# Security Cam Cloud Service

# Cloud Service for Hosting Multiple Security Cam Instances

## Introduction

The Cloud Server is intended for use with the Security Cam NVR project.

The Security Cam (NVR, Network Video Recorder) project is primarily designed to run without the need for a cloud service, inside a secure LAN, with access from WAN being made available with port forwarding. The Cloud Server can be used to provide access to a number of NVR instances without the port forwarding set up, as the NVR makes a client connection to the Cloud Service through which the web interactions are multiplexed.

The Cloud Server is intended to be run at a public internet address, to which instances of Security Cam are configured to make client connections. The NVR does not need to have a local user account set up to connect to the Cloud Service. Instead a user account is created on the Cloud Service for each NVR connected to it. When the user account is created, the required username, password and email address are entered along with the NVR's unique product ID by which the Cloud Service identifies the specific NVR, When an NVR has no local account, it will attempt to connect to the Cloud Service by default.

## Description

The Cloud server application consists of a Java (Grails) server side with an Angular 12 web application for the client side. The Angular client has two operating modes, as an admin application (for the admin user), and client mode for users who login to use their NVR. In client mode, the server side acts as a proxy to the connected NVRs with user accounts, so most restful API calls are made through this proxy to the users NVR. The Cloud Server can handle multiple NVRs and each connected NVR must have a user account set up on the Cloud Server to give client access to it. Each NVR is associated with its user account with a unique product ID that is set on the NVR on initial installation, and is entered along with the account data when the account is originally set up. Each connected NVR has its own individual proxy interface to its web server backend. The Cloud Server logs onto the NVRs using a special secure access Cloud Account.

#### Cloud Service Features

- Hosts multiple NVRs with each one having its own user account
- When not logged in
  - Login as admin or to one of the client accounts.
  - Register a new client (NVR) account.
- Admin Access
  - Change admin account password.
  - Show list of connected NVRs
  - Indicate which NVRs have Cloud accounts
  - Indicate which NVRs with Cloud accounts are connected to the Cloud.
  - For each NVR, show number of users viewing the NVR through the Cloud Service.
  - Change users Cloud account password.
  - Change users Cloud account email address.
  - Enable/Disable users Cloud account.

  - Delete Users Cloud Account.
  - Show only accounts where the NVR is offline (not connected to Cloud)
  - Show only connected NVRs with no Cloud user account set up.
  - NVR list filter for username/product id
- Client NVR access
  - Most features present through direct access to the NVR are present with client access on the Cloud. Camera web admin pages are not accessible through the Cloud as they are with direct NVR access. The Admin functions are not present, though you can add or remove the local NVR account.
  - NVR configuration
  - Add/Remove local NVR account.

### Run time platform, for Cloud Server

The current build configuration (as created with./gradlew buildDebFile) is for Raspberry pi V4 running headless (server) version of Ubuntu 23.10 (Mantic Minotaur). The application runs on Java on the server side, so it can easily be adapted to other platforms.

### Tomcat Web Server

Tomcat 9 (https://tomcat.apache.org/) hosts the server (Web Back End) and client (Web Front End) of the NVR, giving access to these through port 8080.

### Web Front End

The Web Front End (client) is an Angular application using Angular CLI version 12.0.5 or later. This forms the user interface of the web application. To get more help on the Angular CLI use `ng help` or go check out the Angular CLI Overview and Command Reference page.

### Web Back End

The Web Back End (server) is a Grails application (https://grails.org/), which provides a Restful API for the Angular Web Front End in admin mode. In client mode, the Restful API is mainly from the NVR via the account proxy.

## Building the project

Ready built .deb files are included in the Releases section, otherwise read the directions below.

**The project is verified to build with the following:-**

- Angular CLI: 15.2.0 or greater
- Node: 18.17.1
- npm: 9.9.7
- Package Manager: npm 9.6.7
- Grails Version: 5.3.2
- openjdk version "19.0.2" 2023-01-17
- Gradle 7.6

Using other versions may cause build issues in some cases.

### Set up build environment

```
git clone git@github.com:richard-austin/cloud-server.git
cd cloud-server
```

### Build for deployment to Raspberry pi

```
./gradlew buildDebFile
```

This will create a deb file with a name of the form cloud_*VERSION-nn-ID-dirty*_arm64.deb Where:-

- *VERSION* is the most recent git repo tag
- *nn* Is the number of commits since the last git tag (not present if no commits since last tag.)
- *ID* The last git commit ID (not present if no commits since last tag.)
- *dirty* "dirty" is included in the name if there were uncommitted changes to the source code when built.

When the build completes navigate to where the .deb file was created:-

```
cd xtrn-scripts-and-config/deb-file-creation
```

scp the .deb file to the Raspberry pi

## Installation on the Raspberry pi

The Raspberry pi should be running Ubuntu 23.10 (Mantic Minotaur) OS.

```
sudo apt update
sudo apt upgrade
```

(restart if advised to after upgrade)

Navigate to where the .deb file is located

```
sudo apt install ./deb_file_name.deb
```

- Wait for installation to complete.
- The Tomcat web server will take 1 - 2 minutes to start the application.
- *If this is the first installation on the Raspberry pi..*
    - *Generate the site certificate..*

```
cd /var/cloud
sudo ./install-cert.sh
```

    Fill in the details it requests (don't put in any information you are not happy with being publicly visible, for example you may want to put in a fake email address etc.)

  - nginx will not have started in the absence of the site certificate, so restart nginx.

```
sudo systemctl restart nginx
```

# Initial Setup

### Set up admin user account password

The admin account is set up with the default password *elementary*, this should be changed first of all.

- Set a browser to https://*cloud-server_ip_addr*
- Ignore the warning which may be given as a result of the home generated site certificate and continue to application which will show the menu bar.
- Click on the *Log in* option on the menu bar
- Enter *admin* as the user name and *elementary* as the password.
- Click confirm.
- Click on *General* on the right had side of the menu bar.
- Click on *Change Password*
- Enter *elementary* as the current password
- Enter you new password and again in the confirm box.
- Click on *Change Password*
- The new password is now set up.

# Admin Mode

To enter administrator mode: -

- Set a browser to https://cloud-server_ip_addr (ip address of the Cloud Server).
- Click on the *Log in* option on the menu bar.
- Enter *admin* as the user name and the admin password you set above as the password.
- On the menu bar, select *Admin -> Accounts Admin*. A table listing connected NVRs and NVR Cloud Server accounts will be shown.

# Client Mode

In client mode you are connected to your NVR and can use the functions of that NVR. This includes viewing live CCTV streams, selecting recordings by date and time and viewing them, set certain camera parameters and configure camera setup including Wi-Fi.

### Requirements To Access NVRs Through The Cloud

- There must be at least one NVR with its cloudProxy -> cloudHost configuration in application.yml set to the ip address of the Cloud Server. The cloudPort number is normally 8081.
- The Cloud Server may be hosted at a public IP address or within the same LAN as the NVRs.
- On the NVRs which are to connect to the Cloud, ensure the cloud proxy is enabled (checkbox checked at General -> Set CloudProxy Status).
- There must be a Cloud user account for each NVR you connect to the cloud. To set up Cloud user accounts, you will need the unique product ID for each of the NVRs. The product ID is shown towards the end of the text which is displayed during the initial installation of the NVR software. It can also be seen on the User Accounts list with the Cloud admin account.
- Set up a Cloud user account for NVR: -
  - Connect a web browser to the Cloud.
  - Select *Create Account* on the menu bar.
  - Enter the username for the intended NVR (this is for the cloud account and does ***not*** have to be the same username as an existing user account on the NVR).
  - Enter the NVRs 16 character unique product ID.
  - Enter the account password and confirm it (this is for the cloud account and does ***not*** have to be the same password as an existing user account on the NVR).
  - Enter the email address for the account and confirm it (required for reset password links).
  - Click the *Register Account* button.

With the Cloud user account and the NVR CloudProxy connected to the Cloud, you can now log in.

#### Login to an NVR client account

- Set a browser to https://cloud-server_ip_addr (cloud server ip address)
- Select "Log in" end enter the Cloud account username and password which was set up for the required NVR. There may be a warning about the self generated site certificate, which can be safely ignored.

When logged into an NVR client account, most functions are the same as when connected directly to the NVR itself. The differences between direct NVR access vs access through the Cloud are: -

- The Camera Settings -> Camera Admin options where the camera admin pages are hosted is not supported on the Cloud.
- The Camera Settings -> Quick Camera Setup option is not present with the options (only for SV3C and ZXTech cameras) appearing directly under the Camera Settings menu.
- The Setup Guest Account option is not available through Cloud Access.
- The General -> Change Account Email option is not available via the Cloud. Instead, use General -> Admin Functions, then select "Create or Update User Account" (which is also present with direct NVR access).
- With Cloud access, there is the option "General -> Remove Local NVR Account" which is not present with direct NVR access.

#### Client Functions Only Available In Cloud Client Mode

- ***Remove Local NVR Account***
  - Removes the local user account on the NVR. After this operation it will not be possible to log in directly to the NVR. With no local user account on the NVR, this option will be replaced with

***Register Local NVR Account***

- ***Register Local NVR Account***
  - Create a user account for direct login to the NVR. Selecting this option brings up a dialogue box in which you enter the required username, and enter and confirm the account password and email address.
  - Fill in those details and click the ***Register Account*** button to create the user account.

With a local user account on the NVR, the ***Register Local NVR Account*** option will be replaced by the ***Remove Local NVR Account*** option.

The email address entered on the form is used to send reset password links for direct NVR login. Reset password links for Cloud accounts are sent to the email address associated with the Cloud account. The email address is also used to send changed public IP address warnings (useful when accessing the NVR from outside the LAN through port forwarding on the router).