



Overview	3
Requirements	4
Connecting to Systems	5
Connecting to a Local System	5
Connecting to a Cloud System	8
Server Certificate Validation	10
Viewing Cameras	12
Archive	14
Camera Options	15
Motion Search	17
2-way Audio	17
Fisheye Dewarping	18
Soft Triggers	18
PTZ	19
Viewing Layouts	20
Client Configuration	22

Overview

This user manual is intended to assist in the general usage of the Nx Witness Mobile Client.

Features of the Nx Witness Mobile Client:

- Connect to Local or Cloud Systems
- View live streams from cameras
- Access layouts created in the Desktop Client
- Search through the recorded archive
- PTZ camera control
- Fish-eye camera dewarping
- Two-way audio
- Soft triggers
- Push notifications

The Nx Witness Mobile Client has no administrative capabilities. We recommend using the Nx Witness Desktop Client and referring to the associated [in-client user manual](#) to learn about its administrative functionality.

Requirements

You need to meet the following requirements to use the Nx Witness Mobile Client to access a System:

- A supported iOS or Android device on a [compatible OS version](#).
- An active System.
- The Server and Mobile Client must be on compatible versions.
 - 📄 **Note:** We recommend always keeping the Server and Mobile Client up to date to maintain compatibility.
- Mobile devices must be able to communicate with the system through one of the following options:
 - Through the LAN as a Local User.
 - Through the WAN/Internet as a Local User with the appropriate firewall settings or port forwarding.
 - Through the cloud connection as a cloud user.

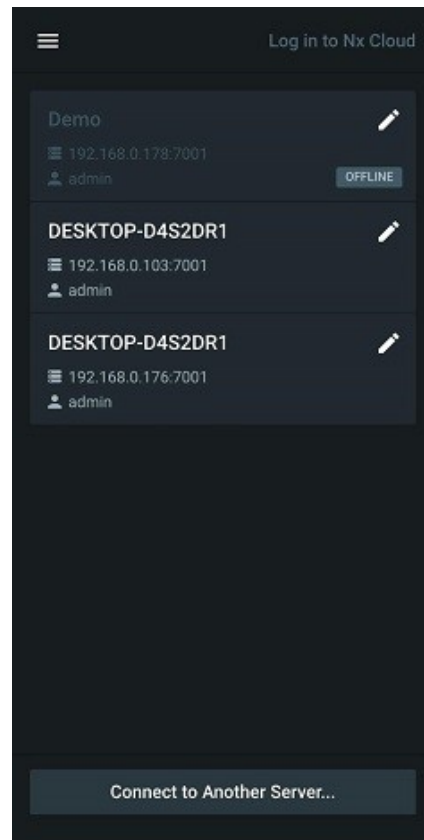
Connecting to Systems

The Nx Witness Mobile Client can connect to both Local and Cloud Systems. You can connect to Local Systems that have been automatically discovered on the network or by manually inputting the Server information.

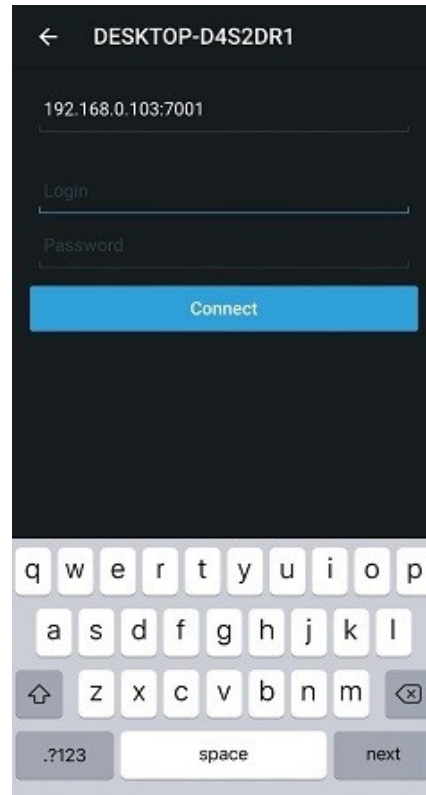
Connecting to a Local System

Automatically Discovered

1. Launch the Nx Witness Mobile Client app to access the Welcome Screen.
2. Tap on the System you want to connect to.

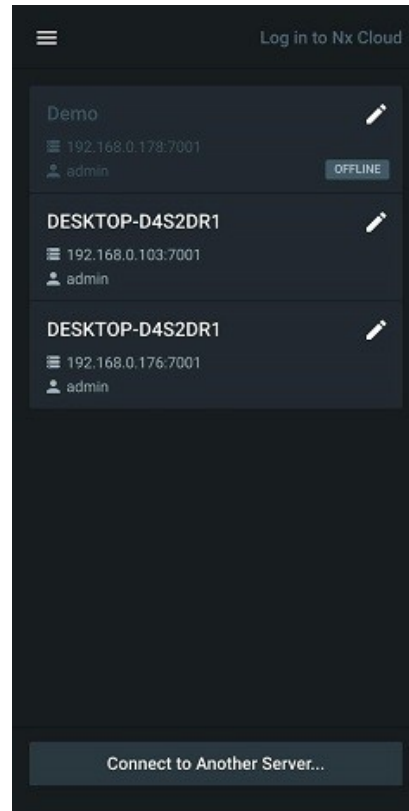


3. Enter your login credentials.
The Server information will be prefilled.
4. Tap on **Connect** to log in.

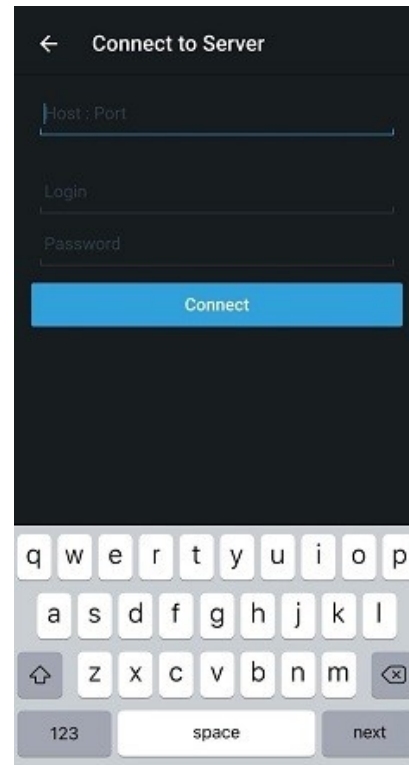


Manual Connection

1. Launch the Nx Witness Mobile Client app to access the Welcome Screen.
2. Tap on **Connect to Server / Connect to Another Server.**

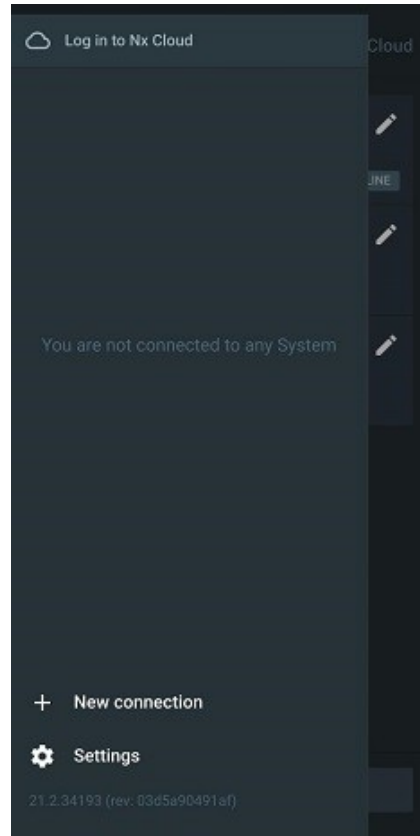


3. Enter the Server's information and your login credentials.
4. Tap on **Connect** to log in.

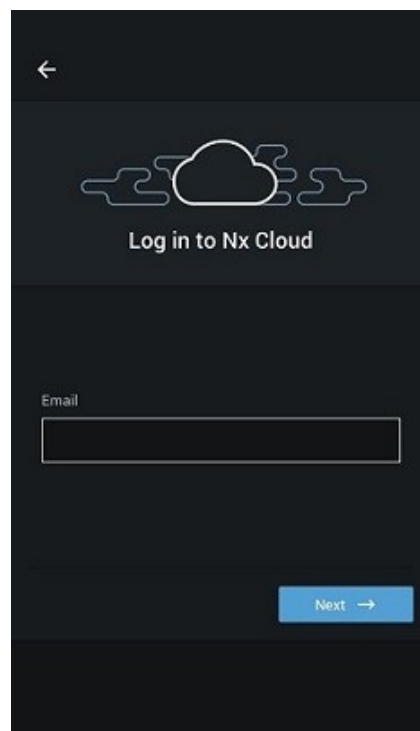


Connecting to a Cloud System

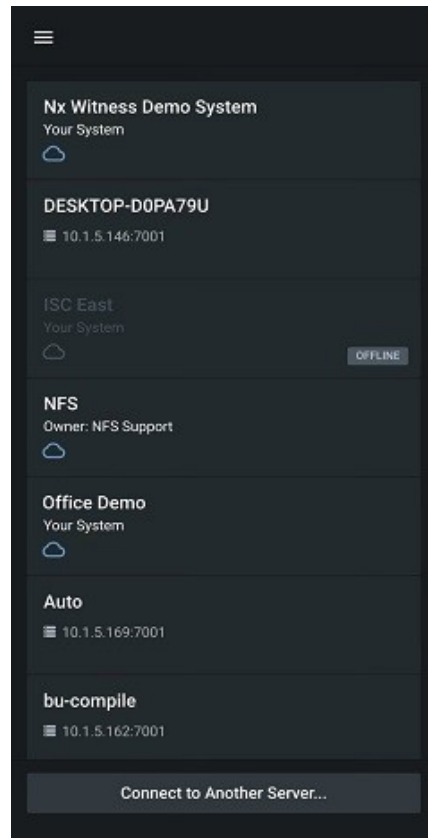
1. Launch the Nx Witness Mobile Client app to access the Welcome Screen.
2. Open the **Main Menu** to access the side panel.



3. Tap on **Log in to Cloud** and enter your Cloud login credentials.

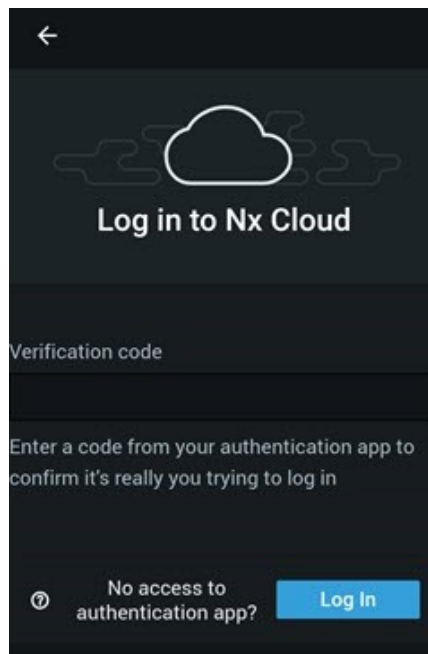


4. You will see the Welcome Screen. Tap on the System you want to connect to.




5. You will be prompted for a Two-Factor Authentication (2FA) verification code if the selected System requires 2FA for Cloud users.

A previously generated backup code can also be used by selecting **No access to authentication app?**



Server Certificate Validation

Nx Witness Server certificate validation occurs on the communication between Nx Witness Server, Nx Witness Clients (Desktop Client and Mobile Client), and Nx Cloud to enhance the security of Nx Witness by ensuring you are connecting to a trusted location. While the Client connects to the System, the System will provide all servers' public keys to the Client for validation. No matter which level is configured, there will be no warning message displayed at all when you connect to the System with a valid (public) certificate and matching hostname.

 **Note:** A valid certificate must be issued by a public Certification Authority (CA) and contains the completed information of the certificate chain. A public certificate without a certificate chain will be considered invalid in Nx Witness.

For other types of certificates, the behavior will depend on the Client's validation level.

Validation Levels

See [Client Configuration](#) ²² to learn how to change the validation level in the Mobile Client. The Server certificate validation level can also be modified in the Desktop Client (see the Desktop Client User Manual for more details).

- **Disabled** – The Client will skip the validation process and connect to the System directly. The user will not see a warning message. However, it is still NOT recommended to turn the validation off since certificate validation is recommended as a part of the security hardening process of any System.
- **Recommended** (default) – It allows the user to connect to the System with any certificate, but it may require the user's confirmation. You may still see the warning message in the following situations:
 - *Connected to an UNKNOWN System* – When a Client attempts to connect to a new System for the first time, that means the Client has no information about the servers' certificates before. When the System provides the certificate(s) that is custom/self-signed, or public certificate without chain information, a "Connecting to Server for the first time?" prompt may appear stating that the SSL certificate could not be verified automatically. Once the Client approves this connection, the certificate will be stored at the Client's end. It is expected that no warning message will pop up again for any further connections until the certificate expires/changes.
 - *Connected to a KNOWN System* – When a user attempts to use the Client to connect a known System but whose certificate(s) cannot be verified successfully (for example, mismatched with the Client's pinned certificate, expired certificate, etc.), the Client will display the warning message: "Cannot verify the identity of Server". The user will be asked to take further action and check the certificate's problems. The user can check click *Connect* to proceed if the user would like to connect to the Server. This message will be seen every time the user attempts to connect to the System until the issue with the certificate has been fixed.

- **Strict** – With this mode, the servers that use the default self-signed certificates will also be rejected by the Client. It forces the user to connect to Servers with only a valid (public) certificate and correct hostname. The user will see the warning message below when they attempt to connect to the System with an invalid certificate or mismatched hostname.

Checking the Certificate's Details

You can use the Desktop Client or Web Admin to check the Server's SSL certificate validity and information (see the Desktop Client User Manual for more details).

Renewing the Certificate

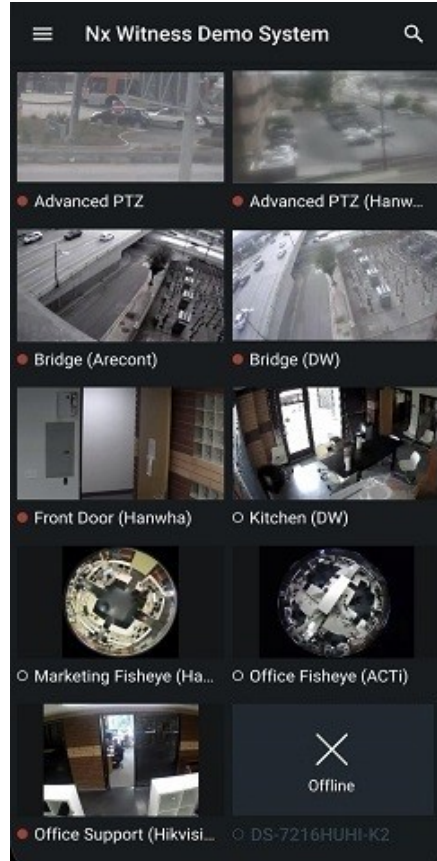
To renew an expired certificate do one of the following:

- For self-signed certificates from the VMS, restart the Server to renew its certificate and try again.
- For public certificates or other self-signed certificates, contact your VMS administrator to renew the Server's certificate

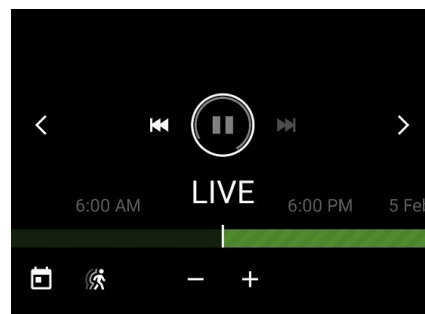
Viewing Cameras

The *All Cameras* layout on the Nx Witness Mobile Client is the default screen after connecting to a Server and contains all the cameras on the System.

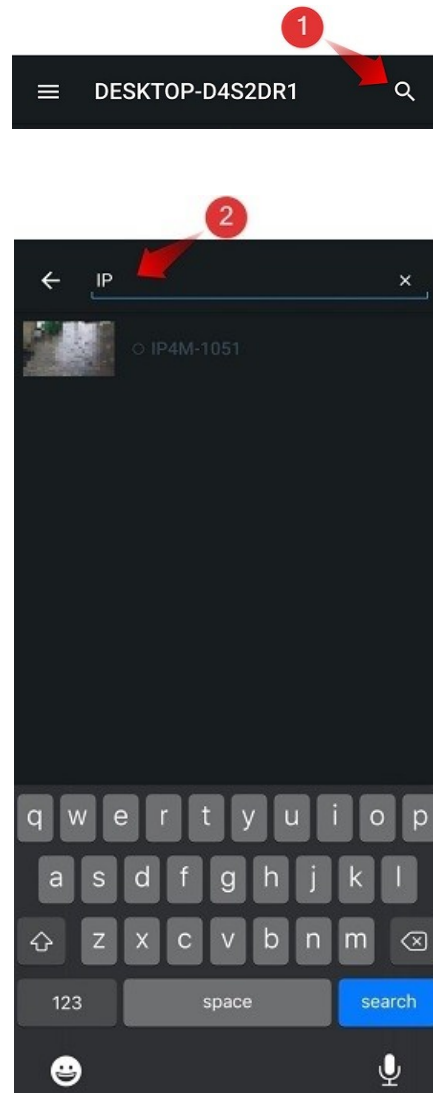
1. Tap on any camera to open its stream.



2. Tap on the < or > icons to switch between cameras.

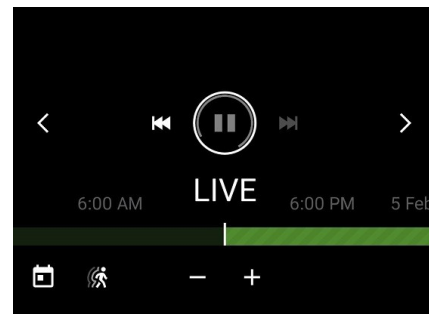


3. If you are looking for a specific camera, use the search field at the top to narrow down the selection that is shown on the primary layout.



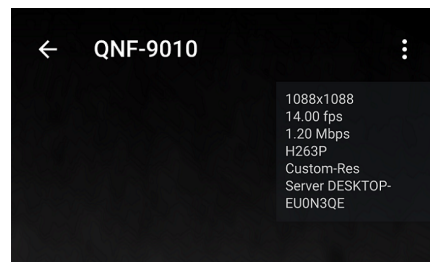
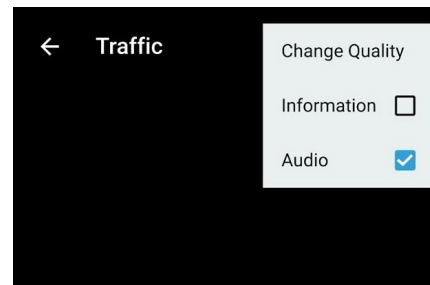
Archive

1. Tap on a camera to open its live stream.
2. If the camera has an archive you can do either of the following:
 - Tap and drag your finger across the timeline to your desired position.
 - Tap the calendar icon and select a date for the archive rewind to.
3. Use the playback controls to play/pause or jump one hour backwards or forwards.
4. Click **LIVE** at the bottom of the screen to return to the live stream.




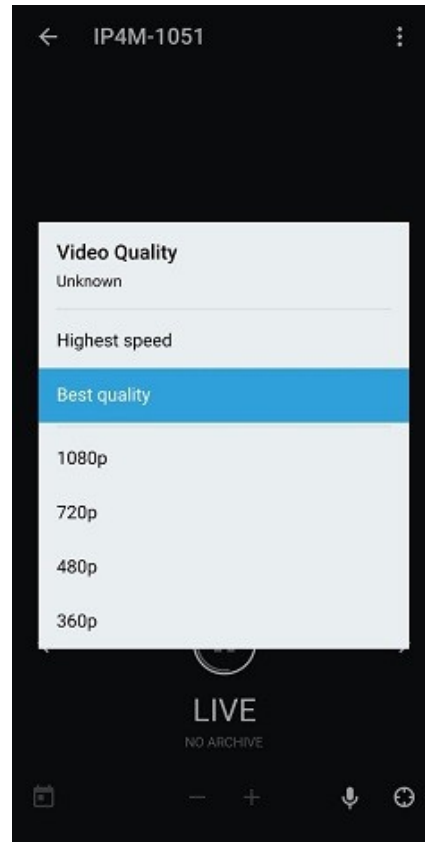
Camera Options

1. Tap on a camera to open its live stream.
2. Tap on the vertical dots at the top right to access the following options:
 - *Change Quality* – Choose between highest speed, best quality, or a custom resolution.
 - *Information* – Enables/disables displaying the camera's resolution, FPS, bandwidth, encoding, stream quality, and parent Server.
 - *Audio* – Enables/disables hearing audio from the camera.



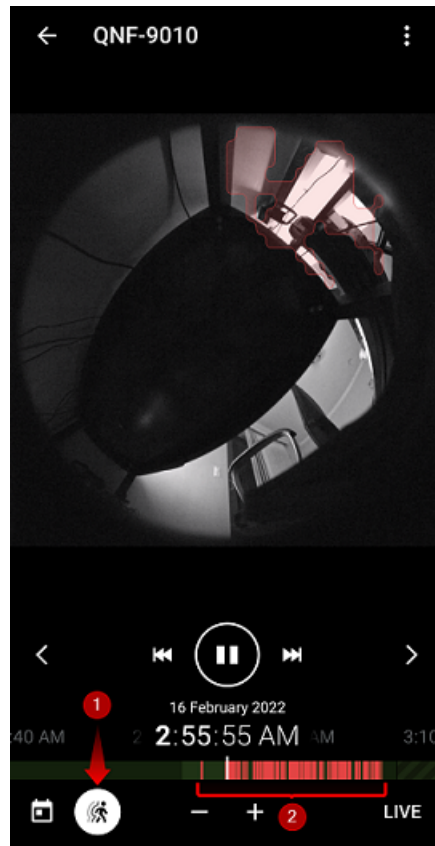
3. To change the quality of the stream, tap on **Change Quality** and select from the list of available options (varies between cameras).

 **Note:** ARM-based servers prohibit the use of transcoding and not all options mentioned above are available.



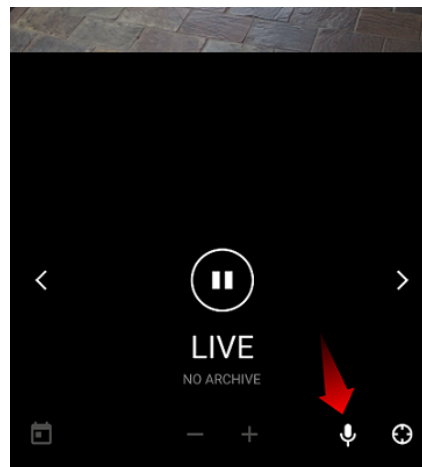
Motion Search

Cameras with motion recording segments in the archive will display a motion icon. Tap the motion icon to see motion data in the archive.



2-way Audio

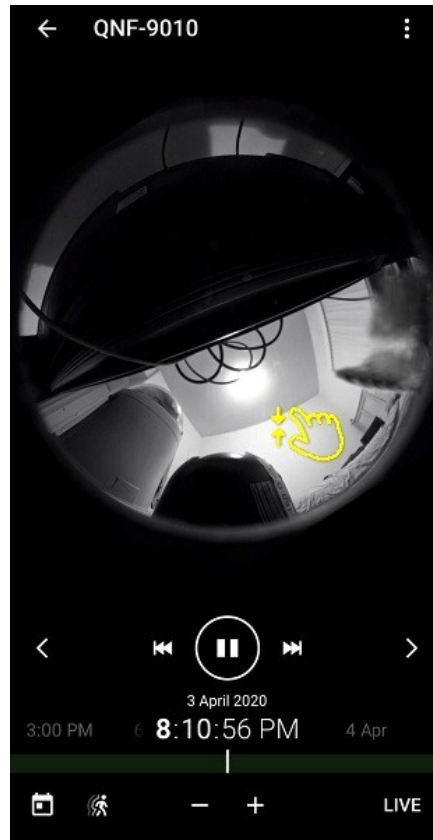
Supported 2-way audio cameras will display a microphone icon. Tap and hold the microphone icon to initiate 2-way audio communication.



Fisheye Dewarping

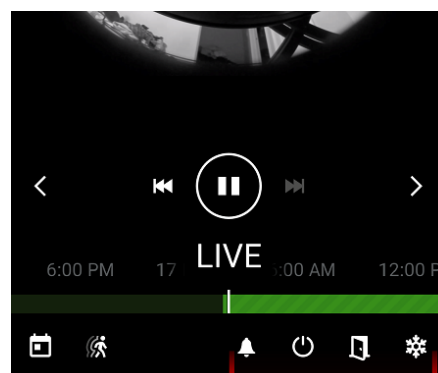
Fisheye cameras can be dewarped via the Nx Witness Mobile Client, but this setting must be enabled via the Desktop Client.

Open the desired camera and use your finger to move around or pinch to zoom.



Soft Triggers

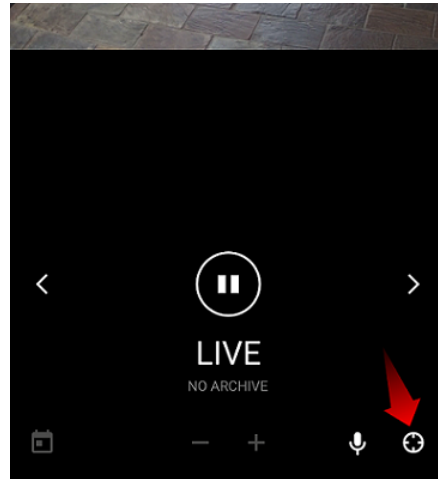
Soft Triggers must be created on the Nx Witness Desktop Client but can be activated on enabled cameras by clicking on the appropriate icon. You can configure each Soft Trigger to have a different icon.



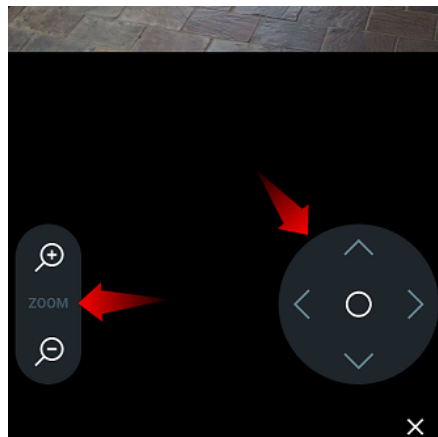
PTZ

Supported PTZ cameras will display a PTZ icon on the bottom right of their view.

1. Tap the PTZ icon to see the PTZ controls.

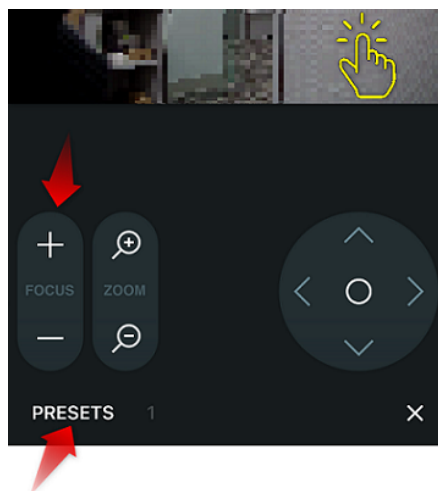


2. Tap on + / - to zoom and tap on the arrows to change direction (or hold and drag the center dot). The dot can also be held and dragged for continuous movement.



3. Cameras with Advanced PTZ functionality may also present additional controls:

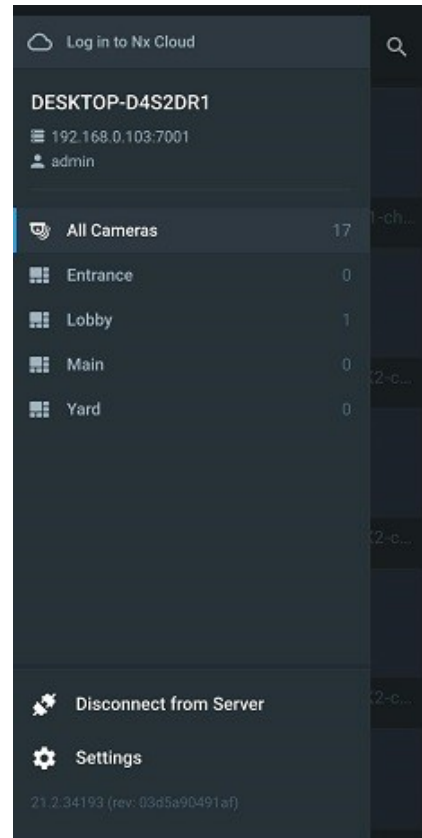
- Tap + / - to adjust camera focus.
- Tap on **PRESETS** to see a list of available PTZ presets. Select a PTZ preset to execute it.
- Tap and hold anywhere on the camera stream to re-center the PTZ camera to that location.



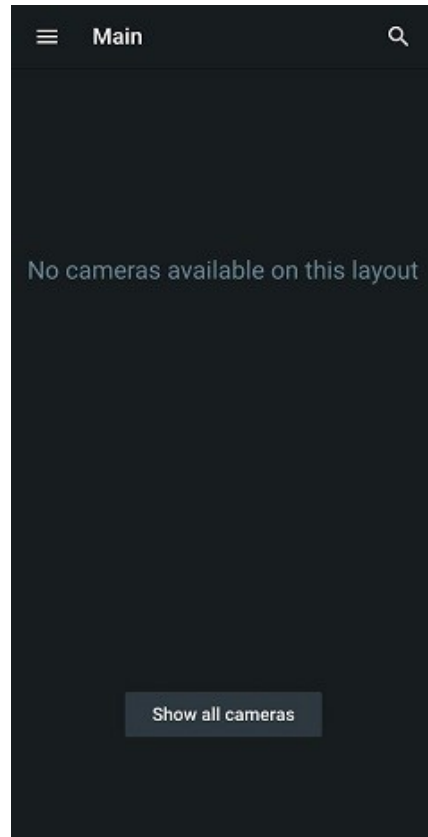
Viewing Layouts

Only existing layouts can be accessed on the Nx Witness Mobile Client as new layouts must be created on the Nx Witness Desktop Client. I/O module controls are not available in the Mobile Client, but you can configure a Soft Trigger and set I/O output as the action.

1. Open the **Main Menu** to open the side panel and see all accessible layouts.




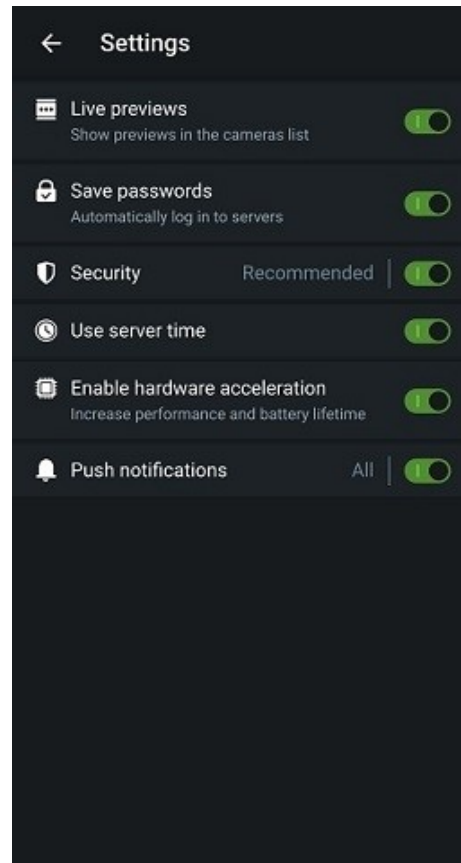
2. Tap on a layout to view it. If a layout has no cameras, you can tap **Show all cameras** to return to the *All Cameras* layout.




Client Configuration

The Nx Witness Mobile Client has the following settings which can be modified from **Main Menu > Settings**:

- **Live Previews** – Displays frequently updated previews for cameras on the layout. Only keyframes from the secondary stream of cameras on the layout are played, so the refresh time depends on the secondary stream and keyframes that camera sends in the secondary stream. If disabled, previews update only once every 5 minutes.
 - **Save passwords** – Log in to different Systems without re-entering your credentials.
 - **Security** – Server SSL certificate verification options:
 - Recommended (default) - Allows you to connect to Nx Witness Servers with valid self-signed and public certificates.
 - Strict - Allows you to connect to Nx Witness Servers with only valid public certificates.
 - Disabled - The certificate will not be checked.
-  **Note:** After updating the Nx Witness Mobile Client to a new version and connecting to a Server, a prompt may appear stating that the SSL certificate could not be verified. The prompt should not appear the next time you connect to the same Server as long as its certificate remains valid.
- **Use server time** – Use Server time instead of Client time.



- *Enable hardware acceleration* – (iOS only) Video streams that use non-standard resolutions cannot be displayed on iOS devices with hardware acceleration enabled. Disable this option to use software decoding to display video streams that use non-standard resolutions.
- *Push notifications* – Receive push notifications from events on either *All Systems* or *Selected Systems*. Tap on the text to the left of the switch to configure this setting.

 **Note:** Push notifications are only available on cloud systems while logged in as a cloud user.



Still need help? Visit us at <http://support.networkoptix.com>