Genetec Clearance™ User Guide for Guests

Document last updated: December 18, 2024

Legal notices

Document information

Document title: Genetec Clearance™ User Guide for Guests

Original document number: EN.706.003-1.0.B(1)

Document number: EN.706.003-1.0.B(1)

Document update date: December 18, 2024

You can send your comments, corrections, and suggestions about this guide to documentation@genetec.com.

About this guide

This guide is intended for guest users of the Genetec Clearance™ system. This guide describes how to use the Genetec Clearance™ system to view cases.

Notes and notices

The following notes and notices might appear in this guide:

- **Tip:** Suggests how to apply the information in a topic or step.
- **Note:** Explains a special case or expands on an important point.
- **Important:** Points out critical information concerning a topic or step.
- **Caution:** Indicates that an action or step can cause loss of data, security problems, or performance issues.
- **Warning:** Indicates that an action or step can result in physical harm, or cause damage to hardware.

IMPORTANT: Content in this guide that references information found on third-party websites was accurate at the time of publication, however, this information is subject to change without prior notice from Genetec Inc.

Contents

1

Introduction to Clearance

Learn about the Clearance collaborative investigation management system.

This section includes the following topics:

What is Clearance?

Genetec Clearance™ is an evidence management system that you can use to help accelerate investigations by securely collecting, managing, and sharing evidence from different sources.

Using Clearance, you can import data from video surveillance systems, body-worn cameras, cell phones, in-car systems, computer aided dispatch (CAD), record management systems (RMS), and so on, so that evidence can be reviewed and shared within a single application. Clearance enables collaboration across independent agencies and private sector organizations, by helping investigators and invited third parties share their evidence online.

You can access the system from any standard browser, and no installation is required. All data and files that are imported to the system are automatically encrypted.

Clearance is also integrated with Active Directory, this means that organizations can use their existing Active Directory service to authenticate users and manage system access.

Advantages of Clearance

- Collect your digital evidence in one centralized location
- Manage who has access to the system and to case information
- Simplify investigations by collaborating with users
- Secure case information
- Find cases and files easily within the system

For a condensed overview of Clearance, see the Clearance Cheat Sheet.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

About Clearance information security

All data and files imported in Clearance are encrypted, and all communication with the platform is secure. These encryption and security measures ensure that sensitive data, files, and communications are only seen by users with the appropriate access.

Storage encryption

All data and files imported in Clearance are automatically encrypted using AES-256 with symmetric keys that are dynamically generated, ensuring that each file has a unique key. The Advanced Encryption Standard (AES) key is encrypted with a public key that can only be validated by users who have access to the files.

Communications encryption

All communication with the platform is secured using the Hypertext Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS) certificates signed by trusted certificate authorities such as Digicert. Clients validate the identity of the servers by using symmetric keys with TLS.

Protecting data integrity

All data imported in Clearance is validated with a digital signature. Digital signatures are based on a 512-bit Secure Hash Algorithm 2 (SHA-2) and are encrypted using an asymmetric private key to protect data integrity and restrict access to users with a valid public key. The system stores all original files without modifications.

User authentication

Clearance supports Windows Active Directory (AD) by using Microsoft Active Directory Federation Services or any system supporting the OpenID Connect standard. The authentication system is based on a passive authentication model with OAuth 2.0 and OpenID Connect.

Using an identity server (AD or others) means that you can connect directly to the authentication page for your organization. By using these authentication standards, the administrator can define how users are authenticated: password, tokens, biometric, or a combination of several of these techniques.

Clearance can use AD for user and password management, this means that organizations can enforce password rules and expiration requirements, multi-factor authentication, the number of failed log in attempts before deactivating a user credential, and so on.

Audit trails

All actions that are performed on cases and uploaded files are logged in the Clearance audit trail reports. These audit trail reports include detailed information about the following: the user, the activity type, the date of addition, change, removal of cases or files, and IP address accessed when the action occurred. System administrators can review audit logs of files, including when they have been created, imported, exported, shared, edited, redacted, and so on. Logs are also kept to provide details about when videos are viewed and by who.

About email notifications in Clearance

To inform users or guest users about specific events in Genetec Clearance™, email notifications are sent.

Email notifications are sent to users in the following situations:

- When an account is created
- When a user is added to a case
- When a user is added to a file
- When a password is reset
- When a case that a user has subscribed to is modified
- When a new request is made
- When a request you filed is complete
- When a case is transferred

IMPORTANT: E-mail notifications are sent from *noreply@clearance.network*. If you do not have this email in either your Inbox or Spam (or Junk) folders, contact your account administrator.

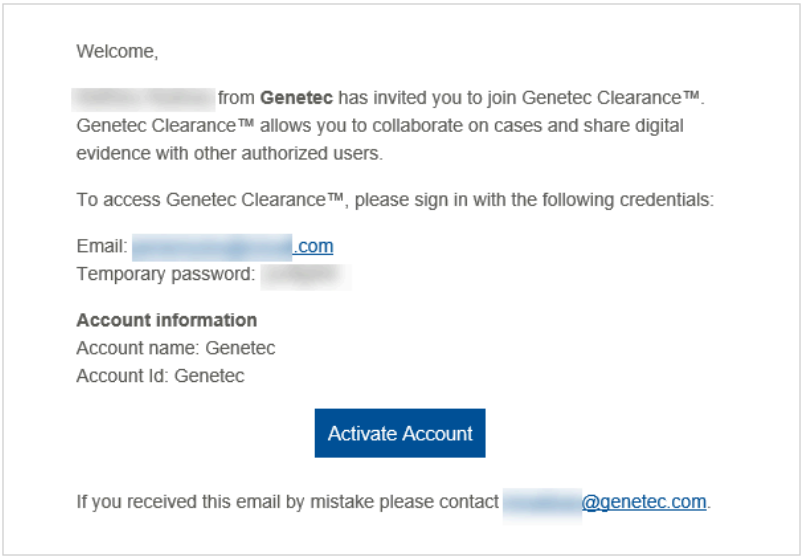
The email notification can also include one or more of the following:

- The *account ID*.
- The name of the person inviting you to a case or file.
- The name of the person who reset your password.
- The name of the person who transferred you a case and the organization they are a part of.
- The name of the person you transferred a case to and the organization they are a part of.

NOTE: The account ID is highlighted in **bold** in all email notifications.

Account created

An email with the subject "Invitation to join Clearance" is sent.


Welcome,

[redacted] from **Genetec** has invited you to join Genetec Clearance™. Genetec Clearance™ allows you to collaborate on cases and share digital evidence with other authorized users.

To access Genetec Clearance™, please sign in with the following credentials:

Email: [redacted].com
Temporary password: [redacted]

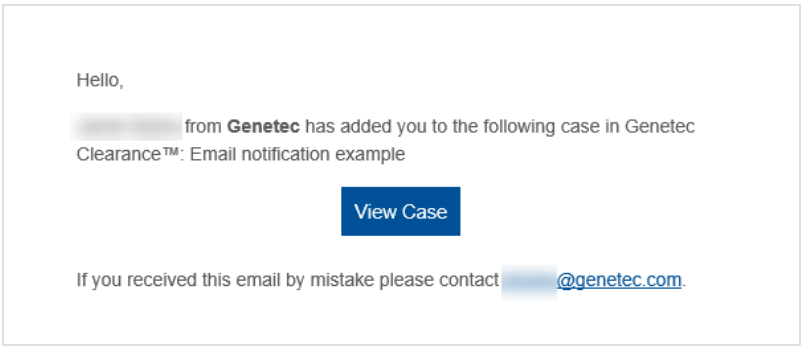
Account information
Account name: Genetec
Account Id: Genetec

Activate Account

If you received this email by mistake please contact [redacted]@genetec.com.

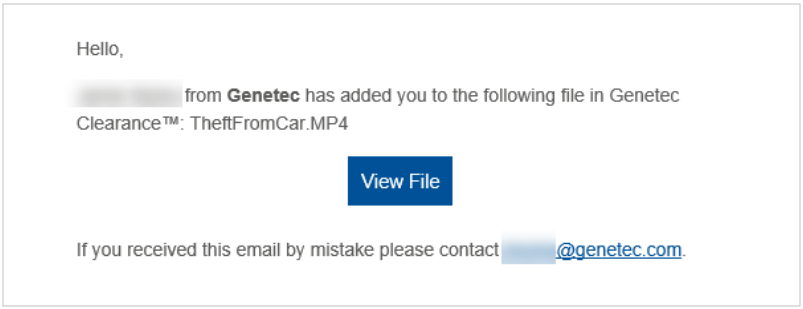
User added to a case

An email with the subject "*[username]* has added you to a case" is sent.



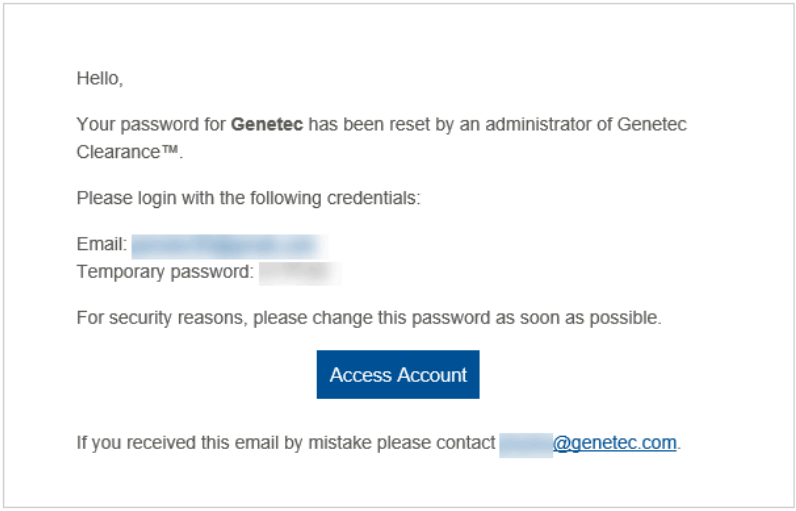
User added to a file

An email with the subject "*[email address]* has added you to a file" is sent.



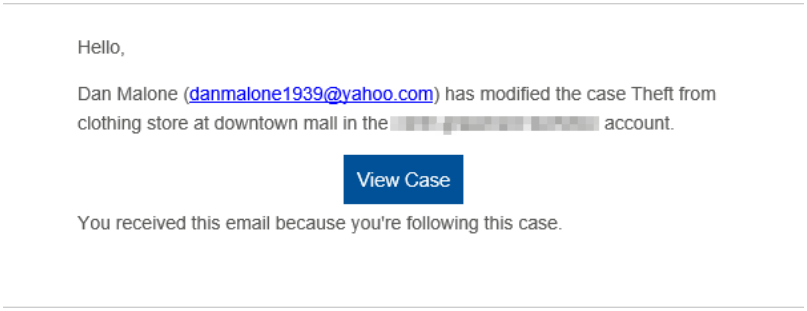
Password reset

An email with the subject "Your password has been reset" is sent.



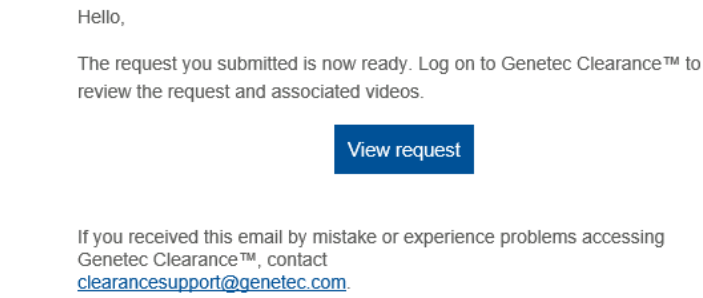
Case modified

An email with the subject "A case you're following has been modified | Case name" is sent.



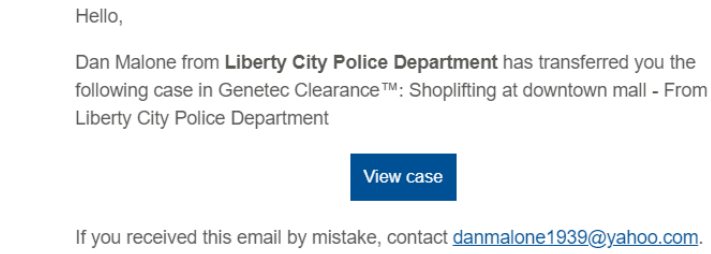
Video request ready

An email with the subject “A request you submitted is ready” is sent.



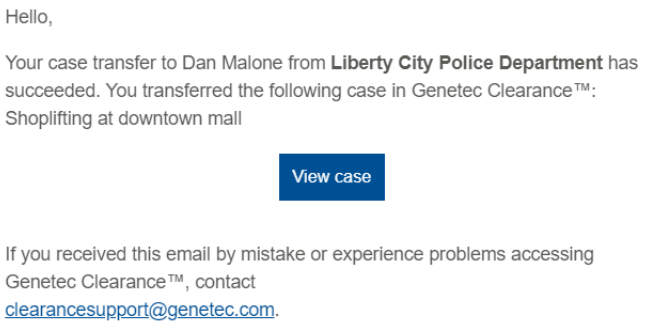
Incoming case transfer

An email with the subject “Someone has transferred you a case” is sent.



Case transfer successful

An email with the subject “Case transfer to someone succeeded” is sent.



Hello,

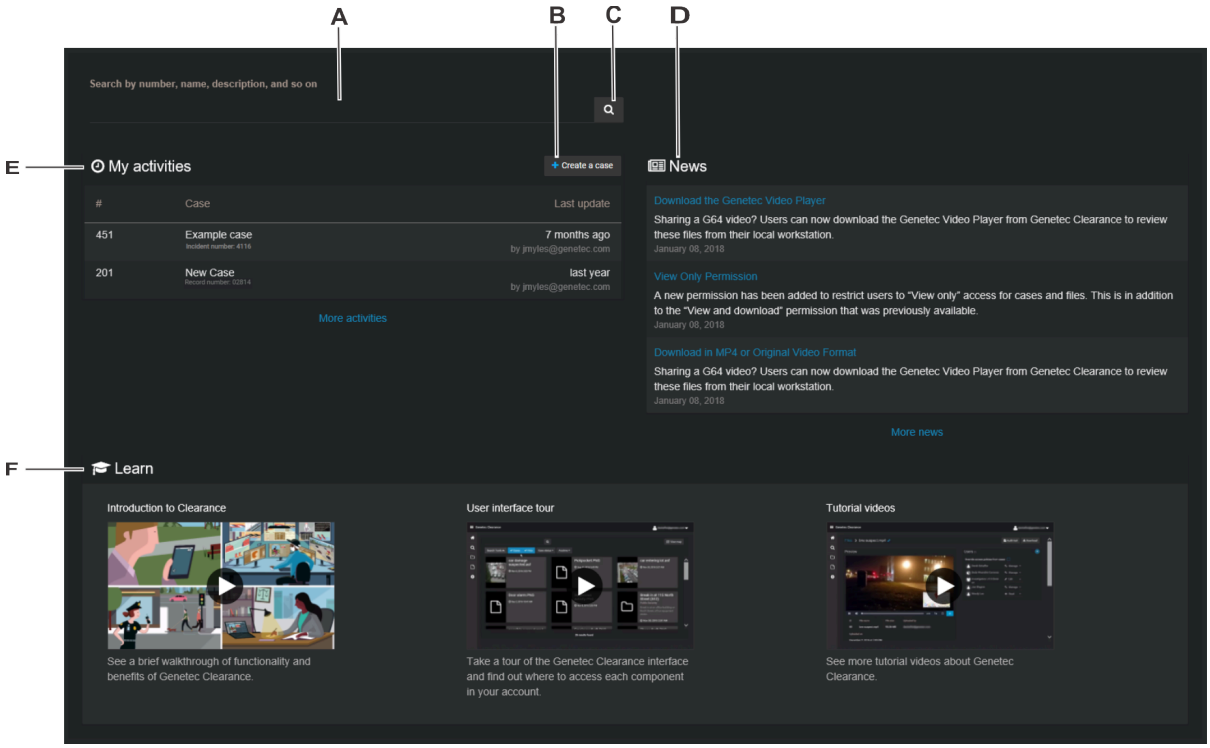
Your case transfer to Dan Malone from **Liberty City Police Department** has succeeded. You transferred the following case in Genetec Clearance™: Shoplifting at downtown mall

View case

If you received this email by mistake or experience problems accessing Genetec Clearance™, contact clearancesupport@genetec.com.

Overview of the Home page

On the *Home* page, you can create a case, search for cases or files, or view recent case or file activity. From the *News* section you can gain an awareness of new functions as they become available. From the *Learn* section, you can access tutorial videos and additional learning content.



NOTE: Menu tab options in the left navigation bar are not displayed in the *Home* page for Guest user accounts.

The *Home* page includes the following:

A	**Search box**	Enter keywords to help you find a case or file. You can search by case number, file name, description, and so on.
B	**Create a case**	Create a new case.
C	**Search button**	Open the *Search* page. The search results only show cases or files that contain your keywords.
D	**News**	Visit the *News* section to learn about new functions or important announcements as they become available. • Click **More news** to display all news items. • (Optional) Click a news item to display additional related information if available.

E	**My activities**	Check recent case or file activity. • Click a case or file to open the *Case* or *File* page. • Click **More activities** to display all activities. **NOTE:** For Guest users *My activities* only displays a list of the cases or files that have been shared with the Guest user.
F	**Learn**	Browse learning content. Click a thumbnail to watch a tutorial video or access additional learning content.

2

Getting started

Learn how to log on, log off, and change languages in Clearance.

This section includes the following topics:

Logging on to Clearance

After you have activated your user account through the activation link, you can log on to your Clearance account to view and manage evidence.

Before you begin

Make sure that you have done the following:

- Enabled cookies in the web browser that you are using
- Activated your Clearance account by clicking on the activation link in your email

Procedure

1 Using your web browser, select the required host as detailed in your account activation email:

- Host 1: or https://www.clearance.network (US)
- Host 2: https://eu.clearance.network (Europe)
- Host 3: https://au.clearance.network (Australia)
- Host 4: https://usgov.clearance.network (US Government)
- Host 5: https://ca.clearance.network (Canada)

2 On the *login* page, enter your email address and click **Login**.

You are redirected to your user account's sign-in page.

3 (Optional): Select an account if required.

- The account ID is shown in the URL at the top of every page.

  For example, *https://hostname/accountid/currentpage*.
- The account ID can change depending on the account that is logged in.

TIP: You can switch accounts at any time by clicking **Change account** from the account options under the user ID.

The *Home* page is displayed and you are ready to use Clearance.

Logging off from Clearance

To exit from Clearance, you can log off from your user account.

What you should know

You are logged off the system automatically after a specified period of inactivity. The inactivity period varies depending on your environment configuration.

To log off from Clearance: At the top of the page, click your name, and then click **Sign out** from the drop-down menu.

TIP: After you are signed out of your account, ensure that you close all browser windows.

Changing language settings in Clearance

To change the language in Clearance you must update your browser language settings.

Procedure

Changing language settings in Google Chrome:

1 In Google Chrome browser, Click **More** (⋮) in the top right of the browser session.

2 Click **Settings**.

3 Scroll to the bottom of the *Settings* page and click **Advanced**.

4 Scroll to the **Languages** section and click the down arrow.

5 Click **Add Languages** to add the language that you require.

6 Click **More** (⋮) .

7 Click **Display Google Chrome in this language** and click **RELAUNCH**.

The Clearance user interface can now be displayed in the browser language that you selected.

3

Using Clearance

Learn how to use the Clearance collaborative investigation management system.

This section includes the following topics:

Activating your account

To begin using Clearance, you must activate your account directly from the email that contained the invitation to join the site.

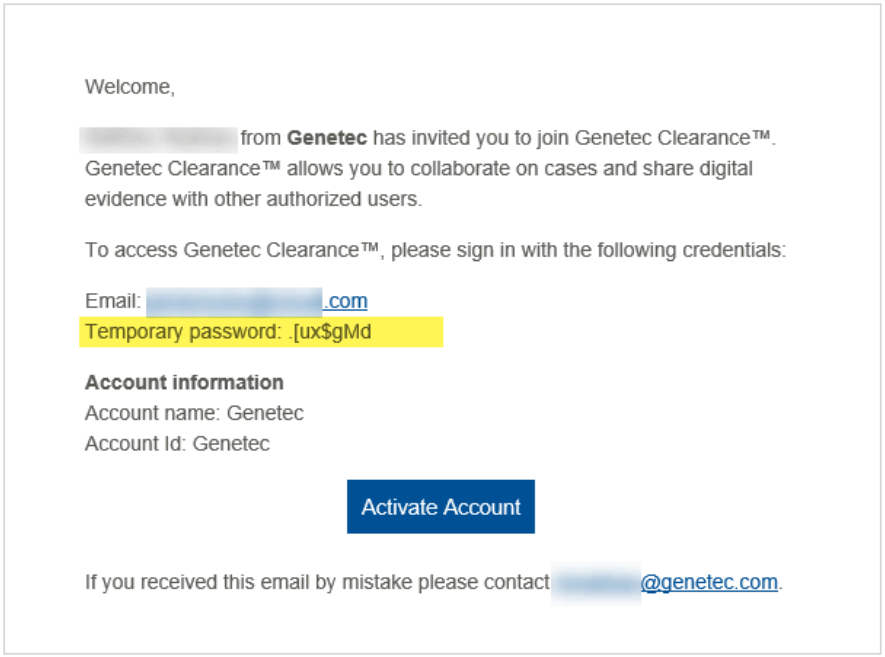
Before you begin

Make sure that you have a secure connection to the web.

Procedure

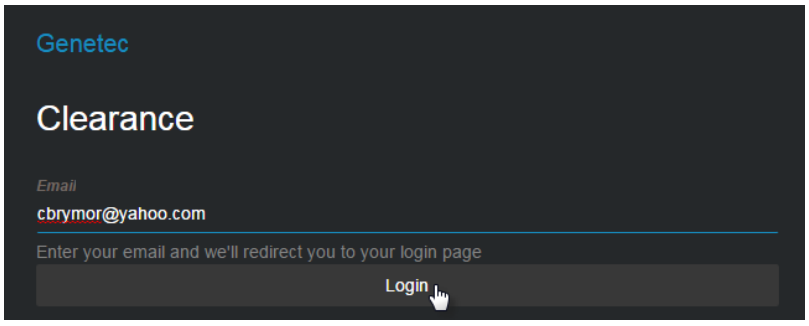
1 Sign in to your email account.

2 In your *Invitation to join Clearance* email, click **Activate Account**.



IMPORTANT: This e-mail is sent from *noreply@clearance.network* to help administrators setup their spam filters. If you do not have this email in either your Inbox or Spam (or Junk) folders, contact your account administrator.

3 On the Clearance site, enter your email address and then click **Sign in**.



You are redirected to *https://login.microsoftonline.com*.

4 On *https://login.microsoftonline.com*, enter your temporary password and then click **Sign in**.

If you cannot sign in, click **Can't access your account?** to reset your password.

NOTE: If you are logging in using an Active Directory account, contact your Active Directory system administrator for assistance.

5 Enter a password, and then click **Update password and sign in**.

The homepage opens.

Your account is activated. You can begin using the system.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Permission levels

Permission levels in Clearance are used to define the level of access granted on a case or a file. The different permission levels include *View only*, *View and download*, *Edit*, and *Manage*, and they can be granted to an integration, user, group, or department.

- **Manage:** Full access to a case or file. For cases, users can create cases, view and edit case details, download files, delete or restore files, share, and change access policies for the case. For files, users can view, edit, download, delete, restore, share, and change access policies for the file.
- **Edit:** For cases, users can create cases, view and edit the case details, and download files but cannot share cases with others or change the case access policies. For files, users can view, edit details, and download the files but cannot share cases with others or change the file access policies.
- **View and download:** For cases, users can create cases and view the case information, and download files but cannot edit or share the case with others. For files, users can view and download files but cannot edit or share files.
- **View only:** For cases, users can create cases and view the case information, but cannot edit or share the case with others. For files, users can only view files.

The following permission levels are used in Clearance:

Privilege	View only	View and download	Edit	Manage
Case permissions				
View cases	✓	✓	✓	✓
Create case summary report			✓	✓
Edit cases			✓	✓
Add files to a case			✓	✓
Share cases				✓
Add users to a case				✓
Remove users from a case				✓
Create file request				✓
File permissions				
View files	✓	✓	✓	✓
Download files		✓	✓	✓
Create and edit tags and fields			✓	✓
Share files				✓
Add users to a file				✓
Remove users from a file				✓

NOTE: Users with *View only* permissions for a case will not be able to view PDF files included in the case. .

Security policies

Account administrators can provide users with additional privileges in the Configurations menu Security Policies page.

- These policies are separate from the *Manage*, *Edit*, *View and download*, or *View only* permission levels specified for users in cases or files.
- Some security policies also require users to have *Manage* permission for cases or files affected by the policy. For example, the ability to view audit trails, protect cases, and delete cases.

Security policy	View only	View and download	Edit	Manage
Features that require security policies				
Access files not associated with any case[1]	✓	✓	✓	✓
View audit trail				✓
Protect case				✓
Protect file				✓
Delete case				✓
Delete file				✓
Share cases with users	✓	✓	✓	✓
Access audit trail				✓
Create eDiscovery receipt				✓
Hide visual watermark	✓	✓	✓	✓
Manage devices[2]				
Restore cases[2]				
Restore files[2]				

[1]Account administrators can specify the permission level that each user or user group has for files not associated with any case.

[2]Users can restore cases and files from the recycle bin or manage devices regardless of their case or file permission levels.

NOTE: Access to security policies can only be granted to regular users and is not available for guest users.

Video Request Policies

Video requests are managed using security policies and the following applies:

- Guest users can submit video requests (if invited).
- Account administrators can create or modify video request policies.

Video request policy	Default value	Where can you set this ?
Export video before approval	Disabled	In the **Configurations** > **Video request policies** page
Manage and invite requesters	Account administrators	In the **Configurations** > **Video request policies** page
Approve video requests	Account administrators	In the **Configurations** > **Video request policies** page
Auto-approve video requests	Account administrators	In the **Configurations** > **Video request policies** page
Default access policy for all video requests	Account administrators (*Manage* privilege) and Requester (*View and download* privilege)	In the **Configurations** > **Video request policies** page
Manage video request forms	Account administrators	In the **Configurations** > **Video request policies** page
Submit video requests	Account administrators and regular users	On the *User* page in the *Privileges* section.

Uploading files to cases

To share digital evidence with other authorized investigators, you can upload videos, media, and other file types to new and existing cases. You can then view, download, or edit the files.

What you should know

You can add up to 5000 files to a case, regardless of the folder or subfolder location. Cases can have unlimited folders or subfolders.

Video files are converted to MP4 files during upload. If the file format is not supported the upload might fail. Depending on the size of your file, the upload might take a few minutes.

Procedure

1 Open an existing case.

2 In the *Files* section, click and select one of the following:

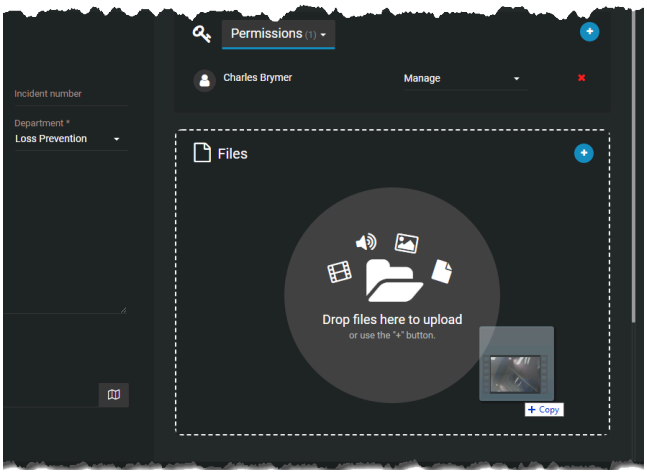
- **Add files from computer**
- **Add files from Clearance**
- **Create folder**

NOTE: The **Add files from Clearance** option is not available for guest users.

3 If you selected **Add files from computer**, do the following:

a) Select the files you need using one of the following methods:

- Select files that are saved on your local or network drive.
- Drag files into the **Files** field of the case.



b) After selecting the files you need, click **Open**.

c) (Optional) To remove files that you no longer require, click **More** ( ) and click **Remove**.

The file is removed from the case, but remains in the system and can still be searched, edited, viewed, and downloaded.

4 If you selected **Add files from Clearance**, do the following:
   a) In the *Add files to case* dialog box, select the required files by clicking **Add to case**.
   b) (Optional) To filter results and identify files to add to a case, click the **Search criteria** menu and then click **Add to case**.
   c) (Optional) To remove files that you no longer need, click **Remove from case**.
   d) Click **Done**.

5 If you selected **Create folder**, do the following:
   a) Enter a folder name and click **Create**.
   b) (Optional) Create any additional folders or subfolders that you require.
   c) (Optional) Click **More** ( ) next to a file or folder to move, rename, or remove them as required.

   NOTE: Click **Subscribe** to receive updates when new files are added to the case.

The files are now associated with the case, and users assigned to the case can view, edit, and download the file.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

File formats you can preview in Clearance

A file in Clearance is a piece of digital evidence, such as a video, image, document, or other type of file. Files can be grouped within one or more cases.

If the file format is not listed here, you must download the file to preview it.

Video formats

The following video formats can be previewed in Clearance:

- ASF (.asf)
- AVI (Uncompressed 8 bit/10 bit) (.avi)
- AV3
- FLV with H.264 and AAC codecs (.flv)
- G64 (g64)
- G64x
- GXF (.gxf)
- Matroska (.mkv)
- MP4 (.mp4 and .m4v)
- MPEG2-PS, MPEG2-TS, 3GP (.ts, .ps, .3gp, .3gpp, .mpg)
- MXF (.mxf)
- QuickTime (.mov)
- Windows Media Video (WMV) (.wmv)

NOTE: Certain formats, such as .avi, .asf, and .G64, are container file formats. Because they can contain unsupported media files, it is possible that certain videos in these formats are unsupported by the media player.

Extended video format library

The extended video format library is included by default with all Plan 600 and Plan 1000 accounts. It can also be purchased as an add-on with Clearance Plan 100 and Plan 200 subscriptions.

NOTE: Encrypted files can be shared, but not previewed in Clearance.

Audio formats

The following audio formats can be previewed in Clearance:

- MP3 (.mp3)
- WAV (.wav)

Image formats

The following image formats can be previewed in Clearance:

- Bitmap (.bmp)
- GIF (.gif)
- JPG (.jpg)
- JPEG (.jpeg)
- PNG (.png)

NOTE: Thumbnail previews are displayed in the *Case* page, *Evidence preview* window, or search results for the following files: BMP, PNG, JPEG, GIF, Icon, and MP4.

Document formats

The following document formats can be previewed in Clearance:

- Portable Document Format PDF (.pdf)

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Reviewing media

After media files have been uploaded, you can play them from either the file page or the evidence player page. You can also play videos with GPS trail location data, if GPS data is available.

Procedure

To watch uploaded media files from the *Case* page:

1 From the *Case* page in Clearance, click a file.
The evidence player opens.

To watch uploaded media files from the *File* page:

1 From the Clearance search page, open a file.

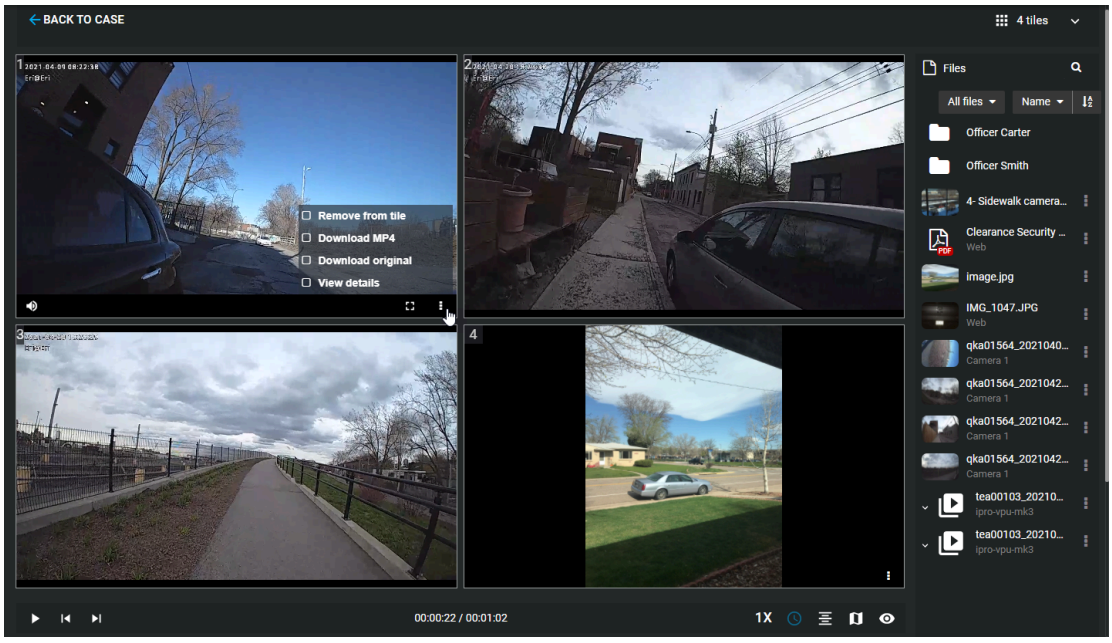
2 Click **Play** ( ).

3 Click to enter the evidence player, where the multi-tile view can be accessed.
The evidence player opens.

From the evidence player:

1 Click **Tile layout** (1 tile) and choose to arrange files in **4 tiles** or **6 tiles**.

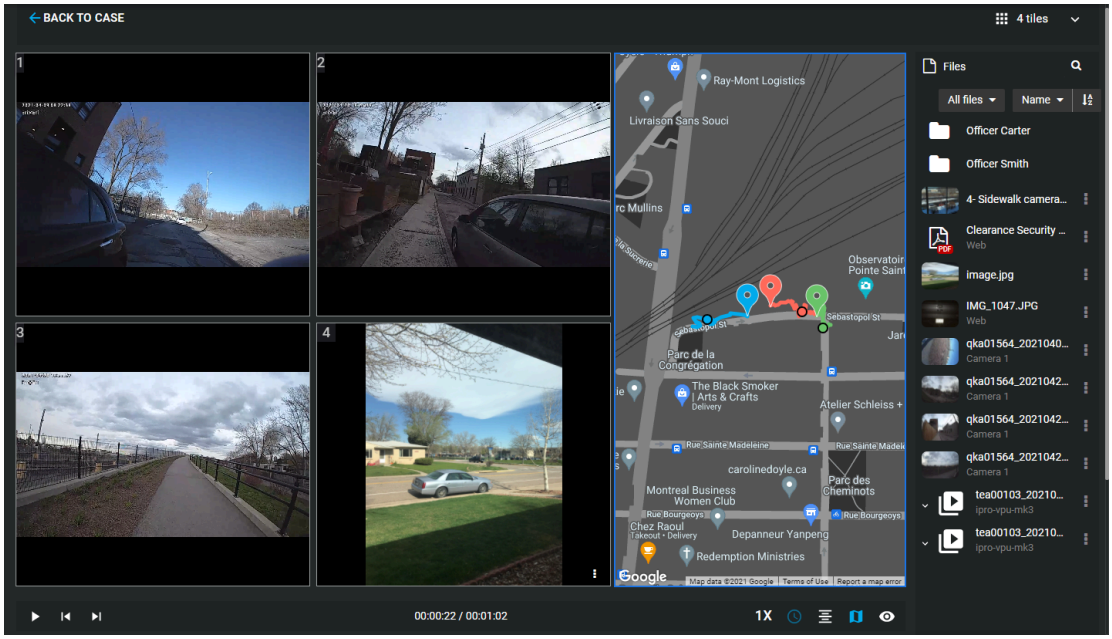
2 Click the files you want to examine, or drag and drop them into the tiles.



3 After you have loaded a video into one of the tiles, click **More** ( ) and choose to remove, download, redact, or view the details of a file in any tile. You can also choose to open a file in a new tab.

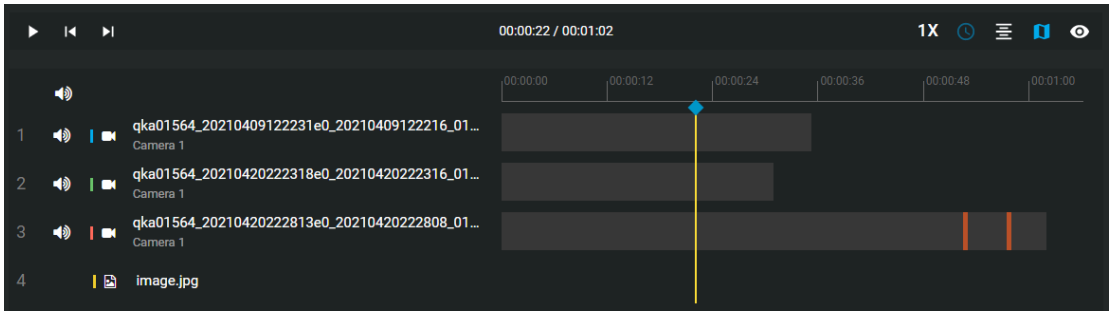
4 (Optional) If available, click **GPS trail** ( ) to display the GPS trail location data for a video.

NOTE: In the GPS data tile, a marker moves along the GPS trail to indicate the GPS location in relation to the video timeline.



5 Click **Play** ( ) to start playback for the videos loaded in the tiles.

6 When playing video, click the time bar to skip to any point in the videos that you have stationed in the tiles.



Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

After you finish

Refer to the video player controls definitions list for an inventory of controls.

Video player controls

Use the video player controls in Clearance to get a better sense of what you are looking at.

Butt	Command	Description
	Play	Play the video.
	Pause	Pause the video.
	Mute	Mute the video.
	Unmute	Un-mute the video.
1.5x	**Playback speed**	Select the video playback rate (0.5x, 1.0x, 1.5x, or 2.0x).
	Full screen	Select the full screen display mode.
	Default screen	Revert to the default display mode.
	Relative time	Display *relative time*.
	Absolute time	Display *absolute time*.
	Show visual watermark	Display *visual watermark*
	Hide visual watermark	Hide visual watermark. **NOTE:** To configure the visual watermark, refer to Configuring your account information.
	GPS trail	Show or hide the GPS trail location data if available. **NOTE:** GPS trail location data is only available when watching videos, and only if the video was captured using a device that provides GPS coordinates.
	Show metadata	Show or hide metadata associated with the file if any is available.
	Digital zoom	Scroll your mouse wheel forwards to zoom in and backwards to zoom out, or spread and pinch your laptop track pad.
	Skip frame forward	Move forward one frame in the video.
	Skip frame backward	Move backward one frame in the video.
	Chronological playback	Playback all videos in chronological sequence.

Butt	Command	Description
	Simultaneous playback	Playback all videos simultaneously.
	Take snapshot	Capture a still image snapshot of the video you are viewing. The snapshot is saved to the case the video file is associated with. • The user who took the snapshot and anyone with *Manage* permissions on any associated cases can access the snapshot. • Users must have *Edit* or *Manage* permissions on a video file to take a snapshot of it.

Downloading files

After files have been uploaded in the system, you can download them from either the File page or the Case page.

What you should know

You can only view video files directly in the system if they were uploaded in a supported file format. If an unsupported file format is uploaded it will not be viewable in the application. For other formats, you must download the file to view the video.

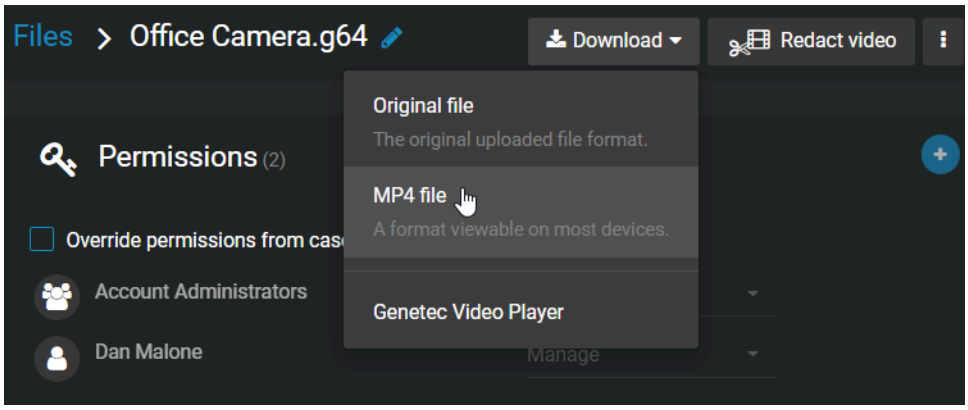
To download a file, you must have the *View and download* permission level for that file. After a file is downloaded, no user activity on the file is tracked outside of the system.

Procedure

1 Open an existing file.

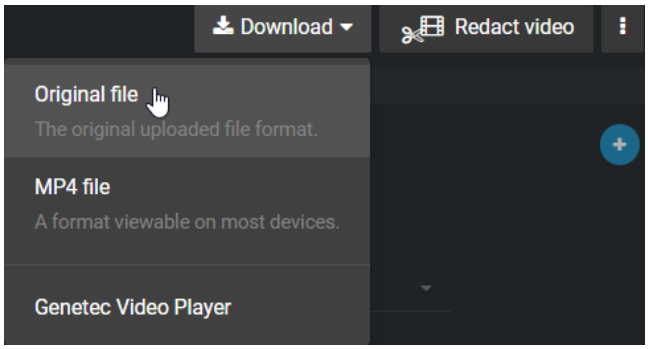
2 Click **Download**.

Example: The following image shows an MP4 file being downloaded from the Case page.



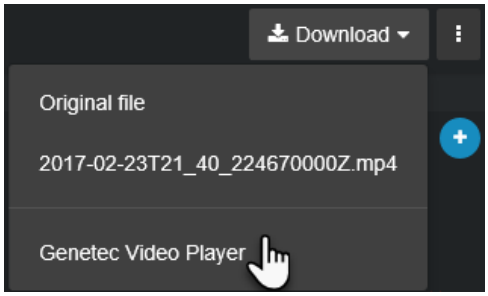
a) (Optional) Click **Original file** when you want to download the file in its original format, if the file is not an MP4.

Example: The following image shows a G64 file being downloaded from the File page.



b) (Optional) Click **Genetec™ Video Player** when you want to download the video player that is required to view a G64 or G64x file on your local machine.

Example: The following image shows the Genetec™ Video Player being downloaded from the File page.



NOTE: If a malware scan flags a file as suspicious, then only users included in the *Download malicious files* security policy can download it. For more information on this security policy, refer to Security policy definitions list.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Registry and video request overview

The registry is the Genetec Clearance™ module that simplifies the video request process and improves collaboration between participants and investigators. The registry can include a list of cameras that authorized users can request video from.

Using the registry module, organizations can do the following:

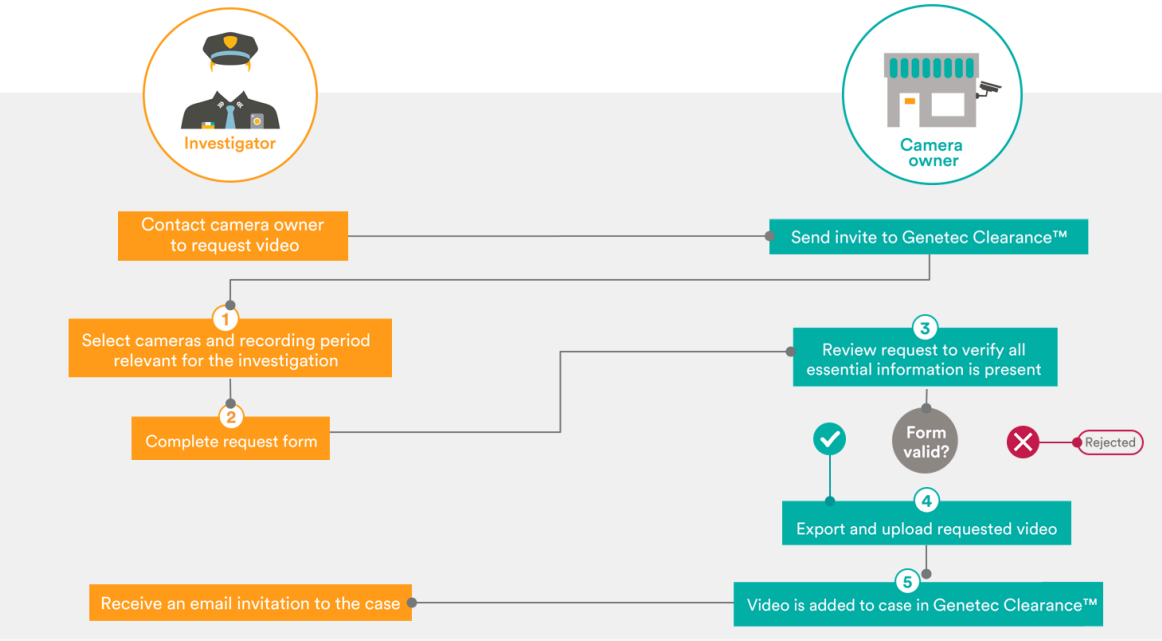
- Share the list of fixed and vehicle-based cameras in your Security Center system so that users can submit video requests.

  IMPORTANT: You must have the Genetec Clearance™ Plugin installed to request video from cameras and vehicles. For more information, refer to About Clearance Plugin for Security Center.
- Maintain a list of public safety program participants, from whom video can be requested.
- Configure request forms that users must complete when requesting video.
- Configure participant enrollment forms for public safety initiatives.
- Define Clearance users that can approve new requests.
- Maintain searchable records of all past requests.
- Query requests based on their status.
- Automatically upload video from Security Center using the Genetec Clearance™ Plugin.

The registry enhances situational awareness for investigators. It provides detailed information about cameras of interest, including their GPS coordinates and thumbnails showing the camera view.

Video request workflow

The following diagram illustrates the workflow processes that occur between Clearance and the Clearance Plugin when a video request is submitted.



1. A registry of cameras and participants is published in Clearance so that investigators can find devices that are near incidents under investigation.
2. The investigator submits a request form.

   An email notification is sent to the camera owners to review new requests. Authorized users can view the status of their current and past requests in Clearance.

3. Camera owners validate the video request, ensuring that all required details are received before releasing the video to the requester.
4. When the request is approved, video is exported from Genetec™ Security Center, or other systems integrated using the Clearance APIs, based on the date and time provided by the requester.

   NOTE: If the system is not integrated with other sources, evidence can be uploaded using a file request link generated on the request.
5. After the available recordings have been uploaded to Clearance, an email notification is sent to the investigator. You can configure permission levels in the system to grant the investigator *view-only* or *view and download* permissions.

Searching for cameras of interest

To help you find the most relevant footage for an incident, you can search for camera devices and community participants that exist nearby the location of an incident.

Before you begin

- To take advantage of instant video uploads after request approval, ensure that the Clearance plugin is installed and activated on all your Security Center workstations. To download the Clearance plugin for Security Center, click **here**.
- Create request forms in Clearance to ensure compliance with corporate standards and an efficient review process when managing requests. These request forms can be customized and are used to gather additional information specific to your organization and the approval workflow.
- To take advantage of camera functions on georeferenced maps in Clearance, ensure you have installed the latest version of the Clearance Plugin, and added cameras to your maps. For more information, see Adding cameras to your maps.

What you should know

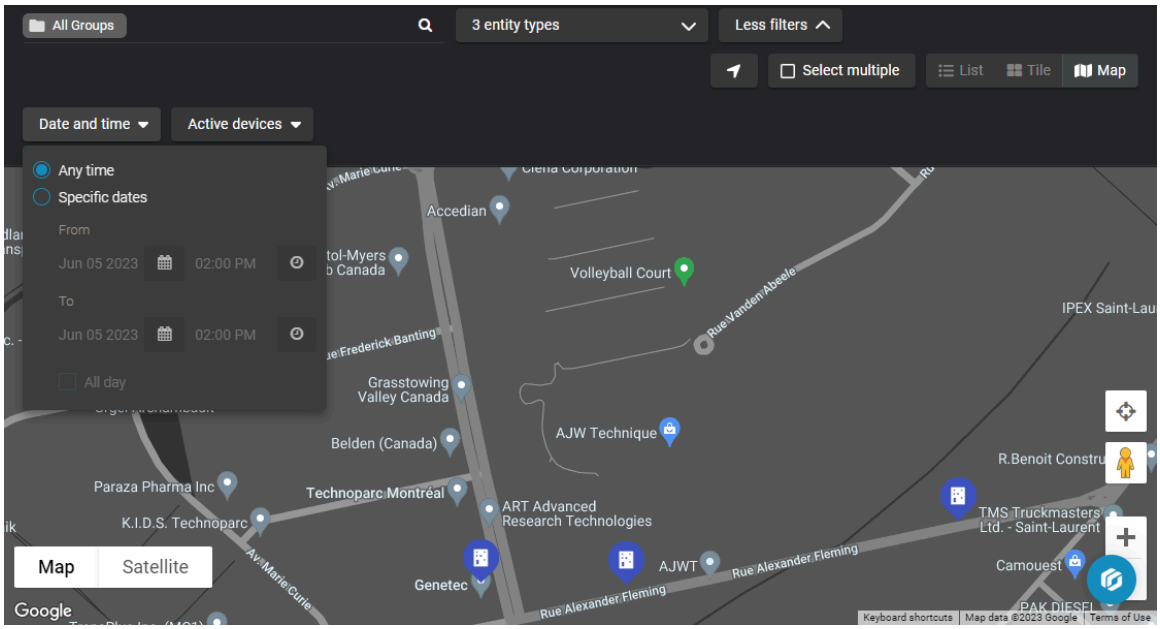
- Use a view that suits your search criteria:
  - **Map:** Use this view when you do not know the name or location of cameras.
  - **List:** Use this view when you know the names or descriptions of cameras you want to request video from.

Procedure

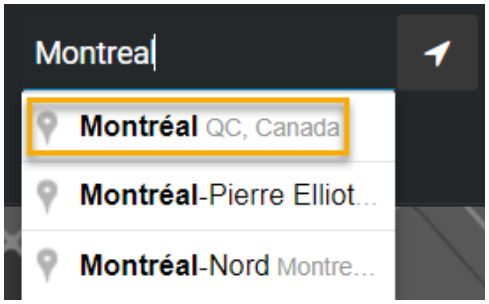
To search for cameras in the *Map* view:

1 Click **Registry** ( ).

2 Click **View map**.



3 In the location box, enter a location name and select the correct location from the results list.



4 (Optional) From the search bar, you can filter for cameras, vehicles, and participants.

5 In the search box, enter camera information and click **Search** ( ).

Example: Camera name, camera ID (original device ID from client), or a Clearance camera ID.

6 (Optional) Click **Location** ( ) to center the map on your current browser location.

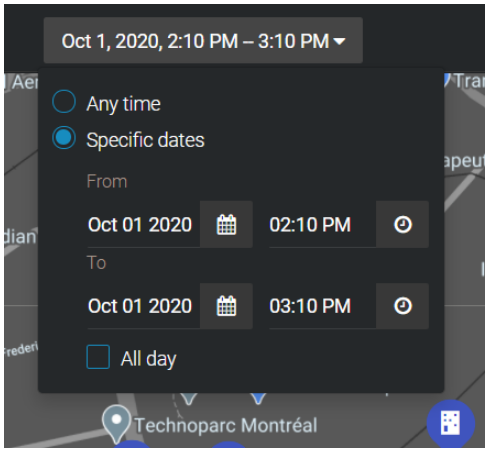
7 (Optional) Filter for cameras, participants, vehicles, or all three.

8 Adjust the *Map* view results by dragging the map location or using the zoom controls.

9 Click **More Filters** to expand the search menu.

a) Click **Date and time** and enter a specific date range that relates to the incident that you are investigating.

Using the **Date and time** search helps you find cameras with archived footage that relates to the specified period of the incident being investigated.



b) Click **Device status** and choose to display online devices, offline devices, or both.

10 Click the camera icons ( ) to check cameras found using the search criteria. Click a thumbnail from the list to check the content relevance.

TIP: Click **View details** and check the description, location, how long the video is stored for, owner information, timezone, and the camera IDs to verify if the video is of interest.

11 (Optional) To find a specific location on the map, click **Enter location** ( ).

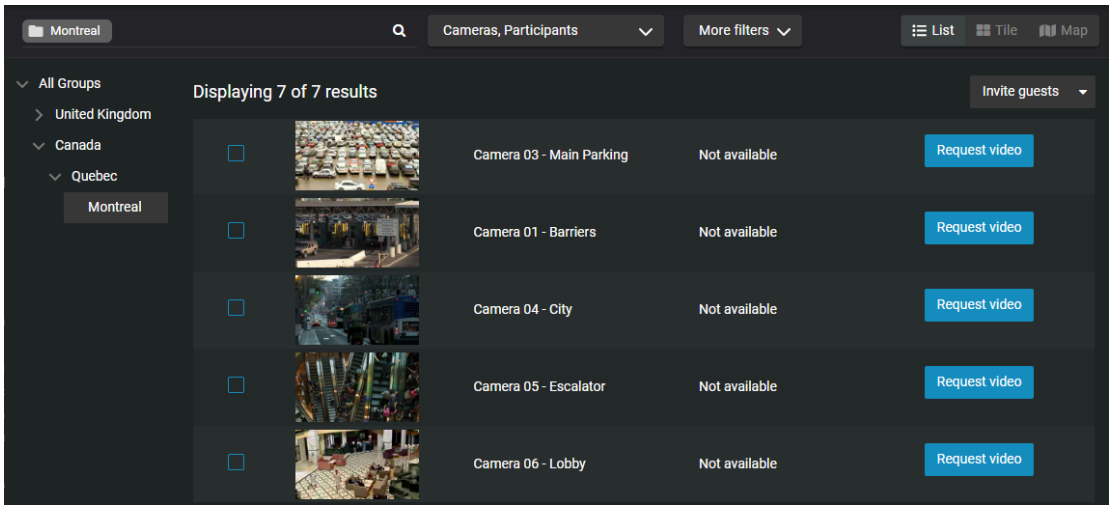
12 To select multiple cameras from the map:

- Click **Rectangle selection** ( ) and select multiple cameras on the map using a rectangle shape.
- Click **Polygon selection** ( ) and select multiple cameras on the map using a polygon shape. Drawing a polygon is useful when selecting cameras that are dispersed across a random area.

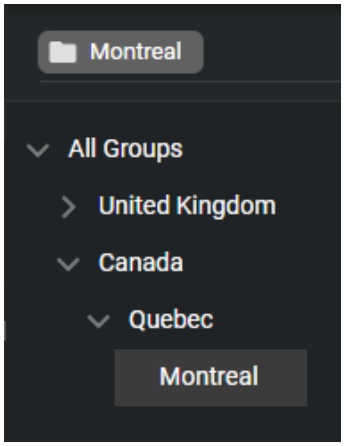
To search for cameras in the *List* view:

1 Click **Registry** ( ).

2 Click **List view** ( ).



3 (Optional) If you know the group the relevant cameras are included in, select it from the group list.



4 (Optional) From the search bar, you can filter for cameras, vehicles, and participants.

5 In the search box, enter camera information and click **Search** ( ).

For example, camera name, camera ID, or description.

6 Click **More Filters** to expand the search menu.

7 Click **Date and time** and enter a specific date range that relates to the incident that you are investigating.

Using the **Date and time** search helps you find cameras with archived footage that relates to the specified period of the incident being investigated.

8 Click the camera thumbnails to check for possible cameras of interest.

TIP:

- Click one or more thumbnails to see the video details and check the description, location, how long the video is stored for, owner information, timezone, and the camera IDs to verify if the video is of interest.
- Click the thumbnail of a vehicle to review the field of view of each of its associated cameras.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

After you finish

Submit your video request.

Requesting video

To review incidents and solve crimes, you can use the Genetec Clearance™ registry to identify cameras, vehicles, and participants of interest near the incident location. You can then request video from these cameras and participants to review your operations and aid investigations.

Before you begin

Search for cameras of interest.

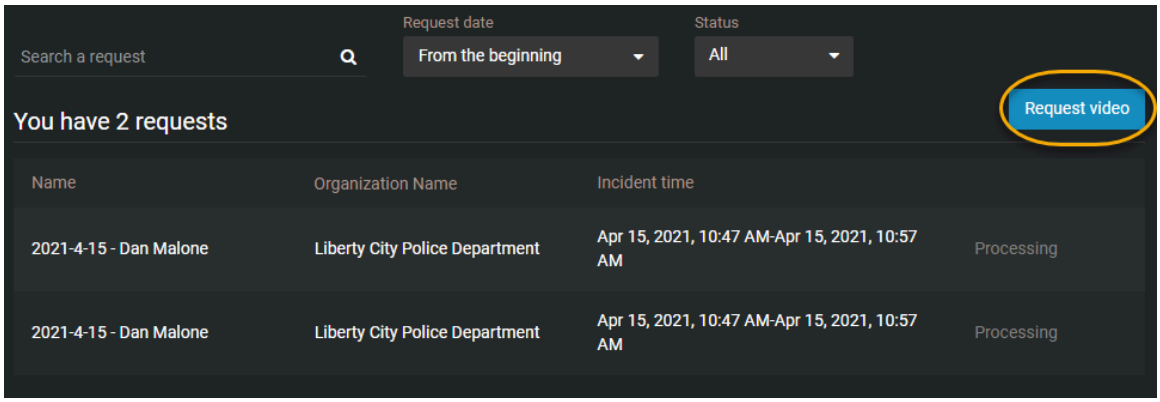
What you should know

- Organizations can invite Clearance users to submit video requests.
- Guest users can also submit requests if they have been assigned the *request videos* video request policy. They must also have been invited to submit video requests.
- You can submit a video request from the **Requests** page, or the **Registry**.

Procedure

To submit a video request from the *Requests* page:

1 Click **Requests** ( ) and then click **Request video**.



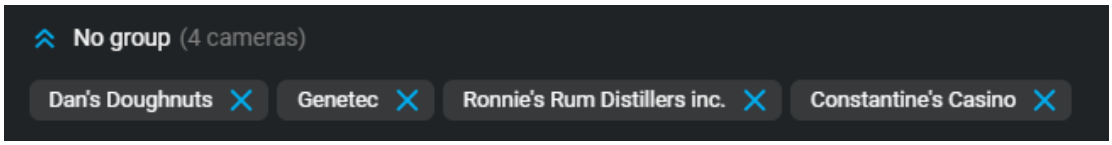
2 From the **Request video** menu, select a type of request form.

3 Choose to associate the request with a camera from the list, or select the vehicle or geographical location you need video from.

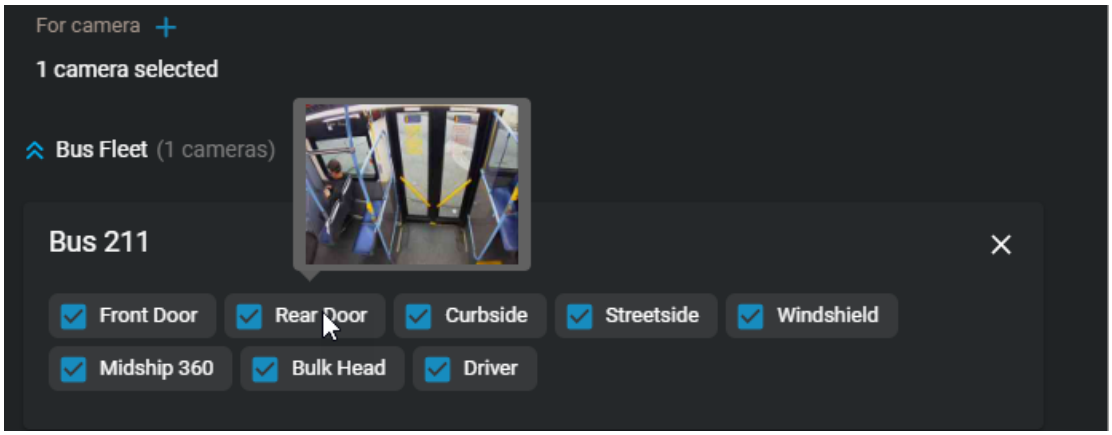
- Click **Add** ( ) to associate the request with a camera, vehicle, or participant from the list.
- Click **Map** ( ) to select the geographical location you need video from.
  - Click **Enter location** ( ) to locate a specific address on the map.
  - Click **Rectangle selection** ( ) to select multiple cameras on the map using a rectangle shape.
  - Click **Polygon selection** ( ) to select multiple cameras on the map using a polygon shape. Drawing a polygon is useful when selecting cameras that are dispersed across a random area.

TIP:

- If you select multiple cameras, or a vehicle containing multiple cameras, you can remove or deselect them as needed.



- If you selected a vehicle, hover over the associated cameras to see a preview of the camera's field of view.



4 Assign a name to the request.

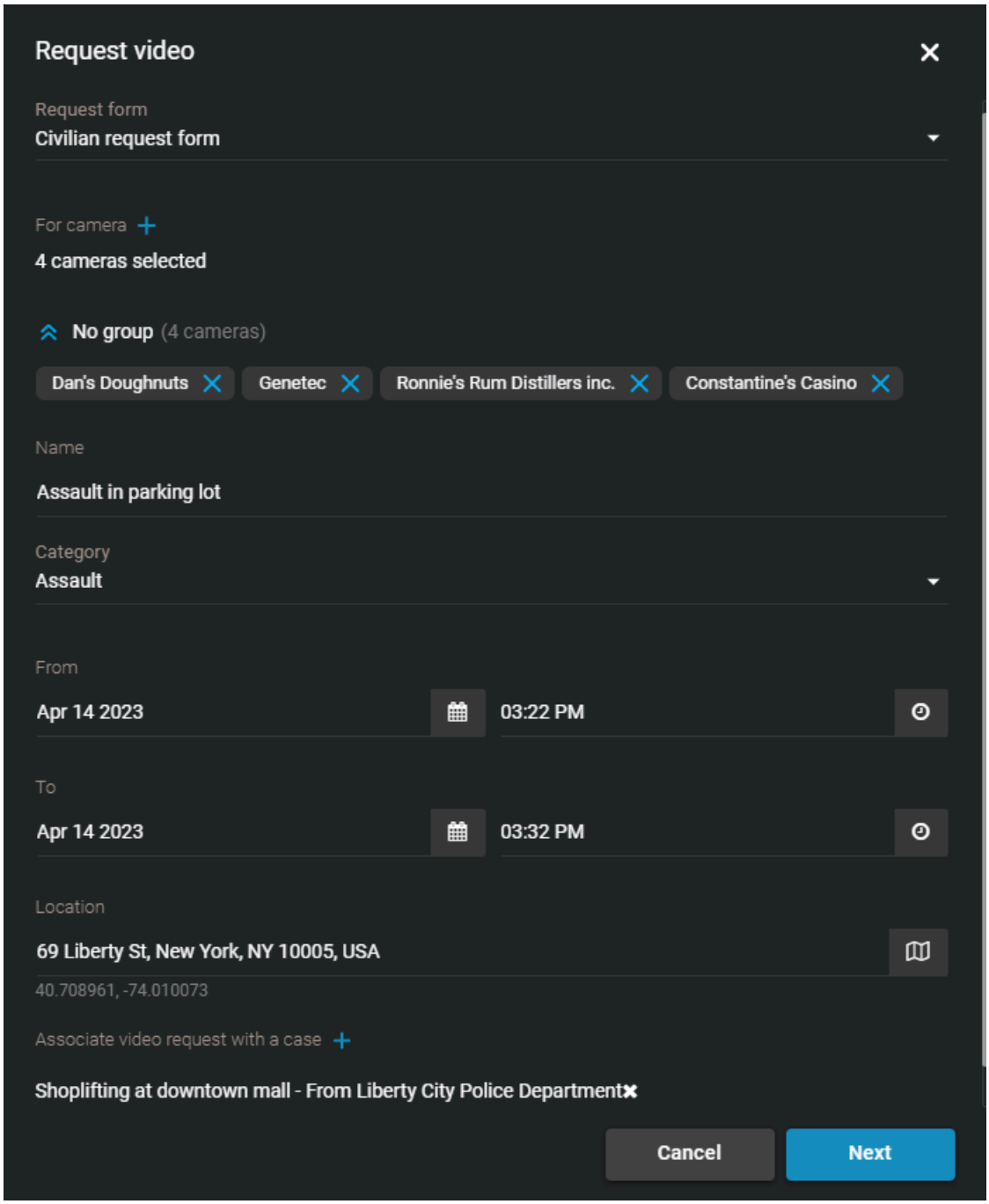
5 Choose a category for the request.

6 In the **From** and **To** fields, enter the date and time range that you require video from.

NOTE: You can select a maximum time range of 2 hours or 120 minutes.

7 In the **Location** field, enter the address or location that you require or click **Map view** ( ) to choose a location in the map view.

8 (Optional) To associate videos with an existing case, click **Select case** (+) and select the case you require.



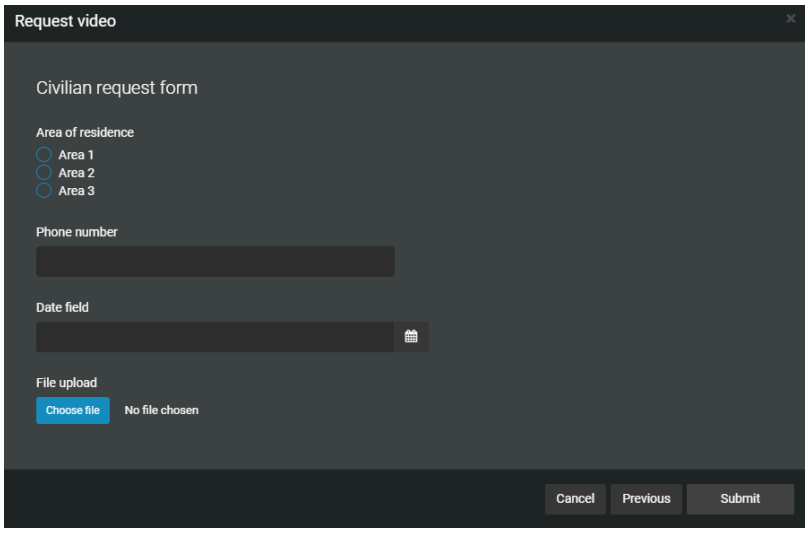
NOTE:

- You can only link videos to cases that you have permission to access. This permission level remains unchanged after the video request approval.
- If you do not select a case, the system creates one for you automatically.
- Fields that are common between the request and the associated new case are automatically copied from the request to the case. Common fields that are copied from requests to cases include the following:
  - Name
  - Category
  - Date and time

- Location

9 Click **Next**.

10 If a request form opens, complete the fields.



11 Click **Submit**.

Your video request is submitted for review and approval.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

Canceling a video request

In some situations, you might need to cancel a video request after it has been submitted. For example, if the request contained the wrong camera, time period, or missing or inaccurate information.

What you should know

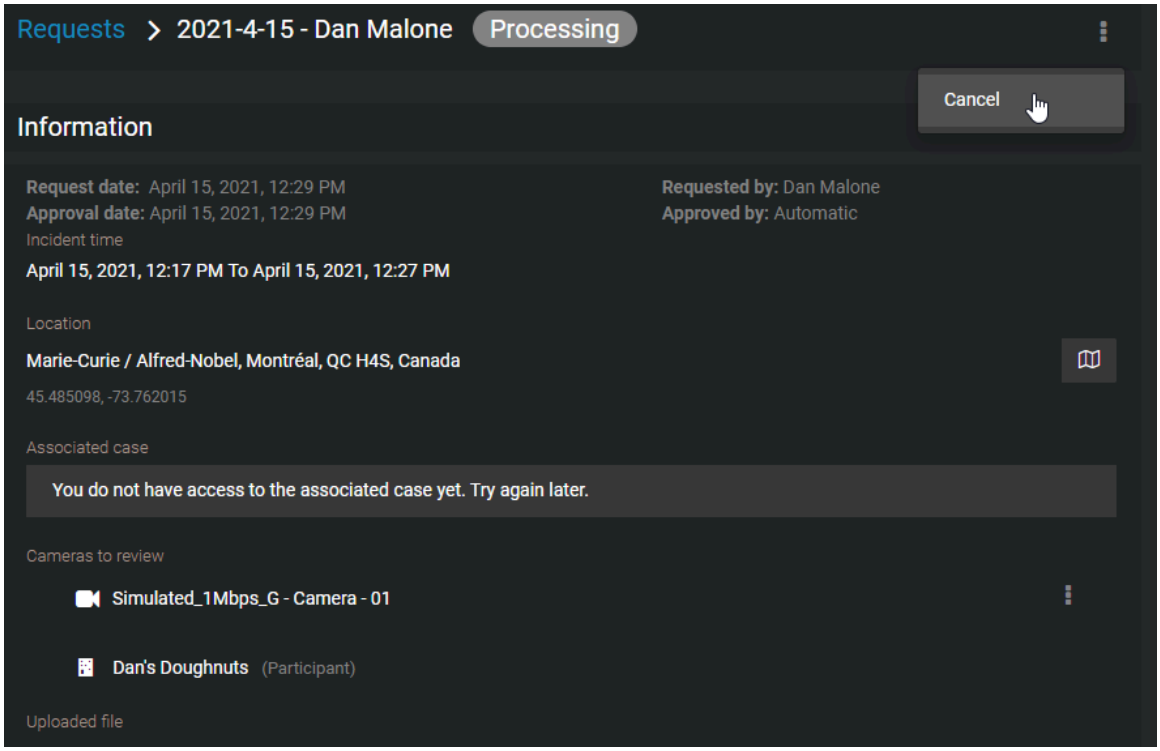
- Only a requester can cancel their request.
- Requests cannot be canceled after they have been approved.

Procedure

1 Click **Requests** ( ).

2 Select the pending request that you want to cancel.

3 Click .



4 Click **Cancel**.

Example

Watch this video to learn more. Click the **Captions** icon (**CC**) to turn on video captions in one of the available languages.

After you finish

If required, you can resubmit your request after resolving any issues with the request content.

4

Public upload requests

Add files to an incident without viewing the case contents.

This section includes the following topics:

Sharing files using a file request

Use a public file request when you want anyone to add files to an incident without viewing the case contents.

Before you begin

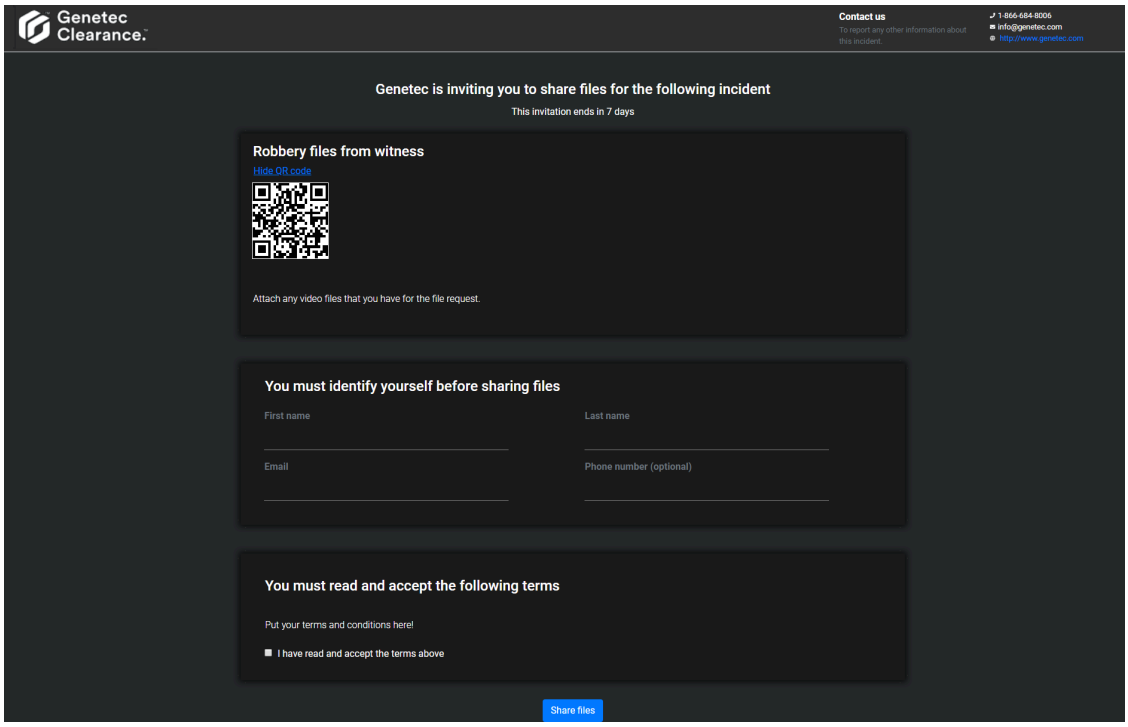
Ensure that you have received a file request containing a file request link that you can use to submit files.

What you should know

- The person receiving the public file request must complete the identity information and accept the file request terms before they can share files.
- When a file request is used to share a file, *Public upload* audit trail information is stored.
  - Who uploaded the file shown in the preview list as **Uploaded by**. For example, user@host.com (public upload).
  - Who created or modified the file shown in the file audit trail details information as Public upload.
- reCAPTCHA is used to protect public uploads from malicious activities.

Procedure

1 Click the file request link or scan the QR code to open the file request.



2 Complete the identity information section so that you can be contacted regarding the files that you shared.

NOTE: User contact information is optional when **Allow anonymous uploads** is enabled.

a) Enter a **First name**.

b) Enter a **Last name**.

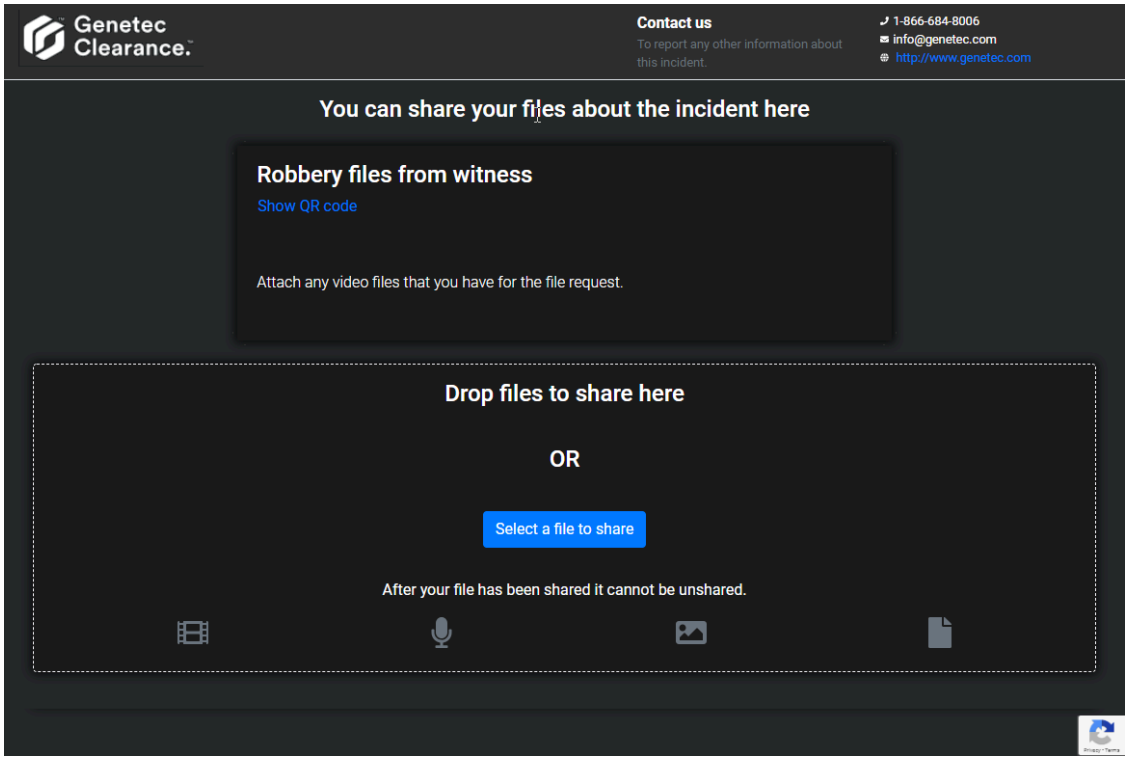
c) Enter an **Email address**.

d) (Optional) Enter a **Phone number**.

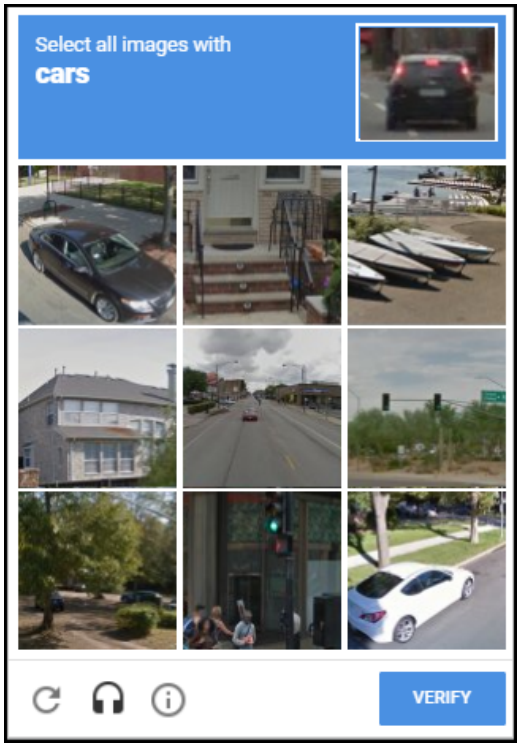
3 Read the file request terms.

a) Select **I have read and accept the terms above** if you accept the terms and want to share files.

4 Click **Share files**.

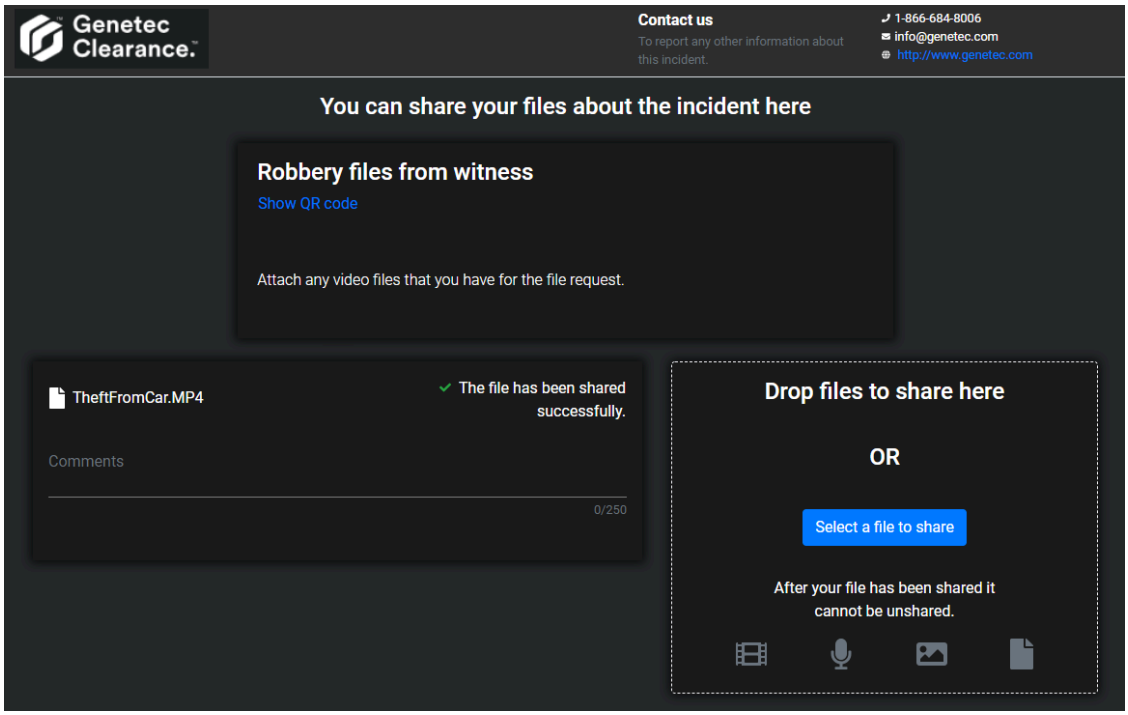


5 Drag and drop one or more files or click **Select a file to share**.



a) If reCAPTCHA is triggered, the user must validate they are a human to continue. Click **Verify** to continue.

The shared file is immediately added to the case.



5

Genetec Video Player

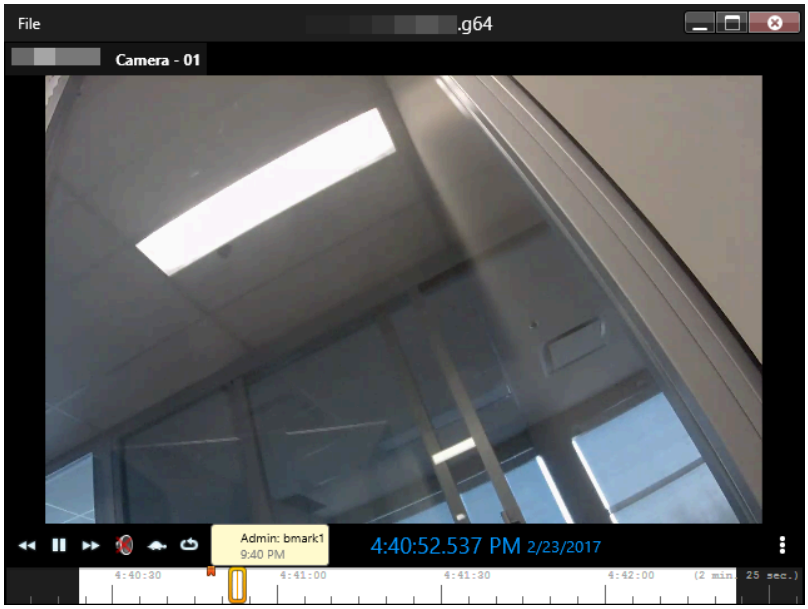
View exported G64 and G64x video files from Security Desk, or on a computer that does not have Security Center installed, in Clearance.

This section includes the following topics:

About Genetec™ Video Player

Genetec™ Video Player is a standalone media player you can use to view G64 and G64x video files exported from Security Desk. You can also use it to view video on a computer that does not have Security Center installed.

The following image shows the Genetec™ Video Player playing a G64 video file.



- The toolbar options are used to control the video playback.
- The more ( ) icon is used to access additional options. For example, **Toggle digital zoom**, **Toggle full view**, or **Copy a snapshot to clipboard**.
- The timeline is used to access bookmarks or a specific point in the video playback.

Downloading Genetec™ Video Player

Before you can use the Genetec™ Video Player to view G64 or G64x video files on your local workstation, you must download and install the player.

What you should know

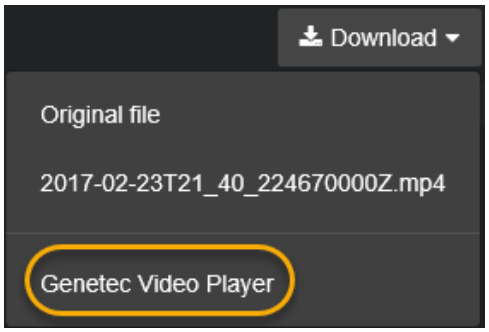
When a *G64* or *G64x* video file has been uploaded into Clearance, users can download the Genetec™ Video Player so that they can download, share, and playback the original files.

Procedure

1 Do one of the following:

- Open an existing case, and then select a G64 video file in the **Files** field.
- From the *Home* page, click **Files**, and then select a G64 video file.

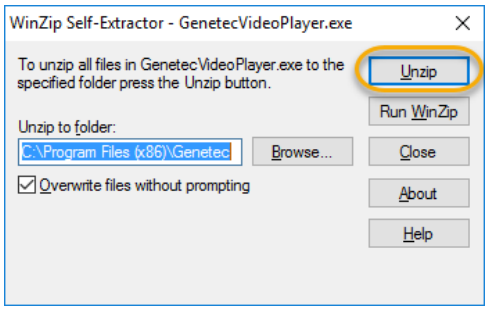
2 Click **Download** and then click **Genetec™ Video Player**.



3 Download the Genetec™ Video Player install package.

4 Double-click or select the *GenetecVideoPlayer.exe* installer *.exe* file and click **RUN**.

a) Select the folder location where you want to unzip the download.
For example, *C:\Program Files (x86)\Genetec* and click **Unzip**.



b) When the files have been extracted, click **OK**.

c) Click **Close**.

The Genetec™ Video Player is now available for use on your local machine.

After you finish

You can now use the Genetec™ Video Player to view G64 or G64x video files.

Viewing G64 or G64x video files in the Genetec™ Video Player

You can use the Genetec™ Video Player to view G64 or G64x video files that have been download onto your local machine, or in situations where G64 or G64x files have been shared with you.

Before you begin

- Ensure that you have the Genetec™ Video Player installed on the machine that you want to use to view G64 or G64x video files.
- Ensure that you have downloaded the *G64* or *G64x* video files that you want to view.

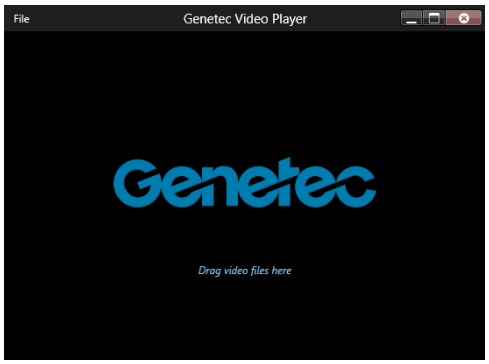
What you should know

To download a file, you must have the *View and download* permission level for that file. After a file is downloaded, no user activity on the file is tracked outside of the system.

Procedure

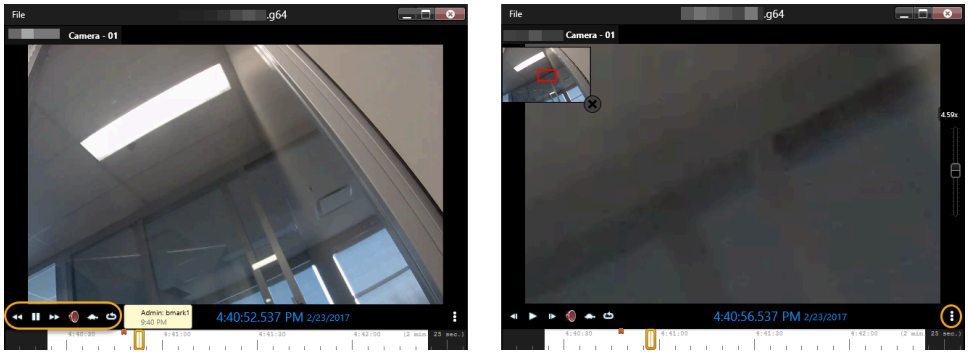
1 Start the Genetec™ Video Player on your local machine.

For example, double-click the *Genetec Video Player.exe* in *C:\Program Files (x86)\Genetec\GenetecVideoPlayer*



2 Drag and drop a g64 or G64x video file onto the Genetec™ Video Player window.

3 When a video file is dragged onto the player, the video starts playing automatically.



a) Use the toolbar to control the video playback.

b) Click **More** ( ) to **Toggle digital zoom**, **Toggle full view**, or **Copy snapshot to clipboard**.

c) Use the timeline to access bookmarks or a specific point in the video playback.

Glossary

absolute time

In Clearance, absolute time refers to the actual recording start and end times of the video evidence. For example, 08:35:00 AM - 08:40:00 AM.

access policy

An access policy refers to the permission levels granted to various integrations, users, groups, and departments on a particular case or file in a Clearance account.

account

An account defines a customer organization's settings for Clearance. There is one account per Clearance system.

Account Administrator

The Account Administrator in Clearance is a predefined user group with full access to the site, whose members typically act as site administrators. Only members of the Account Administrator group have access to the Configurations menu, from which they can create and manage users, groups, departments, categories, and access policies.

body-worn camera

A body-worn camera (BWC), also known as a wearable camera, is a video recording system that is typically used by law enforcement to record their interactions with the public or gather video evidence at crime scenes.

case

A case in Clearance is a record of an incident. You can share cases with internal and external organizations, and add digital evidence such as videos, images, and documents to cases.

category

Categories in Clearance are used to classify cases. Each category defines an incident type and a retention policy.

Clearance

Genetec Clearance™ is an evidence management system that you can use to help accelerate investigations by securely collecting, managing, and sharing evidence from different sources.

Clearance (plugin)

The Genetec Clearance™ plugin is used to export video recordings and snapshots from Security Center to Clearance. You can also create a registry of Security Center cameras in a Clearance account that you can use to send notifications to operators and automate exports when video requests are received.

Clearance (role)

The Genetec Clearance™ role manages video exports to a Clearance account. This role also handles communications between Security Center and the Clearance web application.

Clearance Capture

Genetec Clearance™ Capture is a Google Chrome extension that is used to capture evidence from websites and social media and upload the evidence directly to your Clearance account.

Clearance Seen

Genetec Clearance™ Seen is a mobile app that officers and security personnel can use to capture videos, images, and audio recordings from their phone, and upload evidence directly to their Clearance account. Evidence can quickly be added to cases and shared with investigators and other parties, all while maintaining its safety and security.

department

A department in Clearance is a collection of users, integrations, and groups. The department's access policies are added to the policies that its members already have. Users, integrations, and groups can belong to more than one department.

eDiscovery

In Clearance, eDiscovery is the process where electronic data is sought, secured, located, explored, and retrieved with the intention of using it as evidence in a civil or criminal case.

eDiscovery receipt

In Clearance, an eDiscovery receipt is an audit-compliant digital proof of receipt report (in PDF format) for evidence being shared between two parties. For example, between the District Attorney's office and the Attorney of the defendant. The report includes evidence shared, how it was sent, and a list of items shared.

file

A file in Clearance is a piece of digital evidence, such as a video, image, document, or other type of file. Files can be grouped within one or more cases.

G64

G64 is a Security Center format used by archiving roles (Archiver and Auxiliary Archiver) to store video sequences issued from a single camera. This data format supports audio, bookmarks, metadata overlays, timestamps, motion and event markers, and variable frame rate and resolution.

G64x

G64x is a Security Center format used to store video sequences from multiple cameras that are exported or backed up simultaneously. This data format supports audio, bookmarks, metadata overlays, timestamps, motion and event markers, variable frame rate and resolution, and watermarking.

Genetec Clearance™ Uploader

is an application used to automatically upload media from body-worn cameras, sync folders, or other devices to Clearance, or a Security Center video archive, depending on which *.json* config file is used.

Genetec™ Video Player

Genetec™ Video Player is a standalone media player you can use to view G64 and G64x video files exported from Security Desk. You can also use it to view video on a computer that does not have Security Center installed.

group

A group in Clearance is a collection of users and integrations. The group's access policies are added to the policies that its members already have. Users and integrations can belong to more than one group.

integration

An integration in Clearance is an external device or application that is authorized to transfer data to the Clearance account.

participant

A participant is an individual or business that wishes to share videos with a Clearance account. You can add participants' cameras to the Clearance registry to make them available to system users.

permission level

Permission levels in Clearance are used to define the level of access granted on a case or a file. The different permission levels include *View only*, *View and download*, *Edit*, and *Manage*, and they can be granted to an integration, user, group, or department.

Plan Manager

(Obsolete) Plan Manager is a module of Security Center that provides interactive mapping functionality to better visualize your security environment. The Plan Manager module has been replaced by the Security Center role, Map Manager, since version 5.4 GA.

plugin

A plugin (in lowercase) is a software component that adds a specific feature to an existing program. Depending on the context, plugin can refer either to the software component itself or to the software package used to install the software component.

plugin role

A plugin role adds optional features to Security Center. A plugin role is created by using the *Plugin* role template. By default, it is represented by an orange puzzle piece in the *Roles* view of the *System* task. Before you can create a plugin role, the software package specific to that role must be installed on your system.

Plugins

The *Plugins* task is an administration task that you can use to configure plugin-specific roles and related entities.

redaction

Redaction in Clearance is the act of obscuring faces, audio, or other sensitive information from supported video files.

registry

The registry is the Genetec Clearance™ module that simplifies the video request process and improves collaboration between participants and investigators. The registry can include a list of cameras that authorized users can request video from.

relative time

In Clearance, relative time refers to the duration of the video recording with no reference to when the recording started. For example, a 5 minute recording would be shown as 0:00 - 05:00.

requester

In Clearance, a requester is a user who can request video from camera sources of interest. This includes requesting video from a public or privately owned camera defined in the Clearance registry.

retention policy

A retention policy in Clearance defines how long a case remains in the system after it is closed or how long a file is retained before it is permanently deleted. A retention policy can prescribe a finite or indefinite duration.

role

A role is a software component that performs a specific job within Security Center or Security Center SaaS.

security policy

A security policy in Clearance defines which users and groups have access to a particular system feature.

System for Cross-Domain Identity Management

In Clearance, the System for Cross-domain Identity Management (SCIM) protocol is used to synchronize users and groups from an identity management system into cloud-based products.

Trimming

Trimming is the act of shortening a recording and isolating parts that are relevant to your case. When trimming is performed, the original video is preserved and the trimmed version is saved as a copy.

user

A user identifies a person in a Clearance account. You configure what cases and files a user can access through access policies, and what features they can use through security and video request policies.

video request

A video request is a request from an authorized user to a camera owner, to share recordings for an investigation in Genetec Clearance™.

video request policy

A security policy in Clearance defines which users and groups have access to a particular feature related to the video request module.

visual watermarking

Visual watermarks add a transparent overlay to videos and images in Clearance. The overlay displays identifying information about the user that is currently logged in, organization details, and timestamps indicating when the user viewed or shared the video or image. The visual watermark deters the unauthorized use or distribution of content. Visual watermarking can only be removed by users who have the hide visual watermark permission.

Technical support

Genetec™ Technical Assistance Center (GTAC) is committed to providing its worldwide clientele with the best technical support services available. As a customer of Genetec Inc., you have access to TechDoc Hub, where you can find information and search for answers to your product questions.

- **Genetec TechDoc Hub:** Find articles, manuals, and videos that answer your questions or help you solve technical issues.

  Before contacting GTAC or opening a support case, it is recommended to search TechDoc Hub for potential fixes, workarounds, or known issues.

  To access the TechDoc Hub, log on to Genetec Portal and click TechDoc Hub. Can't find what you're looking for? Contact documentation@genetec.com.
- **Genetec Technical Assistance Center (GTAC):** Contacting GTAC is described in the Genetec Advantage Description.

Technical training

In a professional classroom environment or from the convenience of your own office, our qualified trainers can guide you through system design, installation, operation, and troubleshooting. Technical training services are offered for all products and for customers with a varied level of technical experience, and can be customized to meet your specific needs and objectives. For more information, go to http://www.genetec.com/support/training/training-calendar.

Licensing

- For license activations or resets, contact GTAC at https://portal.genetec.com/support.
- For issues with license content or part numbers, or concerns about an order, contact Genetec Customer Service at customerservice@genetec.com, or call 1-866-684-8006 (option #3).
- If you require a demo license or have questions regarding pricing, contact Genetec Sales at sales@genetec.com, or call 1-866-684-8006 (option #2).

Hardware product issues and defects

Contact GTAC at https://portal.genetec.com/support to address any issue regarding Genetec appliances or any hardware purchased through Genetec Inc.