone** tab.
   **Note**: If the **Milestone** Preferences tab is not displayed, it's possible that you didn't select the Milestone VMS Extension when you installed SAFR.
4. To connect to the Milestone XProtect server and enable access to the cameras connected to Milestone server enter the following.
   - **Username**: SAFR user created when you installed and configured Milestone above. (e.g. `safr-roles`)
   - **Password**: Password created for the SAFR user.
   - If you created the user (in this example `safr-roles`) as a Windows user versus basic user, check the "Windows credentials" box.

- **Directory**: IP address or domain address of server running Milestone XProtect. If all in one server for a small deployment or PoC, "localhost" should work.

See the Operation Guide for a complete description of the settings on the Milestone Preferences tab.

### 77.3.1 Customizing Ports for SAFR Server Services

For smaller deployments in which you want to run both SAFR and Milestone XProtect on the same machine, you must customize the port assignments in SAFR to ensure SAFR and Milestone XProtect do not conflict.

SAFR uses the following ports by default:

- **COVI**: 8080
- **Event**: 8082
- **VIRGA**: 8084
- **CVOS**: 8086

To customize ports, do the following:

1. Stop or disable any conflicting software using the required ports.
2. Install the SAFR Platform.
3. Open *Notepad* as Administrator and open `C:\Program Files\RealNetworks\SAFR\safrports.conf`.
4. Edit any conflicting ports to new values. (e.g. CoviHTTP=18080)
5. Run `C:\Program Files\RealNetworks\SAFR\bin\configure-ports.bat`. Running this batch script stops, reconfigures, and re-starts SAFR services.
6. Run `C:\Program Files\RealNetworks\SAFR\bin\check.bat`. `check.bat` displays the new port settings.

## 77.4 Verify your Connection

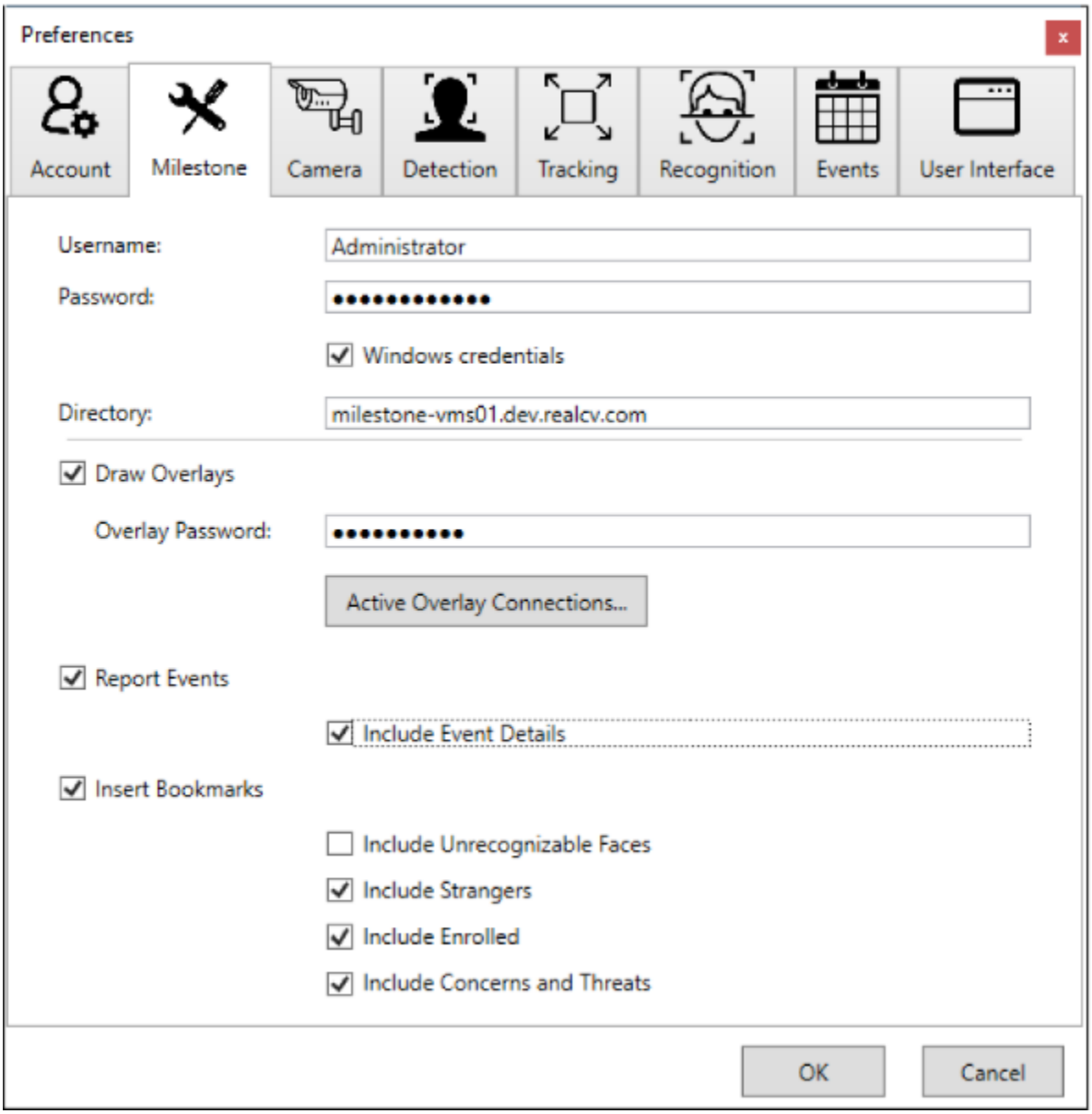
To verify successful connection to the Milestone system, open the **Preferences > Camera** tab. Cameras connected to the Milestone system should be visible. All cameras connected to the Milestone system have a Milestone prefix in their names.

# 78 SAFR-Milestone Operation Guide

Integrating SAFR's facial recognition and analysis capabilities into Milestone enables you to use SAFR's video feed information overlays within Milestone 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 infomation 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 Milestone alerts and other actions within the Milestone system. Milestone's metadata within bookmarks are enriched with SAFR's additional information, allowing you to more easily find relevant bookmarks.

## 78.1 SAFR Milestone Preferences




- **Username**: Name of the user with the necessary permissions to connect SAFR to Milestone.
- **Password**: Password of the user with the necessary permissions to connect SAFR to Milestone.
- **Windows credentials**: Indicates whether the user is a Windows user or a basic user.

- **Directory**: IP address or hostname of a Milestone server.
- **Draw Overlays**: Enables the use of SAFR overlays on Milestone cameras.
  - **Overlay Password**: This is the password that should be configured/used in Milestone to access SAFR to receive overlay data. See the Interpret Video Feed Overlays page for information about SAFR overlays. After you add the *overlay password*, SAFR needs to be restarted.
  - **Active Overlay Connections**: TBD
- **Report Events**: Enable to allow the reporting of SAFR events to Milestone. Note that only events reported to the SAFR Events server are reported to Milestone.
  - **Include Event Details**: Increases the verbosity of events in attaching JSON to the event that includes all of the technical details of the event. This is useful if an operator is using macros to handle the event for decision-making.
- **Insert Bookmarks**: Adds bookmarks to the video stream related to events. Allows operators to search video for events or recognized person names. Use caution when deciding what to include since many faces can cause many bookmarks to be created.
  - **Include Unrecognizable Faces**: When enabled, adds bookmarks when a face is detected but SAFR does not have enough information to determine if they are a stranger or a known person. This can result in an overwhelming number of bookmarks, so it's disabled by default. However, this setting can be useful when monitoring areas with very few people.
  - **Include Strangers**: When enabled, adds bookmarks when a face is recognized and determined to be a stranger. This option is generally useful for secured areas where only known people should be.
  - **Include Enrolled**: When enabled, adds bookmarks when a face is recognized and determined to be a known person.
  - **Include Concerns and Threats**: When enabled, adds bookmarks when a face is recognized and determined to be a known concern or threat.

## 78.2 Connect Cameras to Milestone

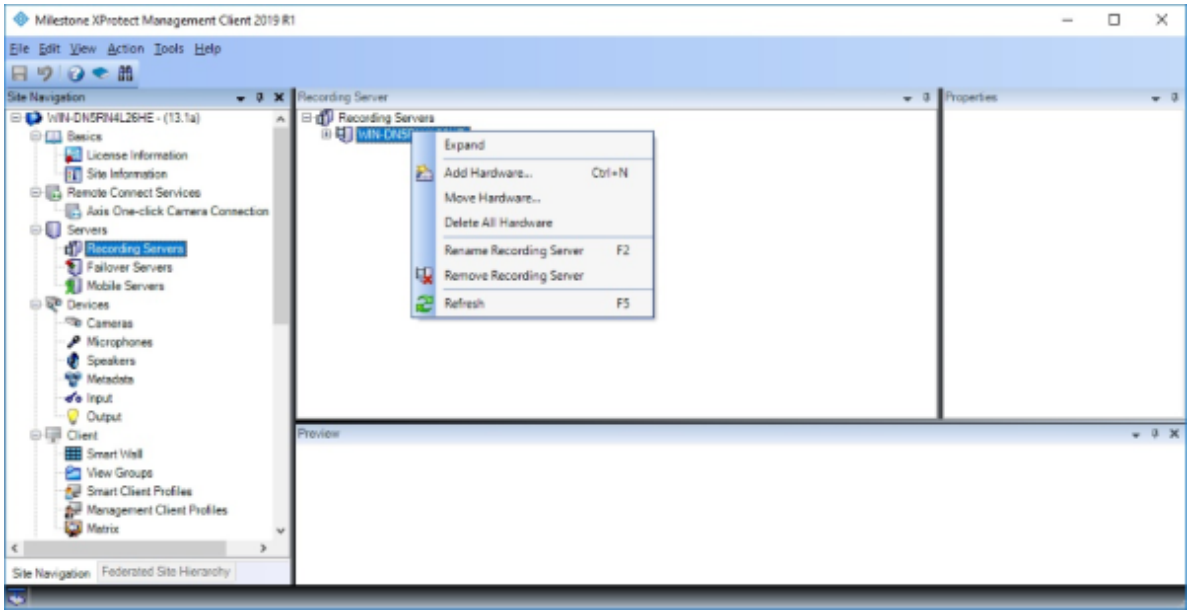
It is very likely that cameras are already connected to the Milestone server but if additional cameras are to be added use the Milestone Management client. The best information on how to do this is in the *Milestone XProtect Administration Guide*. However, what follows is a brief explanation of the procedure:

1. Open the Administration client.
2. Go to Recording Servers.
3. Right-click the Recording Server to which you want to add a camera.
4. Select **Add Hardware**.
5. Select a method to auto-discover the camera. For this example, use auto-discover.
   - Enter the username and password for the camera.
6. Check the box next to each manufacturer of the cameras you want to add. Click **Next**.
7. Add any username and password combination used to connect to the camera.
8. Cameras appear in the list as they are discovered. Check the box next to each camera you want to add.
9. The hardware for each camera is listed. Check the box for each part to be added. Types of parts are camera feeds, microphones, speakers, and others.
10. Hardware parts need to be added to groups. At the left, select the default group for each type of hardware. At the right, you can override the group for individual hardware parts.
11. Click **Finish** to add the selected hardware.

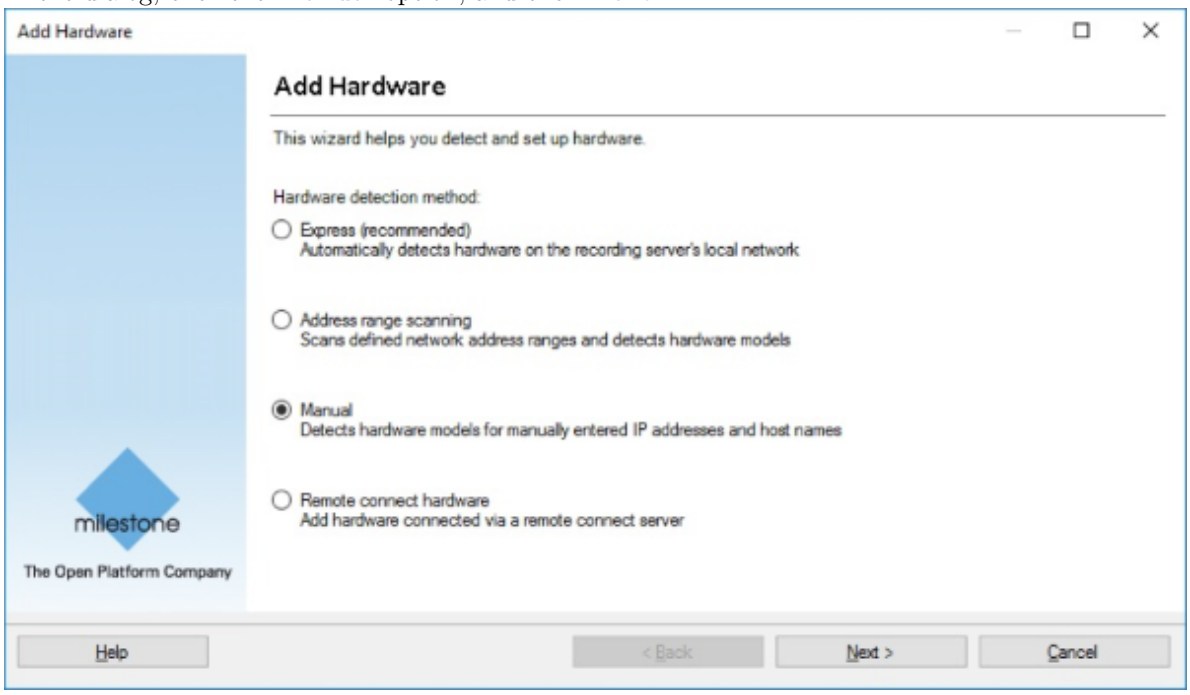
**Note**: The *XProtect Smart Client* has to be restarted to pick up newly added cameras.

## 78.3 Create Overlay Metadata Driver on Milestone Server for each Camera.

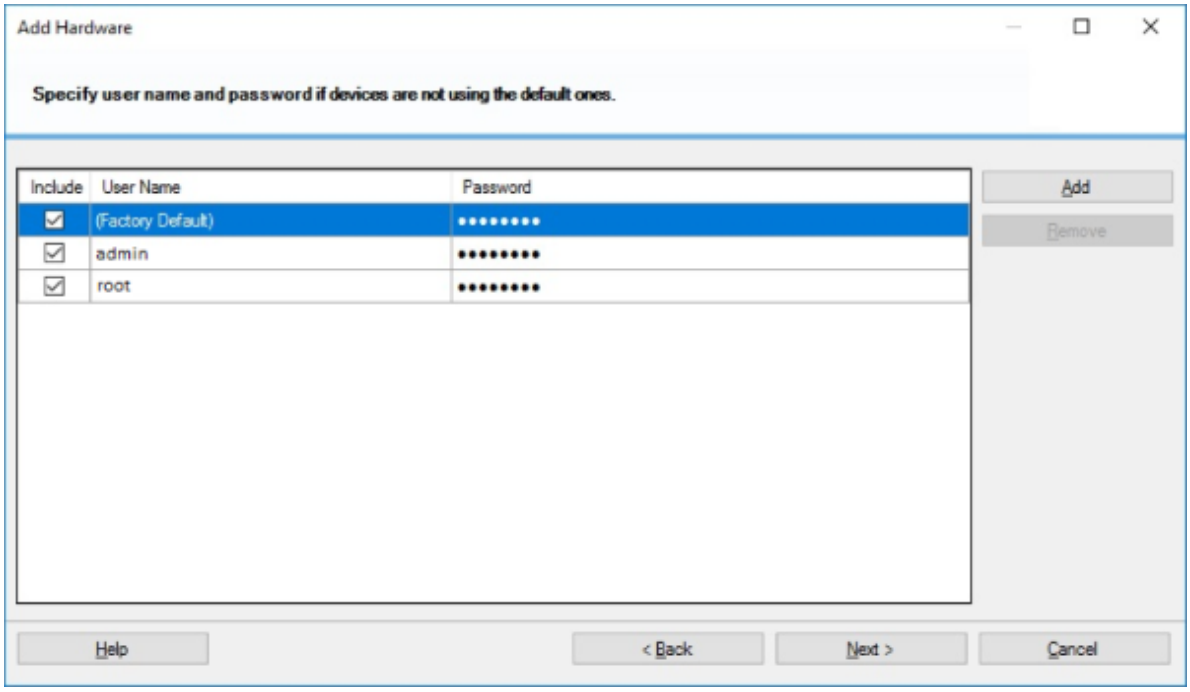
1. Open the Milestone XProtect Management Client. In the left pane, under Servers, click **Recording Servers**.
2. In the center pane, right-click the appropriate server name, and click **Add Hardware**.



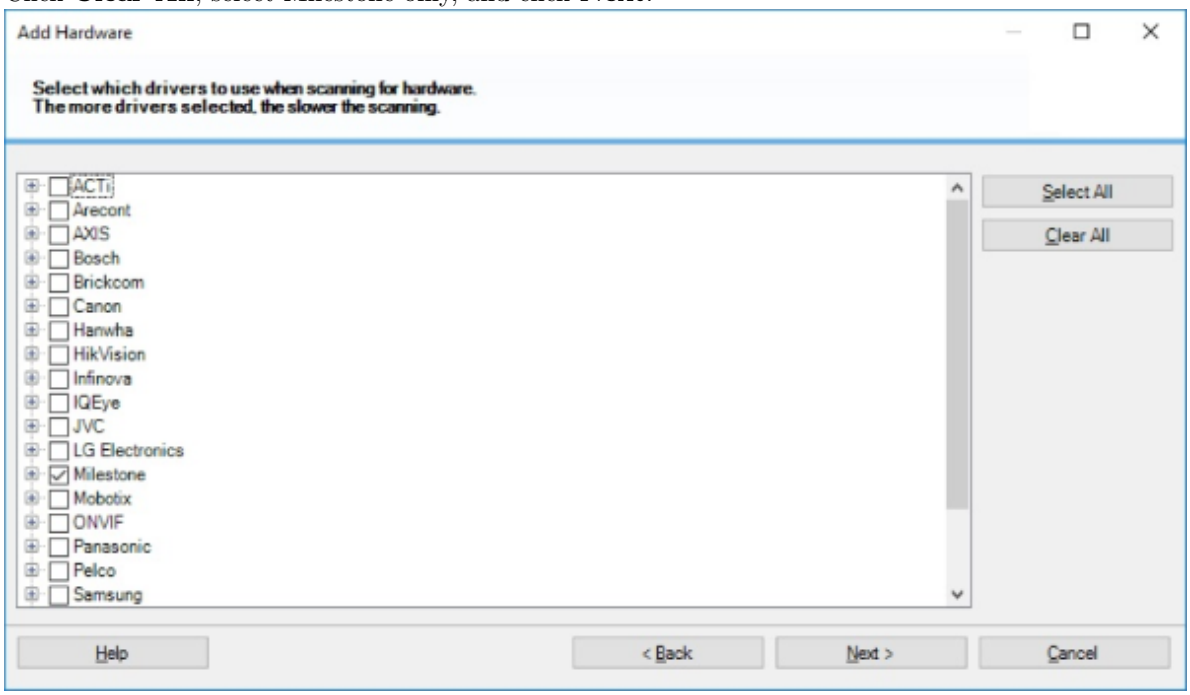

3. In the dialog, click the **Manual** option, and click **Next**.



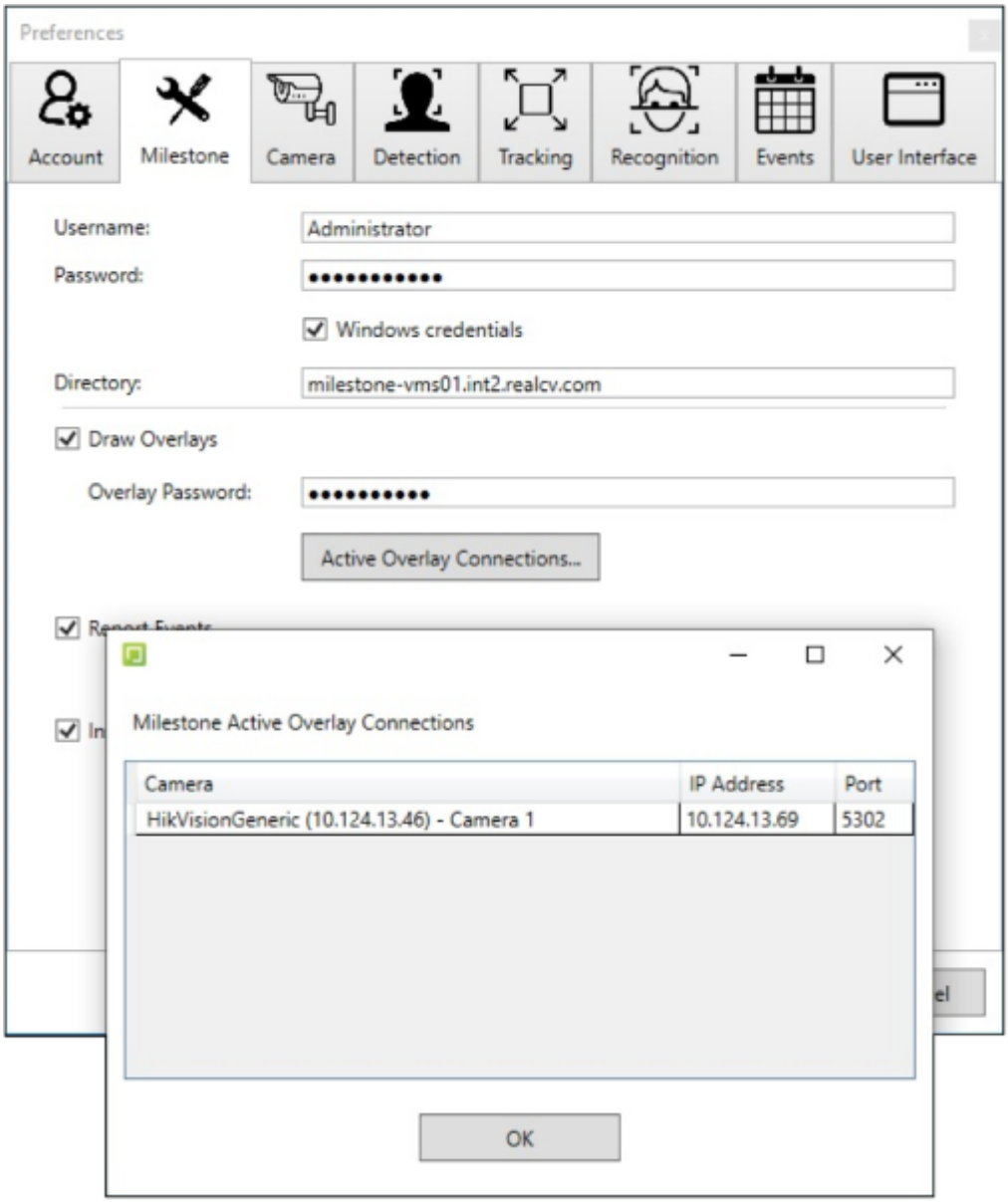

4. If not already in the list, click **Add** to include the password from the SAFR > Preferences > Milestone tab **Overlay Password** field. Include a username of your choice. (e.g. *SAFR*)
   - If you make changes to the overlay password on the **SAFR > Milestone** tab, make sure that you click **OK** at the bottom of the window. Then make sure the password on the Add Hardware username/password page includes the changed password. If not, the add hardware operation will fail.
5. After you have edited the username and password table, click **Next**.



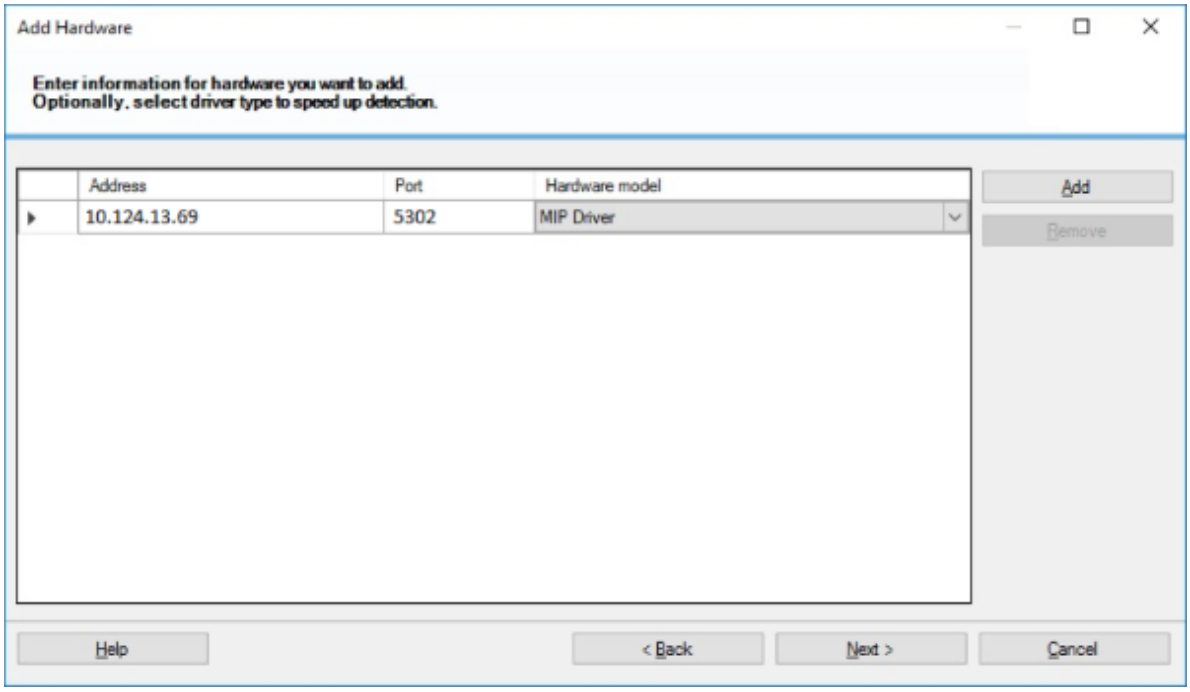

6. Click **Clear All**, select Milestone only, and click **Next**.



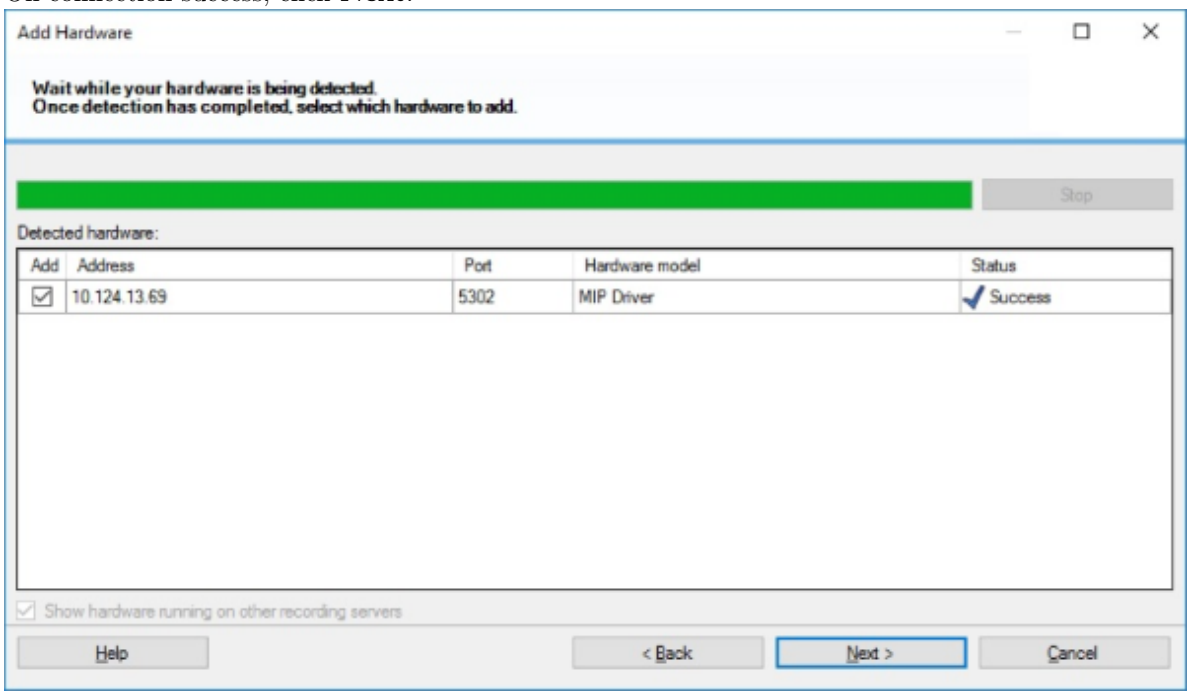

7. Add the IP address and port number of the SAFR client active overlay connections. To find this information, go to SAFR > Properties > Milestone tab, and click **Active Overlay Connections**. The dialog provides a table of camera names, IP addresses, and port numbers. Please note the IP address of the SAFR Desktop client and not the IP address of the camera itself.
   - The password in the *Overlay Password* field must be included in the Add Hardware username/-password table or the add hardware operation will fail.



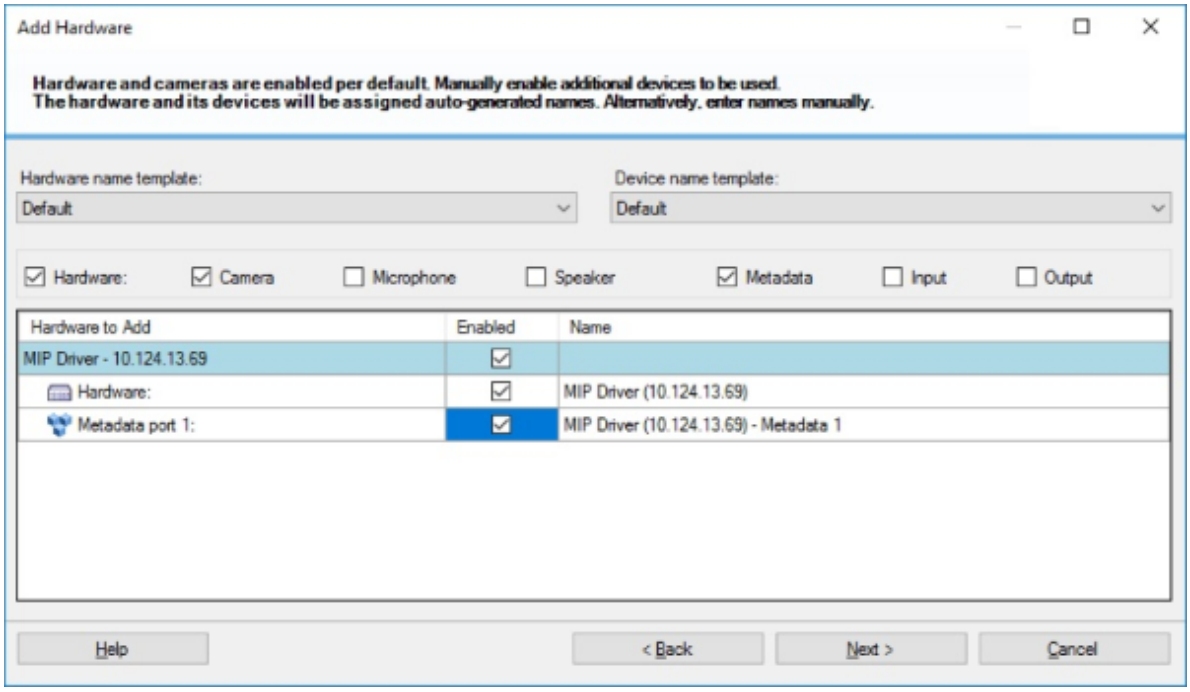

8. From the **Hardware Model** menu, select **MIP Driver**. Click **Add** to create more rows for additional MIP driver addresses and ports if needed. Click **Next**.



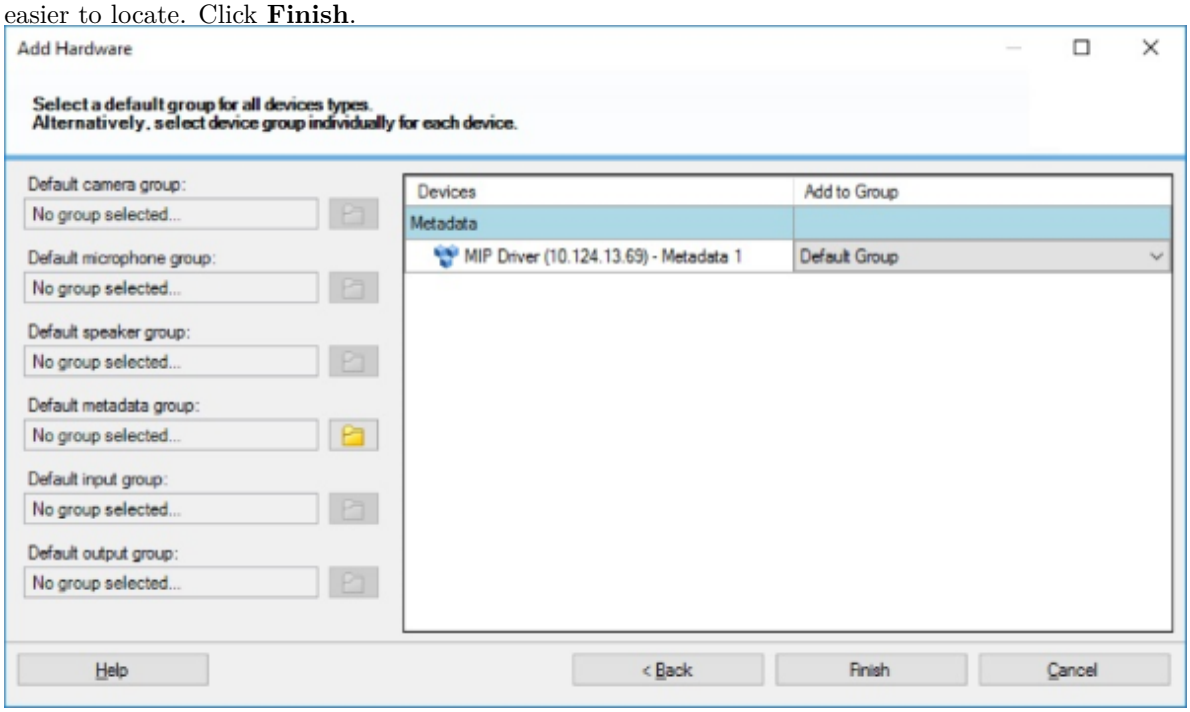

9. On connection success, click **Next**.



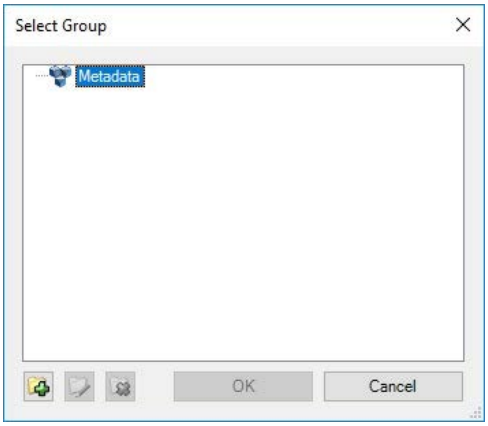

10. Select the **Metadata** check box. We recommended that you click the **Name** field for the MIP driver (Metadata Port 1) and rename it to include the name of the camera to assist you when associating the camera with the MIP driver later. Click **Next** to add the hardware.




11. From the **Add to Group** menu, associate the MIP driver with a specific metadata group to make it easier to locate. Click **Finish**.




12. If the menu does not include a choice, or if you receive an *Assign Device to a Device Group* message, do the following:
    1. In the list in the left pane, to the right of the Default Metadata Group field, click the folder icon.
    2. In the Select Group dialog, in the lower-left corner, click the folder-plus icon to add a group.



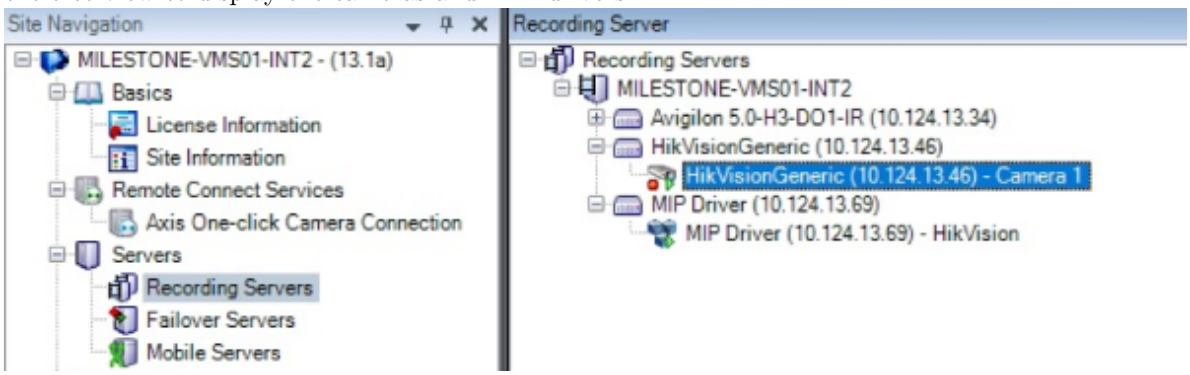

3. Provide a name for the device group, and click **OK**.


4. From the **Add to Group** menu, you can now select the new device group.

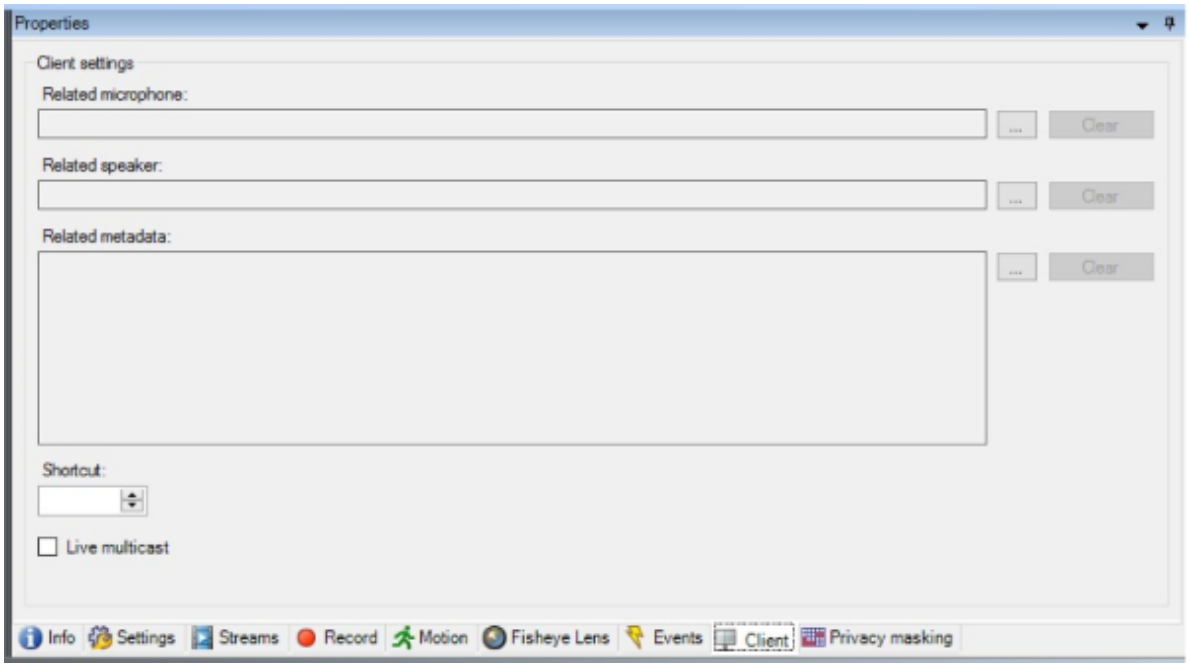
13. After the driver has an associated device group, click **Finish**.

## 78.4 Associate the Milestone Integration Platform (MIP) Device with the Camera.

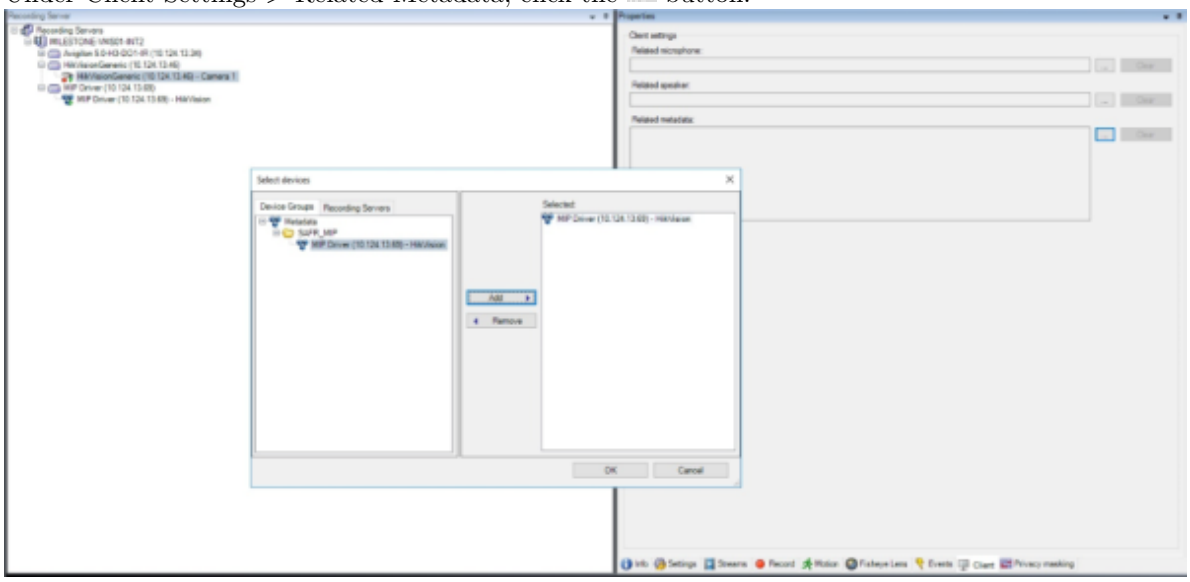
1. In the Milestone XProtect Management Client, in the left pane, click **Recording Servers** and expand the tree view to display the cameras and MIP drivers.



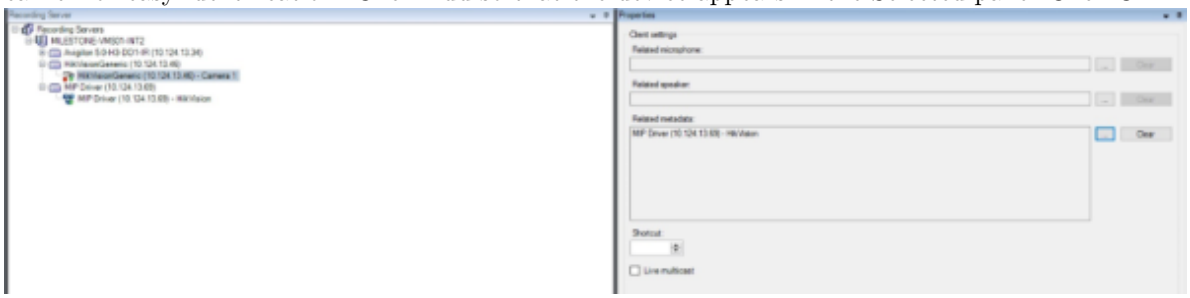

2. With the camera highlighted, in the right-pane, at the bottom of the window, click **Client**.




3. Under Client Settings > Related Metadata, click the ... button.



4. In the Select Devices dialog, on the Device Groups tab, click to highlight the MIP device you renamed earlier for easy identification. Click Add so that the device appears in the Selected pane. Click OK.



5. Click **Save** to save the changes.

In the right Related Metadata field, the MIP device name is displayed and is now associated with the

highlighted camera in the left pane.

## 78.5 Connect SAFR to Milestone Video Feeds

Once the camera is in the Video Archiver, it shows up as a Milestone camera in SAFR. If it does not, try closing and re-opening SAFR.

To get the SAFR enhancement to show up on the Milestone camera feed:

1. Open the SAFR Desktop client.
2. Select the Milestone version of the camera (It has Milestone as the first part of the camera name.) from the menu in the main windows (upper left).

On successful connection to the Milestone camera, video from the camera plays in the SAFR Desktop client window.

If overlays have been configured, you can see the enhancements by watching the camera's video feed in XProtect:

1. Open XProtect.
2. Go to the Live tab.
3. Drag and drop a camera from the left side into one of the tiles in the middle.

The camera feed should start up and show the same overlays that are in SAFR (for example, ovals, names).

To connect to additional cameras:

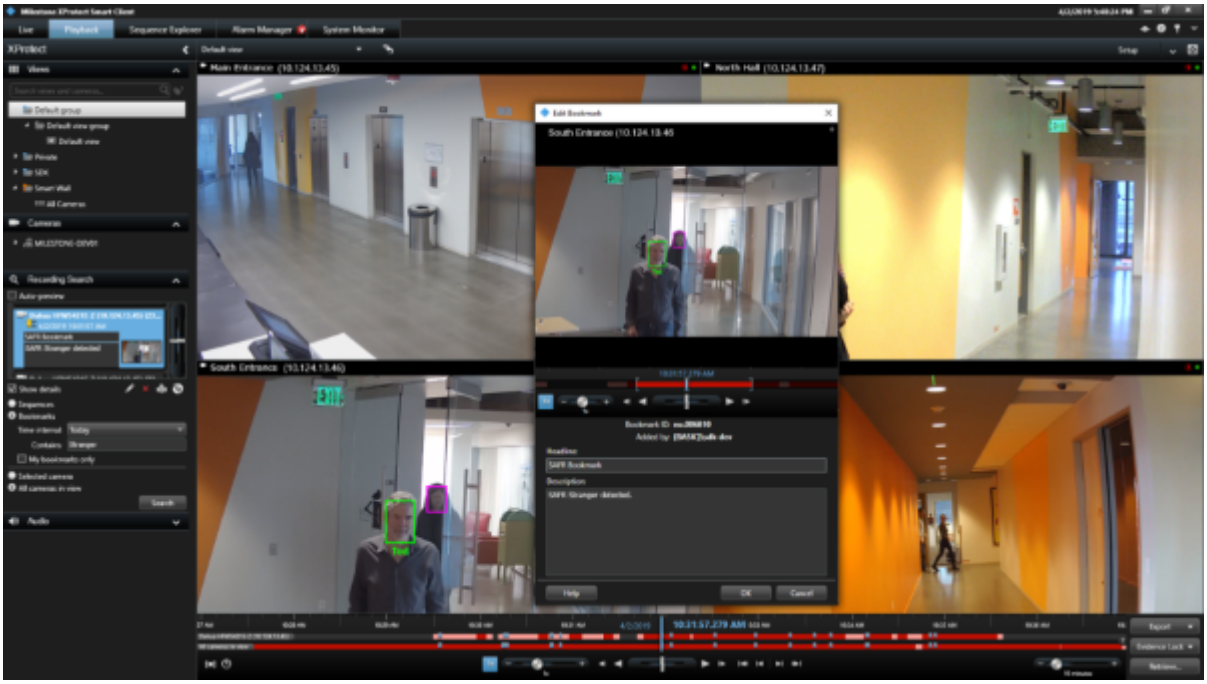
1. Open another instance of the SAFR Desktop client by selecting **New** from the **File** menu.
2. Repeat the previous steps to connect to a different Milestone camera feed.
   On successful connection to the Milestone camera, video from the camera plays in the SAFR Desktop client window.
3. Repeat this process for as many video feeds as desired (up to the capacity of the machine SAFR is installed on).
4. If more capacity is needed, install SAFR on additional machines and repeat the setup process.

**Note**: By default, the SAFR Desktop client for Milestone operates in *Enrolled Monitoring* video processing mode and generates events and bookmarks into the Milestone system for every enrolled person. If a different mode is desired for a selected camera, choose a different mode from the video window mode selector menu.

## 78.6 Automatic Bookmarks

Milestone 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.



**Note**: The purple indicator identifies the person is a stranger.

## 78.7 SAFR Identities

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

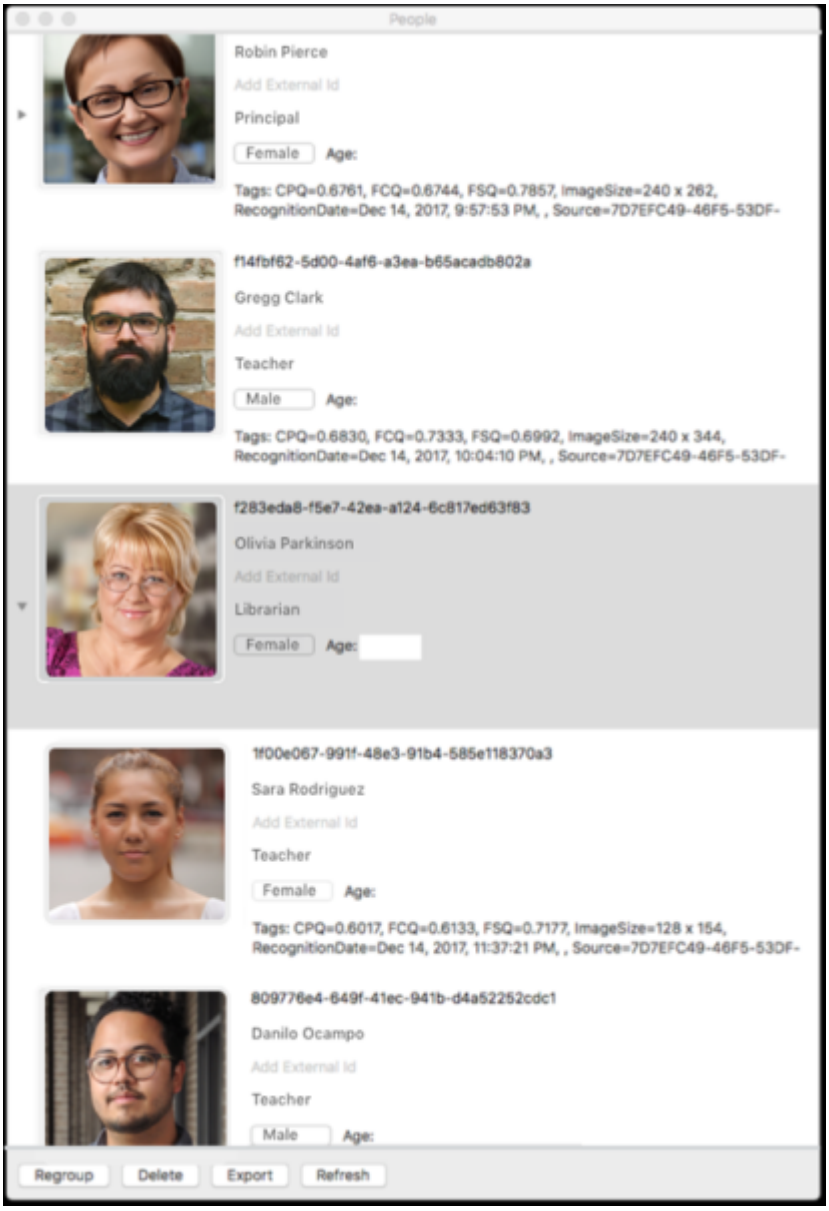
1. Open the Desktop client.
2. Click **File > Import Faces**.
3. Select the image.
   - For an image, each recognized face is enclosed by a box, and you have the option to type a name.
   - For a video, each recognized person is learned automatically as long as the faces meet the minimum criteria for 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

Users added to SAFR are not synchronized to Milestone. These users exist only in SAFR.

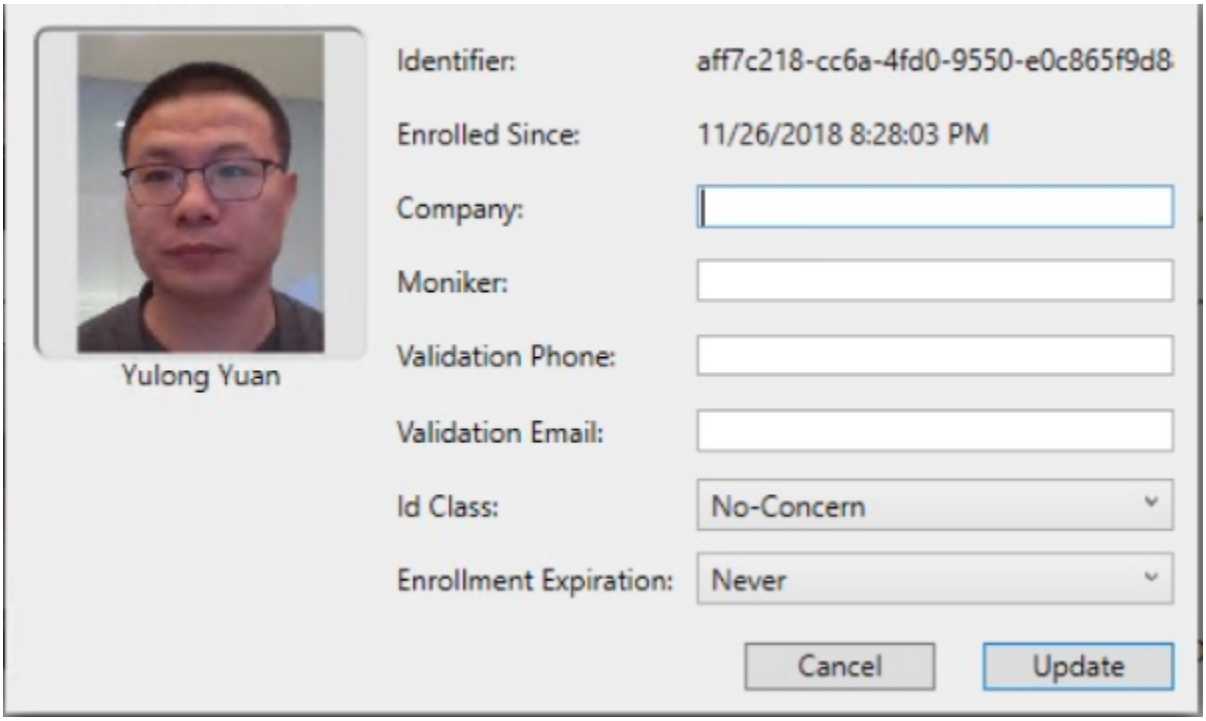
It may be desirable to edit people properties to control which events get triggered when that person is recognized. For example, setting a person's *ID Class* to *Concern* or *Threat* triggers the respective alarms. The most important people attributes are *Name*, *Image*, *Person Type*, and *ID Class*.

The *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:



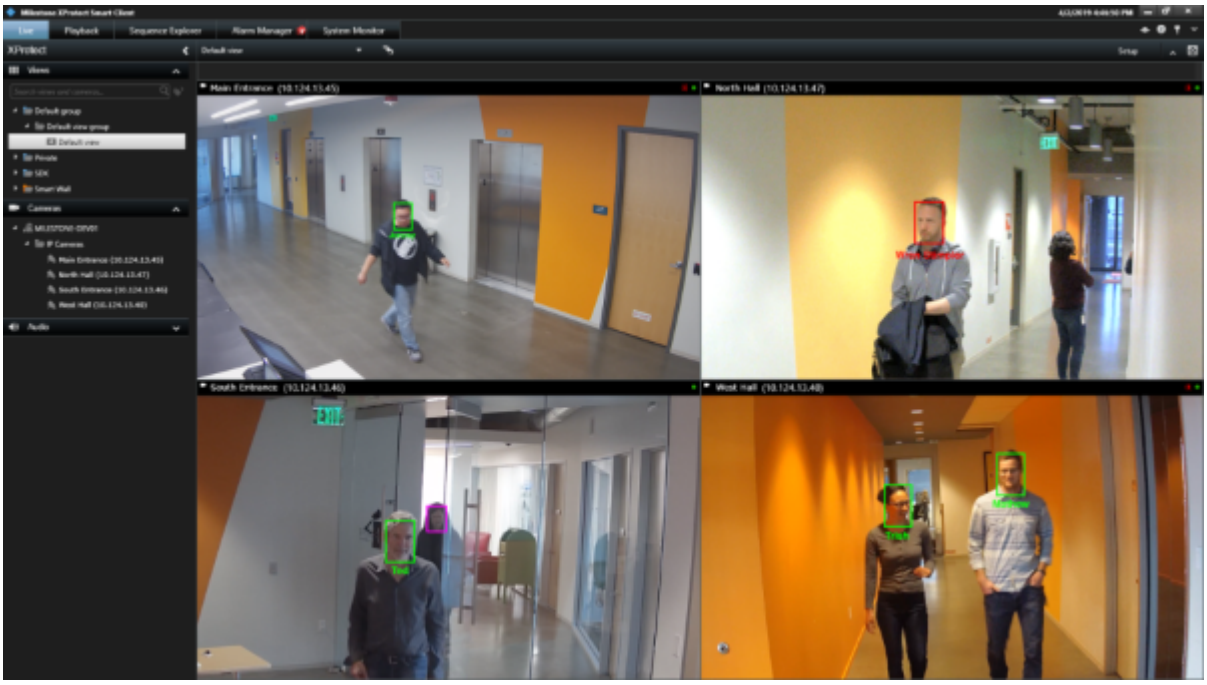

The *Person Type* and *Name* can be edited by clicking the respective fields on the People screen. To edit *ID Class*, double-click the person and choose the desired value from the ID Class menu in the People Edit dialog as shown in the following illustration:




## 78.8 SAFR Overlays

SAFR for Milestone enhances video monitoring by providing overlays that gives the security personnel more information, including person types, threat classification, and name. It can even be used to augment the video views with age and gender information that may be useful in reporting suspects.

The following illustration shows how overlays give more information about the subjects in view:



The person in the top left is a stranger, the person in the top right is a recognized person with low probability, and the person in the bottom left is a known threat. The information is conveyed by the color of their

overlays. The following list describes the default colors used in SAFR overlays:

- **Gray**: Unrecognizable. A face was detected but it wasn't of sufficient quality to attempt recognition.
- **Purple**: Stranger. The person has been recognized, but they're not in Genetec's cardholder database nor in SAFR's Person Directory.
- **Blue**: Registered person without a name. The face was recognized as matching one already in the database.
- **Green**: Registered person with a name.
- **Yellow**: Concern. The registered face has been tagged as a concern.
- **Red**: Threat. The registered face has been tagged as a threat.

## 78.9 SAFR Video Processing Modes

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

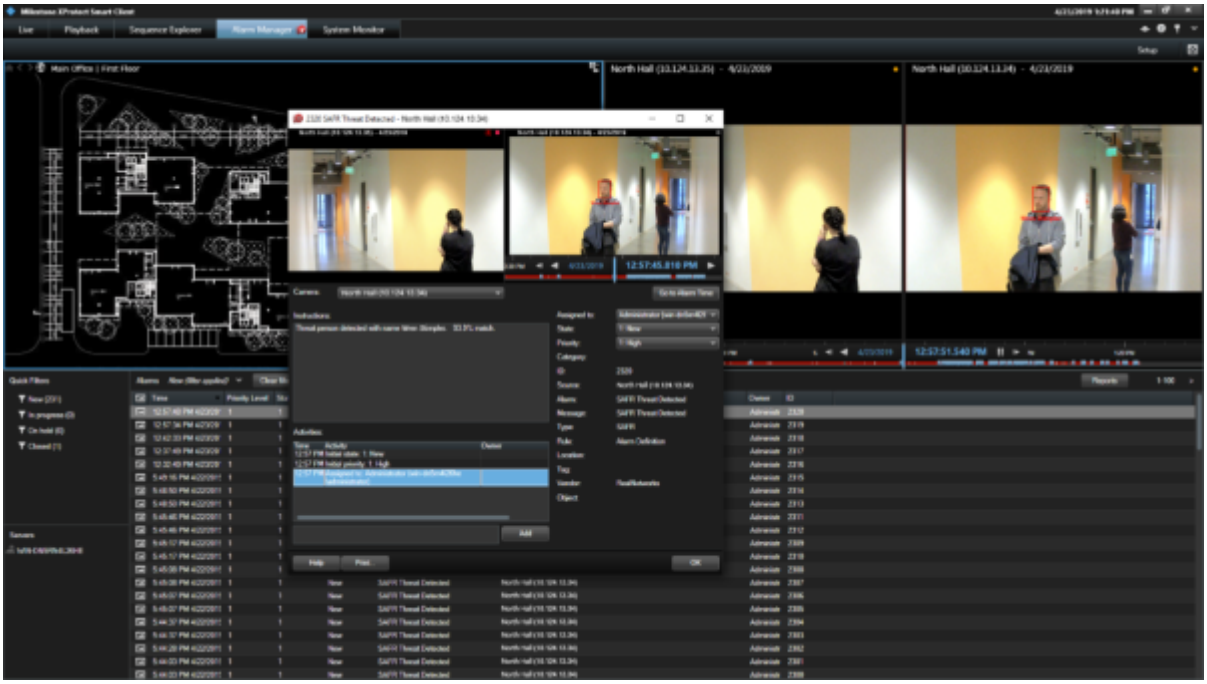
- **Secure Access**: Trigger events only for cardholders (or persons registered directly in SAFR) only when there is a high confidence match. Useful for secure entry (for example, unlocking doors).
- **Smile to Unlock**: Same as *Secure Access* but includes an additional trigger event if the user smiles.
- **Enrolled Monitoring**: Trigger events for cardholders (or persons registered directly in SAFR) but with lower confidence.
- **Enrolled and Stranger Monitoring**: Same as *Enrolled Monitoring* but triggers events for strangers also.

## 78.10 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 combinations of these conditions that can be triggered. The following shows multiple events populated in the Milestone alerts panel:



**Note**: Clicking any of the events on this screen allows the video from that event to be replayed.

## 78.11 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 not many faces found or recognized, check that the Milestone video feeds are of a sufficiently large frame size.
- If events are not being triggered, ensure the correct SAFR video processing mode is selected.
- If overlays are not displayed after configuration, the issue may involve a Windows Defender firewall security alert either before or after your system has been rebooted. The result is that the SAFR application is blocked. Configure Windows Defender Firewall Inbound Rules to enable SAFR and Client.

# 79 SAFR-Avigilon Integration Guide

Integrating SAFR's facial recognition and analysis capabilities into Avigilon enables you to use SAFR's video feed information overlays within Avigilon's 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 infomation such as age, gender, sentiment, name, company, known associates, and any other configurable information you want to create.

## 79.1 Integration Overview and Requirements

A typical deployment requires the following:

- A machine running the Avigilon Control Center (ACC) Server
- One or more machines running the ACC Client.
- 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.

### 79.1.1 System Requirements

Avigilon has the following requirements:

- Avigilon 7.4.0 or later

SAFR has the following requirements:

- Each machine running the SAFR Desktop client must meet the following requirements:
  - Windows 10.
  - The Desktop client must be version 2.0.106 or later.
  - Additional system requirements as described here.
- Local SAFR deployments require at least one machine running SAFR Platform 2.0.106 or later.
- Each machine running SAFR Server must meet the following requirements:
  - Windows 10.
  - Additional system requirements as described here.

## 79.2 Install the Avigilon Client and Server

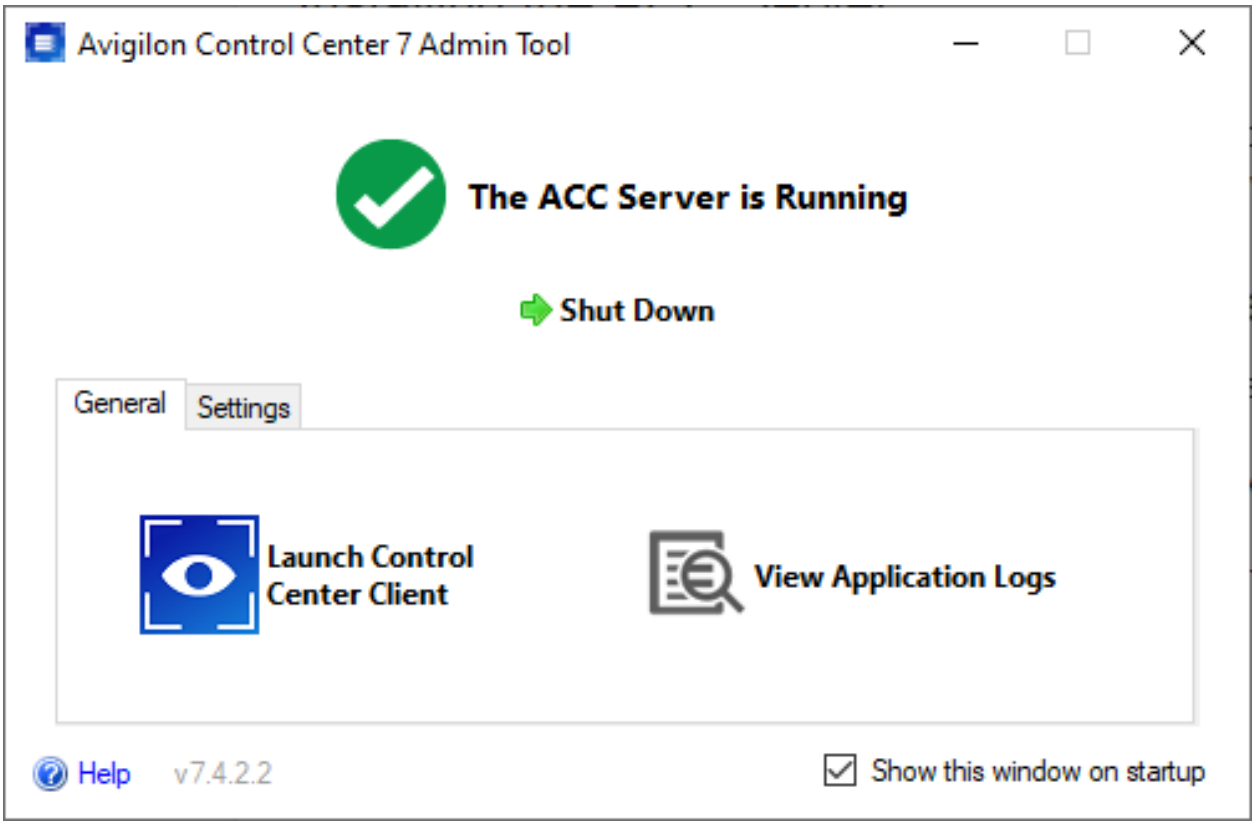
Download and install the ACC Client and the ACC Server from the Avigilon website:

- Full install (server + client): https://partners.avigilon.com/prm/English/s/assets?id=134904

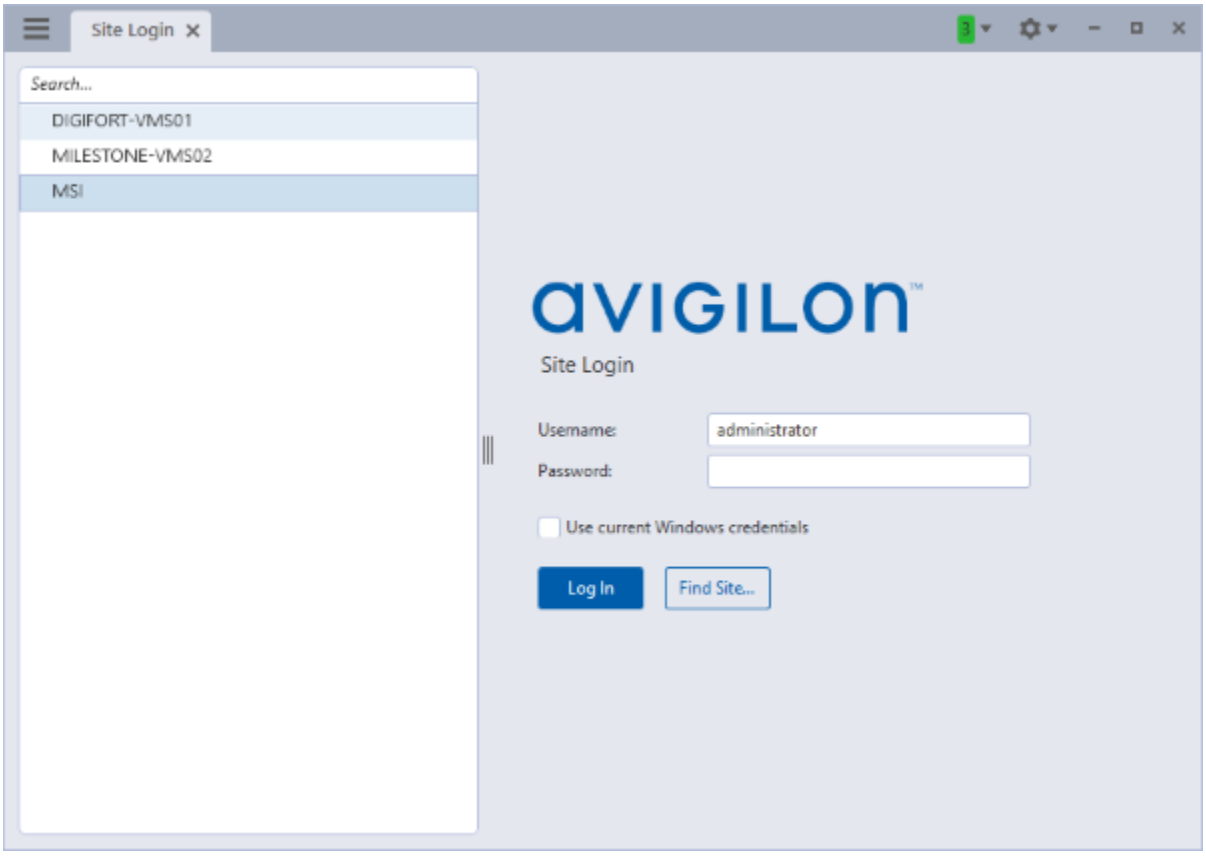
If you've already installed the ACC Server and merely want to install a second ACC Client, there's a client-only install location:

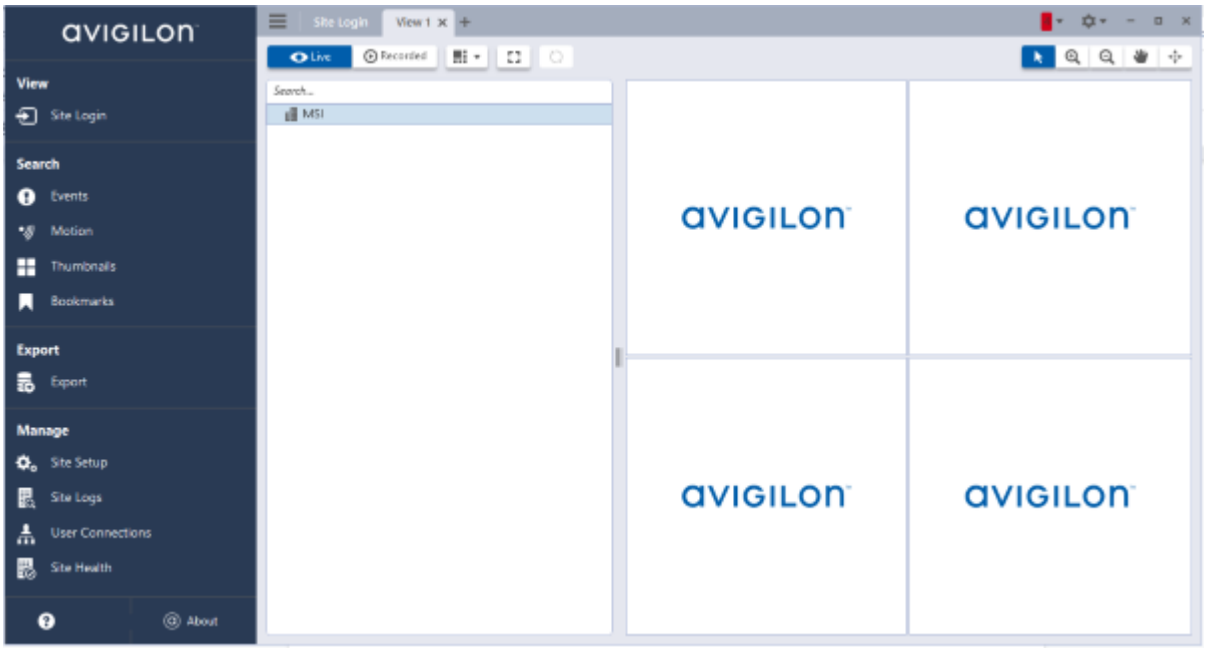
- Client-only install: https://www.avigilon.com/products/acc/7#download (scroll down to the "SOFTWARE DOWNLOADS" section)

The ACC Admin Tool can be used to manage network and storage configurations.




When logging in to the site for the first time, the default credentials use administrator as the username without a password. You'll be asked to immediately enter a new password.




## 79.3 Install the ACC Web Endpoint Service

To install the ACC Web Endpoint Service, download and install the ACC 7 Web Endpoint Service from the Avigilon website at https://www.avigilon.com/support/. Note that the ACC Web Endpoint Service must be installed on the same machine as the ACC Server.

Once installed, you can view the health of the ACC 7 Web Endpoint Service at https://localhost:8443/

## 79.4 Change the Default Port

The default port for the ACC Web Endpoint Service is 8443. You can change the default port by doing the following:

1. In the `%ProgramData%\Avigilon\` folder, open the WebEndpoint.config.yaml file in a text editor.
2. Add the following config parameter to the file, where `123` is the new port number:

   ```
   publicRestInterface: port: 123
   ```

3. Save the config file and restart the ACC Web Endpoint Service.

The default port is updated. All commands should be sent to the new port.

## 79.5 Using Insecure Connections

Although the default connection type used between SAFR and Avigilon is secure, (i.e. HTTPS) insecure connections (i.e. HTTP) are also supported. To change to an insecure connection, do the following:

1. In the %ProgramData% folder, open the WebEndpoint.config.yaml file in a text editor.
2. Add the following config parameter to the file:

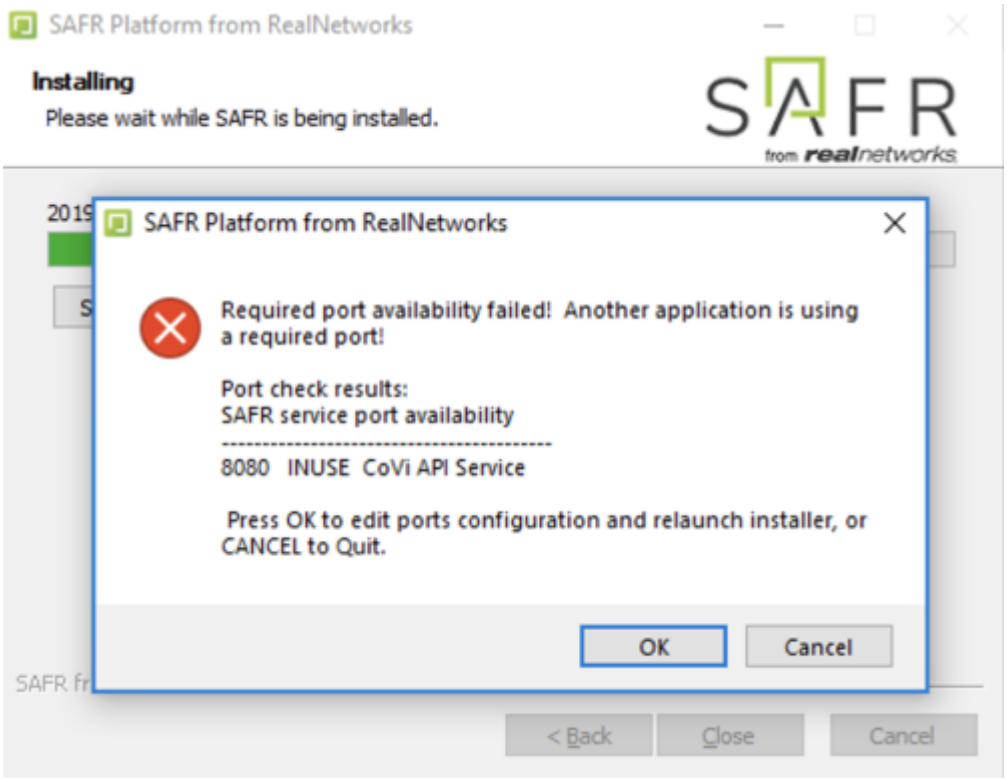
   ```
   publicRestInterface: secure: false
   ```

3. Save the WebEndpoint.config.yaml file and restart the ACC Web Endpoint Service.

All communication with the WebEndpoint will now be done insecurely using HTTP.

## 79.6 Install and Configure SAFR

1. Go to the SAFR Download Portal.
2. If you're doing a cloud deployment, download and install Windows SAFR Edge. Make sure to select the Genetec SDK install option.
3. If you're doing a local deployment, download and install Windows SAFR Platform. Make sure to select the Genetec SDK 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**.

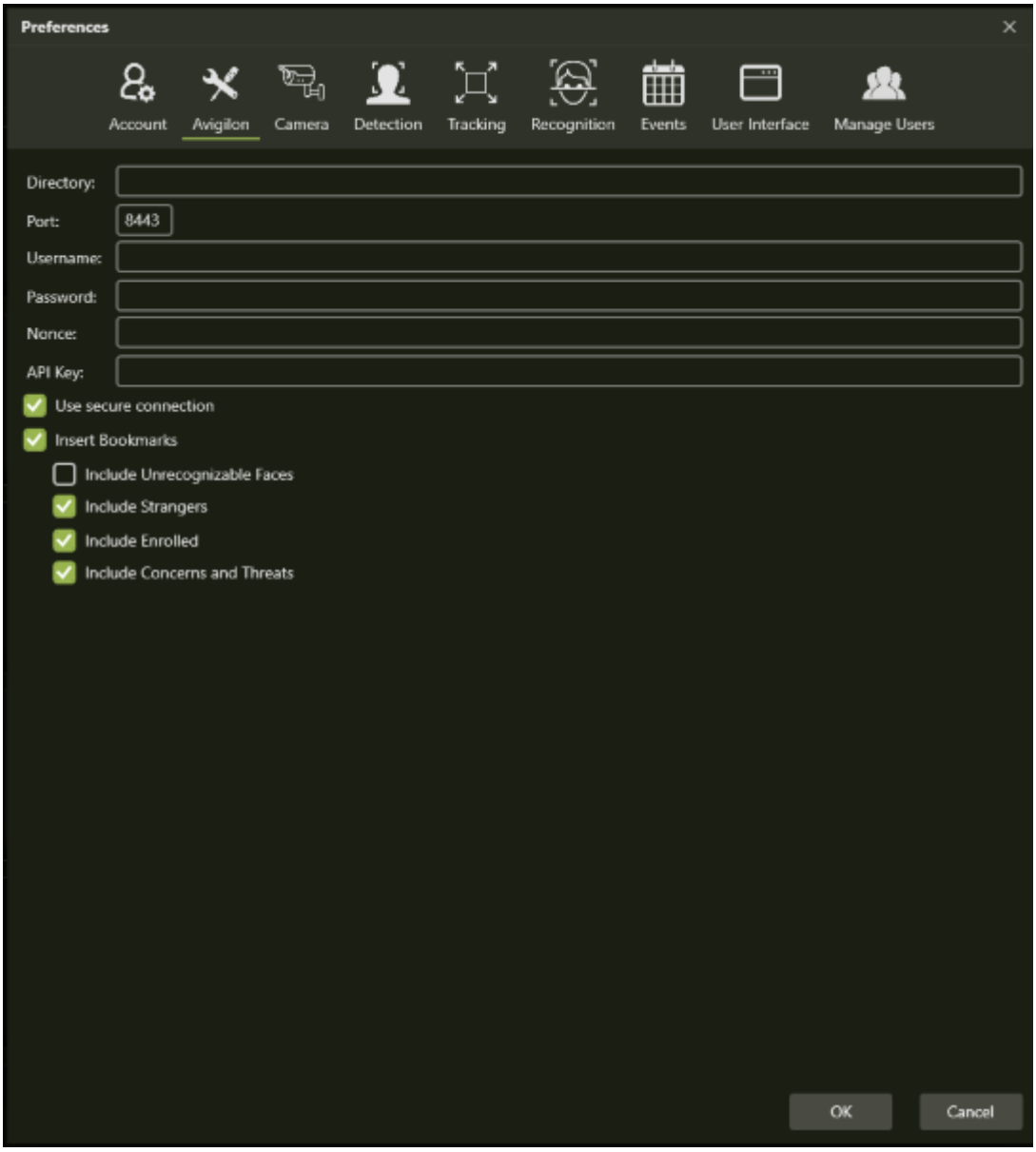
The Platform installer will then restart and the new port values will be used. You can find the modified *safrports.conf* file at `C:\Program Files\RealNetworks\SAFR\`.

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.

### 79.6.1 Configure SAFR

You can configure several Avigilon-specific preferences by opening the SAFR Desktop client, going to the Preferences Window and clicking on the Avigilon tab.




- **Directory**: IP address or hostname of the machine where the ACC server is installed.
- **Port**: The port number that the Avigilon server is configured to use. By default, Avigilon uses port 8443. See Change the Default Port above for information on how to change the port that the Avigilon server uses.
- **Username**: The username of a user that has been added to the Avigilon server via the "Users and Groups" tool.
- **Password**: The password of a user that has been added to the Avigilon server via the "Users and Groups" tool.
- **Nonce**: This value will be provided to you by Avigilon when you obtain a license. It will look something like `FO#26133902`.
- **API Key**: This value will be provided to you by Avigilon when you obtain a license. It will look something like `349f16ea6b3bc5cfd89dfeca3be33a602fcfe7e73b6b7437646a80ae1ed7ce3a`.
- **Use secure connection**: Specifies if SAFR uses a secure connection with Avigilon. By default, Avigilon uses secure connections. Only uncheck this if you have configured Avigilon to use non-secure connections. See Using Insecure Connections above for more information.

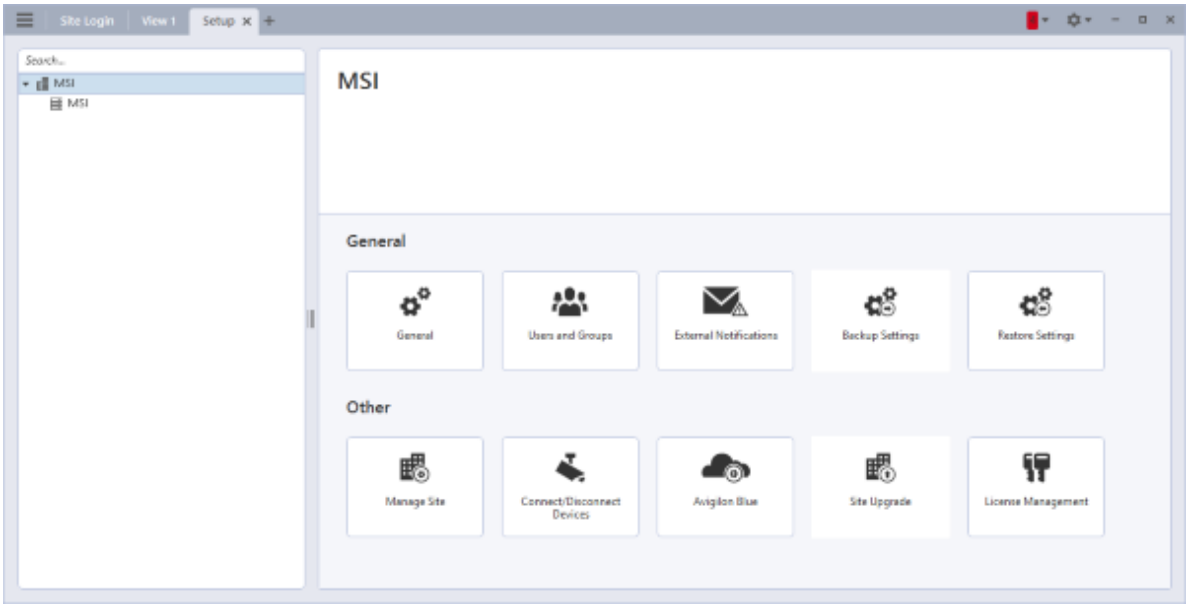
# 80 SAFR-Avigilon Operation Guide

Integrating SAFR's facial recognition and analysis capabilities into Avigilon enables you to use SAFR's video feed information overlays within Avigilon 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 infomation such as age, gender, sentiment, name, company, known associates, or any other configurable information you want to create.

## 80.1 Connect Cameras

To connect a camera to Avigilon, do the following:

1. Open the hamburger menu and select "Site Setup".
2. Select "Connect/Disconnect Devices".




## 80.2 Bookmarks

To view bookmarks, open the hamburger menu and select "Bookmarks".

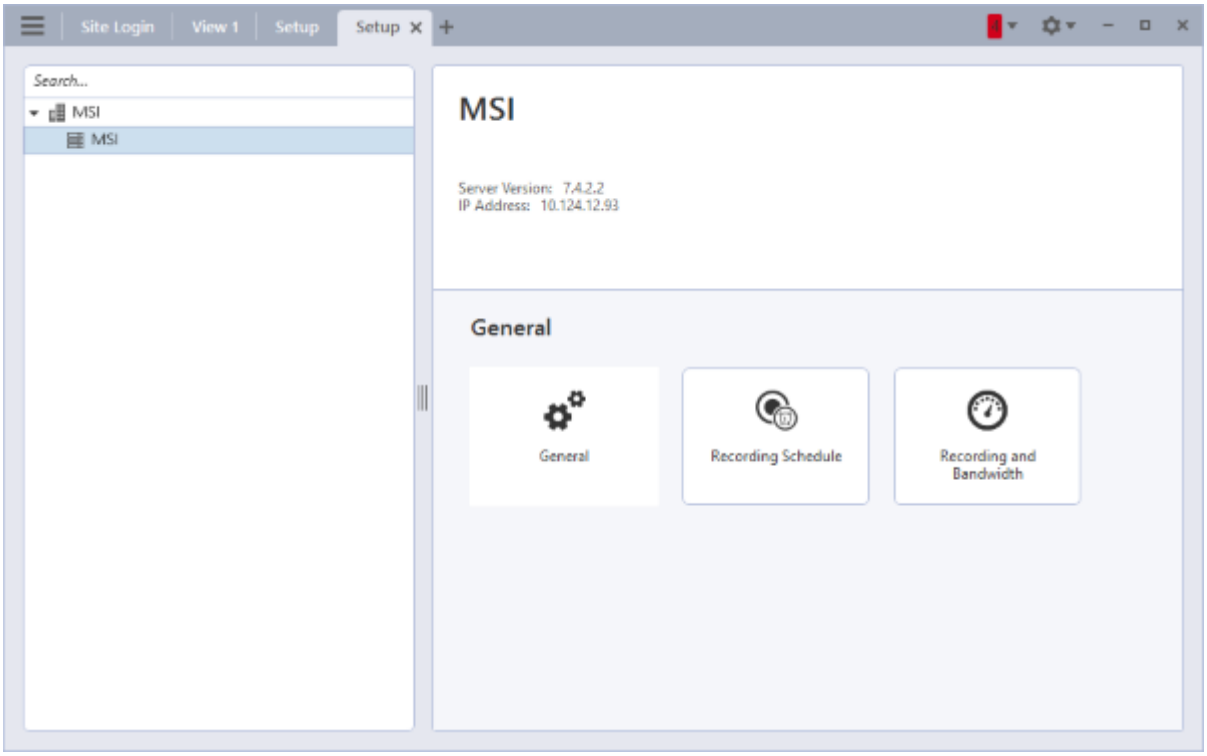
Selecting a bookmark in the left pane will show bookmark details and the associated video clip. Note that if there is no recorded video for the bookmark, then you may see a blank video or a snapshot of the current 'live' stream.

Bookmark titles are created to allow easy searching for relevant events

| Bookmark Title | | Bookmark Description |
|---|---|---|
| SAFR Unrecognizable Face | idClass="unidentified" | SAFR Unrecognizable face detected. |
| SAFR Stranger | idClass="stranger" | SAFR Stranger detected. |
| SAFR Unnamed Person | idClass="noconcern" && personType="" && name="" | SAFR Enrolled person detected without name. 98.2% match. |
| SAFR Person <name> | idClass="noconcern" && personType="" && name=<name> | SAFR Enrolled person detected with name <name>. 100.0% match. |

| Bookmark Title | | Bookmark Description |
|---|---|---|
| SAFR Person <personType> | idClass="noconcern" && personType=<personType> && name="" | SAFR Enrolled person detected of type <personType>. 100.0% match. |
| SAFR Person <personType> <name> | idClass="noconcern" && personType=<personType> && name=<name> | SAFR Enrolled person detected of type <personType> with name <name>. 100.0% match. |
| SAFR Smile <personType> | personType=<personType> && name="" | SAFR Smile activation by enrolled person of type <personType> without a name. 100.0% match. |
| SAFR Smile <personType> <name> | personType=<personType> && name=<name> | SAFR Smile activation by enrolled person of type <personType> with name <name>. 100.0% match. |
| SAFR Concern Person | idClass="concern" && personType="" && name="" | SAFR Concern person detected without a name. 100.0% match. |
| SAFR Concern Person <name> | idClass="concern" && personType="" && name=<name> | SAFR Concern person detected with name <name>. 100.0% match. |
| SAFR Concern Person <personType> | idClass="concern" && personType=<personType> && name="" | SAFR Concern person detected of type <personType>. 100.0% match. |
| SAFR Concern Person <personType> <name> | idClass="concern" && personType=<personType> && name=<name> | SAFR Concern person detected of type <personType> with name <name>. 100.0% match. |
| SAFR Threat Person | idClass="threat" && personType="" && name="" | SAFR Threat person detected without a name. 100.0% match. |
| SAFR Threat Person <name> | idClass="threat" && personType="" && name=<name> | SAFR Threat person detected with name <name>. 100.0% match. |
| SAFR Threat Person <personType> | idClass="threat" && personType=<personType> && name="" | SAFR Threat person detected of type <personType>. 100.0% match. |
| SAFR Threat Person <personType> <name> | idClass="threat" && personType=<personType> && name=<name> | SAFR Threat person detected of type <personType> with name <name>. 100.0% match. |

One way to make sure all bookmarks have recorded clips is to adjust the recording schedule to ensure video is recorded.




## 80.3 More Information about ACC Software

For more information about installing, configuring, and using ACC software, see https://www.avigilon.com/support/software/acc7/avigilon-acc7.4-installworkflowchecklist-en-rev2.pdf

# 81 May 2020 Release Notes

## 81.1 Windows

### 81.1.1 Lite Desktop Client

- Added Intel RealSense camera support
- Added 3D Liveness Detection (Beta)
- Added Mask Detection integration
- Added easy way to add feeds for background processing
- Bug fixes

### 81.1.2 Windows Desktop Client

- All the Lite Desktop client changes
- Added Vehicle Detection (Beta)
- Bug fixes

### 81.1.3 Windows SAFR Edge

- All the Windows Desktop client changes

### 81.1.4 Windows SAFR Platform

- All the Windows Desktop client changes
- Bug fixes

# 82 April 2020 Release Notes

## 82.1 Web Console

- Security fixes
- Detection List and image quality metrics display in remote video feed viewer

## 82.2 Windows

### 82.2.1 Lite Desktop Client

- VIRGA Processor Naming and Identification
- Added Video File Analyzer and Camera Feed Analyzer to Operator Console Tools menu
- Detection List and image quality metrics display in remote video feed viewer

### 82.2.2 Windows Desktop Client

- All the Lite Desktop client changes
- Contrast Enhancement: Global vs Local contrast enhancement
- Windows VIRGO auto naming based on PC Name

### 82.2.3 Windows SAFR Edge

- All the Windows Desktop client changes

### 82.2.4 Windows SAFR Platform

- All the Windows Desktop client changes
- Internal database update to keep date of birth reference instead of age
    - This results in people aging in the database with the passage of time.
    - At start, the database silently converts records to new format.

## 82.3 Linux

### 82.3.1 SAFR Linux Ubuntu and CentOS Platform

- All the Windows SAFR Platform changes

### 82.3.2 Jetson

- All the Windows SAFR Platform changes
- Higher efficiency (faster) face recognition leveraging FP16

## 82.4 macOS

### 82.4.1 macOS Desktop Client

- All the Lite Desktop client changes

### 82.4.2 macOS SAFR Edge

- All the macOS Desktop client changes

### 82.4.3 macOS SAFR Platform

- All the Windows SAFR Platform changes

## 82.5 iOS Mobile Client

- Bug fixes

## 82.6 Android Mobile Client

- Enable sorting of People alphabetically by last name or by registration date
- Order by last name is now supported by the GET /rootpeople API call
- People can now be searched by name

## 82.7 SAFR SDK

- Windows:
  - Cropping API Updates
  - Contrast Enhancement: Global vs Local contrast enhancement
  - Bug fixes
- Android:
  - No updates
- Linux:
  - Cropping API Updates
  - Contrast Enhancement: Global vs Local contrast enhancement
  - Bug fixes
- Jetson:
  - Cropping API Updates
  - Contrast Enhancement: Global vs Local contrast enhancement
  - Bug fixes

## 82.8 Embedded SDK

- Platforms being released:
  - Windows:
    - eSDK-full (includes NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
      - Bug fixes
    - eSDK-lite (no NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
      - Bug fixes
  - Linux x86 Ubuntu 16.04:
    - eSDK-full (includes NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
      - Bug fixes
    - eSDK-lite (no NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
      - Bug fixes
  - Linux ARM Ubuntu 18.04:
    - eSDK-lite (no GPU support)
      - Bug fixes
  - Jetson - Linux ARM Ubuntu 18.04:
    - eSDK-Jetson (NVIDIA GPU support)
      - Bug fixes
  - Android ARM - Android 5.0 or later:
    - eSDK-lite (no GPU support)
      - Bug fixes
    - eSDK-lite 64 bit (no GPU support)
      - Bug fixes

# 83 March 2020 Release Notes

## 83.1 Web Console

- Increased Video Viewer Frame Rate video feed viewer
- Video feed viewer overall support
- Event Archive support for Unauthorized Direction of Travel Detection action events.
- Email and SMS Server Configuration in Status Tab
- Support for Unauthorized Direction of Travel Detection feed configuration attributes
- Support for Cropping Parameters feed configuration attributes
- Support for Contrast Enhancement Integration feed configuration attributes
- Support for person detection input size configuration

## 83.2 Windows

### 83.2.1 Lite Desktop Client

- SAFR 2.0 UX
  - Live monitoring in single-window app
  - Inline camera settings UX
  - Handling password change for licensor userId
  - Option to disable Operator Console as primary window.
- Increased Video Viewer Frame Rate - support up to 30fps (new platform needed)
  - 30fps, 480p video for local deployments (configurable in VIRGA Tenant Config)
  - 5fps, 480p video for cloud deployments (configurable in VIRGA Tenant Config)
- Video Feed Viewer overlays
  - Right click on feed video to open context menu with overlay options.
- Video contrast enhancement (~20% improvement):
  - Contrast Enhancement Integration
- Unauthorized Direction of Travel Detection configuration and display in Event Archive

### 83.2.2 Windows Desktop Client

- All the Lite Desktop client changes
- Avigilon Integration
- More efficient face detection on NVIDIA GPUs
- Person detection input size configuration: NORMAL (default),SMALL, and LARGE.
  - SMALL: 26% faster than NORMAL
  - LARGE: 66% slower than NORMAL
- VIRGO for Windows updated:
  - VIRGO support for multiple remote video feed viewers
  - VIRGO support for video overlays (shown on remote video feed viewers).
  - VIRGO support for video feed Cropping Parameters
  - VIRGO support for Unauthorized Direction of Travel Detection configuration
  - VIRGO support for person detection input size configuration
  - VIRGO support for Contrast Enhancement Integration configuration.
  - VIRGO stability fixes
- Updated higher accuracy person detection model
  - Max Accuracy and Balanced modes improvement: 3%
  - Max Speed mode improvement: 7.1%
  - Balanced vs. Max Speed accuracy advantage: 36.2%

### 83.2.3 Windows SAFR Edge

- All the Windows Desktop client changes
- SMS Notifications support in SAFR Actions

    - Support for SMS Server Config in SAFR Actions (AWS SNS)
    - Support for configuring SMS alerts triggered by events in SAFR Actions
- Support for Unauthorized Direction of Travel Detection action events

#### 83.2.4 Windows SAFR Platform

- Age Model update with accuracy age recognition model
    - 15% improvement on Asian faces
    - 9.4% general improvement
- Increased Video Viewer Frame Rate
- Security Patches
- All the Windows SAFR Edge changes

### 83.3 Linux

#### 83.3.1 SAFR Linux Ubuntu and CentOS Platform

- All the Windows SAFR Platform changes

### 83.4 Jetson

- Person detection added
- Higher efficient (faster) face detection
- All the Windows SAFR Platform changes
- All the Windows SAFR Platform changes

### 83.5 macOS

#### 83.5.1 macOS Desktop Client

- Increased Video Viewer Frame Rate
    - support up to 30fps (new platform needed)
    - 30fps, 480p video for local SAFR Platform (configurable in VIRGA Tenant Config)
    - 5fps, 480p video for Cloud SAFR Platform (configurable in VIRGA Tenant Config)
- Video Feed Viewer overlays
    - Right click on feed video to open context menu with overlay options.
- Unauthorized Direction of Travel Detection configuration and display in Event Archive

#### 83.5.2 macOS SAFR Edge

- All the macOS Desktop client changes

#### 83.5.3 macOS SAFR Platform

- All the SAFR Window Platform changes

### 83.6 Android Mobile Client

- Addition of Android Events:
    - New side-menu navigation
    - Recent Matches view
    - Watchlist person view
        - Profile
        - Timeline
    - Deep-links from SMS or email
- Bug Fixes

## 83.7 iOS Mobile Client

- Bug fixes

## 83.8 SAFR SDK

- Windows:
  - Contrast Enhancement Integration
  - More efficient face detection on NVIDIA GPUs
  - Updated higher accuracy person detection model
- Android:
  - Bug fixes
- Linux:
  - Contrast Enhancement Integration
  - Updated higher accuracy person detection model
- Jetson:
  - Contrast Enhancement Integration
  - More efficient face detection on NVIDIA GPUs
  - Updated higher accuracy person detection model

## 83.9 Embedded SDK

- Platforms being released:
  - Windows:
    - eSDK-full (includes NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
      - Person detection
      - Bug fixes
    - eSDK-lite (no NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
      - Bug fixes
  - Linux x86 Ubuntu 16.04:
    - eSDK-full (includes NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
      - Person detection
      - Bug fixes
    - eSDK-lite (no NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
      - Bug fixes
  - Linux ARM Ubuntu 18.04:
    - eSDK-lite (no GPU support)
      - Bug fixes
  - Jetson - Linux ARM Ubuntu 18.04:
    - eSDK-Jetson (NVIDIA GPU support)
      - Person detection
      - More efficient face detection
      - Bug fixes
  - Android ARM - Android 5.0 or later:
    - eSDK-lite (no GPU support)
      - Bug fixes
    - eSDK-lite 64 bit (no GPU support)
      - Bug fixes

# 84 January 2020 Release Notes

## 84.1 Web Console

- New report: Queue Dashboard.
- Traversal Dashboard improvements.
- Traffic Dashboard optimizations.
- Attendance Dashboard enhancement.

## 84.2 Windows

### 84.2.1 Lite Desktop Client

- Sign-in UX changes to support operator workflows.
- Option to require sign-in on every start.
- User Administration.
- Option to disable Windows auto-update when in SAFR Kiosk Mode.
- Video Feed Viewer hides stats by default. Right click to display stats.
- Video Feed Viewer supports 10fps, 720p video (new platform needed).
- Genetec FR Plugin Improved SSL error handling and GUI option to turn off SSL.

### 84.2.2 Windows Desktop Client

- All the Lite Desktop client changes.
- VIRGO for Windows stability fixes.

### 84.2.3 Windows SAFR Edge

- All the Windows Desktop client changes.

### 84.2.4 Windows SAFR Platform

- All the Windows Desktop client changes.
- Installer options to install without SAFR Desktop and to customized path.
- Returned installer option to force CPU Face Recognition service.
- Initiated model initialization during installation to reduce initialization time upon launch.

## 84.3 Linux

### 84.3.1 Linux Ubuntu and CentOS SAFR Platform

- VIRGO enhancements.

## 84.4 Jetson

- SAFR Jetson Ubuntu 18.04 Platform has been implemented.

## 84.5 macOS

### 84.5.1 macOS Desktop Client

- Bug fixes.

### 84.5.2 macOS SAFR Edge

- Bug fixes.

#### 84.5.3 macOS SAFR Platform

- Bug fixes.

### 84.6 Android Mobile Client

- Added support for arm64-v8 architecture.
- Bug Fixes.

### 84.7 iOS Mobile Client

- Bug fixes.

### 84.8 SAFR SDK

- Windows:
  - Added Image analyzer support for person (object) and badge detections.
- Android:
  - Added support for arm64-v8 architecture.
  - Bug fixes.
- Linux:
  - Added Image analyzer support for person (object) and badge detections.
- Jetson:
  - Initial release

### 84.9 Embedded SDK

- Platforms being released:
  - Windows:
    - eSDK-full (includes NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
    - eSDK-lite (no NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
    - Changes:
      - Bug fixes.

# 85 December 2019 Release Notes

## 85.1 Web Console

- New Traversal Dashboard report

## 85.2 Windows

### 85.2.1 Lite Desktop Client

- Enhanced Event Archive GUI
- Person activity view
- CBP Face Acquisition System
- Advanced configuration of Center Pose Quality for strangers/learning: pitch, roll, and yaw
- Identity retention configuration
- Full Screen, Locked Screen, Auto-restart, Auto-logon, and Kiosk mode for Windows

### 85.2.2 Windows Desktop Client

- All the Lite Desktop client changes
- Enhanced Person Detection Accuracy - especially in crowded scenes
- Ximea Camera Integration

### 85.2.3 Windows SAFR Edge

- All the Windows Desktop client changes

### 85.2.4 Windows SAFR Platform

- All the Windows Desktop client changes
- All the System Console changes
- Concurrent face matching (3.5X lower matching latency on 8 core processor)
- Higher face-recognition throughput on non-GPU machines
- SAFR offline licensing

## 85.3 Linux

### 85.3.1 Linux Ubuntu VIRGO

- Person-face consolidated tracking enhancements
- Advanced configuration of Center Pose Quality for strangers/learning: pitch, roll, and yaw
- Enhanced Person Detection Accuracy - especially in crowded scenes

### 85.3.2 Linux Ubuntu and CentOS SAFR Platform

- All the Linux VIRGO changes
- All the System Console changes
- Concurrent face matching (3.5X lower matching latency on 8 core processor)
- Higher face-recognition throughput on non-GPU machines
- Identity retention configuration
- SAFR offline licensing

## 85.4 macOS

### 85.4.1 macOS Desktop Client

- Person-face consolidated tracking enhancements

- Event retention configuration GUI revision
- Identity retention configuration GUI
- Advanced configuration of Center Pose Quality for strangers/learning: pitch, roll, and yaw

#### 85.4.2 macOS SAFR Edge

- All the macOS Desktop client changes

#### 85.4.3 macOS SAFR Platform

- All the macOS Desktop client changes
- SAFR offline licensing

### 85.5 Cloud

- Concurrent face matching (3.5X lower matching latency on 8 core processor)
- Identity retention configuration

### 85.6 Android Mobile Client

- Hardware Video Decode
- Active Camera Connect
- Bug Fixes

### 85.7 iOS Mobile Client

- Dark mode bug fixes

### 85.8 SAFR SDK

- Windows:
  - Enhanced Person Detection Accuracy - especially in crowded scenes
- Linux:
  - Bug fixes
- macOS:
  - Bug fixes
- Android:
  - Bug fixes
- iOS:
  - Bug fixes

### 85.9 Embedded SDK

- Addition of new models: Age, Gender, Sentiment, Occlusion, Composite Signatures, Pose Profile, and Face/No-Face
- Platforms being released:
  - Windows:
    - eSDK-full (includes NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
    - eSDK-lite (no NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
  - Linux x86 Ubuntu 16.04:
    - eSDK-full (includes NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)

    - eSDK-lite (no NVIDIA GPU support, includes auto-selection between non-AVX and AVX2 support)
- Linux ARM Ubuntu 18.04:
    - eSDK-lite (no GPU support)
- Jetson - Linux ARM Ubuntu 18.04:
    - eSDK-Jetson (NVIDIA GPU support)
    - Include model compilation/optimization tool
- Android ARM - Android 5.0 or later:
    - eSDK-lite (no GPU support)

# 86 November 2019 Release Notes

## 86.1 Web Console

- Support for Anonymous vs. Known identity event retention configuration
- Support for Face-Person enhanced tracking
- Video feed occlusion detection config support
- Video feed config support to limit stranger reporting only to occluded strangers

## 86.2 ARES

- hasRootEventId filter was added

## 86.3 Windows

### 86.3.1 SAFR Windows Desktop Lite

- Support for Occlusion Detection configuration in Video Feeds
- Support for Anonymous vs. Known identity event retention configuration
- Preferences to limit stranger reporting only to occluded strangers
- Improved person import GUI
- Enabled person import directly from Event Archive
- Support for Mobotix Camera Events
- Support for Event time offset for offline videos
- Image quality metrics in Person Details dialog

### 86.3.2 Desktop Client

- All the SAFR Desktop Lite changes
- Enhanced person-face tracking and reporting
    - Consolidated person/face event reporting
    - Consolidated person/face event display
- Support for false face detection filtering
- Support for Genetec FR Plugin Integration
- Updated Virgo for Windows

### 86.3.3 SAFR Windows Edge

- Updated SAFR Desktop
- Updated ARES

### 86.3.4 SAFR Windows Platform

- Higher accuracy Face Recognition Model (v5 signatures)
- Faster (2x) DB Matching
- Redundant CVOS support
- Support for Anonymous vs. Known Identity event retention
- Support for Face No-Face Classification
- Updated System Console
- Updated ARES
- Filtering of secondary faces on import via REST API

## 86.4 Linux

### 86.4.1 SAFR Linux Ubuntu VIRGO

- Occlusion Detection

- Enhanced person-face tracking and reporting
  - Consolidated person/face event reporting
  - Consolidated person/face event display
- Face No-Face Classification Integration

### 86.4.2 SAFR Linux Ubuntu and CentOS Platform

- Higher accuracy Face Recognition Model (v5 signatures)
- Faster (2x) DB Matching
- Redundant CVOS support
- Port conflict resolution at install time
- Support for Anonymous vs. Known Identity event retention
- Support for Face No-Face Classification
- Updated VIRGO
- Updated System Console
- Updated ARES
- Filtering of secondary faces on import via REST API

## 86.5 macOS

### 86.5.1 macOS Desktop Client

- Occlusion Detection
- Enhanced person-face tracking and reporting
  - Consolidated person/face event reporting
  - Consolidated person/face event display
- Face No-Face Classification Integration
- Support for Anonymous vs. Known identity event retention configuration
- Model Upgrade GUI

### 86.5.2 SAFR macOS Edge

- Updated SAFR Desktop
- Updated ARES

### 86.5.3 SAFR macOS Platform:

- Higher accuracy Face Recognition Model (v5 signatures)
- Faster (10x) DB Matching
- Support for Anonymous vs. Known Identity event retention
- Support for Face No-Face Classification
- Updated System Console
- Updated ARES
- Filtering of secondary faces on import via REST API

## 86.6 Cloud:

### 86.6.1 SAFR Platform

- Higher accuracy Face Recognition Model (v5 signatures)
- Faster (2x) DB Matching on Windows
- Redundant CVOS support via NFS
- Support for Anonymous vs. Known Identity event retention
- Support for Face No-Face Classification
- Updated System Console
- Filtering of secondary faces on import via REST API

### 86.6.2 Download Portal

- Updated Android System Requirements
- Removed Create new account link

## 86.7 Android SAFR App and SDK:

- Bug fixes

## 86.8 Embedded SDK (Windows and Android)

- Composite signature support
- Faster multi-core face signature matching

# 87 September 2019 Release Notes

## 87.1 SAFR Windows

### 87.1.1 1. Central Video Feed Management

Video feeds on Windows can now be configured and managed centrally for the entire cluster of SAFR Windows (and Linux) Platform machines. This means that a large deployment can be configured from a single machine using the Desktop client (preferred) or the System Console. SAFR no longer requires video feed windows to remain open, nor do Windows users need to remain logged. SAFR will now also automatically resume processing on system reboot. This makes SAFR on Windows a fully resilient service that can handle power outages and be easily managed even when distributed on many machines.

To enable this, SAFR Windows Platform now comes with Virgo for Windows which performs video feed processing in the background. Windows Virgo supports Genetec, Milestone and Digifort VMS feeds as well as ONVIF, direct RTSP URL, and USB camera feeds. You can configure Windows Virgo via the Windows Desktop client or the System Console. The Windows Desktop client is recommended as a configuration tool in all cases and is required if configuring VMS feeds. When adding a feed simply select an auto-detected camera and choose operation mode.

### 87.1.2 2. Redundant DB Configuration

As was already available on Linux, SAFR Windows Platform can now be configured for redundant DB operation. This means that all DB information (this includes face signatures, person meta-data and events but does not yet include images) will be stored in two or more separate machines and loss of one DB machine will automatically fail-over to another. Redundant DB operation also enables horizontal scalability of the face-matching operation which is distributed across all participating DB machines thus increasing size of deployment achievable (hardware estimator provides number of DB machines needed).

Keep in mind that you must have an odd number of DB machines for automatic failover to function and that the maximum number of redundant DB machines is 50.

### 87.1.3 3. Watchlist Synchronization across SAFR Platforms and Accounts

SAFR can now be configured to synchronize watchlists from one SAFR Platform or Account to any number of other SAFR Platforms or Accounts. This means that SAFR Platform can now be deployed in a distributed manner with many independent SAFR Platforms at different locations and yet be kept updated with a watchlist maintained centrally (e.g. in Cloud).

You can configure SAFR Platform to synchronize one directory per account (tenant) from the System Console Status tab. Max latency for synchronization is 10 minutes and max throughput is ~20 records per second per sync connection. It might thus take up to 10 minutes to perform initial sync of 10K records.

### 87.1.4 4. 5X Faster DB Matching Speed

DB matching speed and efficiency have been improved 5x. This means that matches are 5x faster and require 5x less processing power. This translates to significant TCO savings for deployments requiring large watchlists.

On single CPU core, 1 million faces can now be matched in 350-400ms.

### 87.1.5 5. SAFR Actions for Occlusion

SAFR Actions and Action Relay Event Service (ARES) now supports occlusion event attributes. This means you can configure actions to trigger specifically on occluded faces. For more information, search on “occlusion” in *Action Relay Event Service - ARES manual*.

### 87.1.6 6. Person (Body) Detection Balanced Mode

Person detection balanced mode delivers 50% more throughput than max accuracy mode with only slight degradation in accuracy. This is now the default mode for person detection and is recommended for all cases when high accuracy of person body detection is needed (e.g. tracking in visually complex environments with several persons present).

In comparison, max speed person detection mode delivers 300% more throughput than balanced mode but with significant reduction in accuracy. However, this mode is commonly adequate for low complexity tracking such as casino tables or teleconferencing rooms.

## 87.2 SAFR Linux

### 87.2.1 1. Multi-GPU Scalability

SAFR Linux Platform now offers enhanced scalability across multiple NVIDIA GPUs. SAFR Linux VIRGO has been optimized to be even less reliant on CPU and to maximize use of NVIDIA GPUs. This means that a single large machine can support 6 NVIDIA T4 processors which amounts to a SAFR recognition payload of 90 1080p@15fps feeds or 75 4K@15fps feeds (inclusive of recognition).

This capability is also available in standalone VIRGO Ubuntu download from Developers page.

### 87.2.2 2. Person Body to Face Recognition Linkage

Person body detection and tracking is now enhanced with face recognition and thus takes on identity established through face recognition. As person body detection is more accurate than face (due to size and being detectable in nearly any orientation) this means that identity tracking with combined person body and face detection is more accurate than face alone. When more accurate account of identity presence before the camera is needed, person events can now be used which are augmented with associated face attributes.

This function is automatically enabled when both person (body) detection and face recognition are enabled.

### 87.2.3 3. The Following New SAFR Windows features are also now available on Linux

- Watchlist synchronization across SAFR Platforms and Accounts
- 5X faster DB Matching speed
- Person (body) detection balanced mode

## 87.3 macOS Desktop Client

### 87.3.1 1. Pose Based Liveness Detection

This features previously introduced on Linux is now also available on macOS. It enables liveness detection based on consistent change in face orientation (pose) as an alternative to smile action. It can be used for walk-up and walk-through secure access scenarios that require liveness confirmation when paired with well positioned cameras.

### 87.3.2 2. Person Body to Face Recognition Linkage (Same as Linux)

## 87.4 SAFR Android

### 87.4.1 Faster SAFR Native Face Detector

SAFR native face detector is now multi-threaded on Android and offers higher frame-rate and accuracy than Google Vision face detector (available when Google Play is present on the device). The Android Mobile client now delivers excellent face detection performance at ~15fps while utilizing 35% CPU and Google Pixel phone.

### 87.4.2 Frame Skipping Logic to Maintain Low Latency of Detection and Recognition

When video frame rate is higher than detection rate device can deliver, video frames will be appropriately skipped for analysis in order to not cause backlog of processing that would increase latency in detection and recognition.

## 87.5 SAFR Embedded SDK (Windows and Android)

1. Person record export / import API
2. Face landmark coordinates (eyes, nose, mouth)
3. Face signature export / import API

## 87.6 SAFR SDK

**Windows:**

- Bug Fixes

**Android:**

- Multi-threaded face detector with higher face detection throughput.
- Frame skipping logic to maintain low latency of detection and recognition.

# 88 August 2019 Release Notes

## 88.1 SAFR Windows

- Occlusion Detection:

  SAFR now has the ability to detect faces that are occluded. Occlusion constitutes any obstruction of the key facial features such as from a scarf, hand, glasses, hair draping over the face, etc... This capability is currently integrated to accomplish two features:

  1. To filter out any occluded faces while learning them in the wild and thus prevent storing ambiguous face references in the SAFR person database.

     For example, such a feature is used when learning and memorizing players sitting at the casino table to prevent learning them with an occlusion feature such as a wineglass in front of their face which may later create recognition inaccuracies.

  2. To update occurrence event records with better face images without the occlusion and thus increase the value of the image stored with the event for presentation and investigation purposes.

  You will find the occlusion recognition switch in the **Recognition** tab under SAFR Preferences as well as max tolerable occlusion level adjustment for newly learned faces.

- Core Face Recognition Optimizations for NVIDIA GPUs:

  These optimizations enable up to 463 recognitions per second on NVIDIA GTX 1080Ti graphics cards. This is 14x more recognition throughput in comparison to the maximum achievable on 4 Core 3.4GHz Intel Xeon Skylake-SP processor. The improvement is even more pronounced when all face attributes are computed together (identity, age, gender, sentiment). In such case optimization delivers 320 combined recognitions per second which is 40x more throughput in comparison to maximum achievable on 4 Core 3.4GHz Intel Xeon Skylake-SP processor. These optimizations also reduce recognition latency by 50% and thus enable even faster and more reliable recognition. All this results in cost reductions for on-premise core recognition subsystem deployments from $2,477 to $518 per 100 recognitions per second and from $10,667 to $797 for 100 all-attributes recognitions per second.

  Note that these optimizations introduced a necessary one-time GPU calibration step which is performed when the system is started for the first time with GPU(s) present. It takes about 3 minutes per recognition model (15 minutes total) and per GPU for the system to be properly calibrated. Until this is completed, you will see System Initializing message in video view and recognition will not be be operational.

- Person Body Detection NVIDIA GPU Optimizations

  Person detection speed was improved by 30% and throughout by 50%. This means person detection is faster and more fluid than before. Maximum person detection throughput for our max accuracy model is 115 frames per second on NVIDIA GTX 1080Ti and 329 frames per second on NVIDIA Quadro RTX 6000. Maximum person detection throughput for our max speed model is 625 frames per second on NVIDIA GTX 1080Ti and 1052 frames per second on NVIDIA Quadro RTX 6000.

- Customizable options were added to our popular traffic dashboard (available from the Reports tab in the System Console). These options enable traffic dashboard to be customized in color, logo, language, and time-range. The traffic dashboard can now also be linked directly from another web site and all customization options are available as URL query parameters. This feature enables easy integration of the dashboard into customers' portals who may wish to display the dashboard in colors and logos of their brand.

- A new attendance dashboard was added to the Report tab in the System Console. For a specified time range and location, it displays all recognized individuals in attendance along with the time interval they were observed present. This dashboard can be used as a replacement of punch-card system that

tracks employee attendance when properly combined with entry and exit camera monitoring ingress and egress at the work site.

- Installer has been equipped with more customizable options to allow SAFR Logs to be removed from deployment and heap auto-configure behavior to automatically scale memory allocation for SAFR based on system memory available. These options enable SAFR Platform to be deployed on very small PCs (8GB RAM, 32GB Disk, $550) that can independently monitor 2 1080p video feeds. For example, such a small configuration could be used for a small SAFR Platform deployed at a casino table. The heap auto-config also enables SAFR to scale up on larger system and thus reliably handle higher recognition throughput and event traffic.
- To further protect privacy, SAFR now also limits retention of system logs associated with events to the same time frame as configured for events retention in the SAFR database. This means that no trace of individual whereabouts is kept beyond the configured retention time. Recognition logs have also been reduced in their default logging level so as not to include any personally identifiable information (PII).

## 88.2 SAFR Linux

- The Linux release inherited the following improvements introduced above for Windows:
  - Customizable options for Traffic Dashboard.
  - New Attendance Dashboard.
  - Log retention and log content changes to protect privacy.
- Database fail-over is now enabled on Linux. This means when SAFR is deployed on multiple machines with Database redundancy enabled, failure of the primary machine (containing primary Database) will not degrade secondary nodes that are running redundant Database from full functionality.

## 88.3 SAFR SDK

- RTSP support has been added to iOS and Android SAFR SDK. This means that SAFR SDK can now process video feeds delivered via rtsp protocol widely supported by IP cameras and can be thus used to process video feeds from a detached camera. For example, iOS or Android device can be used to process video feed from body camera connected to the device via WiFi.
- iOS SAFR SDK is available in our Partner Cloud and Production environment.
- Android SAFR SDK is available in our Partner Cloud environment and will be further validated and pushed to production next week.
- Windows SAFR SDK has person body detection added to its capabilities which enables developers to implement alerts based on body detection and traffic counting. Also new in Windows SAFR SDK is availability of pitch, roll and yaw face attributes which describe orientation of the face around all three axis.

## 88.4 Mobile Clients

- iOS and Android Mobile clients have been equipped with same RTSP support described above for SAFR SDK. To connect an RTSP feed, press-and-hold camera selection button in bottom right corner. You will be able to register several RTSP feeds that will be stored and made available for selection.
- iOS SAFR application is awaiting review by Apple and will be available next week in the app-store.
- Android SAFR application will also be available next week on SAFR Partner and Production Cloud portal.

## 88.5 SAFR Cloud

- Occlusion detection is now available in SAFR Cloud and can be utilized by developers via SAFR REST APIs or be used through the Desktop client for Windows.
- Customizable Traffic Dashboard and Attendance Dashboard described above are also available in SAFR Cloud.

## 88.6 SAFR Stability

- 67 defects were fixed for this release.

## 88.7 Follow-up Update

A small follow-up update was released later in Auguest.

1. The Mobile client for Android was released with the following new capabilities:
   - RTSP video feeds are now supported. This means that Mobile clients can now process video feeds delivered via RTSP protocol widely supported by IP cameras and can be thus used to process video feeds from a detached camera. For example, Android devices can be used to process video feeds from body cameras connected to the device via WiFi. To connect an RTSP feed, long-press camera selection button in bottom right corner. You will be able to register several RTSP feeds that will be stored and made available for selection.
   - Google Play Services are no longer required on Android device. SAFR now includes own SAFR face detector. You can switch between Google and SAFR detectors for integrated camera use. SAFR face detector provides higher detection accuracy but is slightly slower when processing feeds from devices integrated camera due image conversion overhead which we will look to eliminate in the future. RTSP feeds are always processed via SAFR face detector which offers higher detection accuracy and speed over Google supplied face detector.
2. SAFR Cloud, SAFR Windows Platform, SAFR Windows SDK, and SAFR Android SDK were released with a few more bug fixes.