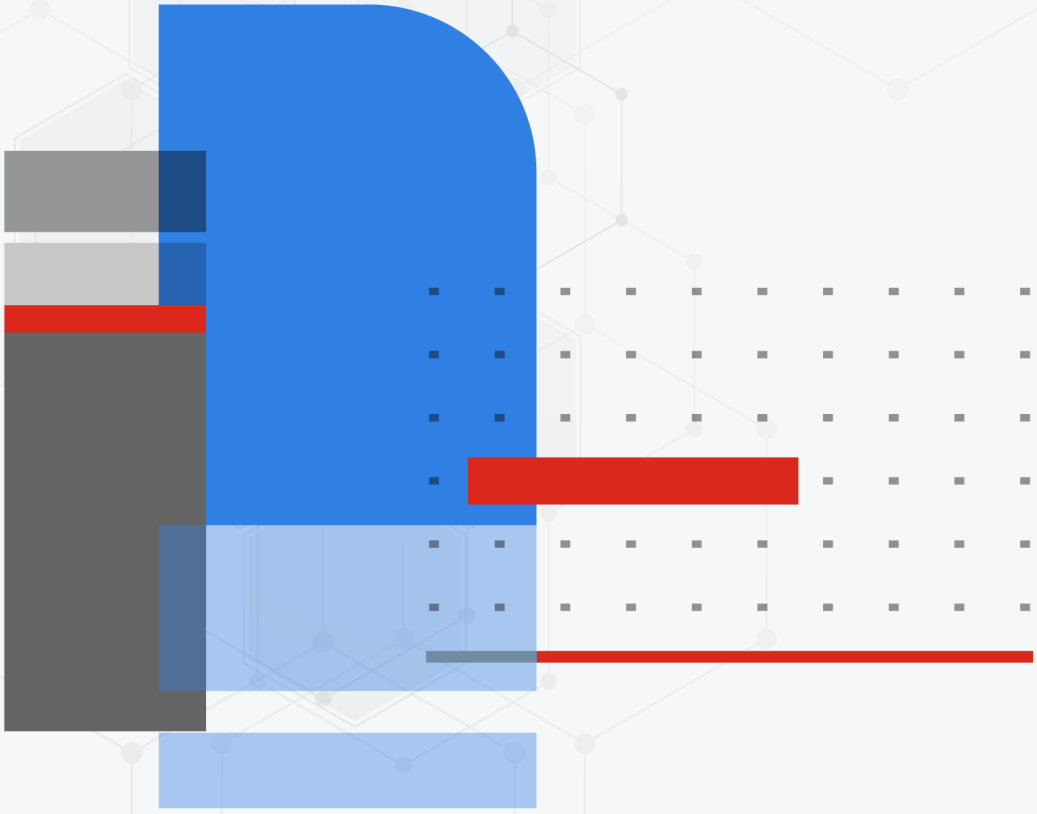
Portal Guide

FortiCamera Cloud 24.2.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 09, 2024
FortiCamera Cloud 24.2.0 Portal Guide
00-242-1029978-20240509

TABLE OF CONTENTS

Change log

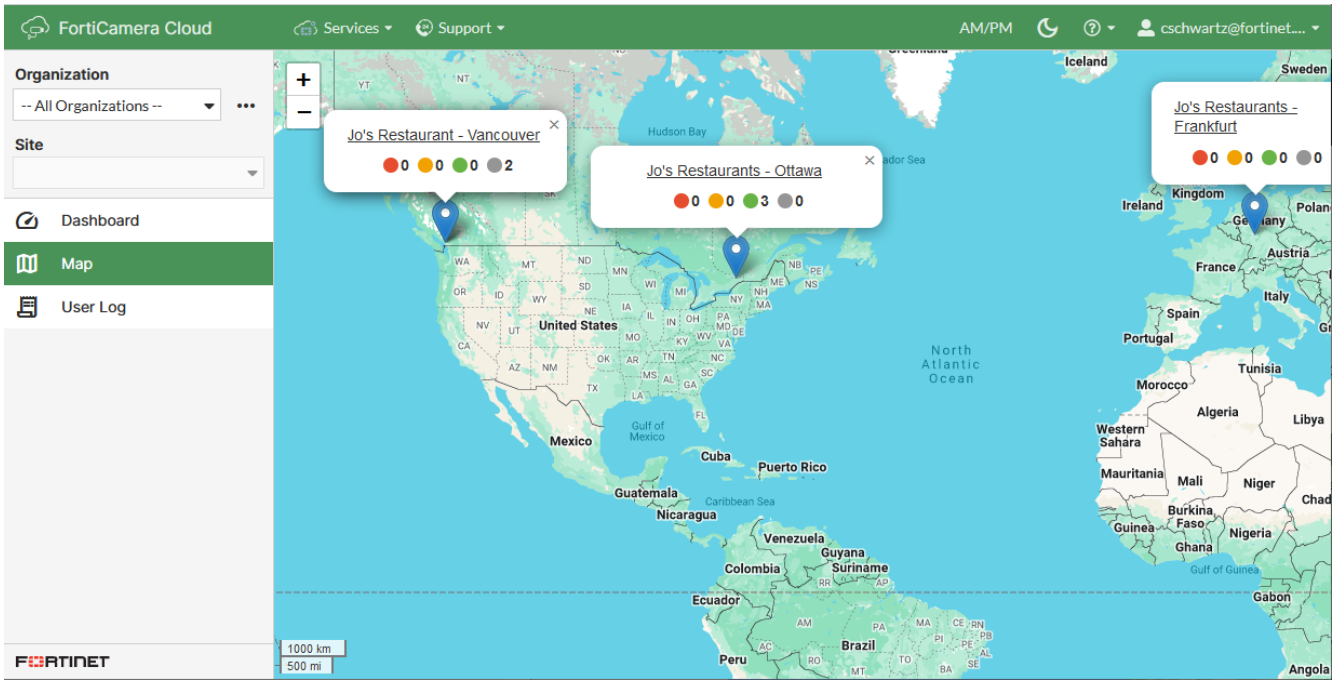
The following is a list of documentation changes. For a list of software changes, see the Release Notes.

Date	Change Description
2024-05-07	Initial release of FortiCamera Cloud 24.2.0 Portal Guide.

Introduction

FortiCamera Cloud is a cloud-based Video Surveillance as a Service (VSaaS) platform. FortiCamera Cloud provides management and analytical capabilities across your entire FortiCamera deployment, and you can use it to deploy, set up, and view video streams from your FortiCamera devices. Permissions can be fine-tuned with organization-level and site-level privileges.

Hybrid deployment is also supported for flexible combinations and extended storage with FortiRecorder.



Requirements

The following are required to use FortiCamera Cloud:

Requirement	Description
FortiCloud account	You can log in with either a FortiCloud or FortiCare account (email address or IAM account type).
FortiCamera cameras (registered)	You must register all FortiCamera devices with FortiCare in order to claim the cameras within FortiCamera Cloud. For details, see Registering FortiCamera devices in FortiCare on page 8.

Requirement	Description
Licenses	Purchase FortiCamera Cloud service entitlement licenses from Fortinet and register them in the same FortiCare account as the cameras. There is a trial period of 7 days. If you want to connect cameras that are not cloud native (in a hybrid deployment, through FortiRecorder), then you must also buy and install a license for these cameras. For details, see the FortiRecorder Administration Guide.
Internet access	Your computers and cameras must have Internet access to communicate with FortiCamera Cloud. If you have a firewall between them, see also Appendix A: Port numbers on page 46.
Browser	For a list of currently supported web browsers, see the FortiCamera Cloud Release Notes.

Getting started

Before you log into FortiCamera Cloud, physically connect FortiCamera cameras and then register them in FortiCare.

Hybrid versus cloud native deployment

If you have a new deployment, you might only use cloud native cameras (for example, FortiCamera MC51-C and FortiCamera CD55-C) with FortiCamera Cloud.

Hybrid deployment, however, is also supported. In this deployment pattern, you can have a mix of cameras: some are cloud native, and others are not. Cameras that are not cloud native are connected indirectly, via a FortiRecorder. On FortiRecorder, you enable *Managed in cloud mode* for each camera that you want to connect to FortiCamera Cloud. Then you can view video from *all* cameras—both cloud native and others—together in FortiCamera Cloud. Only local network settings, local storage, and local settings are configured on FortiRecorder for the cameras that are not cloud native.

Advantages of hybrid deployment include:

- Simple migration from private network to cloud-based deployment
- Extended storage and retention capabilities beyond what cloud native FortiCamera models currently support

To use local network cameras with FortiCamera Cloud, upload a license to the FortiRecorder and then enable *Managed in cloud mode*. For details, see the *FortiRecorder Administration Guide*.

For example, the following SKU is a stackable license for on-site camera models, used in a hybrid deployment with FortiRecorder. To use it, log in to:

https://support.fortinet.com/

as the owner, and apply it to the FortiRecorder serial number.

SKU	Contents
FRC-CLM-20	FortiRecorder Cloud Mode for camera license Perpetual license for 20 cameras Electronic license certificate

Registering FortiCamera devices in FortiCare

After an initial 7-day grace period, all cameras require a subscription license to use the FortiCamera Cloud service.

For example, the account owner can order a license for any number of cameras ("seats"), with a subscription for 1, 3, or 5 years, like the following:

SKU	Contents
FC1-10-FCCLD-518-02-DD	FortiCamera Cloud plus FortiCare Premium support Subscription license certificate

Licenses can be used across multiple organizations if they belong to the same owner.

1. Physically connect your FortiCamera devices. For details, see the Quick Start Guide for your model.
2. Go to:
   https://support.fortinet.com
   and log in as the owner.

For simplicity, this document has instructions performed by the default *Owner* account. Owners have full privileges for the assets (cameras and licenses) registered to that organization. Each organization can have assets from one FortiCare account, and has one owner.

Some parts of FortiCamera Cloud are only available to the owner, or users to whom the owner has granted permissions.

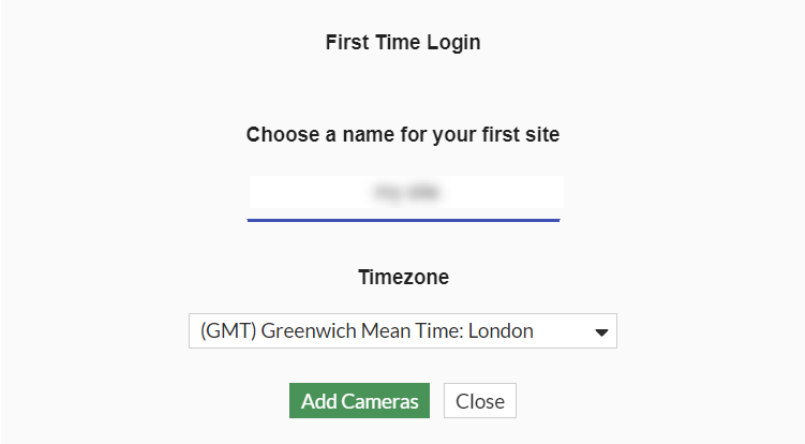
3. Register your devices. For details, see FortiCloud Asset Management documentation.
4. Register the subscription license in the same account.
   - **To renew an existing subscription:** Register a new contract with the same number of cameras.
   - **To add more camera subscriptions:** Contact your Fortinet partner or Fortinet customer service. Request a co-term quote. Co-term licensing aligns all of your subscription expiry dates.
5. If this is the first time that you are logging into FortiCamera Cloud, continue with First time login to FortiCamera Cloud on page 9. Otherwise continue with Claiming cameras on page 11.

First time login to FortiCamera Cloud

1. Go to:
   https://forticamera.forticloud.com/
   Alternatively, go to support.forticloud.com. After you log in, in the *Services* dropdown list at the top, select FortiCamera Cloud.
2. Click *Login* and enter your user name and password.
   The *First Time Login* page appears.
3. Enter a name for your first organization, select the geographic *Region* where the organization will be deployed, and click *Add Organization*.

Select the region carefully. The region cannot be changed after the organization has been created. It determines the location of the datacenter that hosts cloud services for the organization.

4. Enter a name for your organization's first deployment site, and select its *Timezone*.
5. If you registered cameras in FortiCare, click *Add Cameras*. Otherwise click *Close*. (You can register and claim cameras later.)



6. Select the cameras that you want to claim for your organization.
   For details, see Claiming cameras on page 11.

Organizations and sites

In FortiCamera Cloud, cameras are part of deployment sites, and sites are owned by an organization. This groups your cameras and allows you to use them according to their location. Organizations claim cameras to make them part of their device inventory.

Configuring organizations

Organizations determine:

- Region where the cloud service for this site is hosted.
- Inventory of the cameras that are deployed into sites.
- User permissions within that organization.

One user can belong to multiple organizations. can hold multiple sites.

Adding an organization

1. Go to *Organization* > *Add*.
2. In the *Organization Name* field, enter a unique name.
3. From the *Region* dropdown list, select either:
   - *Global*
   - *United States*
   - *Canada*
   - *Europe*.

Region should be selected carefully. The region cannot be changed after the organization has been created.It determines the location of the datacenter that hosts cloud services for the organization.

4. Click *Save*.
   Your organization is now listed in the *Organization* dropdown list.

Renaming an organization

1. From the *Organization* dropdown list, select the organization you want to rename .
2. Go to *Organization* > *Rename*.
3. Enter a *New Organization Name*, and then click *Save*.

Claiming cameras

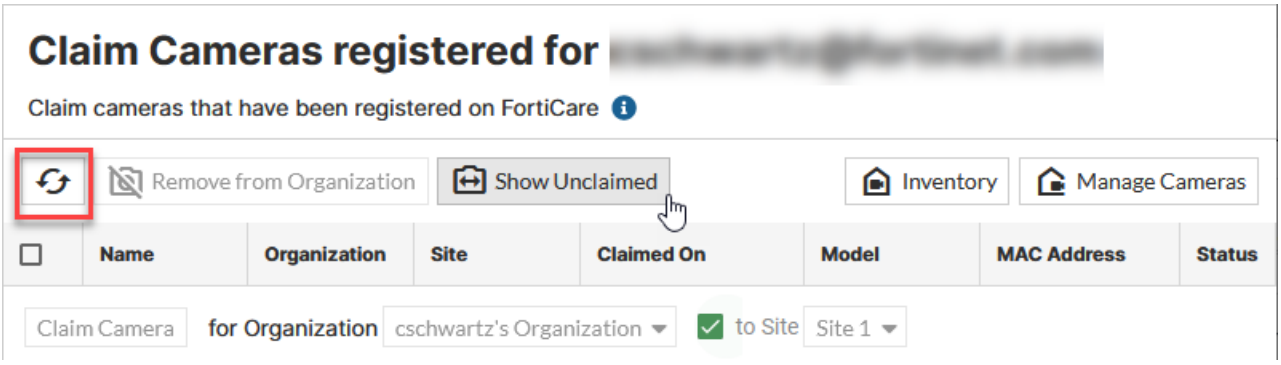
If you are the owner of an organization, and if FortiCamera devices are registered to your FortiCare account, you can assign the cameras to the organization. Claiming cameras into an organization's inventory makes them available for other users in the organization who do not own the camera.

See also Registering FortiCamera devices in FortiCare on page 8.

1. If required, change the *Video encryption* setting for the organization.

Video encryption settings cannot be changed after the organization claims cameras.

2. From the *Organization* dropdown list, select the organization that will claim the registered cameras.
3. Go to *Organization* > *Claim Camera*.
   The *Claim Cameras* screen appears, showing a list of all cameras registered to your FortiCare account.
   If you do not see your registered cameras, click *Refresh*.



Cameras can only be claimed if they are not already claimed by another organization.
The *Status* column indicates whether the camera is visible to FortiCamera Cloud. This can help you to find the cameras that are new.

4. Select the checkboxes of the cameras that you want to claim.

5. At the bottom of the list, select which *Organization* and optionally which *Site* to assign the cameras to, and then click *Claim Camera*.

Organizing the inventory

If cameras have been claimed by your organization, you can group them according to site. Only those cameras that have been registered to your FortiCare account, and have been claimed by an organization, appear in the organization's inventory.

1. From the *Organization* dropdown list, select the organization whose inventory you want to manage.
2. Go to *Organization* > *Inventory*.
   Alternatively, if you are on the *Claim Cameras* screen, click *Inventory*.
   The inventory screen appears. It displays a list of all cameras claimed by the organization, and which sites the cameras belong to (if any).
3. Select the checkboxes of cameras that you want to add to the site.
4. At the bottom of the list, select which *Site* to assign the cameras to, and then click *Add Camera*.
   You can also remove cameras from a site and reassign them to a new site.

Organization settings

You can view general organization settings, and edit some of them such as your organization's users (see Configuring user and administrator accounts on page 15). The *Region*, however, cannot be changed.

To change video encryption

1. Go to *Organization* > *Setting*.
2. Click the *General* tab.
3. If you have not yet claimed any cameras, then you can enable or disable *Video encryption*.
   This only affects encryption at rest (files stored on the camera's disk). It does not change encryption in transport (video streams over the Internet), which are always encrypted.

Configuring sites

Multiple deployment sites can belong to an organization, with cameras potentially spread across the geographic locations of those sites.

Some features depend on the physical location of the site:

- Timezones for cameras vary by the site's location.
- Maps can show each site's location.

Adding a site

You can also edit or delete a site.

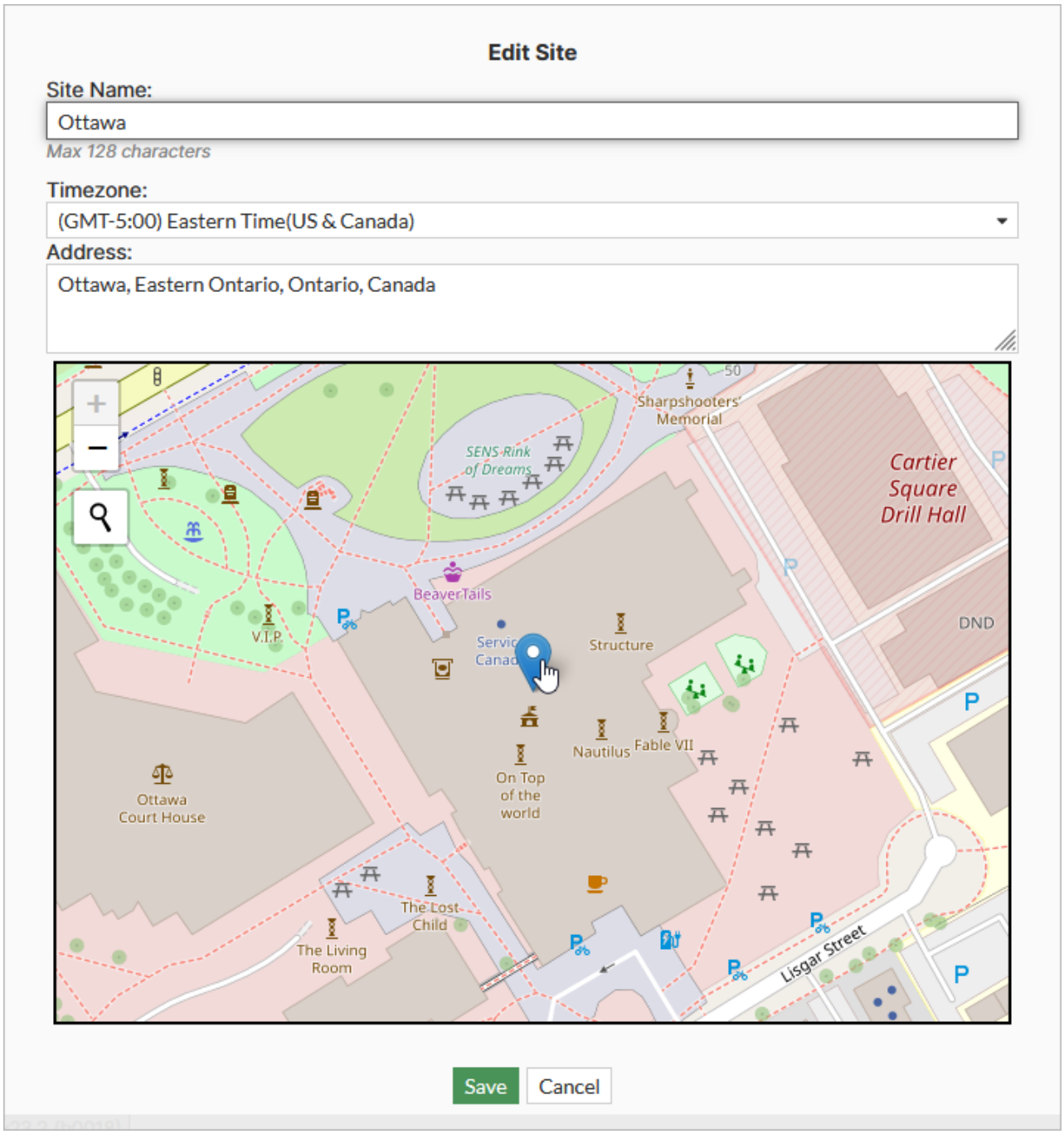
1. From the *Organization* dropdown list, select the organization that the new site belongs to.
2. Go to *Site* > *Add*.
   For new organizations, this is the only available option.

3. Configure the following settings:

Setting	Description
Site Name	Enter a unique name for the site.
Address	Enter the street address. If you are not certain of the site's exact address, enter as much as you know. You can search for the complete address in the next step.
Timezone	Enter the timezone at the site's physical location. Cameras deployed to this site will use the site's timezone for on-screen display.

4. In the global map panel, click the-search icon. Enter or paste the *Address* that you entered above, and press *Enter*. The map geolocates your site's address, as marked on the map with a pin.

If the map's search results have multiple addresses, you might need to select the correct address for your site. The *Address* field might be automatically updated to match it.



5. Click *Add*.

Site settings

For a site, you can view its settings and configure its users and their access-privileges.

To change site settings

1. Go to *Site* > *Setting*.
2. Click the *General* tab.

3. View the assigned *Timezone* of the site, which can be modified from the available dropdown menu.
4. Enable or disable *Firmware Auto-upgrade*.

   If automatic updates are enabled, when there is a new camera software upgrade available, FortiCamera Cloud automatically upgrades the site's cameras during the 3 hour window that starts at the *Selected Time*. If automatic camera upgrades are disabled, the dashboard will indicate a status of *Attention* when new software is available, but then you must update each camera manually. For details, see Firmware updates on page 31.

   Recordings are interrupted until the camera reboots.

5. Click *Save*.

To configure site users

1. Go to *Site* > *Setting*.
2. Click the *User* tab.

   If you want to view user-lists for each site, select the site from the dropdown list.
3. Click *Add* to create a new user profile, or select an existing user profile and click *Edit*.
4. Configure the same settings that are available when configuring a user at the organization level. For details, see Configuring user and administrator accounts on page 15.
5. Click *Save*.

The *User* tab in *Site* > *Setting* allows you to manage user accounts at one specific site. This is useful since it allows administrators that only have access to site user privileges to manage the users for their site.

Configuring user and administrator accounts

You can manage user accounts for both a whole organization and its individual sites.

1. Go to *Organization* > *Setting*.

   Alternatively, go to *Site* > *Setting* and click the *User* tab.
2. Click *Add* to create a new user, or select an existing user and click *Edit*.
3. Configure the following settings:

GUI item	Description
Name	Enter the name of the user (spaces permitted).
Email	Enter the email address of the user.
Scope	An organization or site. Click *Add Organization Permission* or *Add Site Permission* (depending on whether the row is for an organization or individual site) to enable the *Permission* column for it. All sites belonging to the organization can grant privileges to the user.

4. For rows where you clicked a button to add permissions, configure the following settings:

GUI item	Description
Permission	The list of available privileges varies by the user's scope: an organization, or a site. For the scope of an organization, select either: • *Organization Settings - General*: Grant the organization user the ability to create new sites and site users. • *Organization Settings - User*: Grant the organization user access to their specific privileges and to create new users within the organization. For the scope of a site, select either: • *Camera Video*: Grant camera video privileges to this user. For details, see Playing video from cameras on page 24. If this privilege is granted, see *Target* to select which cameras are permitted. • *Camera Settings*: Grant camera settings privileges to this user. For details, see Camera settings on page 26. If this privilege is granted, see *Target* to select which cameras are permitted. • *Site Settings - General*: Grant the site user the ability to access a site (for example, access a site's dashboard). • *Site Settings - User*: Grant the site user the right to create users for the site.
Target	Define which of the site's cameras you want to permit the user to access. Select either: • *All*: All cameras belonging to the site. • *List*: Select this option and then in the dropdown that appears, click *Choose* to select specific cameras you want to permit to this user.
Level	Define the level of access you want to grant for of each of the user's privileges. For organization and site settings and camera settings privileges, select either of the following: • *Full*: Grant full read and write permissions. • *Read*: Grant only read permissions. For camera video privileges, select either: • *Export*: Grant ability to download video files. • *Playback*: Grant ability to playback video. • *Live*: Grant ability to view live video feed.  Add as many privileges as required. For example, you can grant export, playback, and/or live video access.
Action	Click *Delete* to remove a privilege.

5. Click *Save*.
6. Continue with Inviting users to join an organization on page 17.

Example: Site administrator role

In this example, we have configured a user who has:

- Access to the organization, Jo's Restaurants, but no permission to add sites or users at the organization level.
- In Ottawa, permission to live video, playback, and video exporting for all of its cameras.
- In Ottawa, permissions to change camera settings.
- No access to the Vancouver site.

The permissions define the role of a site administrator who can manage the site's users and cameras.

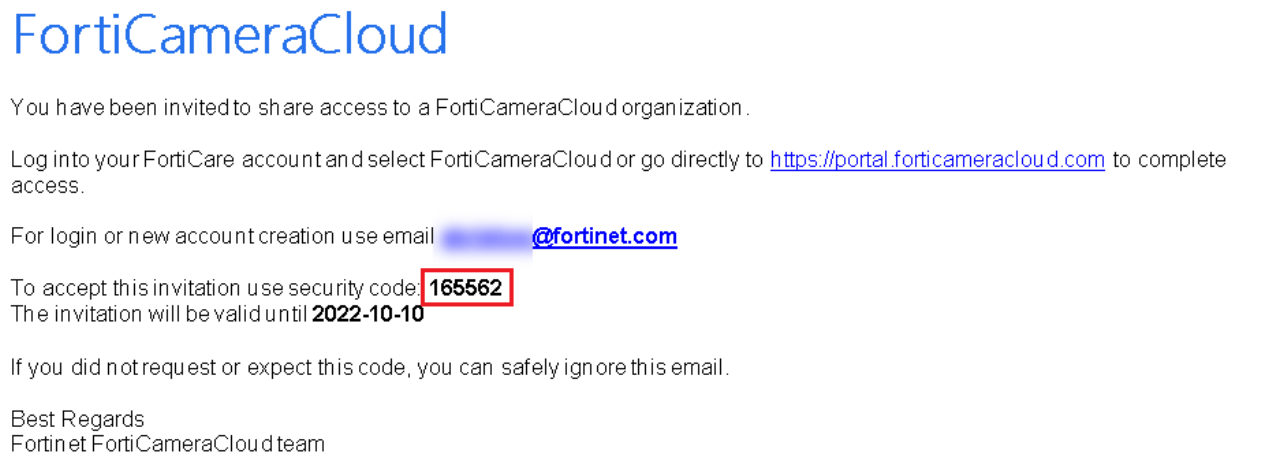
Scope	Permission	Target	Level
Jo's Restaurants (organization)			
Ottawa (site)	Camera Video	All	Export
	Camera Settings	All	Full
	Site Settings -- General		Full
	Site Settings -- User		Full
Vancouver (site)	None		

Inviting users to join an organization

Once you have created a user account (see Configuring user and administrator accounts on page 15), you can invite that person to join an organization.

1. From the *Organization* dropdown list, select the name of the organization that you want the user to join.
2. Go to *Organization* > *Setting*.
3. Click the *User* tab.
4. Select the user you want to invite.
5. Click *Share* and then click *Confirm*. (If you change your mind, or accidentally invite an incorrect email address, you can click *Revoke*.)

   On the *User* tab, the user now has a status of *INVITED*. An invitation is sent to the user's email address. It includes a verification code ("security code").


FortiCameraCloud

You have been invited to share access to a FortiCameraCloud organization.

Log into your FortiCare account and select FortiCameraCloud or go directly to https://portal.forticameracloud.com to complete access.

For login or new account creation use email [redacted]@fortinet.com

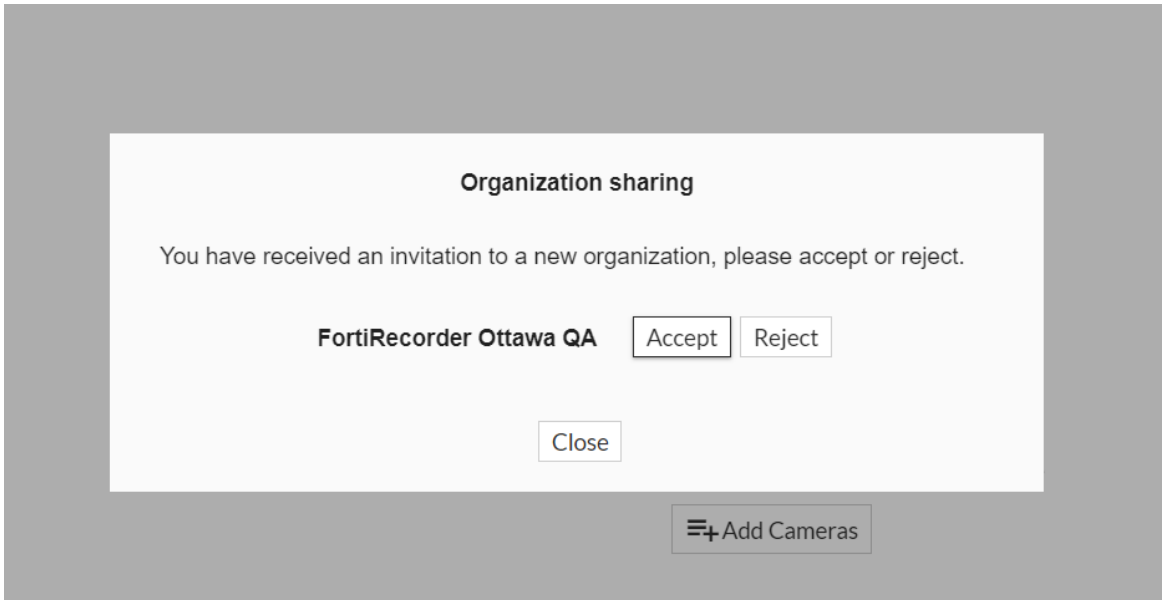
To accept this invitation use security code: **165562**
The invitation will be valid until **2022-10-10**

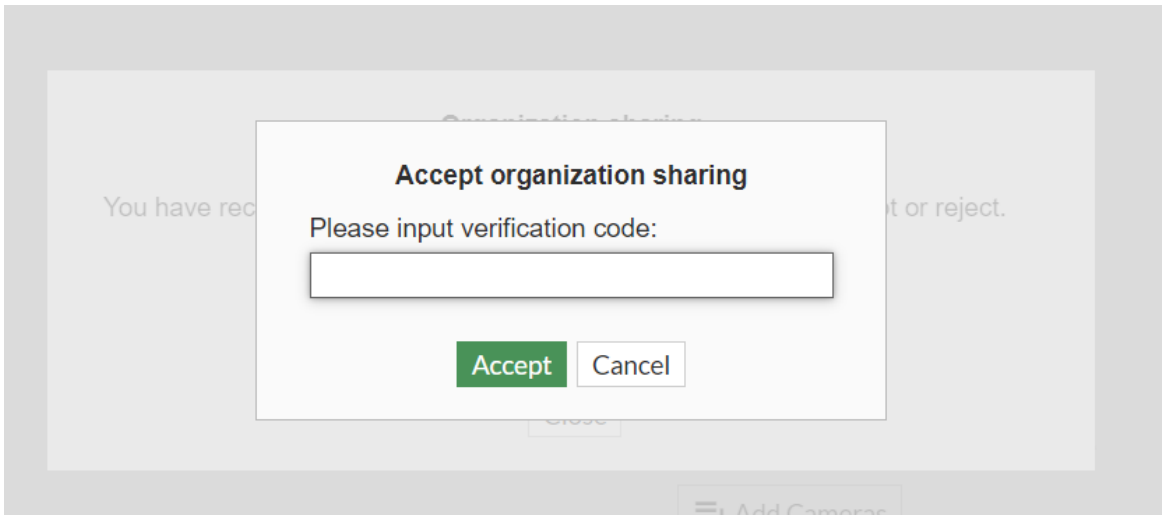
If you did not request or expect this code, you can safely ignore this email.

Best Regards
Fortinet FortiCameraCloud team

If the user does not receive the email, and you need to help them, then on the *User* tab, you can hover your mouse cursor over the *Verification Code* column to view the user's verification code.

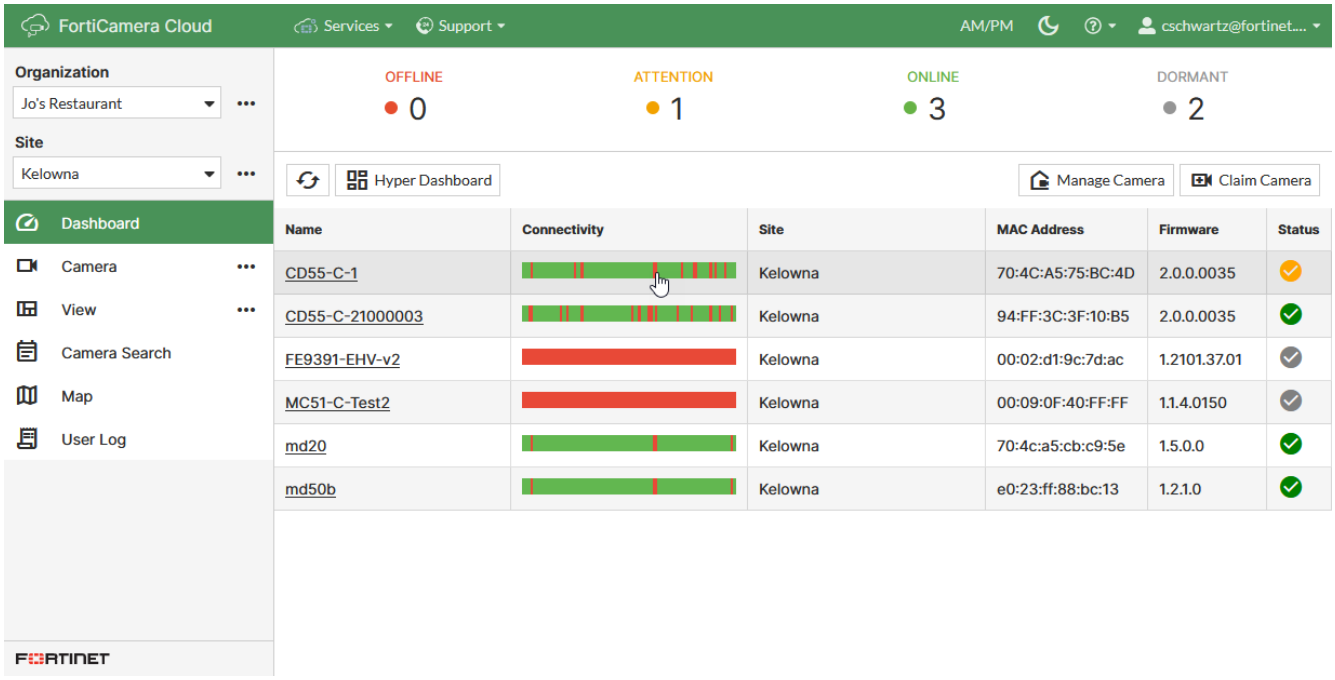
6. The user must log into the FortiCamera Cloud portal, click *Accept*, and then enter the verification code before it expires.




Accept organization sharing
Please input verification code:
Accept
Cancel

Dashboard

When you log into FortiCamera Cloud, initially it displays the first item in the navigation menu: *Dashboard*. The dashboard displays a list of cameras that belong to the currently selected organization and deployment site. If you are logged in as the owner, or have been invited to multiple organizations, you can also click *Hyper Dashboard* to view a list of all cameras, in all of your organizations(see Hyper Dashboard on page 22).



The summary at the top of the dashboard indicates the number of cameras that have each *Status* type:

- ***Offline***: Click to list the cameras that are not connected to FortiCamera Cloud, for 6 days or less.
- ***Attention***: Click to list the cameras that require attention due to an available firmware upgrade, license issues, or configuration synchronization.
- ***Online***: Click to list the cameras that are connected.
- ***Dormant***: Click to list the cameras that have been offline for 7 days or more. Dormant and offline categories are separate so that you can distinguish temporary network interruptions from problems that require more urgent attention.

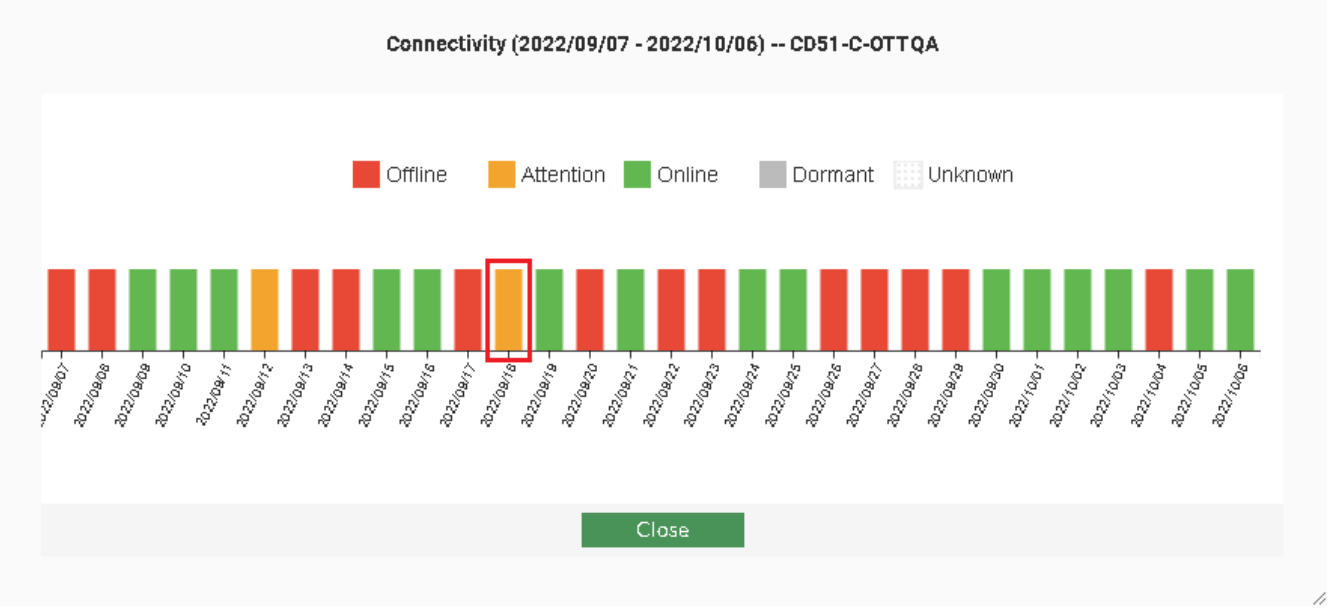
For each camera on the dashboard, there are the following columns:

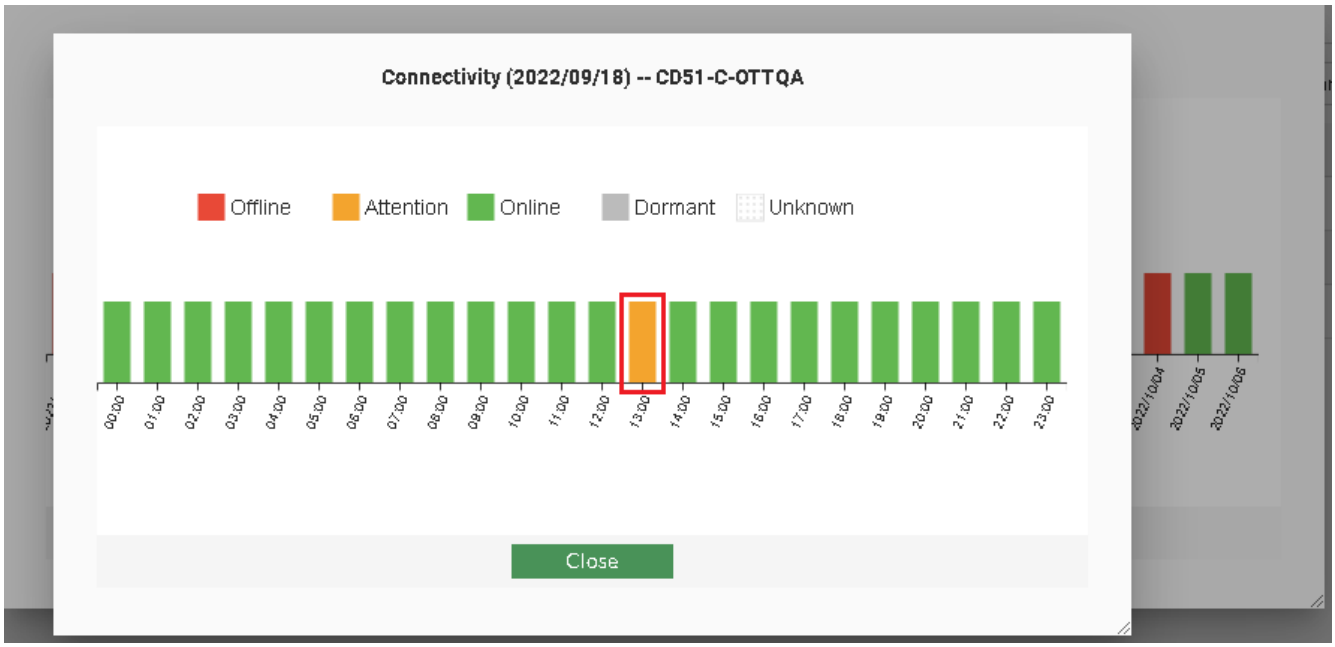
Column	Description
Name	The name of the camera. Click it to view the live video feed from the camera. See Playing video from cameras on page 24.
Connectivity	Displays the network connectivity history as a color-coded timeline of the previous month. To drill down and view details by day, hour, or minute, click that part of the bar.

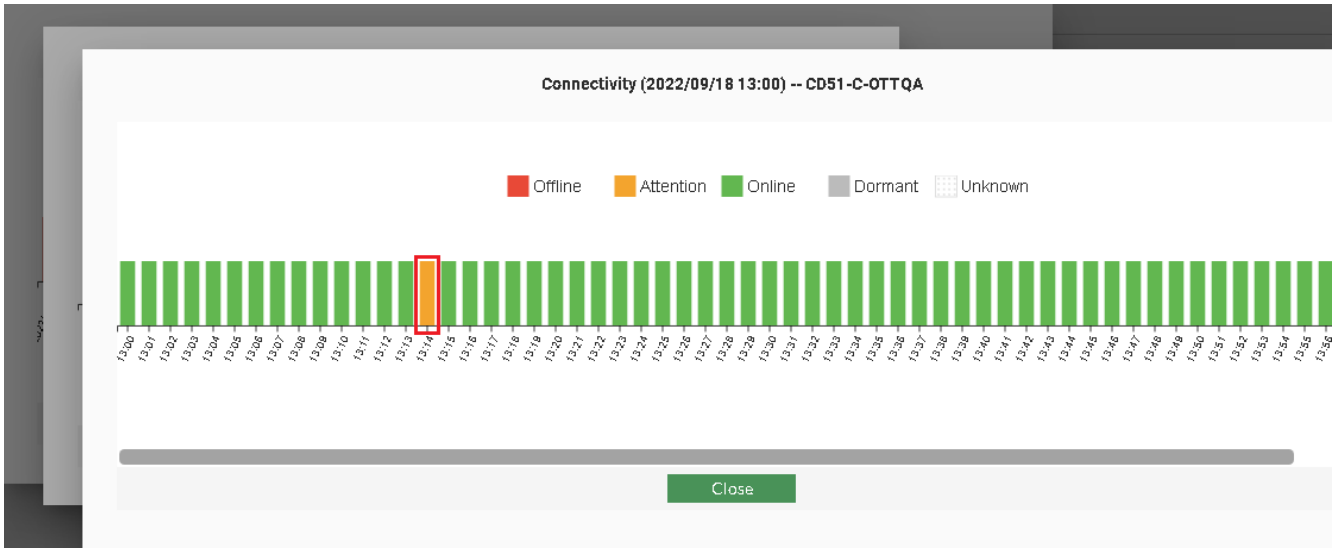
Column	Description
Site	The deployment site of the camera. See Configuring sites on page 12.
MAC Address	The hexadecimal physical address for the Wi-Fi card or physical network adapter of the camera. See also Network settings on page 31.
Status	A check mark icon whose color corresponds to the status summary at the top of the dashboard, such as *Online* or *Offline*. If you hover your mouse cursor over the icon, a tooltip indicates the reason for the status, such as *Rebooting*.

For example, if a camera status is *Offline* at any time during the previous month, then that part of the bar is red to indicate that status. You can click that time range to drill down and investigate the exact time range.

As another example, the following image shows that at 13:14 on September 18th 2022, the *Attention* status occurred. If you hover your mouse cursor over the *Status* icon, or over that time range in the *Connectivity* column, a tooltip indicates the cause of the status (for example, an out-of-sync configuration).

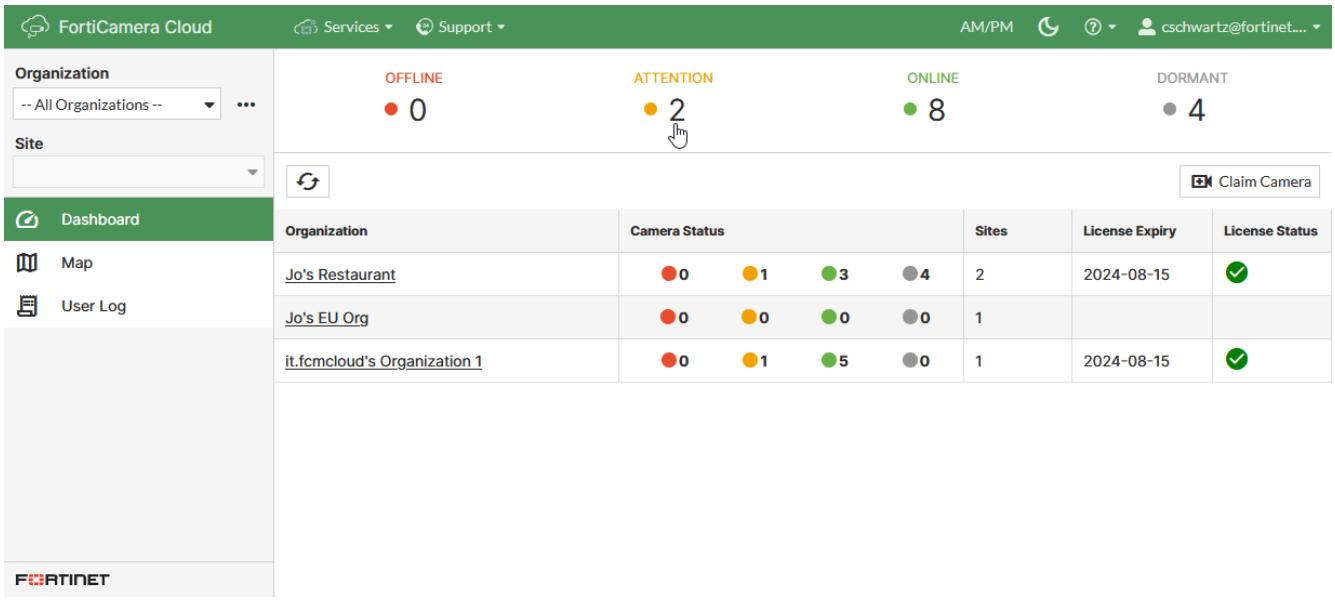






Hyper Dashboard

If your account is the owner of multiple organizations, or have been invited to multiple organizations, then you can go to *Dashboard* and click the *Hyper Dashboard* button. It display a status summary of all cameras, in all organizations and all sites.This can be useful if, for example, you manage a large company or are a managed service provider (MSP), and need to quickly see a list of all cameras that is not filtered by site or organization.



Similar to an organization-level dashboard, the hyper dashboard has a summary at the top which indicates the number of cameras that have each status, such as *Online* or *Offline*. You can click the status category to view a list of cameras filtered by that status.

For each organization on the hyper dashboard, there are the following columns:

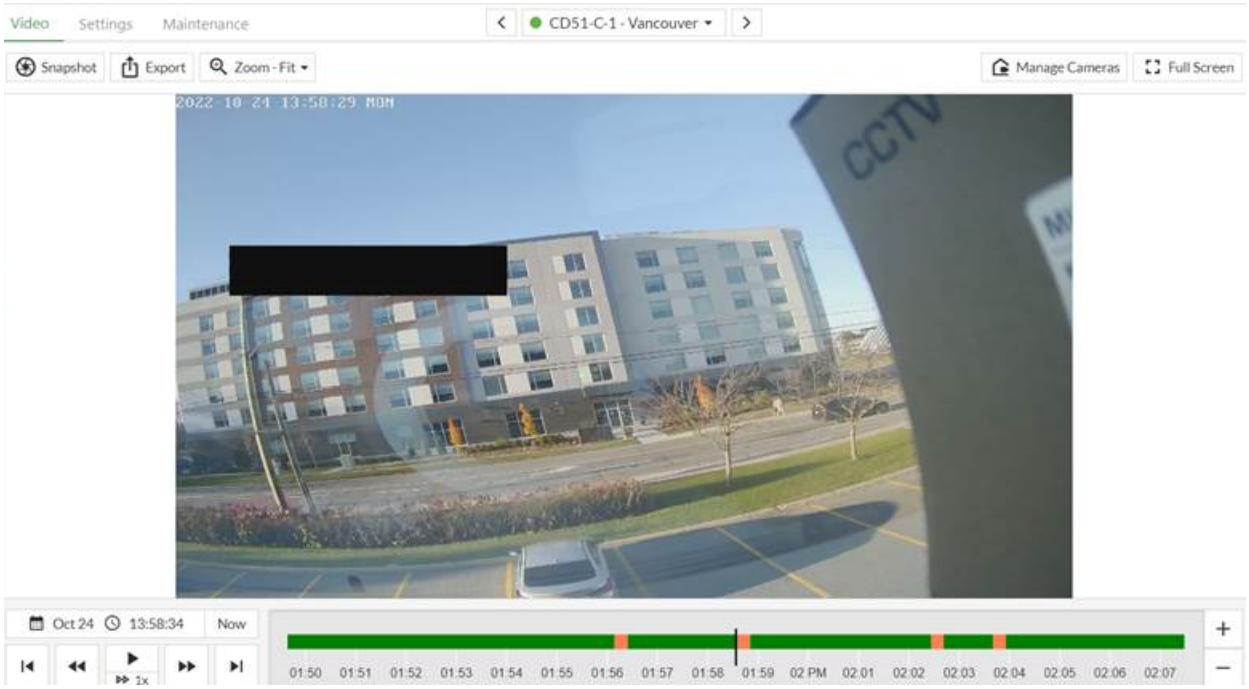
Column	Description
Organization	The name of the organization. Click the name to view the dashboard for that organization. See Dashboard on page 20 and Configuring organizations on page 10.
Camera Status	Corresponds to the status summary at the top of the organization-level dashboard. See Dashboard on page 20
Site	The deployment location of the camera. See Configuring sites on page 12.
License Expiry	The end date for the service subscription. See Camera licenses on page 35.
License Status	Indicates whether any cameras in the organization have invalid licenses.

Playing video from cameras

You can display the live video stream from any camera that you have permissions to view. From there, if you have permissions, a timeline appears below that you can use to view previously recorded video.

In the image below, the black rectangle is a privacy window that hides an area in the video.

1. From the *Organization* dropdown, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. Click the *Video* tab.
4. Use the available controls:



GUI Element	Description
Camera name (dropdown list)	Select from the dropdown list of cameras at the top of the window. The live video feed from the camera is displayed in the center of the screen. Optionally, to filter the dropdown list of cameras, select the *Organization* and *Site* from those dropdown lists first. If the dropdown list shows *-All Sites-*, then every camera of the organization is available in the list. You can switch between cameras by clicking the left and right arrows that are next to the list.
Snapshot (button)	Click to download a PNG file of the current frame in a live video feed or previous recording.

GUI Element	Description
Export (button)	Click to export and download a video clip as an MP4 file. In *Start time*, select a date and time that defines where the video clip begins, and then in *Time range* select the duration in seconds, up to a maximum of 300 seconds (5 minutes). This button requires the *Export* camera video privilege. For details, see Configuring user and administrator accounts on page 15.
Zoom (button)	Select from a list of magnifications to zoom into the video. Once zoomed in, you can drag to pan left, right, up, or down. To revert to a zoom level that fits the window or screen, click the *Fit* button next to *Zoom*.
Manage Cameras (button)	Click to go to the *Manage Cameras* screen.
Full Screen (button)	Click to display in full screen mode, where the video from the camera and its timeline occupy all of your screen. Press the *Esc* key on your keyboard to exit full screen mode.
Camera feed	Displays the live video stream from the currently selected camera.
Timeline	Displays available recordings in green and motion detection events in red. Initially, the timeline plays the live video feed from the camera. To play a previous recording, drag the indicator across the timeline to the timestamp where you want to begin. To change the scale of the timeline (zoom in or zoom out), either: • Position your mouse cursor over the exact point in the timeline where you want to zoom in or zoom out, and then scroll your mouse wheel. • Click the + and - buttons that are next to the timeline. The video player has the following controls: • *Pause* or *Play* • Directly jump to a specified date and time • *Now* (to return to the live feed) • *Previous Motion* and *Next Motion* to jump between different motion detection events • Fast forward and rewind +/-15 seconds • Select a playback speed, including slow motion  Playing a previous recording requires the *Playback* camera video privilege. For details, see Configuring user and administrator accounts on page 15.

Camera settings

You can configure many settings that affect how cameras record video and connect to the network. You can also use FortiCamera Cloud to perform basic maintenance such as software updates.

Camera settings

Settings for each camera are divided, with each category on a separate sub-tab.

Image settings

1. From the *Organization* dropdown, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. At the top of the screen, select the name of the camera whose settings you want to change.
4. Go to *Setting* > *Image*.

5. Configure the following settings:

Setting	Description
Zoom	Adjust the field of view angle (as a percentage) from wide angle to telephoto lens.
Focus	Select either *Manual* or *Full Auto* to adjust the camera focus manually or to use automatic focus.
Orientation	If the image is sideways or upside down because (for example) the camera was mounted sideways or upside down, then select the correct orientation of the image.
HDR	Enable or disable High Dynamic Range (HDR) to help even out high contrast and make image details more visible. Harsh light can otherwise cause overexposure, where it is difficult to distinguish details: bright areas are too bright, and shadows are also too dark.
DNR	Enable or disable Digital Noise Reduction (DNR) to reduce image noise that can occur in low light.
DNR Level	Use the slider to fine tune DNR. The valid range is from 1 to 10.
Overlay	Enable to display the camera name and current time as a watermark on the video image.
Privacy Window	If you want to exclude an area of the video from motion detection (for example, for privacy reasons), click *Add Privacy Window* and then drag the black rectangle(s) to position them or drag their corners to resize.

6. Click **Save**.

Video recording settings

You can individually configure the video recording settings of each camera.

Alternatively, you can save time by configuring a video profile that can be reused by many cameras. For details, see Video profiles on page 33.

1. From the *Organization* dropdown, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. At the top of the screen, select the name of the camera whose settings you want to change.
4. Go to *Setting* > *Video*.

5. Configure the following:

GUI item	Description
Select Profile	Enable to use a video profile, and then select it from *Video Profile*. For details, see Video profiles on page 33. Disable to show all the settings below, and configure them for the camera individually, on this tab.
Recording Schedules	Define whether the camera is recording video and when: • *Always*: Always record video. • *Schedule*: Record video at specific scheduled times. To define the time ranges, select it from *Schedule Profile*. For details, see Scheduled recording on page 34. • *Never*: Never record video.
Resolution	Select an image resolution: *720P*, *1080P*, *2K*, or *5M*. **Note:** A higher resolution reduces the maximum duration that can be recorded.
Quality	Select a suitable image quality: *Standard*, *Enhanced*, or *High*. A lower quality enables stronger compression and longer duration of recordings.
Motion Only Recording	When enabled, recordings without any motion detected are only kept for a short period of time. This is useful to reduce disk space usage.
Delete Recording	Indicate whether to delete recordings when the disk does not have free space, or when the recording is older than a specified number of days (see also Retention on page 31).
Audio Recording	Enable to turn on the camera's microphone for live audio recording.

6. Click *Save*.

Night mode settings

1. From the *Organization* dropdown, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. At the top of the screen, select the name of the camera whose settings you want to change.
4. Go to *Setting* > *Night Mode*.

5. Configure the following :

Setting	Description
Night Mode	Turn night mode either on, off, or automatically turn itself on or off depending on ambient lighting. In low light situations, night mode shows high sensitivity greyscale video.
IR LEDs	Turn infrared (IR) LEDs *On during Night Mode* (to illuminate the camera's view) or turn them *Off*.
IR Intensity	Use the slider to fine tune the IR LEDs intensity, for situations where nearby objects are too close to the camera. The valid range is from 1 to 10.
Transition	Select *Manual* to fine tune the *Day Transition* and *Night Transition* light levels at which night mode is turned on and off, or select *Auto*.

6. Click *Save*.

Motion detection settings

1. Go to *Camera*.
2. At the top of the screen, select the name of the camera whose settings you want to change.
3. Go to *Setting* > *Motion*.
4. If you want to limit motion detection to a specific area in the video, click *Motion Detection Window* to add a semi-transparent rectangle on the video image.
5. Drag all motion detection rectangles to where you want them in the video image. Resize the rectangles by dragging the corners.
   Multiple motion detection areas can be created.

Any *Motion Detection Windows* that either fully or partially overlap any existing *Privacy Windows* may not function as intended.

6. Drag the *Sensitivity* slider indicate how sensitive you want motion detection to be.
   For example, if you're monitoring large outdoor automobile traffic, but you don't want motion to be detected for smaller objects (such as passing pedestrians or animals), you can use a less sensitivity level.
7. Click *Save*.

Wi-Fi settings

For camera models that have Wi-Fi network capabilities, you can configure those settings.

1. From the *Organization* dropdown, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. At the top of the screen, select the name of the camera whose settings you want to change.
4. Go to *Setting* > *Wireless*.

5. Configure the following settings:

Setting	Description
Status	Enable or disable the camera's Wi-Fi connectivity.
SSID	Enter a WiFi network name, or click the magnifying search icon to select from a list of available Wi-Fi networks.
Security Mode	Set the SSID security mode: *None*, *WPA Personal*, *WPA2 Personal*, *WPA Enterprise*, or *WPA2 Enterprise*. Once selected, configure the following: • *WPA Encryption*: Select whether to use *TKIP* or *AES* encryption. • *Passphrase* (Personal only): Click *Change* to enter the passphrase to use for authentication. • *WPA Protocol* (Enterprise only): Select whether to use *TLS* or *PEAP* protocol. • *WPA Username* (Enterprise only): Enter the username to use for authentication. • *WPA Password* (Enterprise only): Enter the password of the username.

6. Click *Save*.

Maintenance and more camera settings

General settings

1. From the *Organization* dropdown, select the name of the organization that claimed the camera.
2. Go to *Cameras*.
3. At the top of the screen, select the name of the camera whose settings you want to change.
4. Go to *Maintenance* > *General*.
5. Configure the following settings:

Setting	Description
Status LED	Enable or disable the camera status LED. Click *Blink* to make the camera's LED blink for 1 minute.
Bluetooth	Click *Enable* for Bluetooth connectivity on the camera. This can be used for setup via the FortiRecorder Mobile app. Use the slider available to control the amount of time that the camera's Bluetooth will search for connections.
System	Click *Reboot* to restart the currently selected camera.  Recordings are interrupted until the camera reboots.

6. Click *Save*.

Network settings

To view a camera's MAC address, instead see Dashboard on page 20.

To view the camera's IP address, gateway, and DNS configuration

1. From the *Organization* dropdown, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. At the top of the screen, select the name of the camera whose settings you want to change.
4. Go to *Maintenance* > *Network*.

Storage settings and disk space usage

For the disk space usage, you can view statuses such as the following:

Item	Description
Storage Size	Total disk space in gigabytes (GB).
Used Space	Used disk space in gigabytes (GB).
Free Space	Unused disk space in gigabytes (GB).
Capacity	Total number of days of recording that can be stored. Varies by the currently configured bitrate (resolution and image quality).
Retention	Total number of days of recording that are currently stored. See also Delete Recording on page 28.

If required, you can also format the disk. This deletes all recordings.

If you format the camera storage disk, the stored recordings are deleted. You cannot undo it. If required, download a backup of the recordings before you format the disk.

1. From the *Organization* dropdown, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. At the top of the screen, select the name of the camera whose settings you want to change.
4. Go to *Maintenance* > *Storage*.
5. Click *Format*.

Firmware updates

If you did not enable automatic camera software updates (see Site settings on page 14), then when new software is available, you must update the camera manually.

1. From the *Organization* dropdown, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. At the top of the screen, select the name of the camera whose settings you want to change.
4. Go to *Maintenance* > *Firmware*.
5. To determine if the camera's firmware is up-to-date, verify the *Current Version* field. If it is not up-to-date, click *Update*.

Recordings are interrupted until the camera reboots.

Camera management

If you go to *Camera* > *Manage Camera*, you can configure video profiles and schedules, and rename or manage your inventory of claimed cameras.

To rename a camera, select it, and then click *Rename*. (If the camera is in a hybrid deployment and is connected via FortiRecorder, then you cannot rename the camera in FortiCamera Cloud. Instead, log into FortiRecorder, and rename the camera there.)

After you create a custom video profile, to apply it, you must select it in the camera's video settings. Similarly, to apply a schedule, you must select it in either a video profile that is used by multiple cameras, or the video settings for an individual camera. For details, see Video recording settings on page 27.

Video profiles

Video profiles contain the same video settings that are available when configuring individual cameras (see Camera settings on page 26). Profiles can save you time if you have many cameras that require the same settings. Instead of repeatedly configuring the same settings on every camera, you can configure the profile once, and then simply select it for each camera.

1. Go to *Camera* > *Video Profile*.
2. Click *New*.
3. Configure the following settings:

GUI item	Description
Name	Enter a name for the video profile.
Recording Schedule	Select whether the camera is recording video and when: • *Always*: Always record video. • *Schedule*: Select and use an existing *Schedule Profile*. For details, see Scheduled recording on page 34. • *Never*: Do not record.
Resolution	Select an image resolution: *720P*, *1080P*, *2K*, or *5M*. **Note:** More resolution will reduce the maximum amount of time that can be recorded.
Quality	Select a suitable image quality: *Standard*, *Enhanced*, or *High*. Less quality can increase compression and the maximum amount of time that can be recorded.
Motion Only Recording	When enabled, recordings where no motion was detected are only kept for a short period of time. **Tip:** Enable this option to reduce disk space usage if you do not require continuous recording.
Delete Recording	Select whether recordings are deleted when the storage runs out of space, or

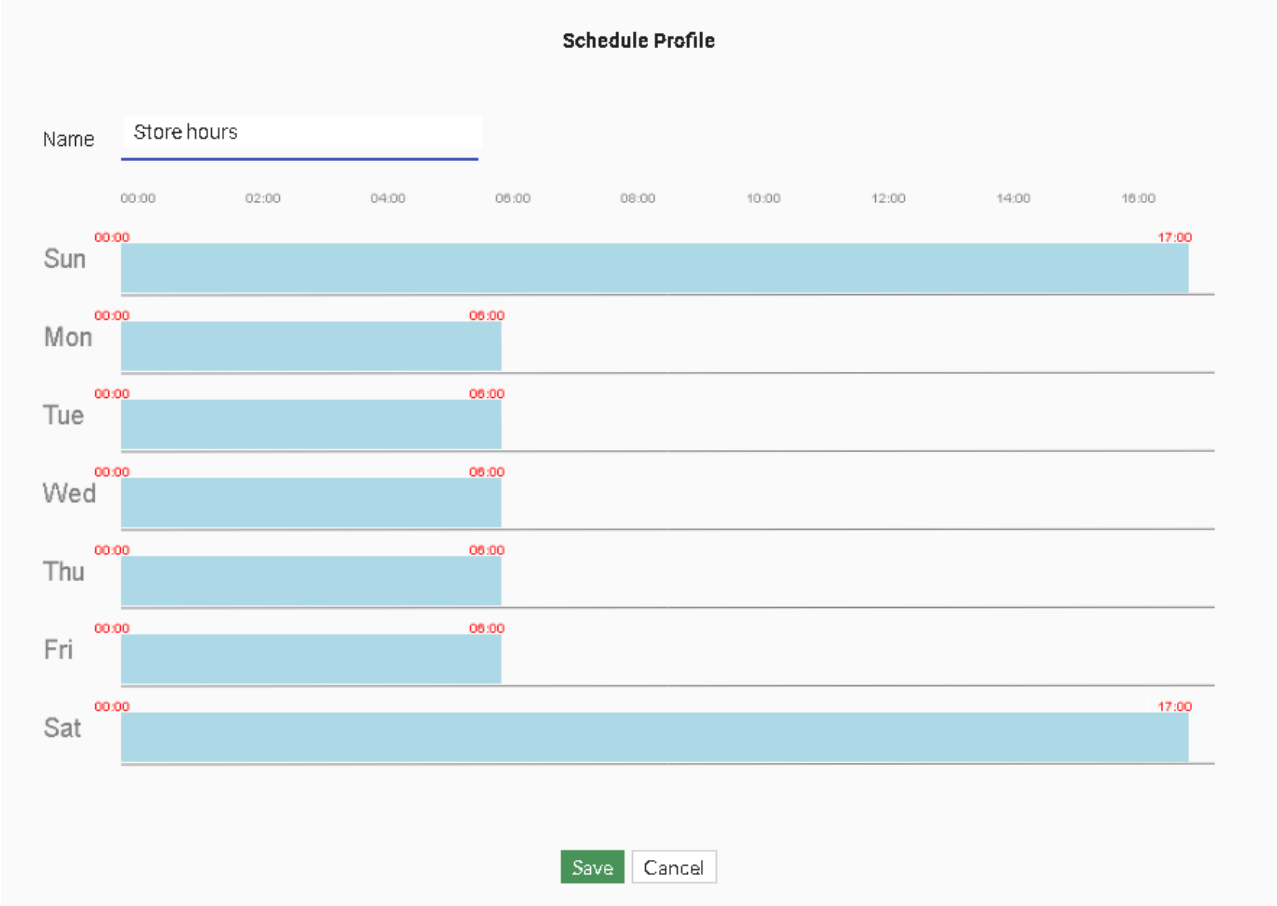
GUI item	Description
	when the recording is older than a specified number of days.
Audio Recording	Enable to turn on the camera's microphone for sound recording.

4. Click *Add*.
   To use the profile, select it instead of a camera's individual video settings. For details, see Video recording settings on page 27.

Scheduled recording

Schedules determine when the camera will record video. For continuous recording, select the entire time range during every day of the week. If you need to minimize disk space usage, however, you can limit the recording to specific times, such as when a business is closed.

1. Go to *Camera* > *Schedule Profile*.
2. Click *New*.
3. In the *Name* field, enter a unique name for the schedule.
4. For each day of the week, drag your cursor over the time period that you want the camera to record video.
   For example, in the following screenshot, the camera is scheduled to record during weekends from 00:00 (12:00 AM/midnight) to 17:00 (5:00 PM). On weekdays, the camera is scheduled to record each morning from 00:00 to 6:00 AM.



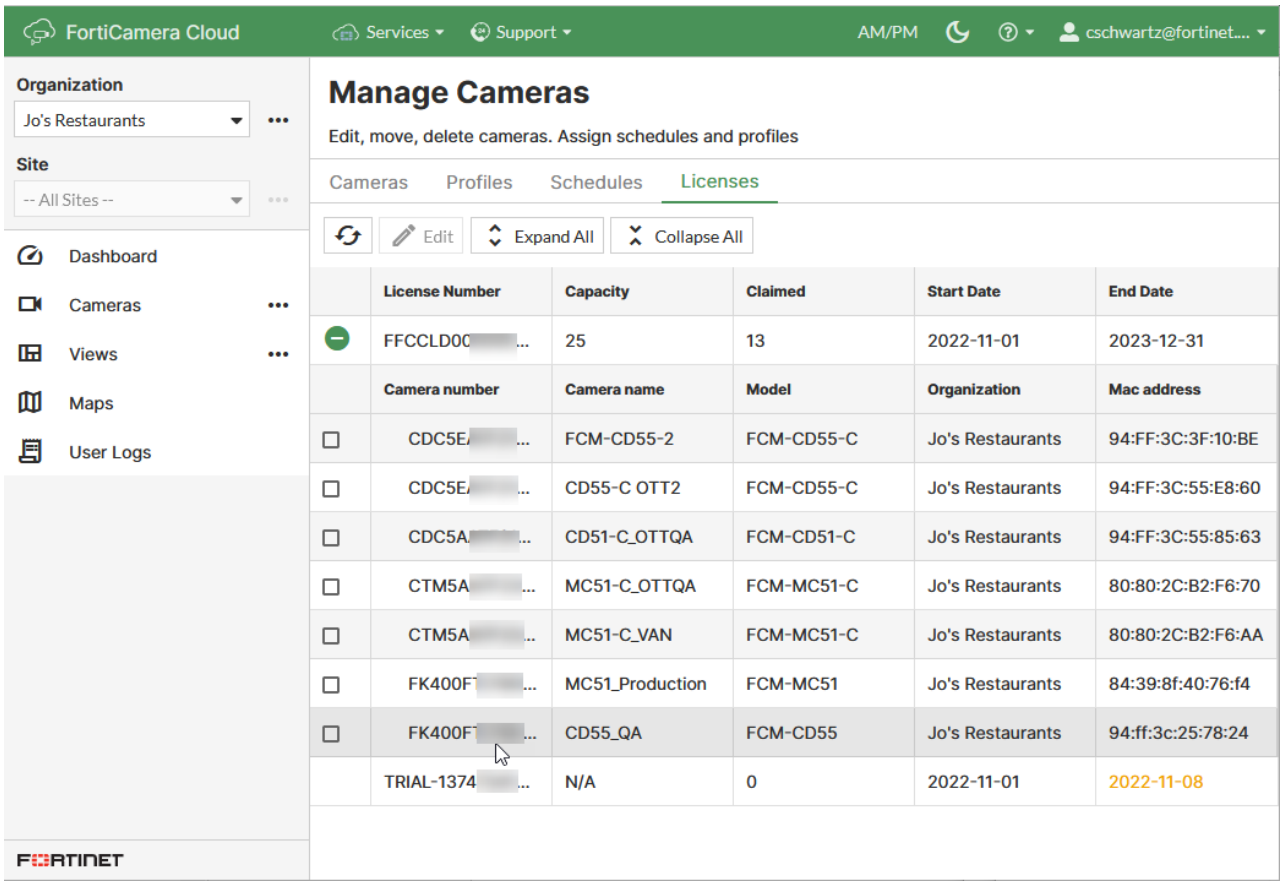
5. Click *Save*.
   To use the schedule, select it in a video profile that is used by multiple cameras, or a camera's individual video settings. For details, see Video recording settings on page 27.

Camera licenses

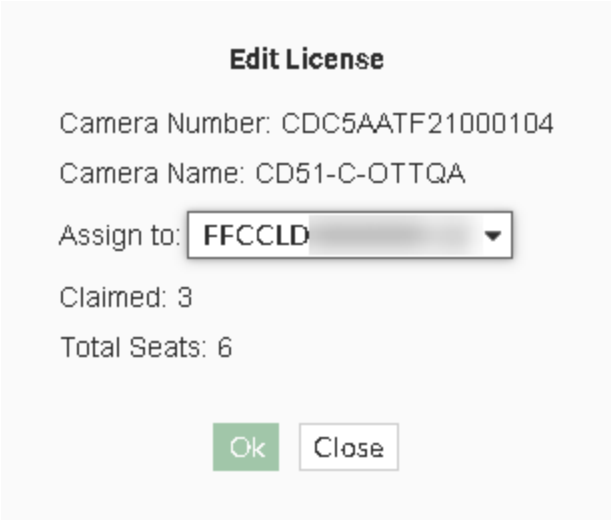
You can show all applied camera licenses and their expiry information. You can also transfer cameras to other subscription licenses.

To transfer a FortiCamera Cloud subscription license to another camera

1. Go to *Camera* > *Manage Camera*.
2. Click the *Licenses* tab.
   License information includes license *Capacity*, how many licenses have been *Claimed* by your cameras, and the dates when the license is valid or expired (*Start date* and *End date*).
   Cameras that have claimed licenses are also listed, displaying their camera serial number, name, model, MAC address, and which organization they belong to.



3. In the *Camera number* column, click the serial number of the camera to edit its license information.
4. If required, from the *Assign to* dropdown list, select an available license.



5. Click *OK*.

View panes and monitor walls

In smaller deployments, you might only have a few cameras. You can simply go to *Camera* and use the dropdown list to switch between each camera, such as the storage room camera and the front of the store. However as your organization grows, if you have more cameras or multiple security staff, it can be useful to group cameras into a layout of view panes on *View*, and perhaps also to create a monitor wall.

Monitor walls are where one of your computers has multiple monitors, which are often mounted together on a wall in your security operations center (SOC) so that everyone in the team can see those monitors. Each person in the team can change views on their own computer, yet also see the view on the team's monitor wall. In this way, FortiCamera Cloud can grow with your team, and help them to work together.

Each monitor—an individual monitor, or one in a monitor wall—is divided into one or more view panes. Each view pane can show the video stream from one camera at a time. Grid layouts define the arrangement of the group of view panes. You can show up to a maximum of 30 cameras in a layout.

View shows live video streams. For playback of previous recordings, go to *Camera* instead.

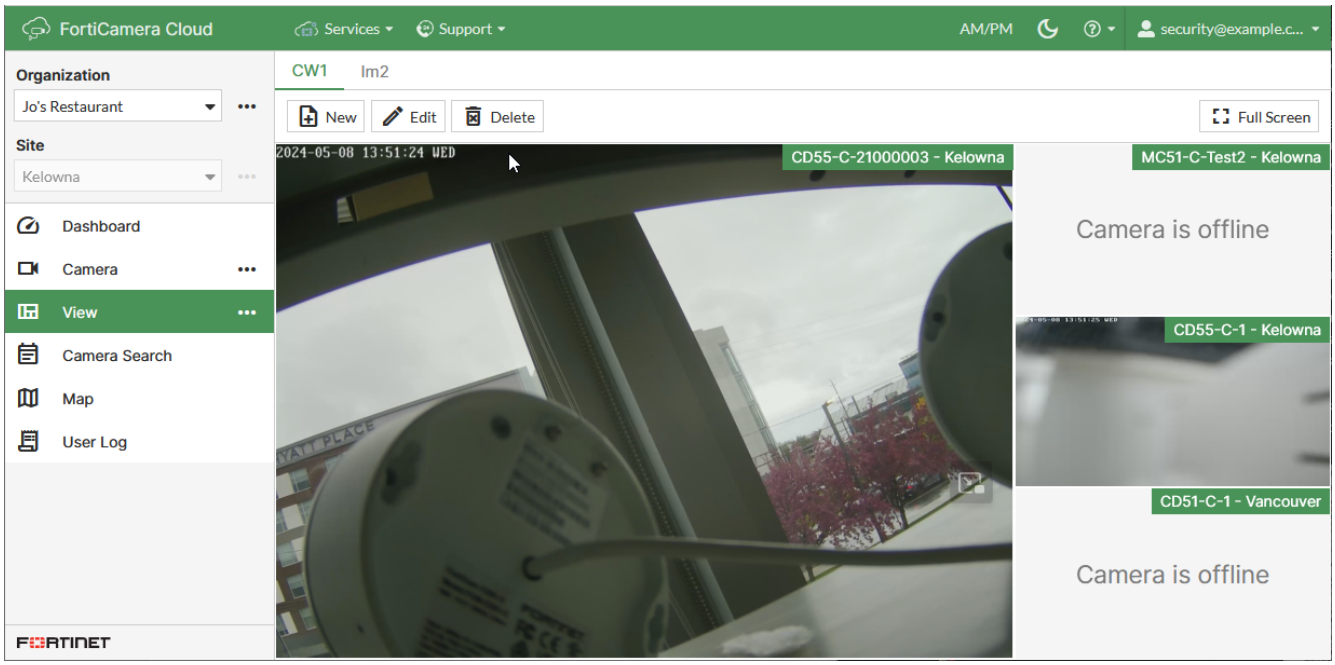
Using views

To be able to quickly display a group of cameras in an arranged layout, configure a view.

If you have only one group of view panes, go to *View*. It displays the view panes automatically.

If you have multiple groups of view panes, and you want to switch between them, go to *View* and then click the tabs named for each group at the top of the screen.

To maximize the window and remove the window title bar, click the *Full Screen* button in the top right corner. To exit full-screen mode, press the *Esc* key.



To configure a group of view panes

1. Go to *View* > *New View*.
2. Configure the following:

Setting	Description
Name	Enter a unique name.
Layout	Select the grid layouts for the view panes that will contain video from the cameras: • *1 x 1* • *1 x 2* (1 row, 2 columns) • *1 + 2* (1 large vertical view pane in the left column, and 2 smaller view panes in the right column) • *2 x 2* • *1 + 3* • *2 x 3*
Fill	Select either: • *No Fill*: If the resolution and aspect ratio of the video from the camera does not match the view pane, do not fill the extra space. • *Stretch Fill*: Stretch video to match the aspect ratio of the view pane.
Cameras	Select which camera(s) the view panes will show.

3. To rearrange the cameras in your view panes, drag each camera to a different view pane. The cameras will change places.
4. Click *Save*.

Visual search

Large sites may have many people and vehicles. When an incident occurs, manually tracking and correlating movements across motion detection videos from multiple cameras can be time-consuming. AI-assisted visual search can help you to more quickly find what you're looking for.

Visual search does not require training. Built-in recognition on the cameras can identify multiple visual attributes, such as bags, hats, vehicle type, color, and more.

Choose a camera location with neutral daytime lighting. Dim or colored lights affect a camera's ability to accurately detect the color, and therefore can affect visual search results.

Like with any motion detection recording, results may be better if you avoid reflections, and adjust the angle and field of view (FOV) until people and vehicles appear large enough that important details are visible. For example, visual search cannot find people with hats if only part of their head is visible.

Visual search requires camera models that support it, such as FortiCam-FD55-CA.

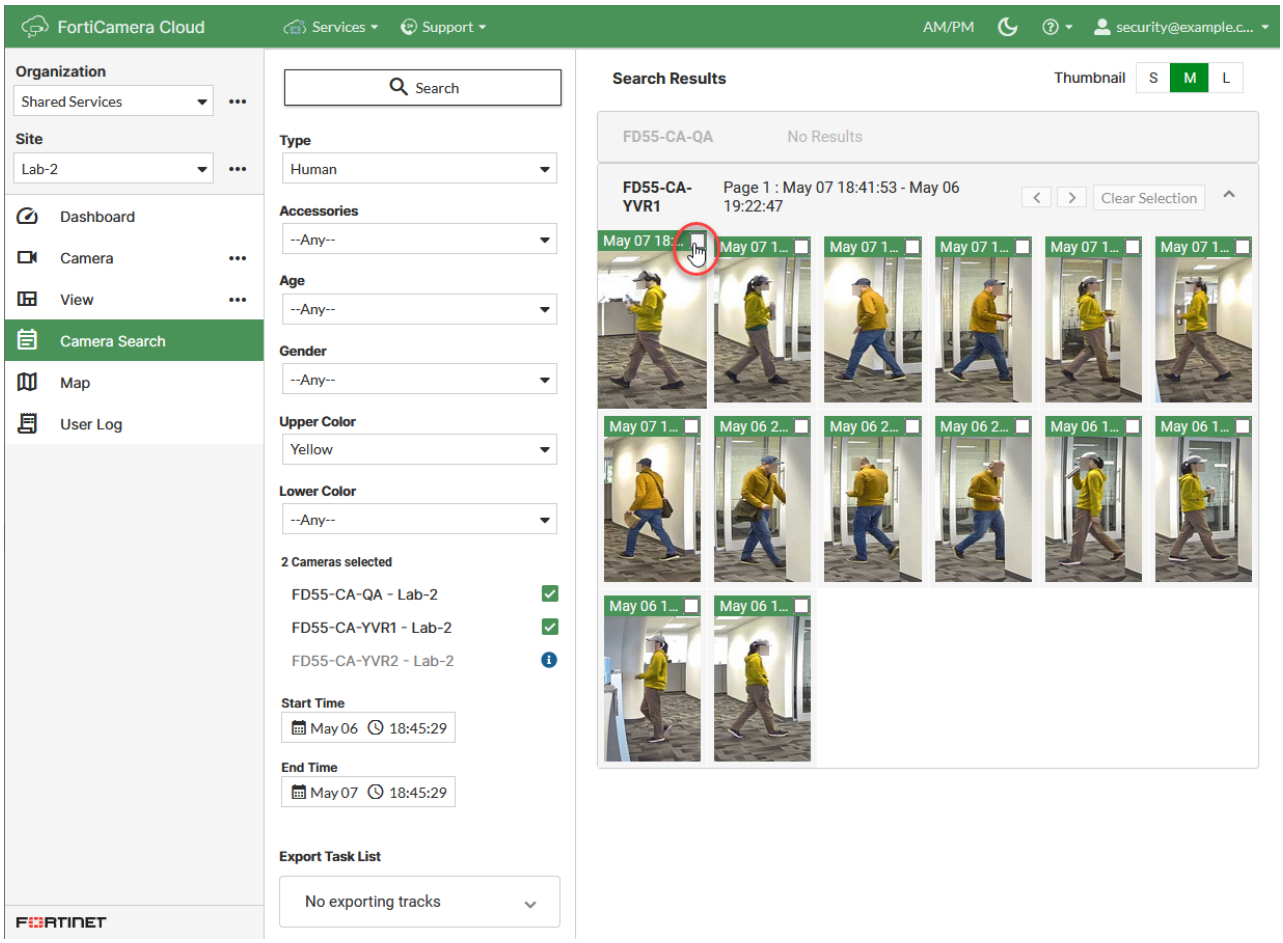
If you also have other camera models, you can still use the timestamps found in visual search to manually find corresponding motion detection events in the timelines of other cameras.

To search videos for visual attributes

1. Go to *Camera Search*.
2. Select the attributes that you are looking for (for example, *Type* is *Vehicle* and *Vehicle Color* is *Blue*), and then click *Search*.

   Thumbnail images that look like your criteria are displayed.

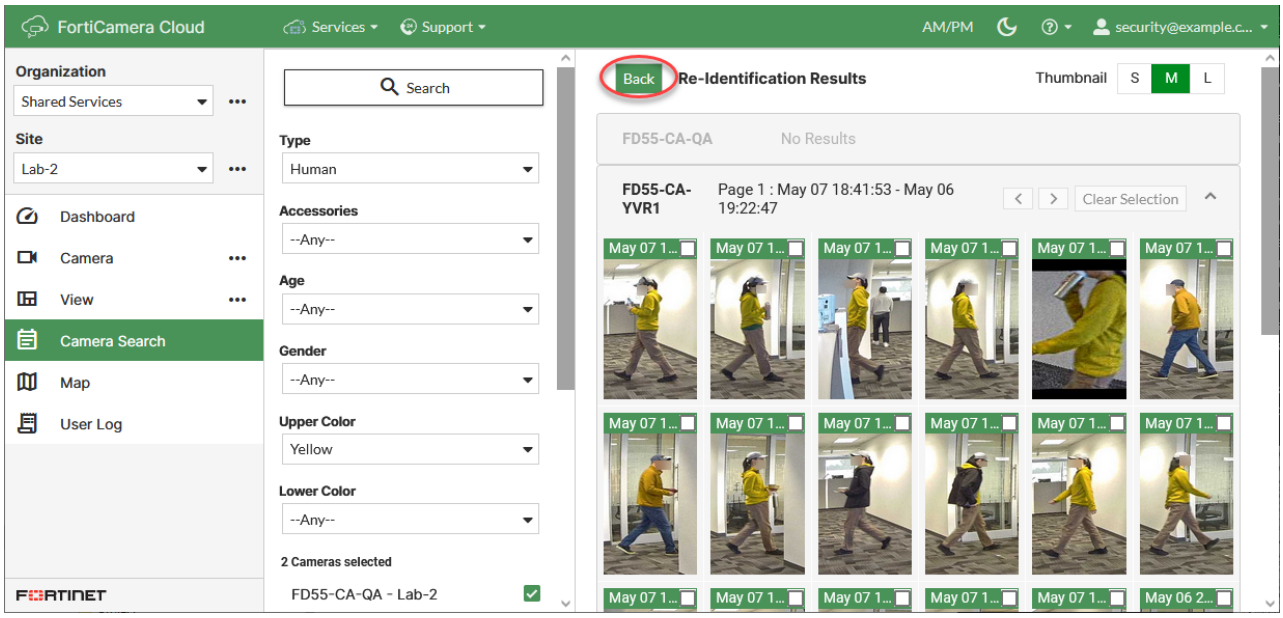
   If you want to view a video recording, click its thumbnail. Optionally you can click *Export* to download the video recording.
3. If you want to find more detections of that person or vehicle, mark the checkbox on the thumbnail.



The *Search* button changes to *ReID Search*. Optionally, you can now also adjust *Likelihood* to find other video recordings where the match is very similar(*Strict*) or somewhat similar (*Wide*). Then click *ReID Search*.

More matches are displayed.

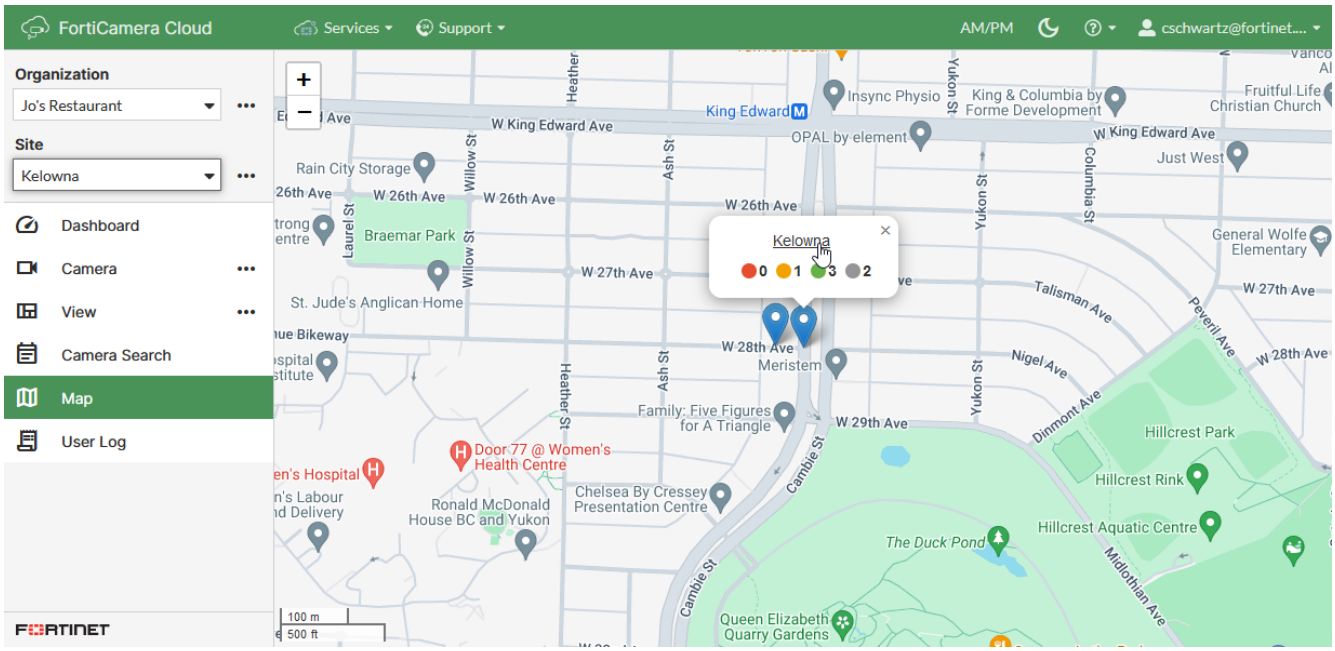
When you are done, click *Back* to return to the start of the search.


FortiCamera Cloud
Services
Support
AM/PM
security@example.c...
Organization
Shared Services
Site
Lab-2
Dashboard
Camera
View
Camera Search
Map
User Log
Search
Type
Human
Accessories
--Any--
Age
--Any--
Gender
--Any--
Upper Color
Yellow
Lower Color
--Any--
2 Cameras selected
FD55-CA-QA - Lab-2
Back
Re-Identification Results
Thumbnail
S
M
L
FD55-CA-QA
No Results
FD55-CA-YVR1
Page 1 : May 07 18:41:53 - May 06 19:22:47
Clear Selection

Maps

To view a map with all deployment sites, optionally select from the *Organization* dropdown if you want to filter the list of sites, and then go to *Map*.

The map has markers for each site, with color-coded camera status indicators. You can click the name of the site to view its dashboard.



Logs

To view or download log messages, optionally select from the *Organization* dropdown if you want to filter the list, and then go to *User Log*.

Understanding the log messages

FortiCamera Cloud appliances can log activities including:

- read and write access of camera configuration
- read access of live video feeds
- other activity such as formatting disks, claiming cameras for an organization, and user login and logout

Log severity levels

Each log message contains a *Level* field that indicates the severity of the event that caused the log message.

Name	Description
ERROR	An error condition exists and functionality could be affected.
WARNING	Functionality could be affected.
INFO	General information about system operations.

Log types

Each log message contains a *Category* field that indicates the permissions involved and type of the event.

Category Name	Description
Configuration	• Write access to camera configurations
Access	• Read access (for example, viewing a video wall or organization settings, but not changing them)
Action	• Write access to organization settings (for example, claiming cameras, adding sites) • Special access (for example, formatting the disk on a camera)

Displaying and sorting logs

You can show, hide, and re-order the display of logs.

1. Go to *User Log*.
2. From the *All Categories* and *All Levels* dropdown lists, select the type and severity levels of the logs that you want to view. Logs that don't match will be hidden.
3. Optionally, in *Search*, enter the exact text that you want to search for. Only matching log messages will be shown. For details, see Searching logs on page 44.
4. To sort logs in ascending or descending order, click a column header.
5. To view the next page, previous page, or a specific page range of log messages, use the arrows and dropdown list in the top right corner.

Searching logs

When you go to *User Log* and view log messages, you can locate a specific log message by searching for it.

In the *Search* field, type the word or phrase to search for. Search will find text in the *User*, *Client IP*, and *Message* fields of the log message by default.

If you enter multiple words, they must occur uninterrupted and in the same order as the log messages that you want to find.

For example, if you enter:

```
admin
```

as a keyword, then search results will include:

```
User 'admin@example.com' log in
```

because part of the word appears in the middle of the log message. However, if you enter:

```
User log in
```

then no search results will be found, because in the log messages, those words are always interrupted by the name of the account, and therefore the word order does not exactly match your search key phrase.

Filter configuration

Search results can be filtered to include only matches from specified columns.

1. Go to *User Log*.
2. In the *Search* field, enter the word or phrase to search for.
3. Click *Filter Configuration* (the check list icon next to the *Search* field).
4. Enable the columns where you want to include matches from them in search results. Disable all other columns.
5. Click *OK*.
   The search results refresh, with matches filtered by your new criteria.

Example: Filter authentication logs

If you search for:

`admin@example.com`

then there could be many results. User names can be in either the *User* or *Message* column for many different log messages of various types and severities, such as:

Time	User	Client IP	Category	Level	Message
2024-05-18 14:12:54	admin@example.com	10.0.0.5	Configuration	INFO	Update camera CDC5AATF21000000 settings: camera_video successfully. Changed items: delete recordings=When run out of space
2024-05-08 16:22:45	admin@example.com	10.0.0.8	Access	INFO	Accessed organization: Jo's Restaurant.
2024-05-08 16:22:44	admin@example.com	10.0.0.9	Access	INFO	User 'admin@example.com' log in.
2024-05-08 16:13:01	admin@example.com	10.0.0.5	Access	INFO	Accessed camera wall.

If you want to focus only on login events, then you would disable all columns except for *Message*. This excludes log messages where `admin@example.com` only appears in the *User* column. Then search results would show only login events such as:

Time	User	Client IP	Category	Level	Message
2024-05-08 16:22:44	admin@example.com	10.0.0.9	Access	INFO	User 'admin@example.com' log in.

Appendices

This section contains reference tables.

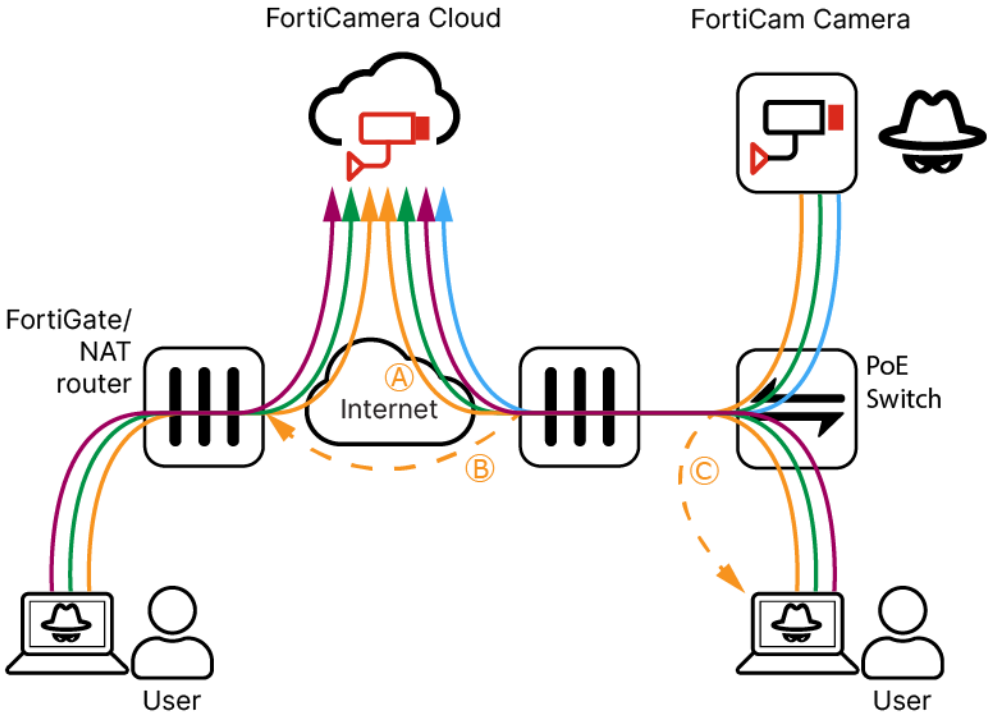
Appendix A: Port numbers

Communications between FortiCamera Cloud, cameras, FortiRecorder (if any), and your computer require that any routers and firewalls between them permit specific protocols and port numbers.

The following table describes the listening (destination) port numbers and protocols on FortiCamera Cloud servers at the domain names matching the patterns:

```
*.forticameracloud.com
ntp1.fortiguard.com
ntp2.fortiguard.com
```

All FortiCamera Cloud services are regionalized, so if you have sites in multiple regions, then each site communicates with different destination IP addresses for FortiCamera Cloud services. Cameras, administrators' web browsers, and (if any) FortiRecorder must be allowed to connect to all of the IP addresses that those domain names resolve to.



Protocol	Destination Port Number	Source IP Address	Purpose
TCP	443	Administrators' web browsers	HTTPS for GUI access
UDP	3478	Cameras **Note:** If cameras are not cloud native, then the source IP addresses are **not** the cameras directly. It is through FortiRecorder, which acts as a private relay. Firewall policies therefore must allow communications from FortiRecorder source IP addresses too. See also the FortiRecorder Administration Guide.	SRTP for video streams **Tip:** Depending on the path that route negotiation selects, the destination IP address can be either: **A. Cloud relay** — A FortiCamera Cloud relay receives communications from both the camera and the user's web browser. Through the relay, browsers indirectly receive video from the camera. **B. Through NAT** — A router or firewall that performs NAT is in front of the user's web browser, such as an external interface VIP on a FortiGate that operates in NAT mode. TURN and STUN establish the path through NAT. Then NAT rewrites the IP address so that the video stream from the camera can reach the private network IP address of the web browser. **C. Direct** — The user's web browser. For faster performance, instead of the cloud relay path, try a firewall policy that allows video streams to use a shorter routing path, either: • direct • through NAT
TCP	10000	Cameras	TLS secure tunnel for camera configuration, notifications, and queries. Does not include video streams.
TCP	15673	Administrators' web browsers	Secure WebSocket (WSS) for negotiating the best route for video streams
TCP	61614	Cameras	TLS for negotiating the best route for video streams
UDP	123	Cameras	Time synchronization (NTP)

Many firewalls automatically allow replies if a policy has already allowed a client to start a TCP connection or UDP session with a server.

If your policy does not, then in addition to allowing initial packets listed in the preceding table, you must also configure the policy to allow replies in the opposite direction: from FortiCamera Cloud servers to ephemeral port numbers on clients.

www.fortinet.com