Portal Guide

FortiCamera Cloud 25.4.a

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

December 18, 2025
FortiCamera Cloud 25.4.a Portal Guide
00-254-1238464-20251218

TABLE OF CONTENTS

Change log

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

Date	Change Description
2025-12-18	Initial release of the FortiCamera Cloud 25.4.a 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.

Getting started

Before you can use the FortiCamera Cloud service, you must physically connect and add cameras. Other basic prerequisites such as user accounts and organization setup must also be completed.

Follow these steps **in sequential order** for a basic functional deployment.

1. Requirements on page 7
2. Deployment topology planning: Hybrid vs. cloud native on page 8
3. Buying licenses on page 10
4. Registering licenses and devices with Fortinet on page 11
5. Configuring your firewall/router on page 12
6. First login to FortiCamera Cloud on page 13
   (If you need multiple organizations/sites) More organizations, sites, and cameras on page 15
7. Camera setup on page 25
8. Configuring user and administrator accounts on page 37
9. Preferences on page 41

Requirements

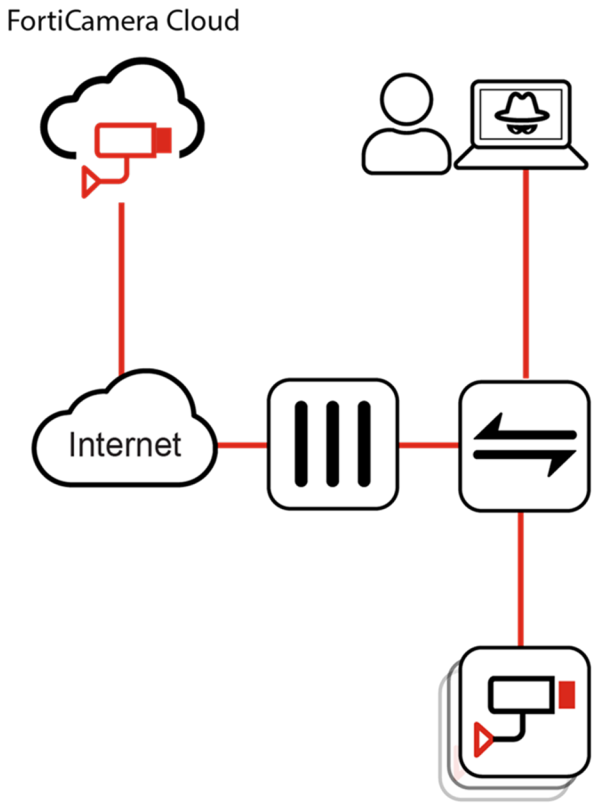
Please review that you have the required materials to use FortiCamera Cloud.

Requirement	Description
FortiCloud account	You can log in with either a FortiCloud or FortiCare account (email address or IAM account type).  REST API access requires an 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 licenses and devices with Fortinet on page 11.  Supported features vary by camera models, which may have different hardware capabilities and firmware versions. See also Firmware updates on page 29.
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.

Requirement	Description
	If you want to connect cameras that are not cloud native, or if cloud native cameras connect through FortiRecorder (in a hybrid deployment), then you must also buy and install a cloud management feature license on FortiRecorder for these cameras.
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: Port numbers on page 60.
Browser	For a list of currently supported web browsers, see the FortiCamera Cloud Release Notes.
Screen resolution	1920 x 1080 pixels Please adjust your screen resolution accordingly. Otherwise the GUI may not display properly.

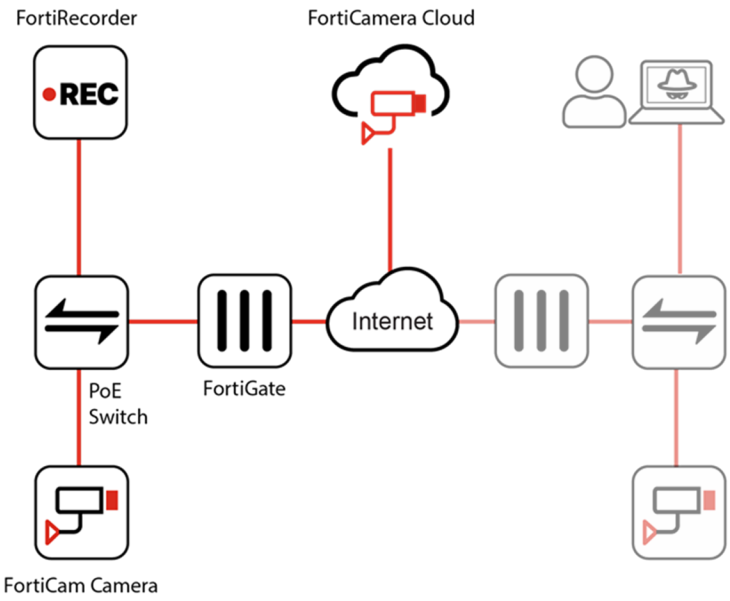
Deployment topology planning: Hybrid vs. cloud native

If you are making a new deployment, you might only use cameras that are cloud native ("-C" in the model name; for example, FortiCamera MC51-C, CD55-C, FD55-CA, or FB85-CA). Cloud native FortiCamera models can connect directly to FortiCamera Cloud, and do not need a local NVR, so the deployment scales easily.



Hybrid deployment, however, is also supported. In this deployment pattern, you can have a mix of cameras: some may be cloud native; others are not.

Cloud native cameras can be connected either directly or indirectly, via a FortiRecorder. Cameras that are not cloud native **must** be connected indirectly, via a FortiRecorder.



Advantages of hybrid deployment include:

- Flexible choice of camera models
- Extended storage and retention capabilities beyond the SD disk in cloud native FortiCamera models
- Gradual migration from private network/LAN deployment to cloud-based deployment, if needed

Hybrid deployments require a feature license on FortiRecorder. For instructions, see hybrid deployment with FortiCamera Cloud and FortiRecorder.

If a cloud-native camera model has already connected to FortiCamera Cloud before, and you want to re-deploy it in a hybrid network, you must remove the camera from the organization's managed inventory (un-claim) first.

Buying licenses

FortiCamera Cloud service and support requires a subscription. If your deployment plan will integrate with FortiRecorder, you also need to buy licensing for that feature on FortiRecorder.

Details are in the next sections.

FortiCamera Cloud service subscription

After an initial 7-day grace period, all cameras require an annual subscription 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.

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

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

- **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 so that in future, subscription renewals can be made simultaneously for all cameras.

Hybrid cloud mode for cameras via FortiRecorder

If you want to manage and play video from cameras in FortiCamera Cloud that connect through FortiRecorder (a hybrid deployment), also buy the cloud mode feature license.

Cloud native cameras can be connected through FortiRecorder if you want more features that FortiRecorder provides, such as large local storage and to connect with cameras that are **not** cloud native.

All FortiRecorder models, except FortiRecorder VM on AWS pay-as-you-go (PAYG), can be licensed for hybrid deployment.

This feature license does not increase the maximum number of cameras that can connect to each FortiRecorder, and does not include a FortiCamera Cloud service subscription.

SKU	Contents
FRC-CLM-20	FortiRecorder Cloud Mode for camera license Stackable Perpetual license for 20 cameras to connect through FortiRecorder to FortiCamera Cloud Feature license certificate

Registering licenses and devices with Fortinet

When you register a device with Fortinet, also apply any associated feature licenses and service subscriptions, such as a FortiCamera Cloud subscription.

If devices are already registered and claimed in an organization, and you need to transfer them to another FortiCamera Cloud owner, don't follow this procedure. Instead contact Fortinet Technical Support.

Later, once the cameras have been claimed by an organization, in addition to FortiCloud Asset Management, you can view the license expiry dates in FortiCamera Cloud.

1. Go to:
   https://support.fortinet.com
   and log in as the owner.

   For simplicity, this document shows instructions performed by the default account role, *Owner*.

   Owners are superuser accounts. Each organization has only one owner. Only the owner can claim cameras and licenses, and therefore the organization only has assets from that FortiCare account.

   Other parts of FortiCamera Cloud are available to users that have been granted permissions.

2. Register your cameras and (if any) FortiRecorder with Fortinet.
   For details, see FortiCloud Asset Management documentation.
3. Register the FortiCamera Cloud service entitlement license.
   The service entitlement license can be used only by registered cameras in the same FortiCare account.
   For hybrid deployments, cameras will not use the service license directly. Instead, cameras will be licensed through FortiRecorder, and FortiRecorder will connect with the service.

   FortiCamera Cloud service subscriptions are not permanently bound to a specific camera. You can replace cameras or transfer the subscription to another camera if needed.

4. (Hybrid deployments only) Apply the feature license for hybrid deployment to the FortiRecorder serial number.
   Then log into FortiRecorder, set it up, and upload the hybrid mode license file.
5. Physically plug in your FortiCamera devices. For details, see the Quick Start Guide for your model.
6. (Hybrid deployments only) Add the cameras to FortiRecorder and then enable *Managed by cloud*.

Configuring your firewall/router

Cameras may be able to connect to FortiCamera Cloud with no adjustment to your network.

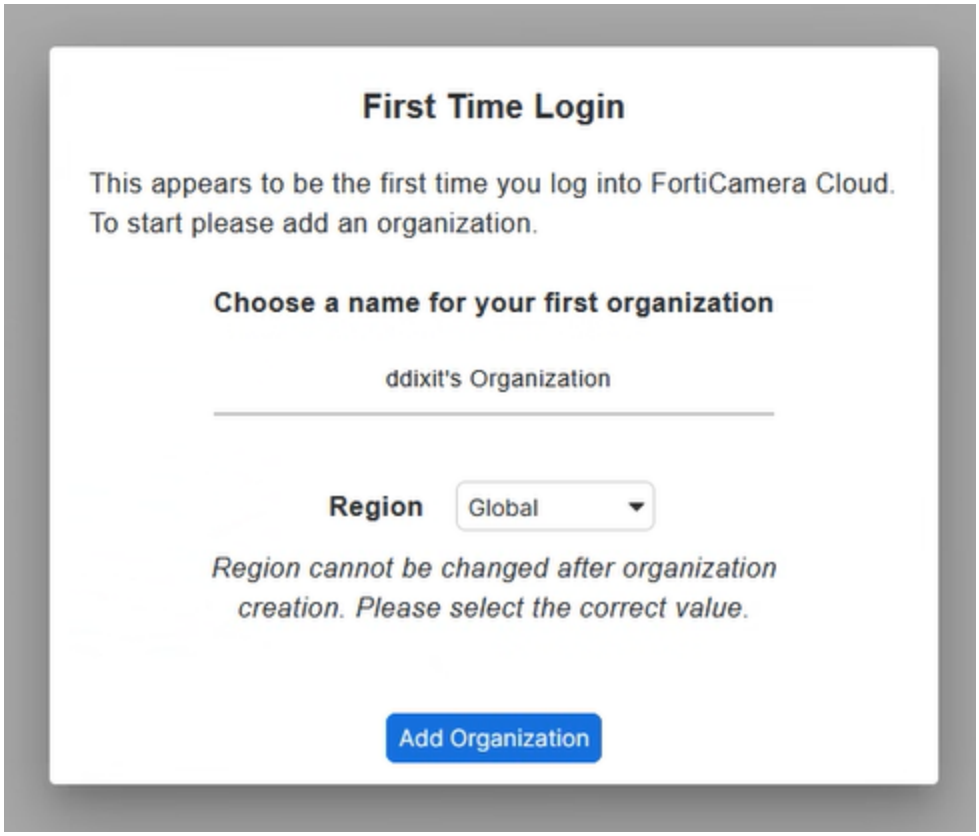
Otherwise, if your office's FortiGate, third-party firewall, or Internet router has policy or NAT settings that restrict connections between cameras and users, FortiRecorder, and FortiCamera Cloud, adjust settings to allow required network traffic. For details, see Appendix: Port numbers on page 60 and the FortiGate Administration Guide or other documentation for your firewall/router.

First login to FortiCamera Cloud

When the owner logs into FortiCamera Cloud for the first time, it prompts for basic initial setup.

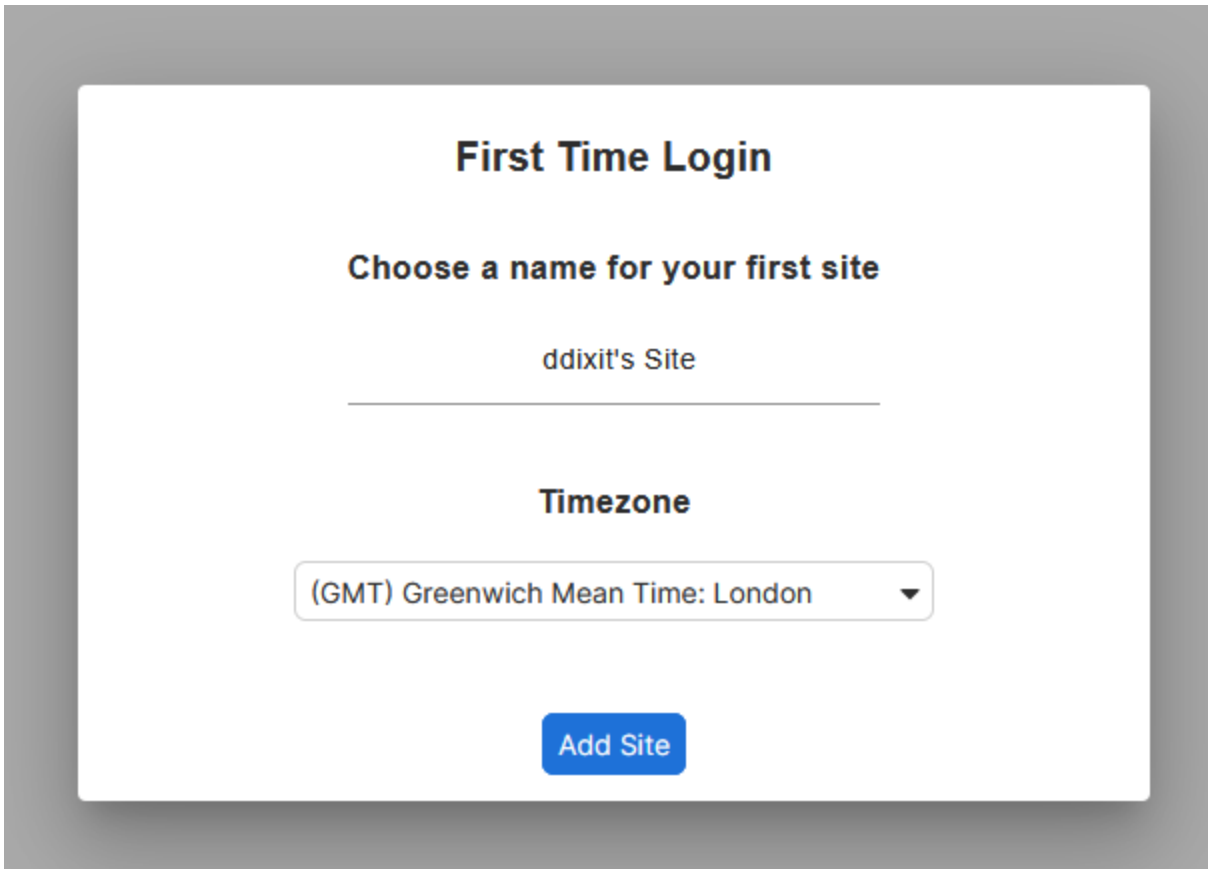
If this is not the first time that you are logging into FortiCamera Cloud, instead continue with Camera setup on page 25.

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 the owner's 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 then click *Add Organization*.

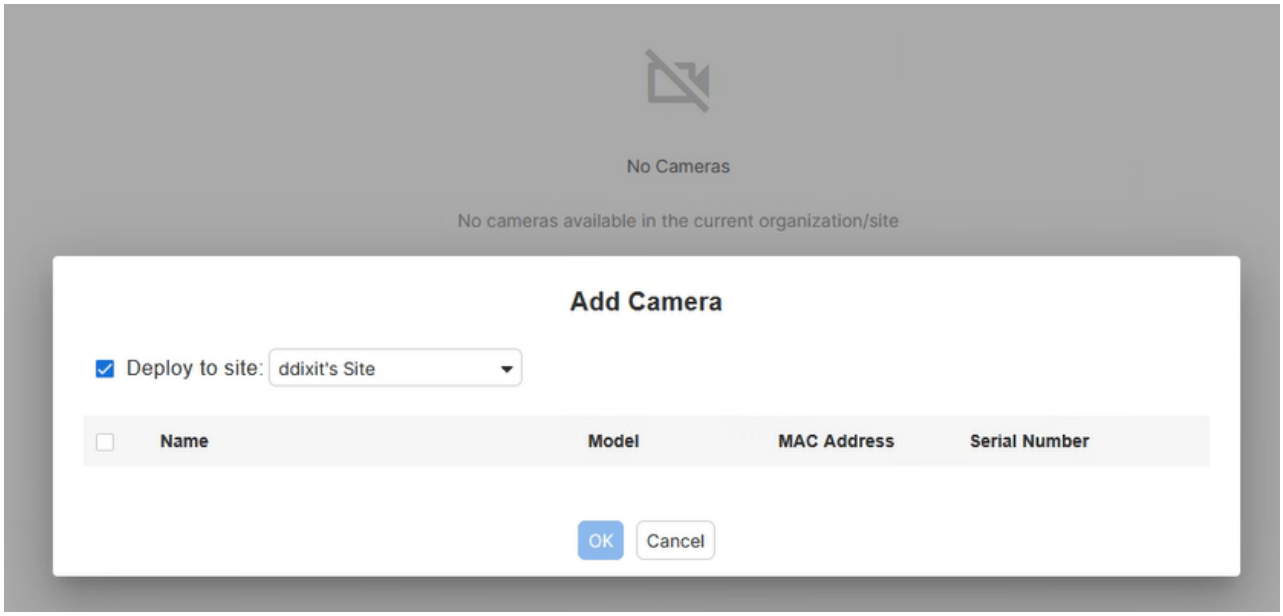


Select the region carefully. The region cannot be changed after the organization has been created. It determines the location of the datacenter that hosts cloud services for the organization.

4. Enter a name for your organization's first deployment site, and select its *Timezone*.



5. If you registered cameras in FortiCare, click *Add Camera*. Select the cameras that you want to add to each site and click *OK*.



Otherwise click *Cancel*. (You can register and add more cameras later.)

More organizations, sites, and cameras

Upon your first login to FortiCamera Cloud, a setup wizard prompted you to create at least one organization and site, and to add cameras.

If you need to create more organizations and sites, or claim more cameras for deployment at those sites, you can do this next.

Configuring organizations

Organization owners and organization administrators can change or add more sub-organizations as your organization grows.

Each sub-organization can hold multiple sites where you deploy cameras that the organization owns, and you can grant permissions for users in the organization to restrict their access to specific sites and cameras.

To add an organization

1. Go to *Management* .
   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. Click *Add Organization* .
   This button appears at the bottom left corner of the page, and only if you have owner or organization administrator permissions.
3. In the *Organization Name* field, enter a unique name.
4. 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.
5. Click *Save*.

Video encryption settings

1. Go to *Management* .
   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. From the organization structure, select the organization.
   (The next tab has different settings if a site is selected instead.)

3. Click the *General* tab.
4. If you have not yet claimed any cameras for the organization, or have removed them from the organization, then you can enable or disable *Video encryption*.

   This only affects encryption at rest (files stored on each camera's disk). It does not change encryption in transit (video streams over the Internet), which are always encrypted.

Video recording settings

Video profiles contain some of the same video settings that are available when configuring individual cameras (see Camera setup on page 25). 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.

To create a video profile

1. Go to *Management* .

   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. From the organization structure, select the organization.

   (The next tab is not available if a site is selected instead.)
3. Click the *Video Profile* tab.
4. Click *New*.
5. 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 Schedules on page 17. • *Never*: Do not record.
Resolution	Select an image resolution: *720P*, *1080P*, *2K*, or *5M*. **Note:** A greater resolution will reduce the maximum amount of time that can be recorded. Lesser resolution may be automatically used while viewing the live streams from multiple cameras in a video grid.
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 when the recording is older than a specified number of days (see also

GUI item	Description
	Retention on page 29).
Audio Recording	Enable to turn on the camera's microphone for sound with live video streams and recordings.

6. To use the profile, select it instead of a camera's individual video settings. For details, see Video recording settings on page 32.

Schedules

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.

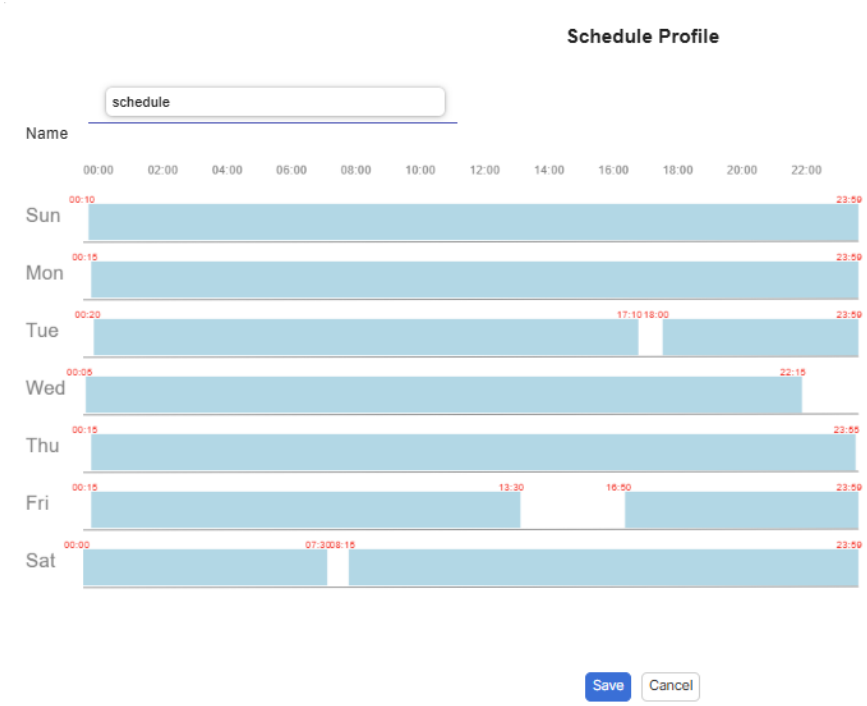
If you need to temporarily disable recording on a specific camera, but do not want to change the schedule, then you can disable the camera instead.

1. Go to *Management* .

   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. From the organization structure, select the organization.

   (The next tab has different settings if a site is selected instead.)
3. Click the *Schedule Profile* tab.
4. Click *New*.
5. In the *Name* field, enter a unique name for the schedule.
6. 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. Times are relative to the time zone of the site. See Timezone on page 21.



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 32.

Configuring sites

Multiple deployment sites can belong to an organization, with cameras potentially spread across the geographic locations of those sites. This allows you to group your cameras and grant permissions to users by physical location or by the structure of your organization.

Some features depend on the physical location of the site:

- Timezones for cameras vary by the site's location. Firmware auto-upgrade windows and recording schedules for cameras are also relative to the site's local time and timezone.
- Maps can show each site's location.
- Persons of interest and license plates of interest are synced to cameras in the same site so that all nearby cameras can coordinate to monitor for that person or vehicle. Notifications about those events are therefore also relative to each site, and you can avoid notifying staff that are fara away and unable to investigate.

To add a site

1. Go to *Management* .

   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. From the organization structure, select the organization that the new site will belong to.
3. Click *Add Site* .

This button appears at the bottom left corner of the page, and only if you have owner or organization administrator permissions.

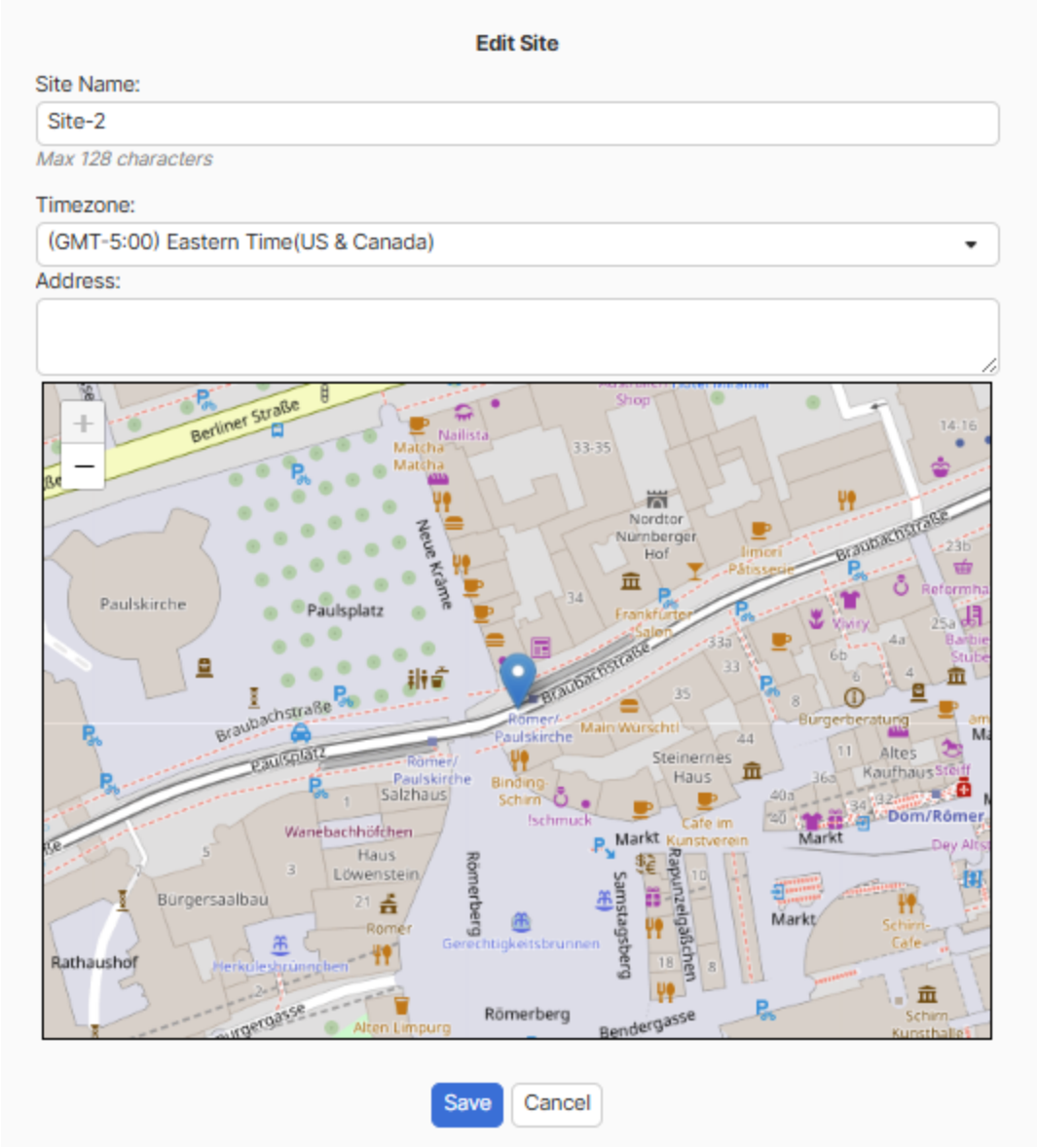
4. Configure the following settings:

Setting	Description
Site Name	Enter a unique name for the site.
Timezone	Select the time zone of the site. Many times such as the timestamp video overlay, timeline, recording schedules, firmware upgrades, logs, and notifications are relative to the site's local time zone.
Address	Enter the street address that will be used to display the site on the map. 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.

5. 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.



Camera maintenance windows

By default, cameras managed by FortiCamera Cloud automatically upgrade their software when a new version is available. You can schedule the maintenance window at a convenient time, or disable automatic upgrades if necessary.

To schedule camera firmware upgrades

1. Go to *Management* .

   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. From the organization structure, select the site.

   (The next tab has different settings if an organization is selected instead.)

3. Click the *General* tab.
4. Configure the following settings:

Setting	Description
Timezone	Select the time zone of the site. Many times such as the timestamp video overlay, timeline, recording schedules, firmware upgrades, logs, and notifications are relative to the site's local time zone.
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 time in *Selected Time*. If automatic camera upgrades are disabled, the camera status will indicate *Attention* when new software is available, but then you must update each camera manually. Firmware upgrades may add support for new features in FortiCamera Cloud, but also fix issues and patch security vulnerabilities. You should upgrade cameras as soon as possible. For details, see Firmware updates on page 29. When the update is complete, the camera's software version should show the new version the next time that it connects to FortiCamera Cloud/  Recordings are interrupted until the camera reboots.
Selected Time	Select the start of the automatic firmware upgrade window for cameras at the site.

Persons of interest and known persons

Notifications about persons of interest or known individuals for investigations can be triggered, depending on the face recognition capabilities of cameras at the site. To do so, you must provide images of the persons.

1. Go to *Management* .
   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. From the organization structure, select the site.
   (The next tab is not available if an organization is selected instead.)
3. Click the *Person of Interest* tab.
4. Click *New* to create a new list of persons of interest, or select an existing profile and click *Edit*.
5. In *Name*, enter a name.

 Some people have the same name, or their names are unknown, so a unique name is not required. However a unique name is better for troubleshooting and so that notifications are specific. Try adding a short identifier to the name, such as `Unknown (bald, mustache)`.

6. Optionally, enter a *Description*.
7. Click *Save*.
   The list is now available when you configure a person.
8. Click the *Person Profile* tab.
9. Click *New* to create a new person profile, or select an existing profile and click *Edit*.
10. In *Name*, enter a unique name.
11. Click + to upload photos of their face.

For best results, use several photos of the person's face, shown from different angles. This helps to correctly identify the person even if they are looking in another direction. If you do not have a photo yet, you can use visual search results later to update the person profile and improve face recognition accuracy.

Optionally, if you want to add them to a list of persons of interest, select the lists.

12. Click *Save*.

Notifications cannot occur until:

- face and person of interest detection is enabled on cameras
- cameras receive the list of persons of interest via configuration sync
- notification rules indicate whom to notify about persons of interest

Firewalls and other devices must allow required network connections in order for the configuration sync to succeed. If a camera has not received the list yet, *Status* shows that the configuration is not synchronized with FortiCamera Cloud.See also Appendix: Port numbers on page 60 and Motion detection and AI recognition settings on page 33.

License plates of interest

Notifications about persons of interest or known individuals for investigations can be triggered, depending on the license plate recognition capabilities of cameras at the site. To do so, you must define which license plates.

1. Go to *Management* .
   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. From the organization structure, select the site.
   (The next tab is not available if an organization is selected instead.)
3. Click the *License Plate of Interest* tab.
4. Click *New* to create a new list of license plates of interest, or select an existing profile and click *Edit*.
5. In *Name*, enter a unique name.
6. Optionally, enter a *Description*.
7. In *License Plate*, enter a license plate number, and then click *Add*.
   Wild cards (* and ?) are supported for partial plate matches. Spaces do not affect matches.
   For example, * matches all license plates; `XYZ*` matches any license plate that starts with `XYZ`; `A?? 2B3` matches any license plate that is six characters long, where the second and third character is not known.
   Repeat this step if you want to add more license plate patterns.
8. Click *Save*.

Notifications cannot occur until:

- license plate detection is enabled on cameras
- cameras receive the list of license plates of interest
- notification rules indicate whom to notify about license plates of interest

Firewalls and other devices must allow required network connections in order for the configuration sync to succeed. If a camera has not received the list yet, the camera status indicates that the configuration is not synchronized with FortiCamera Cloud and communications may have been disrupted.See also Appendix: Port numbers on page 60 and Motion detection and AI recognition settings on page 33.

Notifications

Notifications can be sent to users based upon what the site's cameras detect.

1. Go to *Management* .
   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. From the organization structure, select the site.
   (The next tab is not available if an organization is selected instead.)
3. Click the *Notification Rule* tab.
4. Click*New* to create a new group of notifications, or select an existing one and click *Edit*.
5. Configure the following settings:

Setting	Description
Name	Enter a unique name for the notifications.
Camera	Select which cameras in the site will monitor for notification triggers.
Notification Type	Select the triggers for notifications, such as: • *Person of Interest*: Detection of the face of a person of interest. See Persons of interest and known persons on page 21. • *Motion*: Motion detection. See Motion detection and AI recognition settings on page 33. • *Camera Status*: Camera status changes. See About camera status and connectivity on page 42. • *License Plate of Interest*: Detection of a license plate of interest. See License plates of interest on page 22. Available notification types vary by camera models at the site.
User	Select which users to notify. Available users depend on which users have permissions to access playback of previous recordings (see Configuring user and administrator accounts on page 37). Each user can choose how to receive their notifications (see Notifications on page 54).

Adding cameras to the inventory

After registering FortiCamera devices to the owner's FortiCare account and creating sub-organizations and sites, the owner or organization administrator must assign the cameras to the inventory at a site. This makes cameras available for other users in the organization to access the camera.

If you want to either:

- sell or give the camera to another organization
- transfer a camera to another FortiCamera Cloud subscription
- remove a camera so that the camera can be managed only by FortiRecorder instead, or in a hybrid deployment together with FortiRecorder

then you can also remove the camera.

Cameras can only be claimed while they are not yet claimed by another organization.

For hybrid network deployments, the camera must be claimed only **after** you add it to FortiRecorder. Otherwise FortiCamera Cloud will lock the camera to it, and not allow other management services. When you try to add the camera, FortiRecorder will indicate this problem with an authentication error.

1. From the organization and site dropdown menu at the top of the page, select the name of the site whose inventory you want to manage.
2. Go to *Camera*  .
3. Either:
   - Click *Add Camera*. In the dialog, select cameras that are not already claimed. In *Deploy to site*, select the name of a site in the organization, and then click *OK*.
   - Click *Manage Camera*. In the dialog, click *Add*, select cameras that are not already claimed. In *Deploy to site*, select the name of a site in the organization, and then click *OK*. Alternatively, you can click *Remove* to un-claim cameras from the organization or site.

     The *Status* dropdown can help you to find cameras that have been plugged in and are visible to FortiCamera Cloud ("online").

   The *Add Camera* and *Manage Camera* buttons appear at the bottom of the page, and only if you have the required permissions.

Camera setup

Before users with a *Monitor* or *Operator* role can use the cameras, the owner (or an administrator to whom the permission has been delegated) may need to:

- upgrade firmware
- format the camera's disk
- turn off the status LED
- optimize motion detection regions
- adjust some model-specific or default camera settings

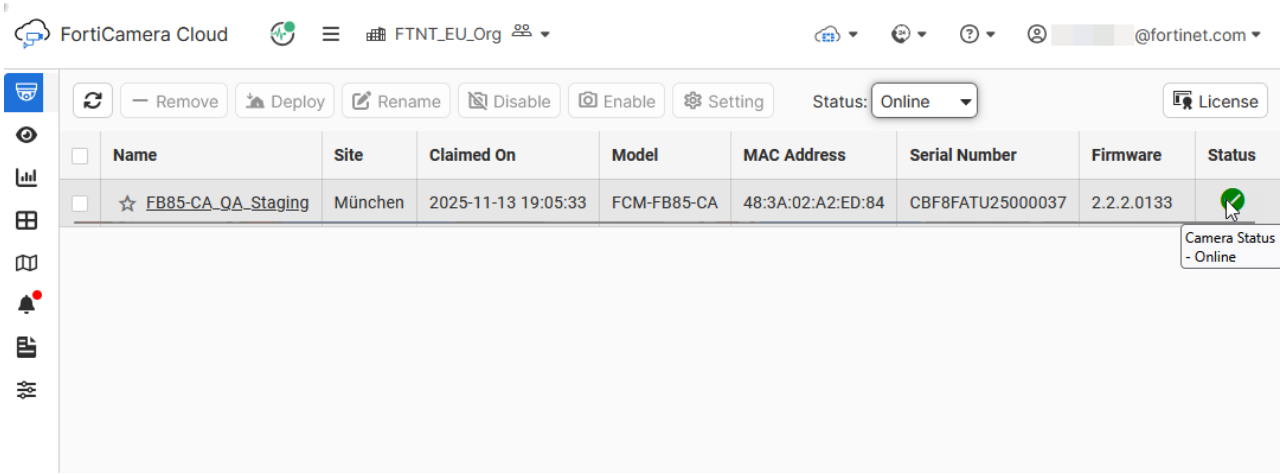
Sequential order is indicated by the order of headings below. Some settings have prerequisites and dependencies. For example, if you want to format the camera's disk, then to simplify and avoid data loss, you should do this before the camera begins to store video.

Cameras must be connected to FortiCamera Cloud (*Status* is *Online*) in order to get your setting changes.

To show only cameras that are online

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera* .
3. Click *Manage Camera*.

   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
4. In the *Status* dropdown list, select *Online*.



GUI item	Description
Remove	See Adding cameras to the inventory on page 24.
Rename	Click and then enter a unique name for the camera in the organization. **Note:** 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.
Disable or **Enable**	See Disabling cameras on page 27.
Setting	See Network settings on page 27 etc.
Status (dropdown)	Select which cameras to show based upon their status.
License	See Camera licenses on page 26.
Name	Name of the camera in the organization.
Claimed On	Date when the owner claimed the camera.
Model	Name of the camera model.
MAC Address	Hexadecimal physical network address for the camera. Network administrators may require this for network access control on Wi-Fi access points or switches.
Serial Number	Serial number of the camera.
Firmware	FortiCam software version number. See also Camera maintenance windows on page 20 and Firmware updates on page 29.
Status	See About camera status and connectivity on page 42.

Camera licenses

You can show all trial and purchased FortiCamera Cloud subscription licenses and their expiry information. You can also transfer cameras to other subscription licenses.

If you need to renew licenses, or if they are not applied to any owner or device yet, see Registering licenses and devices with Fortinet on page 11.

To transfer a FortiCamera Cloud subscription license to another camera

1. Log into FortiCamera Cloud as the license owner.
   Other accounts do not have the required permissions.
2. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
3. Go to *Camera* .
4. Click *Manage Camera*.
   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
5. Click *License*.

License information includes *Capacity* (how many cameras are allowed to use the license), *Claimed* (how many cameras are currently using the license), 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.

6. In the *Camera number* column, click the serial number of the camera to edit its license information.

   Alternatively, select the checkbox of the row, and click *Edit*.
7. If required, from the *Assign to* dropdown list, select an available license.
8. Click *OK*.

Disabling cameras

Disabled cameras have a slashed camera icon next to their names in this list.

Disabled cameras:

- Do not record, even if usually the schedule or motion detection settings would start a recording.
- Do not play live streams or previous recordings.
- Do not detect people and keep data for visual search and notifications about persons of interest.
- Do not notify you about expired licenses.

This can be useful if the camera is claimed but not yet mounted, damaged, or if the area is temporarily closed to recording for privacy reasons.

Disabled cameras can have various statuses, depending on when they previously connected to FortiCamera Cloud.

To disable a camera

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera*  .
3. Click *Manage Camera* and then select a camera.

   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
4. Click *Disable*.
5. Click *Confirm*.

   If you need to re-enable the camera later, select it again and then click *Enable*.

Network settings

For cameras that are cloud-native, this tab displays the local network settings that the camera uses to connect to FortiCamera Cloud, such as the camera's IP address (*Ethernet*), router (*Gateway*), and DNS servers. The tab also indicates whether or not these network settings have been manually configured, or retrieved automatically from DHCP server.

For cameras that are in a hybrid deployment with FortiRecorder, this tab also displays the IP address and firmware version of the FortiRecorder.

If your network administrator uses network access control such as MAC address filtering, the camera's MAC address is not located on this tab. Instead, see the *MAC Address* column in the list of cameras.

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

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera* .
3. Click *Manage Camera* and then select a camera and click *Setting* .
   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
   Alternatively, click the camera's thumbnail image and then click*Camera setting* in the upper right corner.
4. Go to the *Maintenance* tab and then the *Network* sub-tab.

Wi-Fi settings

If the camera supports a Wi-Fi connection, then wireless network settings are also available.

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera* .
3. Click *Manage Camera* and then select a camera and click *Setting* .
   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
   Alternatively, click the camera's thumbnail image and then click*Camera setting* in the upper right corner.
4. Go to the *Set up* tab and then the *Wireless* sub-tab.
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.

Setting	Description
	• *WPA Username* (Enterprise only): Enter the username to use for authentication. • *WPA Password* (Enterprise only): Enter the password of the username.

Firmware updates

If you did not enable automatic camera software updates (see Firmware Auto-upgrade on page 21), then when new software is available, you must update the camera manually.

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera* .
3. Click *Manage Camera* and then select a camera and click *Setting* .

   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.

   Alternatively, click the camera's thumbnail image and then click*Camera setting* in the upper right corner.
4. Go to the *Maintenance* tab and then the *Firmware* sub-tab.
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.

Storage settings and disk space usage

For the camera's local disk space usage, you can view statuses such as the following:

Item	Description
Status	Whether or not the disk is available.
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. This includes video clips for notifications and visual search. See also Delete Recording on page 33.

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 and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. Click *Manage Camera* and then select a camera and click *Setting*.
   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
   Alternatively, click the camera's thumbnail image and then click*Camera setting* in the upper right corner.
4. Go to the *Maintenance* tab and then the *Storage* sub-tab.
5. Click *Format*.

General settings

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera*.
3. Click *Manage Camera* and then select a camera and click *Setting*.
   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
   Alternatively, click the camera's thumbnail image and then click*Camera setting* in the upper right corner.
4. Go to the *Maintenance* tab and then the *General* sub-tab.
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 1minute.
Bluetooth	Click *Enable* for Bluetooth connectivity on the camera. This can be used for setup via the FortiCamera Mobile app (formerly called FortiRecorder Mobile). Use the slider available to control the amount of time that the camera's Bluetooth will search for connections. This button appears only if the camera supports Bluetooth connections.
System	Click *Reboot* to restart the currently selected camera. Recordings are interrupted until the camera reboots.

Image settings

Image resolution is configured separately, in Video recording settings on page 32.

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera* .
3. Click *Manage Camera* and then select a camera and click *Setting* .

   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.

   Alternatively, click the camera's thumbnail image and then click*Camera setting* in the upper right corner.
4. Go to the *Set up* tab and then the *Image* sub-tab.
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 1to 10.
Overlay	Enable to display the camera name and current date and timestamp as a watermark on the video image. See also Timezone on page 21. Because each person may have a different preference, your time display preference does not apply.
Privacy Window	If you want to exclude an area of the video (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. **Note:** Verify that the privacy mask does not overlap motion detection areas.

Video recording settings

If you have many cameras that require the same settings, instead of repeatedly configuring the same settings on every camera, you can configure a profile once in the organization, and then simply select it for each camera. See Video recording settings on page 16 and Schedules on page 17.

Otherwise you can configure the video recording settings separately for each camera.

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera* .
3. Click *Manage Camera* and then select a camera and click *Setting* .

   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.

   Alternatively, click the camera's thumbnail image and then click*Camera setting* in the upper right corner.
4. Go to the *Set up* tab and then the *Video* sub-tab.
5. Configure the following:

GUI item	Description
Select Profile	Enable to use a video profile, and then select it from *Video Profile*. Or click *New* to create a new profile. The video profile defines how the video will be recorded, such as schedule, resolution, and quality. See also Video recording settings on page 16. Disable to show all the settings below, and configure them for the camera individually, on this tab.
Recording Schedules	Select 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*, or click *New* to create a new schedule. See also Schedules on page 17. • *Never*: Never record video.
Resolution	Select an image resolution: *720P*, *1080P*, *2K*, or *5M*. This setting is available only if *Select Profile* is disabled. **Note:** A greater resolution reduces the maximum duration that can be recorded. Lesser resolution may be automatically used while viewing the live streams from multiple cameras in a video grid.
Quality	Select a suitable image quality: *Standard*, *Enhanced*, or *High*. A lower quality enables stronger compression and longer duration of recordings. This setting is available only if *Select Profile* is disabled.
Motion Only Recording	When enabled, recordings where no motion was detected are only kept for a short period of time.

GUI item	Description
	This setting is available only if *Select Profile* is disabled. **Tip:** Enable this option to reduce disk space usage if you do not require continuous recording.
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 29). This setting is available only if *Select Profile* is disabled.
Audio Recording	Enable to turn on the camera's microphone for live video streams and recordings. This setting is available only if *Select Profile* is disabled.

Night mode settings

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera* .
3. Click *Manage Camera* and then select a camera and click *Setting* .
   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
   Alternatively, click the camera's thumbnail image and then click*Camera setting* in the upper right corner.
4. Go to the *Set up* tab and then the *Night Mode* sub-tab.
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*.

Motion detection and AI recognition settings

All cameras can use motion detection to trigger recordings.

FortiCamera models with "-CA" in the name, such as FortiCam FB85-CA, also support AI-based features such as facial recognition and license plate recognition, and have settings for them. Metadata about recognized occurrences is transmitted to FortiCamera Cloud if the features are enabled, and if you have opened network ports for metadata.

1. From the organization and site dropdown menu at the top of the page, select the name of the organization that claimed the camera.
2. Go to *Camera* .
3. Click *Manage Camera* and then select a camera and click *Setting* .

   This button appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.

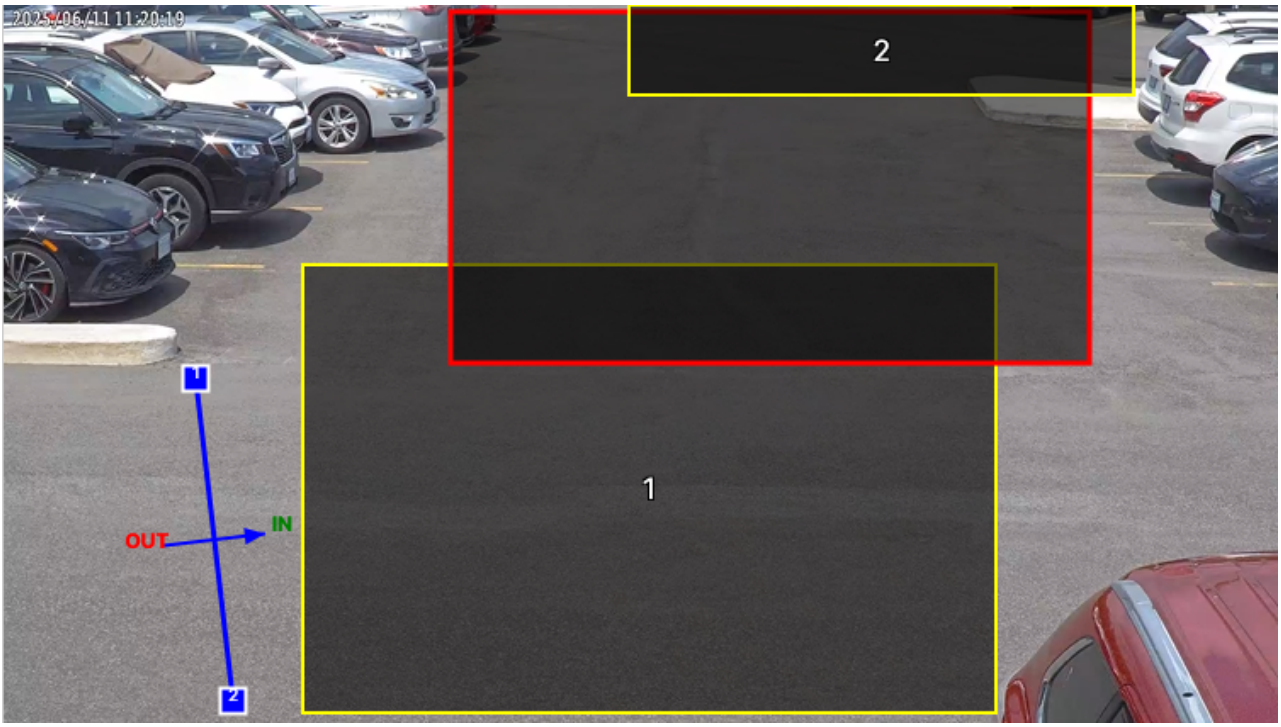
   Alternatively, click the camera's thumbnail image and then click*Camera setting* in the upper right corner.
4. Go to the *Set up* tab and then the *Detection* sub-tab.
5. In the *Motion* section, if you want to enable motion detection-triggered video recordings, enable *Detection* and then click + *Detection Window*.

   A semi-transparent rectangle outlined in **yellow** appears on the video image, indicating which area will detect motion. Multiple motion detection areas can be created. If you want to add another, click + *Detection Window* again.

   Drag all motion detection rectangles into place. Resize the rectangles by dragging the corners.

	Any motion detection area that either fully or partially overlaps any existing *Privacy Window* area may not function as intended.

	Avoid motion detection regions with, for example, blinking lights, animals, trees that move in the wind, or water ripples. Extra recordings will occur with no benefit. Retention periods may also be impacted.



Drag the *Motion Sensitivity* slider indicate how sensitive you want motion detection to be, and *Item Size* to indicate the percentage of pixels actively changing relative to the background in the motion detection area. If you want to trigger recording only when the camera detects a person or vehicle (not, for example, an animal, or trees moving in the wind), enable *Person Detection* and/or *Vehicle Detection*.(These settings only appear for camera models that support them.)

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 sensitive level or enable vehicle detection.

If you want to use motion detection to save disk space when no motion has been detected, see alsoMotion Only Recording on page 32.

6. In the *Analytics* section, configure whether or not the camera's built-in AI will analyze the motion detection video stream to recognize people, vehicles, etc., and store metadata about when they occur. This is required by features such as notifications, charts, and visual search. (These settings only appear for camera models that support them.)

Setting	Description
Analytics	In the below area, enable/disable person, face, and license plate detection and adjust the match precision level. **Note**: You may need to fine tune the precision level depending on your camera locations, light conditions and other factors.
Person / Vehicle	Enable to record metadata when people or vehicles are detected. This includes basic attributes such as car color, age, and gender, but not specific known faces from person profiles.

Setting	Description
	To record the direction (whether they are entering, leaving, or just moving nearby), click + *Crossing Line/Area*. A **blue** dividing line or rectangle appears. Select either *Area* or *Line* to change between them. Drag the corners to indicate which part of the view is inside (**IN**) or outside (**OUT**). The arrow indicates the direction of movement from inside to outside. If you want to indicate the opposite direction, select *Inversed*.
Human ID	Enable to record metadata when specific people are detected.
Face	Enable to record faces when faces are detected. *Persons of interest* require face recognition, and therefore cannot be enabled if *Face* is disabled.
Face ID	Enable to record metadata when specific faces are detected, such as persons of interest.
Likelihood	Select how similar a face must be in order to be detected as matching. *Wide* will match more faces, which can help with appearance changes such as haircuts and glasses, but may also include more incorrect matches.
License Plate	Enable to store metadata when vehicle license plates are detected. To specify which area will be analyzed for items that look like license plates, click + *Region of Interest*. A **red** rectangle appears. Drag the corners to adjust the area. *License plates of interest* require license plate recognition, and therefore cannot be enabled if *License Plate* is disabled.
Plate ID	Enable to record metadata when specific license plates are detected, such as license plates of interest.
Match	Select how similar a vehicle license plate must be in order to be detected as matching. *Wide* will match more, which can help with unusual license plates, but may also include more incorrect matches.
Motion	In the below area, enable/disable motion detection and adjust the detection sensitivity. **Note**: You may need to fine tune the detection sensitivity depending on your camera locations, light conditions and other factors.
Detection	Enable/disable motion detection. Then adjust the motion sensitivity, person sensitivity, and vehicle sensitivity. You can also add a maximum of three detection windows. And in each window, you can: • Specify the item size relative to the window size to detect. For example, 20 means 20% of the window size. • Enable/disable Person Detection. • Enable/disable Vehicle Detection. **Note**: In the detection window, if either person detection or vehicle detection is enabled, other motions will be ignored.

While analytics options are disabled, the camera does not use AI to detect **new** occurrences, but **existing** data is still kept, and can still be used by visual search unless you format the disk to erase the data. See also Storage settings and disk space usage on page 29.

Configuring user and administrator accounts

Like other FortiCloud services, user and administrator accounts for FortiCamera Cloud first must be created with FortiCloud Identity & Access Management (IAM) so that they can authenticate. Then the owner or administrators in your FortiCamera Cloud service can assign roles to authorize access to your specific sub-organizations, sites, and cameras.

To delegate responsibilities from the owner in a way that can scale as your business grows, administrators can create more administrator accounts with the same scope (organization or site). They cannot, however, give access to other organizations or sites.

FortiCamera Cloud REST API accounts and tokens are configured separately in FortiCloud IAM.

1. Go to *Management* .
   This menu item appears at the bottom left corner of the page, and only if you have owner, organization administrator, or site administrator permissions.
2. From the organization structure, select the organization or site that the new user will belong to.
3. Click the *User* tab.
4. Click *New* to create a new user, or select an existing user and click *Edit*.
5. Configure the following settings:

GUI item	Description
Name	Enter the name of the user. Spaces are permitted.
Email	Enter the email address of the user. Email addresses are not required to be unique. Each user can belong to multiple different organizations and sites.
Role	Either select one of the predefined roles: • *Organization Admin*: Can change the organization's and/or site's general settings and users (see *Scope and Access* and *Permission and Value*). Can view and download live and previously recorded videos from selected cameras at the assigned sites, including any associated notifications and visual search of recorded video. Cannot claim cameras and assign them to a site's inventory. • *Site Admin*: Can change the site's general settings and site's users. Can view and download live and previously recorded videos from selected cameras at the assigned sites, including any associated notifications and visual search of recorded video. Cannot claim cameras. Cannot change organization-level settings.

GUI item	Description
	• *Operator*: Can view and download live and previously recorded videos from selected cameras at the assigned sites, including any associated notifications and visual search of recorded video. Cannot manage the organization or site's users nor general settings. • *Monitor*: Only can view live video streams from selected cameras at the assigned sites. Cannot use visual search, notifications, or play previously recorded video. Cannot manage the organization or site's users nor general settings. or select *Custom User*and then define a role with customizable permissions. **Note:** For each scope (*Scope and Access*), the *Custom User* role can be defined differently. There is a maximum of one role customization per scope. **Note:** The *Owner* role also exists, but cannot be selected. Each organization can have only one account with the *Owner* role. This default role is assigned during the first login, when the owner creates their first organization. Organization owners have a special permission that cannot be granted to any other user: owners can claim cameras to make them part of the organization's device inventory. Please contact Fortinet Support if you need to transfer ownership of the organization.

6. If *Role* is *Site Admin*, *Operator*, or *Monitor*, mark the checkboxes of the sites that the user should be able to access. For *Operator* and *Monitor*, you can further restrict access if you want to allow them to use only specific cameras at those sites.
7. If *Role* is *Custom User*, settings appear so that you can grant permissions to each feature. Configure the following settings:

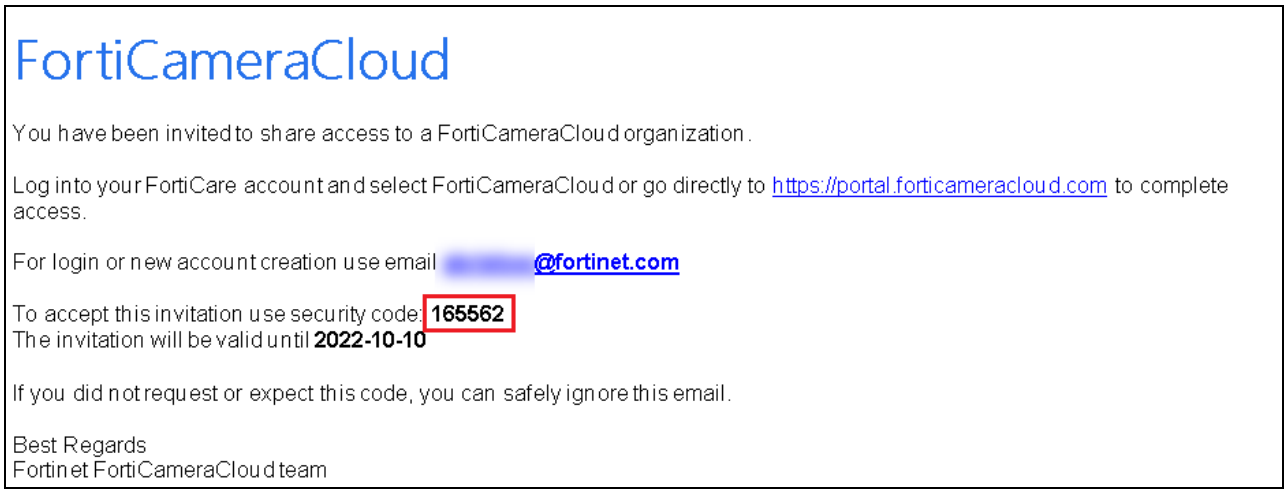
GUI item	Description
Scope and **Access**	Mark the *Access* checkboxes if you want to grant privileges for the role in each *Scope* (sub-organization or site).
Permission and **Value**	In the scope of an organization, there are permissions for: • *Organization Setting - General*: Organization and sub-organization settings such as the region, video profiles, and schedules. See also Configuring organizations on page 15. • *Organization Setting - User*: Users within the organization, including organization administrators. In the scope of a site, there are permissions for: • *Site Setting - General*: Site settings such as the timezone, camera firmware auto-upgrades, persons of interest, license plates of interest, and notification rules. See also Configuring sites on page 18 **Note:** This permission is not required by roles like *Monitor* that use the notifications and visual search, but do not configure the settings (the site's notification rules, persons of interest, or license plates of interest,

GUI item	Description
	etc.). • *Site Setting - User*: Users within a site, including site administrators. • *Camera Selection*: Cameras at the site. Also configure which camera operations are allowed in *Camera Video*. • *Camera Video*: Downloading and playing live and/or previously recorded video from a selected camera, including features that rely on those recordings such as viewing video clips in notifications and visual search. This setting does not appear if *Camera Selection* is *None*. • *Camera Setting*: Camera settings. This setting does not appear if *Camera Selection* is *None*. **Note:** This also includes permissions in *Camera Video* so that the user can test the effects of camera setting changes. For each *Permission* row, in its *Value*, select which privileges to grant. For most permissions, select either: • *Full*: Grant full read (view) and write (modify) permissions. • *Read*: Grant only read permissions. • *None* For *Camera Selection* permissions, select either: • *All*: All cameras belonging to the site. • *List*: Select this option and then click the *Choose* button that appears to select which cameras you want to permit to this user. Selectable cameras are determined by the site's inventory. • *None* For *Camera Video* permissions, select either: • *Export*: Grant ability to download video files and to play previously recorded and live video. • *Playback*: Grant ability to play previously recorded and live video. This includes features that require them, such as visual search and notifications. • *Live*: Grant ability to play only live video streams.

8. Click *Save*.
9. To email an invitation to the person, select that account and click *Share* 

and then click *Confirm*. (Before the person accepts the invitation — their *Status* is still *Invited* or *Expired* — if you have accidentally sent the invitation to the wrong email address or the verification code has been accidentally compromised, then you can click *Revoke*. Otherwise click *Delete* and recreate the account.)

   The *Status* column should show *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

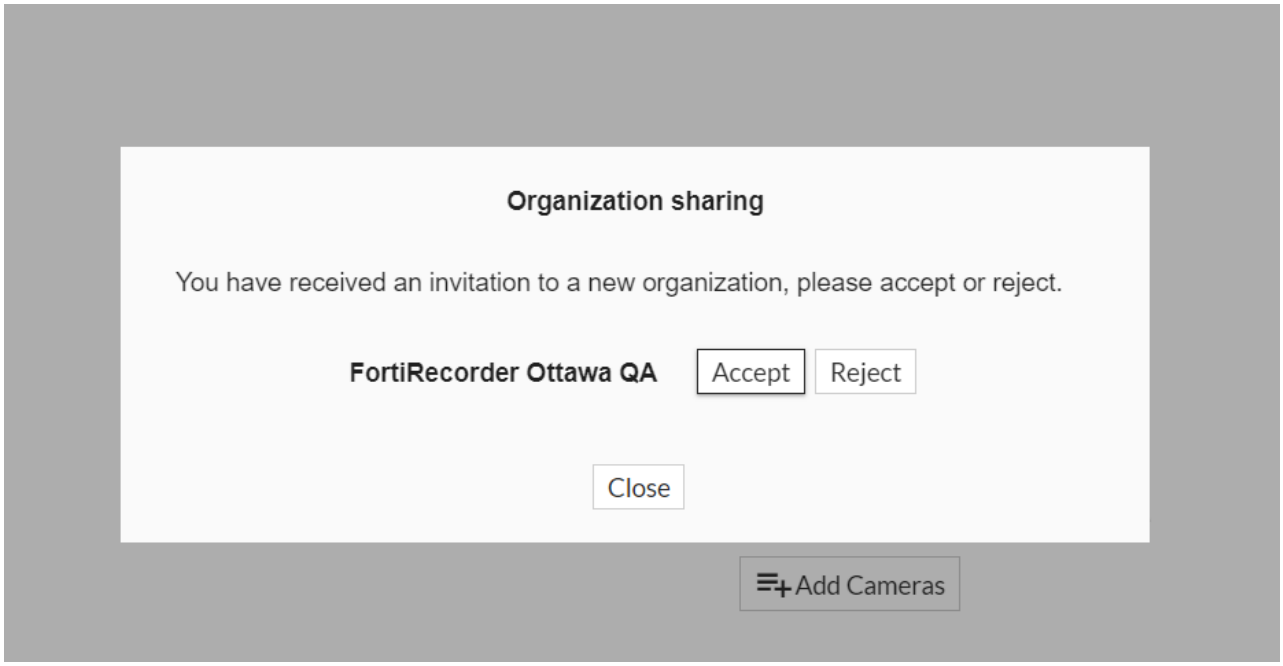
To accept this invitation use security code: **165562**
The invitation will be valid until **2022-10-10**

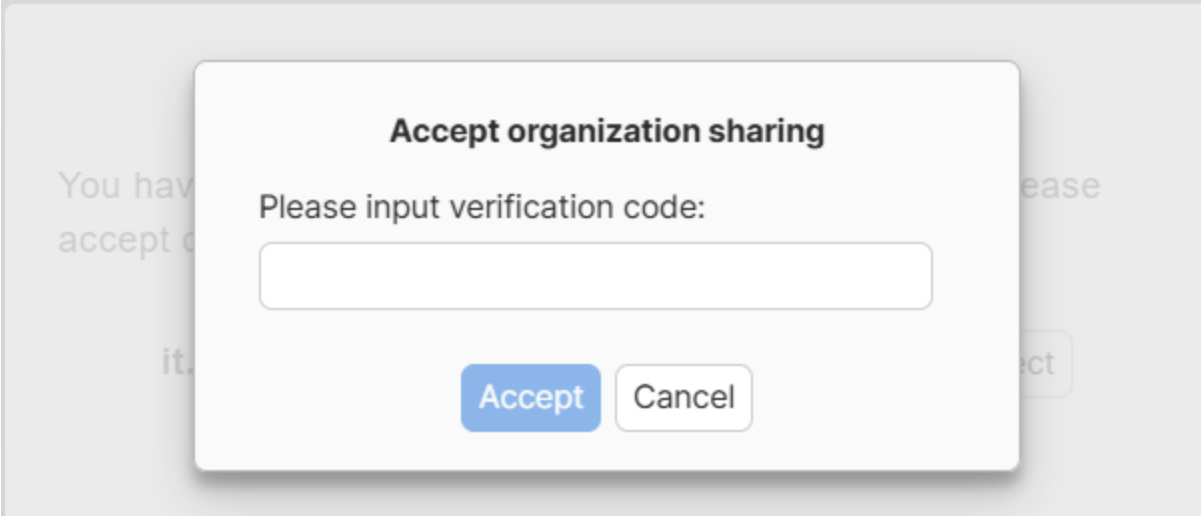
If you did not request or expect this code, you can safely ignore this email.

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 security code.

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





Preferences

You can set some preferences for your account in FortiCamera Cloud.

1. In the top right corner of FortiCamera Cloud, click your username, and then select *User Preference*.
2. Configure the following settings:

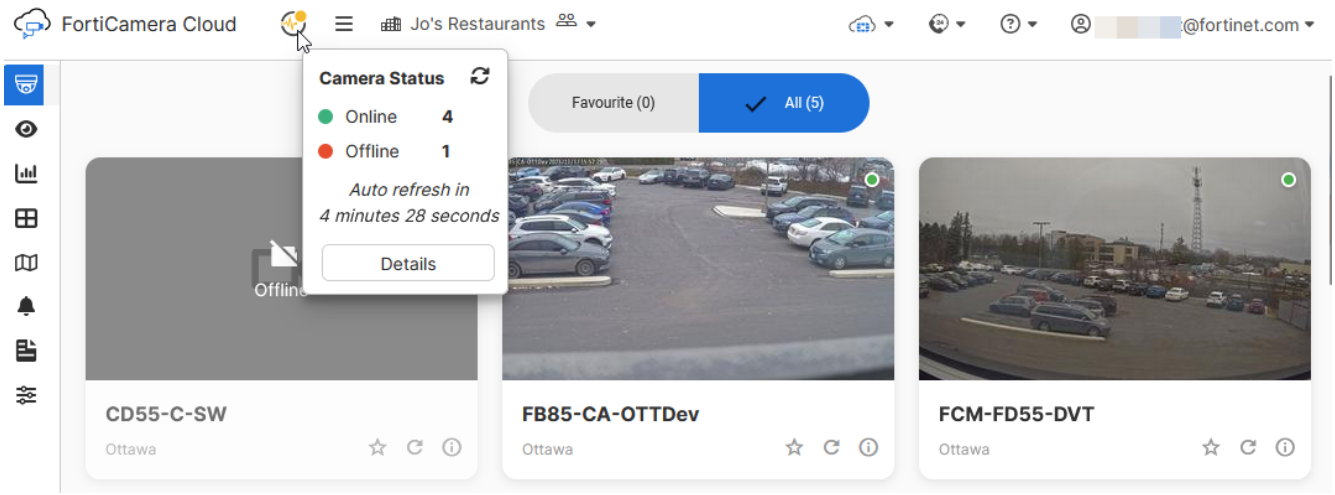
Setting	Description
Time Display	Select whether to display timestamps in a 12-hour (AM and PM) or 24-hour clock in various features such as charts, visual search, logs, and the video player timeline. See also Timezone on page 21.
Notification	Select how you want to use to receive notifications: • *Email*: At your account's email address. See Configuring user and administrator accounts on page 37. • *Mobile App*: In the FortiCamera Mobile app (formerly called FortiRecorder Mobile) for iOS or Android. The device where you receive notifications must be able to connect to the Internet. For performance tips and details for network administrators, see Appendix: Port numbers on page 60. The list of options does not include the notifications list in FortiCamera Cloud because it cannot be disabled and is always available. Notifications are defined for each site.

About camera status and connectivity

Cameras must be online to use their features in FortiCamera Cloud.

Once cameras are deployed to sites, owners and administrators can use notifications, logs, and the camera status indicator at the top left corner to monitor for issues such as temporary recording interruptions, or cameras being unexpectedly disconnected. Mouse-over the status indicator to get a summary of how many cameras have each status.

Other roles can also see a camera status dot on each thumbnail imagein their list of cameras so that they are aware, for example, if a camera is temporarily not available.



Camera Status	Description
Online	Connected recently, and has a configuration synchronized from FortiCamera Cloud.
Attention	Requires attention due to, for example, an: • invalid license • firmware upgrade now available • storage disk error • configuration synchronization error (for example, if you updated persons of interest, but settings were not yet pushed to the camera and therefore visual search cannot find those persons yet)
Offline	Not connected to FortiCamera Cloud since 6 days ago or less. If the camera should be online, verify that the camera is receiving adequate power. Your network administrator may need to adjust firewall or other settings to allow the camera to connect to the Internet or (for hybrid deployments) FortiRecorder. See Appendix: Port numbers on page 60.
Dormant	Offline for 7 days or more.

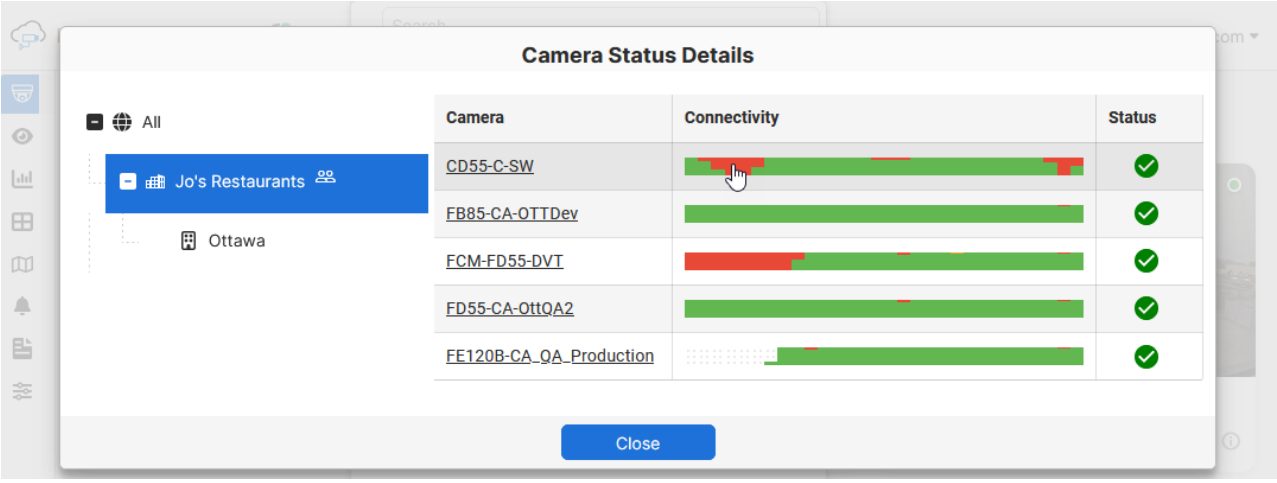
Camera Status	Description
	Note: Disabled cameras are not dormant. To find cameras that you have intentionally disabled, find their icons in the site's camera inventory instead.

To get camera network connectivity details:

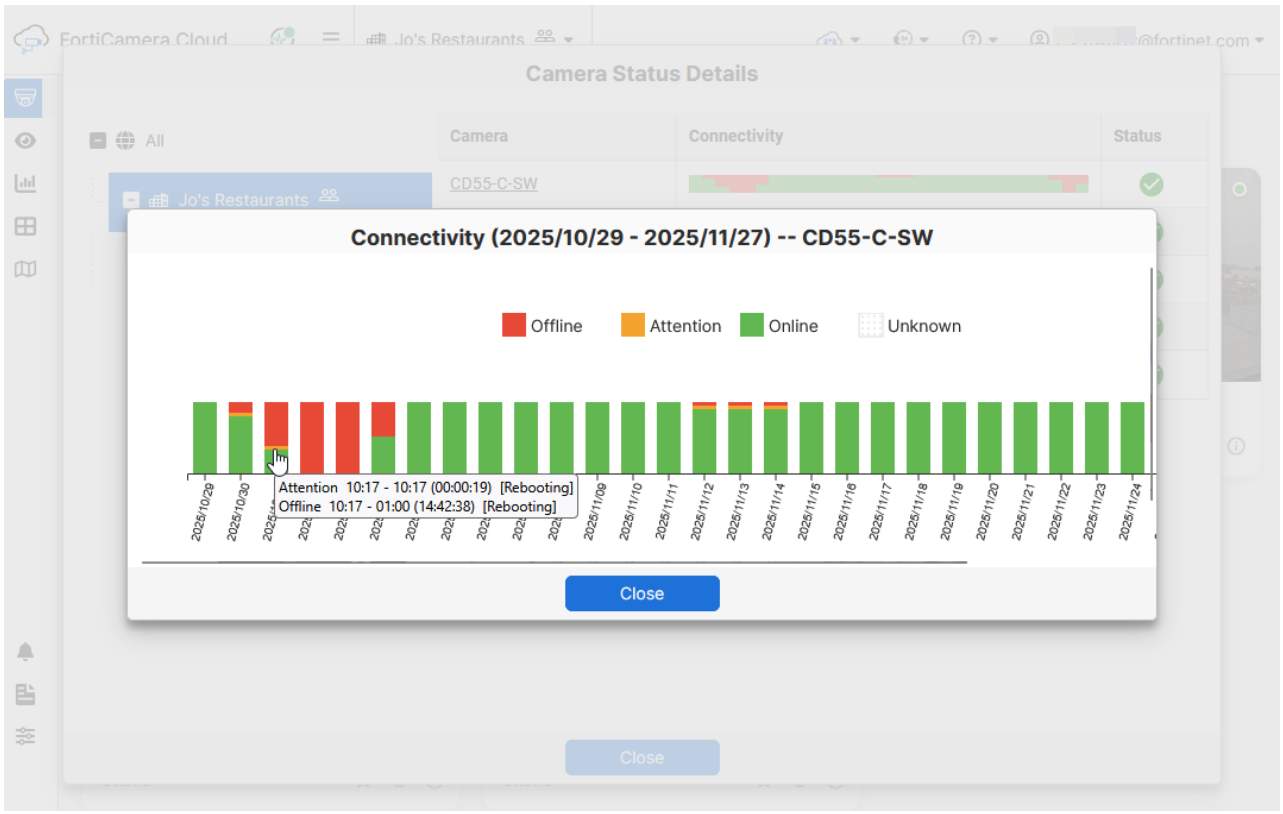
1. Open the camera status dropdown menu.
2. Click *Details*.
3. Click the name of the organization.

   Network connectivity graphs for each camera's *Connectivity* column indicate how much time that camera has been online during the current time period.

   Connectivity status names are often the same as the overall camera status names, but their meaning differs slightly. ***Attention*** indicates a temporary but expected network connection disruption due to a camera reboot or software update. ***Unknown*** (white with gray dots) is for new cameras when they have not connected to FortiCamera Cloud yet.



4. To get more information about an outage time range and cause, click the camera's *Connectivity* column, and then mouse-over or click the status. An explanation and time range appears in the tooltip.



Playing video from cameras

You can display the live video stream from any enabled 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.

1. Go to *Camera* .

   Initially, thumbnail images from all of your favorite cameras are displayed, regardless of organization or site.
2. If you want to play video from a camera that is **not** a favorite, click the *All* tab, or select a specific organization and site from the dropdown list at the top of the page.
3. To play video from the camera, click on a camera's thumbnail image.

   The live video stream should start to play. The timeline and controls also allow you to play previously recorded video.

   Color dot badges on the upper right corner of each thumbnail image indicate the camera status. If the live video stream is not available because, for example, the camera is rebooting, then a "!" icon in the lower right corner appears. When you hover your mouse over the icon, the reason appears in a tooltip.
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. Permissions may restrict which cameras you have access to select.
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.
Snapshot (button)	Click to download a PNG image file of the current frame in a live video feed or previous recording.
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 30 minutes (1800 seconds). This button requires the *Export* camera video privilege, or a role that is not *Monitor*. For details, see Configuring user and administrator accounts on page 37.
Mute / Unmute (button)	Click to enable or disable playing sound in the live video feed or previous recording.
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*.

GUI Element	Description
Favorite (button)	Click to include the camera when you view your list of favorite cameras. Click again if you want to remove the camera from the list of favorites.
Enter Search Mode (button)	Click to use visual search. This button appears only if the camera model supports AI-based recognition, and if those settings are enabled. See also Motion detection and AI recognition settings on page 33. This button requires the *Export* or *Playback* camera video privilege, or a role that is not *Monitor*. For details, see Configuring user and administrator accounts on page 37.
Camera Info (button)	Click to display information such as the serial number, model, license status, last time when the camera connected to FortiCamera Cloud (used to detect dormant or online status), MAC address (may be required for network access control on Wi-Fi access points or switches), and in *Type*, whether or not the camera is managed via *Cloud* (FortiCamera Cloud) or *FRC*(hybrid deployment with FortiRecorder).
Camera setting (button)	See Camera setup on page 25. This button requires the *Full* camera setting privilege, or a role that is organization administrator or site administrator. For details, see Configuring user and administrator accounts on page 37.
Live (button)	If this button is gray, click it to jump to the current time on the timeline and view the live video stream. The button is red while viewing the live video stream.
Timeline	Displays available recordings in **green** and motion detection events in **orange**. 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* • Click the date and time to directly jump to a specified date and time. Time ranges can be displayed as either a 12-hour (AM/PM) or 24-hour clock. See Time Display on page 41. Alternatively, click and drag the timeline. **Note:** Times on the camera timeline are relative to the time zone at the site. This may be different from your own local time zone. • *Previous Motion* and *Next Motion* to jump between different motion detection events • Fast forward and rewind +/-15 seconds • Select a playback speed, including fast and slow motion such as *1/8X*

GUI Element	Description
	and *4X* This area requires the *Export* or *Playback* camera video privilege, or a role that is not *Monitor*. For details, see Configuring user and administrator accounts on page 37.

Visual (activity) 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. To quickly find what you're looking for, search your video clips for more occurrences (also called visual search or "ReID") with similar visual attributes such as clothing color or faces.

Visual search with FortiCamera Cloud does not require training. Built-in, pre-trained AI models can recognize multiple visual attributes, such as bags, hats, vehicle type, color, and more.

Disabled cameras cannot be selected when using activity search. If you enable the camera later, activity search results will not include occurrences from the time when the camera was disabled. Similarly, search results do not include occurrences while AI-based detection of faces and/or human bodies was disabled on the camera.

For best results, 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 activity 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, activity search cannot find people with hats if only some of their head is visible.

Activity search results omit each camera's Privacy Window area, if any.

To search videos for visual attributes

1. On each camera, enable AI-based detection of criteria such as faces and/or human bodies.
   The camera will start to collect information about when it sees objects in those categories.

   Activity search requires camera models with built-in AI, such as FortiCam FD55-CA and FB85-CA.

   If some of your cameras do not support activity search, then you can still use activity search results to get timestamps and then manually find corresponding motion detection events in the timelines of other cameras.

   ---

2. Go to *Activity Search* .
   This feature is available only if you have a *Operator* role or greater, or video playback permissions.
3. Select a site.
4. Select either *People* or *Vehicle*.
5. In *Camera Selection*, select one or more cameras.
6. Select the search criteria such as *Vehicle Color*, and then click*Search*.
   Thumbnail images that look like your criteria are displayed.
7. If you want to play a video recording, click its thumbnail (either in the timeline or in the search results area).
   Time ranges can be displayed as either a 12-hour (AM/PM) or 24-hour clock. See Time Display on page 41. Times are relative to the time zone at the site. See Timezone on page 21.

Analytics

Charts, tables, and heatmaps (frequent paths of motion) can be used to visualize your motion detection statistics.

Motion detection triggers recordings of vehicles and people, and camera models that support this feature will automatically process the video stream so that they can try to recognize attributes such as vehicles or a person's gender and age. Charts can be made from this video metadata.

Before you use charts, however, you must configure some settings. This gives required metadata for some charts.

General steps to use charts are:

1. Enabling the cameras' built-in AI to analyze the video stream and record metadata for charts (see Motion detection and AI recognition settings on page 33)
2. Defining direction and inside and outside areas in the camera view (see Motion detection and AI recognition settings on page 33)
3. Wait for metadata to be recorded during the time range
4. Go to *Analytics*  , and then select an organization or site.

   This feature is available only if you have a *Operator* role or greater, or video playback permissions.

Each camera's Privacy Window, if any, hides part of the snapshot image that is used in heatmaps. However as long as part of the motion occurs in other areas such as the motion detection window, does not affect the total counts or direction of motion detected.

For data that shows the direction, you can select which to include:

- **IN**
- **OUT**
- **NC** — Neither in nor out. "Not counted" can occur if the person or vehicle remained in the inside or outside area, and never moved between them, and therefore the in/out direction is not defined.

Occupancy estimates are also based upon the direction. It counts of how many people or vehicles were estimated to be in the building site, based on entries and exits observed.

Time ranges can be displayed as either a 12-hour (AM/PM) or 24-hour clock. See Time Display on page 41.

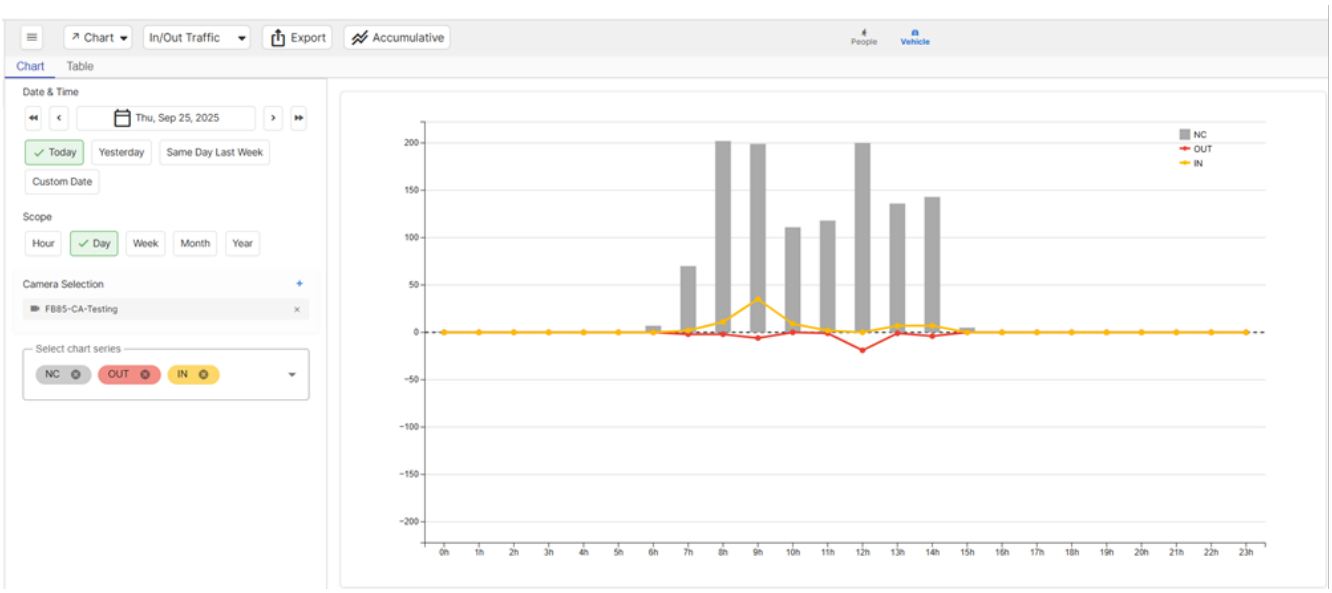
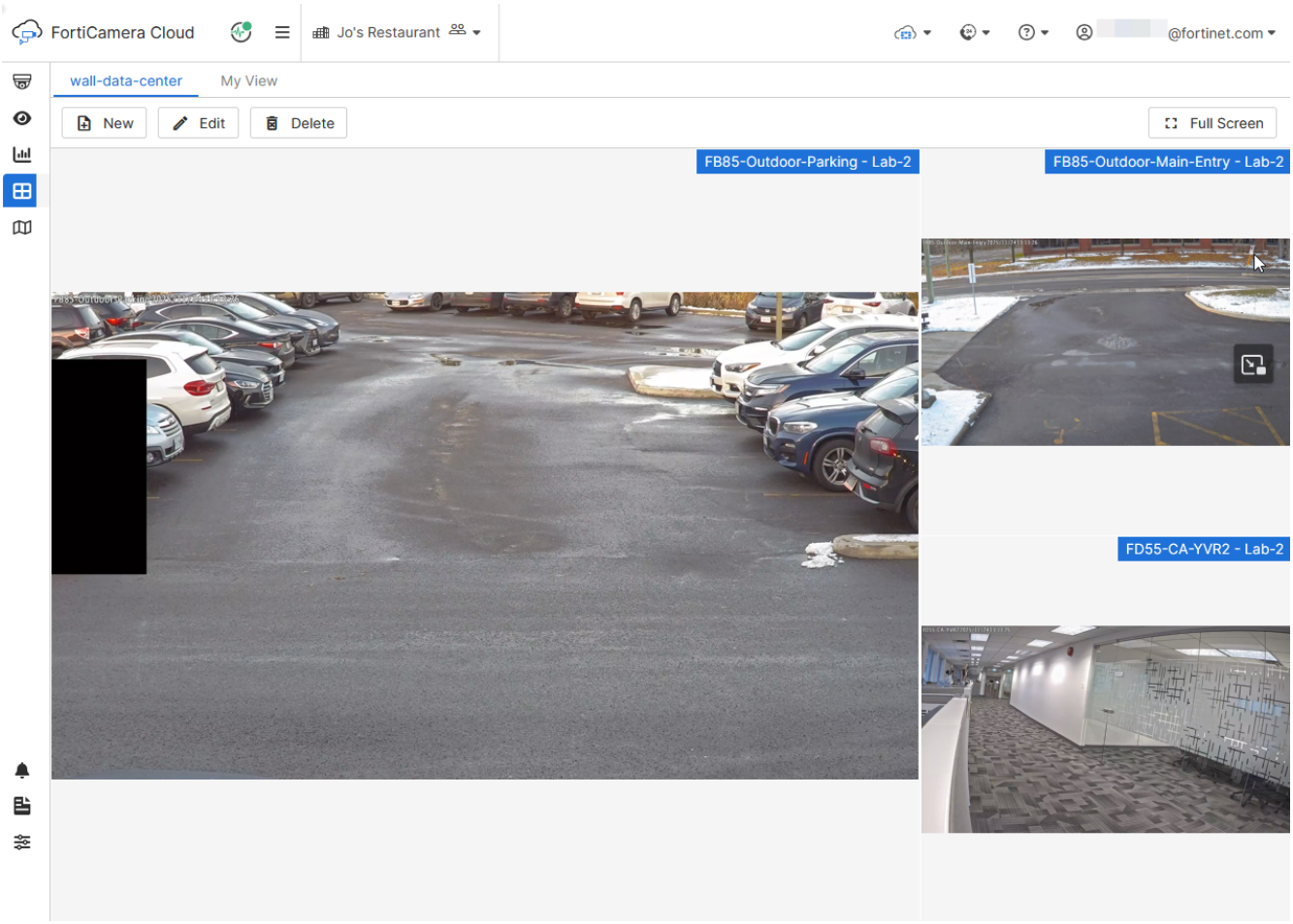


Chart
In/Out Traffic
Export
Accumulative
People
Vehicle
Chart
Table
Date & Time
Thu, Sep 25, 2025
Today
Yesterday
Same Day Last Week
Custom Date
Scope
Hour
Day
Week
Month
Year
Camera Selection
FB85-CA-Testing
Select chart series
NC
OUT
IN
NC
OUT
IN
200
150
100
50
0
-50
-100
-150
-200
0h
1h
2h
3h
4h
5h
6h
7h
8h
9h
10h
11h
12h
13h
14h
15h
16h
17h
18h
19h
20h
21h
22h
23h

Video grid

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. You can use this to create a monitor wall.



Low resolution video streams are automatically used when viewing in a grid layout. This ensures performance and efficient use of network bandwidth when you are viewing video from many high-resolution cameras at the same time. If you need to see a specific camera's video in more detail, you can double-click its pane in the grid to go to a dedicated video player.

1. Go to *Video Grid* .
2. Click *New* and configure the following:

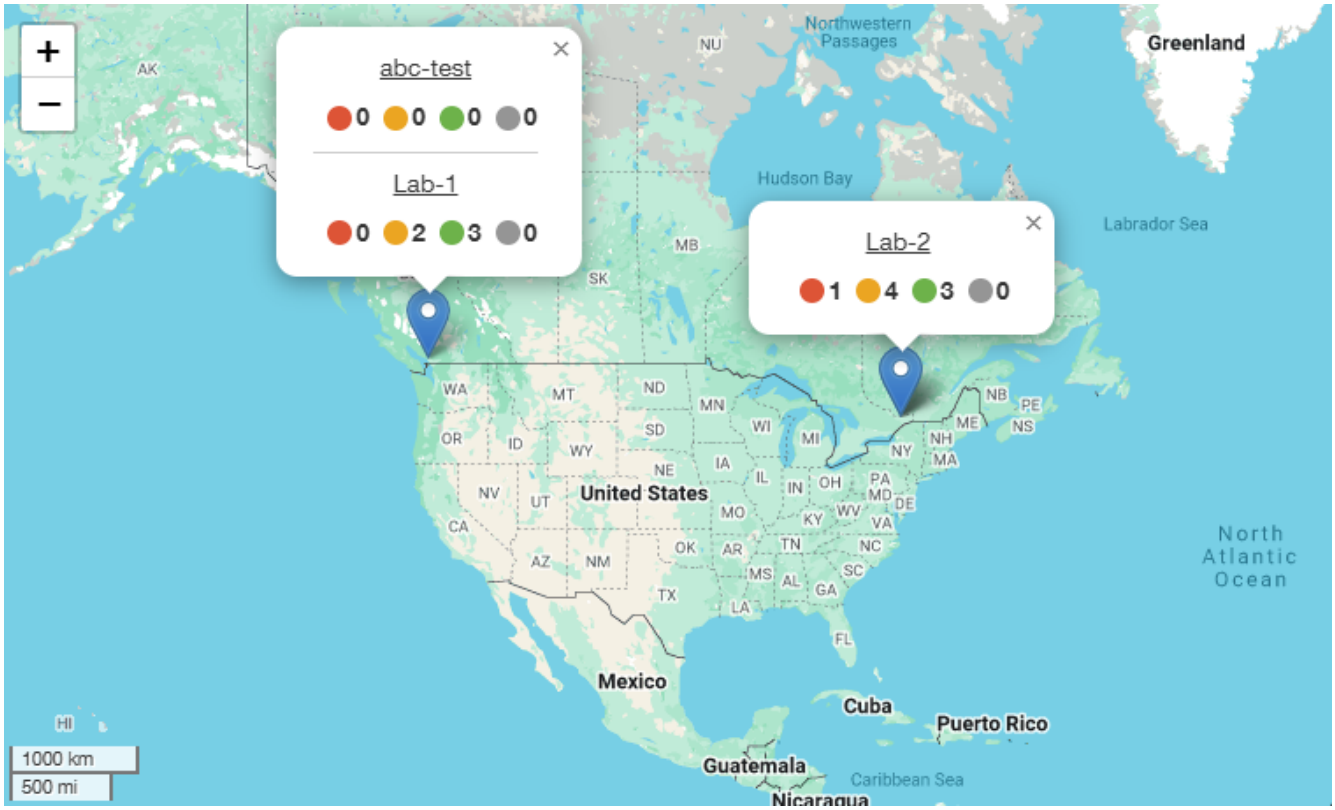
Setting	Description
Name	Enter a unique name.
Layout	Select the grid layouts for the view panes that will contain video from the cameras: • *1 x 1* • *1 x 2* (1 row, 2 columns) • *1 + 2* (1 large vertical view pane in the left column, and 2 smaller view panes in the right column) • *2 x 2* • *1 + 3* • *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*.

Map

Go to *Map* to view a map with all deployment sites.

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



Notifications

If a site is configured to send notifications for events such as:

- offline cameras
- motion detection
- persons of interest
- license plates of interest

then when an event occurs, FortiCamera Cloud will notify you.

Each user can choose their preferred methods to receive notifications. For details, see Preferences on page 41.

Maximum number of notifications in the list varies by how much storage is available to the cameras, and how long video recordings are retained. See Storage settings and disk space usage on page 29.

To view notifications

1. Go to *Notification* .

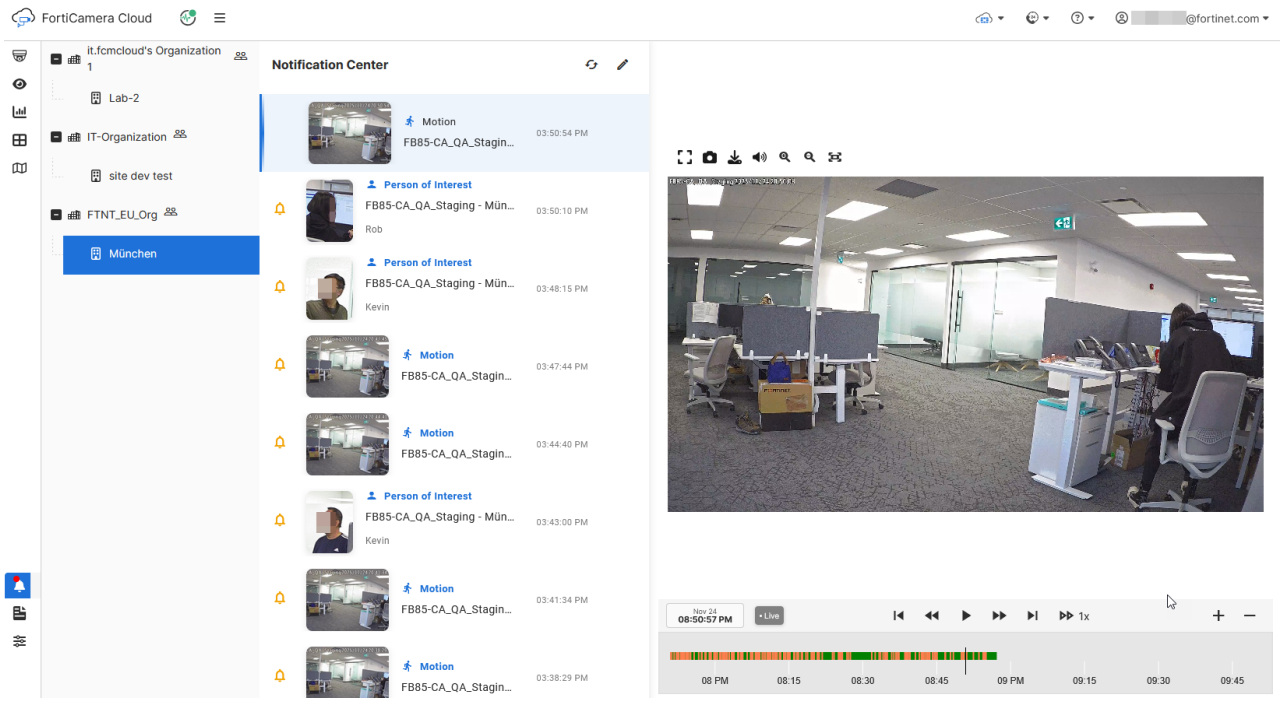
   This menu item appears at the bottom left corner of the page, and only if you have an *Operator* role or greater, or video playback permissions.

   New notifications since the previous time when you opened this menu are indicated by a red dot badge on the icon, and in the list by a yellow bell icon. This indicator is dismissed when you leave the page.

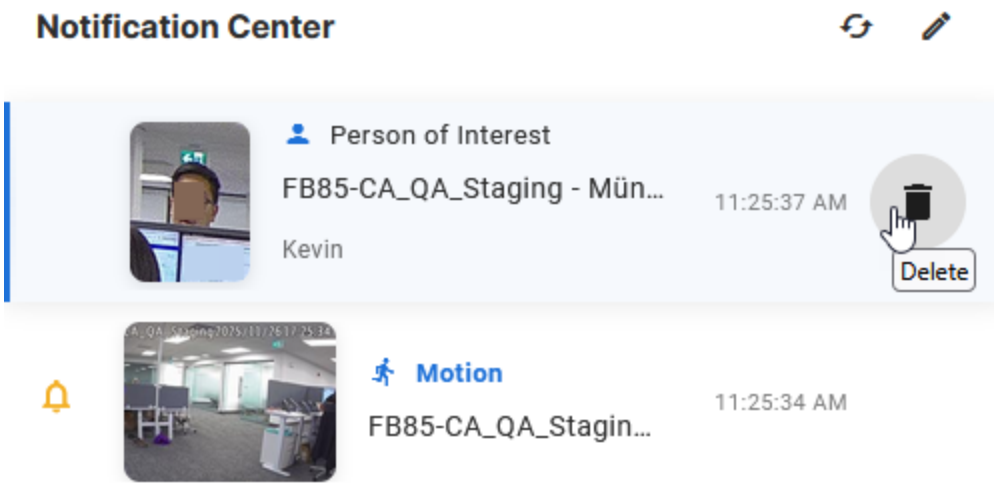
   Notification lists do not continually refresh, so if you have been viewing notifications for a few minutes and need to get newer notifications, click the refresh button in the top right corner of the dialog.

   Times in the list of notifications are relative to your local time zone. This ensures that events are sorted in the order that they really occurred, and not mixed up based upon whether each site has an earlier or later time zone. When you play a notification's video clip, however, the timeline will be relative to that specific site's local time zone.
2. To play a video clip, click its row in the notifications list.

   Corresponding video clips play automatically. Text color also indicates that the notification automatically toggles from **unread** to **read** status.

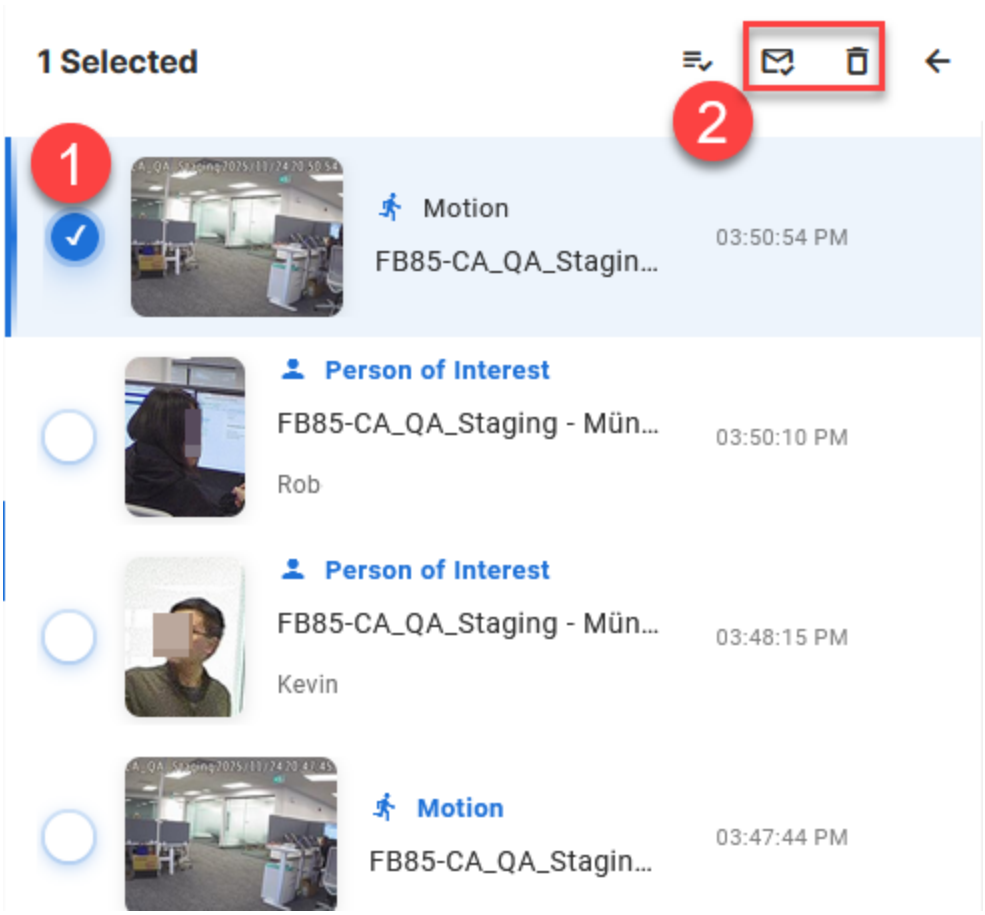


3. To delete a notification, mouse over its row, and click the trash button that appears.



Alternatively, to delete many videos or acknowledge them as read, click the edit button in the top right corner of the dialog, select those notifications or click the select-all button, and click the mark-as-read or trash button.

To cancel the multiple selection dialog, click the cancel button


1 Selected
1
2
Motion
FB85-CA_QA_Stagin...
03:50:54 PM
Person of Interest
FB85-CA_QA_Staging - Mün...
03:50:10 PM
Rob
Person of Interest
FB85-CA_QA_Staging - Mün...
03:48:15 PM
Kevin
Motion
FB85-CA_QA_Stagin...
03:47:44 PM

Logs

FortiCamera Cloud records log messages for security audit and troubleshooting purposes.

Searching logs

When you are viewing 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 *Log* .
   This menu item appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
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.

Displaying and sorting logs

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

1. Go to *Log*  .

   This menu item appears at the bottom of the page, and only if you have owner, organization administrator, or site administrator permissions.
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 Logs on page 57.
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.

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, adding cameras to 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.

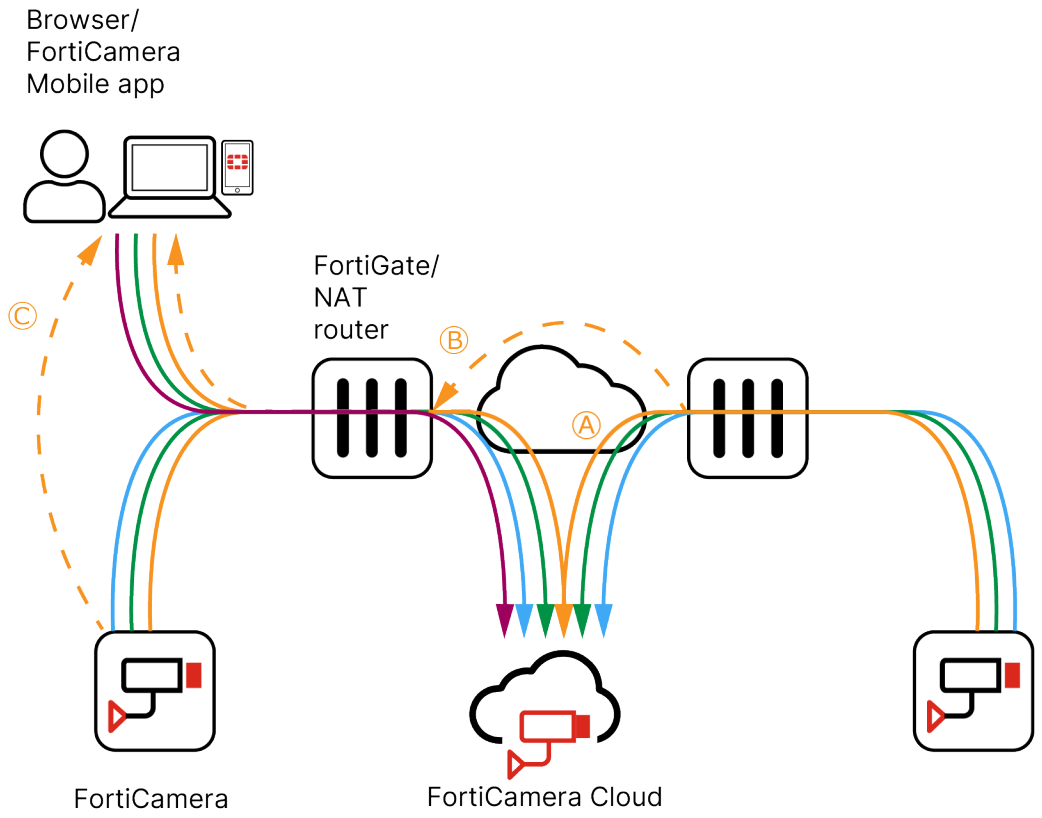
Log types

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)

Appendix: Port numbers

Firewalls and routers must allow specific network services between FortiCamera Cloud, your cameras, FortiRecorder (if any), and endpoint devices such as security staff computers. The following table for network administrators describes the required listening port numbers and protocols.



Source IP Address	Protocol	Destination Port Number	Purpose
• Users (FortiCamera Mobile app, web browsers) • Cameras	**UDP**	**123**	• Time synchronization (NTP).
• Users	**TCP**	**443**	• HTTPS for GUI access.
• Users • Cameras (or FortiRecorder)	**UDP**	**1024 to 65535**	• **All paths.** STUN and TURN for video stream route selection.

Source IP Address	Protocol	Destination Port Number	Purpose
Note: If cameras are **not** cloud native, then source IP addresses are FortiRecorder instead. It acts as a private relay. See also the FortiRecorder Administration Guide.			• **Path A only.** SRTP for metadata, audio, and video media streams.
• Users • Cameras (or FortiRecorder)	**UDP**	**1024 to 65535** **Note:** Destination IP addresses: Firewalls/ NAT routers in front of cameras/ users.	• **Path B only.** STUN for NAT traversal and video stream route selection. • **Path B only.**SRTP for metadata, audio, and video media streams.
• Users • Cameras	**UDP**	**1024 to 65535** **Note:** Destination IP addresses: Cameras/ users.	• **Path C only.** STUN for video stream route selection. • **Path C only.** SRTP for metadata, audio, and video media streams.
• Cameras	**TCP**	**10000**	• TLS secure tunnel for camera configuration, notifications, and queries. Does **not** include video streams.
• Users	**TCP**	**15673**	• Secure WebSocket (WSS) signaling, including to start a video stream.
• Cameras	**TCP**	**61614**	• TLS for signaling, including to start a video stream.

Source port numbers are ephemeral port numbers (1024 to 65535).

Destination IP addresses are always FortiCamera Cloud unless otherwise mentioned.

FortiCamera Cloud server addresses include:

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

All FortiCamera Cloud services are regionalized. Domain names may point to different nearby IP addresses in each geographic region. If you only allow traffic with known external services, but your firewall does not support addresses defined by fully qualified domain name (FQDN), then to get each FQDN's regional IP addresses, run lookup commands on a computer at each site. For example:

```
nslookup ntp1.fortiguard.com
```

Video streams can use multiple routes.

For fastest performance, allow traffic along all paths:

- **Path A: Through FortiCamera Cloud** — Through a TURN relay server, which then forwards through the router/firewall to you.
- **Path B: Through NAT** — Faster. Through NAT (router/firewall), which then forwards to you. Routers/firewalls must support NAT traversal with STUN.

  Example: You are behind a FortiGate with source NAT, and access a remote site's camera.
- **Path C: Direct** — Fastest. Local cameras stream video directly to you through a local OSI Layer 2 switch. No NAT occurs.

  Example: You access a camera in the same building.

After users and cameras connect to FortiCamera Cloud through path A, they receive each other's NAT or private IP address and port via the relay. They try better routes: path C and B. If it does not succeed, SRTP video streams use the default: path A.

Signaling and media streams may use different paths.

Many stateful firewall policies automatically allow **replies** if they have already allowed a TCP connection or UDP session to start.

If your firewall does not, then you must also configure it to allow packets in the opposite direction. This requires that you open ephemeral port numbers (1024 to 65535).

Normally, for path B, the first STUN packet to the router/firewall is dropped.

Yours or cameras' next outgoing STUN packet automatically adds a mapping to the router/firewall's session table (also called a hole punch) so that further incoming packets can reach their destination.

More dropped packets indicate a problem. Double NAT and symmetric NAT (some vendors also call it dynamic NAT, PAT, or carrier grade NAT) do not support STUN.

For details, see RFC 4787 (Endpoint-Independent Mapping).

Disable SSL/TLS deep inspection by firewalls such as FortiGate.

Currently cameras cannot be configured to trust a custom certificate authority (CA) or your firewall's server certificate, and so if you enable deep inspection, cameras' secure connections to FortiCamera Cloud will fail.

If you use network access control such as MAC address filtering, and need to view camera MAC addresses, see Camera setup on page 25.

www.fortinet.com