Genetec™
Clearance.™

Genetec Clearance™ User Guide

Document last updated: February 27, 2025

Genetec™

Legal notices

The contents of this guide are furnished for informational use only and are subject to change without notice. Genetec Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Genetec Inc. reserves the right to revise and improve its products as it sees fit. This document describes the state of a product at the time of document's last revision, and may not reflect the product at all times in the future.

In no event shall Genetec Inc. be liable to any person or entity with respect to any loss or damage that is incidental to or consequential upon the instructions found in this document or the computer software and hardware products described herein.

All specifications are subject to change without notice.

Document information

Document title: Genetec Clearance™ User Guide

Original document number: EN.706.002-1.0.B(1)

Document number: EN.706.002-1.0.B(1)

Document update date: February 27, 2025

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

About this guide

This guide is intended for administrators and users of Genetec Clearance™. This guide describes how to set up and use Genetec Clearance™.

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

Preface

Legal notices ii
About this guide iii

Chapter 1: Introduction to Clearance

What is Clearance? 2
About email notifications in Clearance 3

Chapter 2: Getting started

Deploying and using Clearance 8
Deploying and using the Registry and Video Request modules in Clearance 10
Logging on to Clearance 12
Logging off from Clearance 13
Changing language settings in Clearance 14
Clearance videos 15

Chapter 3: Release notes

What's new in Clearance 17
Previous features and enhancements 18
System requirements for Clearance 25
Supported languages 26

Chapter 4: User interface tour

Overview of the menu tabs in Clearance 28
Overview of the Home page 30

Chapter 5: Account setup

Setting up your account 33
Activating your account 34
Configuring your account information 36
Configuring your report templates 39
Setting the retention period for cases and files 40
Permission levels 43
Creating user groups 46
Creating user accounts 48
Synchronizing users and groups using SCIM protocol 50
About SCIM synchronization using an API 50
Provisioning users and user groups using SCIM 51
SCIM and Clearance attributes mapping 52
Adding existing users to groups 53
Creating integrations 54
Creating departments 55
Setting a default department 57
Creating incident categories 58
Defining video request policies 59
Video request policy definitions list 61

Defining security policies . . . 63
Security policy definitions list . . . 63
Creating fields . . . 66
Configuring ID templates . . . 67
Creating forms . . . 69
Creating video request forms . . . 69
Creating participant enrollment forms . . . 74
Resetting user passwords . . . 84
Searching for users or groups . . . 85
Creating support tickets . . . 86
Downloading a user list report . . . 87

Chapter 6: Managing cases

Creating cases . . . 89
Creating a file request . . . 91
Creating a case summary report . . . 93
Creating an eDiscovery receipt . . . 96
Example of a case . . . 99
Assigning personnel to a case . . . 101
Sharing cases . . . 102
Pinning cases to the homepage . . . 104
Transferring cases . . . 106
Inviting guests to view cases . . . 108
Copying cases . . . 111
Changing access policies for cases . . . 112
Searching for cases or files . . . 113
Searching for cases or files using map view . . . 115
Searching for files or folders in a case . . . 117
Previewing evidence in cases . . . 119
Reopening cases . . . 120
Protecting cases from deletion . . . 121
Deleting cases . . . 122
Restoring cases . . . 124
Viewing the audit trail history of cases . . . 125
About closed cases . . . 126

Chapter 7: Managing devices

About device licenses . . . 129
Activating device licenses . . . 129
Assigning devices to users . . . 130
Removing device assignments from users . . . 132
Deactivating device licenses . . . 134
Enrolling Axis and Reveal body-worn cameras . . . 136

Chapter 8: Managing i-PRO devices

Adding i-PRO body-worn cameras . . . 138
Adding i-PRO BWC MK3 body-worn cameras . . . 138
Adding i-PRO BWC 4000 body-worn cameras . . . 141
Adding i-PRO in-car systems . . . 144
Configuring i-PRO ICV 4000 systems . . . 144

Adding i-PRO ICV MK3 in-car systems . . . 146
Configuring an i-PRO Gateway . . . 148
Adding i-PRO ICV MK3 in-car systems . . . 150
Configuring i-PRO five fields . . . 152
About i-PRO automatic case creation and file tagging . . . 154
About device groups . . . 155
Creating device groups . . . 155
Adding devices to groups . . . 156
Configuring device groups . . . 156
About device group configurations . . . 157
Defining device policies . . . 159
Managing i-PRO user account policies . . . 159

Chapter 9: Managing files

About Clearance information security . . . 164
Uploading files to cases . . . 165
Configuring file details . . . 167
Reviewing media . . . 168
Video player controls . . . 170
Sharing files . . . 172
Inviting guests to view files . . . 173
Associating cases with a file . . . 175
Linking files to another case . . . 177
Searching evidence by device assignment . . . 178
File formats you can preview in Clearance . . . 180
Downloading files . . . 182
Changing access policies for files . . . 185
Protecting files from deletion . . . 187
Deleting files . . . 188
Restoring files . . . 190
Viewing the audit trail history of files . . . 191

Chapter 10: Managing video requests

Registry and video request overview . . . 193
Searching for cameras of interest . . . 195
Requesting video . . . 199
Inviting guests to submit video requests . . . 203
Reviewing video requests . . . 206
Approving video requests . . . 209
Canceling a video request . . . 213

Chapter 11: Managing video editor content

About the video editor . . . 215
Trimming video . . . 218
Redacting video in Clearance . . . 220
Redacting video manually in Clearance . . . 228
Redacting audio . . . 234

Chapter 12: Reviewing dashboards

About the Clearance dashboard . . . 237

Configuring the Clearance dashboard 237

Chapter 13: Public upload requests

Sharing files using a file request 246

Chapter 14: Clearance plugin

About Clearance Plugin for Security Center 250

Chapter 15: Clearance Drive

About Clearance Drive 252
Installing Clearance Drive 253
Clearance Drive user interface tour 256
Managing cases using Clearance Drive 258
Transferring files using Clearance Drive 261
Configuring settings in Clearance Drive 262

Chapter 16: Clearance Uploader application

About Clearance Uploader 264
Installing the Clearance Uploader 266
Configuring the Clearance Uploader 268
Uploading media using the Clearance Uploader 270
Monitoring Clearance Uploader activities 273
Viewing Clearance Uploader event logs 276

Chapter 17: Genetec™ Video Player

About Genetec™ Video Player 278
Downloading Genetec™ Video Player 279
Viewing G64 or G64x video files in the Genetec™ Video Player 280

Chapter 18: Clearance Seen

About Clearance™ Seen 283

Chapter 19: Frequently asked questions

How can I create a bookmark to my Clearance account? 285
Why is a preview of a PDF not displayed in Clearance? 288
How can I avoid errors when accessing my Clearance account through my browser history? . . 290
Why does my file fail to upload to Clearance? 292
Why does the download link fail to work in Google Chrome? 293
Change to Clearance login 294
Glossary 295
Technical support 299

1

Introduction to Clearance

Learn about the Clearance collaborative investigation management system.

This section includes the following topics:

- "What is Clearance?" on page 2
- "About email notifications in Clearance" on page 3

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 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.

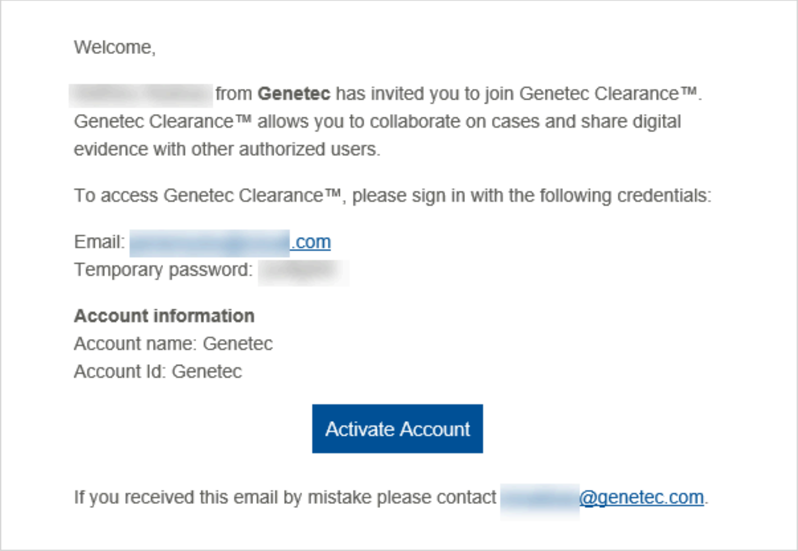
The email notification can also include one or more of the following:

- 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:

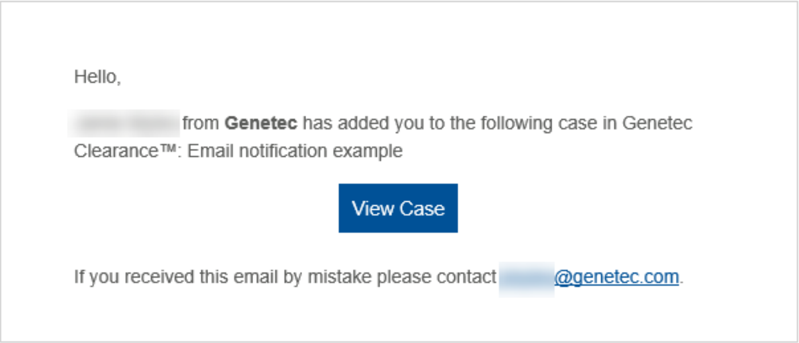
Email: [redacted].com
Temporary password: [redacted]

Account information
Account name: Genetec
Account Id: Genetec

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.



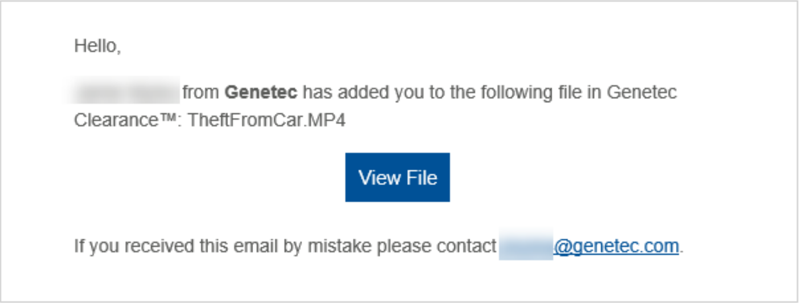
Hello,

[redacted] from **Genetec** has added you to the following case in Genetec Clearance™: Email notification example

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

User added to a file

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



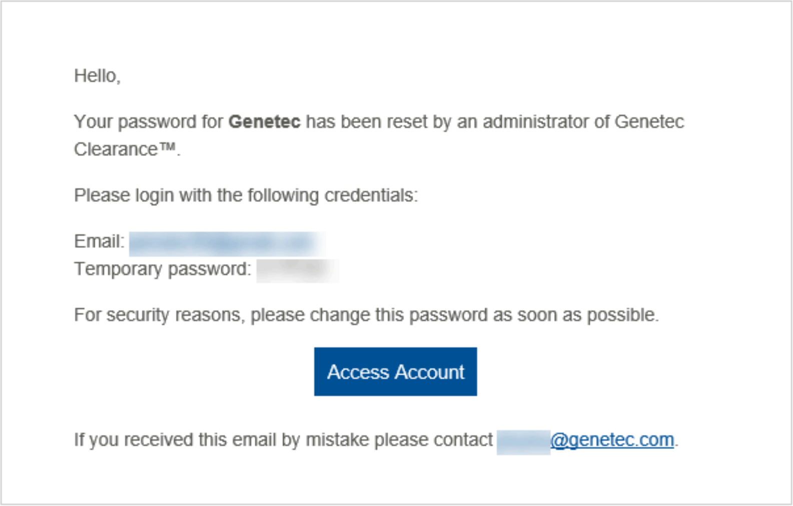
Hello,

[redacted] from **Genetec** has added you to the following file in Genetec Clearance™: TheftFromCar.MP4

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

Password reset

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



Hello,

Your password for **Genetec** has been reset by an administrator of Genetec Clearance™.

Please login with the following credentials:

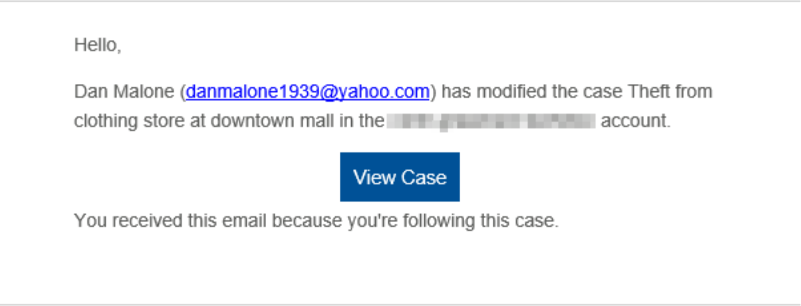
Email: [redacted]
Temporary password: [redacted]

For security reasons, please change this password as soon as possible.

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

Case modified

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



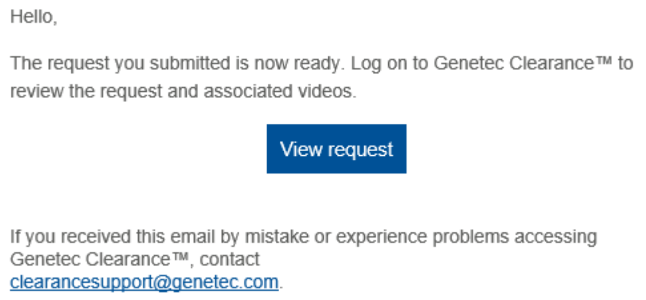
Hello,

Dan Malone (danmalone1939@yahoo.com) has modified the case Theft from clothing store at downtown mall in the [redacted] account.

You received this email because you're following this case.

Video request ready

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



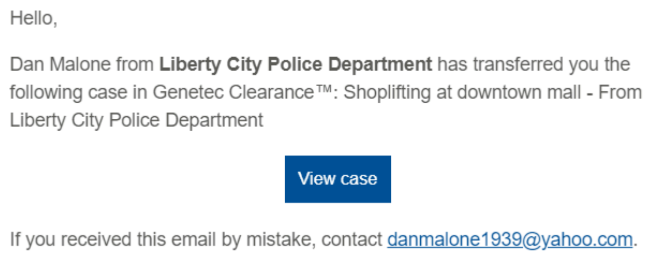
Hello,

The request you submitted is now ready. Log on to Genetec Clearance™ to review the request and associated videos.

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

Incoming case transfer

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



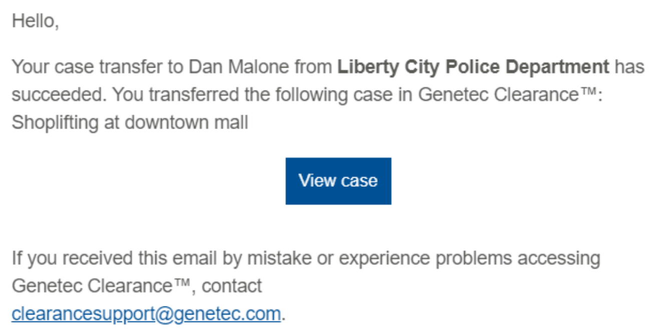
Hello,

Dan Malone from **Liberty City Police Department** has transferred you the following case in Genetec Clearance™: Shoplifting at downtown mall - From Liberty City Police Department

If you received this email by mistake, contact danmalone1939@yahoo.com.

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

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

Related Topics

Activating your account on page 34
Sharing cases on page 102
Sharing files on page 172
Resetting user passwords on page 84

2

Getting started

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

This section includes the following topics:

- "Deploying and using Clearance" on page 8
- "Deploying and using the Registry and Video Request modules in Clearance" on page 10
- "Logging on to Clearance" on page 12
- "Logging off from Clearance" on page 13
- "Changing language settings in Clearance" on page 14
- "Clearance videos" on page 15

Deploying and using Clearance

This topic organizes the setup, customization, and operation of Clearance into stages. Use it to make sure you are getting the most out of Clearance.

Step	Description	Where to find more information
Account setup and user management		
1	**Set up your account:** Configure your account information and establish your organization's network of users, groups, departments, and categories.	1. Activate your account 2. Configure account information 3. Create departments 4. Create user groups 5. Create users 6. Create categories
2	**Define policies:** Control access to and set retention policies for cases and evidence files.	1. Learn about permission levels 2. Define security policies • Refer to the security policy definitions list 3. Define video request policies • Refer to the video request policy definitions list 4. Set retention policies for cases and files
3	**Configure report templates:** Determine the contents and style of the reports used by your organization.	• Configure report templates
Operations		
1	**Build cases:** Create cases to document and track your investigations.	1. Create cases • Example of a case in Clearance 2. Assign personnel to a case 3. Change access policies for cases 4. Upload files to cases 5. Preview evidence in cases

Step	Description	Where to find more information
2	**Manage files:** Use files to support your cases.	• Review list of supported file formats • Configure file details • Change access policies for files • Search for cases or files • Create a file request
3	**Audit investigations:** Create reports that summarize and show actions performed on cases and files.	• Create a case summary report • Create an eDiscovery receipt • View the audit trail of a case • View the audit trail of a file • Learn about dashboards • Configure dashboards

Related Topics

Clearance videos on page 15

Deploying and using the Registry and Video Request modules in Clearance

This topic organizes the setup, customization, and operation of the Clearance registry and video request workflow into stages. Use it to make sure you are getting the most out of Clearance.

Step	Description	Where to find more information
Registry and video request setup		
1	**Set up the registry:** • Ensure your organization has an adequate subscription. • Learn about the registry and video request workflow.	• Registry and video request workflow overview
2	**Define policies:** • Control access level of access to the registry and video request modules.	• Define video request policies • Refer to the video request policy definitions list
3	**Create and customize video request forms and request IDs:** • Determine the contents and style of the forms used by your organization. • Configure ID templates that are automatically assigned to new requests.	• Create request forms • Create video request forms • Create participant enrollment forms • Configure ID templates for your requests
4	**Use participant enrollment to collaborate with partner organizations** • Create participant enrollment forms and, optionally, embed them in your organization's website so that third-parties can self-register and cooperate with investigations. • Participants navigate to the website where the form is embedded, complete the form, and then receive a confirmation email. After they validate using the link in the confirmation email, they are notified that their participation has been verified.	• Embed participant enrollment forms • Prompt potential partner organizations to enroll in the registry: • Send users a link to the enrollment form • Direct users to your organization’s website where the form is hosted • Learn about content security policies and how they can affect forms hosted on your organization's website
Video request workflow		

Step	Description	Where to find more information
1	**Initiate video requests:** • Search the registry for cameras of interest to your investigations. • Create video requests and gain access to relevant video recordings. • Invite guests to request video relevant to their investigations.	• Search for cameras of interest • Create video requests • Invite guests to submit video requests
2	**Conclude video requests:** • Review video requests and decide whether to approve or deny them. • Approve video requests that comply with your organization's requirements. • Cancel video requests that contain errors, do not conform to your organization's requirements, or are unnecessary.	• Review video requests • Approve video requests • Cancel video requests

Related Topics

Clearance videos on page 15

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.

Related Topics

Activating your account on page 34

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

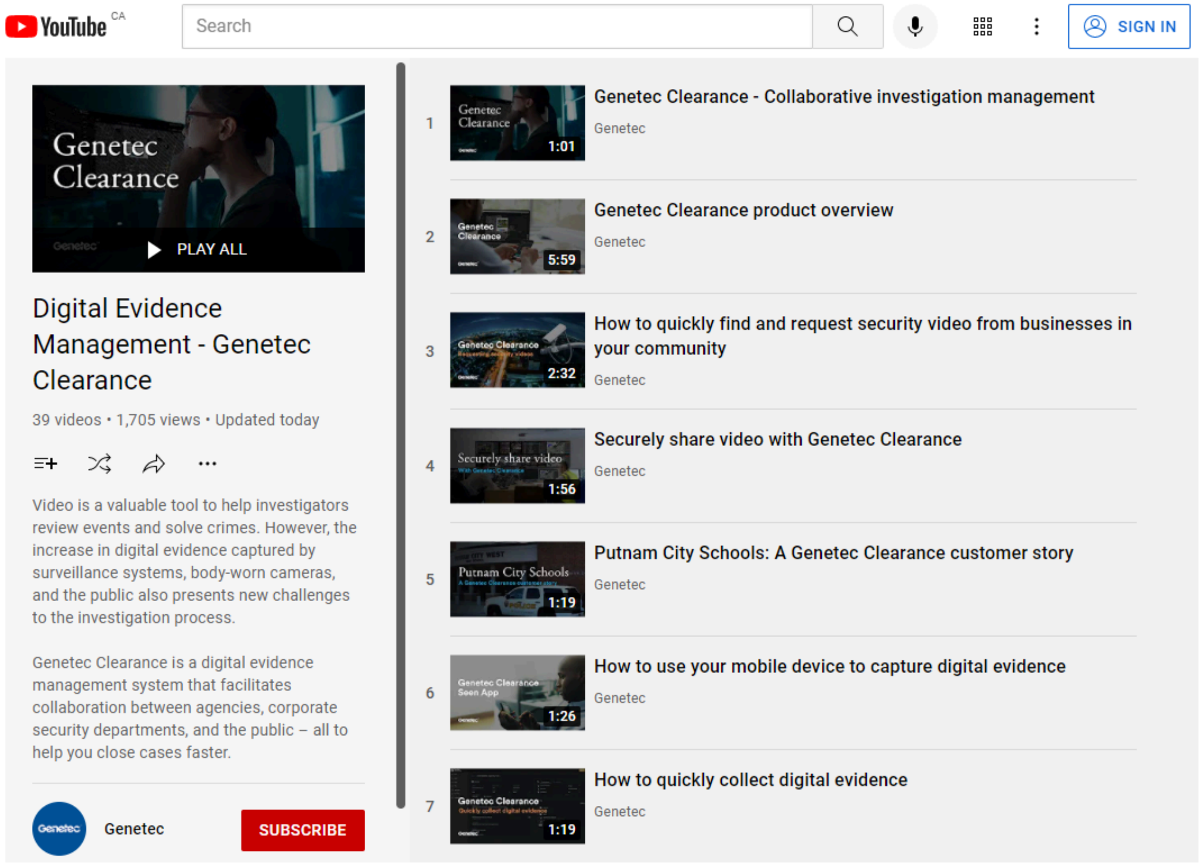
Changing language settings in Google Chrome:

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.

Clearance videos

Use the Clearance videos to help you learn about key features and understand the product. You can access all the videos in one place, the Clearance videos playlist.



Digital Evidence Management - Genetec Clearance

39 videos • 1,705 views • Updated today

Video is a valuable tool to help investigators review events and solve crimes. However, the increase in digital evidence captured by surveillance systems, body-worn cameras, and the public also presents new challenges to the investigation process.

Genetec Clearance is a digital evidence management system that facilitates collaboration between agencies, corporate security departments, and the public – all to help you close cases faster.

1 Genetec Clearance - Collaborative investigation management — Genetec — 1:01

2 Genetec Clearance product overview — Genetec — 5:59

3 How to quickly find and request security video from businesses in your community — Genetec — 2:32

4 Securely share video with Genetec Clearance — Genetec — 1:56

5 Putnam City Schools: A Genetec Clearance customer story — Genetec — 1:19

6 How to use your mobile device to capture digital evidence — Genetec — 1:26

7 How to quickly collect digital evidence — Genetec — 1:19

Click the image to access the Clearance videos playlist.

Videos can also be launched individually from relevant topics or the documentation homepage.

3

Release notes

Check out what's new in the latest release of Clearance.

This section includes the following topics:

- "What's new in Clearance" on page 17
- "Previous features and enhancements" on page 18
- "System requirements for Clearance" on page 25
- "Supported languages" on page 26

What's new in Clearance

Check out what is new in the latest update to Genetec Clearance™.

What's New: February 2025

- **Evidence multi-selection:** You can now select up to fifty files at a time when adding evidence to a case, allowing you to centralize files associated with different cases to one primary investigation.
- **Absolute and relative time toggle in the video editor:** You can now toggle between absolute and relative time when redacting a project in Clearance. The option is available when absolute time is included with the original video clip.
- **Filter search page by evidence source:** You can now filter your searches to display the sources from which evidence was uploaded to help build your cases in Clearance.

  This search filter is a helpful tool to identify your evidence, and help you audit device and app usage. For example, you can validate what videos were uploaded from body-worn cameras, or what files were uploaded from third-party requests. You can also search for multiple evidence sources at once.

  Evidence sources include:

  - Body-worn cameras
  - Clearance Drive
  - In-car video systems
  - Mass data import tool
  - Public uploads
  - Security Center
  - Video editor projects
  - Web portal uploads

For a complete list of all prior announcements, see Previous features and enhancements on page 18.

Previous features and enhancements

Genetec Clearance™ includes the following features and enhancements.

What's New: January 2025

- **Attach files to cases in bulk:** You can now select multiple files and folders from a case and directly add them to a new case. This helps you centralize files from multiple investigations, so all relevant information can be reviewed and shared from a principal case.

  Up to 50 files can be associated at a time. Case association details are captured in the audit trail.
- **Pin your active cases:** You can now pin cases to the homepage in Clearance to quickly locate the ones you're working on or that are under review. You can access your list of pinned cases from the toolbar.

What's New: December 2024

- **Adjust column width:** You can now expand the column width in the *Search*, *Requests* and *Registry* modules to display all information contained in fields of interest.

What's New: November 2024

- **User list report:** Admins can now download a CSV that lists all the users in their organization's Clearance account. Admins can then filter the report by username, email, state (Active or Inactive), and type (Regular or Guest).
- **Video trimming update:** You can now generate a video clip up to 8 hours long using the video trimming feature. For more information, see the following: About the video editor on page 215.

What's New: October 2024

- **AutoVu Cloudrunner Integration:** Automatic license plate recognition (ALPR) reads and reports can now be exported from AutoVu Cloudrunner™ to Clearance. This integration of the two products enables you to securely manage and share vehicle-based evidence.

  Cloudrunner is an ALPR system that captures advanced vehicle-based details to help investigators build cases and solve crimes. It is paired with cloud-based software accessible on a web portal. Cloudrunner and Clearance's infrastructure design facilitate a timely deployment.

  Integration benefits:

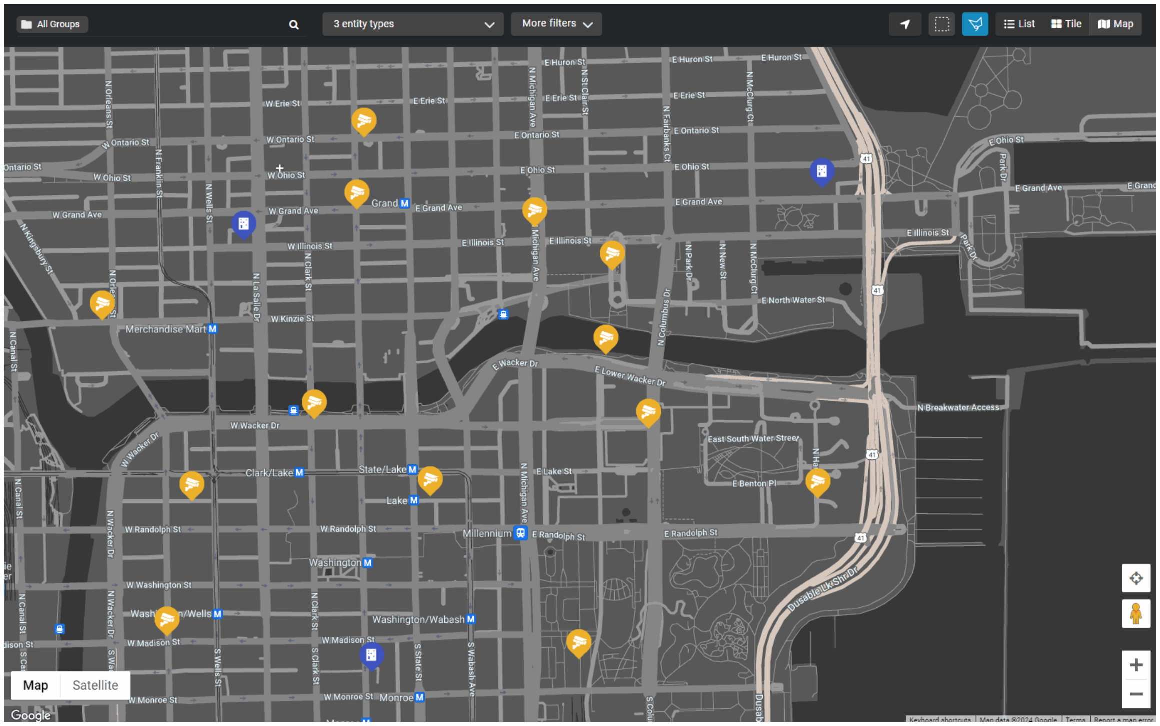
  - Facilitates the collection and management of vehicle-based evidence
  - Enhances collaboration on investigations by letting users easily share ALPR evidence with internal and external partners
  - Ensures that ALPR data is encrypted and that the chain of custody is maintained when shared

  Learn more here: https://www.genetec.com/product-releases/securely-share-evidence-from-cloudrunner-to-clearance

  Note: Cloudrunner is currently only available in North America. For more information about Cloudrunner, contact Cloudrunner-bd@genetec.com

What's New: September 2024

- **Polygon area selection option in camera registry:** In areas with dense camera coverage, it can be difficult to specify the cameras of interest from the map view. You can now define an area of interest when selecting cameras from the map view in the camera registry. This allows you to include only the cameras that are relevant to your video request.



- **New codec support:** New video formats have been added to the extended video codec library. They include h265, cam, dmd, ethe, mul, nov, pw3, sdv, wnm, and xba files.

  The extended video format library is included by default with all Plan 600 and Plan 1000 subscriptions. You can also purchase it as an add-on with other Clearance packages. For more information, contact your Genetec reseller.

What's New: August 2024

- **Video trimming notifications:** A new notification system now alerts users when their video trimming and stitching jobs are complete. The list of your recent notifications is located at the top of the page. Notifications are preserved during your browser session.
- **New version of Clearance Drive:** Transferring large files to Clearance? Use Clearance Drive to upload and download them faster than using your web browser.

  Learn more about Clearance Drive here. Click here to download the latest version.
- **Redesigned video editor:** We've updated the technology used by the video editor portal and revamped its look and feel. The update provides smoother navigation when creating redaction projects and streamlines the UI with the rest of the application.

What's New: July 2024

- **New Clearance plugin for Security Center:** The Clearance plugin for Security Center version 3.5.116.0 is now available. For more information, see the Clearance Plugin guide on the Tech Doc Hub.
- **Video conversion enhancements :** Updates to the video conversion pipeline provide improved support for standard video formats, including AVI, ASF, and MOV.

What's New: June 2024

- **Video trimming enhancements:** You can now trim and save videos directly to cases from the video trimming window. For i-PRO in-car recordings that include multiple microphones, you can choose which audio channel to merge and associate with the video. For more information, refer to Trimming video on page 218.

What's New: May 2024

- **Assigned officer name for BWC and in-car recordings:** Recordings uploaded from body-worn and in-car cameras now display the assigned officer's name next to the file name on the case and multi-tile pages.
- **Copy metadata to snapshots:** Files created from the snapshot feature now retain metadata from the original video. This metadata includes timestamps, the category, description, custom fields, location, and tags. For more information, refer to Video player controls on page 170.

What's New: April 2024

- **New version of the Clearance plugin for Security Center:** The Genetec Clearance™ plugin for Security Center version 3.5.98 is now available. The release includes the following improvements:
  - **Automated evidence exports:** In the latest version of the Genetec Clearance™ Plugin, you can use event-to-action to automate video exports to Clearance. When recordings in Security Center need to be protected, they can be uploaded automatically and preserved in Clearance. For example, videos linked to door forced open or intrusion events can be uploaded directly to a case. Operators and other stakeholders can then review the footage in Clearance from their web browser. The configurable retention settings available in Clearance create opportunities for organizations to extend video retention for event-related recordings. Distinct retention settings are useful for video evidence that requires special consideration or that must be shared with team members in other departments.
    - For more information, refer to Genetec Clearance™ Plugin Guide.
    - To download the plugin, click here.
  - **Raise custom event on Clearance export state:** You can now configure a custom event to notify Security Center users about the state of an export, such as if an export fails.
  - **Filter by export state in Clearance Activities Report:** You can now filter results by export state in the Genetec Clearance activities task, allowing you to better track export failures and other details.
  - **View other user exports privilege:** You can now assign a privilege that allows users to see other users' exports in the notification tray.
  - **Multi-factor authentication for Guest user accounts:** Clearance has transitioned users to the Genetec™ Login authentication system. Genetec Login is used across Genetec web applications and ensures that a single identity is used across all Genetec products. As part of the transition, Multi-factor authentication (MFA) is mandatory for all users that sign into Genetec applications. The second factor is a pin that is sent to the email address associated with the user's account.
    Users can manage their MFA preference from https://login.genetec.com/profile. The portal allows them to choose to send the second factor by email or by SMS.

What's New: February 2024

- **Upcoming change to Clearance login:** In the coming weeks, an update will be made to the Clearance login system that might affect you. Following the change, users who do not use a Single Sign-On (SSO) integration must reset their passwords the first time they login to Clearance. For more information, refer to Change to Clearance login on page 294.

What's New: November 2023

- **Reassign files to another officer:** Users can now reassign files recorded from body-worn cameras and in-car systems to a different officer. The file's associated officer and its permissions are updated when the assignment is changed. A user must belong to the *Manage Devices* policy and have *Manage* permissions on an evidence to modify the assigned officer field.
- **Genetec Fleet Monitoring integration:** Organizations can now publish a list of their vehicles equipped with Security Center in the Clearance registry module. Video can be requested from these on-board systems and automatically uploaded to Clearance for review and sharing.
- **New version of the Clearance plugin for Security Center:** The Genetec Clearance™ plugin for Security Center version 3.5.63 is now available. The release includes the following improvements:

    - **Support for vehicle requests:** You can now request video, along with telemetric data and metadata, from vehicles equipped with Genetec Security Center. When enabled, video requests can be made from the Clearance registry and request modules. Click **here** for more information.
    - **Default department support:** The default department configured in your Clearance account is now automatically populated when exporting video from Security Desk.
    - **Throttle number of concurrent exports:** Admins can throttle the number of concurrent exports from their Archivers to accommodate bandwidth limitations. Contact Genetec Support for information about this option.
    - **Bug fixes and performance enhancements:** A number of fixes and performance improvements are available in this release. Refer to the Genetec Clearance Plugin Guide 3.5.63 release notes for a complete list.

- **Case and file tagging with i-PRO uploads:** Recordings tagged from the i-PRO Front End system and body worn web app can now be automatically associated with cases in Clearance. The association is based on files sharing the same incident or case file number. Case permissions are set based on the default department configured in the account.

  A license is required to activate this feature. For more information, contact your reseller.
- **Playback vehicle metadata:** Vehicle metadata, including speed, latitude and longitude positions, and triggers can now be played in sync while reviewing video from on-board systems. The metadata can be uploaded from systems integrated with the Clearance APIs and is available with Genetec Security Center mobility systems and i-PRO in-car systems.

What's New: September 2023

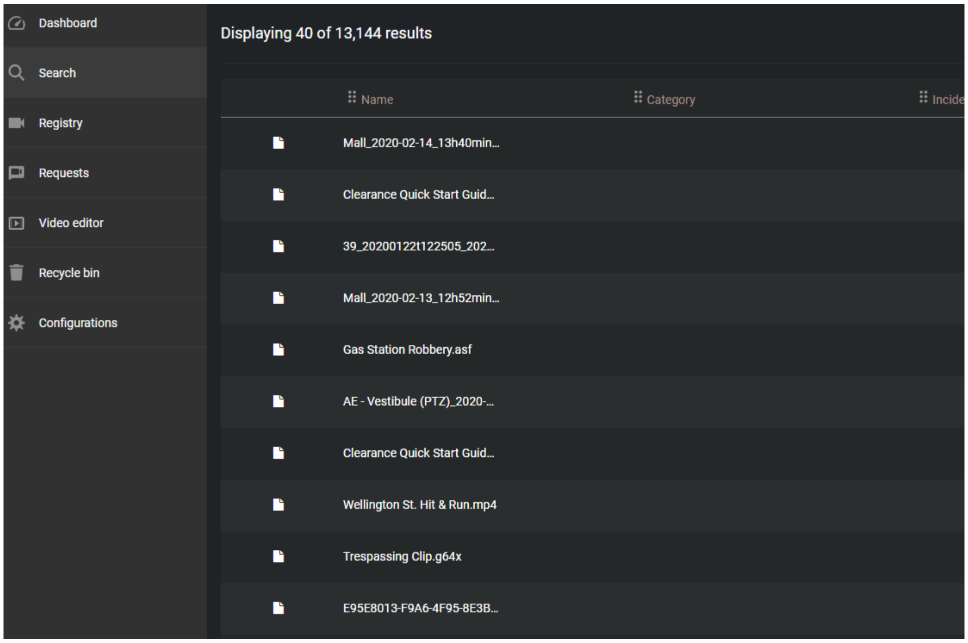
- **Set Default department:** Administrators can now set a default department that is pre-selected when users create new cases. This default selection helps mitigate entry error by applying a base template for case permissions. The default department can also be leveraged by integrations that use the Clearance API, allowing them to apply the default template when creating new cases in Clearance. For more information, refer to Setting a default department on page 57.

What's New: August 2023

- **Automatic case naming:** Case names can now be automatically generated when cases are created in Clearance. This feature ensures that a standard naming convention is respected and eliminates the risk of data entry error.
- **Display landmark names:** You can now use landmark names to tag case and file locations. Landmarks can consist of buildings, transit stations, and monuments. A location tag is automatically generated based on the type of location returned from the results.

What's New: July 2023

- **Thumbnail preview in search:** You can now preview a thumbnail of images and videos by hovering over the results of their search. For more information, refer to Searching for cases or files on page 113.



Displaying 40 of 13,144 results

Name	Category	Incide
Mall_2020-02-14_13h40min...		
Clearance Quick Start Guid...		
39_20200122t122505_202...		
Mall_2020-02-13_12h52min...		
Gas Station Robbery.asf		
AE - Vestibule (PTZ)_2020-...		
Clearance Quick Start Guid...		
Wellington St. Hit & Run.mp4		
Trespassing Clip.g64x		
E95E8013-F9A6-4F95-8E3B...		

What's New: June 2023

- **File groups automatically populate in multi-tile view:** The multi-tile view is now automatically populated with multiple evidence files when a group of files is opened. For more information, refer to Reviewing media on page 168.

What's New: May 2023

- **Manage permissions required in departments:** It is now mandatory for at least one user, or user group, to be assigned manage permissions when configuring a department. This ensures that the desired stakeholders have full rights to cases when they are created. For more information, refer to Creating departments on page 55.
- **Camera groups are now available in the registry module:** You can now publish camera groups in the Clearance registry module based on the areas that are configured in Security Center. The update accelerates the identification of cameras relevant to a request and allows users to select devices in a desired region more easily. Groups can be published from the Security Center plugin and are supported through API integration with other video systems. Click **here** to download version 3.5.38 of the Clearance plugin for Security Center.
- **Send reports from Genetec Mission Control™ to Clearance:** Security Center operators can now export incident reports and associated videos to cases in Clearance. Organizations can now quickly share access to event information and preserve incident details in accordance with operating procedures. The integration is supported in Mission Control version 3.1.2, and requires the Clearance plugin for Security Center version 3.5.38 and later.

What's New: March 2023

- **Preview thumbnails in Search:** You can now preview thumbnail images of files in search results. Thumbnails are only available for files that each user has access to. This update speeds up the process of identifying files and cases that require your review.

What's New: December 2022

- **New version of the Clearance plugin for Security Center:** The Clearance plugin for Security Center version 3.5 includes the following improvements:
  - Participant locations in Security Center Maps: The new plugin displays participants from the Clearance camera registry module in the Maps task. The integration with Clearance allows Security Desk operators can use the Clearance integration to identify the location of participants near incidents they are monitoring and provides a link to access participant details and initiate a video request.
  - Deactivated departments and categories: Deactivated departments and categories are no longer available for selection in the Security Desk export wizard.
  - Scalability improvements: This update offers improved performance when adding thousands of entities in the plugin camera selection.
- **Security policy to download files flagged by malware scan:** A new security policy has been added that allows administrators to download files that have been flagged as potentially malicious by a malware scan. Only users included in this security policy can download files that have been flagged by the malware scan.

  NOTE: The malware scan supports files that are up to 4GB in size.
- **Clearance Drive updates:** Clearance Drive will automatically be updated for users who have already installed the application. If you have not yet installed Clearance Drive, you can learn more about it here. The update includes bug fixes and upload performance improvements.

What's New: October 2022

- **Download Clearance Drive:** With Clearance Drive you can transfer digital evidence faster when connected to a high-speed network. Use this app to search, copy, and transfer large quantities of evidence to Clearance from a dedicated application or from the File explorer. For more information, refer to Installing Clearance Drive on page 253. Click here to download the app.

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

  available languages.

  ▶
- **Map I-PRO evidence metadata to files in Clearance:** Notes, case file numbers, and other metadata tagged to videos from the i-PRO Front-End application are now mapped to the associated fields when evidence is uploaded to Clearance. This feature applies to users who are included in the **Manage i-PRO user account credentials** device policy and have configured their i-PRO user account password. For more information, refer to Defining device policies on page 159

What's New: September 2022

- **Support for i-PRO snapshot metadata:** Timestamp and officer assignment details are now displayed on snapshots captured from i-PRO BWC cameras.
- **Collapse and expand video timeline:** Users can now collapse the multi-tile player timeline into a single, consolidated view to simplify video playback and review.
- **Case and file list export:** Custom fields, assigned officer, and the URLs of each case and file are now included in the search result export. All results from a search can be exported as a CSV file from the Search page.

What's New: August 2022

- **i-PRO BWC and in-car device management:** You can now update the firmware and configuration of i-Pro body-worn cameras and in-car systems directly from Clearance. A new setting also allows administrators to create device groups, in which cameras can be logically grouped based on their model and the team of officers they are assigned to. New firmware and configurations can then be dispatched to individual devices or to the groups that have been defined in Clearance. The capability is supported with the i-PRO BWC MK3, BWC 4000, and VPU 4000 systems. For more information about supported firmware versions and i-PRO BWC Configuration Tool version requirements, refer to the following: About device groups on page 155.

What's New: April 2022

- **Import folder hierarchy to cases:** Folders you upload to cases in Clearance now maintain the same file structure, saving time organizing the folder hierarchy in your cases.

What's New: March 2022

- **Restrict access to camera details in registry:** Administrators can now define which users are able to view and select cameras as part of their video requests. You can use this video request policy to control access to camera information, while still permitting users to make video requests involving cameras they have access to.
- **Automatically map request attributes to cases:** To reduce data entry, standard fields that are common between video requests and cases now have their values automatically mapped when a new case is generated from a request. This includes time range, category, and location information. The Category field is only available to Regular users when entering a new request and is hidden from Guests. For more information, see Requesting video on page 199.

What's New: February 2022

- **Support for multiple form types:** You can now publish multiple request form versions to tailor the information that is collected for different request scenarios. For example, a form can be configured for internal requests that has different fields than the one used by external parties. The applicable form is selected by the requesting party when entering a new request and follows the organization’s approval workflow.
- **Faster G64 conversion:** The G64 service has been updated to reduce the time required to convert recordings from Security Center. With this improvement, Clearance can more efficiently scale when there are spikes in the number of G64 files that are sent for conversion.
- **Automatic case and request ID numbers:** You can now automatically generate incident, record, and request ID numbers to facilitate the classification of cases and requests. Administrators can define the convention used to generate IDs and support the inclusion of common properties such as the date, user or creator name, and other system properties as part of the ID template. For more information, see Configuring ID templates on page 67.
- **Video trimming:** You can now trim long video recordings when sending files to the video editor. Choose to keep only the relevant sequence of a longer video and accelerate the redaction and review of the recording. For more information, see Trimming video on page 218.

What's New: January 2022

- **Sort search columns:** You can now sort results in the **Search** page in ascending or descending order to quickly find the cases and files that you are looking for.
  - Name
  - Creation time
  - Created by
  - Start time
  - End time
  - State
  - Device serial number
  - Last modified time
  - Last modified by
- **Internet Explorer 11 end of support:** With the upcoming end of life of Internet Explorer 11 scheduled in June 2022, the browser is no longer supported by Clearance. For the best experience using Clearance use Google Chrome or Microsoft Edge.

System requirements for Clearance

For Genetec Clearance™ to run efficiently in your web browser, the computer or mobile device that you use must meet certain software and hardware requirements.

The requirements for Clearance software are as follows:

Desktop Requirements

- Cookies and JavaScript are enabled in the web browser that you are using.

Clearance is compatible with the following desktop operating systems and web browsers.

Operating system	Supported browsers
Microsoft® Windows 7, 8.0, 8.1, 10	Microsoft® Edge, and Google Chrome
Mac OS 10.5.7	Apple Safari 6

Mobile Requirements

Clearance is compatible with the following mobile operating systems and web browsers.

Operating system	Supported browsers	Supported Devices
Android	Google Chrome (latest version only)	Android tablets and phones
iOS 9.0 and later	Apple Safari 6 and Google Chrome	iPads, iPad Minis, and iPhones

NOTE: Performing video *redaction* on a mobile device is not supported.

Clearance Uploader Requirements

The following desktop operating system requirements are required to run the Clearance Uploader.

- Microsoft® Windows 7 and later
- Microsoft® Windows Server 2008 R2 and later
- Microsoft .Net Frameworks 4.6
- Minimum ram requirement is 2GB
- Storage requirements can vary depending on the temporary storage that the application requires for video

Genetec Clearance™ Capture Requirements

To use the Genetec Clearance™ Capture Google Chrome extension you must have Google Chrome browser version 59 or later.

Supported languages

Clearance is available in the following languages.

Clearance web portal

- English
- French
- Spanish
- German
- Dutch

Clearance public upload feature

- English
- French
- Spanish
- German
- Arabic
- Dutch

Clearance Uploader

Clearance Uploader is available in English only.

Documentation

- *Clearance User Guide* (English, French, and Spanish)
- *Clearance User Guide for Guests* (English, French, and Spanish)

IMPORTANT: Translation of documentation is ongoing. Documentation in languages other than English might not be complete at the time of release. For the latest version of the documentation, see the Genetec TechDoc Hub.

4

User interface tour

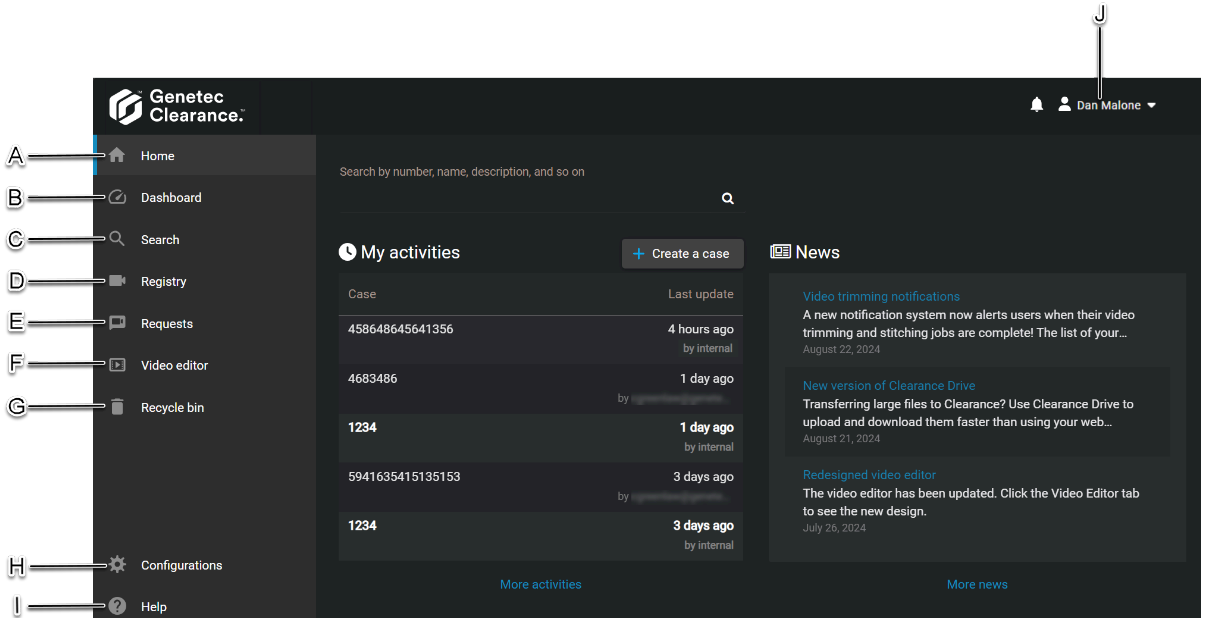
Get familiar with the user interface in Clearance.

This section includes the following topics:

- "Overview of the menu tabs in Clearance" on page 28
- "Overview of the Home page" on page 30

Overview of the menu tabs in Clearance

The menu tabs in Clearance are always available, no matter where you are in the user interface.



Case	Last update
458648645641356	4 hours ago by internal
4683486	1 day ago by [redacted]
1234	1 day ago by internal
5941635415135153	3 days ago by [redacted]
1234	3 days ago by internal

Video trimming notifications
A new notification system now alerts users when their video trimming and stitching jobs are complete! The list of your...
August 22, 2024

New version of Clearance Drive
Transferring large files to Clearance? Use Clearance Drive to upload and download them faster than using your web...
August 21, 2024

Redesigned video editor
The video editor has been updated. Click the Video Editor tab to see the new design.
July 26, 2024

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

A	**Home**	Visit the homepage to conduct a search or visit the news, *my activities*, and learn sections.
B	**Dashboard**	View storage and case data metrics on your account dashboard.
C	**Search**	Search and filter the complete list of cases, files, and cameras in Clearance.
D	**Registry**	Build a registry of cameras and view it as a list or map.
E	**Requests**	Check the history of all requests and their statuses.
F	**Video editor**	Display a list of editing projects and use it to search for, open, and modify redacted files.
G	**Recycle bin**	Display a list of cases and files that can be searched and filtered in the recycle bin.
H	**Configurations**	Display a complete list of users, groups, *integrations*, departments, categories, and devices that can be searched and filtered. Modify any one of these entities or configure security policies, retention policies, account information, and report templates.

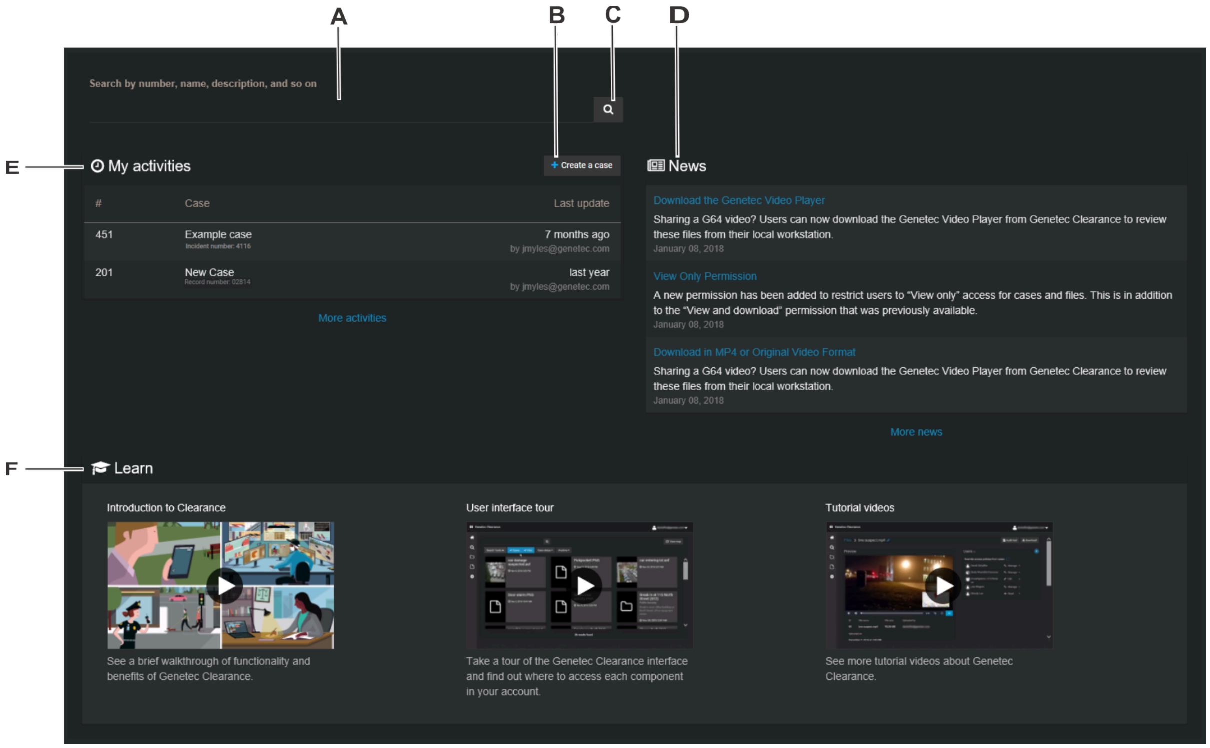
I	**Help**	Open the user guide documentation or create a support ticket.
J	**Account options**	Display additional account options: • **Change account**: Click to return to the logon screen to select another account. • **Sign out**: Click to log off.

Example

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

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.



Search by number, name, description, and so on

My activities

+ Create a case

#	Case	Last update
451	Example case Incident number: 4116	7 months ago by jmyles@genetec.com
201	New Case Record number: 02814	last year by jmyles@genetec.com

More activities

News

Download the Genetec Video Player

Sharing a G64 video? Users can now download the Genetec Video Player from Genetec Clearance to review these files from their local workstation.

January 08, 2018

View Only Permission

A new permission has been added to restrict users to “View only” access for cases and files. This is in addition to the “View and download” permission that was previously available.

January 08, 2018

Download in MP4 or Original Video Format

Sharing a G64 video? Users can now download the Genetec Video Player from Genetec Clearance to review these files from their local workstation.

January 08, 2018

More news

Learn

Introduction to Clearance

See a brief walkthrough of functionality and benefits of Genetec Clearance.

User interface tour

Take a tour of the Genetec Clearance interface and find out where to access each component in your account.

Tutorial videos

See more tutorial videos about Genetec Clearance.

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.

5

Account setup

Configure your settings in Clearance.

This section includes the following topics:

- "Setting up your account" on page 33
- "Activating your account" on page 34
- "Configuring your account information" on page 36
- "Configuring your report templates " on page 39
- "Setting the retention period for cases and files" on page 40
- "Permission levels" on page 43
- "Creating user groups" on page 46
- "Creating user accounts" on page 48
- "Synchronizing users and groups using SCIM protocol " on page 50
- "Adding existing users to groups" on page 53
- "Creating integrations" on page 54
- "Creating departments" on page 55
- "Creating incident categories" on page 58
- "Defining video request policies" on page 59
- "Defining security policies" on page 63
- "Creating fields" on page 66
- "Configuring ID templates" on page 67
- "Creating forms" on page 69
- "Resetting user passwords" on page 84
- "Searching for users or groups" on page 85
- "Creating support tickets" on page 86
- "Downloading a user list report" on page 87

Setting up your account

With Clearance, you can collaborate on cases and share digital evidence and media with other authorized investigators. As a site administrator, you must set up your account before inviting others to join the site.

Procedure

1. Activate your Clearance account.
2. Configure your account information.
3. Create departments for your organization.
4. Create user groups so that you can assign the same access policy to multiple users for a case or file.
5. Create user accounts so that users can join the Clearance site.
6. Create categories for the different types of incidents so that you can properly classify incidents when creating cases.
7. Create a sample case.

Example

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

▶

Activating your account

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

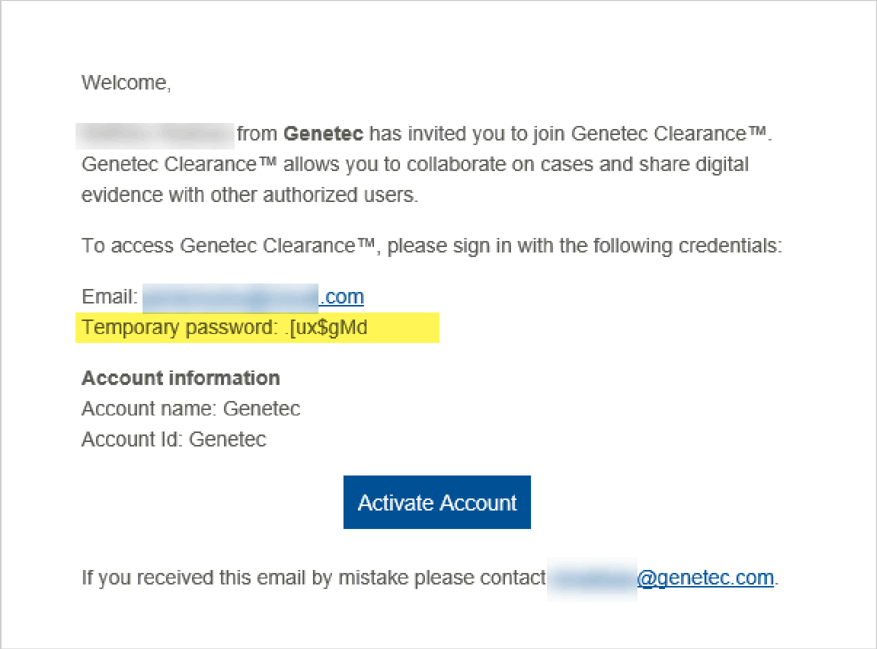
Before you begin

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**.



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:

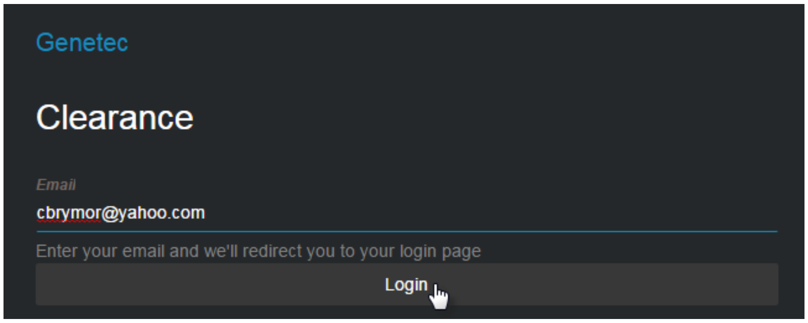
Email: [redacted].com
Temporary password: .[ux$gMd

Account information
Account name: Genetec
Account Id: Genetec

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

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**.



Email: cbrymor@yahoo.com

Enter your email and we'll redirect you to your login page

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.

▶

Related Topics

Logging on to Clearance on page 12

About email notifications in Clearance on page 3

Configuring your account information

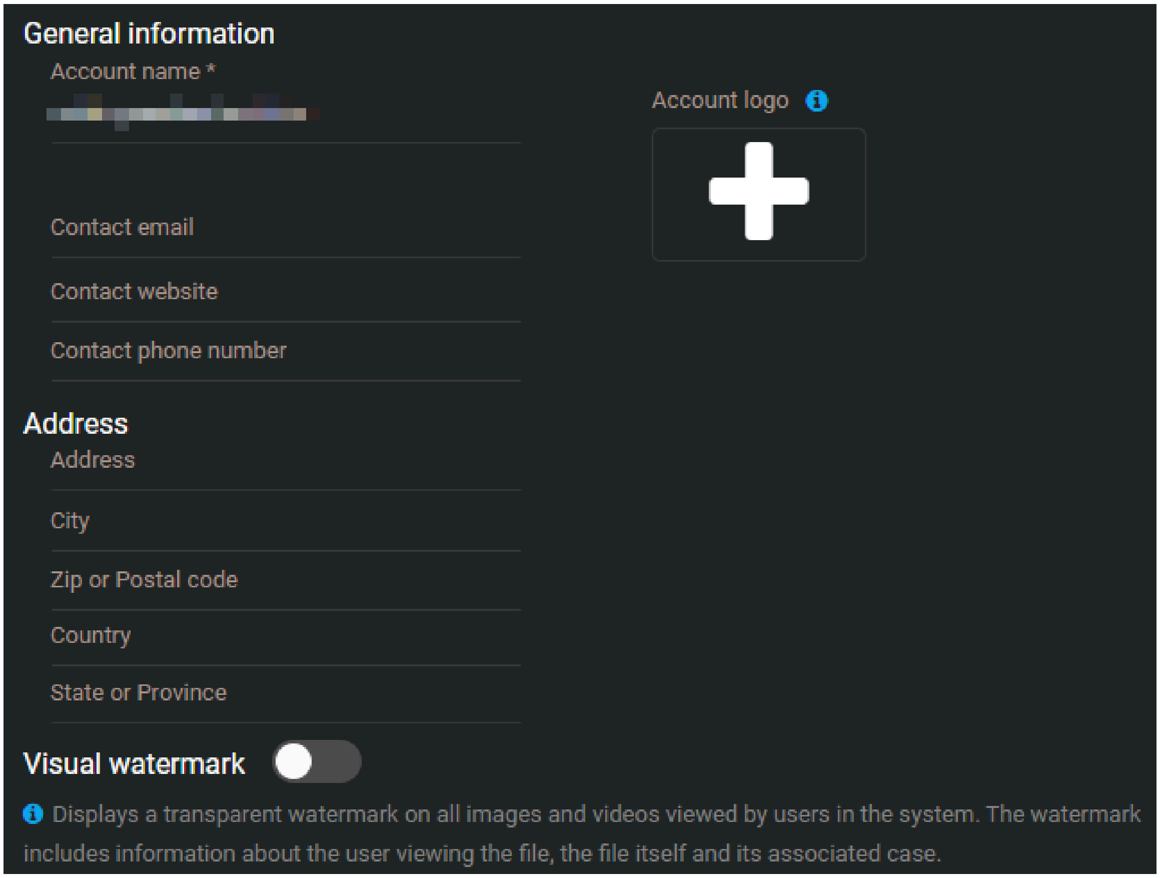
Before you can change your file request terms and conditions, create guest user terms and conditions, or apply the digital watermark feature, you must configure your account information.

Before you begin

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

Procedure

1 Click **Configurations** > **Account information**.



Account name * [redacted]

Visual watermark ○

Displays a transparent watermark on all images and videos viewed by users in the system. The watermark includes information about the user viewing the file, the file itself and its associated case.

2 Complete the following fields:

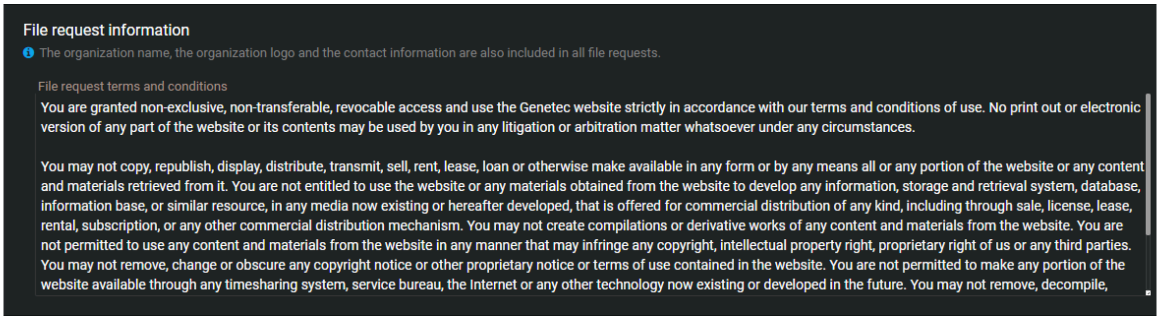
- **Account name:** The name of your organization.
- **Contact email:** An email address listed in system notification emails that can be used by parties whom you share cases and evidence with to contact your organization.
- **Contact website:** A website for your organization.
- **Contact phone number:** A phone number for contacting your organization.

3 Complete the following fields:
   - **Address:** The address of your organization.
   - **City:** The city where your organization is located.
   - **Zip or Postal code:** The Zip or Postal code your organization uses.
   - **Country:** The country where your organization is located.
   - **State or Province:** The state or province where your organization is located.

4 (Optional) Enable the **Visual watermark** option.

   NOTE: Visual watermarks are applied to videos and images previewed in Clearance. The watermark is not applied to files exported from the application.

5 In the **File request information** field, enter your organization's *File request terms and conditions*.



File request information

The organization name, the organization logo and the contact information are also included in all file requests.

File request terms and conditions

You are granted non-exclusive, non-transferable, revocable access and use the Genetec website strictly in accordance with our terms and conditions of use. No print out or electronic version of any part of the website or its contents may be used by you in any litigation or arbitration matter whatsoever under any circumstances.

You may not copy, republish, display, distribute, transmit, sell, rent, lease, loan or otherwise make available in any form or by any means all or any portion of the website or any content and materials retrieved from it. You are not entitled to use the website or any materials obtained from the website to develop any information, storage and retrieval system, database, information base, or similar resource, in any media now existing or hereafter developed, that is offered for commercial distribution of any kind, including through sale, license, lease, rental, subscription, or any other commercial distribution mechanism. You may not create compilations or derivative works of any content and materials from the website. You are not permitted to use any content and materials from the website in any manner that may infringe any copyright, intellectual property right, proprietary right of us or any third parties. You may not remove, change or obscure any copyright notice or other proprietary notice or terms of use contained in the website. You are not permitted to make any portion of the website available through any timesharing system, service bureau, the Internet or any other technology now existing or developed in the future. You may not remove, decompile,

6 In the *Account logo* section, click the logo field.

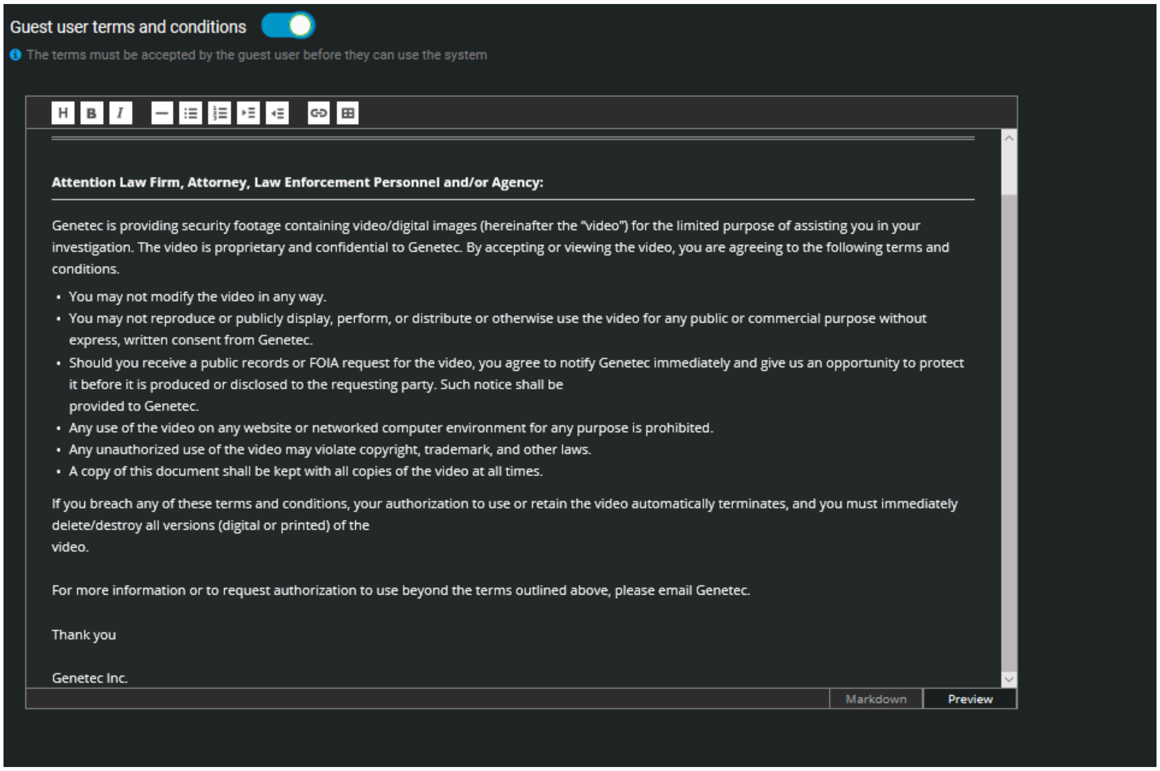
   a) Navigate to and select the image file to use as the logo for your account.

   b) Click **Open**.

   BEST PRACTICE: Use an image file with a transparent background. The maximum recommended size for an account logo is 350 pixels wide by 70 pixels high.

7 (Optional) Enable the **Guest user terms and conditions** option and add your terms and conditions for guests.

Content can be pasted in the *Guest user terms and conditions* text box from a word processing application. You can then edit and reformat the content directly in the text box.


Guest user terms and conditions
The terms must be accepted by the guest user before they can use the system
H
B
I
Markdown
Preview

Attention Law Firm, Attorney, Law Enforcement Personnel and/or Agency:

Genetec is providing security footage containing video/digital images (hereinafter the "video") for the limited purpose of assisting you in your investigation. The video is proprietary and confidential to Genetec. By accepting or viewing the video, you are agreeing to the following terms and conditions.

- You may not modify the video in any way.
- You may not reproduce or publicly display, perform, or distribute or otherwise use the video for any public or commercial purpose without express, written consent from Genetec.
- Should you receive a public records or FOIA request for the video, you agree to notify Genetec immediately and give us an opportunity to protect it before it is produced or disclosed to the requesting party. Such notice shall be provided to Genetec.
- Any use of the video on any website or networked computer environment for any purpose is prohibited.
- Any unauthorized use of the video may violate copyright, trademark, and other laws.
- A copy of this document shall be kept with all copies of the video at all times.

If you breach any of these terms and conditions, your authorization to use or retain the video automatically terminates, and you must immediately delete/destroy all versions (digital or printed) of the video.

For more information or to request authorization to use beyond the terms outlined above, please email Genetec.

Thank you

Genetec Inc.

8 Click **Save**.

Example

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

Configuring your report templates

To modify the terms of acknowledgement in your eDiscovery Receipt report, you must configure your report templates.

Before you begin

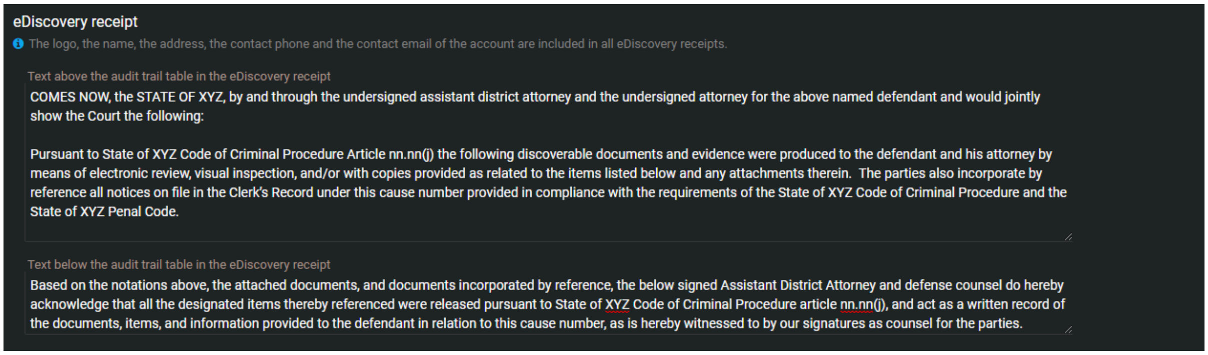
Make sure that you have a secure connection to the web.

What you should know

- The account name, the account logo, and the contact information are clearly displayed in all *eDiscovery receipt* reports.
- The contact information shown in your reports is specific to the account and is automatically generated from fields specified in the **Account information** page.
- The *terms of acknowledgment* statement is typically configured by the account administrator and can include customized criminal code statements which can vary for the office, state, region and so on.

Procedure

1 Click **Configurations** > **Report templates**.



eDiscovery receipt

The logo, the name, the address, the contact phone and the contact email of the account are included in all eDiscovery receipts.

Text above the audit trail table in the eDiscovery receipt

COMES NOW, the STATE OF XYZ, by and through the undersigned assistant district attorney and the undersigned attorney for the above named defendant and would jointly show the Court the following:

Pursuant to State of XYZ Code of Criminal Procedure Article nn.nn(j) the following discoverable documents and evidence were produced to the defendant and his attorney by means of electronic review, visual inspection, and/or with copies provided as related to the items listed below and any attachments therein. The parties also incorporate by reference all notices on file in the Clerk's Record under this cause number provided in compliance with the requirements of the State of XYZ Code of Criminal Procedure and the State of XYZ Penal Code.

Text below the audit trail table in the eDiscovery receipt

Based on the notations above, the attached documents, and documents incorporated by reference, the below signed Assistant District Attorney and defense counsel do hereby acknowledge that all the designated items thereby referenced were released pursuant to State of XYZ Code of Criminal Procedure article nn.nn(j), and act as a written record of the documents, items, and information provided to the defendant in relation to this cause number, as is hereby witnessed to by our signatures as counsel for the parties.

2 In the *Text above the audit trail table in the eDiscovery receipt* section, cut and paste the *Terms of acknowledgement* statements that you require for your organization.

3 In the *Text below the audit trail table in the eDiscovery receipt* section, cut and paste the *Terms of acknowledgement* statements that you require for your organization.

4 Click **Save**.

Your report template is now configured.

Setting the retention period for cases and files

To ensure that evidence is deleted when it is no longer required, you can configure retention periods for cases and files in the recycle bin. You can also configure retention periods to automatically delete files by source or category.

What you should know

NOTE: Users must have *account admin* permission to configure retention policies.

- Digital evidence can be stored in accordance with the requirements of the incident. For example, the incident category of the case will be used to determine the *retention policy*.
- Digital evidence can also be stored based on the device type that is associated with the recordings. For example, *body worn camera (BWC)* video could be kept for 90 days, public surveillance video could be kept for 30 days, and so on.

  If a file is associated with a case, it inherits the retention policy of the case. If the file retention policy is longer than the case retention, then the file retention policy is used.

CAUTION: Modifying retention policies can result in permanent loss of file data or automatic deletion of files.

NOTE: Files will only be deleted if all cases associated with the file(s) are closed. Any files without a category will use the associated case(s) category if applicable. The longest source or category retention policy will be used.

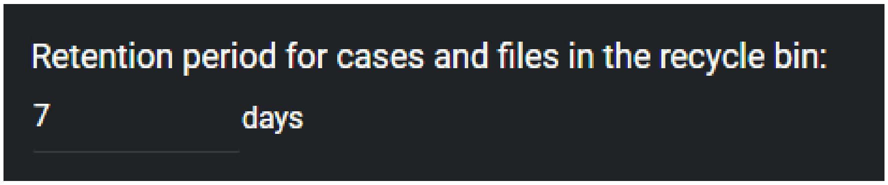
Closing and reopening cases also affects the retention period for files. For example, when a closed case is reopened, the scheduled deletion for files associated with that case is changed back to **Never delete** provided that the file is not in the recycle bin.

Procedure

To set the recycle bin retention period:

1 Click **Configurations** > **Retention Policies**.

2 Select the retention period that you require for cases and files in the recycle bin.
The default setting is 7 days and the maximum is 365 days.



Retention period for cases and files in the recycle bin:
7 days

3 Click **Save**.

4 Select the **I understand and want to modify the retention policies** check box and click **Save Modifications**.

To automatically delete files by source:

1 Click **Configurations** > **Retention Policies**.

2 Specify a retention period for each source that is defined in the system.

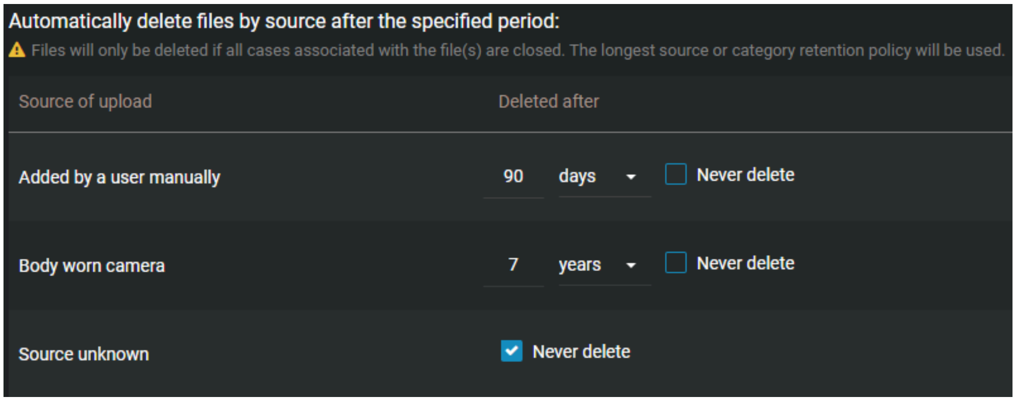
The **Never delete** check box is selected by default, to keep your files indefinitely.

a) (Optional) To specify a retention period in days, clear the **Never delete** check box next to the source that you require and select a value.

The maximum value is 36,500 days.

b) (Optional) To specify a retention period in years, clear the **Never delete** check box next to the source that you require and select a value.

The maximum value is 100 years.



Automatically delete files by source after the specified period:

⚠ Files will only be deleted if all cases associated with the file(s) are closed. The longest source or category retention policy will be used.

Source of upload	Deleted after
Added by a user manually	90 days ▾ □ Never delete
Body worn camera	7 years ▾ □ Never delete
Source unknown	☑ Never delete

3 Click **Save**.

4 Select the **I understand and want to modify the retention policies** check box and click **Save Modifications**.

To automatically delete files by category:

1 Click **Configurations** > **Retention Policies**.

2 Specify a retention period for each category that is defined in the system:

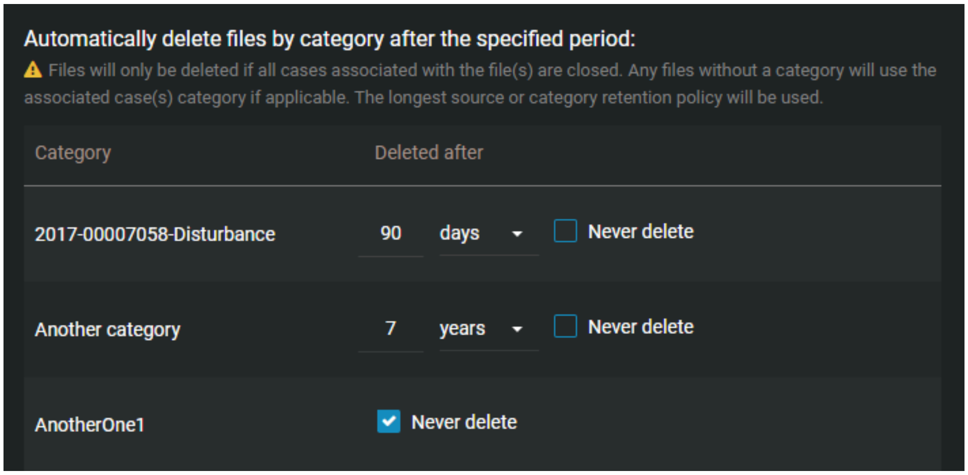
The **Never delete** check box is selected by default, to keep your files indefinitely.

a) (Optional) To specify a retention period in days, clear the **Never delete** check box next to the category that you require and select a value.

The maximum value is 36,500 days.

b) (Optional) To specify a retention period in years, clear the **Never delete** check box next to the category that you require and select a value.

The maximum value is 100 years.



Automatically delete files by category after the specified period:

⚠ Files will only be deleted if all cases associated with the file(s) are closed. Any files without a category will use the associated case(s) category if applicable. The longest source or category retention policy will be used.

Category	Deleted after
2017-00007058-Disturbance	90 days ▾ □ Never delete
Another category	7 years ▾ □ Never delete
AnotherOne1	☑ Never delete

3 Click **Save**.

4 Select the **I understand and want to modify the retention policies** check box and click **Save Modifications**.

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

You can view or search the recycle bin to identify any cases or files that might be affected by the retention periods.

For example:

- If you change the retention period for the recycle bin some files could be permanently deleted.
- If you change the file retention period by source or category files could be automatically deleted and end up in the recycle bin.

Cases and files that have been automatically deleted remain available in the recycle bin for the specified retention period. All deleted cases or files can be restored while they are in the recycle bin.

Related Topics

Deleting cases on page 122

Deleting files on page 188

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. To make PDF files available to these users, see Changing access policies for files on page 185.

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.

Related Topics

Defining security policies on page 63
Security policy definitions list on page 63
Defining video request policies on page 59
Video request policy definitions list on page 61

Creating user groups

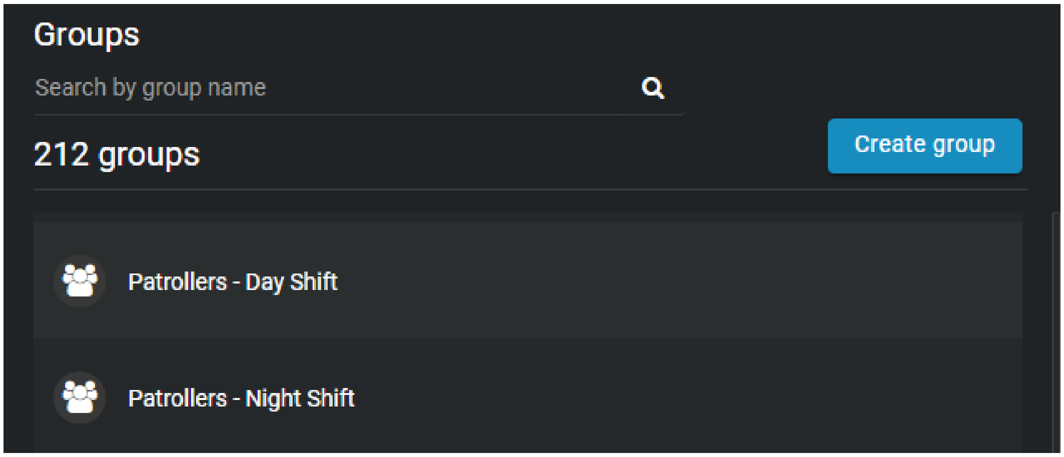
To organize users by rank or role, and to simplify the assignment of permission and security policies in the system, you can create user groups.

What you should know

You can create user groups for specific departments, groups that apply to multiple or all departments, or groups that reside outside departments. Users can belong to multiple groups. You must be an account administrator to create Clearance user groups.

Procedure

1 Click **Configurations** > **Groups**.



2 Click **Create group** (+).

3 In the **Name** field, enter an applicable name for the group.

4 Assign security and video request policies to the group.

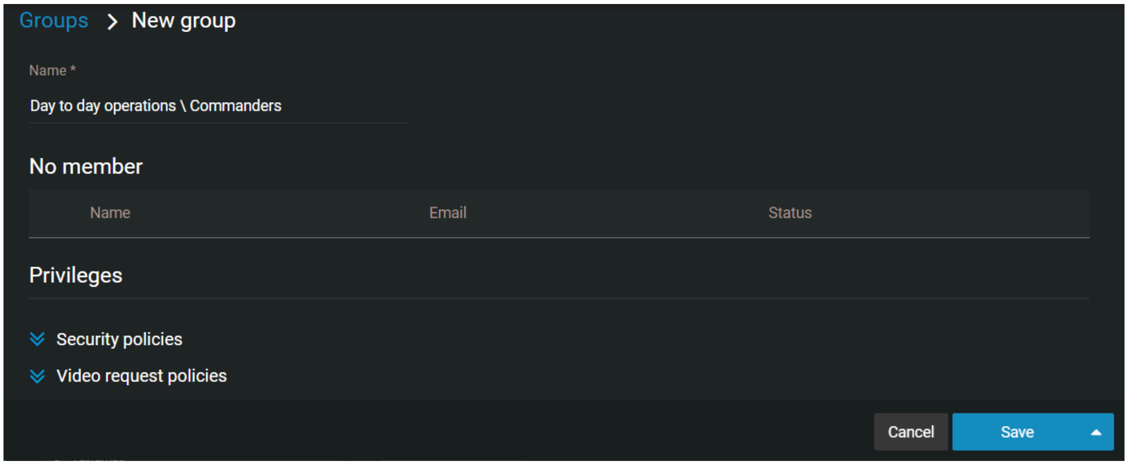
5 Click **Save**.

Your user group is created. To assign access policies to cases for this group, you can either add this group to a department and then define the access policy, or define the group's access policy on a case by case basis.

Example

Let us assume you want the police commanders within your organization to have full access to all new cases, regardless of which departments the cases are assigned to. As shown in figures A and B below, you can create a group named Commanders, add the group to each department within your organization, and then give the group the *Manage* permission level in each department.

Figure A. Create the group



Groups > New group

Name *

Day to day operations \ Commanders

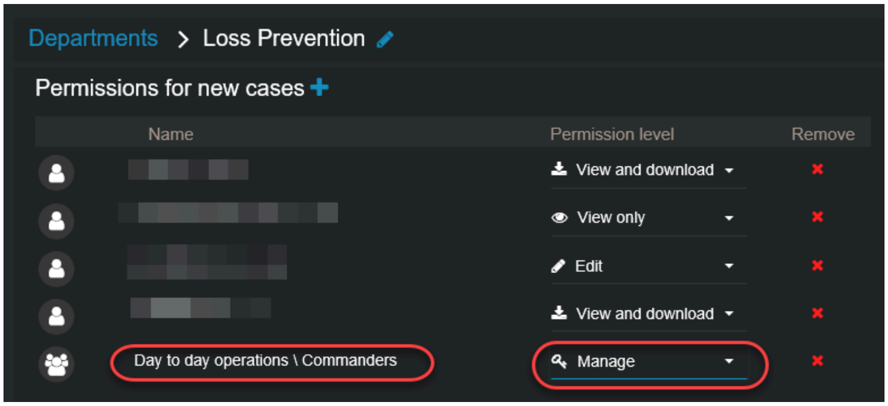
No member

Name	Email	Status

Privileges

- Security policies
- Video request policies

Figure B. Add group to department and assign access policies for new cases



Departments > Loss Prevention

Permissions for new cases

Name	Permission level	Remove
[redacted]	View and download	✖
[redacted]	View only	✖
[redacted]	Edit	✖
[redacted]	View and download	✖
Day to day operations \ Commanders	Manage	✖

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

Create user accounts to add new users to the group, or add existing users to the group.

Related Topics

Defining video request policies on page 59

Creating user accounts

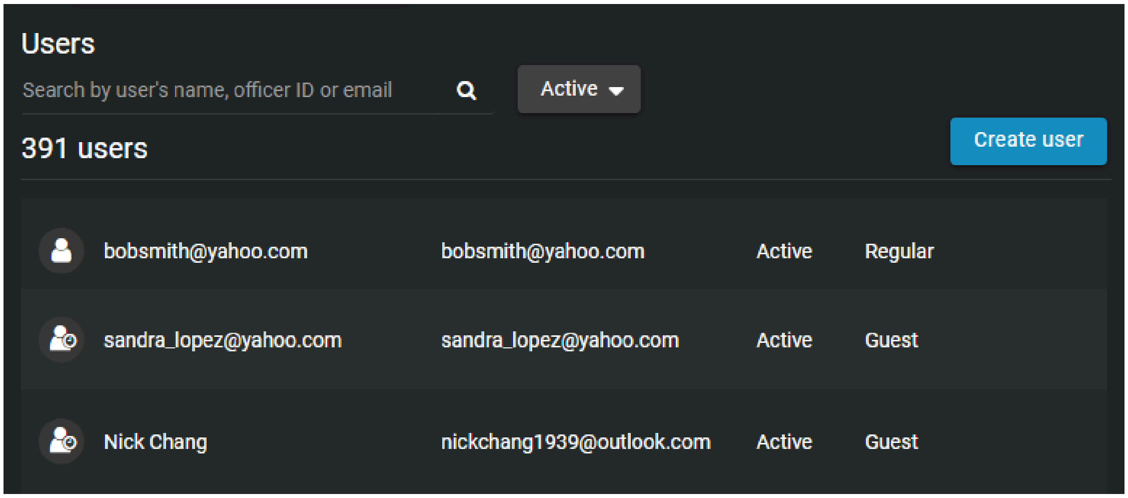
Before someone can use Genetec Clearance™, you must create a user account for that person. After you have created the user's account, they can be granted access to cases and files.

What you should know

You must be an account administrator to create users in Clearance.

Procedure

1 Click **Configurations** > **Users** > **(** + **)** .



bobsmith@yahoo.com	bobsmith@yahoo.com	Active	Regular
sandra_lopez@yahoo.com	sandra_lopez@yahoo.com	Active	Guest
Nick Chang	nickchang1939@outlook.com	Active	Guest

2 Enter values for the following settings:

- **Username:** The user’s email address. This field is mandatory.
- **First name:** The user's first name. To ensure that the user is searchable in the system, enter the user's actual name, not a nickname.
- **Last name:** The user's last name. To ensure that the user is searchable in the system, enter the user's actual name, not a nickname.
- **Groups:** The group that the user is assigned to. You can create groups for specific departments, groups that apply to multiple or all departments, or groups that reside outside departments. Users can belong to multiple groups.
- **Officer ID:** The user’s identification number. You can search for users by their officer IDs.

  NOTE: You can modify or reassign an officer ID from the **Officer ID** field on the *User edit* page.
- **Mobile phone:** The user’s phone number. You can add a maximum of two phone numbers. You cannot search for users by their phone number.
- **Work phone:** The user's work phone number.
- **Status:** A user can either be Active (by default) or Inactive. If a user is no longer working for your organization, you can set the status of the user to Inactive. Inactive users are still searchable.
- **Type:** A user can either be a guest or regular user. Guests cannot perform searches in the system and cannot access the **Configurations** menu. Regular users have full access, but can only access the **Configurations** menu if they are part of the Account Administrator group.
- **Picture:** Upload a photo of the user so that they can easily be identified.
- **Devices:** The devices that are associated with the user. For example, a *body-worn camera*.
- **Privileges:** Assign security and video request policies.

3 Click **Save**.

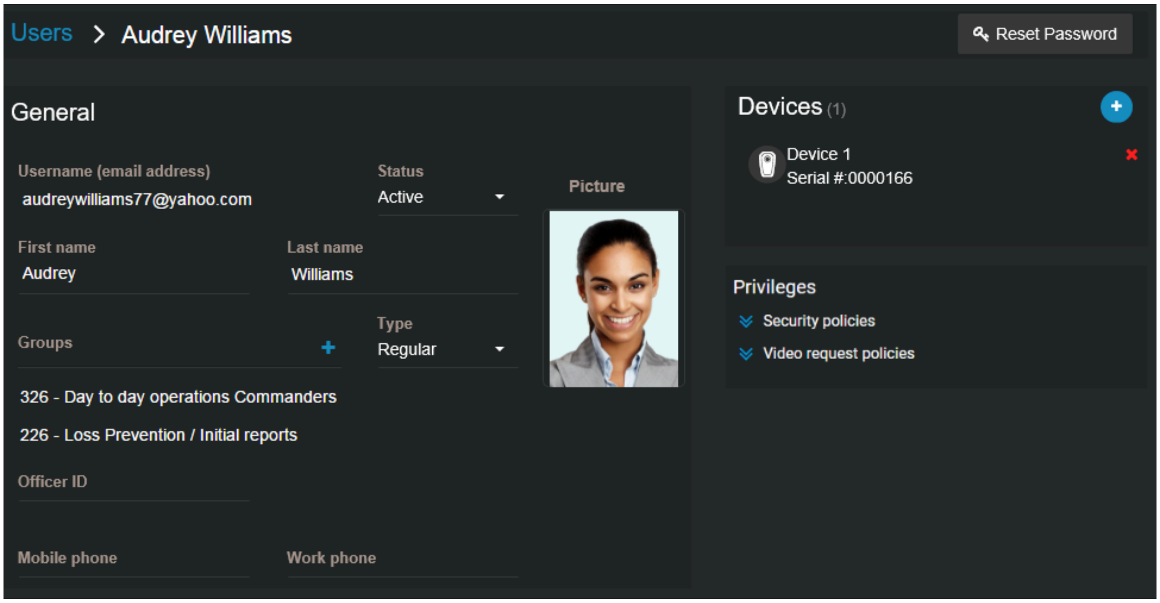
The user account is created. An email inviting the user to join Clearance is automatically sent to the user.

TIP: Click **Save and add new** to create additional user accounts.

Example

The image below shows an example of a user (Audrey Williams) who is a member of two groups: *Day to day operations Commanders* and *Loss Prevention Initial reports*. Because Audrey is a member of these two groups, she will automatically be assigned to new cases that are assigned to departments that these two groups are members of.

For example, if a new case is assigned to the Loss Prevention Department, and Audrey is a member of the Initial Reports group within this department, Audrey will receive an email, notifying her that she has been assigned to a new case.



Username (email address)
audreywilliams77@yahoo.com

Status
Active

First name
Audrey

Last name
Williams

Groups
326 - Day to day operations Commanders
226 - Loss Prevention / Initial reports

Type
Regular

Officer ID

Mobile phone

Work phone

Device 1
Serial #:0000166

Security policies
Video request policies

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

▶

Related Topics

Defining video request policies on page 59

Synchronizing users and groups using SCIM protocol

Use the SCIM integration to synchronize users and groups from your identity management system so that you do not have to create them.

What you should know

This procedure is intended for IT personnel responsible for their organization's identity administration.

Procedure

1 Learn about the Genetec Clearance™ SCIM integration

2 Synchronize users and groups using SCIM

3 Refer to the SCIM and Clearance attribute mapping information

Related Topics

About SCIM synchronization using an API on page 50

Provisioning users and user groups using SCIM on page 51

SCIM and Clearance attributes mapping on page 52

About SCIM synchronization using an API

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.

The SCIM integration is intended to save Clearance users time in the user and group creation process.

The following information describes Azure Active Directory SCIM synchronization:

- Synchronization of SCIM attributes into Clearance identity attributes is INBOUND only.

  CAUTION: Any changes only made to identities in Clearance can be overwritten by the next synchronization from the Active Directory.
- Synchronization occurs automatically at the intervals specified in the Build a SCIM endpoint and configure user provisioning with Azure AD documentation.
- The first time a synchronization occurs, all Active Directory user attributes are synchronized.
- The next time a synchronization occurs, only Active Directory user attributes that have changed since the last time the agent ran are synchronized.
- Once connected, Azure AD runs a synchronization process every 40 minutes in which it queries the application's SCIM endpoint for assigned users and groups, and creates or modifies them according to assignment details.
- **CAUTION:** If you try to provision a user whose email address is already used in Clearance, the provisioning will fail for that user.
- **IMPORTANT:** Please note that nested groups are not supported in Clearance. If you provision a group that has another group nested in it, they will be created as separate groups in Clearance.
- Group provisioning requires Azure AD Premium P1 or P2

Related Topics

Synchronizing users and groups using SCIM protocol on page 50
Provisioning users and user groups using SCIM on page 51
SCIM and Clearance attributes mapping on page 52

Provisioning users and user groups using SCIM

You can import your existing list of users and groups from Azure Active Directory into Clearance using the SCIM integration.

Before you begin

Design your user and group schema in Azure Active Directory.

On you organization's Azure Active Directory *Overview* page, copy the Tenant ID of your Active Directory Instance and provide it to your Clearance deployment contact. After you have done this, your Clearance contact will provide you with a *Tenant URL* that is used during the provisioning steps.

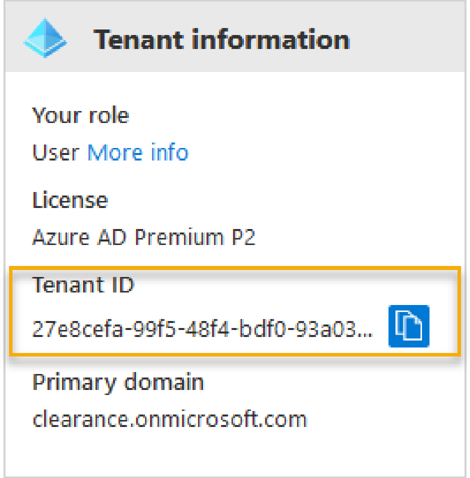
What you should know

This procedure is for IT or security personnel responsible for Azure Active Directory (AD) administration.

NOTE: Group provisioning requires Azure AD Premium P1 or P2

Procedure

1 On you organization's Azure Active Directory *Overview* page, copy the Tenant ID of your Active Directory Instance and provide it to your Clearance deployment contact.



Tenant information

Your role
User More info

License
Azure AD Premium P2

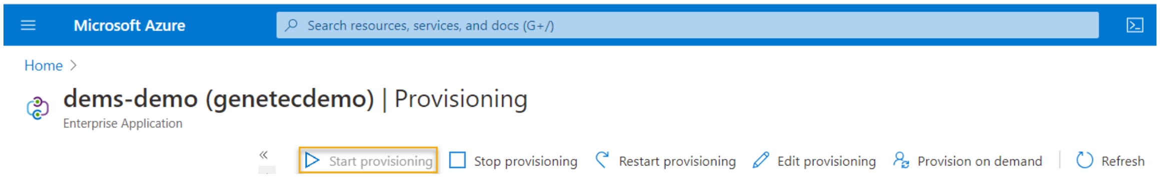
Tenant ID
27e8cefa-99f5-48f4-bdf0-93a03...

Primary domain
clearance.onmicrosoft.com

NOTE: After you have done this, your Clearance deployment contact will provide you with a *Tenant URL* that is used during the provisioning steps.

2 Integrate your SCIM endpoint with the Azure AD SCIM client.

3 Click **Start provisioning**.



The users are synchronized into Clearance.

Related Topics

Synchronizing users and groups using SCIM protocol on page 50
About SCIM synchronization using an API on page 50
SCIM and Clearance attributes mapping on page 52
SCIM and Clearance attributes mapping on page 52

SCIM and Clearance attributes mapping

When you synchronize an Active Directory (AD) with Clearance using the SCIM integration, SCIM attributes are mapped to Clearance identity attributes.

SCIM user attributes	Clearance user attributes
User name	Username (email address)
active	Status
name.givenName	First name
name.familyName	Last name
Any groups the user is included in	Groups
phoneNumbers[type eq “mobile”].value	Mobile phone
phoneNumbers[type eq “work”].value	Work phone

SCIM group attributes	Clearance identity attributes
displayName	Group name
members	Members

Related Topics

Synchronizing users and groups using SCIM protocol on page 50
Provisioning users and user groups using SCIM on page 51
About SCIM synchronization using an API on page 50
Provisioning users and user groups using SCIM on page 51

Adding existing users to groups

To organize users by rank or role and to ensure that their access policies for cases, or security policies are always the same, you can add users to groups.

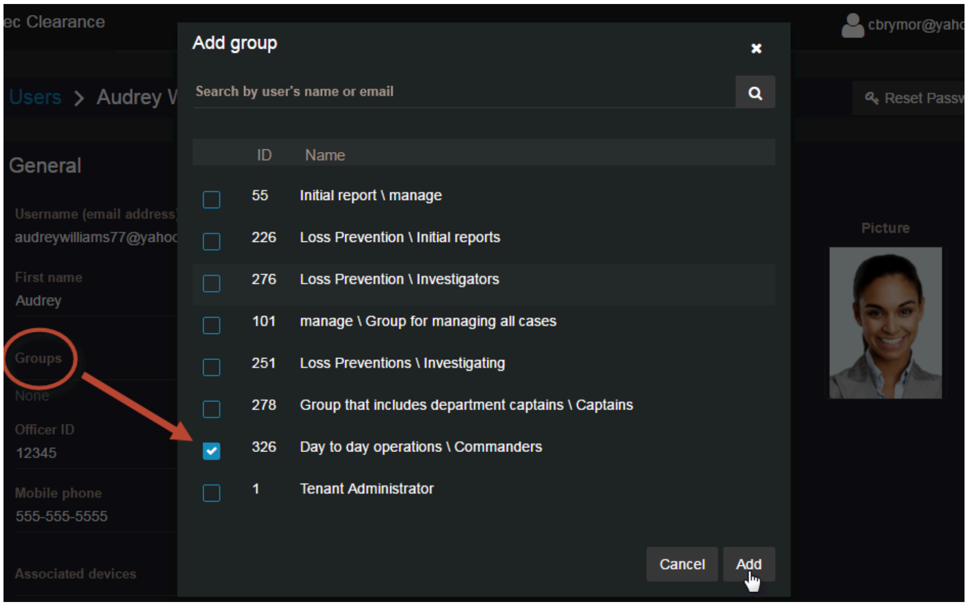
What you should know

Users can belong to multiple groups.

To add new users to a group, create the user account.

Procedure

1. Click **Configurations** > **Users**.
2. Scroll through the list or search for an existing user and double-click the name.
   The user's edit page opens.
3. In the **Groups** field, click ⊕.
4. Select the group you want the user to be a member of, and then click **Add**.



Username (email address): audreywilliams77@yahoc
First name: Audrey
Groups: None
Officer ID: 12345
Mobile phone: 555-555-5555
Associated devices

	ID	Name
☐	55	Initial report \ manage
☐	226	Loss Prevention \ Initial reports
☐	276	Loss Prevention \ Investigators
☐	101	manage \ Group for managing all cases
☐	251	Loss Preventions \ Investigating
☐	278	Group that includes department captains \ Captains
☑	326	Day to day operations \ Commanders
☐	1	Tenant Administrator

5. Click **Save**.

Example

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

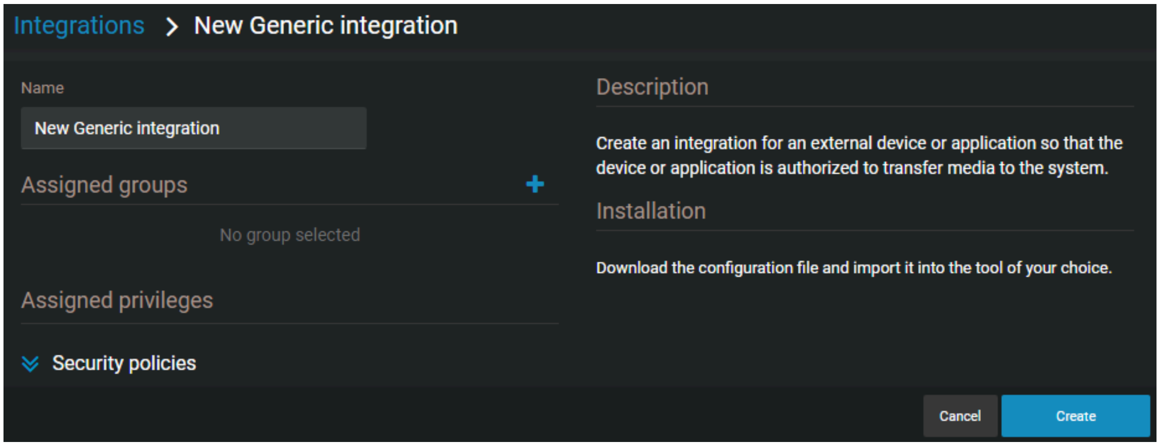
Creating integrations

Before you can configure an external system, such as an application, device, plugin, or API for use with Clearance, you must create an integration. The integration authenticates your external system's communication with the Clearance account so that data can be exchanged and transferred to the Clearance account.

Procedure

1 Click **Configurations** > **Integrations**.

2 Select the integration that you want to create.



Integrations > New Generic integration

Name: New Generic integration

Assigned groups

No group selected

Assigned privileges

Security policies

Description

Create an integration for an external device or application so that the device or application is authorized to transfer media to the system.

Installation

Download the configuration file and import it into the tool of your choice.

3 Enter a name for the integration.

4 (Optional) To add any groups that you require, click **Add** (+).

  a) Select the users and groups that you want to add to the integration.

  b) Click **Add**.

5 Click **Create**.

6 (Optional) Assign security policies as needed.

7 Click **Download configuration** to save a copy of the *{IntegrationName}.json* integration configuration file.

8 Add the configuration file in the **Properties** tab of the Clearance plugin in Config Tool. For more information, refer to *Configuring the Clearance plugin role*.

The external system has been authenticated and can communicate with, or transfer data or media to, your Clearance account.

Related Topics

Installing the Clearance Uploader on page 266
Configuring the Clearance Uploader on page 268
About Clearance Plugin for Security Center on page 250

Creating departments

Departments act as user access templates that allow the initial permissions for users and groups to be automatically applied to cases.

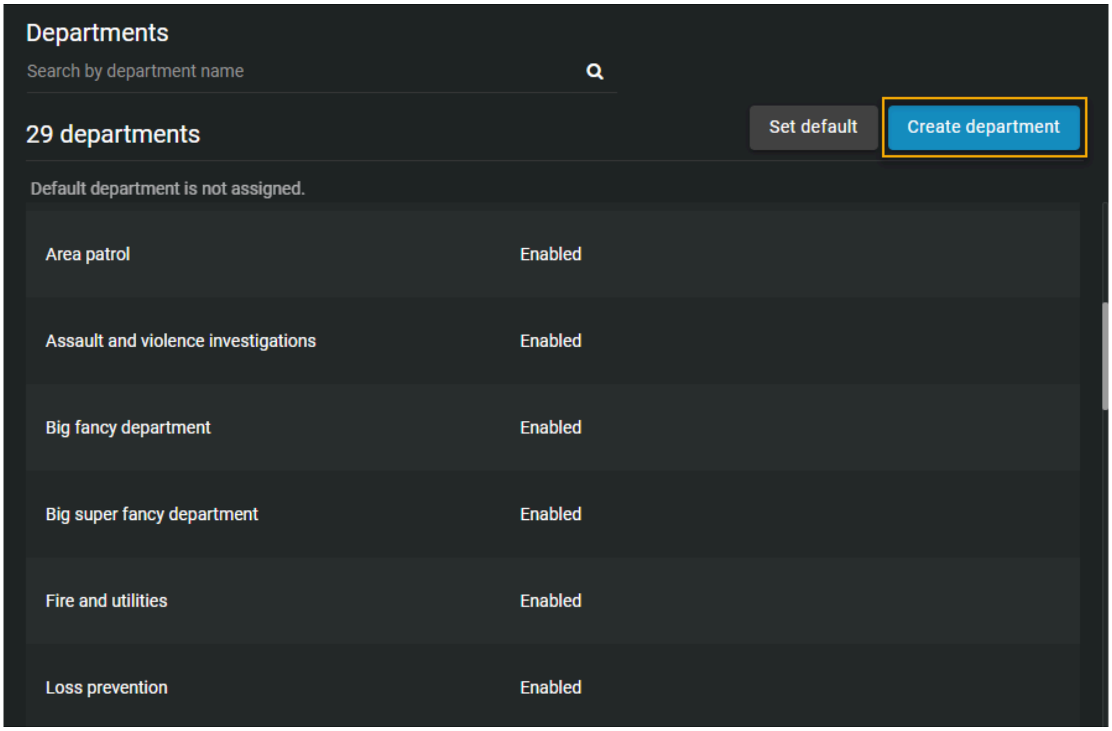
What you should know

Use departments to automatically define the access policy that users and groups within the department have to new cases only, not existing cases. If you add a new user or group to a department which is already assigned to existing cases, you must manually add the new user or group to each of these cases individually.

Example: Let us assume that the Loss Prevention Department is assigned to existing cases, Case A and Case B. A new user, Audrey Williams, enters the Loss Prevention Department, so you add her to the department. When you create Case C and assign the Loss Prevention Department to this case, Audrey automatically has access to the case; however, if you want Audrey to have access to Cases A and B, you must open each of these cases and add her as a user.

Procedure

1 Click **Configurations** > **Departments** > ⊕ .



Departments

Search by department name

29 departments

Default department is not assigned.

Area patrol	Enabled
Assault and violence investigations	Enabled
Big fancy department	Enabled
Big super fancy department	Enabled
Fire and utilities	Enabled
Loss prevention	Enabled

2 Click ✎ and enter a name for the department.

Example: If you have a department within your organization that handles thefts, you can call this department Loss Prevention.

3 In the **Permissions for new cases** field, click ⊕ and then select one of the following:

- **Add existing groups or users:** Add users or groups whose accounts have been created and are current users of the system. If you are setting up your site and there are no current users or groups, you can save the department, create the user accounts or groups, and then add them to the department.
- **Create a group:** Create a group that does not currently exist in the system. When you create a group, add the group's purpose or responsibility in the **Role** field. For example, in the Loss Prevention

Department, you can create a group of users that handles the initial reporting phase of a case, and a group that manages the investigation phase.

4 For each of the users or groups that you have added, use the **Permission level** field to define their respective permission level. You can choose one of the following levels:

- **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.

NOTE: If delete or restore security policies are not active, any users with *manage* permission can delete or restore cases or files. If delete or restore security policies are active, only users with delete or restore permission can delete or restore cases or files if they have *manage* permission.

5 Click **Save**.

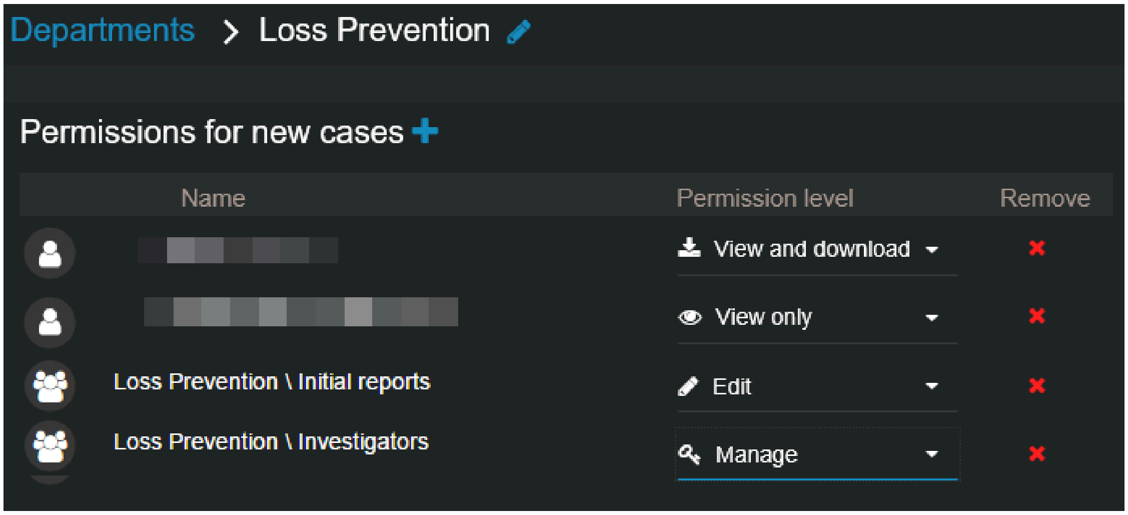
NOTE: At least one user or group must have *manage* permissions in a department. This ensures that cases are always accessible with full permissions by someone from the organization.

6 (Optional) Click **Disable** to disable the department. Disabled departments are hidden from the department selection drop-down menu in the Case page. Existing cases that have the department assigned maintain it unless it is changed manually by a user with sufficient privileges.

Your department is created. For new cases assigned to this department, the users within this department will receive emails, notifying them that they have been assigned to a case.

Example

The following image shows an example of a department that consists of one user and two groups, each of which have been given different permission levels.



Departments > Loss Prevention

Permissions for new cases +

Name	Permission level	Remove
[redacted]	View and download	✖
[redacted]	View only	✖
Loss Prevention \ Initial reports	Edit	✖
Loss Prevention \ Investigators	Manage	✖

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

Setting a default department

To automatically assign a department to all new cases, administrators can configure a default department.

Before you begin

Create departments.

What you should know

When a new case is created, a default department can be assigned to it. You can change the default department at any time.

Procedure

1. From the **Configurations** menu, navigate to the **Departments** page.
2. Click **Set default.**
3. In the **Set or update default department** window, click the **Change to** menu and select a department from the list.
4. Click **Save**.

After you finish

Set up and use i-PRO automatic case and file tagging.

Creating incident categories

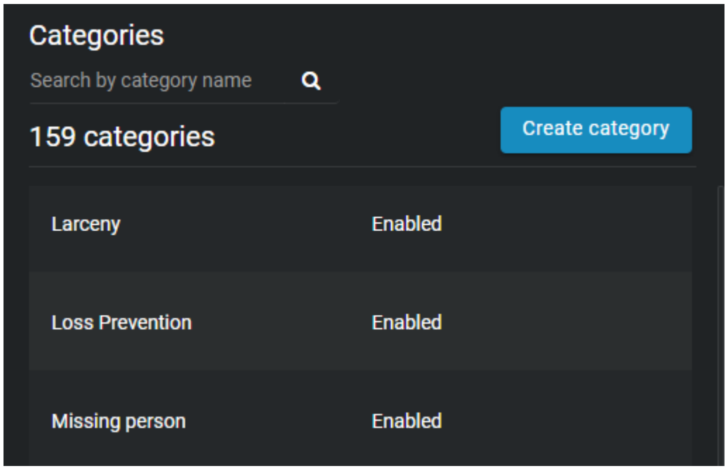
To properly classify incidents when creating cases, you can create categories for the different types of incidents.

What you should know

Categories are used to classify incidents, not to increase the searchability of cases. To increase the chances that a case is found during a search, enter an accurate description and add applicable keyword tags to the case. For example, you can classify shoplifting cases with the **Shoplifting** category, and then from the Case page, you can add tags such as **Arson**, **Loss prevention**, **Offense in progress**, and **Parking enforcement**.

Procedure

1 Click **Configurations** > **Categories** > ⊕ .



Categories

Search by category name

159 categories

Larceny	Enabled
Loss Prevention	Enabled
Missing person	Enabled

2 Click ✎ and enter a name for the category.

3 Select a category retention period in **days** or **years** and enter a value, or select the **Never delete** check box to keep your files indefinitely.

4 Click **Save**.

The **Status** drop-down menu becomes available and your new category is enabled by default. You can now classify new and existing incidents with this category.

NOTE: Categories cannot be deleted. If you no longer want to use a category, you can set its status to Disabled.

Example

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

▶

Defining video request policies

In Clearance, users and guest users can submit requests for video. To manage access to these video requests, system administrators can define video request policies and add existing users or groups to them.

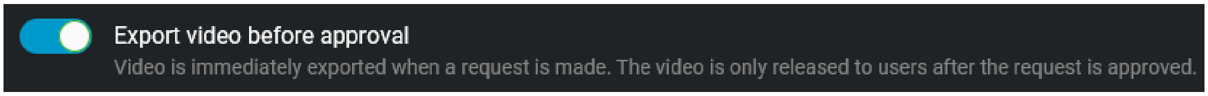
What you should know

You can manage video request policies by user or by groups.

Procedure

1 Click **Configurations** > **Video request policies**.

2 Move the **Export video before approval** slider to the enabled position to export video as soon as a video request is received.



Export video before approval

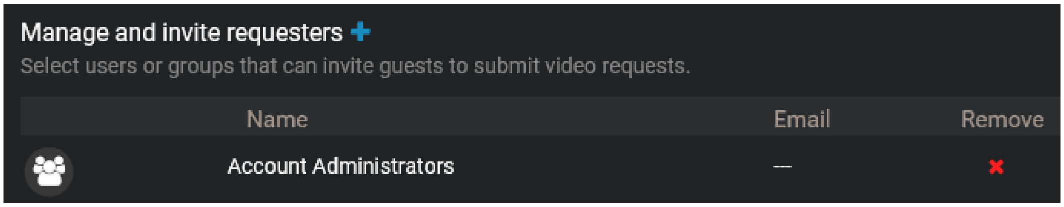
Video is immediately exported when a request is made. The video is only released to users after the request is approved.

When a request is received, the requested video is immediately encrypted by Clearance and exported to a temporary location to prevent the Archiver retention policy from deleting the requested video.

- If the video request is approved, the requested video is transferred to a case in Clearance with all associated camera metadata.
- If the video request is rejected, the video is deleted from the temporary location and is never sent to the requester.

NOTE: If the **Export video before approval** option is disabled, video is not exported until the video request is approved.

3 In the *Manage and invite requesters* section, select users or groups that can invite guests to submit video requests.



Manage and invite requesters +

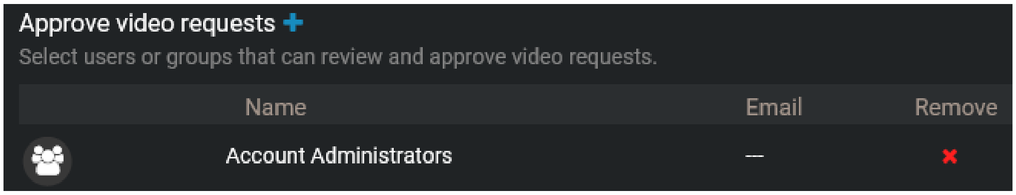
Select users or groups that can invite guests to submit video requests.

	Name	Email	Remove
	Account Administrators	—	✖

a) Click +.

b) Click **Add existing groups or users** or **Create a group** and follow the on-screen prompts.

4 In the *Approve video requests* section, select users or groups that can review and approve video requests.



Approve video requests +

Select users or groups that can review and approve video requests.

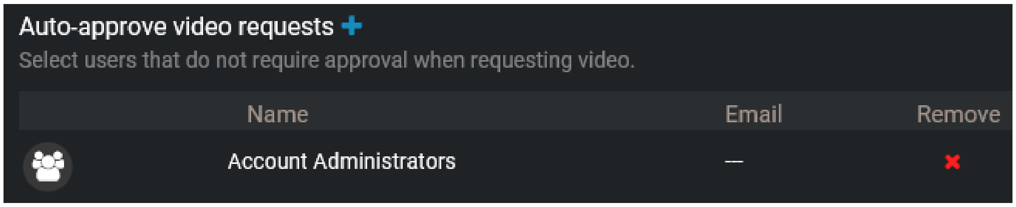
	Name	Email	Remove
	Account Administrators	—	✖

Users specified here are able to review all information in a video request, including the requester, incident date, associated case, associated cameras, and the filled-out video request form. After the request details have been reviewed, the request can be approved or denied.

a) Click +.

b) Click **Add existing groups or users** or **Create a group** and follow the on-screen prompts.

5 In the *Auto-approve video requests* section, select users whose video requests can be automatically approved.



Auto-approve video requests +

Select users that do not require approval when requesting video.

	Name	Email	Remove
	Account Administrators	—	✖

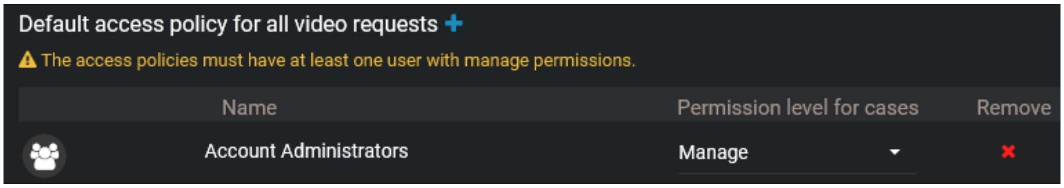
When requests are submitted by these users, the upload into Clearance is immediately started.

a) Click +.

b) Click **Add existing groups or users**, **Add all regular users**, or **Create a group** and follow the on-screen prompts.

If you choose **Add all regular users**, all non-guest users are added to the auto-approve list. Guest users must be added separately.

6 In the *Default access policy for all video requests* section, configure the access policy settings for the requested files.



Default access policy for all video requests +

⚠ The access policies must have at least one user with manage permissions.

	Name	Permission level for cases	Remove
	Account Administrators	Manage ▾	✖

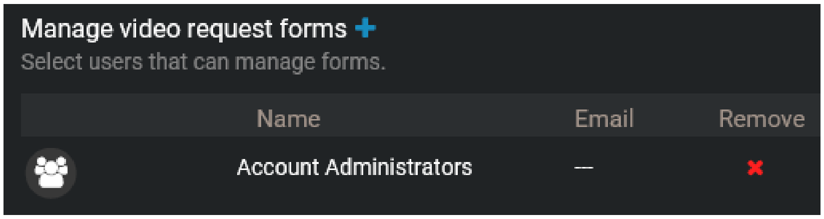
Every approved video request not associated with a pre-existing case inherits this access policy by default. The access policy for requests linked to pre-existing cases does not change.

IMPORTANT: This access policy must have at least one user with *Manage* permissions.

a) Click +.

b) Click **Add existing groups or users** or **Create a group** and follow the on-screen prompts.

7 In the *Manage video request forms* section, select users that can manage forms.



Manage video request forms +

Select users that can manage forms.

	Name	Email	Remove
	Account Administrators	—	✖

Users added to this section can create, modify, delete, and activate forms for submitting video requests.

a) Click +.

b) Click **Add existing groups or users** or **Create a group** and follow the on-screen prompts.

8 Click **Save**.

Your video request policies are now configured and ready for use.

Related Topics

Creating user accounts on page 48

Permission levels on page 43

Creating user groups on page 46

Video request policy definitions list on page 61

Video request policy definitions list

In Clearance, system administrators can define video request policies to control access to video request features for users and groups. A user's level of access associated with these policies can vary depending on case and file permissions.

Video request policy	Definition	Details
Submit video requests	Grants a user or guest the ability to submit video requests. You can configure an expiration date after which the user or guest is removed from this policy.	This video request policy can be granted to any user or guest in Clearance.
Manage and invite requesters	Before guests can submit video requests, they must be invited by a user. This policy defines which users and groups can invite guests to submit video requests.	This policy is not available to guests.
Approve video requests	Before a video request can be completed, it must be reviewed and approved by a user included in the approve video requests policy. This policy defines which users and groups can review and approve video requests.	This policy is not available to guests.
Auto-approve video requests	You can allow users who you trust to have their video requests approved automatically. This policy defines which users and groups do not require approval when requesting video.	This policy can be granted to any user or guest in Clearance.
Manage forms	You can create custom forms that must be completed when new requests are made or when new participants are enrolled in your registry program. This policy defines which users and groups can create and modify forms.	This policy is not available to guests.
Delete participants	Define which users can delete participants from your registry program whose information is no longer current.	This policy is not available to guests.
View participants in the registry	Participants are only visible to users included in this video request policy.	This policy is not available to guests.

Video request policy	Definition	Details
Default access policy for all video requests	A case is automatically generated after a video request has been approved. This policy defines a default list of user and group permissions for cases created from approved requests.	Assign a default permission level (View only, View and download, Edit, or Manage) to each user and group in this policy.
View camera registry	Define which users are able to view and select cameras as part of their video requests.	Use this video request policy to control access to camera information, while still permitting users to make video requests involving cameras they have access to.

Related Topics

Permission levels on page 43

Defining video request policies on page 59

Defining security policies

In Clearance, system administrators can define security policies to control access for users and groups.

What you should know

You can manage security policies by user or by groups.

Procedure

1. Click **Configurations** > **Security policies**.
2. In your security policies section of choice, click ➕ > **Add existing groups or users** .
3. Select which users or groups you want to grant access to, and click **Add**.
   To remove a user or group, click ❌ next to their name.
4. If applicable, grant users and user groups appropriate permission levels:
   - **View only**
   - **View and download**
   - **Edit**
   - **Manage**
5. Click **Save**.
   NOTE: You can also assign these security policies when you create or edit users and groups.

Example

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

▶

Related Topics

Permission levels on page 43
Security policy definitions list on page 63
Transferring cases on page 106

Security policy definitions list

In Clearance, system administrators can define security policies to control access for users and groups. A user's level of access associated with these policies can vary depending on case and file permissions.

Security policy	Definition	Details
Access files not associated with any cases	Defines a user or group’s default permission level for files that are not associated with any case.	Assign a default permission level (*View only, View and download, Edit,* or *Manage*) to each user and group in this policy.

Security policy	Definition	Details
Access audit trail and create eDiscovery receipt	Defines which users and groups can access the activity history of a file or case and create a digital proof of receipt for evidence being shared.	Users can only access the audit trail of and create eDiscovery receipts for files and cases for which they have *Manage* permissions.
Create cases	Defines which users and groups can create cases.	Guest users can be assigned this security policy.
Delete cases and files	Defines which users and groups can delete cases and files.	Users can only delete files and cases on which they have *Manage* permissions.
Restore cases and files from the recycle bin	Defines which users and groups can restore cases and files from the recycle bin.	Users can restore all deleted cases and files from the recycle bin.
Protect or unprotect cases and files from deletion	Defines which users and groups can protect or unprotect cases and files from being deleted.	Users can only protect or unprotect files and cases on which they have *Manage* permissions.
Hide visual watermark	Defines which users and groups can toggle the visual watermarks on videos and images on and off.	A user can hide the watermark on files they have permission to view.
View dashboard	Defines which users can access the dashboard.	This feature is not available to guest users.
Manage devices	Defines which users and groups can add or remove devices and activate or deactivate device licenses.	A device that has been deactivated can be reactivated by users in this security policy.
Add organizations approved for case transfers	Defines which external organizations have been approved to receive case transfers.	The user specified by the sender is automatically granted Manage permissions for any cases transferred.
Share cases	Defines which users and groups can share cases they have access to without having the **Manage** permission.	Users who are included in this security policy can share any case they have permission to view. This feature is not available to guest users.

Security policy	Definition	Details
Access files uploaded from devices	Defines the level of access officers have to files uploaded from devices assigned to them.	Choose to give officers no access, view only, view and download, edit, or manage-level access to recordings from their devices.
Download malicious files	Defines which users can download suspicious files that might contain malware.	Users who have at least *View and Download* on a file are able to download files flagged by the malware scan. **NOTE:** The malware scan supports files that are up to 4GB in size.

Example

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

▶

Related Topics

Permission levels on page 43
Defining security policies on page 63
Transferring cases on page 106

Creating fields

You can tailor the information documented in cases and on files to the needs of your organization using the custom fields feature. Default fields can be renamed and it is possible to create text or drop-down fields. Each custom field is filterable from the Search page.

What you should know

- Only users included in the account administrators group can create or modify fields.

Procedure

To create fields:

1 Click **Configurations** > **Fields and labels**.

2 Choose to create a field template for cases, video requests, or files.

To modify a default field:

1 In the **Default Fields** section, select the field you want to modify and enter a new name for it.

2 To restore a default field, click **Restore default** (↶).

3 Click **Save**.
The default field has been modified.

To create a field:

1 In the **Custom Fields** section, click **Add** (✚) to add a new field.

2 Enter a name for the field.

3 Choose to create a Text or Drop-down field.

a) If you chose to create a Drop-down field, click **Add** (✚) and add values for your drop-down field to show.

4 To re-position your fields, click and drag the **Reorder** control (⠿).

NOTE: The order you assign to your fields here determines the order in which they are shown in the case or file.

5 To delete a field, click **More**, (⋮) and then click **Delete**.

NOTE:

- A case or file can include up to 15 custom fields.
- A drop-down field can include up to 100 options.

6 Click **Create**.
Your field is created.

Related Topics

Creating cases on page 89

Configuring ID templates

You can configure ID templates to automatically assign identifying information to cases and requests in Clearance.

What you should know

- Only users included in the account administrators group can create or modify ID templates.

Procedure

1 Click **Configurations** > **Fields and labels**.

2 Choose to configure automatic IDs for cases or video requests.

3 Turn on the **Automatically generate ID** setting .

4 Configure keys for the ID template.

TIP: Hover over the **Tip** (ⓘ) icon to see a list of supported values you can add to your automatic ID template.

The supported keys and their respective values are as follows:

Key	Value
{D}	Short Day
{DD}	Long Day
{M}	Short Month
{MM}	Long Month
{YY}	Short Year
{YYYY}	Long Year
{###}	Fixed Length Numbers
{N}	Infinite Length Numbers
{FIRSTNAME}	Creator's First Name
{LASTNAME}	Creator's Last Name
{USERNAME}	Creator's Username

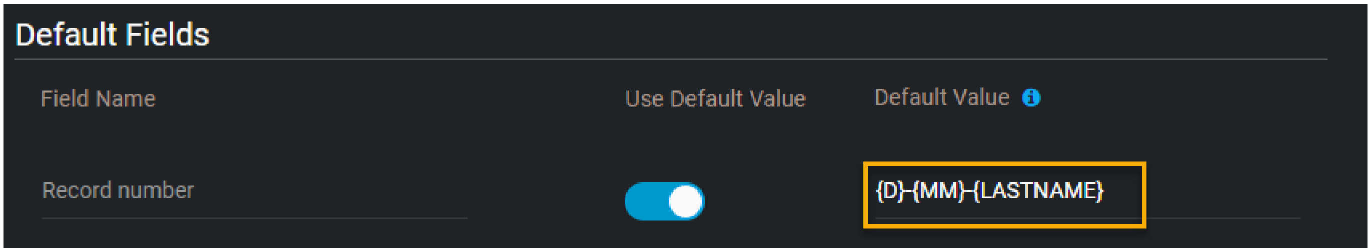
NOTE:

- You can also include fixed characters in the ID template by entering them in the ID template without any brackets, such as in the following example: CCN-1111-{YYYY}-{N}, which would yield the result: CCN-1111-2022-1.
- The {N} keyword is not displayed properly in the case and request views when the template it is included in is also assigned the {###} keyword.

5 Click **Save**.
Your ID template is created.

Example

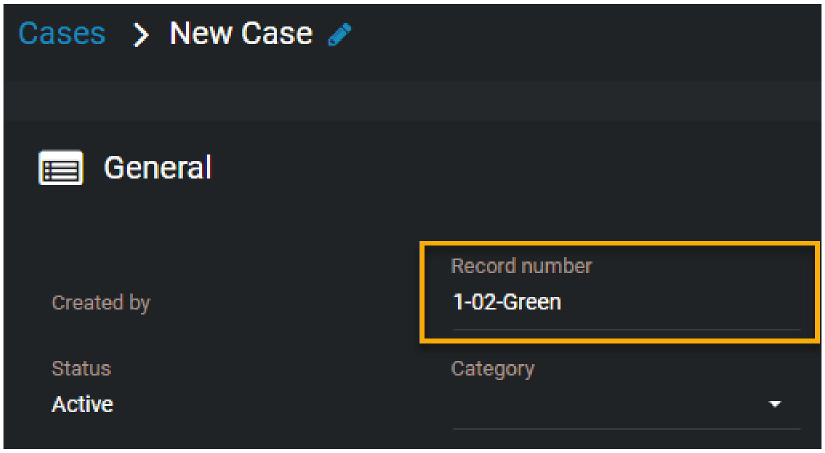
The field is configured:



Default Fields

Field Name	Use Default Value	Default Value
Record number	●	{D}-{MM}-{LASTNAME}

The field appears in new cases:



Created by

Record number
1-02-Green

Status
Active

Category

After you finish

Create a case, Request video.

Related Topics

Creating cases on page 89

Creating forms

System administrators can create and customize video request and participant enrollment forms in Clearance.

What you should know

- Users or groups in the *Manage forms* security policy can create or modify forms. System administrators is the default value for the policy.

Procedure

- Choose one of the following:
  - Create a video request form
  - Create a participant enrollment form

Creating video request forms

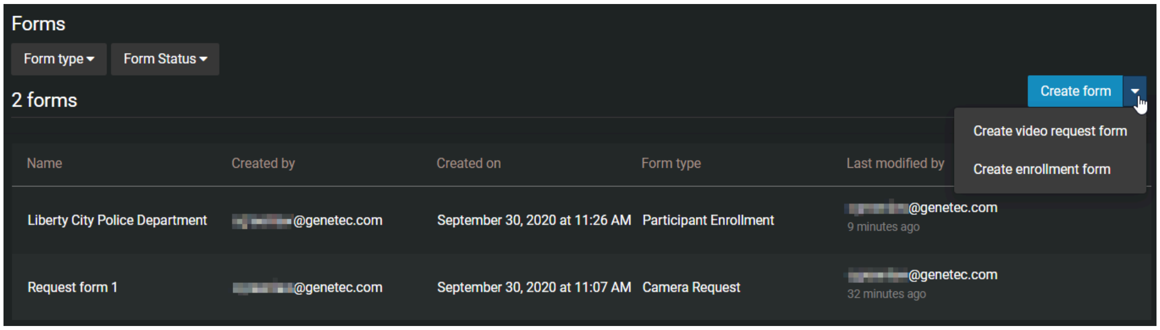
System administrators can create video request forms in Clearance to ensure compliance with corporate standards when managing video requests. These request forms can be customized and are used to gather additional information specific to your organization and the approval workflow.

What you should know

- Users or groups in the *Manage forms* security policy can create or modify video request forms. System administrators is the default value for the policy.
- Only one request form can be active at a time.

Procedure

1 Click **Configurations** > **Forms**.

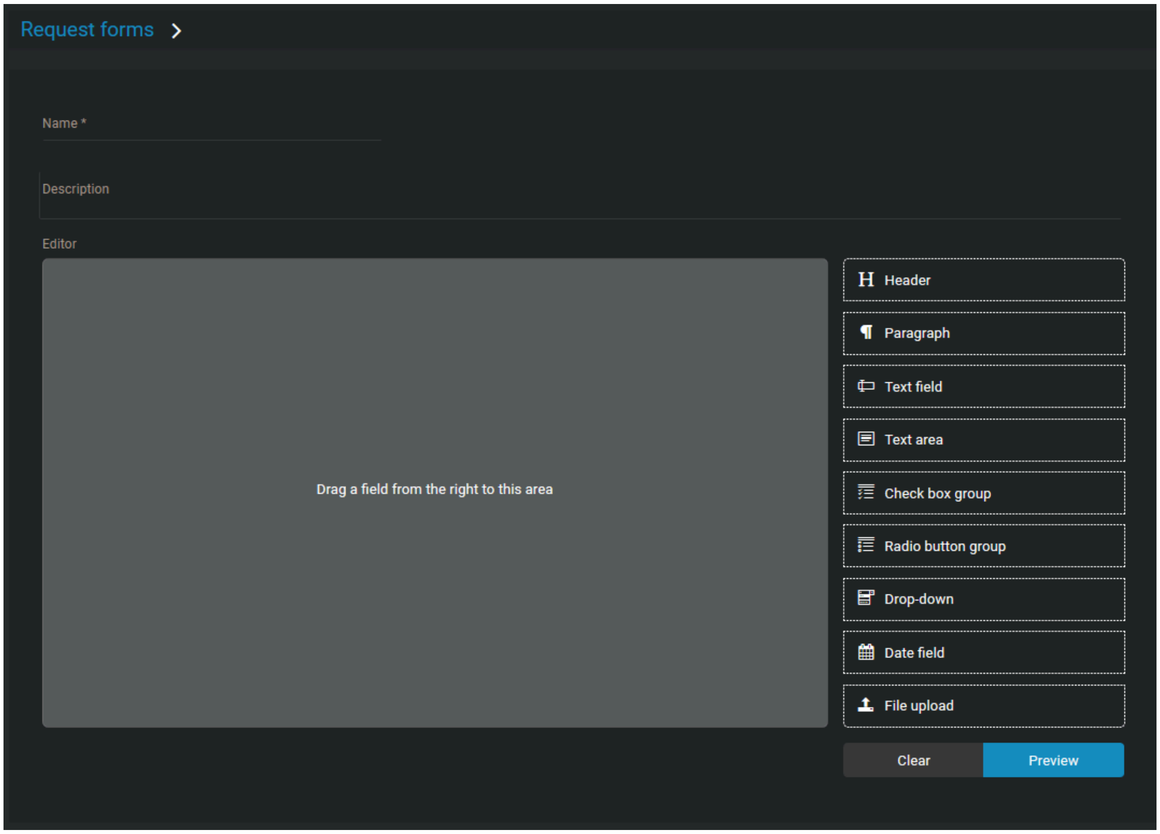


Forms

2 forms

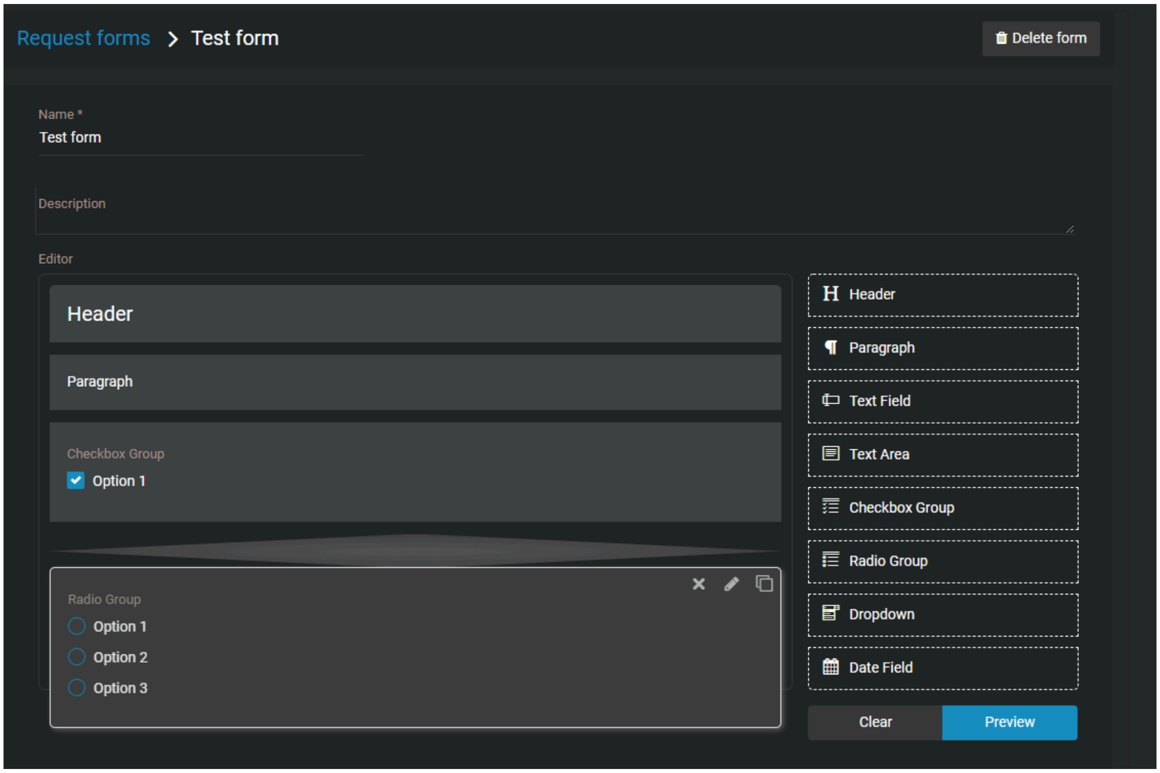
Name	Created by	Created on	Form type	Last modified by
Liberty City Police Department	[redacted]@genetec.com	September 30, 2020 at 11:26 AM	Participant Enrollment	[redacted]@genetec.com 9 minutes ago
Request form 1	[redacted]@genetec.com	September 30, 2020 at 11:07 AM	Camera Request	[redacted]@genetec.com 32 minutes ago

2 Click **Create video request form** (▾).



3 Enter a **Name** and **Description** for the request form.

4 Drag form elements from the list into the *Editor* pane and move to the required position in the form.



Name *
Test form

5 Click ✎ in each form element to modify the form contents and options.

a) (Optional) Configure **Header** options.

- **Header:**
  - **Label:** Enter the name or title of the form element.
  - **Type:** Select the subheading font size you require.
  - **Class:** Specifies advanced customization options. For more information, contact technical support.

b) (Optional) Configure **Paragraph** options.

- **Paragraph:**
  - **Content:** Enter the content that you require.
  - **Type:** Specifies the paragraph formatting required. Choose one of the following: paragraph, address, block quote, canvas, or output.
  - **Class:** Specifies advanced customization options. For more information, contact technical support.

c) (Optional) Configure **Text field** options.

- **Text field:**

    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Placeholder:** Enter hint information that is displayed in the field. For example, *Enter text here* or *Explain the incident*.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Value:** Used to specify a default value for this field in the form.
    - **Max Length:** Specifies the maximum number of numeric characters in the field. For example, you could specify 50 characters or you could set field length to match a use case like badge number length.

d) (Optional) Configure **Text area** options.

- **Text area:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Placeholder:** Enter hint information that is displayed in the field. For example, *Enter text here* or *Explain the incident*.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Value:** Used to specify a default value for this field in the form.
    - **Max Length:** Specifies the maximum number of numeric characters in the field. For example, you could specify 50 characters or you could set field length to match a use case like badge number length.

e) (Optional) Configure **Check box group** options.

- **Check box group:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Inline:** Select the check box to display multiple check box options in a line.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Options:** If you want to pre-fill the options, select one or more check boxes. Enter a name or title for each check box option.
    - **Add Option+:** Add additional option choice elements.

f) (Optional) Configure **Radio button group** options.

- **Radio button group:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Inline:** Select the check box to display multiple radio button options in a line.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Options:** If you want to pre-fill the options, select a radio button. Enter a name or title for each radio button option.
    - **Add Option+:** Add additional option choice elements.

g) (Optional) Configure **Drop-down** options.

- **Drop-down:**

    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Placeholder:** Enter hint information that is displayed in the field. For example, *Enter text here* or *Explain the incident*.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.

h) (Optional) Configure **Date field** options.

- **Date field:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Value:** Used to specify a default value for this field in the form.

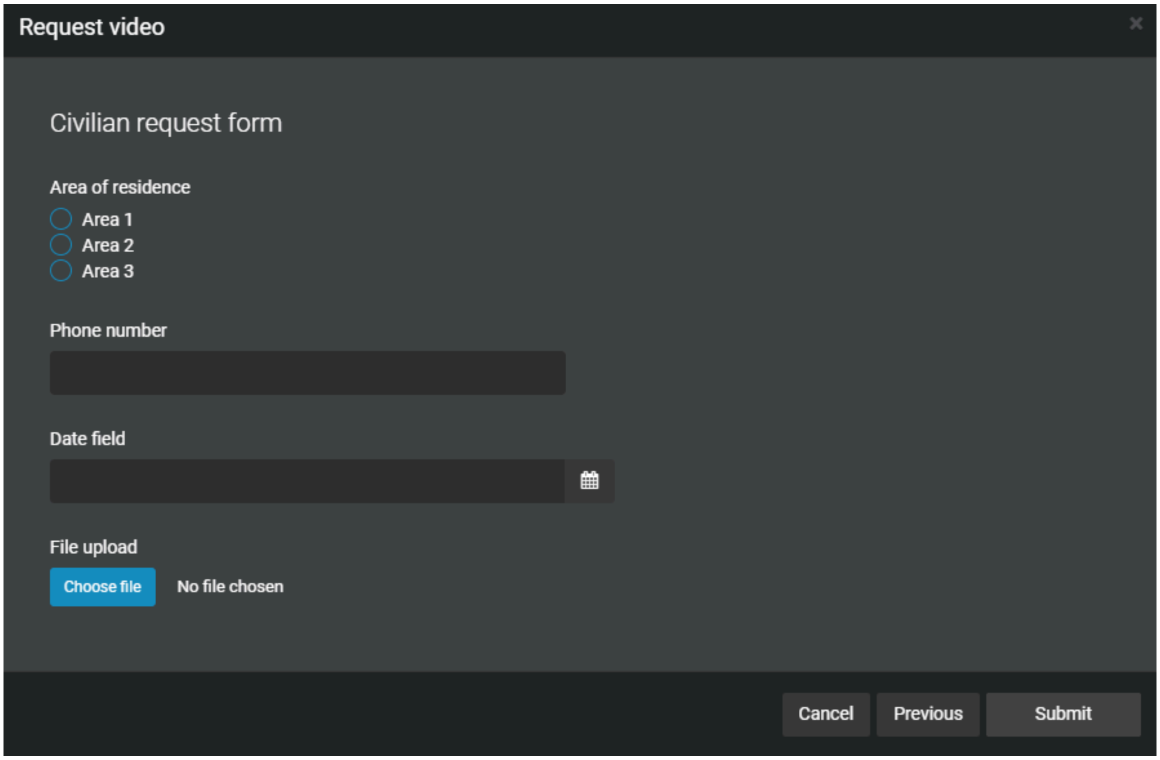
i) (Optional) Configure **File upload** options.

- **File upload:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.

6 (Optional) Click ⧉ to copy a form element.

7 (Optional) Click ✖ to remove a form element.

8 Click **Preview** to see a rendered version of your request form.



Request video

Civilian request form

Area of residence

○ Area 1
○ Area 2
○ Area 3

Phone number

Date field

File upload

Choose file No file chosen

Figure 1: Example video request form

9 Click **Save** to apply your changes.

10 Click **Publish** to publish your request form.

Forms are now available to facilitate video request submission.

After you finish

Invite guests to submit video requests.

Creating participant enrollment forms

System administrators can create participant enrollment forms in Clearance to register local businesses and residents as participants in public safety initiatives. These forms can be customized and are used to capture participant information and enroll them in the Clearance registry.

Before you begin

- Define your security policies.
- Define your video request policies.
- Refer to the security policy definitions list.
- Refer to the video request policy definitions list.

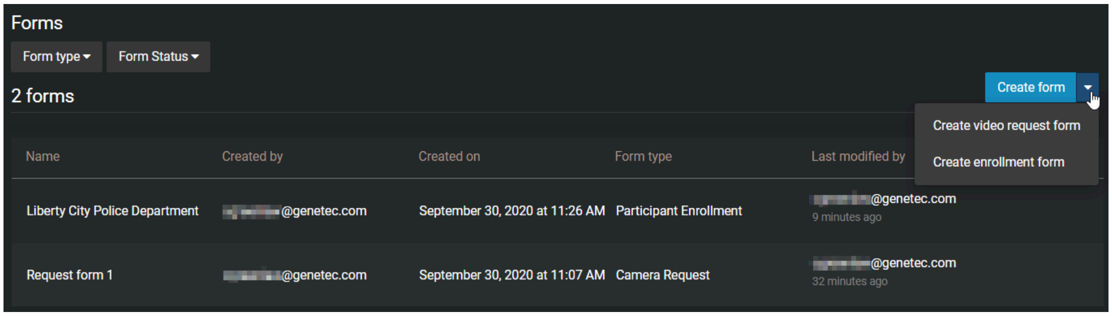
What you should know

- Users or groups in the *Manage forms* security policy can create or modify participant enrollment forms. System administrators is the default value for the policy.

Procedure

1 Click **Configurations** > **Forms**.

2 Click **Create enrollment form** ▾.

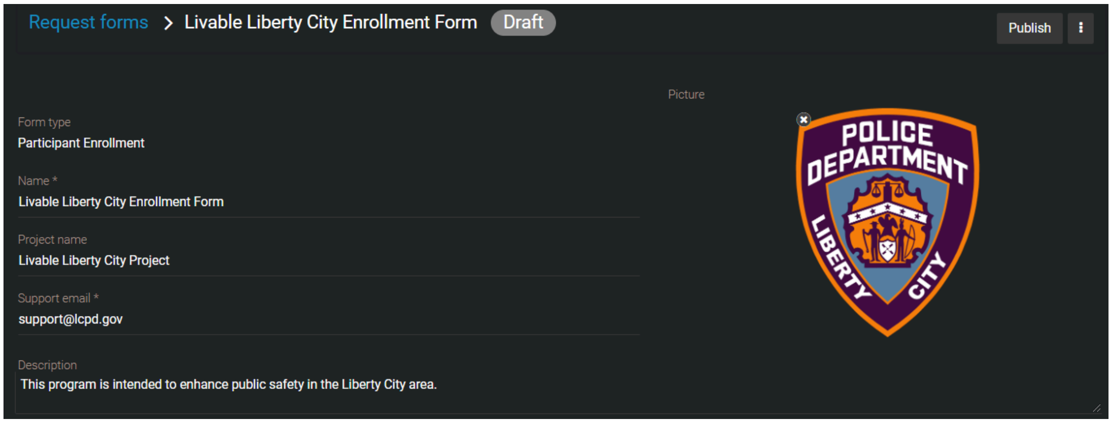


2 forms

Name	Created by	Created on	Form type	Last modified by
Liberty City Police Department	[redacted]@genetec.com	September 30, 2020 at 11:26 AM	Participant Enrollment	[redacted]@genetec.com 9 minutes ago
Request form 1	[redacted]@genetec.com	September 30, 2020 at 11:07 AM	Camera Request	[redacted]@genetec.com 32 minutes ago

3 Enter a **Name** and **Support email** for the enrollment form.

4 (Optional) Enter a **Project name**, **Description**, and **Picture** for the enrollment form.



Form type
Participant Enrollment

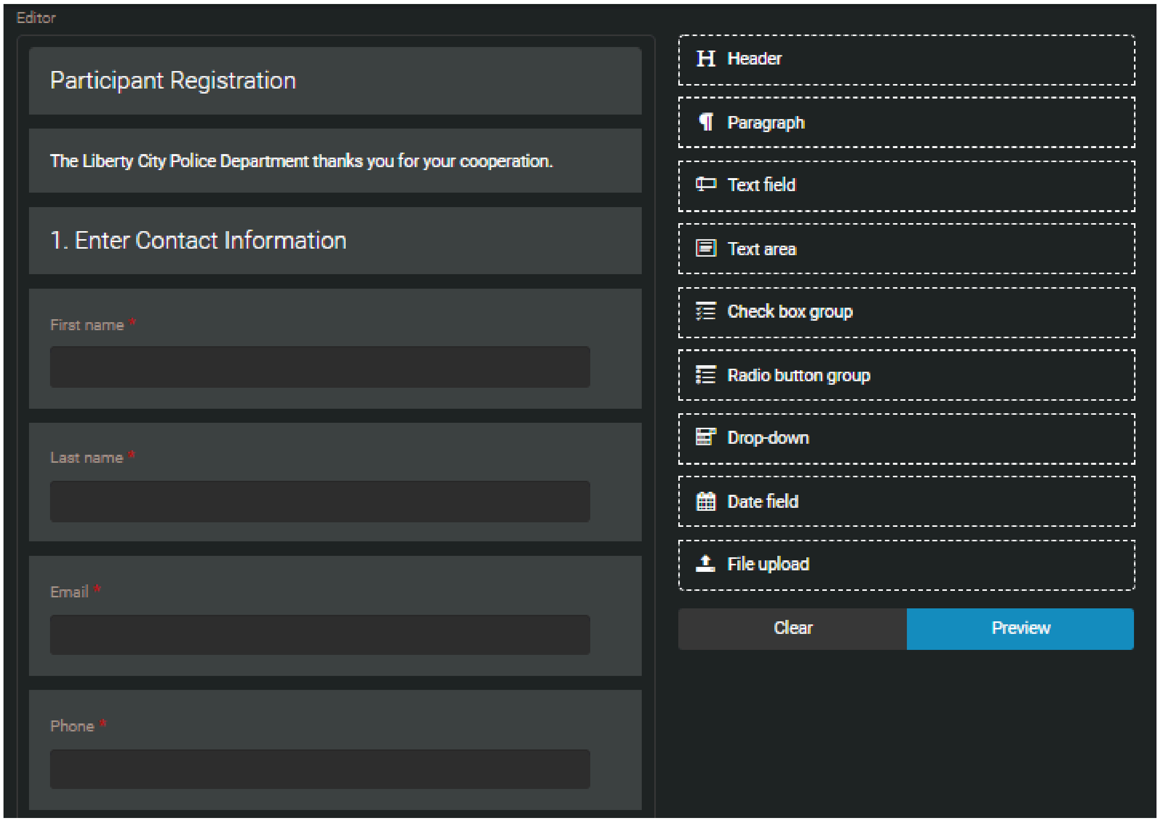
Name *
Livable Liberty City Enrollment Form

Project name
Livable Liberty City Project

Support email *
support@lcpd.gov

Description
This program is intended to enhance public safety in the Liberty City area.

5 Drag form elements from the list into the *Editor* pane as needed and move to the required position in the form.



Editor

Participant Registration

The Liberty City Police Department thanks you for your cooperation.

1. Enter Contact Information

First name *

Last name *

Email *

Phone *

6 Click **Edit** (✎) in each form element to modify the form contents and options.

a) (Optional) Configure **Header** options.

- **Header:**
  - **Label:** Enter the name or title of the form element.
  - **Type:** Select the subheading font size you require.
  - **Class:** Specifies advanced customization options. For more information, contact technical support.

b) (Optional) Configure **Paragraph** options.

- **Paragraph:**
  - **Content:** Enter the content that you require.
  - **Type:** Specifies the paragraph formatting required. Choose one of the following: paragraph, address, block quote, canvas, or output.
  - **Class:** Specifies advanced customization options. For more information, contact technical support.

c) (Optional) Configure **Text field** options.

- **Text field:**

    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Placeholder:** Enter hint information that is displayed in the field. For example, *Enter text here* or *Explain the incident*.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Value:** Used to specify a default value for this field in the form.
    - **Max Length:** Specifies the maximum number of numeric characters in the field. For example, you could specify 50 characters or you could set field length to match a use case like badge number length.

d) (Optional) Configure **Text area** options.

- **Text area:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Placeholder:** Enter hint information that is displayed in the field. For example, *Enter text here* or *Explain the incident*.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Value:** Used to specify a default value for this field in the form.
    - **Max Length:** Specifies the maximum number of numeric characters in the field. For example, you could specify 50 characters or you could set field length to match a use case like badge number length.

e) (Optional) Configure **Check box group** options.

- **Check box group:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Inline:** Select the check box to display multiple check box options in a line.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Options:** If you want to pre-fill the options, select one or more check boxes. Enter a name or title for each check box option.
    - **Add Option+:** Add additional option choice elements.

f) (Optional) Configure **Radio button group** options.

- **Radio button group:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Inline:** Select the check box to display multiple radio button options in a line.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Options:** If you want to pre-fill the options, select a radio button. Enter a name or title for each radio button option.
    - **Add Option+:** Add additional option choice elements.

g) (Optional) Configure **Drop-down** options.

- **Drop-down:**

    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Placeholder:** Enter hint information that is displayed in the field. For example, *Enter text here* or *Explain the incident*.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.

h) (Optional) Configure **Date field** options.

- **Date field:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.
    - **Value:** Used to specify a default value for this field in the form.

i) (Optional) Configure **File upload** options.

- **File upload:**
    - **Required:** Select the check box to make completing this form element mandatory.
    - **Label:** Enter the name or title of the form element.
    - **Help Text:** Enter help text to display when ? is clicked in the form.
    - **Class:** Specifies advanced customization options. For more information, contact technical support.

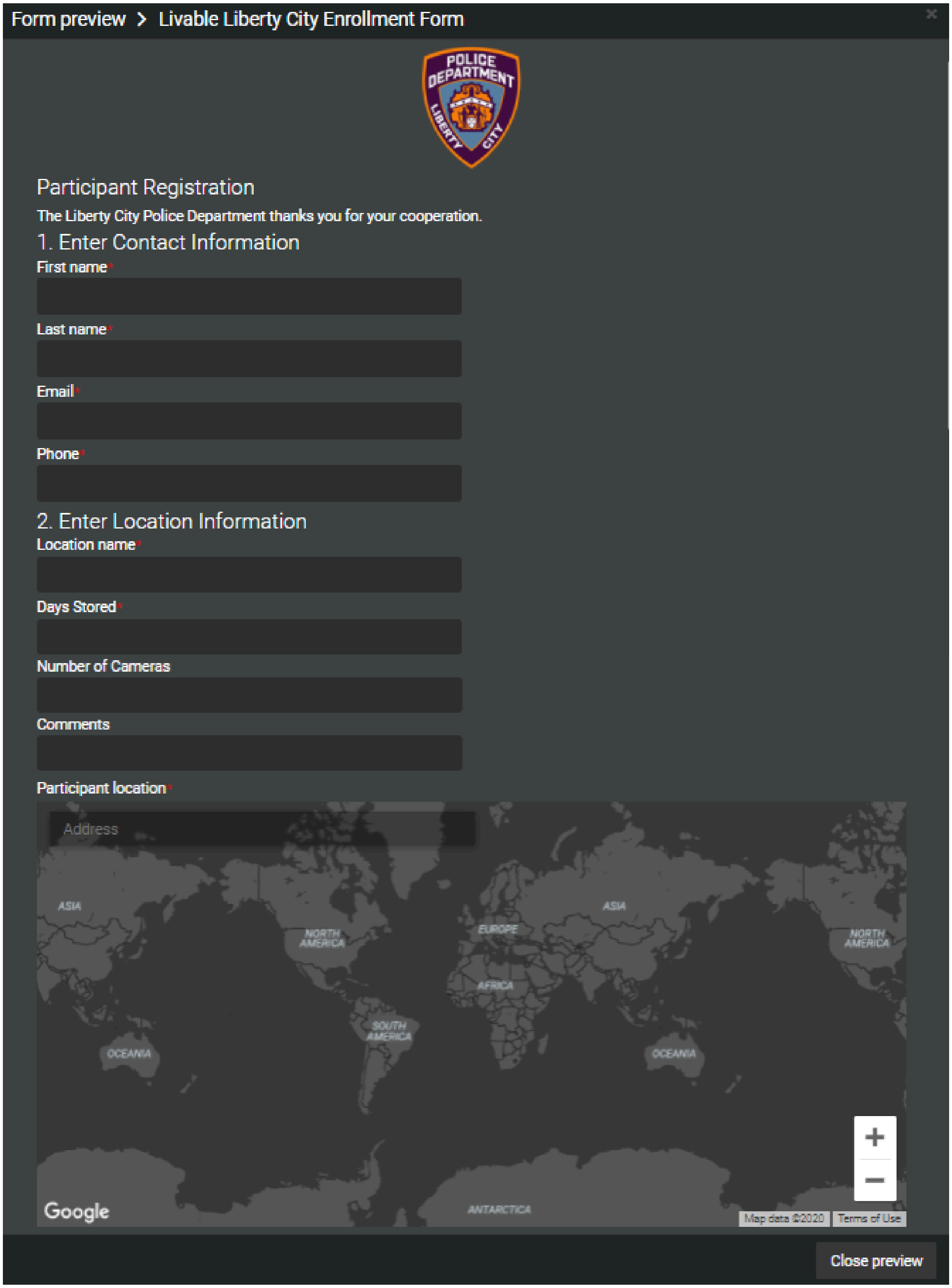
j) Configure **Participant location** options.

- **Label Address:** Specifies the participant's address.
- **Label Latitude:** Specifies the latitude of participant's location.
- **Label Longitude:** Specifies the longitude of participant's location.

7 (Optional) Click ⧉ to copy a form element.

8 (Optional) Click ❌ to remove a form element.

9 Click **Preview** to see a rendered version of your request form.



Form preview > Livable Liberty City Enrollment Form

Participant Registration

The Liberty City Police Department thanks you for your cooperation.

1. Enter Contact Information

First name*

Last name*

Email*

Phone*

2. Enter Location Information

Location name*

Days Stored*

Number of Cameras

Comments

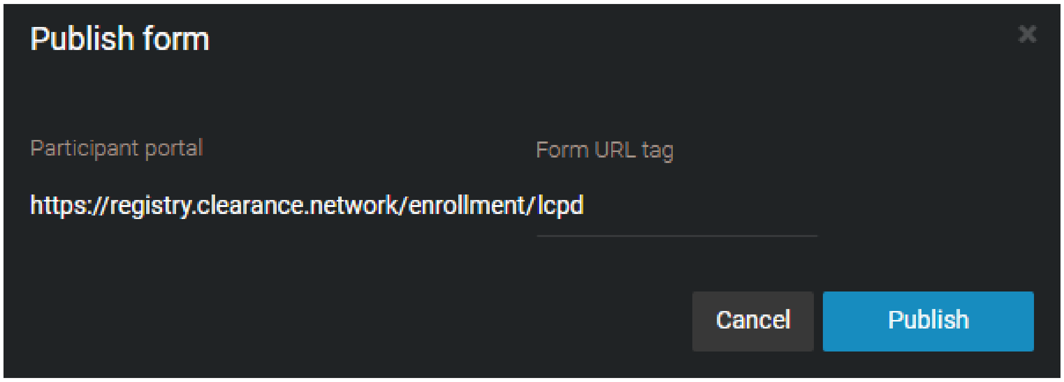
Participant location*

Figure 2: Example video request form

10 Click **Save** to apply your changes.

11 Click **Publish**.

12 Add a **Form URL tag** to your participant enrollment form link.



Publish form

Participant portal: https://registry.clearance.network/enrollment/lcpd

Form URL tag

13 Click **Publish**.

14 (Optional) To create a copy of this form, click **More** (⋮) and then click **Clone** (⧉).

Forms are now available to facilitate participant enrollment in public safety initiatives.

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

Embed your form on your organization's website.

Embedding participant enrollment forms

After you have created a participant enrollment form, you can customize it and embed it on your website so that participants can enroll in your initiative.

Before you begin

- **IMPORTANT**: Learn about content security policies
- Authorize the following URL as part of your content security policy: https://registry.clearance.network

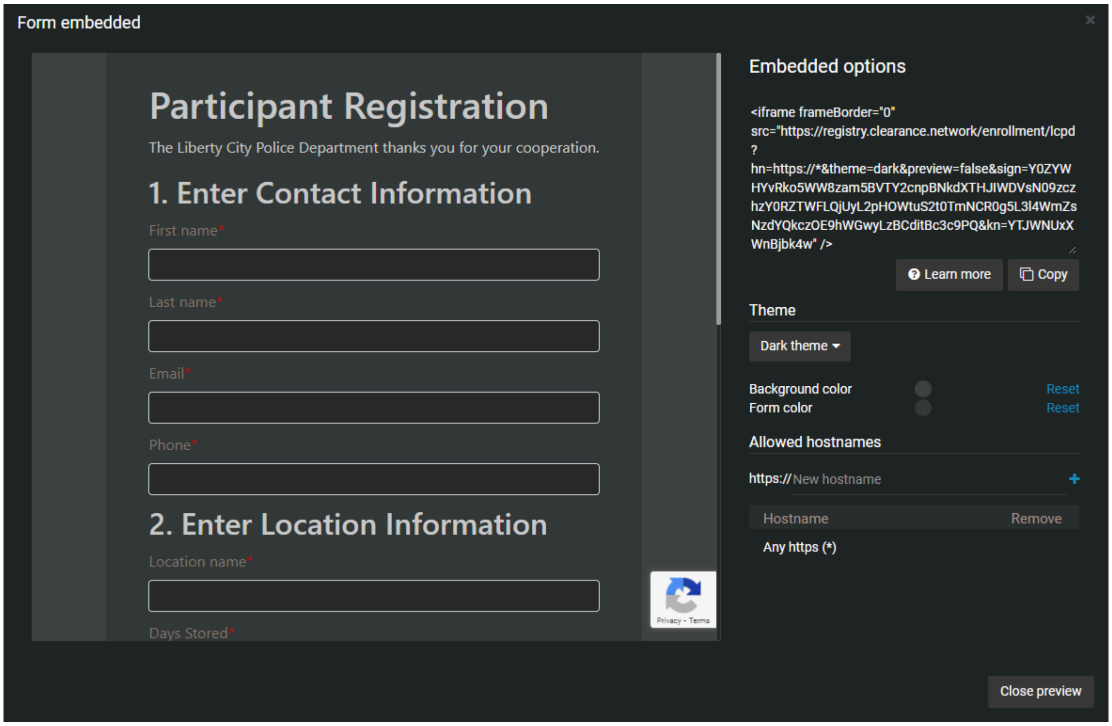
What you should know

- Users or groups in the *Manage forms* security policy can embed participant enrollment forms. System administrators is the default value for the policy.

Procedure

1 Click **Share** (🔗)

2 Click **Embedded** (</>).



Form embedded

Participant Registration

The Liberty City Police Department thanks you for your cooperation.

1. Enter Contact Information

First name*

Last name*

Email*

Phone*

2. Enter Location Information

Location name*

Days Stored*

Embedded options

```
<iframe frameBorder="0"
src="https://registry.clearance.network/enrollment/lcpd
?
hn=https://*&theme=dark&preview=false&sign=Y0ZYW
HYvRko5WW8zam5BVTY2cnpBNkdXTHJIWDVsN09zcz
hzY0RZTWFLQjUyL2pHOWtuS2t0TmNCR0g5L3l4WmZs
NzdYQkczOE9hWGwyLzBCditBc3c9PQ&kn=YTJWNUxX
WnBjbk4w" />
```

Theme: Dark theme

Background color ● Reset
Form color ● Reset

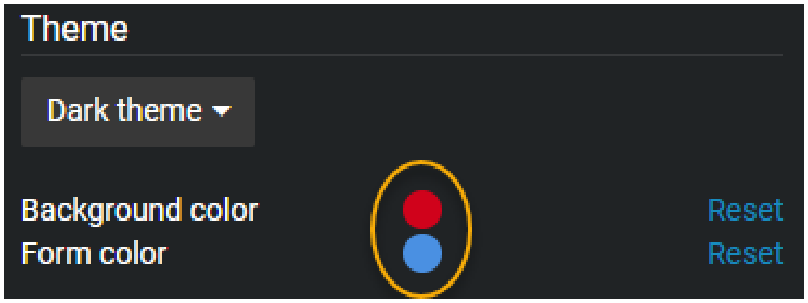
Allowed hostnames

https:// New hostname +

Hostname	Remove
Any https (*)	

3 (Optional) Define a color scheme for your form.

- **Dark theme**
- **Light theme**
- Define specific colors for your enrollment form

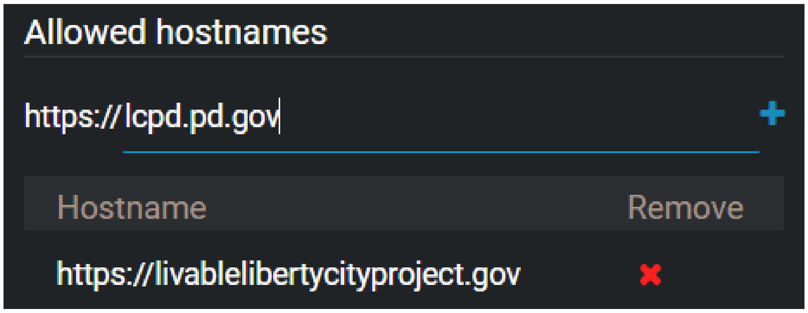


Theme

Dark theme

Background color 🟥 Reset
Form color 🟦 Reset

4 Click **Add** (+) to add allowed hostnames.



Allowed hostnames

https://lcpd.pd.gov

Hostname	Remove
https://livablelibertycityproject.gov	✖

IMPORTANT:

- You must add the hostname of every website that will host this form.
- Only https hostnames are supported.

5 Click **Copy** (⧉) and provide the link to your software developer so that they can embed it on your website.

NOTE: Your content security policies control what can and cannot be hosted on your website. If an error is displayed when you paste the link to your website, visit the following link for instructions on modifying your content security policy https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-src.

After you finish

Test that the form is available on your website.

Related Topics

About content security policies on page 82

About content security policies

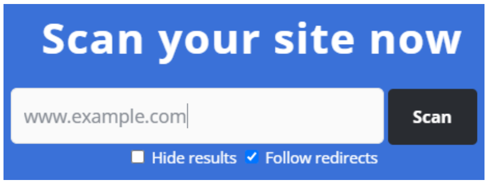
Content security policies control what can and cannot be hosted on your website.

What are content security policies?

- Content security policies are rules that websites use to control what can and cannot be hosted on a website. For example, if you want to embed Google maps on your website, Google maps must be added to your content security policy.
- Your website's content security policies might block you from embedding participant enrollment forms on your website. For more information, refer to your website's content security policies or visit the following link: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-src.

How can I find out if my website's content security policies will block me from embedding a participant enrollment form in Genetec Clearance™?

1. Go to https://securityheaders.com/.
2. Enter your website URL in the search box.

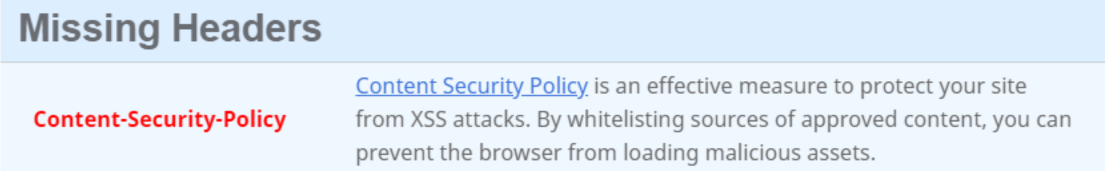


Scan your site now

www.example.com

3. Check the *Missing headers* section.

   - If **Content-security-policy** is listed in the *Missing headers* section, no further action is required at this time.

     Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.

   - If **Content-security-policy** is not listed in the *Missing headers* section, you must add https://registry.clearance.network to your content security policy. For more information contact your software developer.

Related Topics

Embedding participant enrollment forms on page 80

Resetting user passwords

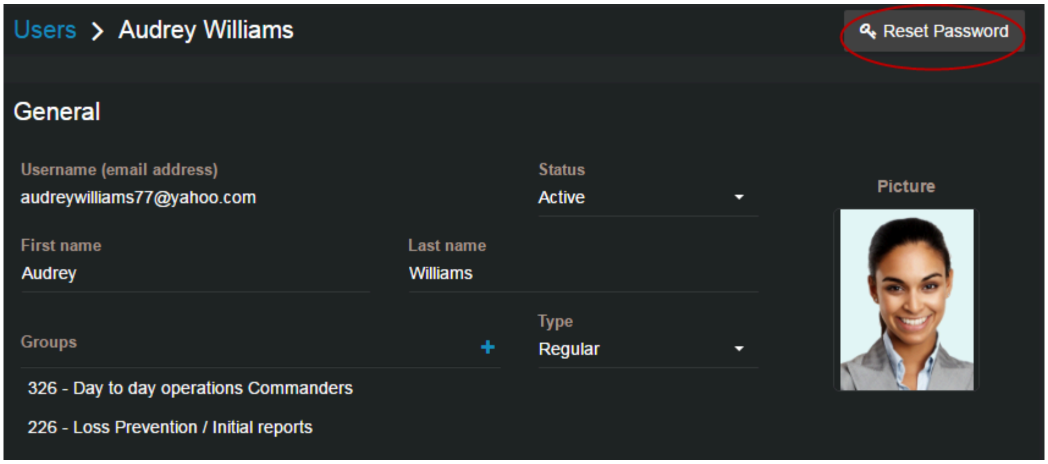
If a user has forgotten their password, you can reset it for them.

What you should know

If the user's account is managed by an Active Directory, their password cannot be reset from Clearance. They must contact their Active Directory system administrator for assistance.

Procedure

1. Click **Configurations**.
2. In the *Users* page, select a user.
3. In the user edit page, click **Reset Password**.



Users > Audrey Williams

Reset Password

General

Username (email address): audreywilliams77@yahoo.com

Status: Active

First name: Audrey

Last name: Williams

Groups

326 - Day to day operations Commanders

226 - Loss Prevention / Initial reports

Type: Regular

Picture

A password reset request is sent to the server. The user receives an email with instructions for resetting their password.

Example

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

▶

Related Topics

About email notifications in Clearance on page 3

Searching for users or groups

If you have many user and groups in the system, you can easily find them by using the search in the *Configurations* tab.

Procedure

1 Click **Configurations**.

2 In the *Users* page, type the name of a user or group, and then type ENTER or click the search button (🔍).

3 To filter your results by users or groups, select **Users** or **Groups**.

4 To filter your results by user status, select **Active** or **Inactive** from the drop-down list.

5 To filter your results by user type, select **Regular** or **Guest** from the drop down list.

Example

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

▶

Creating support tickets

To create a support ticket in Clearance, an account administrator can use the **Contact support** option accessed from the Help section.

What you should know

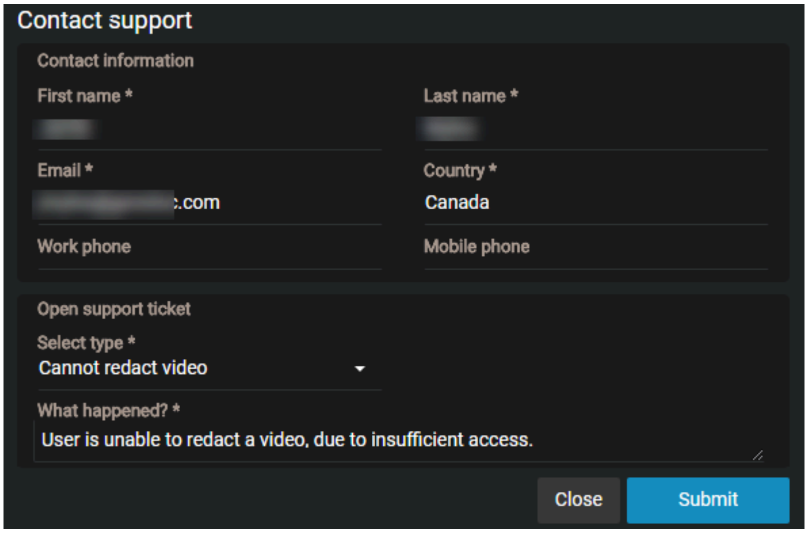
Only account administrators can create support tickets from Clearance.

Procedure

1 Click **Help** (?).

2 Click **Contact support**.

3 Complete the fields. Required fields are identified by an asterisk (*).



Contact support

Contact information

First name *

[redacted]

Last name *

[redacted]

Email *

[redacted].com

Country *

Canada

Work phone

Mobile phone

Open support ticket

Select type *

Cannot redact video

What happened? *

User is unable to redact a video, due to insufficient access.

a) In the *Open support ticket* section, select a ticket type from the **Select type *** drop-down list. For example, **Cannot redact video**.

b) In the **What happened? *** field, enter some text to describe the issue that occurred and how the error can be reproduced.

4 Click **Submit**.

A support ticket is raised containing contact information, problem, context, and account information. This information is then sent to the appropriate support team. A confirmation email from *Clearance Support* will be received.

Downloading a user list report

If you need to audit the users in your Genetec Clearance™ account, you can download a CSV file that lists all the users in your Clearance account.

Before you begin

Only users included in the Account Administrators group can download the user list report.

Procedure

1. Click **Configurations** > **Users**.
2. Click **Export**

   The user list report is downloaded as a CSV file.
3. Open the CSV file.

   TIP: You can filter the report by username, email, state (Active or Inactive), and type (Regular or Guest).

After you finish

For more information about user accounts, see Creating user accounts on page 48.

6

Managing cases

Manage cases to record the details of an incident and link digital evidence in Clearance.

This section includes the following topics:

- "Creating cases" on page 89
- "Creating a file request" on page 91
- "Creating a case summary report" on page 93
- "Creating an eDiscovery receipt" on page 96
- "Example of a case" on page 99
- "Assigning personnel to a case" on page 101
- "Sharing cases" on page 102
- "Pinning cases to the homepage" on page 104
- "Transferring cases" on page 106
- "Inviting guests to view cases" on page 108
- "Copying cases" on page 111
- "Changing access policies for cases" on page 112
- "Searching for cases or files" on page 113
- "Previewing evidence in cases" on page 119
- "Reopening cases" on page 120
- "Protecting cases from deletion" on page 121
- "Deleting cases" on page 122
- "Restoring cases" on page 124
- "Viewing the audit trail history of cases" on page 125
- "About closed cases " on page 126

Creating cases

To record the details of an incident and link digital evidence to the incident, you can create a case, and then share the case with other investigators within or outside your organization.

Before you begin

- Create and configure the department that you want to assign the case to.
- Ensure you are included in the **Create cases** security policy.

What you should know

If a case is no longer active, you can close the case. Closed cases are still part of the system and remain searchable. After a case is closed, only users or groups that have the *Manage* permission level for the case can reopen the case.

Files are automatically added to cases, as indicated by the (📋) icon, when all of the following apply:

- The evidence was recorded using a *body-worn camera* that is activated in Clearance.
- The evidence was recorded by an *assigned personnel* during the incident time range. This includes a 2-minute buffer before the incident start time and after the incident end time.
- A case has relevant assigned personnel.
- The evidence is associated with the same assigned personnel.

Procedure

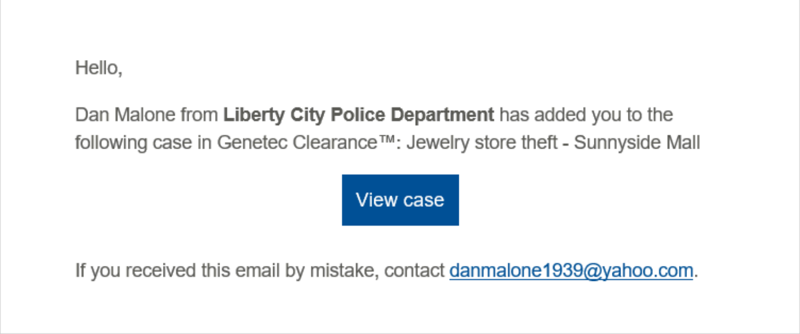
1. From either the *Search* or *Home* page, create a case.
2. Click ✎ and enter a name for the case.
3. Enter values for the following settings:
   - **Record number:** A reference number for the case.
   - **Incident number:** You can use this field to add external reference numbers to a case.
   - **Category:** The type of incident. For example, you can categorize thefts as being either employee theft or shoplifting. You can only select one category per case.
   - **Department:** The department within your organization that is responsible for the case. You can only select one department per case. For example, for a theft case, you can assign the case to the Loss Prevention Department. This field is mandatory.
   - **Incident start time:** Date and time the incident started.
   - **Incident end time:** Date and time the incident ended.
   - **Description:** A description of the case. Be descriptive so that others can easily find your case when searching for cases.
   - **Tags:** One-word keyword entries that identify the case and help users find the case when searching all cases. Ensure that you enter synonyms or alternate words for the type of incident. For example, for a case about theft, you can enter the tags **Stealing** or **Shoplifting**.
   - **Custom fields:** Enter or select a value from the custom fields included in the case.
   - **Location:** Set the location where the incident occurred. Type the location, or click **View map** (🗺) to search for the location on a map.
   - **Related Requests:** Click the links to view video requests associated with the case.
   - **Protect from deletion:** Click the checkbox to protect the case from being deleted.
   - **Subscribe:** Click **Subscribe** to receive email notifications whenever the case is modified.
   - **Permissions:** The users or user groups that you want to share the case with. You can give the users or groups *View only*, *View and download*, *Edit*, or *Manage* permission levels. However, at least one of the users or groups that you add must have full access (*Manage* permission level) to the case.

IMPORTANT: By selecting a department, the users, along with their respective permission levels to new cases, are displayed in the *Permissions* section after the case is saved.

- **Files:** The video files and other file types that you want to associate with the case. You can add files to the case by dragging the files into the **Files** field.

4 Click **Save**.

An email inviting users to view the case details is automatically sent to all of the users you assigned the case to.



Hello,

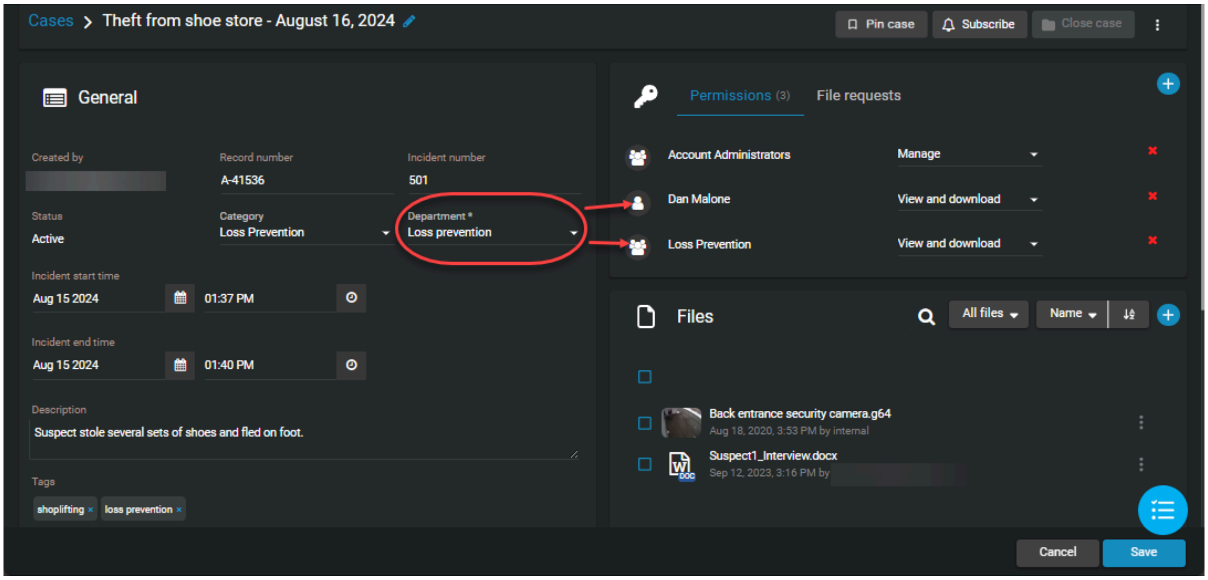
Dan Malone from **Liberty City Police Department** has added you to the following case in Genetec Clearance™: Jewelry store theft - Sunnyside Mall

View case

If you received this email by mistake, contact danmalone1939@yahoo.com.

Example

The following image shows an example of a case about employee theft. Because the case is assigned to the Loss Prevention Department, the members of this department are automatically displayed in the *Permissions* section.



Cases > Theft from shoe store - August 16, 2024

General

Created by [redacted]

Record number A-41536

Incident number 501

Status Active

Category Loss Prevention

Department * Loss prevention

Incident start time Aug 15 2024 01:37 PM

Incident end time Aug 15 2024 01:40 PM

Description Suspect stole several sets of shoes and fled on foot.

Tags shoplifting × loss prevention ×

Permissions (3) File requests

Account Administrators	Manage
Dan Malone	View and download
Loss Prevention	View and download

Files

□ Back entrance security camera.g64
Aug 18, 2020, 3:53 PM by internal

□ Suspect1_Interview.docx
Sep 12, 2023, 3:16 PM by [redacted]

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

Creating a file request

To allow anyone to add files to an incident without viewing the case contents, you can create a public file request, and then share the file request with anyone in or outside your organization.

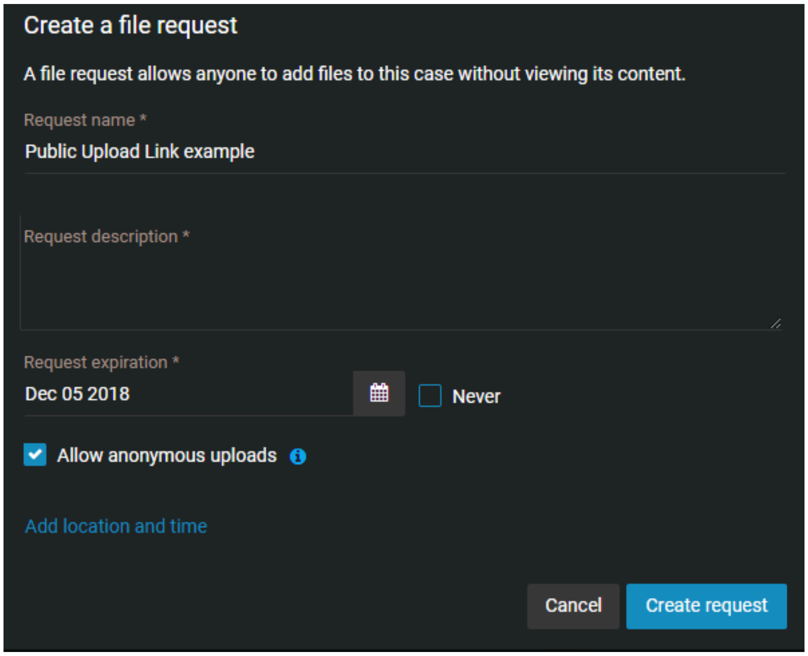
Before you begin

Create and configure the case that you want to associate the file request with.

Procedure

1 From either the *Search* or *Home* page, open a case.

2 Next to **Permissions**, click **File requests** and click add (+).



Create a file request

A file request allows anyone to add files to this case without viewing its content.

Request name *
Public Upload Link example

Request description *

Request expiration *
Dec 05 2018 □ Never

☑ Allow anonymous uploads

3 Enter values for the following settings:

- **Request name:** The name of the file request. This field is used as the title of the file request when it is shared.
- **Request description:** A description of the file request. This field is used as the description of the file request when it is shared. Be descriptive so that others can easily find the files when searching for file requests in cases.
- **Request expiration:** The expiration date of the file request.

4 (Optional) Select **Never** when you want the file request to remain active indefinitely.

5 (Optional) Select **Allow anonymous uploads**.
User contact information is optional when **Allow anonymous uploads** is selected.

6. Click **Add location and time** to add additional information to the file request.

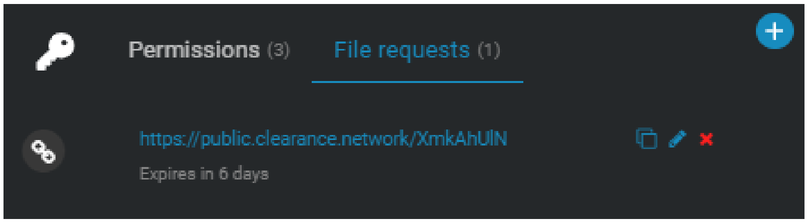
   NOTE: If the case already contains incident location, start time, or end time, these fields are automatically prefilled.

   - **Incident location:** Set the location where the incident occurred. Type the location, or click **View map** (🗺) to search for the location on a map.
   - **Start time:** Sorts the evidence preview list results based on the file start time. Click the ascending or descending arrow to change the **Start time** sort order.
   - **Incident end time:** Date and time the incident ended.

   a) If you clicked **View map** (🗺), select or modify the location and click **Set location**.

7. Click **Create request**.
8. Choose from the following:
   - Click **Copy** to copy the file request link then include in an email.
   - Click **Open link** to test the file request link or to scan the QR code before including in an email.
   - Click **Modify request** if you need to make any changes to the file request.
9. Click **Done** when you are finished.

   The file request link is added to the case in the *File requests* section.



https://public.clearance.network/XmkAhUlN

Expires in 6 days

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

You can return to the case at any time to copy the file request link (⧉), modify the file request (✎), modify expiration date (✎), or delete (✖) the file request.

Creating a case summary report

To export an overview of case information and associated files, use the case summary report. This report is used to create a local copy as a digital record of the case details and the evidence files it includes. This report can also be useful for someone who does not have access to Clearance, or to keep a record of the contents before cases or files are deleted.

Before you begin

- Configure your account info

What you should know

- The account information in the header of each report varies depending on your configuration and can include one or more of the following: the account logo, account name, address, or contact information.
- Only users with at least *View and Download* permissions for the case can access the case summary report.
- The *Uploaded by* column is only displayed in the case summary report when the **Permission details** check box is selected.

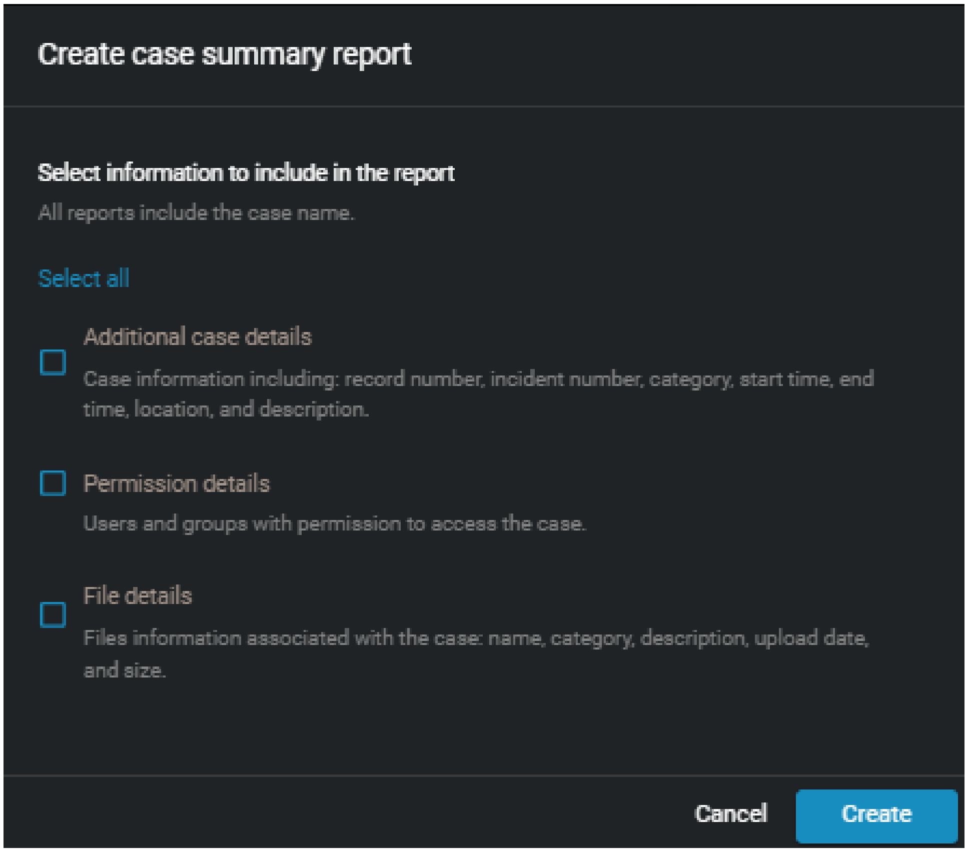
Procedure

1 From either the *Search* or *Home* page, open a case.

2 Click **More** (⋮) and click **Create report**.

3 In the *Select a report* dialog, click **Case summary report**.

4 In the *Create case summary report* dialog, select the check boxes that you require from the following:



Create case summary report

Select information to include in the report

All reports include the case name.

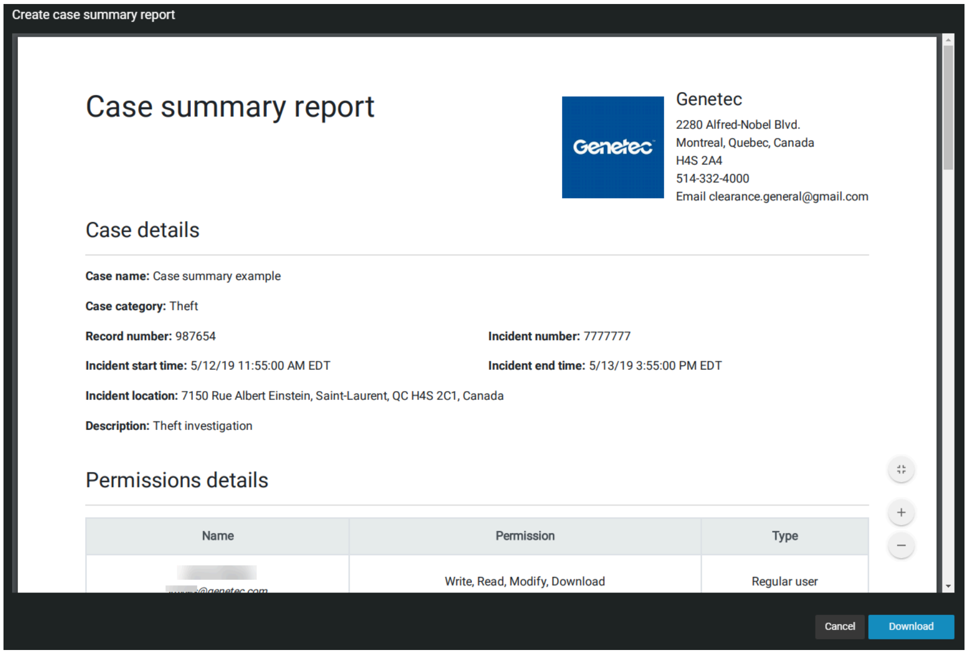
Select all

□ Additional case details
Case information including: record number, incident number, category, start time, end time, location, and description.

□ Permission details
Users and groups with permission to access the case.

□ File details
Files information associated with the case: name, category, description, upload date, and size.

5 Click **Create** to generate the report.



Create case summary report

Case summary report

Genetec
2280 Alfred-Nobel Blvd.
Montreal, Quebec, Canada
H4S 2A4
514-332-4000
Email clearance.general@gmail.com

Case details

Case name: Case summary example

Case category: Theft

Record number: 987654 **Incident number:** 7777777

Incident start time: 5/12/19 11:55:00 AM EDT **Incident end time:** 5/13/19 3:55:00 PM EDT

Incident location: 7150 Rue Albert Einstein, Saint-Laurent, QC H4S 2C1, Canada

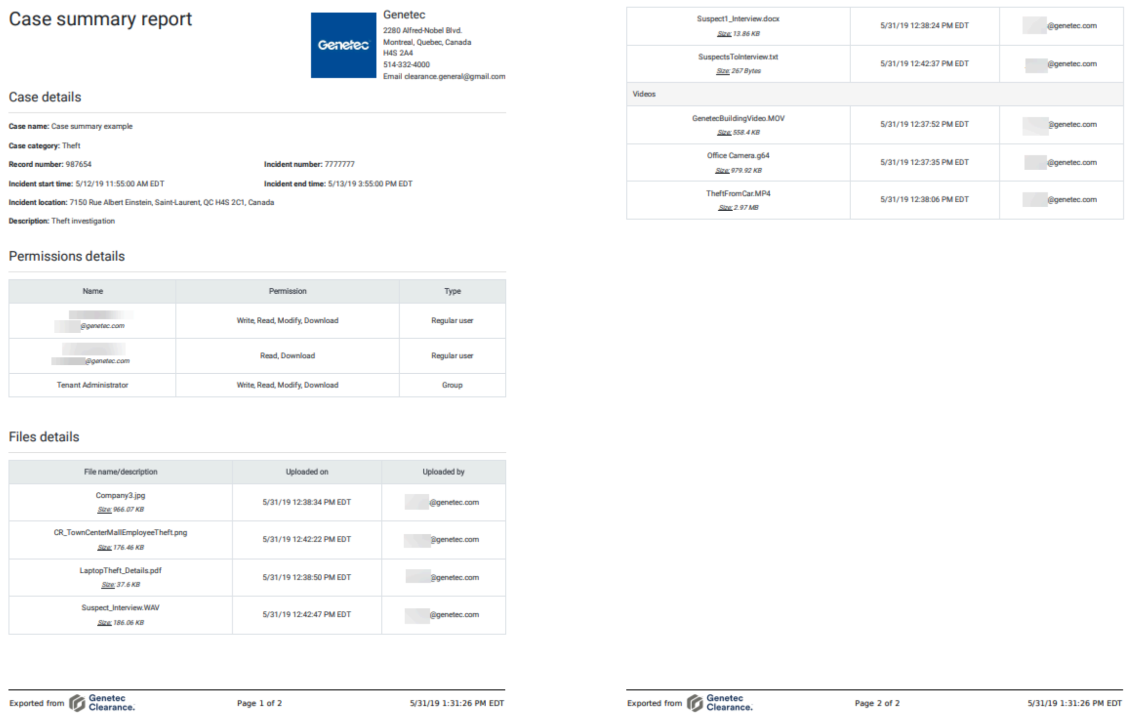
Description: Theft investigation

Permissions details

Name	Permission	Type
[redacted] [redacted]@genetec.com	Write, Read, Modify, Download	Regular user

A copy of the case summary report PDF is stored in Clearance.

6 Click **Download**.
The Case summary report is saved as a PDF format file. For example, *CaseSummary_Case1652.pdf*



Case summary report

Genetec
2280 Alfred-Nobel Blvd.
Montreal, Quebec, Canada
H4S 2A4
514-332-4000
Email clearance.general@gmail.com

Case details

Case name: Case summary example

Case category: Theft

Record number: 987654 **Incident number:** 7777777

Incident start time: 5/12/19 11:55:00 AM EDT **Incident end time:** 5/13/19 3:55:00 PM EDT

Incident location: 7150 Rue Albert Einstein, Saint-Laurent, QC H4S 2C1, Canada

Description: Theft investigation

Permissions details

Name	Permission	Type
[redacted] [redacted]@genetec.com	Write, Read, Modify, Download	Regular user
[redacted] [redacted]@genetec.com	Read, Download	Regular user
Tenant Administrator	Write, Read, Modify, Download	Group

Files details

File name/description	Uploaded on	Uploaded by
Company3.jpg *Size: 966.07 KB*	5/31/19 12:38:34 PM EDT	[redacted]@genetec.com
CR_TownCenterMallEmployeeTheft.png *Size: 176.46 KB*	5/31/19 12:42:22 PM EDT	[redacted]@genetec.com
LaptopTheft_Details.pdf *Size: 37.6 KB*	5/31/19 12:38:50 PM EDT	[redacted]@genetec.com
Suspect_Interview.WAV *Size: 186.06 KB*	5/31/19 12:42:47 PM EDT	[redacted]@genetec.com
Suspect1_Interview.docx *Size: 13.86 KB*	5/31/19 12:38:24 PM EDT	[redacted]@genetec.com
SuspectsToInterview.txt *Size: 267 Bytes*	5/31/19 12:42:37 PM EDT	[redacted]@genetec.com
Videos		
GenetecBuildingVideo.MOV *Size: 558.4 KB*	5/31/19 12:37:52 PM EDT	[redacted]@genetec.com
Office Camera.g64 *Size: 979.92 KB*	5/31/19 12:37:35 PM EDT	[redacted]@genetec.com
TheftFromCar.MP4 *Size: 2.97 MB*	5/31/19 12:38:06 PM EDT	[redacted]@genetec.com

Exported from Genetec Clearance. Page 1 of 2 5/31/19 1:31:26 PM EDT

Exported from Genetec Clearance. Page 2 of 2 5/31/19 1:31:26 PM EDT

After you finish

Forward the **Case summary report** to any required recipients or store a copy for your records.

Related Topics

Configuring your account information on page 36

Creating an eDiscovery receipt

To capture a digital proof of receipt for evidence being shared between Attorney and Defence offices, use the eDiscovery receipt. The eDiscovery receipt is sent to the recipient to obtain a dated acknowledgment and signature. The report is then kept as a digital record of evidence shared, how it was sent, and includes a list of the items shared.

Before you begin

- Configure your account info
- Configure your eDiscovery receipt report template
- Defining security policies on page 63

What you should know

- 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.
- The account information in the header of each report varies depending on your configuration and can include one or more of the following: the account logo, account name, address, or contact information.
- The *terms of acknowledgment* statement is typically configured by the account administrator and can include customized criminal code statements which can vary for the office, state, region and so on.
- Only users with *View and Download* permissions for the case can access the eDiscovery receipt report.
- Only users with *Access audit trail and create eDiscovery receipt* permissions can access the functions.

Procedure

1 Open an existing case.

2 Click **More** (⋮) and click **Create report**.

3 In the *Select a report* dialog box, click **eDiscovery receipt**.

4 In the **Create eDiscovery receipt** dialog, complete the following:

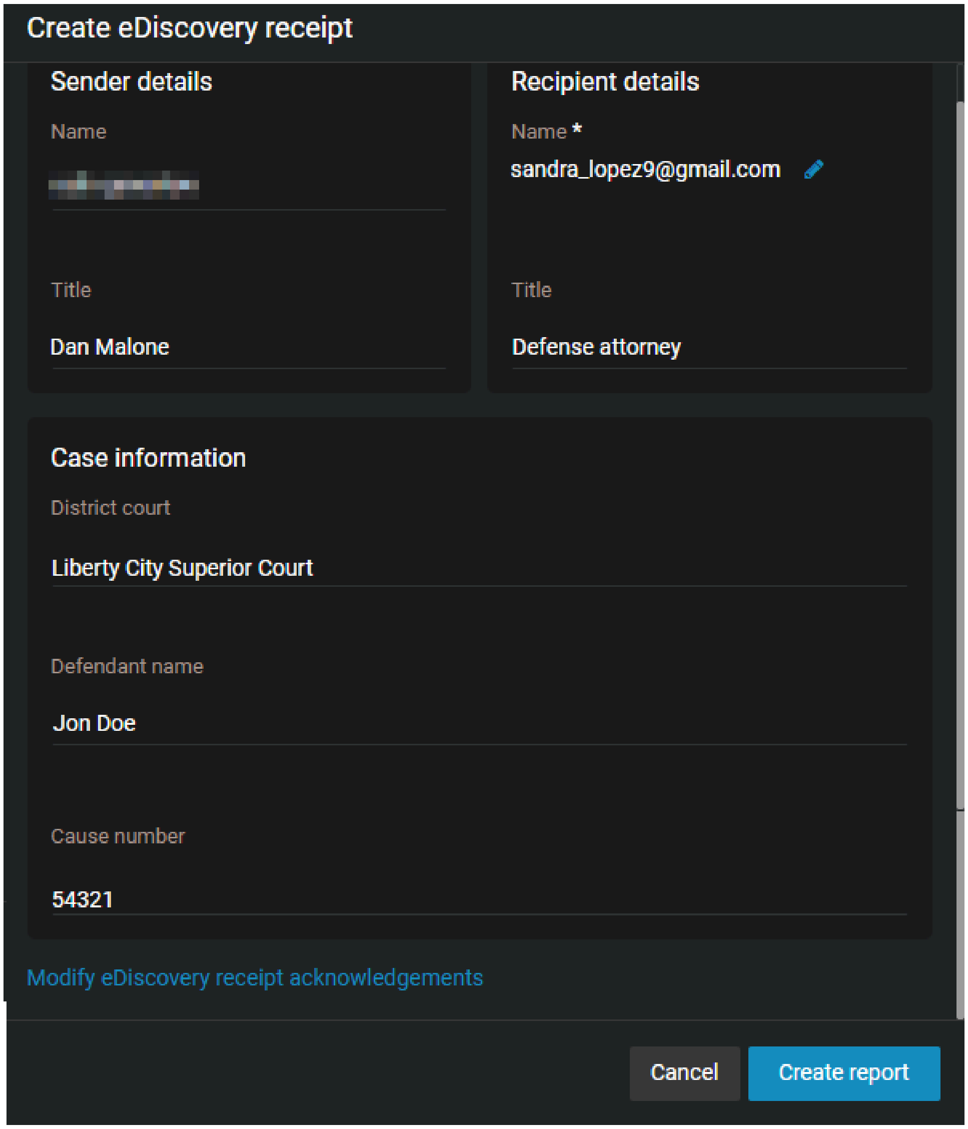
a) (Optional) In the *Sender details* section, enter a **Name** and **Title**.

If the sender title field is left blank, the *user* string is used as the default title. For example, "eDiscovery receipt for files shared with *user*."

b) In the **Recipient details** section, click **Select** to choose a recipient and enter their **Title** if applicable.

c) (Optional) In the *Case information* section, enter the **District court details**, **Defendant name**, and **Cause number**.

5 (Optional) Click **Modify eDiscovery receipt acknowledgments** if you need to amend the terms of acknowledgment.



Create eDiscovery receipt

Sender details

Name

[redacted]

Title

Dan Malone

Recipient details

Name *

sandra_lopez9@gmail.com

Title

Defense attorney

Case information

District court

Liberty City Superior Court

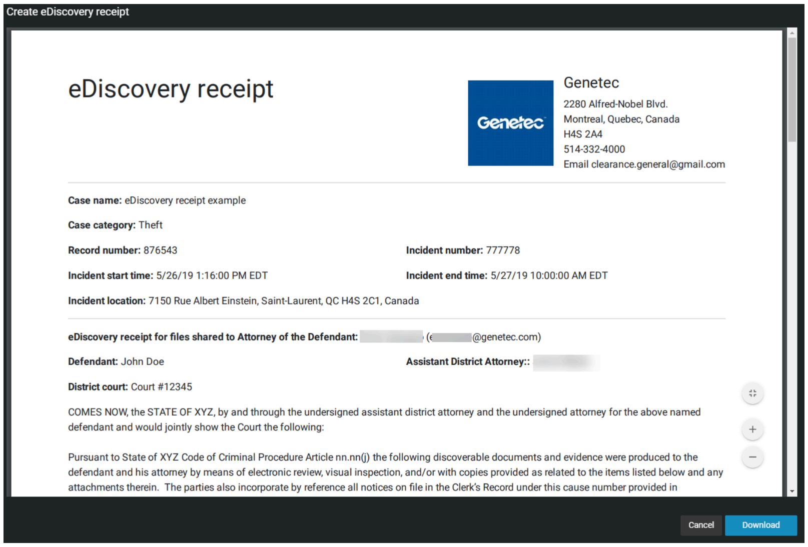
Defendant name

Jon Doe

Cause number

54321

6 Click **Create report**.



eDiscovery receipt

Genetec
2280 Alfred-Nobel Blvd.
Montreal, Quebec, Canada
H4S 2A4
514-332-4000
Email clearance.general@gmail.com

Case name: eDiscovery receipt example

Case category: Theft

Record number: 876543 **Incident number:** 777778

Incident start time: 5/26/19 1:16:00 PM EDT **Incident end time:** 5/27/19 10:00:00 AM EDT

Incident location: 7150 Rue Albert Einstein, Saint-Laurent, QC H4S 2C1, Canada

eDiscovery receipt for files shared to Attorney of the Defendant: [redacted] ([redacted]@genetec.com)

Defendant: John Doe **Assistant District Attorney::** [redacted]

District court: Court #12345

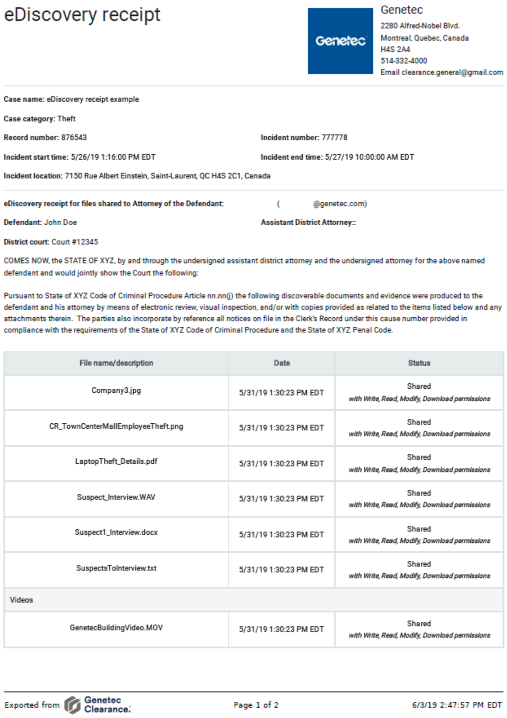
COMES NOW, the STATE OF XYZ, by and through the undersigned assistant district attorney and the undersigned attorney for the above named defendant and would jointly show the Court the following:

Pursuant to State of XYZ Code of Criminal Procedure Article nn.nn(j) the following discoverable documents and evidence were produced to the defendant and his attorney by means of electronic review, visual inspection, and/or with copies provided as related to the items listed below and any attachments therein. The parties also incorporate by reference all notices on file in the Clerk's Record under this cause number provided in

A copy of the eDiscovery receipt report PDF is stored in Clearance.

7 Click **Download**.

The eDiscovery receipt is saved as a PDF format file. For example, *CaseAuditLog_Case1652.pdf*



eDiscovery receipt

Genetec
2280 Alfred-Nobel Blvd.
Montreal, Quebec, Canada
H4S 2A4
514-332-4000
Email clearance.general@gmail.com

Case name: eDiscovery receipt example

Case category: Theft

Record number: 876543 **Incident number:** 777778

Incident start time: 5/26/19 1:16:00 PM EDT **Incident end time:** 5/27/19 10:00:00 AM EDT

Incident location: 7150 Rue Albert Einstein, Saint-Laurent, QC H4S 2C1, Canada

eDiscovery receipt for files shared to Attorney of the Defendant: (@genetec.com)

Defendant: John Doe **Assistant District Attorney::**

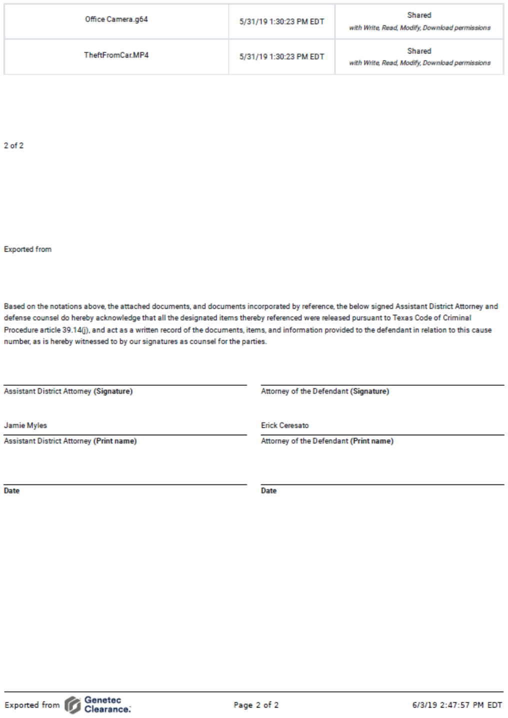
District court: Court #12345

COMES NOW, the STATE OF XYZ, by and through the undersigned assistant district attorney and the undersigned attorney for the above named defendant and would jointly show the Court the following:

Pursuant to State of XYZ Code of Criminal Procedure Article nn.nn(j) the following discoverable documents and evidence were produced to the defendant and his attorney by means of electronic review, visual inspection, and/or with copies provided as related to the items listed below and any attachments therein. The parties also incorporate by reference all notices on file in the Clerk's Record under this cause number provided in compliance with the requirements of the State of XYZ Code of Criminal Procedure and the State of XYZ Penal Code.

File name/description	Date	Status
Company3.jpg	5/31/19 1:30:23 PM EDT	Shared *with Write, Read, Modify, Download permissions*
CR_TownCenterMallEmployeeTheft.png	5/31/19 1:30:23 PM EDT	Shared *with Write, Read, Modify, Download permissions*
LaptopTheft_Details.pdf	5/31/19 1:30:23 PM EDT	Shared *with Write, Read, Modify, Download permissions*
Suspect_Interview.WAV	5/31/19 1:30:23 PM EDT	Shared *with Write, Read, Modify, Download permissions*
Suspect1_Interview.docx	5/31/19 1:30:23 PM EDT	Shared *with Write, Read, Modify, Download permissions*
SuspectsToInterview.txt	5/31/19 1:30:23 PM EDT	Shared *with Write, Read, Modify, Download permissions*
Videos		
GenetecBuildingVideo.MOV	5/31/19 1:30:23 PM EDT	Shared *with Write, Read, Modify, Download permissions*

Exported from Genetec Clearance. Page 1 of 2 6/3/19 2:47:57 PM EDT



Office Camera.g64	5/31/19 1:30:23 PM EDT	Shared *with Write, Read, Modify, Download permissions*
TheftFromCar.MP4	5/31/19 1:30:23 PM EDT	Shared *with Write, Read, Modify, Download permissions*

2 of 2

Exported from

Based on the notations above, the attached documents, and documents incorporated by reference, the below signed Assistant District Attorney and defense counsel do hereby acknowledge that all the designated items thereby referenced were released pursuant to Texas Code of Criminal Procedure article 39.14(j), and act as a written record of the documents, items, and information provided to the defendant in relation to this cause number, as is hereby witnessed to by our signatures as counsel for the parties.

Assistant District Attorney **(Signature)** Attorney of the Defendant **(Signature)**

Jamie Myles Erick Ceresato
Assistant District Attorney **(Print name)** Attorney of the Defendant **(Print name)**

Date **Date**

Exported from Genetec Clearance. Page 2 of 2 6/3/19 2:47:57 PM EDT

After you finish

Send the **eDiscovery receipt** report to the recipient for acknowledgment and signature.

Related Topics

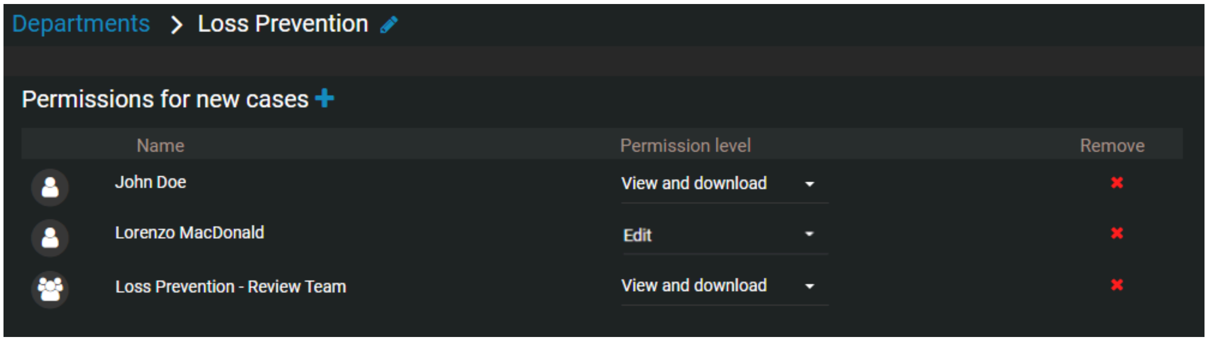
Configuring your account information on page 36
Configuring your report templates on page 39

Example of a case

After you have created your departments, you can create cases for all types of incidents. This example shows how department access policies are applied to a case concerning loss prevention

Figure A. Members of the Loss Prevention Department and their access policies

Two users and one group make up the Loss Prevention department. The access policy for new cases is assigned in the *Departments* page, which defines the permission level for each user and group.



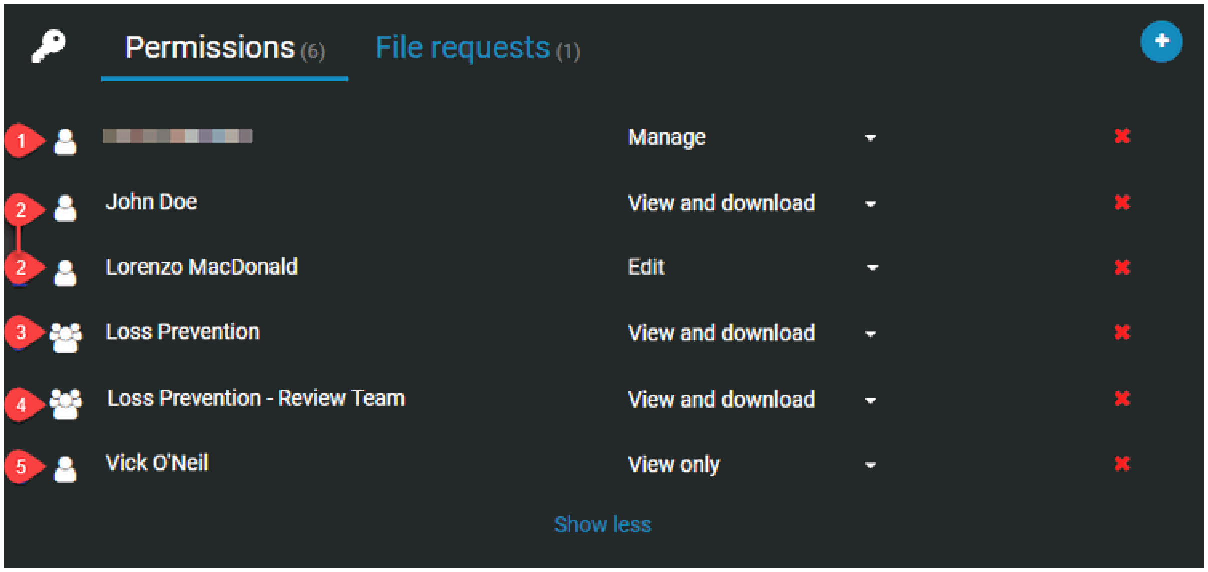
Departments > Loss Prevention

Permissions for new cases +

Name	Permission level	Remove
John Doe	View and download	✖
Lorenzo MacDonald	Edit	✖
Loss Prevention - Review Team	View and download	✖

Figure B. New case assigned to the Loss Prevention Department

After the new case is saved, the members of this department are automatically displayed in the **Permissions** section. The permission levels displayed next to their names match the ones shown in Figure A.



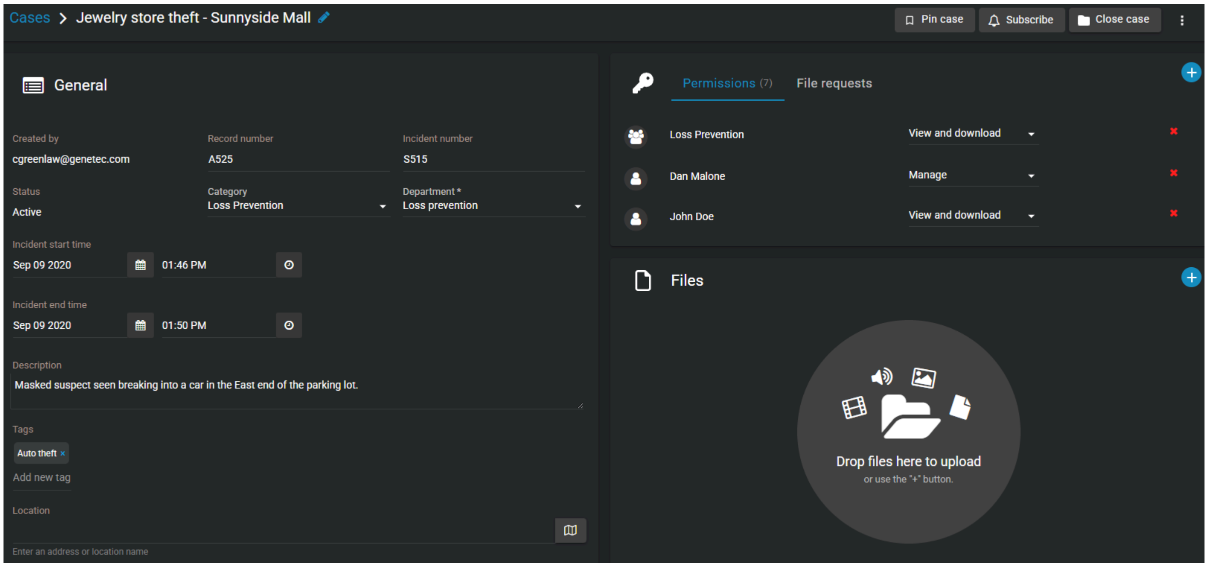
Permissions (6) File requests (1)

1	[redacted]	Manage	✖
2	John Doe	View and download	✖
2	Lorenzo MacDonald	Edit	✖
3	Loss Prevention	View and download	✖
4	Loss Prevention - Review Team	View and download	✖
5	Vick O'Neil	View only	✖

Show less

Number	Permission description
1	Creator (owner) of the case. By default, the creator of a case has full access to the case (*Manage* permission level).
2	Users that are members of the Loss Prevention department. The users' respective permission levels (defined in the department) are displayed here automatically.
3	The Loss Prevention group.

Number	Permission description
4	User group that is a member of Loss Prevention. The group's permission level (defined in the department) is displayed here automatically.
5	User that is not a member of Loss Prevention. By default, users added to cases through the Users field get only Read access to cases. You can change the permission level, as required.



General

Created by: cgreenlaw@genetec.com
Record number: A525
Incident number: S515
Status: Active
Category: Loss Prevention
Department *: Loss prevention
Incident start time: Sep 09 2020 01:46 PM
Incident end time: Sep 09 2020 01:50 PM
Description: Masked suspect seen breaking into a car in the East end of the parking lot.
Tags: Auto theft ×
Add new tag
Location
Enter an address or location name

Permissions (7) File requests

Loss Prevention	View and download
Dan Malone	Manage
John Doe	View and download

Files

Drop files here to upload
or use the "+" button.

Example

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

Assigning personnel to a case

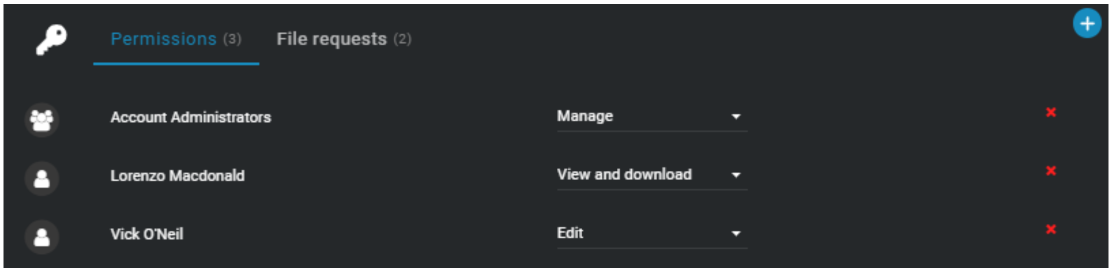
You can add one or more users to the *Permissions* section in the *Case* page to track who was involved in a case or incident.

What you should know

You can only change the assigned personnel for a case if you have the *edit* permission level for that case.

Procedure

1. From either the *Search* or *Home* page, open a case.
2. In the *Permissions* section click **Add** (⊕).
3. Choose to add an existing user, or invite a guest user.
4. In the *search* box, type a user name, officer ID, or email address, and press **Enter** or click the **search** button (🔍).
5. Select the check box for the user that you require and click **Add**.



Permissions (3) File requests (2)

Account Administrators	Manage
Lorenzo Macdonald	View and download
Vick O'Neil	Edit

6. (Optional) Click ✖ **Remove** to remove any personnel that are no longer required.
7. Click **Save**.
   The selected personnel are now assigned to the case.

Sharing cases

To let internal or external members of your organization view, modify, and manage cases, you can share cases with them and define their access rights on a case by case basis.

Before you begin

Create a user account for the user you want to share the case with.

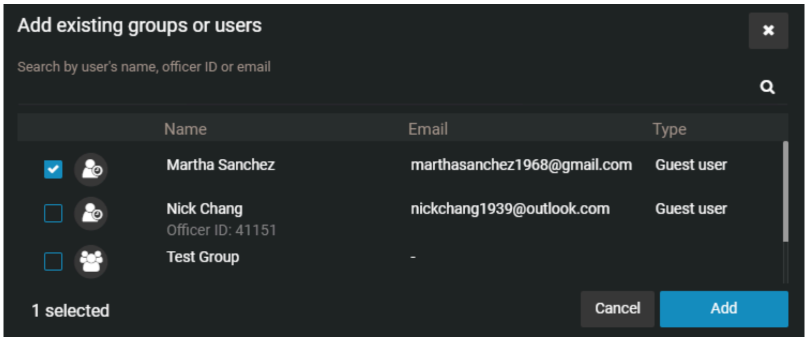
Procedure

1 Open an existing case or create a case.

2 In the **Permissions** section, click one of the following:

- **Add users** (+)
- **Invite guest user** (+)

3 If you selected **Add users**, in the *Add existing users* window, select your user of choice and then click **Add**.



Add existing groups or users

Search by user's name, officer ID or email

	Name	Email	Type
☑	Martha Sanchez	marthasanchez1968@gmail.com	Guest user
□	Nick Chang Officer ID: 41151	nickchang1939@outlook.com	Guest user
□	Test Group	-	

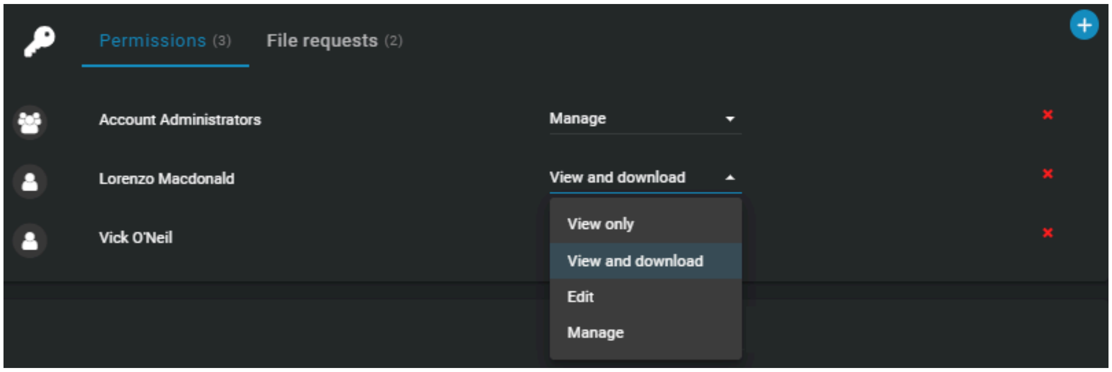
1 selected

4 If you selected **Invite guest user**, enter the email of the guest user you want to share the case with.

a) (Optional) Add a first and last name for the user.

The user is added to the list of users and, by default, is given the View and download permission level for the case.

5 Change the permission level for the user, as required, and then click **Save**.



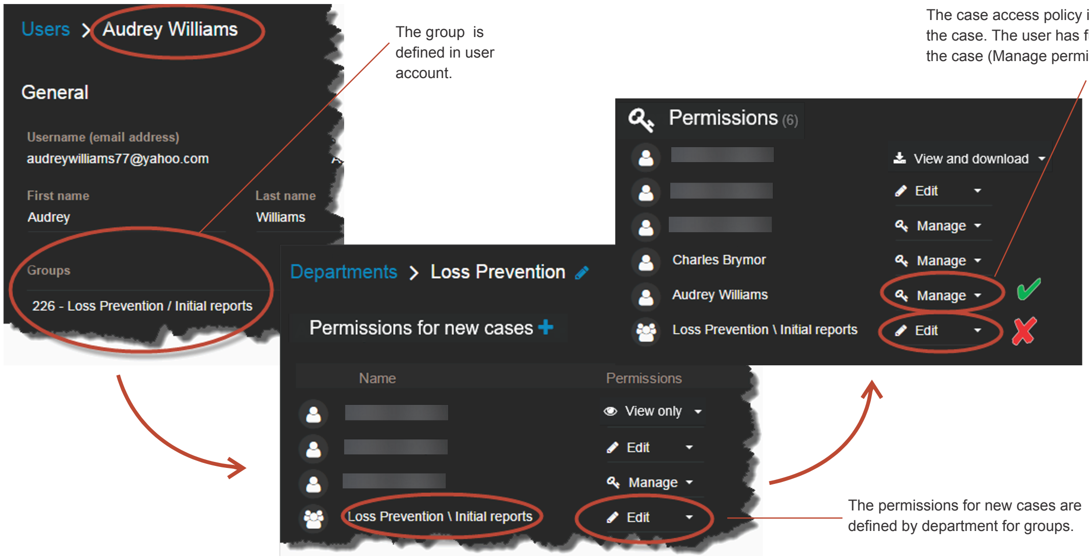
Permissions (3) File requests (2)

Account Administrators	Manage
Lorenzo Macdonald	View and download
Vick O'Neil	

An email is automatically sent to the user, inviting the user to view the case details.

Example

As shown in the following image, let's assume Audrey Williams is a member of the group Initial Reports in the Loss Prevention Department. As defined on the *Departments* page, the Initial Reports group has *Edit* permission level for new cases. However, because Audrey Williams was added to this case as a user and was given the *Manage* permission level, she now has full access.



Users > Audrey Williams

General

Username (email address): audreywilliams77@yahoo.com

First name: Audrey

Last name: Williams

Groups: 226 - Loss Prevention / Initial reports

The group is defined in user account.

Departments > Loss Prevention

Permissions for new cases

Name	Permissions
[redacted]	View only
[redacted]	Edit
[redacted]	Manage
Loss Prevention \ Initial reports	Edit

The permissions for new cases are defined by department for groups.

Permissions (6)

[redacted]	View and download
[redacted]	Edit
[redacted]	Manage
Charles Brymor	Manage
Audrey Williams	Manage ✓
Loss Prevention \ Initial reports	Edit ✗

The case access policy is defined in the case. The user has full access to the case (Manage permission level).

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

Related Topics

About email notifications in Clearance on page 3

Inviting guests to view cases on page 108

Pinning cases to the homepage

You can pin cases to the homepage in Genetec Clearance™ to quickly locate the ones you're working on or that require review.

What you should know

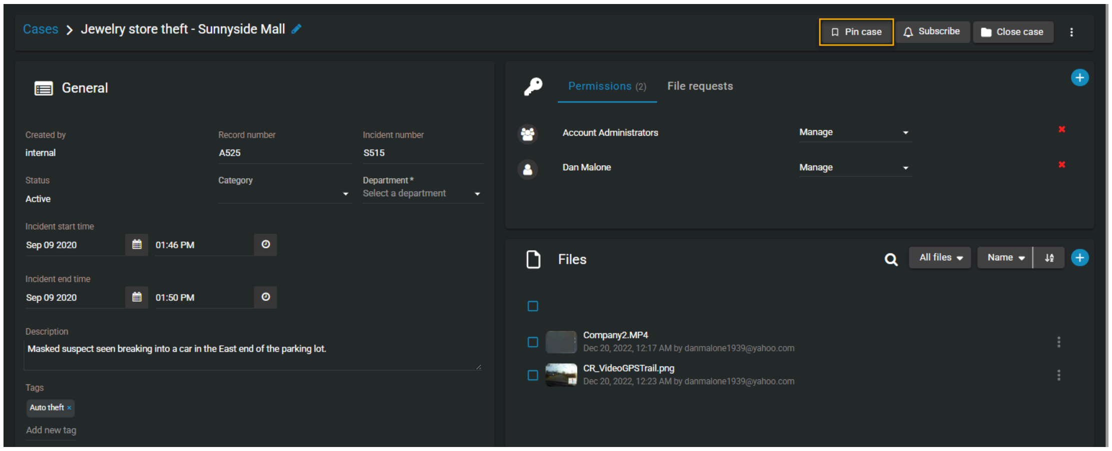
- Each Clearance user has their own list of pinned cases.
- You can pin any case that you have access to, no matter your permission level.
- Each Clearance user can have up to 50 cases pinned to the homepage at one time.

Procedure

To pin a case:

1 Open an existing case or create a case.

2 Click **Pin case**.



Created by: internal

Record number: A525

Incident number: S515

Status: Active

Category:

Department *: Select a department

Incident start time: Sep 09 2020 01:46 PM

Incident end time: Sep 09 2020 01:50 PM

Description: Masked suspect seen breaking into a car in the East end of the parking lot.

Tags: Auto theft ×

Add new tag

Account Administrators	Manage
Dan Malone	Manage

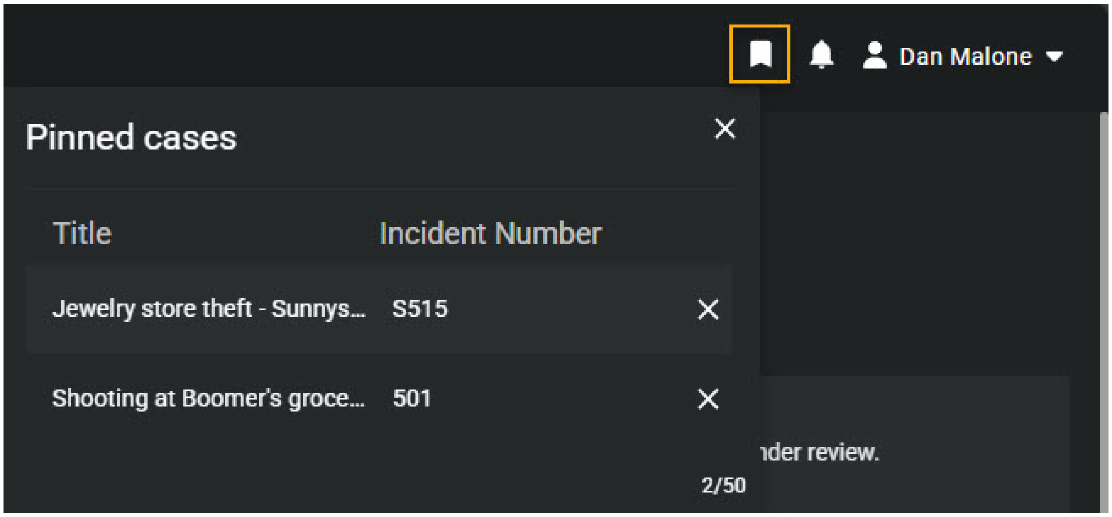
□ Company2.MP4 Dec 20, 2022, 12:17 AM by danmalone1939@yahoo.com

□ CR_VideoGPSTrail.png Dec 20, 2022, 12:23 AM by danmalone1939@yahoo.com

The case is pinned and can be accessed from the toolbar at the top of the screen.

To access pinned cases:

1 Click **Pinned cases** (🔖).



Pinned cases

Title	Incident Number
Jewelry store theft - Sunnys...	S515
Shooting at Boomer's groce...	501

2/50

ıder review.

2 Select the case of interest.

After you finish

(Optional)

- Upload files to the case.
- If necessary, change access policies for the case.

Transferring cases

You can transfer a case and its associated files to other organizations that have a Clearance account. Transferring a case creates a replica of the data that is shared, so each organization can administer their own access rights, permissions, and retention schedules based on their requirements. The transfer and receipt of the case is logged in the audit trail to show how the information has been shared.

Before you begin

- Define your access policies for incoming cases and add the organizations you want to transfer cases to and receive transfers from.

What you should know

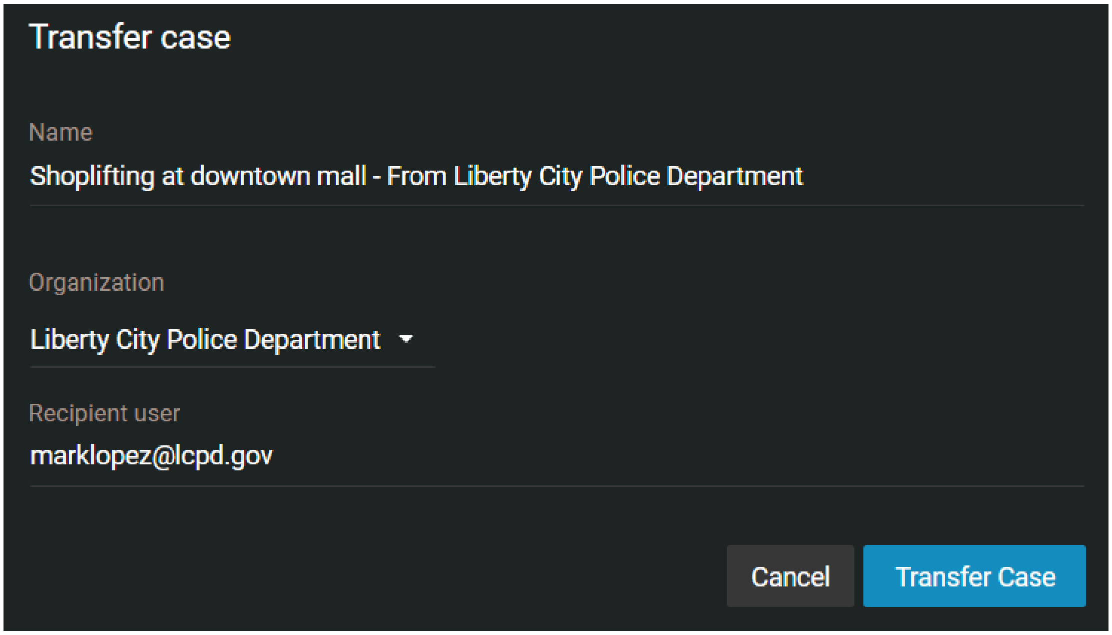
- Any user who has *Manage* permissions for a case can transfer that case to another organization.
- Guest users cannot transfer cases.
- Changes made to transferred cases are not synchronized between accounts, so any changes made after a case is transferred are not synchronized back to the original case.
- The original case will remain open and the audit trail will show that it was transferred.
- The recipient's case audit trail will show the organization that transferred the case, but will not show previous activity that occurred in the original account.
- Cases can only be transferred to other accounts within the same Microsoft Azure data center region, so it is not possible to transfer a case from an account that is hosted, for example, in the United States to one hosted in Canada.

Procedure

1. Select the case you want to transfer.
2. Click **More** (⋮).
3. Click **Transfer case**.

4 Enter a **Name** for the case, the **Organization** you want to transfer it to, and the **Recipient user** you want to transfer the case to.

NOTE: The **Name** field will automatically be populated with the case name followed by the name of the organization that is transferring the case.



Transfer case

Name
Shoplifting at downtown mall - From Liberty City Police Department

Organization
Liberty City Police Department

Recipient user
marklopez@lcpd.gov

5 Click **Transfer case**.

After you have transferred a case:

- An email is automatically sent to the recipient, inviting them to view the transferred case details.
- You will receive an email notifying you when the case transfer is complete.

Related Topics

Defining security policies on page 63

Security policy definitions list on page 63

Inviting guests to view cases

To share a specific case with someone who does not have a Clearance account, without allowing them to search or view other cases, you can invite this person as a guest.

What you should know

A user can be either a guest or regular user. Guests cannot perform searches in the system and cannot access the **Configurations** menu. Regular users have full access but can only access the **Configurations** menu if they are part of the *Account Administrator* group.

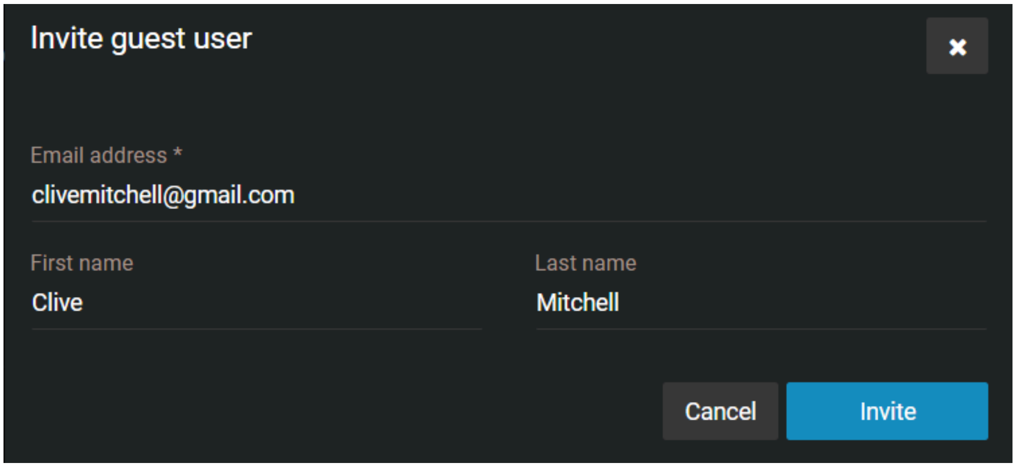
Procedure

1 Open an existing case or create a case.

2 If you are a regular user inviting a guest user, do the following:

a) In the *Permissions* section, click ⊕ > **Invite guest user** .

b) In the *Invite guest user* window, enter the email address and name of the person you want to invite, and click **Invite**.



Invite guest user

Email address *
clivemitchell@gmail.com

First name
Clive

Last name
Mitchell

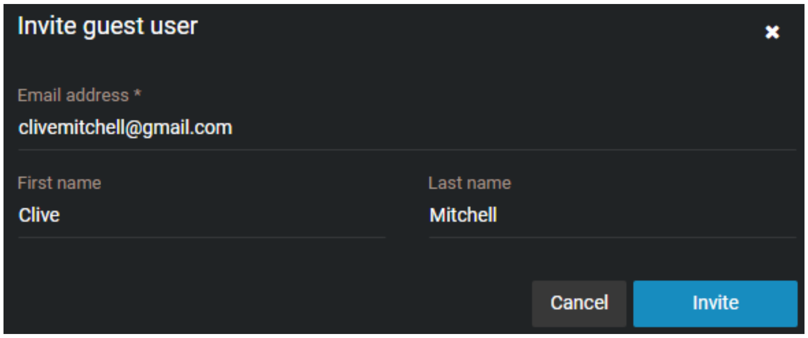
3 If you are a regular user inviting a guest user that has a Clearance account, do the following:

a) In the *Permissions* section, click ⊕ > **Invite guest user** .

b) In the *Invite guest user* window, enter the email address and name of the person you want to invite, and click **Invite**.

c) Select the users that you require from the list and click **Add**.

4 If you are a guest user inviting a guest user, do the following:
   a) In the *Permissions* section, click ⊕ > **Invite guest user** .
   b) Type the email address of the guest user that you want to share the case with.
   c) Click **Invite**.



Invite guest user

Email address *
clivemitchell@gmail.com

First name
Clive

Last name
Mitchell

   The person's email address is displayed in the *Permissions* section for the case, and an email inviting the user to join Clearance is automatically sent.

5 (Optional) Specify an expiration date for the guest user's access to the case.
   The default is **Never expires.**
   NOTE: You cannot specify an expiration date for a guest user with *Manage* permissions.
   a) Under the guest users name, click **Modify the expiration date** (✎).
   b) Clear the **Never** check box and enter an expiration date or use the calendar picker to choose a date.
   c) Click **Modify** to confirm the changes.

6 (Optional) If needed, modify the user's access permissions to the case, and then click **Save**.

An email is automatically sent to the user, inviting the user to view the case details. After activating their account and logging on to the system, the user will only have access to the case that they were invited to view.

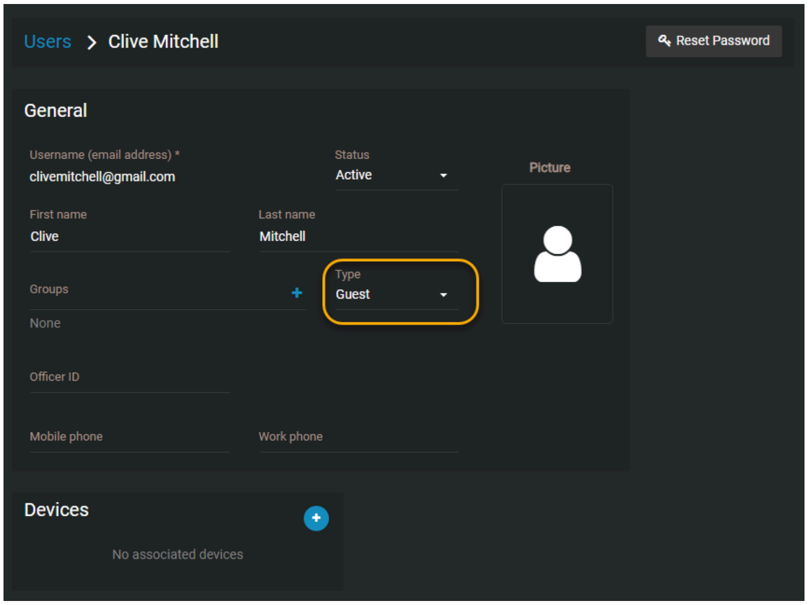
Example

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

When you invite a guest to view a case, the system automatically creates a user account for the guest, with the **Type** field set to **Guest**. From the **Configurations** menu, you can access the user account to edit all of the fields as needed.



Clive Mitchell

General

Username (email address) *
clivemitchell@gmail.com

Status
Active

First name
Clive

Last name
Mitchell

Groups
None

Type
Guest

Officer ID

Mobile phone

Work phone

No associated devices

Copying cases

If you do not want to include the original user permissions or files when sharing a case, you can copy the case and then add or remove permissions or files before sharing the modified case.

Before you begin

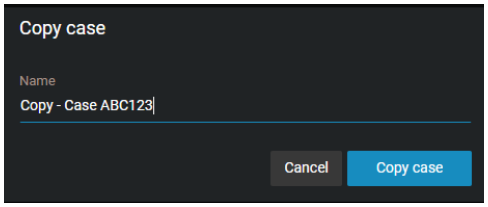
- To copy a case, you must have the *Manage* permission level for the case.

What you should know

- A guest user cannot copy a case.
- Creating a copy of a case consumes one case in the plan’s quota. The user that copied the case becomes the case owner.
- When a case is copied, no email notifications are sent, a unique case number is assigned, and duplicate case names are accepted.
- By default, all files, incident information, descriptions, and metadata from the original case are kept. Access policies and permissions for all users remain the same.
- Audit trail history from the original case is excluded from the copied case. The first audit trail entry (`CreateCopy`) in the copied case records who copied the original case.

Procedure

1. Open an existing case.
2. On the *Case* page title bar, click (⋮) to display additional case options.
3. Click **Copy case**.
   By default, copied cases are named Copy `- original case name`.

   Copy case

   Name
   Copy - Case ABC123

   a) (Optional) Enter a name for the copied case and click **Copy case** again to save the file.
4. Modify the copied case.
   a) (Optional) Add or remove user permissions.
   b) (Optional) Add or remove files.
   c) Click **Save**.

After you finish

You can now share the copied case or invite a guest user to view the copied case.

Changing access policies for cases

After a case has been created in the system, you can modify which users and groups have access to the case, and which permission levels they have.

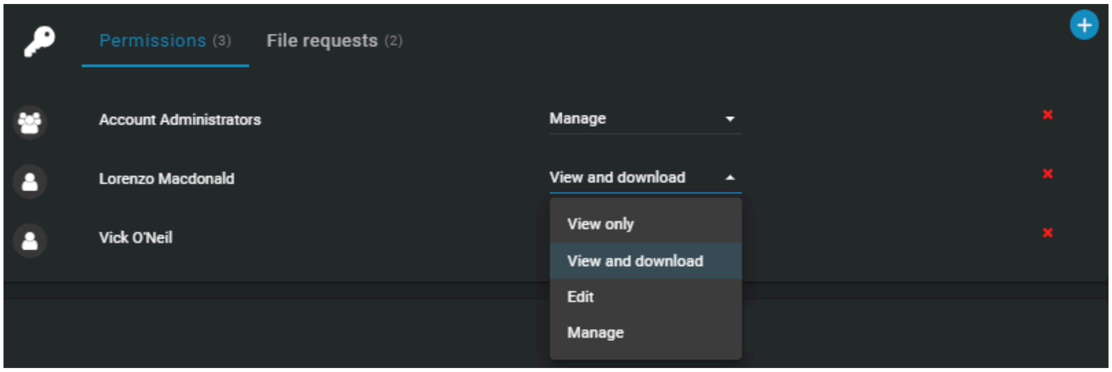
What you should know

You can only change the access policy of a case if you have the *Manage* permission level on that case.

Procedure

1 Open an existing case.

2 From the drop-down list next to a user or group in the **Permissions** section, grant them either the **View only**, **View and download**, **Edit**, or **Manage** permission level on the case.



Account Administrators	Manage
Lorenzo Macdonald	View and download
Vick O'Neil	

3 To remove a user or group from the case, click (✖) next to their name.

4 Click **Save**.

Example

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

▶

Related Topics

Viewing the audit trail history of cases on page 125
Viewing the audit trail history of files on page 191

Searching for cases or files

If you have many cases and files in the system, you can find a specific case or file from the **Search** page by using keyword searches, category, date and time filters, case status, case associations, device assignment filters, or by finding the case or file on a map.

What you should know

- Thumbnail previews are displayed in search results for the following files: BMP, PNG, JPEG, GIF, Icon, and MP4.
- When you select **Specific dates**, any cases or files that have at least 1 minute of their duration within the time range are displayed.

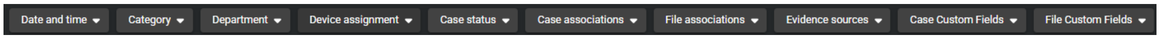
Procedure

1 Click the **Search** tab.

2 In the **Search** field, type keywords or tags related to the case or file, and press Enter or click the search button (🔍).

3 (Optional) Filter your search for cases or files: select either **Cases**, **Files**, or both.

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

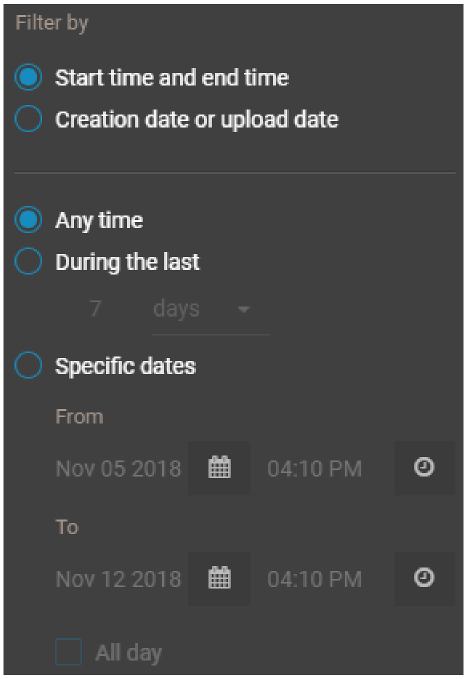


TIP: Click on the name of a column to sort it in ascending or descending order.

5 (Optional) Filter your search by category: click **Category** and select one or multiple categories from the drop-down menu.

TIP: Select **Clear all** to show all categories in the search results.

6 (Optional) Filter your search by date or time: click **Date and time** and select the options that you require.



Filter by

● Start time and end time

○ Creation date or upload date

● Any time

○ During the last

7 days

○ Specific dates

From

Nov 05 2018 04:10 PM

To

Nov 12 2018 04:10 PM

□ All day

- Select **Any time** to search all time ranges.
- Select **Specific dates** to search a specific time range. Enter a date and time, or use the calendar and date icons to select a specific time range.
- Select **All day** to search from 12:00 am to 11:59 pm for the selected days.

7 (Optional) Filter your search by case status:

a) Click **Case status**.

b) Select **Open**, **Closed**, or both.

c) Select **Clear all** when you want to show all open and closed cases in the search results.

8 (Optional) Filter your search by case associations: click **Case associations** and select **With files**, **Without files**, or both.

9 (Optional) Filter your search by file associations: click **File associations** and select **Linked**, **Unlinked**, or both.

10 (Optional) Filter your search by device assignment.

a) Click **Device assignment** and select the options that you require.

b) In the **Search** field, type a user name or email address, and press Enter or click the **Search** button (🔍).

c) Select the user that you require and click **Confirm**.

11 (Optional) Click **Case custom fields** or **File custom fields**, select a field, and enter a value to filter your search using any custom field values you have created.

12 (Optional) Click **Settings** (⚙) to add or modify fields in your search.

TIP: You can drag and drop fields in the search bar to reorder them. The order of your search fields is saved to your browser and appears in the same order the next time you log in.

13 (Optional) Click **Clear** (🗑) to clear your selected fields.

14 (Optional) To export search results as a CSV file: click **Export**.

Further analysis can be performed directly in Excel. For example, analyzing the number of cases or files created on a monthly basis, or the type and nature of events.

The metadata of all the queried files and cases is downloaded and generated in a CSV.

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

Click a case or file thumbnail to open it.

Searching for cases or files using map view

You can find a specific case or file from the **Map** view by using keyword searches and filters for category, date and time, case status, case associations, or device assignment.

What you should know

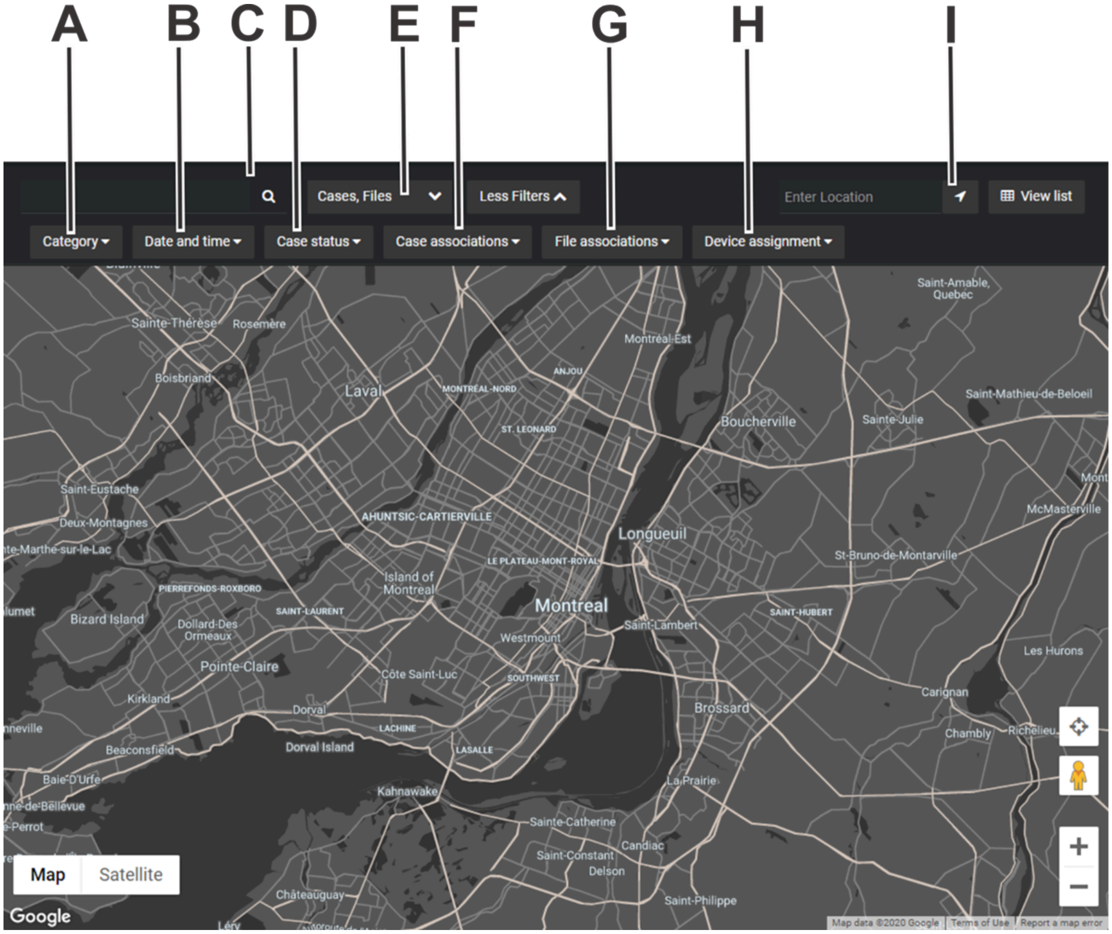
- Thumbnail previews are displayed in search results for the following files: BMP, PNG, JPEG, GIF, Icon, and MP4.
- When you select **Specific dates**, any cases or files that have at least 1 minute of their duration within the time range are displayed.

Procedure

1 Click the **Search** tab, and then click **View map** (🗺).

2 Search for the case or file on the map using one or more of the following filters.

- **A:** (Optional) Filter your search by category: click **Category** and select one or multiple categories from the drop-down menu.
- **B:** (Optional) Filter your search by date or time: click **Date and time** and select the options that you require.
- **C:** In the **Search** field, type keywords or tags related to the case or file, and then press **Enter** or click the **search** button (🔍).
- **D:** (Optional) Filter your search by case status:
- **E:** (Optional) Filter your search for cases, files, or cameras: select **Cases**, **Files**, **Cameras**, or a combination of the three options.
- **F:** (Optional) Filter your search by case associations: click **Case associations** and select **With files**, **Without files**, or both.
- **G:** (Optional) Filter your search by file associations: click **File associations** and select **Linked**, **Unlinked**, or both.
- **H:** (Optional) Filter your search by device assignment.
- **I:** If you know the location of the case or file, type the address, city, street, building name, and so on, in the location bar.



The cases or files that match your search criteria are shown on the map. If you search by location, the map centers on that location. Depending on the zoom level of the map, cases or files that are close together are grouped in bubbles.

3 Click a bubble to open the case or file, or to zoom in to the group of cases or files.

4 Click **View List** to display the search results in a list.

- Click **Show only results from the map search** to only display results found in the map search.
- Click **Show all results** to see all cases or files.

Example

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

▶

Searching for files or folders in a case

You can find specific files or folders from the *List* or *Tiles* view by using keyword searches, file type filters, and sort filters.

What you should know

- Thumbnail previews are displayed in search results for the following files: BMP, PNG, JPEG, GIF, Icon, and MP4.
- When you select **Specific dates**, any cases or files that have at least 1 minute of their duration within the time range are displayed.

Procedure

1 Open an existing case.

2 Click either the **List** (☰) or **Tiles** (▦) view.

3 In the search field (🔍), enter your search criteria to search the whole case and highlight results.

The search criteria can include the file name, extension, folder, or subfolder. The results displayed vary by relevance score and also fuzzy search results.

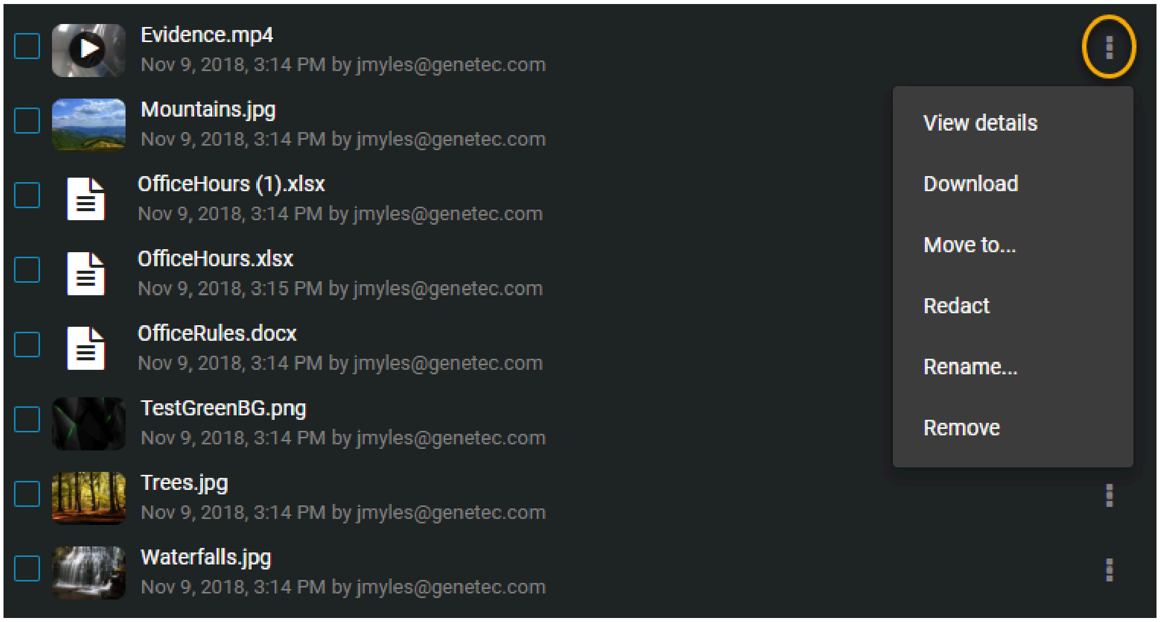
4 Select a filter from the **All files** list:

- **Audio**
- **Documents**
- **Images**
- **Videos**
- **Folders**
- **All files** (default)

5 Select a sort filter from the **Relevance** list:

- **Name** (default)
- **Type**
- **Start time**
- **Uploaded time**
- **Uploaded by**

6 (Optional) Click **More** (⋮) next to a file or folder to perform additional options.



□ Evidence.mp4
Nov 9, 2018, 3:14 PM by jmyles@genetec.com

□ Mountains.jpg
Nov 9, 2018, 3:14 PM by jmyles@genetec.com

□ OfficeHours (1).xlsx
Nov 9, 2018, 3:14 PM by jmyles@genetec.com

□ OfficeHours.xlsx
Nov 9, 2018, 3:15 PM by jmyles@genetec.com

□ OfficeRules.docx
Nov 9, 2018, 3:14 PM by jmyles@genetec.com

□ TestGreenBG.png
Nov 9, 2018, 3:14 PM by jmyles@genetec.com

□ Trees.jpg
Nov 9, 2018, 3:14 PM by jmyles@genetec.com

□ Waterfalls.jpg
Nov 9, 2018, 3:14 PM by jmyles@genetec.com

Previewing evidence in cases

If you have many files in a case, you can quickly navigate and preview all of the files by using the *Evidence preview* window.

What you should know

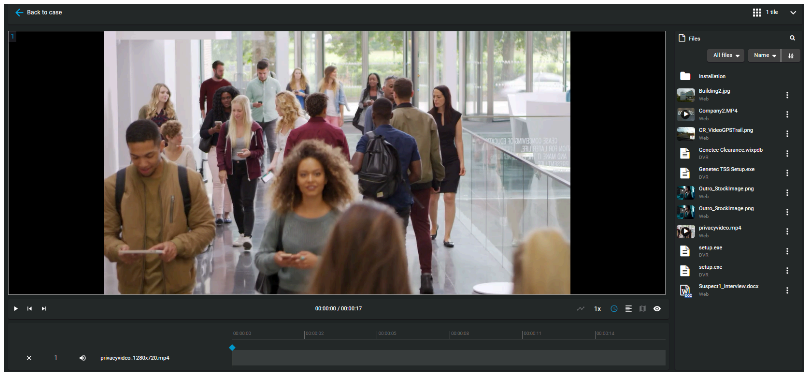
The *Evidence preview* window is used to quickly navigate many evidence files:

- Evidence image files and videos are displayed as thumbnails in the **Files** list in the *Evidence preview* window, so that you can quickly find the evidence that you need. Click a file to open a preview of the evidence in the **Preview** pane to the left of the **Files** list.
- The **View details** button opens the selected file in a new browser tab to keep the focus on the case.
- When a preview is not available for a file, a generic file icon and a download link are displayed.

Procedure

1 Open an existing case and click any file in the *Files* section.

The *Evidence preview* window opens if there are two or more files in the case.



2 To sort the evidence **Files** list, click **Sort by** and select the filter that you require:

- **Uploaded time:** Sorts the evidence preview list results based on the file upload time. Click the ascending or descending arrow to change the **Upload time** sort order.
- **Start time:** Sorts the evidence preview list results based on the file start time. Click the ascending or descending arrow to change the **Start time** sort order.
- **File name:** Sorts the evidence preview list results based on the file name. Click the ascending or descending arrow to change the **File name** alphabetical sort order.
- **File type:** Sorts the evidence preview list results based on the file type. Click the ascending or descending arrow to change the **File type** alphabetical sort order.
- **Uploaded by:** Sorts the evidence preview list results based on who uploaded the files. Click the ascending or descending arrow to change the **Uploaded by** alphabetical sort order.

3 Use the **Scroll bar** to quickly navigate the evidence preview list results.

4 Click a file in the **Files** list to preview the file in the **Preview** pane.

5 Click **View details** to open the file details in a new browser tab, while keeping the focus on the case.

After you finish

- Click **Download** if you want to download a copy of a file.
- Click **Edit** if you want to trim or redact a video file.

Reopening cases

If a case was closed in the system, but it must be re-activated to add more evidence or information, you can reopen the case.

What you should know

After a case is closed, only users or groups that have the *Manage* permission level for the case can reopen the case.

Procedure

1 Search for the case you want to reopen, and select the case.

2 In the case page, click **Reopen case**.

Example

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

▶

Protecting cases from deletion

To keep cases longer than the specified retention policy, you can place an indefinite hold on a case by using the **Protect from deletion** option.

What you should know

- Users must have *manage* permission to protect cases. Protected cases remain in the system, are not deleted, and are unaffected by retention policies.
- Users must also be included in the *Protect or unprotect cases and files from deletion* security policies list. If there are no users on that list, then all users with *manage* permissions have the ability to protect or unprotect cases and files.

Procedure

1. From either the *Search* or *Home* page, open a case.
2. Click to select the case that you want to protect.
3. In the *General* section of the *Case edit* page, select the **Protect from deletion** check box.

The case is now protected from manual deletion by a user or automatic deletion by any retention policies that are in effect.

Deleting cases

To remove the details of an incident and any digital evidence that is linked to the incident, you can delete a case and its associated files.

What you should know

You can manually delete a case or file even when there is a *retention policy* active for the case category. The retention period for the case begins to count down when the case is closed and deletes associated files automatically after the retention period (count down) is reached.

NOTE: Files that have been marked as Protected will not automatically be deleted by the retention policy.

IMPORTANT: You must be included in the **Delete cases and files** security policy to delete a case. Users must also have *manage* permission level for a case to delete it.

Procedure

1 Open an existing case.

2 Click the **Close case**.

3 Click **More**(⋮).

4 Click **Delete case**.

A confirmation message is displayed: Are you sure you want to delete this case? *Case name*.

5 (Optional) Select **Delete all files attached to this case that are not attached to any other case** and then select one of the following:

a) Click **Delete case and files** when you want to delete a case and all the files that are associated with that case.

b) Click **Delete case only** when you want to keep the files that are associated with the case.

6 (Optional) If a case is protected, the **Delete case** option is unavailable and a warning message is displayed. This case is protected from deletion. You must clear the Protect from deletion check box to delete this case.

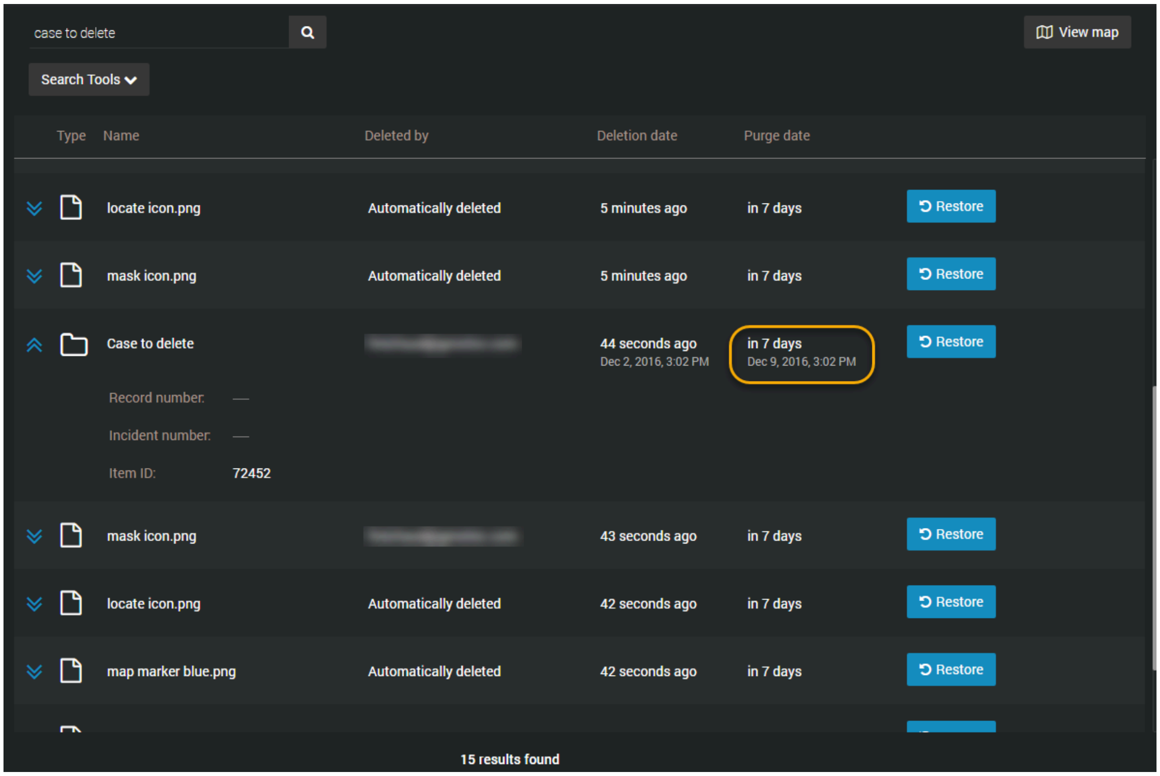
a) Clear the **Protect from deletion** check box.

b) Click **Delete**.

The delete status is displayed. After the case is deleted, you are automatically redirected to the case homepage.

The deleted case is marked for deletion and put in the recycle bin.

Example



Type	Name	Deleted by	Deletion date	Purge date	
	locate icon.png	Automatically deleted	5 minutes ago	in 7 days	Restore
	mask icon.png	Automatically deleted	5 minutes ago	in 7 days	Restore
	Case to delete	[redacted]	44 seconds ago Dec 2, 2016, 3:02 PM	in 7 days Dec 9, 2016, 3:02 PM	Restore
	mask icon.png	[redacted]	43 seconds ago	in 7 days	Restore
	locate icon.png	Automatically deleted	42 seconds ago	in 7 days	Restore
	map marker blue.png	Automatically deleted	42 seconds ago	in 7 days	Restore

Record number: —

Incident number: —

Item ID: 72452

15 results found

After you finish

You can view or search in the recycle bin to understand when the case and any associated files will be purged from the recycle bin. You can also view all active retention policies. When the purge occurs, the case and any associated files are permanently deleted from the Clearance database.

Related Topics

Setting the retention period for cases and files on page 40
Viewing the audit trail history of cases on page 125

Restoring cases

To restore the details of an incident and any digital evidence that is linked to the incident, you can restore a case and its associated files.

What you should know

IMPORTANT: Users must be in the **Restore cases and files from the recycle bin** security policy list. Users must also have *manage* permission level to restore cases. If the list is empty everyone can restore.

Procedure

1 Open the recycle bin.

2 Select the case that you want and click **Restore**.

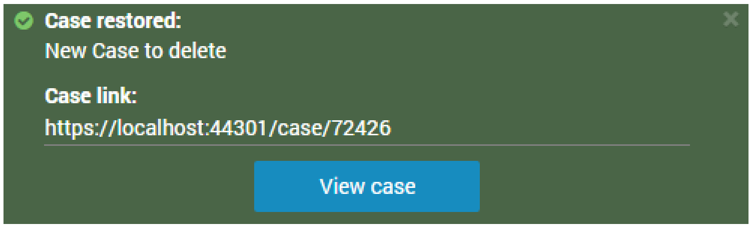
A confirmation message is displayed.

Are you sure you want to restore this case? *Case name*

NOTE: Any restored cases are automatically set to **Protect from deletion**.

3 Click **Restore case**.

When the case is restored, a case restored message is displayed and a Case link web address is also shown.



Case restored:
New Case to delete

Case link:
https://localhost:44301/case/72426

4 (Optional) Click **View case** to open the restored case.

Related Topics

Viewing the audit trail history of cases on page 125

Viewing the audit trail history of cases

You can investigate the complete activity history of a case, such as who made changes and when, by viewing the audit trail of the case.

Before you begin

To view the audit trail of a case, you must have the *Manage* permission level on the case. Audit trail information is never displayed to guest users with *Manage* permission level.

What you should know

The audit trail of a case tracks users who created, viewed, edited, protected, deleted, restored, or copied the case, and when these actions were performed.

Procedure

To view the audit trail history of a case:

1. Open an existing case.
2. Click **More** (⋮).
3. Click **Audit trail**.
4. View the case history.

To download the audit trail report:

1. From the *Audit trail* page, click **Create audit trail report**.
2. Review the report and click **Download**.

Example

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

▶

Related Topics

About Clearance information security on page 164

Deleting cases on page 122

Restoring cases on page 124

Changing access policies for cases on page 112

About closed cases

The purpose of closing a case in Genetec Clearance™ is to limit further modifications to a case that is no longer active and preserve it's contents for future reference. Once a case is closed, only users with *Manage* permissions will be able to modify the case.

- **CAUTION:** When you close a case, the case inherits the retention policy of the category it is associated with. This can put the case and associated files in danger of being unintentionally deleted. For more information see Setting the retention period for cases and files on page 40 and Creating incident categories on page 58.
- When a closed case is reopened, the scheduled deletion is changed back to *Never delete* if the file is not in the recycle bin.
- The date of the last modifications to a closed case are noted in the *Last modified* section.
- Closing and reopening cases affects the retention period for files. For example, when a closed case is reopened, the scheduled deletion for files associated with that case is changed back to NEVER DELETE if the file is not in the recycle bin.

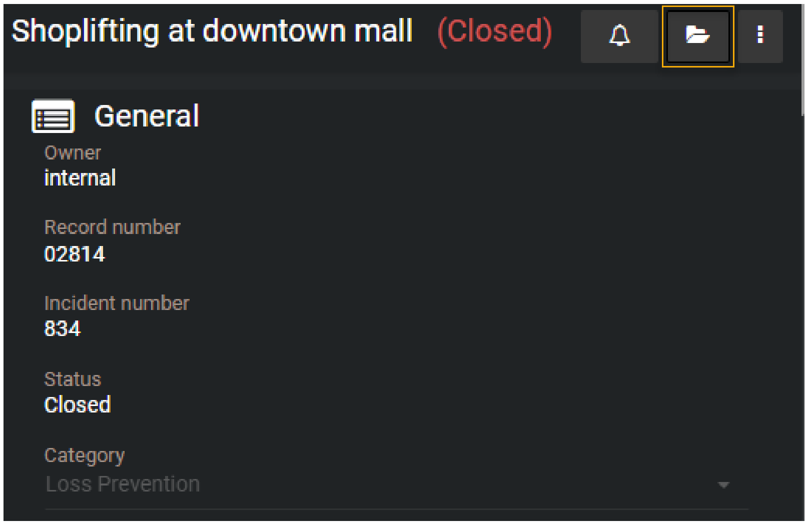
In a closed case for which you have *Manage* permissions you can:

- Subscribe to the case
- Reopen the case
- Delete the case
- View the audit trail of the case
- Create a summary report of the case
- Create an eDiscovery receipt of the case
- Depending on a user's permission level on a file, access, download, and filter through the list of files associated with the case

Adding files to a closed case:

To add files to a closed case, do the following:

1. Reopen the case



Shoplifting at downtown mall (Closed)

General

Owner
internal

Record number
02814

Incident number
834

Status
Closed

Category
Loss Prevention

2. Add the required files to the case

3. Close the case.

7

Managing devices

Add, remove, and configure devices in Clearance.

This section includes the following topics:

- "About device licenses" on page 129
- "Enrolling Axis and Reveal body-worn cameras" on page 136

About device licenses

Before you can use devices in Clearance you must activate licenses for your devices. Your devices can then be assigned to or revoked from users and also have their licenses deactivated.

Device groups conform to the following rules:

- The number of device licenses granted to your account depends on your level of subscription to Clearance.

See the following to manage device licenses:

1. Activate device licenses.
2. Assign devices to users.
3. Remove device assignments.
4. Deactivate device licenses.

Activating device licenses

Activate device licenses in Clearance so that the devices can be assigned to one or more users. To activate a device license, the device must be added in the system.

Before you begin

You must have an active license that supports the number of devices that you require.

What you should know

If you manage a large number of devices, consider defining a naming standard that suits your needs before changing device names. For example, include departments, location codes, or any other useful information in the name.

Procedure

1 Click **Configurations** > **Devices**.

On the *Device details* page the number of activated devices is displayed.

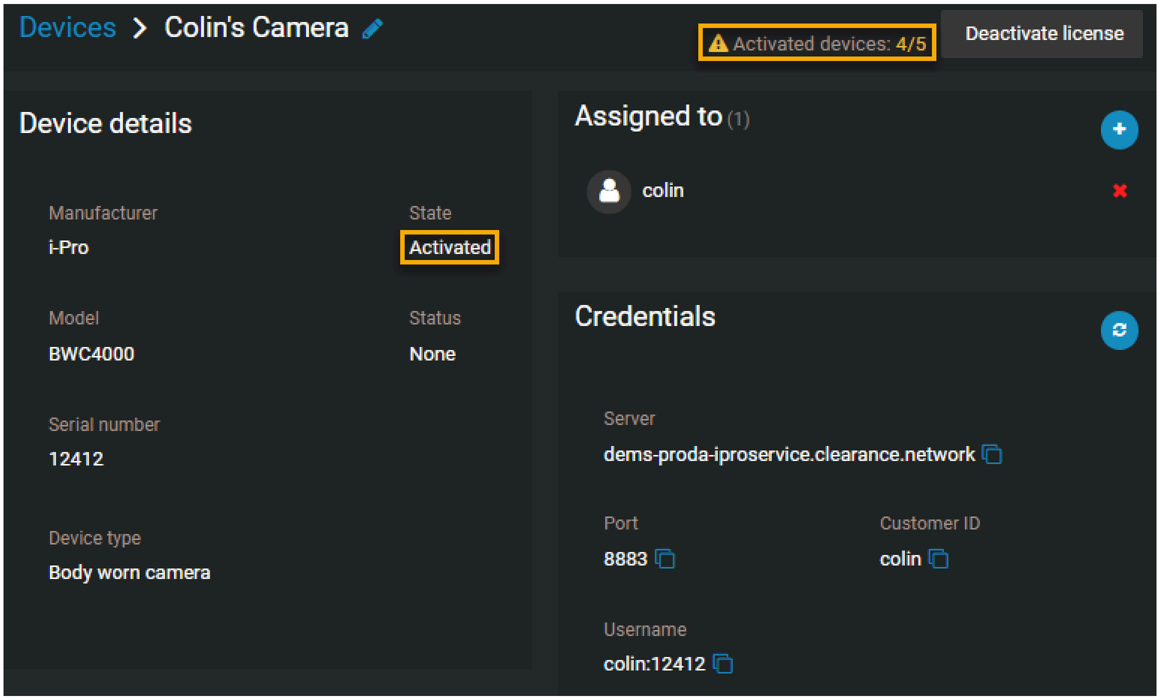
For example Activated devices: 1/15 indicates the number of devices that are active (1), followed by the number of device licenses that are available (15) as specified in your license.

2 Click the **device** that you want to activate a license for.

3 (Optional) Enter or modify the device name and click **Save**.

4 Check the **Activated devices** field to ensure that you have an available license for your device.

5 Click **Activate license**.



Device details

Manufacturer: i-Pro

State: Activated

Model: BWC4000

Status: None

Serial number: 12412

Device type: Body worn camera

Assigned to (1)

colin

Credentials

Server: dems-proda-iproservice.clearance.network

Port: 8883

Customer ID: colin

Username: colin:12412

The device license is now activated.

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

You can now assign the device to a user.

Related Topics

Installing the Clearance Uploader on page 266
Configuring the Clearance Uploader on page 268

Assigning devices to users

You can assign a device to one or more users so that all media recorded using the assigned device is tagged and searchable. You can then search for evidence by device assignment to find all media recorded by users that are associated with the device.

What you should know

To assign a device to a user, the device must exist in the system and the device license must be activated. You can assign a maximum of ten users to a device.

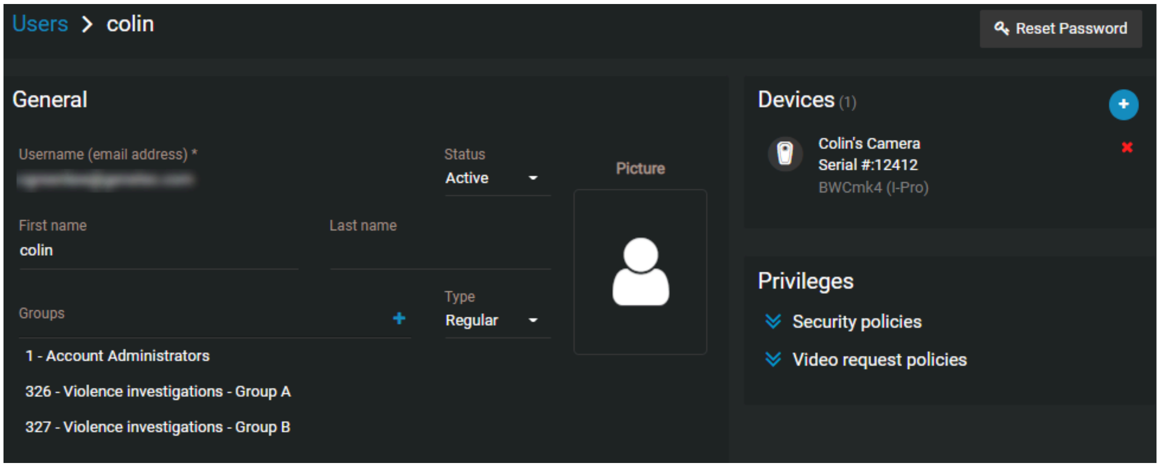
NOTE: When media is uploaded from an assigned device, the device assignment information is included in the *Device details* section of the *File edit* page. You can also view this information on the *User Edit* page.

Procedure

To assign a device to a user:

1. Click **Configurations** > **Users**.
2. In the **Search** field, type a user name or email address, and press Enter or click the **Search** button (🔍).
3. Select the user that you require.
4. In the *Devices* section of the *Users* page, click ⊕.
5. In the *search* box, enter the device information (serial number, make, model), and press **Enter** or click the **search** button (🔍).

   NOTE: Only activated devices are displayed in the search results.
6. Select the device that you require and click **Add**.
7. Click **Save**.



Users > colin

Reset Password

General

Username (email address) *
[redacted]

Status
Active

Picture

First name
colin

Last name

Groups +

Type
Regular

1 - Account Administrators

326 - Violence investigations - Group A

327 - Violence investigations - Group B

Devices (1)

Colin's Camera
Serial #:12412
BWCmk4 (I-Pro)

Privileges

Security policies

Video request policies

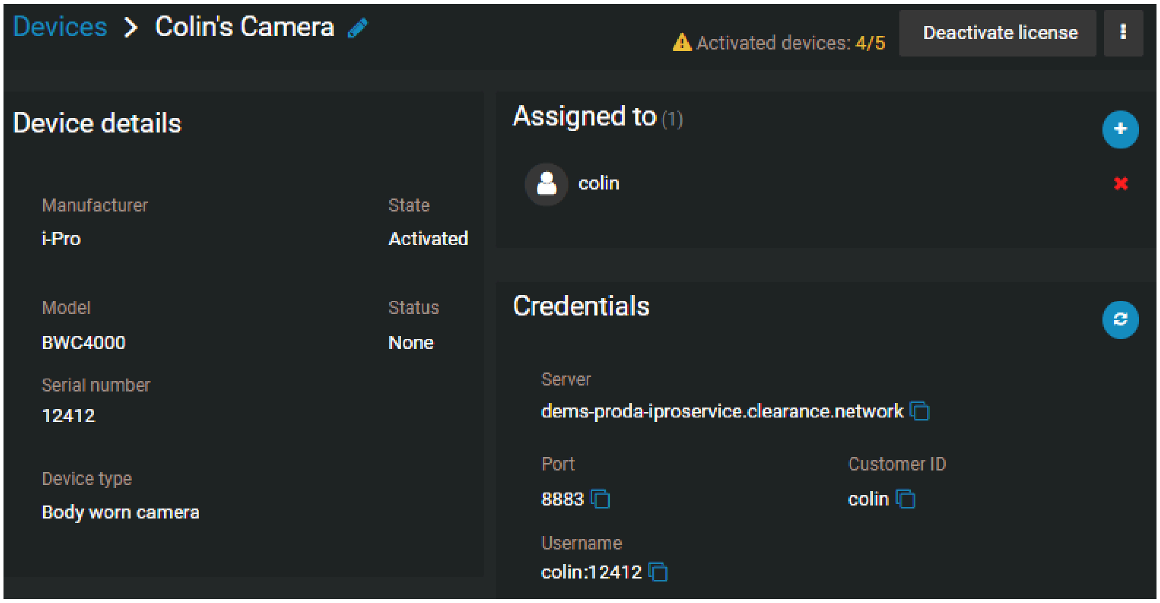
The device is now assigned to the user.

To assign a user to a device:

1. Click **Configurations** > **Devices**.
2. (Optional) In the *search* box, enter the device information (serial number, make, model), and press **Enter** or click the **search** button (🔍).

   NOTE: Only activated devices are displayed in the device search results.
3. Select the device that you require.
4. In the *Assigned to* section of the *Devices* page, click ⊕.
5. In the **Search** field, type a user name or email address, and press Enter or click the **Search** button (🔍).
6. Select the check box for the user that you require and click **Add**.

7 Click **Save**.



Devices > Colin's Camera

⚠ Activated devices: 4/5

Deactivate license

Device details

Manufacturer: i-Pro

State: Activated

Model: BWC4000

Status: None

Serial number: 12412

Device type: Body worn camera

Assigned to (1)

colin

Credentials

Server: dems-proda-iproservice.clearance.network

Port: 8883

Customer ID: colin

Username: colin:12412

The user is now assigned to the device.

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 remove a device assignment, reassign a device to another user, or deactivate a device.

Removing device assignments from users

You can remove device assignments from a user when the device assignment is no longer required.

What you should know

To remove a device assignment, the device must exist in Clearance and the device must be assigned to a user. You can either remove a device assignment from a user, or remove a user from a device.

Procedure

To remove a device assignment from a user:

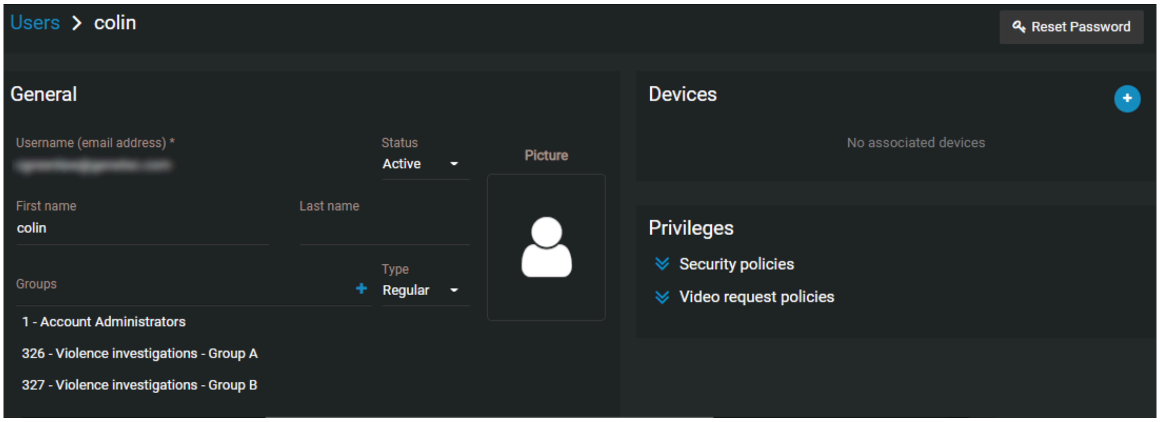
1 Click **Configurations** > **Users**.

2 In the **Search** field, type a user name or email address, and press Enter or click the **Search** button (🔍).

3 Click the **user** that you require.

4 In the *Devices* section of the *Users* page, click ✖ **delete** next to the device assignment that you want to remove.

5 Click **Save**.



Users > colin

Reset Password

General

Username (email address) *
[redacted]

Status
Active

Picture

First name
colin

Last name

Groups

Type
Regular

1 - Account Administrators

326 - Violence investigations - Group A

327 - Violence investigations - Group B

Devices

No associated devices

Privileges

Security policies

Video request policies

The device is no longer assigned to the user.

To remove a user from a device:

1 Click **Configurations** > **Devices**.

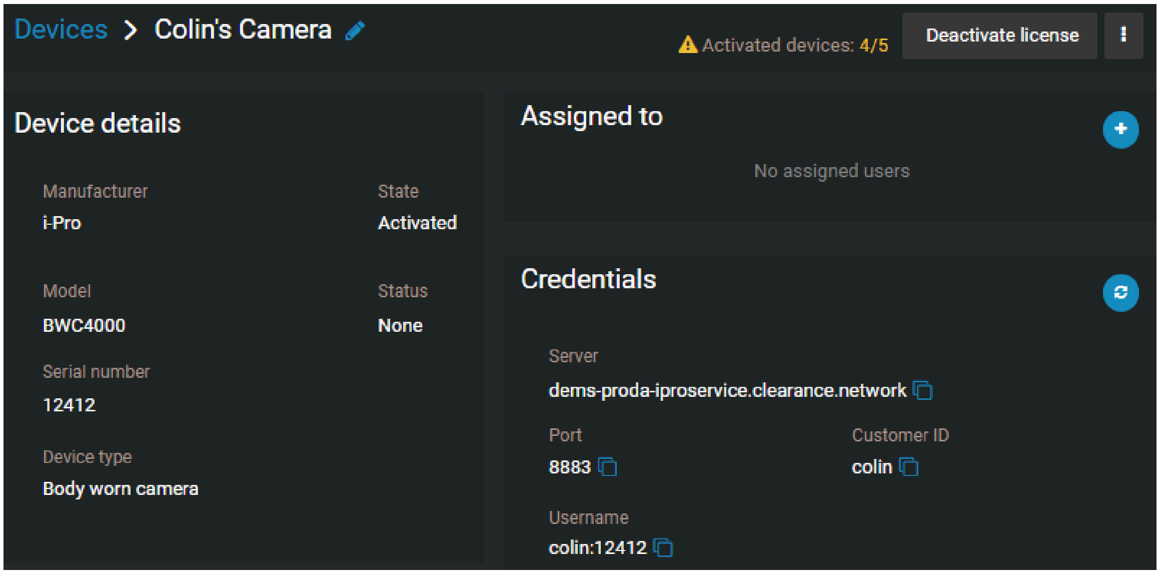
2 In the *search* box, enter the device information (serial number, make, model), and press **Enter** or click the **search** button (🔍).

NOTE: Only activated devices are displayed in the search results.

3 Click the **device** that you require.

4 In the *Assigned to* section of the *Devices* page, click ❌ **delete** next to the user that you want to remove.

5 Click **Save**.



Devices > Colin's Camera

⚠ Activated devices: 4/5

Deactivate license

Device details

Manufacturer
i-Pro

State
Activated

Model
BWC4000

Status
None

Serial number
12412

Device type
Body worn camera

Assigned to

No assigned users

Credentials

Server
dems-proda-iproservice.clearance.network

Port
8883

Customer ID
colin

Username
colin:12412

The user is no longer assigned to the device.

Example

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

▶

Deactivating device licenses

You can deactivate a device license to remove a device from use, to assign the license to a new device, or when a device breaks and requires servicing or replacement. Deactivating a license automatically removes assigned users from the device.

Before you begin

The device must be registered in Clearance and the device license must be activated.

The following prerequisites apply when deactivating licenses:

- You must have an active internet connection.
- You must be a member of the *Manage devices* security policy.
- The Clearance Uploader must be installed and associated with a Clearance account.

Procedure

1 Click **Configurations** > **Devices**.

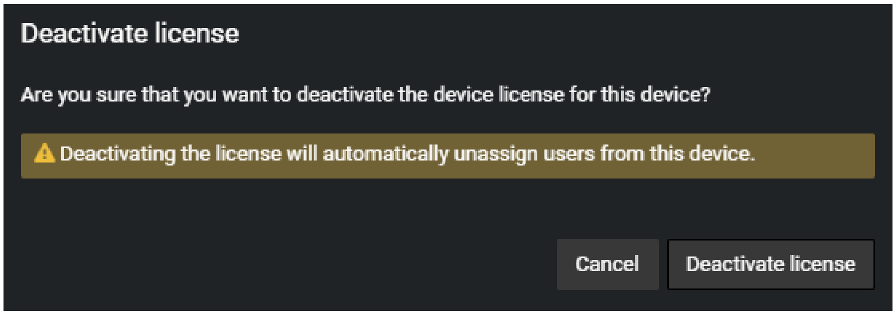
2 (Optional) In the *search* box, enter the device information, and press **Enter** or click the **search** button (🔍).

3 Click the **device** that you require.

On the *Device details* page the number of activated devices is displayed. For example Activated devices: 1/15 indicates the number of devices that are active (1) followed by the device licenses that are available (15) as specified in your license conditions.

4 Click **Deactivate license**.

A warning message is displayed as follows:



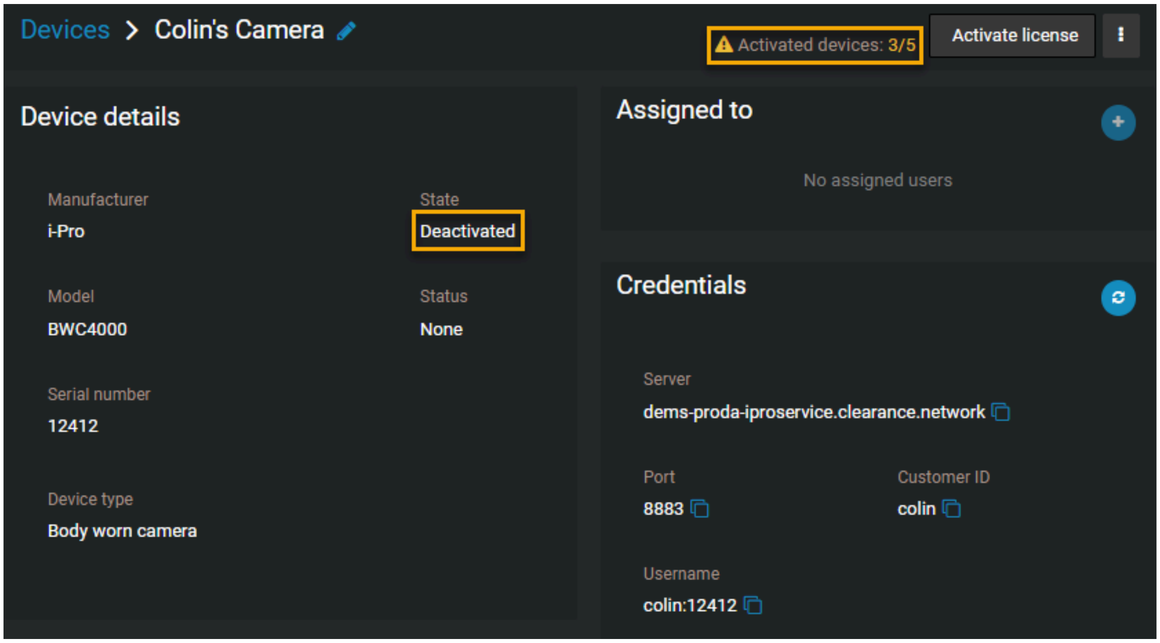
Deactivate license

Are you sure that you want to deactivate the device license for this device?

⚠ Deactivating the license will automatically unassign users from this device.

CAUTION: Deactivating a license automatically removes any assigned users from the device.

5 Click **Deactivate license** again to confirm the action.



The device license is deactivated and an additional device license is now available.

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

You can now activate this device license for a new device if required.

Enrolling Axis and Reveal body-worn cameras

You can add an Axis or Reveal body-worn camera in Clearance by docking the camera in a docking station connected to your system and authenticating it with Clearance.

Before you begin

The following prerequisites apply when registering devices:

- You must have an active internet connection.
- You must be a member of the *Manage devices* security policy.
- You must create an integration for your cameras.

What you should know

The first time that you dock a new camera, the camera is automatically detected.

Procedure

1. In your camera management tool, import the configuration file from the integration associated with the camera.
2. Dock the camera.
3. Click **Configurations** > **Devices** and refresh the Devices page.

   NOTE: The camera serial number is automatically imported as a unique identifier. If a camera was previously added, it is displayed as either Activated or Deactivated.

   Your camera is now in the system and displayed in the devices list with the state **New**.

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

You can now activate the device license.

Related Topics

Installing the Clearance Uploader on page 266

Configuring the Clearance Uploader on page 268

8

Managing i-PRO devices

Add, remove, and configure i-PRO devices in Clearance.

This section includes the following topics:

- "Adding i-PRO body-worn cameras" on page 138
- "Adding i-PRO in-car systems" on page 144
- "Configuring i-PRO five fields" on page 152
- "About i-PRO automatic case creation and file tagging" on page 154
- "About device groups" on page 155
- "Defining device policies" on page 159

Adding i-PRO body-worn cameras

You can add an i-PRO body-worn camera in Clearance by docking the camera in a docking station connected to your system and authenticating it with Clearance.

Before you begin

The following prerequisites apply when registering i-PRO body-worn cameras:

- You must have an active internet connection.
- You must be a member of the *Manage devices* security policy.

What you should know

The i-PRO body-worn camera must be authenticated before you can upload video from it.

Procedure

1. Adding i-PRO BWC MK3 body cameras.
2. Adding i-PRO BWC 4000 body-worn cameras on page 141.

Adding i-PRO BWC MK3 body-worn cameras

To add an i-PRO BWC MK3 body-worn camera in Clearance, dock it in a docking station connected to your system and authenticate it with Clearance.

Before you begin

The following prerequisites apply when registering i-PRO BWC MK3 body-worn cameras:

- You must have an active internet connection.
- You must be a member of the *Manage devices* security policy.

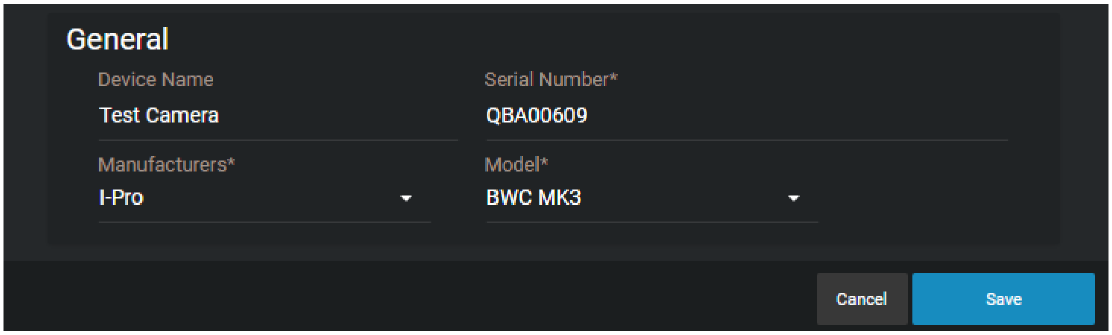
What you should know

The i-PRO BWC MK3 must be authenticated before you can upload video from it.

Procedure

1. Dock the body-worn camera.
2. Click **Configurations** > **Devices**.
3. Click **Create new device**.

4. Enter a name for the BWC MK3, the camera serial number, and specify the manufacturer and model of the camera.



General

Device Name: Test Camera

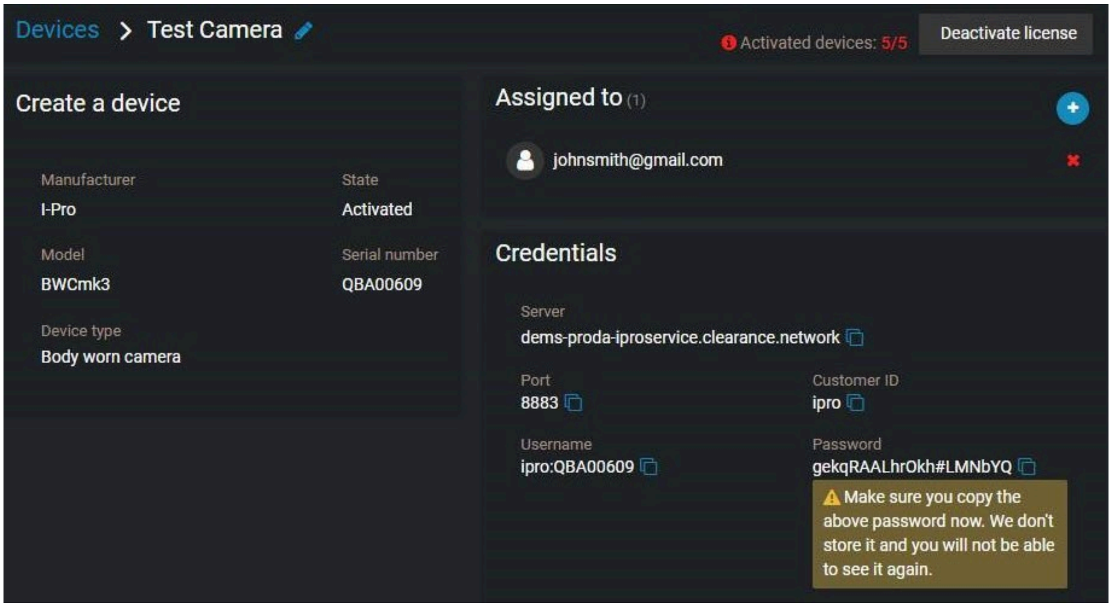
Serial Number*: QBA00609

Manufacturers*: I-Pro

Model*: BWC MK3

5. Click **Save**.

   The body-worn camera is created in Clearance.



Devices > Test Camera

Activated devices: 5/5

Create a device

Manufacturer: I-Pro

State: Activated

Model: BWCmk3

Serial number: QBA00609

Device type: Body worn camera

Assigned to (1)

johnsmith@gmail.com

Credentials

Server: dems-proda-iproservice.clearance.network

Port: 8883

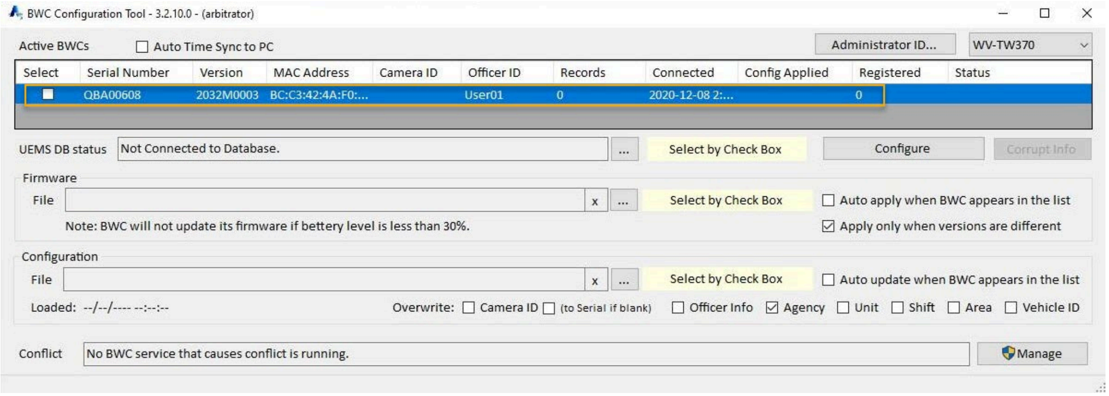
Customer ID: ipro

Username: ipro:QBA00609

Password: gekqRAALhrOkh#LMNbYQ

Make sure you copy the above password now. We don't store it and you will not be able to see it again.

6. From the *BWC Config Tool* window, double click on the body-worn camera you want to activate.



BWC Configuration Tool - 3.2.10.0 - (arbitrator)

Active BWCs ☐ Auto Time Sync to PC

Administrator ID... WV-TW370

Select	Serial Number	Version	MAC Address	Camera ID	Officer ID	Records	Connected	Config Applied	Registered	Status
☐	QBA00608	2032M0003	BC:C3:42:4A:F0:...		User01	0	2020-12-08 2:...		0	

UEMS DB status: Not Connected to Database.

Firmware

File

☐ Auto apply when BWC appears in the list

Note: BWC will not update its firmware if bettery level is less than 30%.

☑ Apply only when versions are different

Configuration

File

☐ Auto update when BWC appears in the list

Loaded: --/--/---- --:--:--

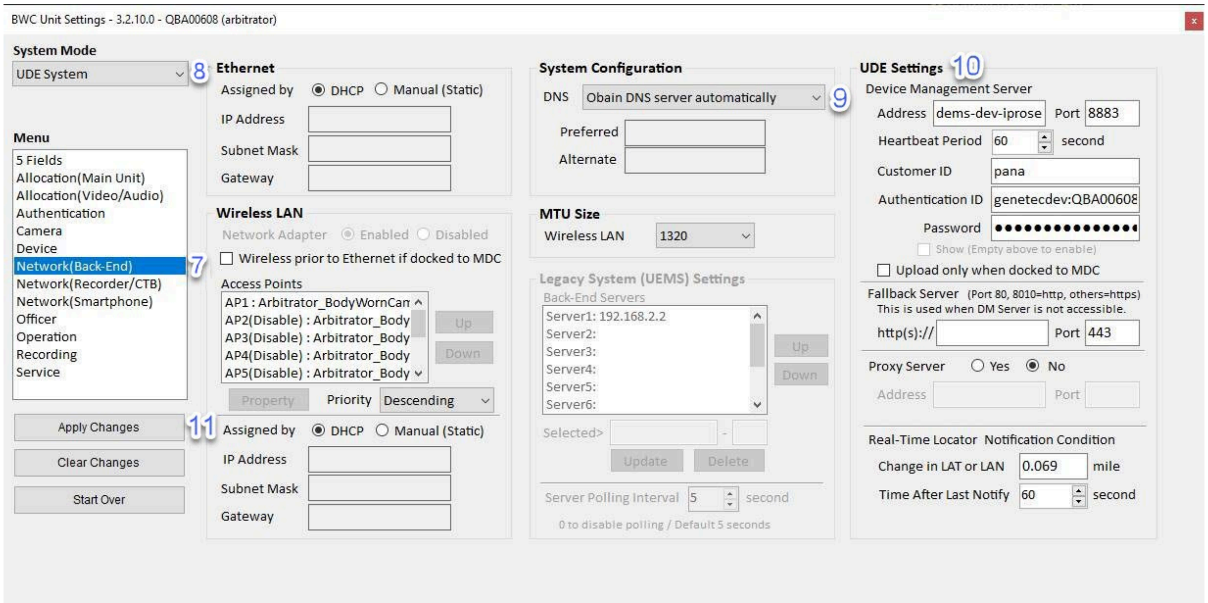
Overwrite: ☐ Camera ID ☐ (to Serial if blank) ☐ Officer Info ☑ Agency ☐ Unit ☐ Shift ☐ Area ☐ Vehicle ID

Conflict: No BWC service that causes conflict is running.

7. In the **Menu** section, select **Network (Back-End)**.
8. Set the **System mode** to **UDE System**.

9 Set the **System Configuration** to **Obtain DNS server automatically**.

NOTE: If this option is not available, you must enter your preferred DNS server manually.



BWC Unit Settings - 3.2.10.0 - QBA00608 (arbitrator)

System Mode: UDE System 8

Menu: 5 Fields, Allocation(Main Unit), Allocation(Video/Audio), Authentication, Camera, Device, Network(Back-End) 7, Network(Recorder/CTB), Network(Smartphone), Officer, Operation, Recording, Service

Apply Changes 11 | Clear Changes | Start Over

Ethernet — Assigned by: ● DHCP ○ Manual (Static); IP Address; Subnet Mask; Gateway

Wireless LAN — Network Adapter: ● Enabled ○ Disabled; □ Wireless prior to Ethernet if docked to MDC

Access Points:
AP1 : Arbitrator_BodyWornCam
AP2(Disable) : Arbitrator_Body
AP3(Disable) : Arbitrator_Body
AP4(Disable) : Arbitrator_Body
AP5(Disable) : Arbitrator_Body

Property | Priority: Descending

Assigned by: ● DHCP ○ Manual (Static); IP Address; Subnet Mask; Gateway

System Configuration — DNS: Obain DNS server automatically 9; Preferred; Alternate

MTU Size — Wireless LAN: 1320

Legacy System (UEMS) Settings — Back-End Servers: Server1: 192.168.2.2, Server2:, Server3:, Server4:, Server5:, Server6:; Selected>; Update | Delete; Server Polling Interval: 5 second; 0 to disable polling / Default 5 seconds

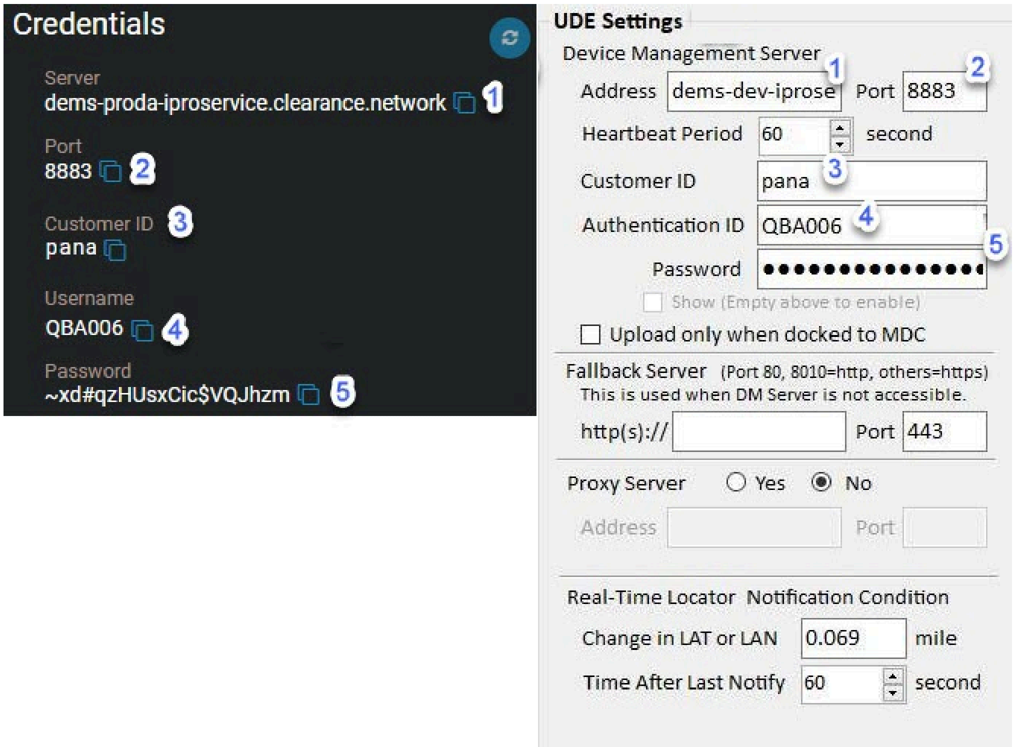
UDE Settings 10 — Device Management Server: Address: dems-dev-iprose, Port: 8883; Heartbeat Period: 60 second; Customer ID: pana; Authentication ID: genetecdev:QBA00608; Password: ●●●●●●●●●●●●●●●; □ Show (Empty above to enable); □ Upload only when docked to MDC

Fallback Server (Port 80, 8010=http, others=https) This is used when DM Server is not accessible. http(s):// Port 443

Proxy Server: ○ Yes ● No; Address; Port

Real-Time Locator Notification Condition — Change in LAT or LAN: 0.069 mile; Time After Last Notify: 60 second

10 From the *Devices* page in Clearance, copy the credentials and paste them in the **UDE Settings** section of your body-worn camera configuration tool window.



Credentials

Server: dems-proda-iproservice.clearance.network 1

Port: 8883 2

Customer ID 3: pana

Username: QBA006 4

Password: ~xd#qzHUsxCic$VQJhzm 5

UDE Settings

Device Management Server — Address: dems-dev-iprose 1; Port: 8883 2

Heartbeat Period: 60 second

Customer ID: pana 3

Authentication ID: QBA006 4

Password: ●●●●●●●●●●●●●●● 5

□ Show (Empty above to enable)

□ Upload only when docked to MDC

Fallback Server (Port 80, 8010=http, others=https) This is used when DM Server is not accessible. http(s):// Port 443

Proxy Server: ○ Yes ● No; Address; Port

Real-Time Locator Notification Condition — Change in LAT or LAN: 0.069 mile; Time After Last Notify: 60 second

11 In the body-worn camera configuration tool window, click **Apply changes**.

12 Click **Activate device**.

13 From the *Devices* page in Clearance, select the relevant device and assign the body-worn camera to a user.

14 (Optional) In the **Device group** field, select a group to include the device in.

NOTE: Device groups are used to manage the firmware version for groups of devices.

15 Click **Save**.

The i-PRO BWC MK3 body-worn camera can now upload recorded video to Clearance.

Related Topics

Configuring i-PRO five fields on page 152

Adding i-PRO BWC 4000 body-worn cameras

Before you can upload video to Clearance with an i-PRO BWC 4000, you must add the i-PRO BWC 4000 in Clearance by docking the camera in a docking station connected to your system, configuring the camera, and authenticating it with Clearance.

Before you begin

The following prerequisites apply when registering i-PRO body-worn cameras:

- You must have an active internet connection.
- You must be a member of the *Manage devices* security policy.

What you should know

- The i-PRO BWC 4000 body-worn camera should have no previously existing configurations when you make these configurations.
- The i-PRO BWC 4000 body-worn camera must be authenticated before you can upload video from it.

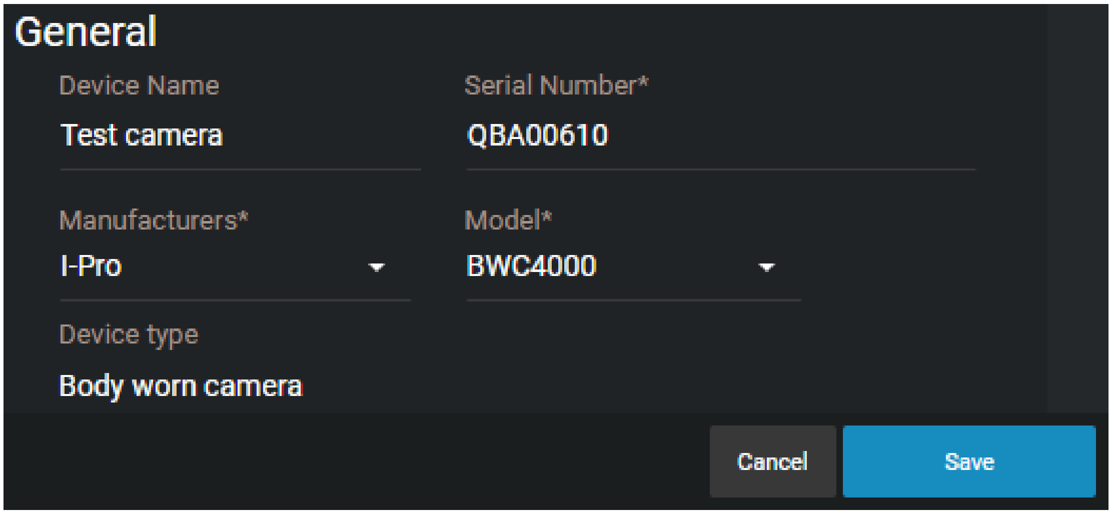
Procedure

1 Dock the camera.

2 Click **Configurations** > **Devices**.

3 Click **Create new device**.

4 Enter a name for the camera, its serial number, and specify the manufacturer and model.



General

Device Name: Test camera

Serial Number*: QBA00610

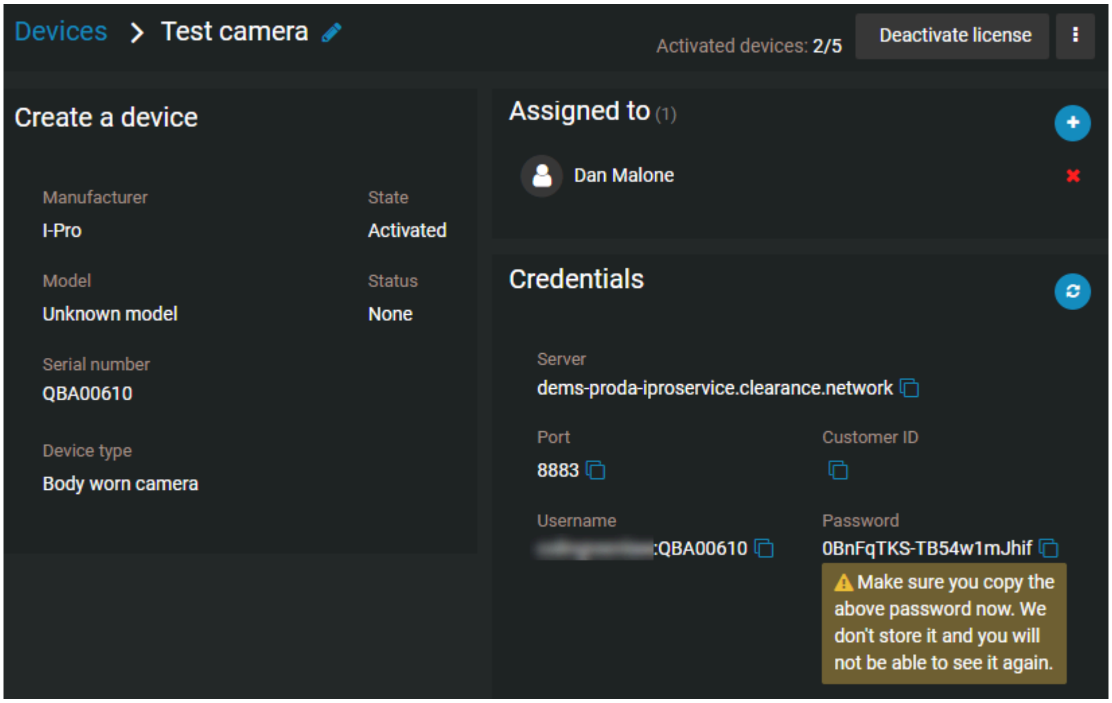
Manufacturers*: I-Pro

Model*: BWC4000

Device type: Body worn camera

5 Click **Save**.

The body-worn camera is created.



Devices > Test camera

Activated devices: 2/5

Create a device

Manufacturer: I-Pro

State: Activated

Model: Unknown model

Status: None

Serial number: QBA00610

Device type: Body worn camera

Assigned to (1)

Dan Malone

Credentials

Server: dems-proda-iproservice.clearance.network

Port: 8883

Customer ID:

Username: [redacted]:QBA00610

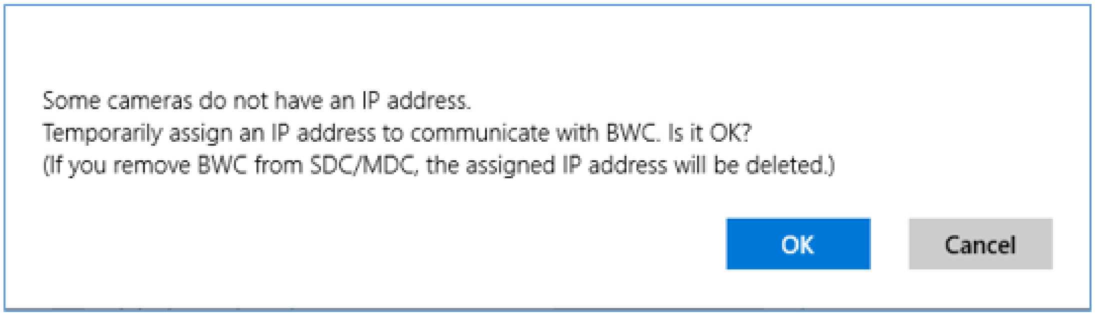
Password: 0BnFqTKS-TB54w1mJhif

⚠ Make sure you copy the above password now. We don't store it and you will not be able to see it again.

6 Log into the BWC 4000 configuration tool.

7 From the *BWC Config Tool* window, click **Detect** (⟳).

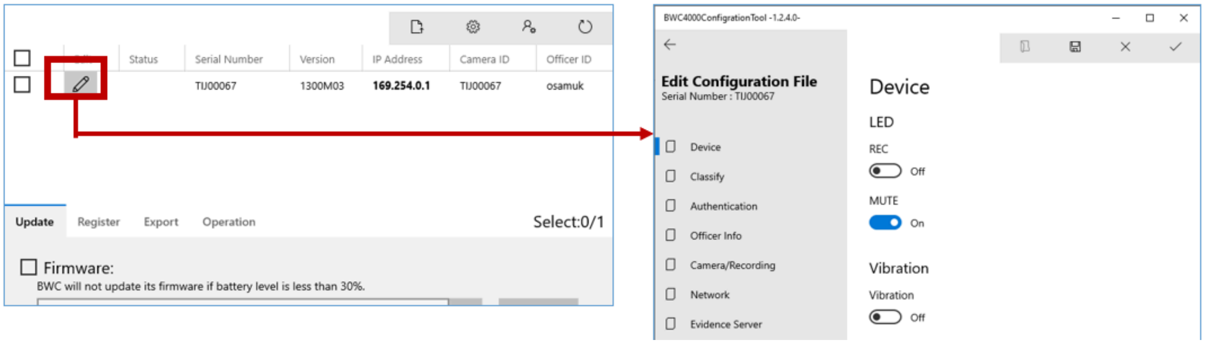
⚠ **Trouble:** If the BWC 4000 is not detected, contact your IT team for support on assigning temporary IP addresses.



Some cameras do not have an IP address.
Temporarily assign an IP address to communicate with BWC. Is it OK?
(If you remove BWC from SDC/MDC, the assigned IP address will be deleted.)

8 Click **Edit** (🖉).

The *BWC 4000 Configuration Tool* window opens.



		Status	Serial Number	Version	IP Address	Camera ID	Officer ID
□	🖉		TIJ00067	1300M03	**169.254.0.1**	TIJ00067	osamuk

□ Firmware:
BWC will not update its firmware if battery level is less than 30%.

BWC4000ConfigurationTool -1.2.4.0-

Edit Configuration File
Serial Number : TIJ00067

Device

LED

REC: Off

MUTE: On

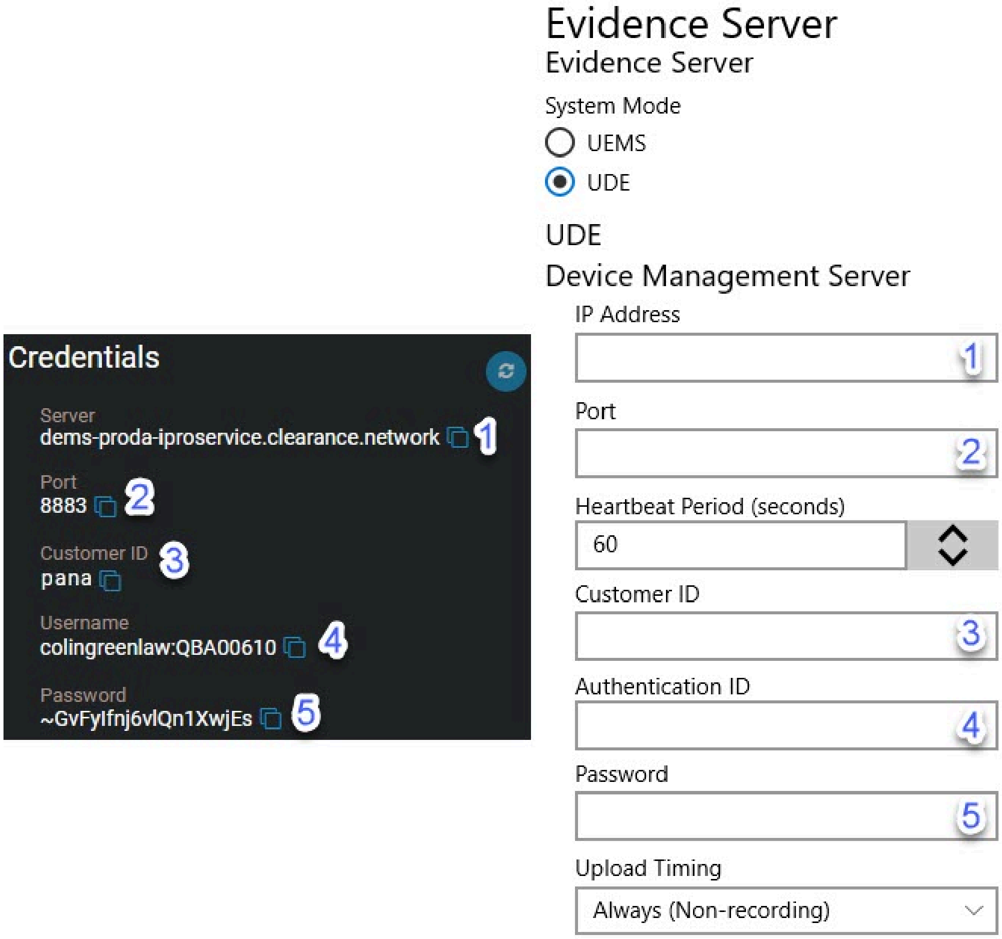
Vibration

Vibration: Off

9 From the *Edit configuration file* window, click the **Evidence server** tab.

10 In the *System Mode* section, select **UDE**.

11 In the *Device Management Server* section, enter the information you copied from the **Credentials** section.



Credentials

Server
dems-proda-iproservice.clearance.network

Port
8883

Customer ID
pana

Username
colingreenlaw:QBA00610

Password
~GvFylfnj6vlQn1XwjEs

Evidence Server

Evidence Server

System Mode

○ UEMS

● UDE

UDE

Device Management Server

IP Address

Port

Heartbeat Period (seconds)
60

Customer ID

Authentication ID

Password

Upload Timing
Always (Non-recording)

12 From the *Devices* page in Clearance, select the relevant device and assign the body-worn camera to a user.

13 (Optional) In the **Device group** field, select a group to include the device in.

NOTE: Device groups are used to manage the firmware version for groups of devices.

14 Click **Activate device**.

The i-PRO BWC 4000 body-worn camera can now upload recorded video to Clearance.

Related Topics

Configuring i-PRO five fields on page 152

Adding i-PRO in-car systems

You can add an i-PRO in-car system in Clearance by creating a device and authenticating it with Clearance.

Before you begin

The following prerequisites apply when registering i-PRO in-car systems:

- You must have an active Internet connection.
- You must be a member of the *Manage devices* security policy.

Procedure

To add i-PRO ICV4000 in-car systems:

1 Configuring i-PRO ICV 4000 systems on page 144.

To add i-PRO ICV MK3 in-car systems:

1 Configuring an i-PRO Gateway on page 148.

2 Adding i-PRO ICV MK3 in-car systems on page 146.

Configuring i-PRO ICV 4000 systems

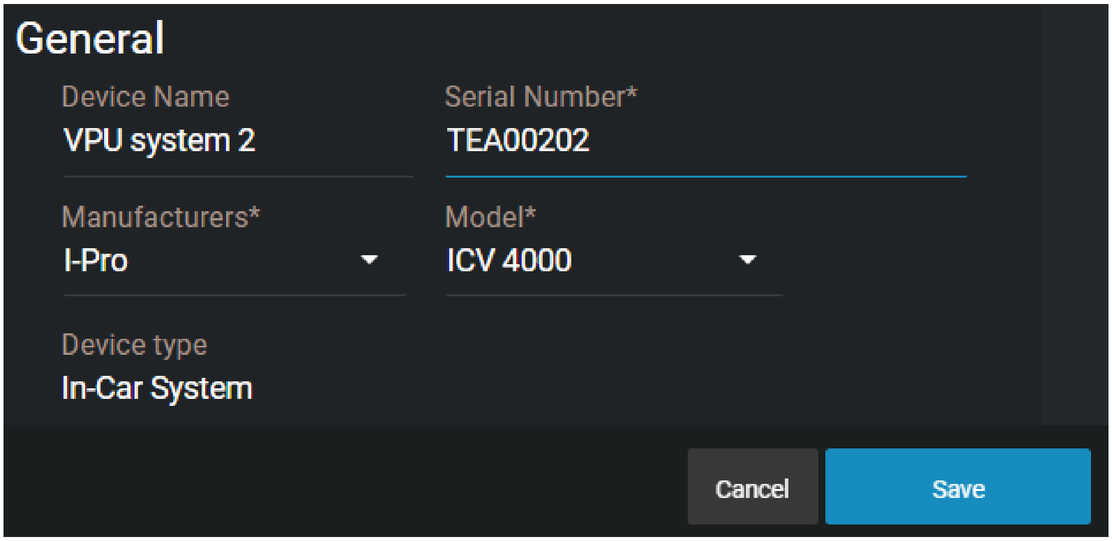
Before you can use your i-PRO ICV 4000 in-car system, you must authenticate with Clearance.

Procedure

1 From the *Devices* page in Clearance, click **Configurations** > **Devices**.

2 Click **Create new device**.

3 Enter a name for the camera, its serial number, and specify the manufacturer and model.



General

Device Name: VPU system 2

Serial Number*: TEA00202

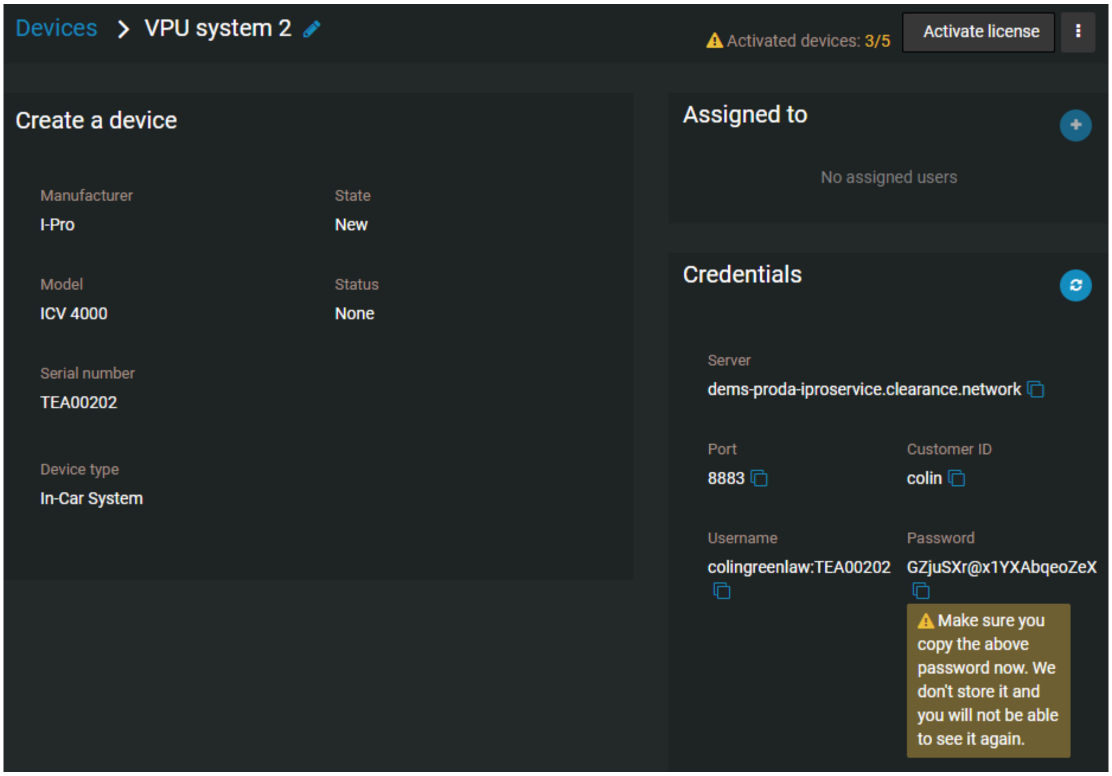
Manufacturers*: I-Pro

Model*: ICV 4000

Device type: In-Car System

4 Click **Save**.

The in-car system is created.



Create a device

Manufacturer: I-Pro

State: New

Model: ICV 4000

Status: None

Serial number: TEA00202

Device type: In-Car System

Assigned to

No assigned users

Credentials

Server: dems-proda-iproservice.clearance.network

Port: 8883

Customer ID: colin

Username: colingreenlaw:TEA00202

Password: GZjuSXr@x1YXAbqeoZeX

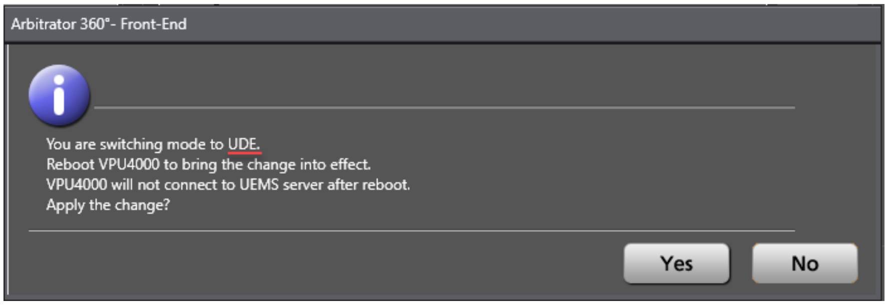
Make sure you copy the above password now. We don't store it and you will not be able to see it again.

5 Log in to the *Arbitrator 360* setup tool.

6 To work with Clearance, the ICV4000 must be in **UDE** mode, rather than **UEMS** mode. To switch your ICV4000 to **UDE** mode, do the following:

a) Click **Switch Operational Mode**.

A dialog box opens displaying the following:



You are switching mode to UDE.
Reboot VPU4000 to bring the change into effect.
VPU4000 will not connect to UEMS server after reboot.
Apply the change?

b) Click **Yes**.

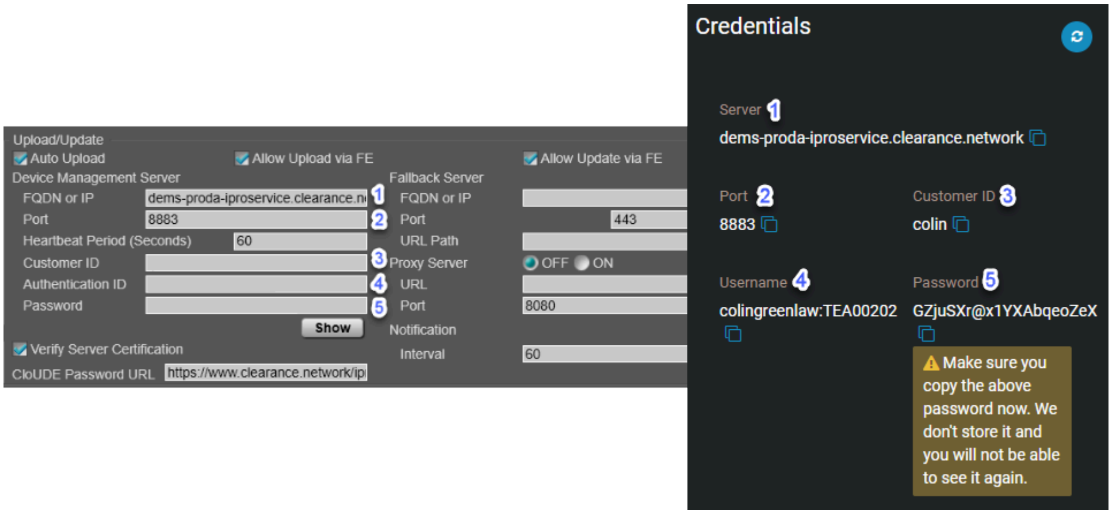
c) Apply your changes.

d) Restart the ICV 4000 device.

e) Close the *Arbitrator 360* tool and then re-open it.

NOTE: If your ICV 4000 is already in **UDE** mode, disregard these steps.

7 In the *Config* tab of the *Arbitrator 360* tool, input your Credentials from Clearance.



Upload/Update

☑ Auto Upload ☑ Allow Upload via FE ☑ Allow Update via FE

Device Management Server

- FQDN or IP: dems-proda-iproservice.clearance.n
- Port: 8883
- Heartbeat Period (Seconds): 60
- Customer ID:
- Authentication ID:
- Password:

Show

☑ Verify Server Certification

CloUDE Password URL: https://www.clearance.network/ip

Fallback Server

- FQDN or IP:
- Port: 443
- URL Path:

Proxy Server ● OFF ○ ON

- URL:
- Port: 8080

Notification

- Interval: 60

Credentials

- Server: dems-proda-iproservice.clearance.network
- Port: 8883
- Customer ID: colin
- Username: colingreenlaw:TEA00202
- Password: GZjuSXr@x1YXAbqeoZeX

⚠ Make sure you copy the above password now. We don't store it and you will not be able to see it again.

NOTE:

- Ensure that the **Verify Server Certification** check box is activated.
- In the **CloUDE Password URL** field, enter one of the following depending on which address line structure your organization uses to access Clearance:
  - https://www.clearance.network/profile
  - https://us.clearance.network/profile

Related Topics

Searching for cases or files on page 113
Configuring i-PRO five fields on page 152

Adding i-PRO ICV MK3 in-car systems

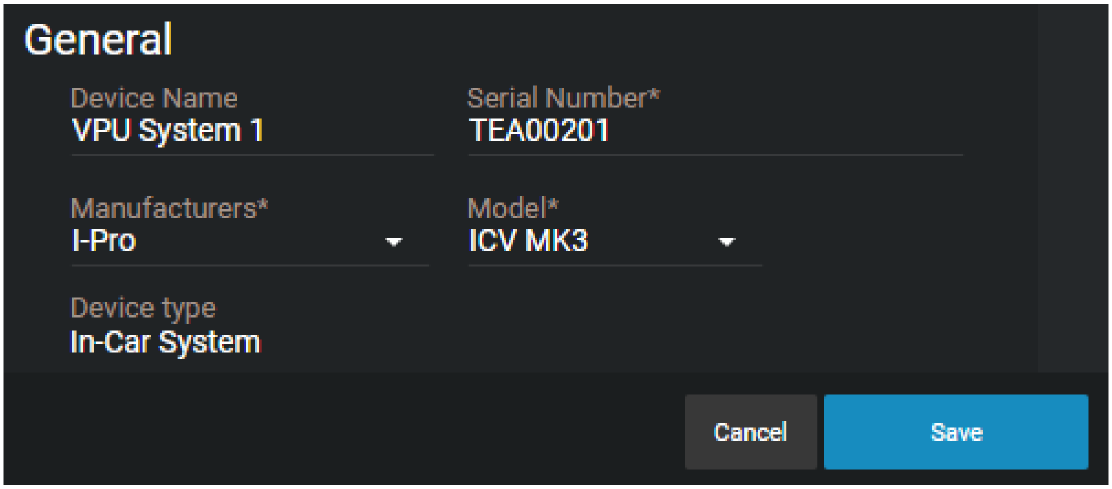
After you have added and configured an i-PRO Gateway with your Clearance account, you can enroll an i-PRO ICV MK3 in-car system.

Procedure

1 From the *Devices* page in Clearance, click **Configurations** > **Devices**.

2 Click **Create new device**.

3 Enter a name for the camera, its serial number, and specify the manufacturer and model.



General

Device Name: VPU System 1

Serial Number*: TEA00201

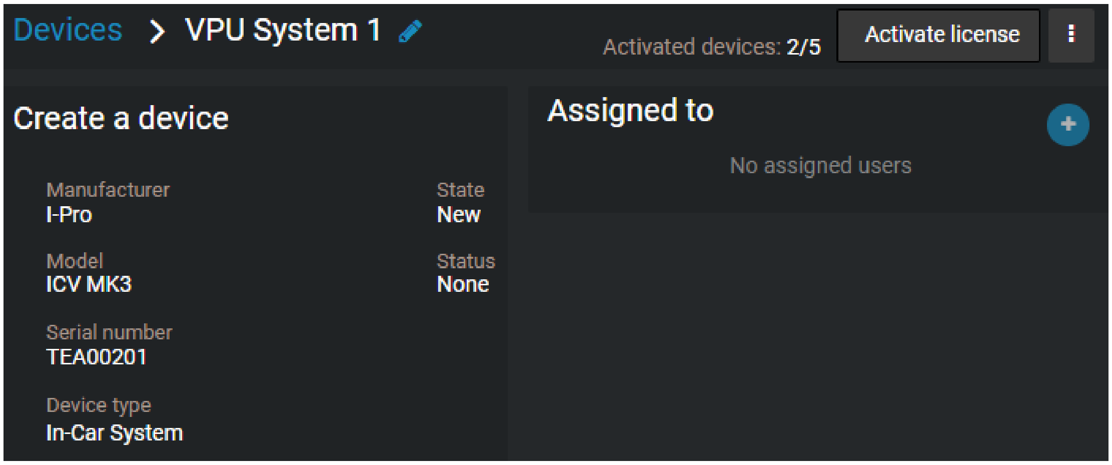
Manufacturers*: I-Pro

Model*: ICV MK3

Device type: In-Car System

4 Click **Save**.

The in-car system is created.



Devices > VPU System 1

Activated devices: 2/5

Create a device

Manufacturer: I-Pro

State: New

Model: ICV MK3

Status: None

Serial number: TEA00201

Device type: In-Car System

Assigned to

No assigned users

After you finish

- Configure an i-PRO Gateway system to use with the i-PRO ICV MK3 in-car system.
- Activate the license for the i-PRO ICV MK3.
- Assign the i-PRO ICV MK3 to a user.

Related Topics

Configuring i-PRO five fields on page 152

Configuring an i-PRO Gateway

Before you can enroll an i-PRO ICV MK3 in-car system in your Clearance account, you must configure an i-PRO Gateway.

What you should know

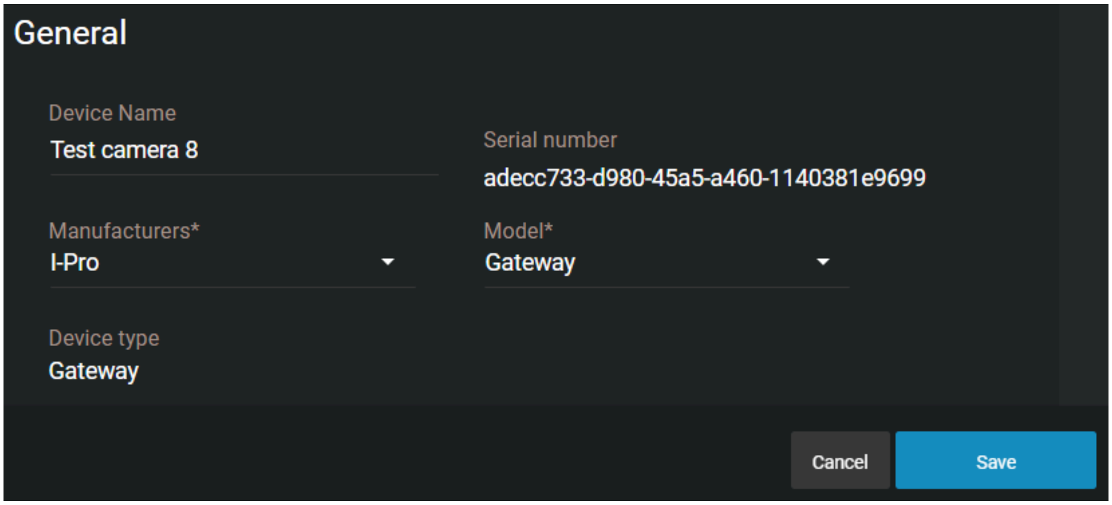
The i-PRO Gateway must be authenticated with Clearance before you can use it with an i-PRO ICV MK3 in-car system.

Procedure

1 From the *Devices* page in Clearance, click **Configurations** > **Devices**.

2 Click **Create new device**.

3 Enter a name for the camera, and specify the manufacturer and model.



General

Device Name: Test camera 8

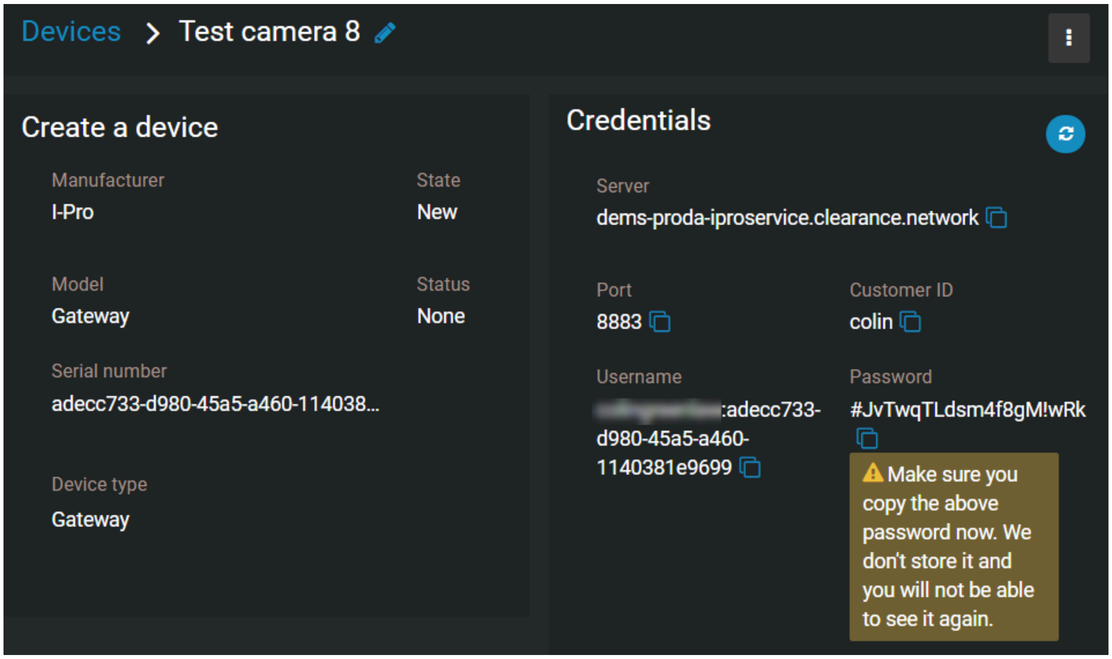
Serial number: adecc733-d980-45a5-a460-1140381e9699

Manufacturers*: I-Pro

Model*: Gateway

Device type: Gateway

4 Click **Save**.
The i-PRO Gateway is created.



Devices > Test camera 8

Create a device

Manufacturer
I-Pro

State
New

Model
Gateway

Status
None

Serial number
adecc733-d980-45a5-a460-114038...

Device type
Gateway

Credentials

Server
dems-proda-iproservice.clearance.network

Port
8883

Customer ID
colin

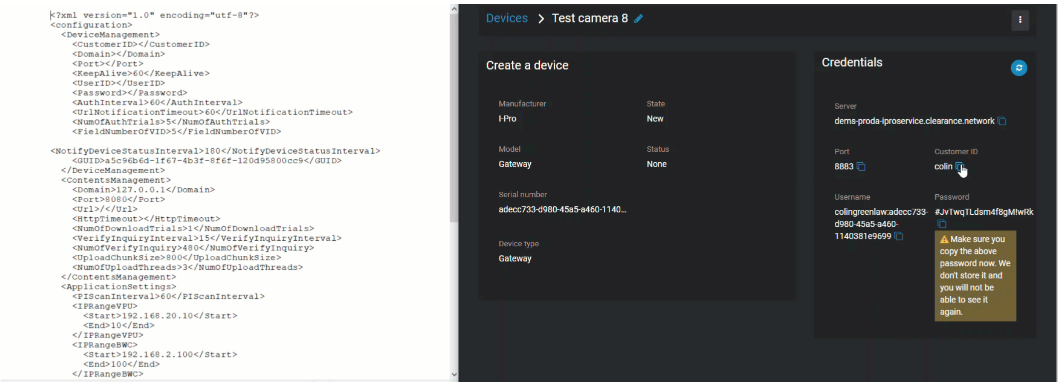
Username
[redacted]:adecc733-d980-45a5-a460-1140381e9699

Password
#JvTwqTLdsm4f8gM!wRk

⚠ Make sure you copy the above password now. We don't store it and you will not be able to see it again.

5 From a file explorer window, open the UEMSLegacyService.xml file.

6 From the *Devices* page in Clearance, copy your credentials and paste them in the corresponding elements in the UEMSLegacyService.xml file.



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <DeviceManagement>
    <CustomerID></CustomerID>
    <Domain></Domain>
    <Port></Port>
    <KeepAlive>60</KeepAlive>
    <UserID></UserID>
    <Password></Password>
    <AuthInterval>60</AuthInterval>
    <UrlNotificationTimeout>60</UrlNotificationTimeout>
    <NumOfAuthTrials>5</NumOfAuthTrials>
    <FieldNumberOfVID>5</FieldNumberOfVID>

<NotifyDeviceStatusInterval>180</NotifyDeviceStatusInterval>
    <GUID>a5c96b6d-1f67-4b3f-8f6f-120d95800cc9</GUID>
  </DeviceManagement>
  <ContentsManagement>
    <Domain>127.0.0.1</Domain>
    <Port>8080</Port>
    <Url>/</Url>
    <HttpTimeout></HttpTimeout>
    <NumOfDownloadTrials>1</NumOfDownloadTrials>
    <VerifyInquiryInterval>15</VerifyInquiryInterval>
    <NumOfVerifyInquiry>480</NumOfVerifyInquiry>
    <UploadChunkSize>800</UploadChunkSize>
    <NumOfUploadThreads>3</NumOfUploadThreads>
  </ContentsManagement>
  <ApplicationSettings>
    <PIScanInterval>60</PIScanInterval>
    <IPRangeVPU>
      <Start>192.168.20.10</Start>
      <End>10</End>
    </IPRangeVPU>
    <IPRangeBWC>
      <Start>192.168.2.100</Start>
      <End>100</End>
    </IPRangeBWC>
```

Devices > Test camera 8

Create a device

Manufacturer
I-Pro

State
New

Model
Gateway

Status
None

Serial number
adecc733-d980-45a5-a460-1140...

Device type
Gateway

Credentials

Server
dems-proda-iproservice.clearance.network

Port
8883

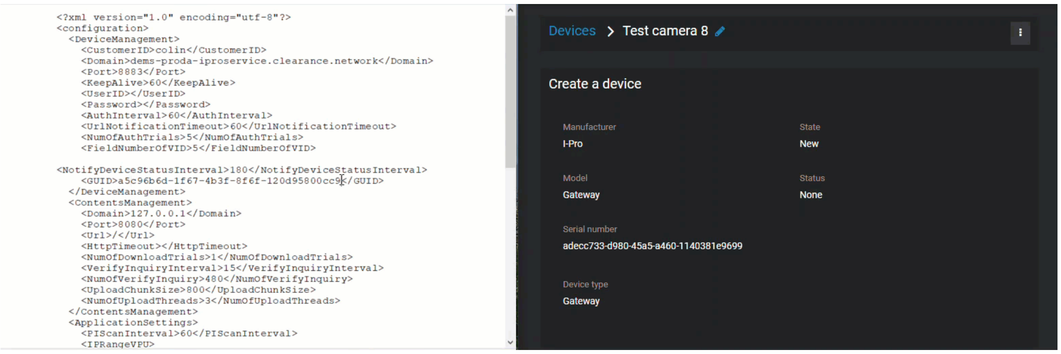
Customer ID
colin

Username
colingreenlaw:adecc733-d980-45a5-a460-1140381e9699

Password
#JvTwqTLdsm4f8gM!wRk

⚠ Make sure you copy the above password now. We don't store it and you will not be able to see it again.

7 From the *Devices* page in Clearance, copy the **Serial number** and paste it inside the <GUID></GUID> element in the UEMSLegacyService.xml file.



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <DeviceManagement>
    <CustomerID>colin</CustomerID>
    <Domain>dems-proda-iproservice.clearance.network</Domain>
    <Port>8883</Port>
    <KeepAlive>60</KeepAlive>
    <UserID></UserID>
    <Password></Password>
    <AuthInterval>60</AuthInterval>
    <UrlNotificationTimeout>60</UrlNotificationTimeout>
    <NumOfAuthTrials>5</NumOfAuthTrials>
    <FieldNumberOfVID>5</FieldNumberOfVID>

<NotifyDeviceStatusInterval>180</NotifyDeviceStatusInterval>
    <GUID>a5c96b6d-1f67-4b3f-8f6f-120d95800cc9</GUID>
  </DeviceManagement>
  <ContentsManagement>
    <Domain>127.0.0.1</Domain>
    <Port>8080</Port>
    <Url>/</Url>
    <HttpTimeout></HttpTimeout>
    <NumOfDownloadTrials>1</NumOfDownloadTrials>
    <VerifyInquiryInterval>15</VerifyInquiryInterval>
    <NumOfVerifyInquiry>480</NumOfVerifyInquiry>
    <UploadChunkSize>800</UploadChunkSize>
    <NumOfUploadThreads>3</NumOfUploadThreads>
  </ContentsManagement>
  <ApplicationSettings>
    <PIScanInterval>60</PIScanInterval>
    <IPRangeVPU>
```

Devices > Test camera 8

Create a device

Manufacturer
I-Pro

State
New

Model
Gateway

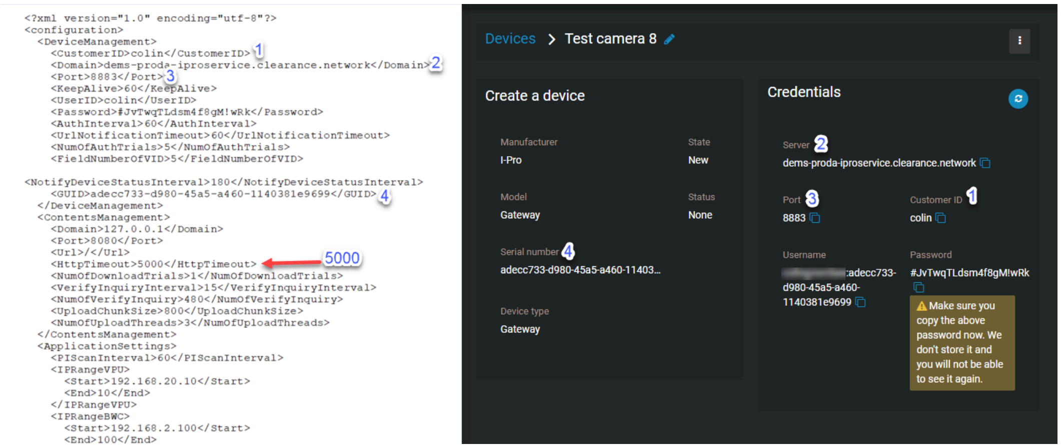
Status
None

Serial number
adecc733-d980-45a5-a460-1140381e9699

Device type
Gateway

8 From the UEMSLegacyService.xml file, change the <HttpTimeout> value to 5000.

```
<HttpTimeout>5000</HttpTimeout>
```



```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <DeviceManagement>
    <CustomerID>colin</CustomerID>
    <Domain>dems-proda-iproservice.clearance.network</Domain>
    <Port>8883</Port>
    <KeepAlive>60</KeepAlive>
    <UserID>colin</UserID>
    <Password>#JvTwqTLdsm4f8gM!wRk</Password>
    <AuthInterval>60</AuthInterval>
    <UrlNotificationTimeout>60</UrlNotificationTimeout>
    <NumOfAuthTrials>5</NumOfAuthTrials>
    <FieldNumberOfVID>5</FieldNumberOfVID>

<NotifyDeviceStatusInterval>180</NotifyDeviceStatusInterval>
    <GUID>adecc733-d980-45a5-a460-1140381e9699</GUID>
  </DeviceManagement>
  <ContentsManagement>
    <Domain>127.0.0.1</Domain>
    <Port>8080</Port>
    <Url>/</Url>
    <HttpTimeout>5000</HttpTimeout>
    <NumOfDownloadTrials>1</NumOfDownloadTrials>
    <VerifyInquiryInterval>15</VerifyInquiryInterval>
    <NumOfVerifyInquiry>480</NumOfVerifyInquiry>
    <UploadChunkSize>800</UploadChunkSize>
    <NumOfUploadThreads>3</NumOfUploadThreads>
  </ContentsManagement>
  <ApplicationSettings>
    <PIScanInterval>60</PIScanInterval>
    <IPRangeVPU>
      <Start>192.168.20.10</Start>
      <End>10</End>
    </IPRangeVPU>
    <IPRangeBWC>
      <Start>192.168.2.100</Start>
      <End>100</End>
```

Devices > Test camera 8

Create a device

Manufacturer: I-Pro
State: New
Model: Gateway
Status: None
Serial number: adecc733-d980-45a5-a460-11403...
Device type: Gateway

Credentials

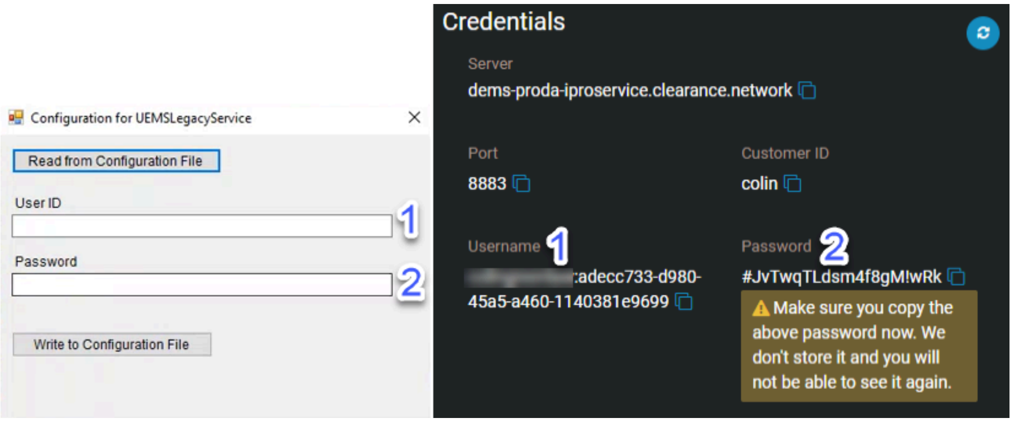
Server: dems-proda-iproservice.clearance.network
Port: 8883
Customer ID: colin
Username: [redacted]:adecc733-d980-45a5-a460-1140381e9699
Password: #JvTwqTLdsm4f8gM!wRk

⚠ Make sure you copy the above password now. We don't store it and you will not be able to see it again.

9 Save and close the UEMSLegacyService.xml file.

10 Open the UEMSLegacyServiceConfiguration.exe file.

11 From the *Devices* page in Clearance, copy the **Username** and **Password** and paste them in the **User ID** and **Password** fields in the *Configuration for UEMSLegacyService* window.



Configuration for UEMSLegacyService

Read from Configuration File

User ID

Password

Write to Configuration File

Credentials

Server: dems-proda-iproservice.clearance.network
Port: 8883
Customer ID: colin
Username: [redacted]:adecc733-d980-45a5-a460-1140381e9699
Password: #JvTwqTLdsm4f8gM!wRk

⚠ Make sure you copy the above password now. We don't store it and you will not be able to see it again.

12 Click **Write to Configuration File**.

13 Open the UEMSLegacyService.xml file. The User ID and Password are present in the file.

14 Ensure the SSLUnused.dat file is removed from UEMSLegacyService.

NOTE: If you need to remove the SSLUnused.dat file, you might need to restart the UEMSLegacyService.

Related Topics

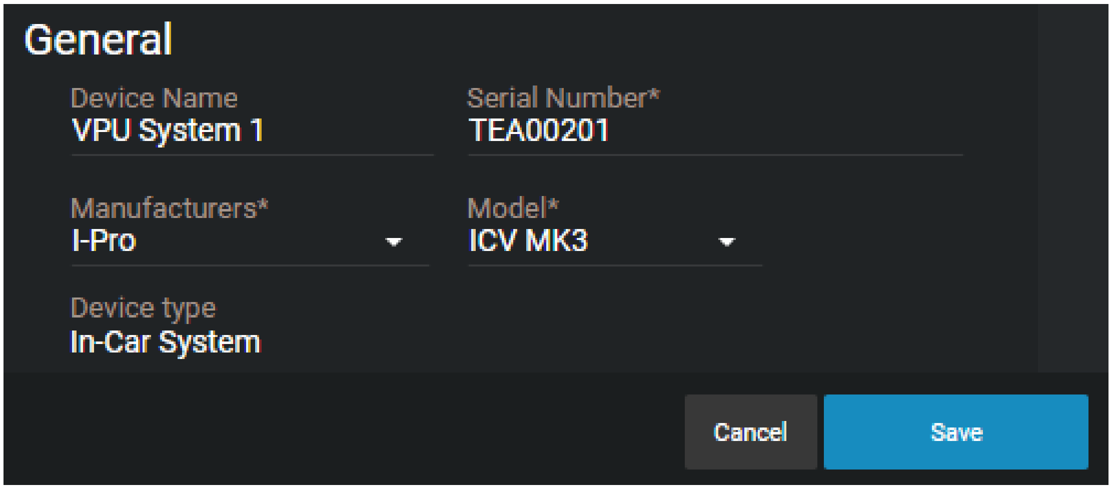
Configuring i-PRO five fields on page 152

Adding i-PRO ICV MK3 in-car systems

After you have added and configured an i-PRO Gateway with your Clearance account, you can enroll an i-PRO ICV MK3 in-car system.

Procedure

1 From the *Devices* page in Clearance, click **Configurations** > **Devices**.
2 Click **Create new device**.
3 Enter a name for the camera, its serial number, and specify the manufacturer and model.



General

Device Name: VPU System 1

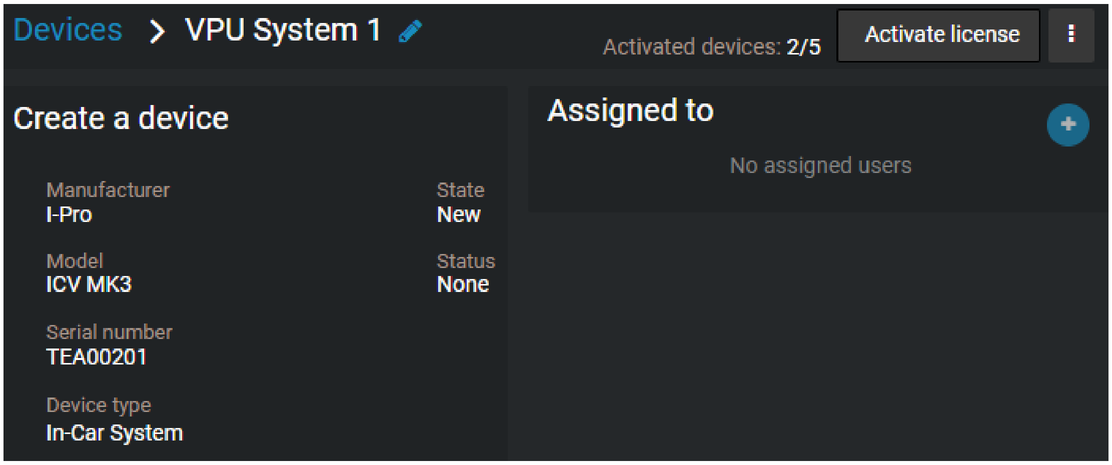
Serial Number*: TEA00201

Manufacturers*: I-Pro

Model*: ICV MK3

Device type: In-Car System

4 Click **Save**.
The in-car system is created.



Devices > VPU System 1

Activated devices: 2/5

Create a device

Manufacturer: I-Pro

State: New

Model: ICV MK3

Status: None

Serial number: TEA00201

Device type: In-Car System

Assigned to

No assigned users

After you finish

- Configure an i-PRO Gateway system to use with the i-PRO ICV MK3 in-car system.
- Activate the license for the i-PRO ICV MK3.
- Assign the i-PRO ICV MK3 to a user.

Configuring i-PRO five fields

To make the metadata fields generated by recordings using i-PRO cameras and in-car systems consistent with Clearance, you must configure the i-PRO five fields.

Before you begin

Add an i-PRO body-worn camera or in-car system.

What you should know

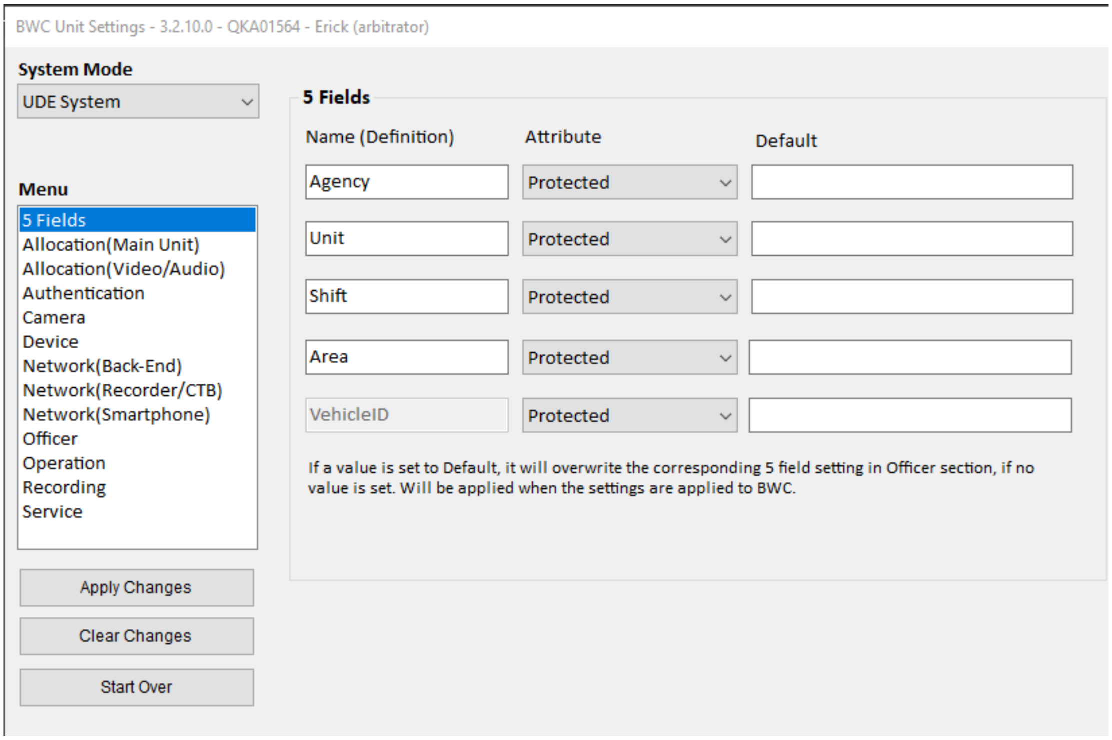
Only users who are part of the *Account Administrators* group can configure fields.

Procedure

1. From the **Configurations** page, click **Fields and labels**.
2. Select the **File** template.
3. Create five fields and name them as follows:
   - Agency
   - Unit
   - Shift
   - Area
   - VehicleID

   NOTE: For instructions on how to create fields, see Creating fields on page 66.
4. From the *BWC unit settings* page of your i-PRO camera or in-car system, select the **5 Fields** configuration.
5. Define your values in the **Default** column.

6 Click **Apply changes**.



BWC Unit Settings - 3.2.10.0 - QKA01564 - Erick (arbitrator)

System Mode: UDE System

5 Fields

Name (Definition)	Attribute	Default
Agency	Protected	
Unit	Protected	
Shift	Protected	
Area	Protected	
VehicleID	Protected	

If a value is set to Default, it will overwrite the corresponding 5 field setting in Officer section, if no value is set. Will be applied when the settings are applied to BWC.

Related Topics

Searching for cases or files on page 113

About i-PRO automatic case creation and file tagging

You can automatically generate cases in Genetec Clearance™ and associate them with recordings tagged from the i-PRO Front End system and body worn web app.

Context:

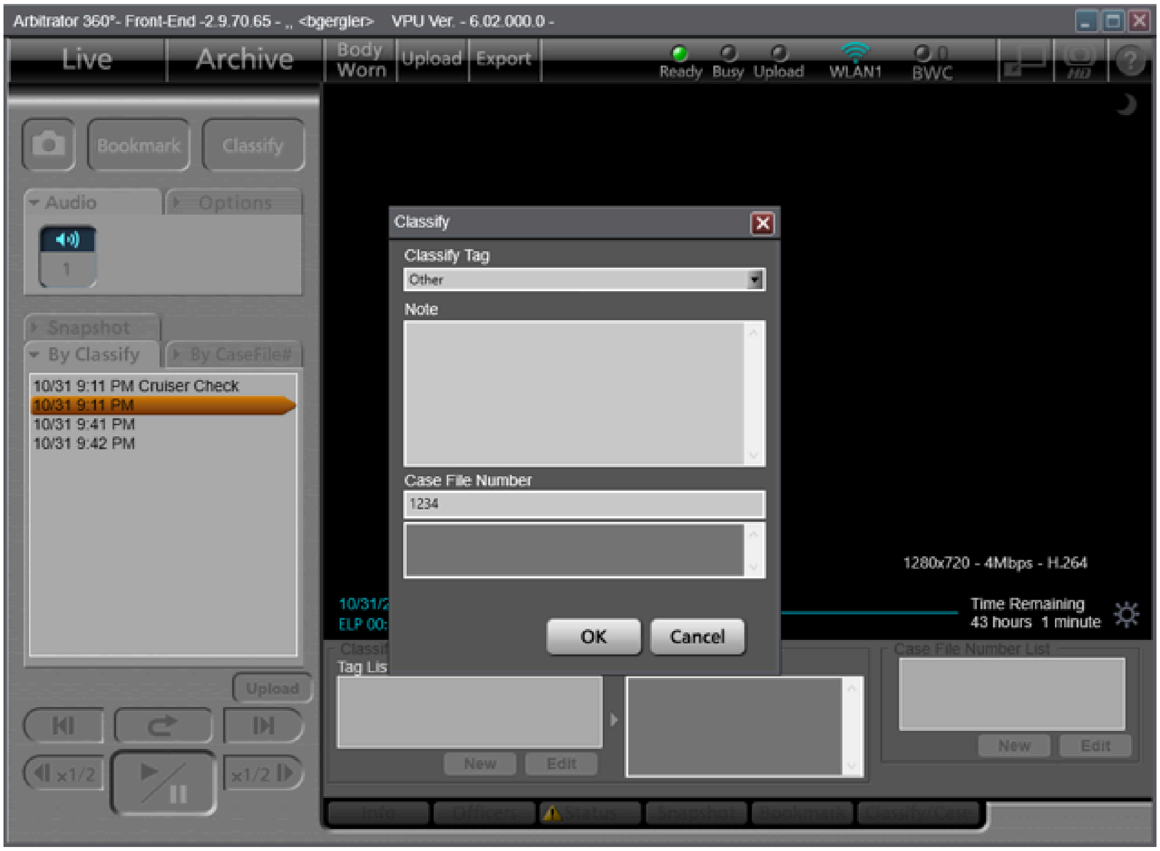
- The association between uploaded evidence and a given case is based on files sharing the same case file number.
- Cases are generated using the default department configured in the account.
- The Case Sync license must be activated to enable the i-PRO automatic case creation and file tagging functionality. Contact your reseller for more info.

How i-PRO automatic case creation and file tagging works:

1. Set a default department.

   NOTE: The default department determines the users and groups that are added to the cases and the permission level that they have.

2. When uploading evidence from a body-worn camera or in-car system, tag the files with a case file number.



Arbitrator 360°- Front-End -2.9.70.65 - ,, <bgergler> VPU Ver. - 6.02.000.0 -

Classify Tag: Other

Note:

Case File Number: 1234

10/31 9:11 PM Cruiser Check
10/31 9:11 PM
10/31 9:41 PM
10/31 9:42 PM

3. After the evidence is uploaded, a new case is generated that includes all files that have been tagged with the same case file number. If the case file number matches an incident number of an existing case, the files are added to that case.

   NOTE: The case file number is generated in a case's *incident number* field.

About device groups

Create and configure device groups to bulk-manage configurations for your i-PRO body-worn cameras and in-car devices.

Device groups conform to the following rules:

- Only i-PRO devices can be included in device groups.
  - The following i-PRO device models can be formed into device groups:
    - BWC MK3
    - BWC 4000
    - VPU 4000
- A device group can only contain one model type of device.

See the following to create, add devices to, and configure device groups:

1. Create device groups.
2. Add devices to device groups.
3. Configure device groups.

Related Topics

Defining device policies on page 159

Creating device groups

Create device groups to manage the configurations for groups of devices.

Before you begin

Add i-PRO body-worn cameras or in-car systems.

Procedure

1 From the **Configurations** menu, select **Device groups**.

2 Click **Create device group**.

3 Configure the device group information:
   a) Assign a name to the device group.
   b) Select a model type for the group.

4 Click **Save**.

After you finish

Add devices to the group.

Adding devices to groups

Add devices to your group and bulk-manage configurations for the devices in the group.

Before you begin

Create a device group.

What you should know

- The following i-PRO device models can be formed into device groups:
  - BWC MK3
  - BWC 4000
  - VPU 4000
- A device group can only contain one model type of device.

Procedure

1. From the **Device groups** page, select the relevant device group.
2. To add devices to the device group, in the **Assigned devices** section, click **Add** (+).
3. In the *Add i-PRO* device window, select the devices you want to add to the group and click **Add**.
4. Click **Save**.

After you finish

Learn about device group configurations.

Configuring device groups

Configure device groups to bulk-control firmware versions and device settings.

Before you begin

Create a device group.

What you should know

- Changes to the configurations of a device group control the configurations for all included devices.
- The setting file is used to bulk-control i-PRO body-worn camera and in-car system configurations made at the device level.
- You can follow these same steps to configure settings at the device level.

Procedure

1. From the **Device Groups** page, select the relevant device group.
2. Configure device settings for the device group.
3. Configure the firmware version for the device group.

4 If you are configuring an in-car system, you can attach cameras to the system by doing the following:
   a) From the in-car system device or device group page, navigate to the **Attached cameras** section.
   b) Click **Add** (+).
   c) From the **Select camera** window, select the cameras you want to attach to the in-car system.
   d) Click **Save**.

5 Click **Save**.

About device group configurations

Device groups are used to dispatch firmware versions and device settings to multiple devices at a time.

Before you can configure a device group, you must create one and add devices to it.

- Changes to the configurations of a device group control the configurations for all included devices.
- The configuration file contains the settings that you want to apply to all the devices in the device group.

To manage configurations for a device group:

- From the **Device groups** page, select the relevant device group.
- Manage device configurations for the device group.
- Configure the firmware version for the device group.
- If you are configuring an in-car system, you can attach cameras to the system by doing the following:
   1. From the in-car system device or device group page, navigate to the **Attached cameras** section.
   2. Click **Add** (+).
   3. From the **Select camera** window, select the cameras you want to attach to the in-car system.
   4. Click **Save**.
- Click **Save**.

Managing i-PRO device configurations

Configure settings in your i-PRO device, save them as a compressed file, and upload the file to a device group in Clearance to map these configurations to all devices in the group.

Before you begin

- Create a configuration file in your i-PRO device manager tool and save it as a .cloude_zip file.

What you should know

- The configuration file can be applied at the device level or at the device group level. The configuration file selected at the device group level overwrites what is selected at the device level.

Procedure

1 From the **Device groups** page, select the relevant device.

2 In the **Configuration** section, browse for a file from the **Configuration file** menu.

3 In the File Explorer window, select the file you created earlier.

4 Click **Save**.

After you finish

(Optional) Configure the firmware version for your i-PRO body-worn cameras and in-car systems.

Configuring i-PRO firmware version

You can control the firmware version used by your i-PRO body-worn cameras and in-car systems to manage updates and test new versions to ensure they work properly.

Before you begin

- Create a device group.
- Add i-PRO devices to the device group.

What you should know

- The firmware version can be configured at the device level, or at the device group level. The firmware version selected at the device group level overwrites what is selected at the device level.
- The firmware configuration procedure is the same for body-worn cameras and in-car systems.
- The following software and firmware versions are supported for i-PRO devices:

Software	Minimum version
Legacy interface server	3.4.12.0
FE (AG-JJLFE20P)	2.9.80.69
BWC 4000 Configuration Tool	1.4.0.3
BWC MK3 Configuration Tool	3.2.12.5

Firmware	Minimum version
VPU 4000 (WJ-VPU 4000)	6.08.000.0
VPUmk3 (WJ-VR30) **NOTE:** This device does not support the firmware update or configuration update functionality.	5.22.000.0
BWC 4000 (WV-BWC 4000)	1700M02
BWC MK3 (WV-TW370)	2036M0001

Procedure

1. From the **Devices** page in Clearance, select the required device.
2. In the **Configuration** section click on the **Firmware target version** menu.
3. (Optional) Click **Show preview versions** to reveal unreleased preview firmware versions.
4. Select a firmware version from the list.

   IMPORTANT: Ensure you are using at least the minimum firmware version.
5. Click **Save**.

After you finish

(Optional) Learn about device groups.

Defining device policies

Define device policies in Clearance to ensure synchronicity between users' devices and their Clearance profiles.

Before you begin

- Add users
- Add i-PRO body-worn cameras
- Add i-PRO in-car systems

Procedure

- Manage i-PRO user account policies.

Managing i-PRO user account policies

Add users to the **i-PRO user account credentials** device policy in Clearance to ensure that i-PRO Front End application credentials are synced with Clearance.

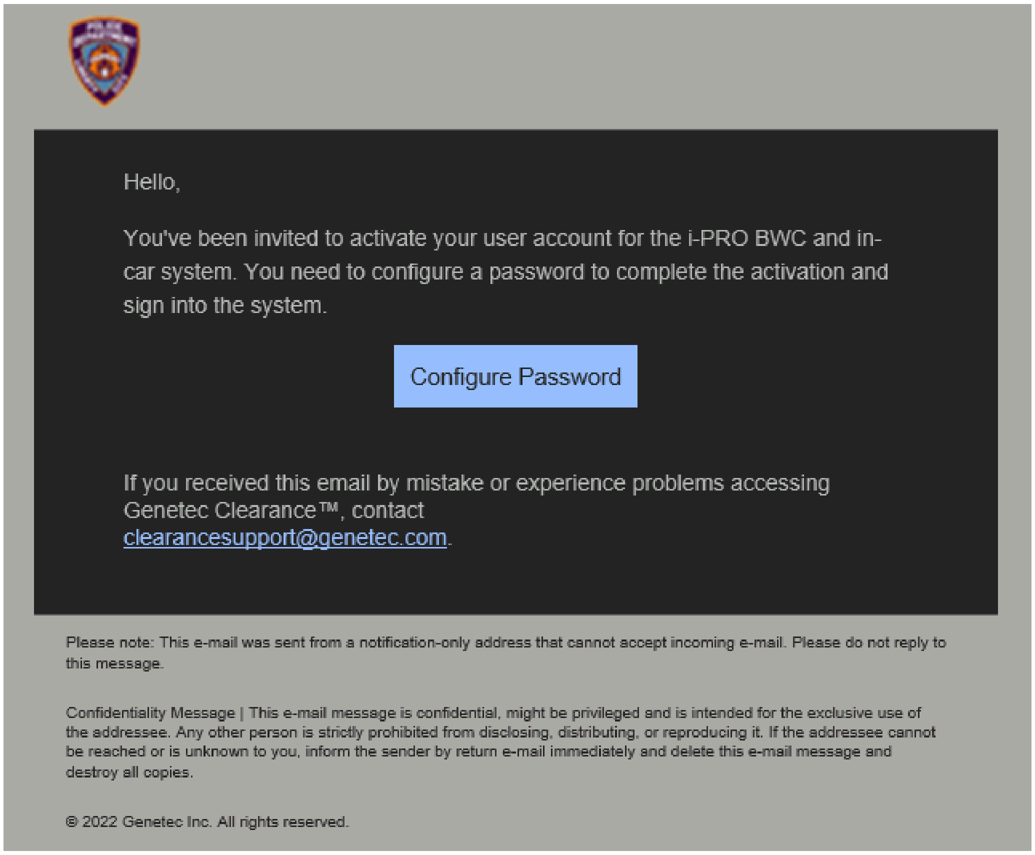
Before you begin

- Add users
- Add i-PRO body-worn cameras
- Add i-PRO in-car systems

Procedure

1. From the **Configurations** menu, select **device policies**.
2. In the **i-PRO user account credentials** section, click **Add** (➕).
3. From the *Add existing groups or users* window, select the users you want to include in the policy.

4 Click **Add**.
The users added to the policy receive an email prompting them to define their credentials.



Hello,

You've been invited to activate your user account for the i-PRO BWC and in-car system. You need to configure a password to complete the activation and sign into the system.

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

Please note: This e-mail was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Confidentiality Message | This e-mail message is confidential, might be privileged and is intended for the exclusive use of the addressee. Any other person is strictly prohibited from disclosing, distributing, or reproducing it. If the addressee cannot be reached or is unknown to you, inform the sender by return e-mail immediately and delete this e-mail message and destroy all copies.

© 2022 Genetec Inc. All rights reserved.

After you finish

Manage i-PRO user account credentials.

Managing i-PRO user account credentials

Define users' i-PRO user account credentials in order for the annotations that they make and details that they note in videos recorded using their i-PRO devices are mapped to the corresponding video files in Clearance.

Before you begin

- Add users to the i-PRO user account policy

What you should know

Ensure you are using an up-to-date version of the i-PRO front-end software and device firmware. For more information, refer to the list of supported i-PRO software and firmware versions:

Software	Minimum version
FE (AG-JJLFE20P)	2.9.81.82
VPU 4000 (WJ-VPU 4000)	6.11.001.0

Software	Minimum version
VPU MK3	5.22.000.0
Legacy Interface Server	3.5.5.0

Procedure

To configure credentials of users within your account:

1 From the **Configurations** tab, select **Device policies**.

2 From the **i-PRO user account credentials** section, find the relevant user and click **Set password manually**.

The profile of the selected user is displayed.

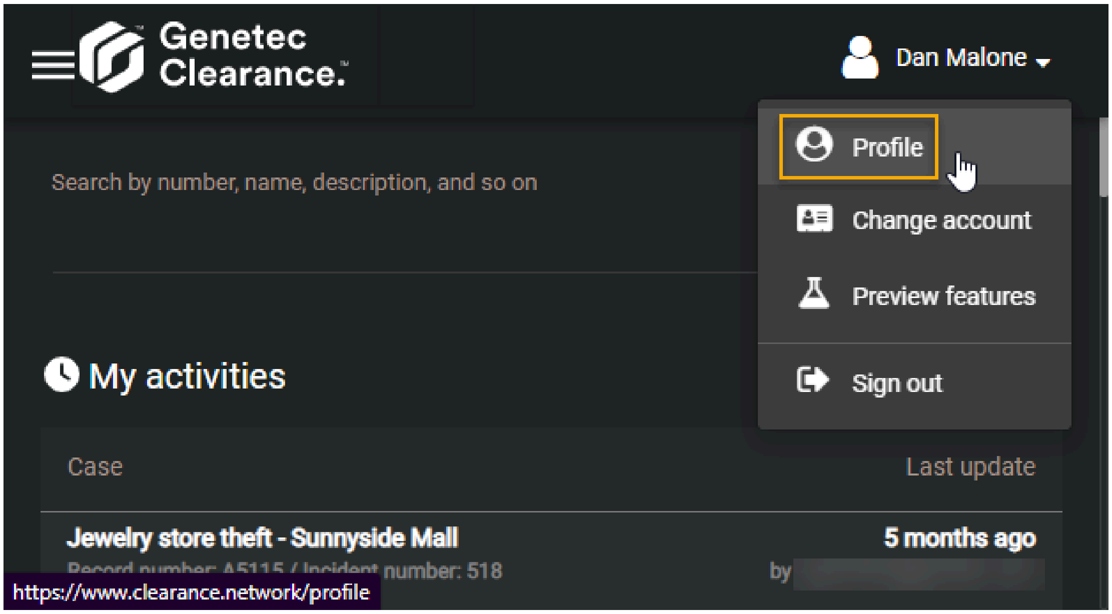
3 In the **i-PRO user account** section, click **Edit** (✎).

4 In the *Edit in-car user credentials* window, define a username and password.

5 Click **Save**.

To configure credentials for your own user profile if you are not an Admin user:

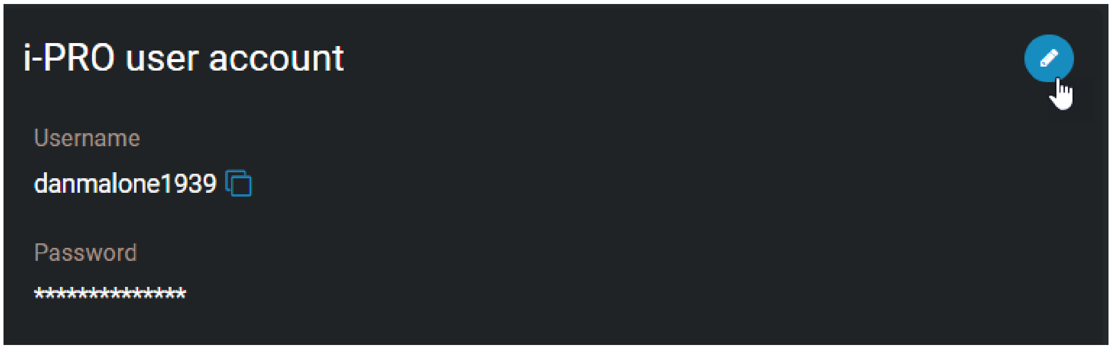
1 Navigate to your Clearance user profile.



Case	Last update
Jewelry store theft - Sunnyside Mall Record number: A5115 / Incident number: 518	5 months ago by [redacted]

https://www.clearance.network/profile

2 From the **i-PRO user account** section, click **Edit** (✎).



i-PRO user account

Username

danmalone1939

Password

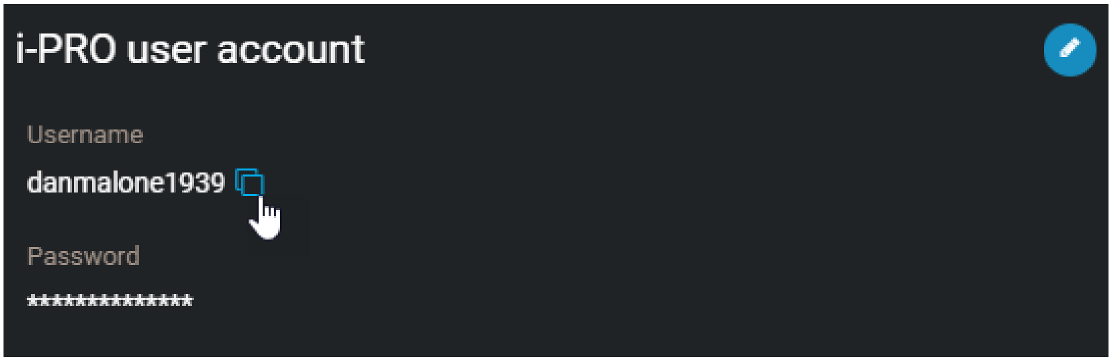
****

3 Define a password.

4 Click **Save**.

To add your i-PRO user account credentials to your i-PRO device configuration tool:

1 From the **i-PRO user account** section of the user page, copy the username.



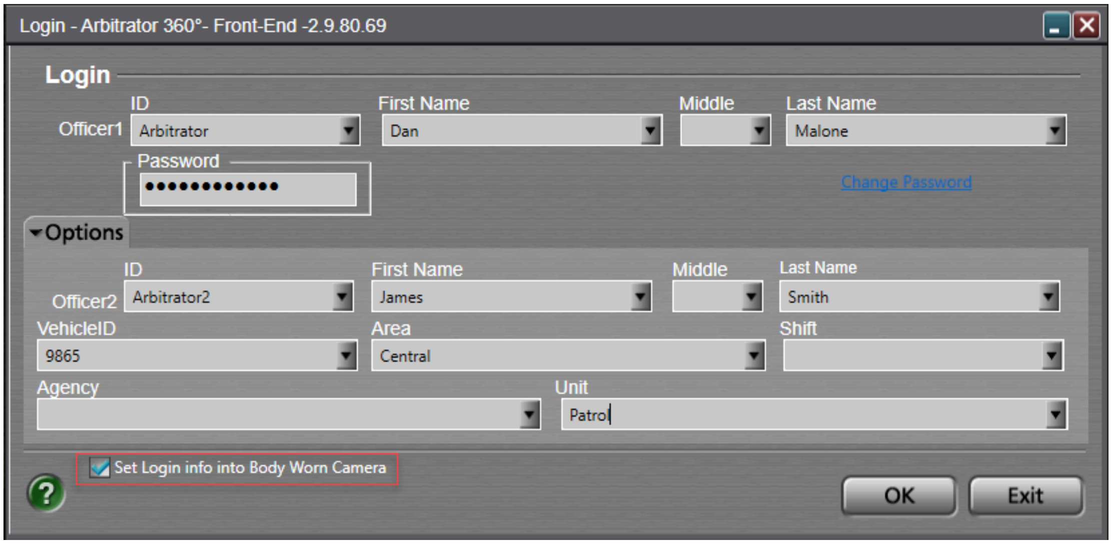
i-PRO user account

Username: danmalone1939

Password: **************

2 From the VPU front-end application, enter the i-PRO user account username and password that you configured in Clearance.

3 Activate the **Set login info into Body Worn Camera** check box.



Login - Arbitrator 360°- Front-End -2.9.80.69

Login

Officer1 — ID: Arbitrator; First Name: Dan; Middle: ; Last Name: Malone

Password: •••••••••••••

Change Password

Options

Officer2 — ID: Arbitrator2; First Name: James; Middle: ; Last Name: Smith

VehicleID: 9865; Area: Central; Shift:

Agency: ; Unit: Patrol

☑ Set Login info into Body Worn Camera

4 Click **OK**.

9

Managing files

Create, share, and associate files in Clearance.

This section includes the following topics:

- "About Clearance information security" on page 164
- "Uploading files to cases" on page 165
- "Configuring file details" on page 167
- "Reviewing media" on page 168
- "Video player controls" on page 170
- "Sharing files" on page 172
- "Inviting guests to view files" on page 173
- "Associating cases with a file" on page 175
- "Linking files to another case" on page 177
- "Searching evidence by device assignment" on page 178
- "File formats you can preview in Clearance" on page 180
- "Downloading files" on page 182
- "Changing access policies for files" on page 185
- "Protecting files from deletion" on page 187
- "Deleting files" on page 188
- "Restoring files" on page 190
- "Viewing the audit trail history of files" on page 191

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.

Related Topics

Viewing the audit trail history of files on page 191

Viewing the audit trail history of cases on page 125

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 or create a case.

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

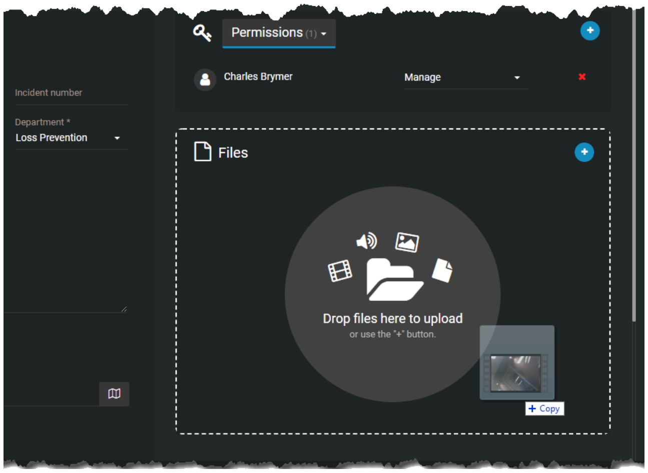
- **Add files from computer**
- **Add files from Clearance**
- **Create folder**

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.



Charles Brymer Manage

Department * Loss Prevention

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 and then click **Add to case**.

b) (Optional) To filter results and identify files to add to a case, click the **More filters** menu.

c) (Optional) To remove files from a case, select the files and then click **Remove**.

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.

▶

Related Topics

Changing access policies for files on page 185
Searching for cases or files on page 113
File formats you can preview in Clearance on page 180

Configuring file details

Configure file details to better classify and compare your evidence files.

Before you begin

Upload a file to a case in Clearance.

Procedure

- From the *General* section of the *File* page, enter information for the following:
  - **Description:** Enter a description of the file.
  - **Start time:** If applicable, enter a start time for the file.
  - **End time:** If applicable, enter an end time for the file.
  - **Category:** Classify the file into one of your categories.
  - **Associated cases:** View the cases the file is associated with and Add the file to cases.
  - **Tags:** Tag the file with keywords to make it findable in searches.
  - **Location:** Define a location to associated with the file, such as where the file was captured.
  - **Custom fields:** Enter values for any custom fields included in the file details.

    NOTE: You can search for values provided in your custom fields using the **Case custom fields** and **File custom fields** search filters.
  - **Scheduled deletion:** Choose to set a deadline after which the file is deleted, or to protect it from deletion.

After you finish

Filter your searches for cases or files using custom fields.

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** (▶).

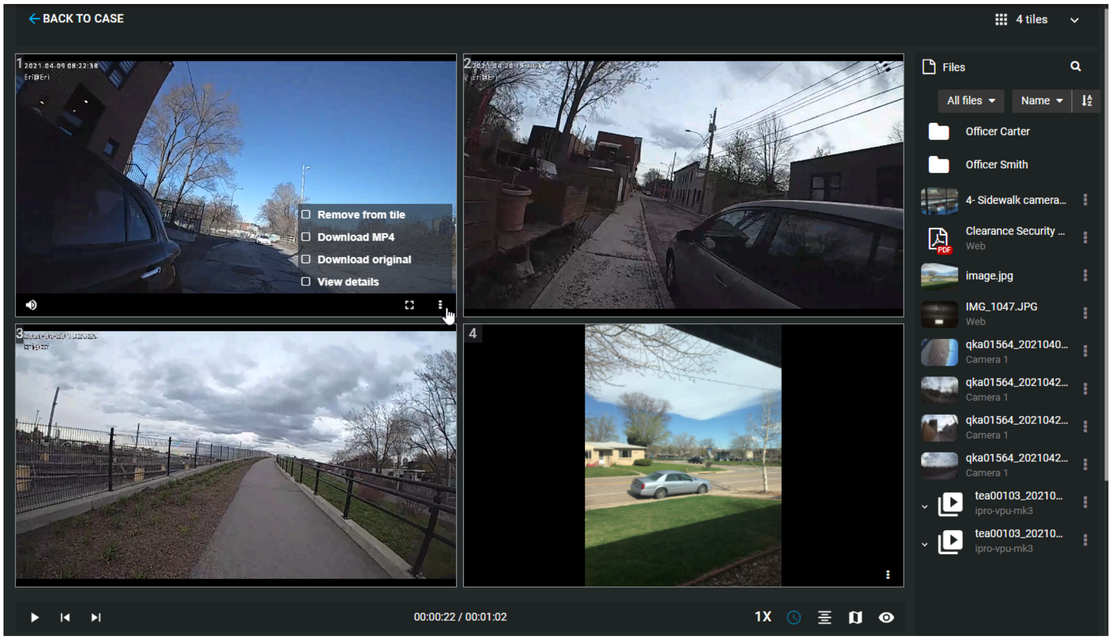
3 Click ▦ to enter the evidence player, where the multi-tile view can be accessed.

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**.

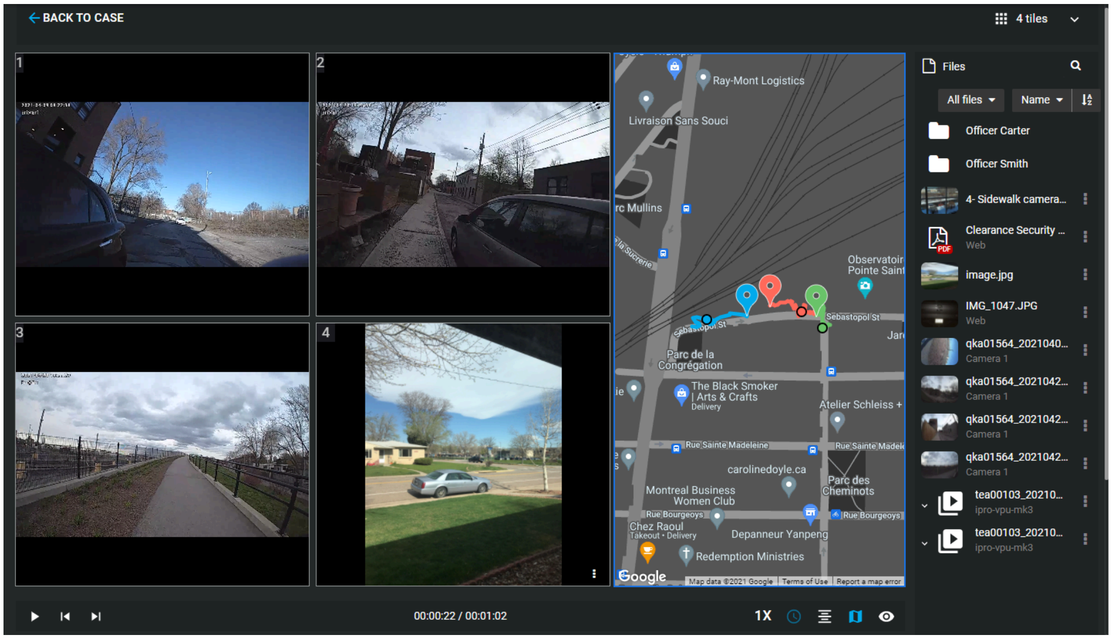
2 Click the files you want to examine, or drag and drop them into the tiles.



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.

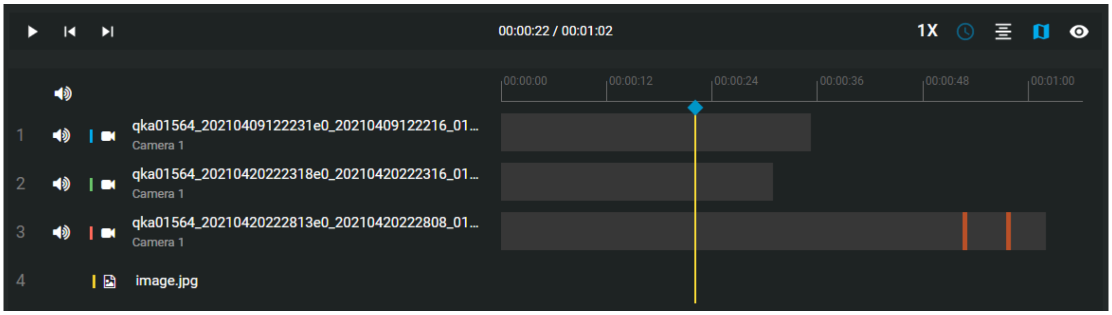
4 (Optional) If available, click **GPS trail** (🗺) to display the GPS trail location data for a video.

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.


00:00:22 / 00:01:02
1X
00:00:00
00:00:12
00:00:24
00:00:36
00:00:48
00:01:00
1
qka01564_20210409122231e0_20210409122216_01...
Camera 1
2
qka01564_20210420222318e0_20210420222316_01...
Camera 1
3
qka01564_20210420222813e0_20210420222808_01...
Camera 1
4
image.jpg

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.

Related Topics

Viewing G64 or G64x video files in the Genetec™ Video Player on page 280
Video player controls on page 170

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 on page 36.
🗺	**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.

Related Topics

Reviewing media on page 168

Sharing files

To let internal or external members of your organization view, modify, and manage files, you can share files with them and define their access rights on a file by file basis.

Before you begin

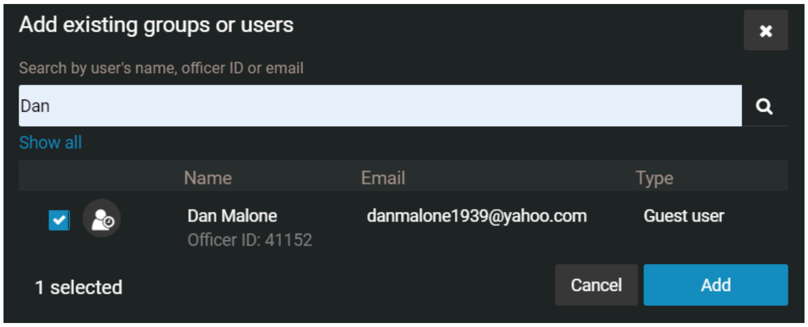
Create a user account for the user you want to share the file with.

Procedure

1 Open an existing file or Upload a file.

2 In the **Permissions** section, click + > **Add users** .

3 In the *Add existing users* window, select the user and then click **Add**.



Add existing groups or users

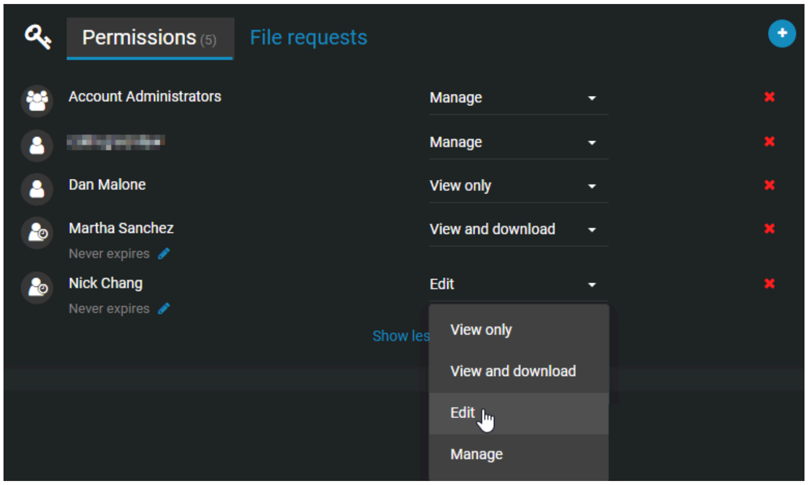
Search by user's name, officer ID or email: Dan

	Name	Email	Type
☑	Dan Malone Officer ID: 41152	danmalone1939@yahoo.com	Guest user

1 selected

The user is added to the list of users and, by default, is given the *View and download* permission level for the file.

4 Change the permission level for the user, as required, and then click **Save**.



Account Administrators	Manage
[redacted]	Manage
Dan Malone	View only
Martha Sanchez Never expires	View and download
Nick Chang Never expires	Edit

An email is automatically sent to the user, inviting the user to view the file details.

Related Topics

About email notifications in Clearance on page 3

Inviting guests to view files on page 173

Inviting guests to view files

If you want to share a specific file with someone who does not already have a Clearance account, without allowing them to search or view other files, you can invite this person as a guest.

What you should know

A user can either be a guest or regular user. Guests cannot perform searches in the system and cannot access the **Configurations** menu. Regular users have full access but can only access the **Configurations** menu if they are in the *Account Administrator* group.

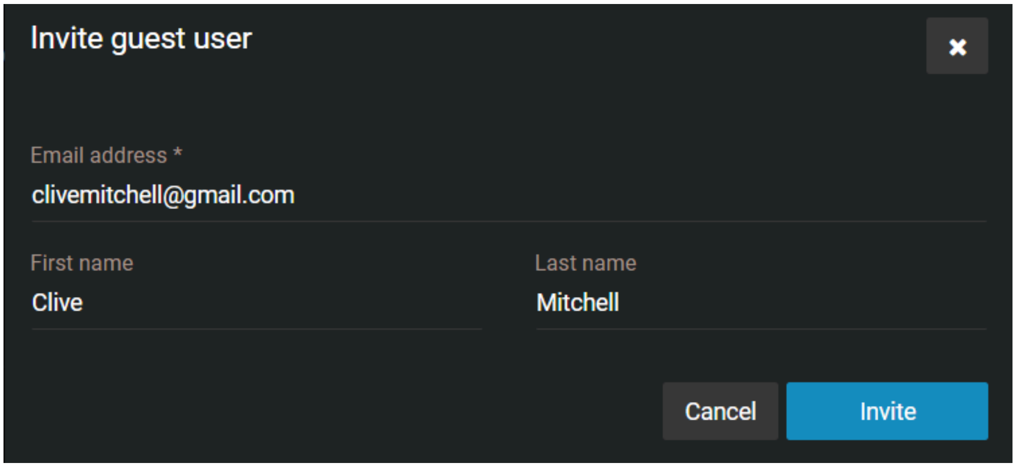
Procedure

1 Open an existing file or Upload a file.

2 If you are a regular user inviting a guest user, do the following:

a) In the *Permissions* section, click ⊕ > **Invite guest user** .

b) In the *Invite guest user* window, enter the email address and name of the person you want to invite, and click **Invite**.



Invite guest user

Email address *
clivemitchell@gmail.com

First name
Clive

Last name
Mitchell

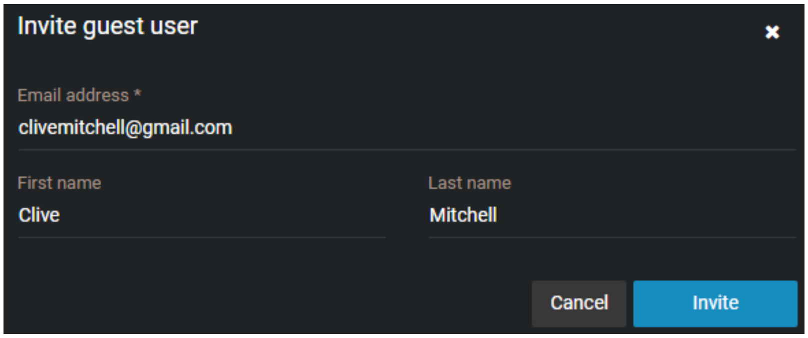
3 If you are a regular user inviting a guest user that has a Clearance account, do the following:

a) In the *Permissions* section, click ⊕ > **Invite guest user** .

b) In the *Invite guest user* window, enter the email address and name of the person you want to invite, and click **Invite**.

c) Select the users that you require from the list and click **Add**.

4 If you are a guest user inviting a guest user, do the following:
   a) In the *Permissions* section, click ⊕ > **Invite guest user** .
   b) Type the email address of the guest user that you want to share the file with.
   c) Click **Invite**.



Invite guest user

Email address * clivemitchell@gmail.com

First name Clive

Last name Mitchell

The person's email address is added to the *Permissions* section for the file, and an email inviting the user to join Clearance is automatically sent.

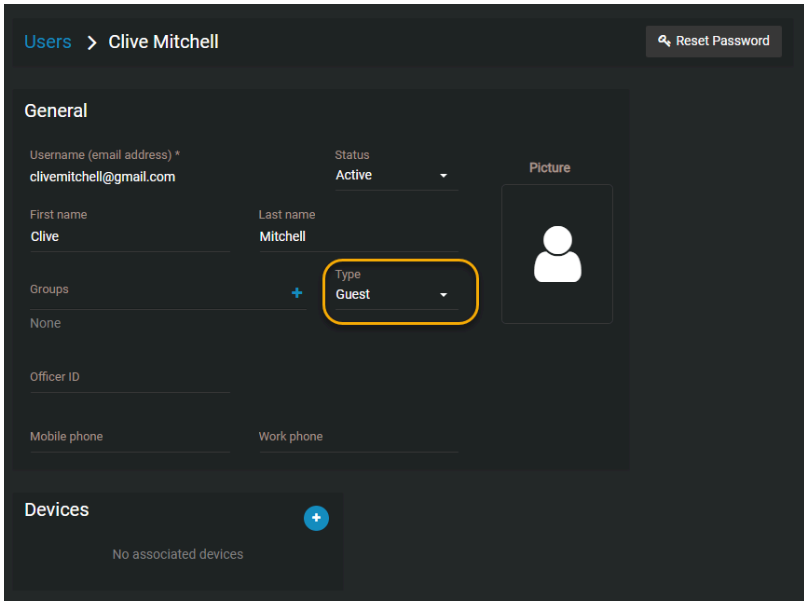
5 (Optional) Specify an expiration date for the guest user's access to the file.
   The default is **Never expires.**
   NOTE: You cannot specify an expiration date for a guest user with *Manage* permissions.
   a) Under the guest users name, click **Modify the expiration date** (✎).
   b) Clear the **Never** check box and enter an expiration date or use the calendar picker to choose a date.
   c) Click **Modify** to confirm the changes.

6 (Optional) If required, modify the user's access rights to the file, and then click **Save**.

An email is automatically sent inviting the user to view the file details. After activating their account and logging on to the system, the user will only have access to the file that they were invited to view.

After you finish

When you invite a guest to view a file, the system automatically creates a user account for the guest, with the **Type** field set to **Guest**. From the **Configurations** menu, you can access the user account to edit all of the fields as required.



Users > Clive Mitchell

General

Username (email address) * clivemitchell@gmail.com

Status Active

First name Clive

Last name Mitchell

Groups None

Type Guest

Officer ID

Mobile phone

Work phone

Devices

No associated devices

Associating cases with a file

To track which files are involved in a case or incident, you can manually associate one or more cases with a file in the *File* page.

What you should know

- To associate one or more cases with a file, you must have the *Edit* permission level for that file.
- To download a file, you must have the *View and download* permission level for that file.

NOTE: Only files that are manually associated with a case can be removed from the **Associated cases** section. Files that are automatically associated with a case based on incident time range cannot be removed from the **Associated cases** section.

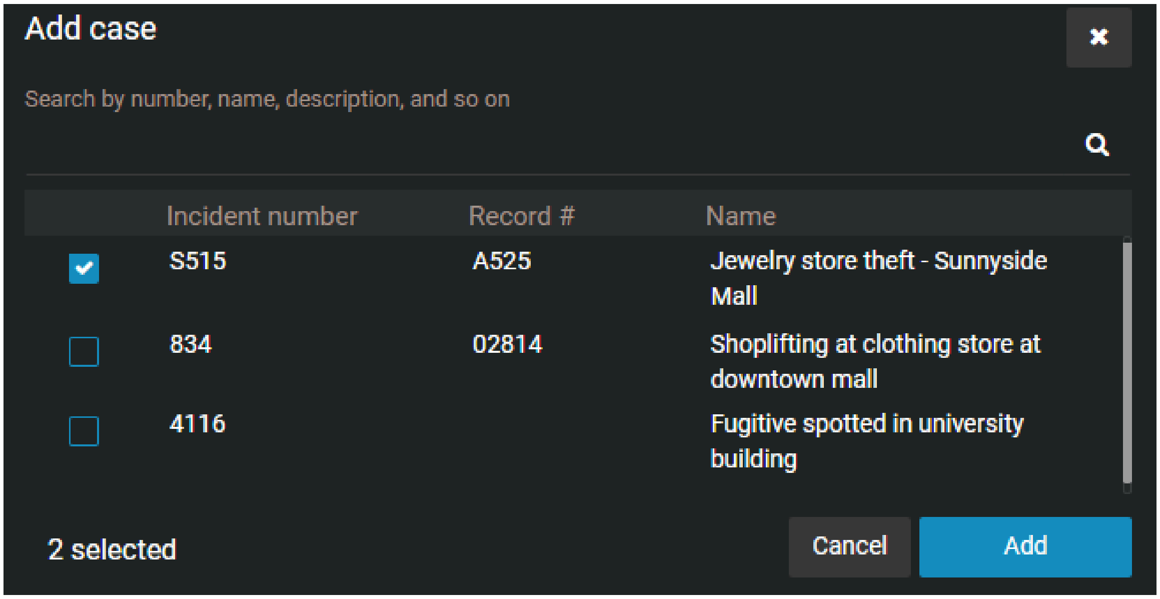
Procedure

1 Open an existing file.

2 In the *General* section of the *File edit* page, next to **Associated cases** click ➕ **Add**.

3 In the *search* box, type a case name, and press **Enter** or click the **search** button (🔍).

4 Select the check box for the case that you require and click **Add**.



Add case

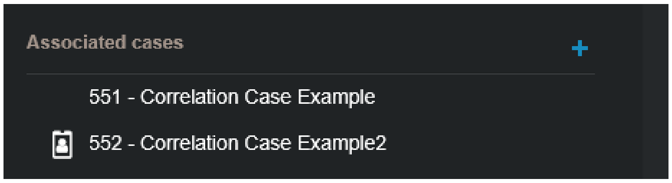
Search by number, name, description, and so on

	Incident number	Record #	Name
☑	S515	A525	Jewelry store theft - Sunnyside Mall
□	834	02814	Shoplifting at clothing store at downtown mall
□	4116		Fugitive spotted in university building

2 selected

5 (Optional) Click ❌ **Remove** to remove any cases that are no longer required.

6 Click **Save**.



Associated cases

551 - Correlation Case Example

552 - Correlation Case Example2

NOTE: Any automatically associated cases are also displayed in the **Associated cases** section.

The file is now associated with the case or cases. Users assigned to the case can view, edit, or download the file.

NOTE: There is a default maximum of 50 manual case associations and 50 automatic case associations.

Linking files to another case

You can link multiple files already associated with one case to another in Clearance.

Before you begin

Upload files to a case.

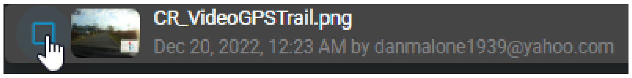
What you should know

- Files can be associated with multiple cases.
- Folders containing files can be linked from one case to another.
- Files that you link from one case to another remain associated with the original case.
- Linking a file to another case does not copy the file. Instead, the same file becomes associated with another case.

Procedure

1 From a case, navigate to the *Files* section.

2 Select the files or folders that you want to link with another case by clicking the box next to the file name.



CR_VideoGPSTrail.png
Dec 20, 2022, 12:23 AM by danmalone1939@yahoo.com

NOTE: You can link up to 50 files from one case to another at one time.

3 Click **Link to**.
The *Link to new case* window opens.

4 Select the case that you want to link the files with.

5 Click **Add**.
The files are now also associated with the other case.

Example

After you finish

(Optional)

- Protect cases from deletion.
- Download files from a case.

Searching evidence by device assignment

To find all evidence recorded by a user associated with a device, you can search evidence by device assignment. You can also use date or time range filters to search evidence by device assignment within a specified time range.

What you should know

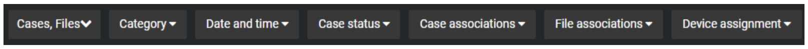
- Thumbnail previews are displayed in search results for the following files: BMP, PNG, JPEG, GIF, Icon, and MP4.
- When you select **Specific dates**, any cases or files that have at least 1 minute of their duration within the time range are displayed.
- All media recorded using an assigned device is tagged and searchable.

Procedure

1 Click the **Files** tab or **Search** tab.

2 Click the **Search Criteria** toolbar menu.

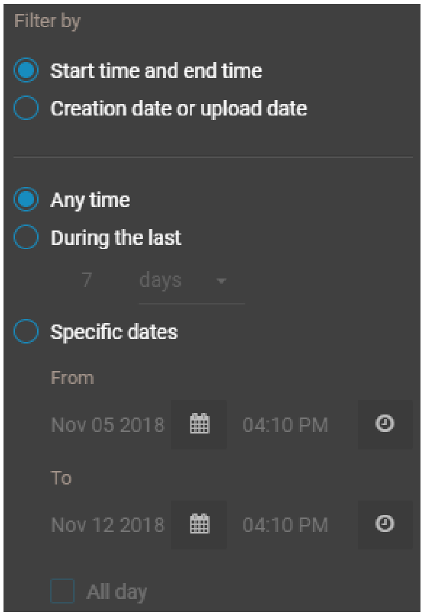
3 To filter your search for files, select **Files**.



NOTE: The Device assignment filter is only available when searching files.

4 (Optional) Filter your search by category: click **Category** and select one or multiple categories from the drop-down menu.

5 (Optional) To filter by date or time, click **Date and time** and select the options that you require.



Filter by

● Start time and end time
○ Creation date or upload date

● Any time
○ During the last
7 days
○ Specific dates
From
Nov 05 2018 04:10 PM
To
Nov 12 2018 04:10 PM
□ All day

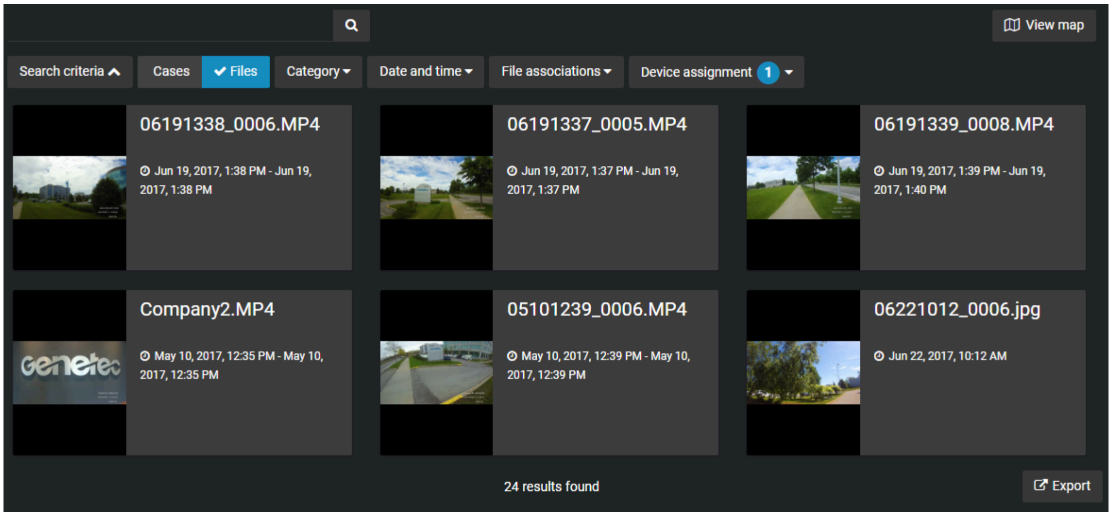
- Select **Any time** to search all time ranges.
- Select **Specific dates** to search a specific time range. Enter a date and time, or use the calendar and date icons to select a specific time range.
- Select **All day** to search from 12:00 am to 11:59 pm for the selected days.

6 (Optional) Filter your search by file associations: click **File associations** and select **Linked**, **Unlinked**, or both.

7 To filter by device assignment, click **Device assignment**.

a) In the **Search** field, type a user name or email address, and press Enter or click the **Search** button (🔍).

b) Select a user and click **Confirm**.



06191338_0006.MP4
Jun 19, 2017, 1:38 PM - Jun 19, 2017, 1:38 PM

06191337_0005.MP4
Jun 19, 2017, 1:37 PM - Jun 19, 2017, 1:37 PM

06191339_0008.MP4
Jun 19, 2017, 1:39 PM - Jun 19, 2017, 1:40 PM

Company2.MP4
May 10, 2017, 12:35 PM - May 10, 2017, 12:35 PM

05101239_0006.MP4
May 10, 2017, 12:39 PM - May 10, 2017, 12:39 PM

06221012_0006.jpg
Jun 22, 2017, 10:12 AM

24 results found

The search filter displays all evidence files created by devices that were assigned to the selected user. Files are also filtered by a date or time range, if specified.

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.

▶

Related Topics

Uploading files to cases on page 165

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.

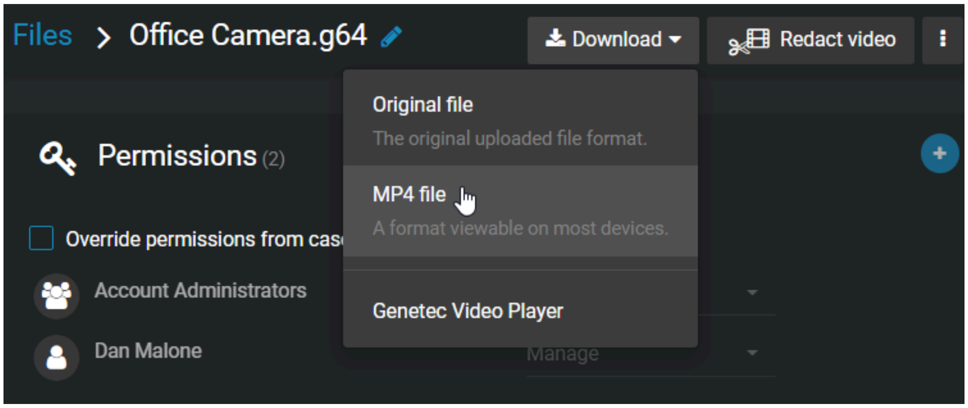
Procedure

To download a file:

1 Open an existing file.

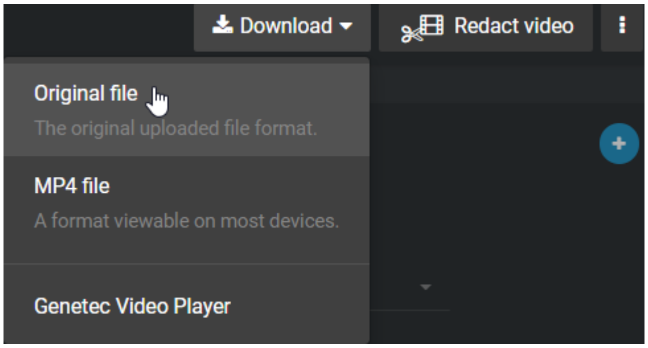
2 Click **Download**.

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


Files > Office Camera.g64
Download
Redact video
Original file
The original uploaded file format.
MP4 file
A format viewable on most devices.
Genetec Video Player
Permissions (2)
Override permissions from cas
Account Administrators
Dan Malone
Manage

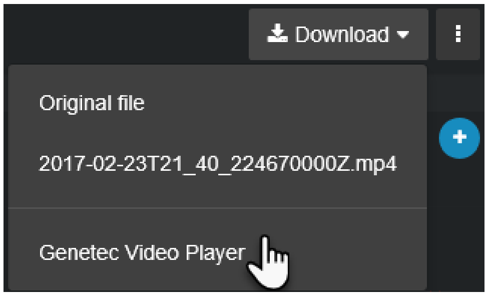
a) (Optional) Click **Original file** when you want to download the file in its original format, if the file is not an MP4.

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


Download
Redact video
Original file
The original uploaded file format.
MP4 file
A format viewable on most devices.
Genetec Video Player

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.

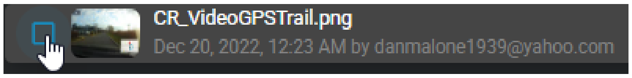


NOTE: If a malware scan flags a file as suspicious, then only users included in the *Download malicious files* security policy can download it. For more information on this security policy, refer to Security policy definitions list on page 63.

To download a file from a case:

1 Navigate to a case.

2 Select the files that you want to download by clicking the box next to the file name.



3 Click **Download**.

Example

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

▶

Related Topics

Reviewing media on page 168
Viewing G64 or G64x video files in the Genetec™ Video Player on page 280

Changing access policies for files

After a file has been uploaded in the system, you can select which users and groups have access to the file, and which permission levels they have.

What you should know

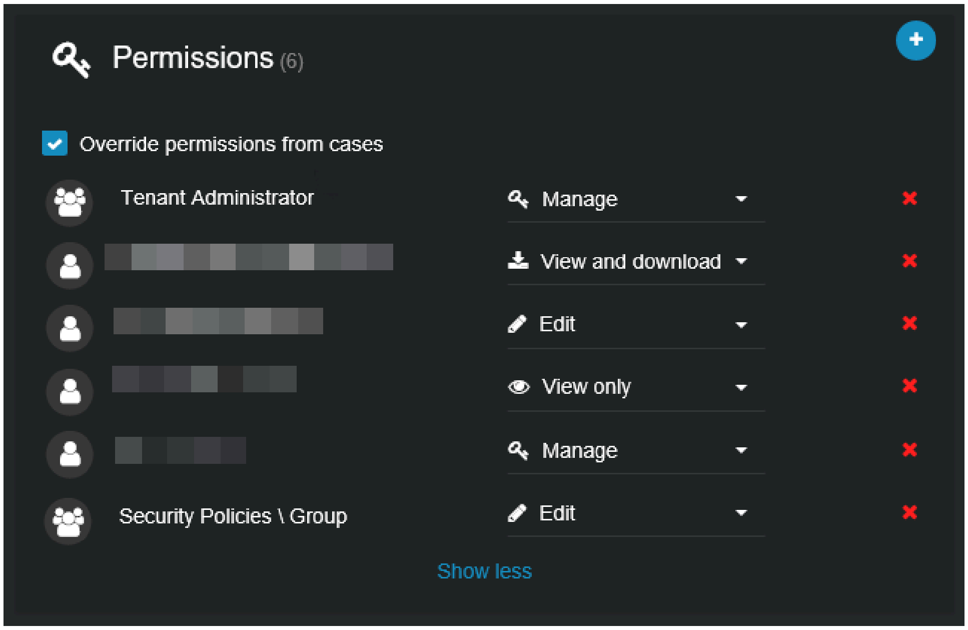
By default, a file inherits the access policy of the case with which it is associated. If a file is associated with multiple cases, user permission levels on the file are defined by the highest ranking permission level from those cases.

- If the file is not associated with a case, the access policy for the file is taken from the default *Security policies* configuration.
- You can only change the access policy of a file if you have *Manage* permission level on the file.
- Users with *View only* permissions on the case will be unable to view PDF files included in the case. If you want a user to view a PDF file, assign them *View and download* permissions on the file.

Procedure

1 Open an existing file.

2 In the **Permissions** section, select **Override permissions from cases**.



Permissions (6)

☑ Override permissions from cases

Tenant Administrator	Manage
[redacted]	View and download
[redacted]	Edit
[redacted]	View only
[redacted]	Manage
Security Policies \ Group	Edit

3 To add users or groups, do the following:

a) Click + > **Add users** .

b) Select which users or groups you want to grant access to, and click **Add**.

4 From the drop-down list next to the users or groups, grant them **View only**, **View and download**, **Edit**, or **Manage** permission level on the file.

5 To remove a user or group, click ✖ next to their name.

6 Click **Save**.

The access policy of the file is overwritten from the access policies of the cases. If you add a user to one of the file's associated cases, the user does not automatically have access to the file. You must manually add that user to 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.

▶

Related Topics

Uploading files to cases on page 165

Protecting files from deletion

To keep files longer than the specified retention policy, you can place an indefinite hold on a file by using the **Protect from deletion** option.

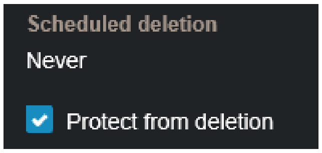
What you should know

- Users must have *manage* permission to protect files associated with a case.
- Users must also be included in the *Protect or unprotect cases and files from deletion* security policies list. If there are no users on that list, then all users with *manage* permissions have the ability to protect or unprotect cases and files.

Procedure

1 Open an existing file.

2 In the *General* section of the *File edit* page, select the **Protect from deletion** check box.



Scheduled deletion

Never

☑ Protect from deletion

3 Click **Save**.

The file is now protected from manual deletion by a user or automatic deletion by any retention policies that are in effect.

Deleting files

To remove any digital evidence that is linked to an incident, you can delete the associated files.

What you should know

You can manually delete a case or file even when there is a *retention policy* active for the case category. The retention period for the case begins to count down when the case is closed and deletes associated files automatically after the retention period (count down) is reached.

IMPORTANT: Users must be in the **Delete cases and files** security policies list. Users must also have *manage* permission level to delete files associated with a case.

Procedure

1 Open an existing file.

2 Click the More icon (⋮) next to **Redact video**.

3 Click **Delete File**.

A confirmation message is displayed. Are you sure you want to delete this file?

4 (Optional) If the file has been protected, the **Delete File** option is unavailable and a warning message is displayed: This file is protected from deletion. You must clear the Protect from deletion check box to delete this file.

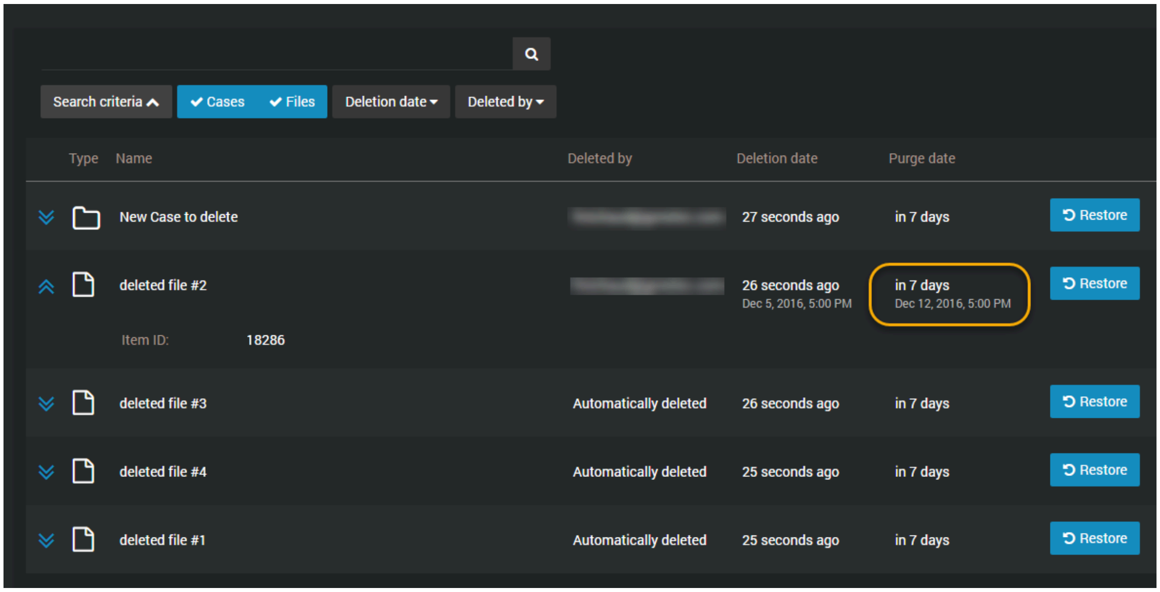
a) Clear the **Protect from deletion** check box.

b) Click **Delete** again.

The deleting status is displayed. After the file is deleted, you are returned to the *Search* page.

The deleted file is marked for deletion and put in the recycle bin.

Example



Type	Name	Deleted by	Deletion date	Purge date
	New Case to delete	[redacted]	27 seconds ago	in 7 days
	deleted file #2	[redacted]	26 seconds ago Dec 5, 2016, 5:00 PM	in 7 days Dec 12, 2016, 5:00 PM
	Item ID: 18286			
	deleted file #3	Automatically deleted	26 seconds ago	in 7 days
	deleted file #4	Automatically deleted	25 seconds ago	in 7 days
	deleted file #1	Automatically deleted	25 seconds ago	in 7 days

After you finish

You can view or search in the recycle bin to understand when the file will be purged from the recycle bin. You can also view all active retention policies. When the purge occurs, the file is permanently deleted from the Clearance database.

Related Topics

Setting the retention period for cases and files on page 40
Viewing the audit trail history of files on page 191

Restoring files

To restore any digital evidence that is linked to an incident, you can restore the associated files.

What you should know

IMPORTANT: Users must be in the **Restore cases and files from the recycle bin** security policy list. Users must also have *manage* permission level to restore files. If the list is empty everyone can restore.

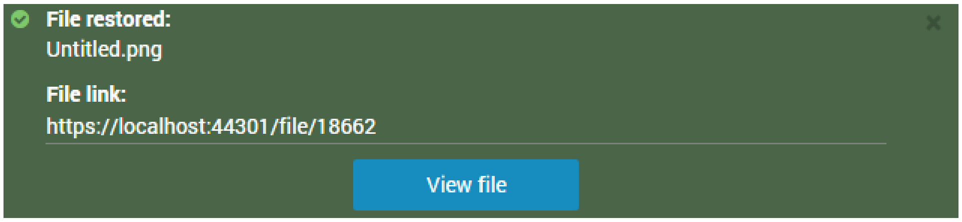
Procedure

1 Open the recycle bin.

2 Select the file that you want and click **Restore**.
A confirmation message is displayed.
NOTE: Any restored files are automatically set to **Protect from deletion**.

Are you sure you want to restore this file?

3 Click **Restore File**.
When the file is restored, a file restored message is displayed and a File link web address is also shown.



File restored:
Untitled.png

File link:
https://localhost:44301/file/18662

4 (Optional) Click **View file** to open the restored file.

Related Topics

Viewing the audit trail history of files on page 191

Viewing the audit trail history of files

You can investigate the complete activity history of a file, such as who made changes and when, by viewing the audit trail of the file.

Before you begin

To view the audit trail of a file, you must have the *Manage* permission level on the file. Audit trail information is never displayed to guest users with *Manage* permission level.

What you should know

The audit trail of a file tracks users who uploaded, viewed, downloaded, edited, protected, deleted, or restored the file, and when these actions were performed.

Procedure

To view the audit trail history of a file:

1 Open an existing file.

2 Click **More** (⋮)

3 Click **Audit trail**.

4 View the file history.

To download the audit trail report:

1 From the *Audit trail* page, click **Create audit trail report**.

2 Review the report and click **Download**.

Example

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

▶

Related Topics

About Clearance information security on page 164

Deleting files on page 188

Restoring files on page 190

Changing access policies for cases on page 112

10

Managing video requests

Learn how to employ video requests in Clearance.

This section includes the following topics:

- "Registry and video request overview" on page 193
- "Searching for cameras of interest" on page 195
- "Requesting video" on page 199
- "Inviting guests to submit video requests" on page 203
- "Reviewing video requests" on page 206
- "Approving video requests" on page 209
- "Canceling a video request" on page 213

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:

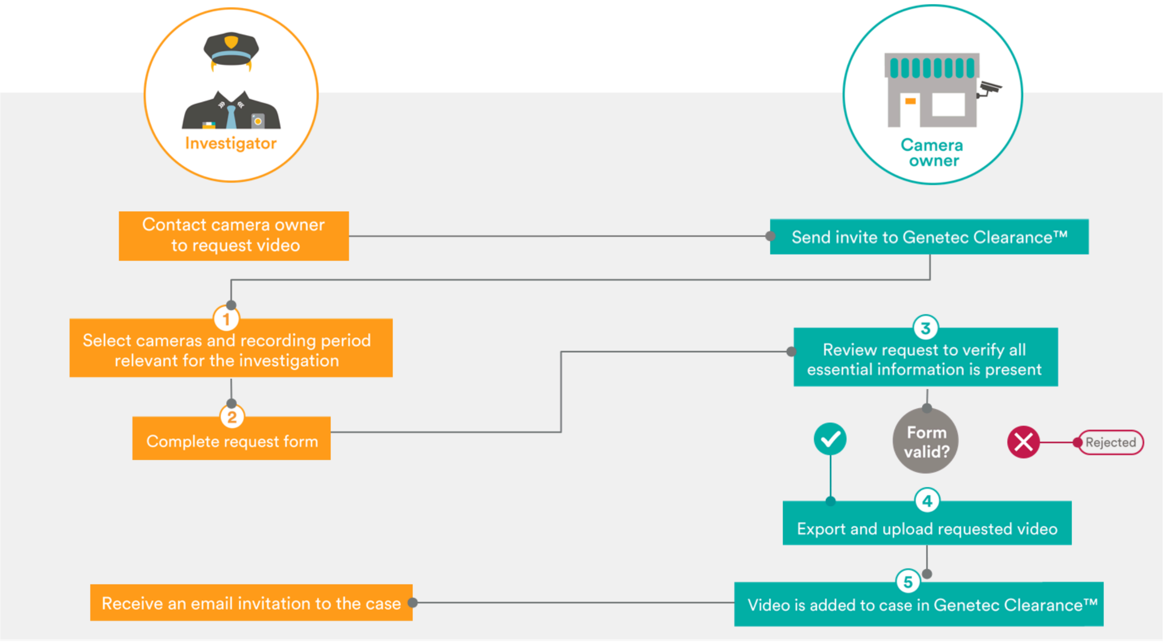
- Share the list of fixed and vehicle-based cameras in your Security Center system so that users can submit video requests.

  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 on page 250.
- 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.


Investigator
Camera owner
Contact camera owner to request video
Send invite to Genetec Clearance™
1
Select cameras and recording period relevant for the investigation
2
Complete request form
3
Review request to verify all essential information is present
Form valid?
Rejected
4
Export and upload requested video
5
Receive an email invitation to the case
Video is added to case in Genetec Clearance™

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

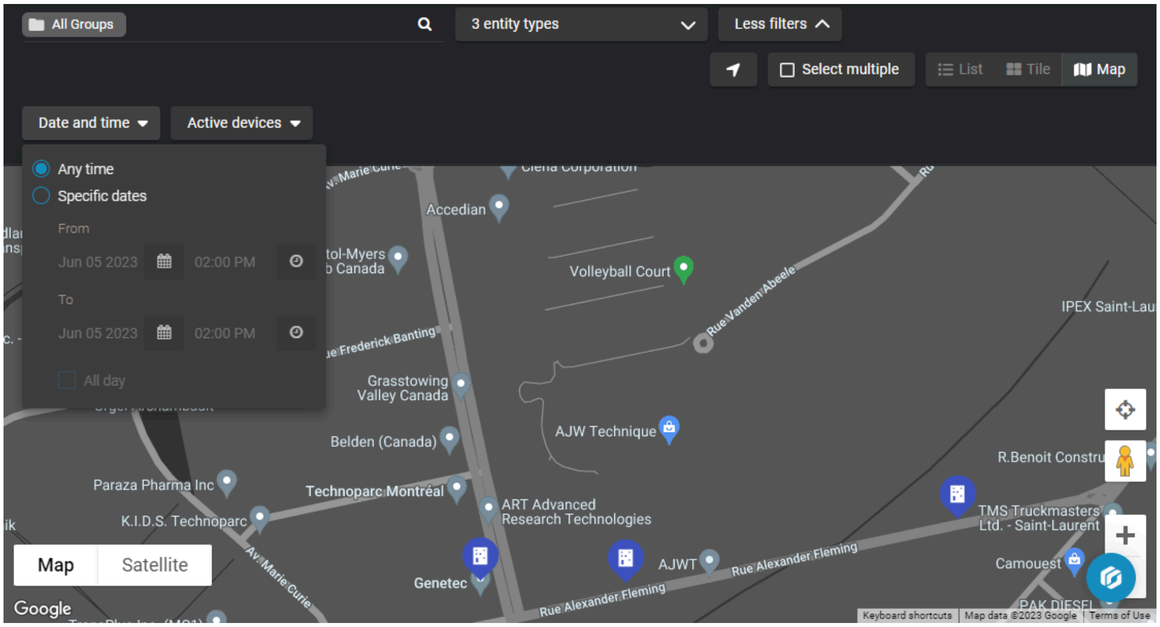
- Use a view that suits your search criteria:
  - **Map:** Use this view when you do not know the name or location of cameras.
  - **List:** Use this view when you know the names or descriptions of cameras you want to request video from.

Procedure

To search for cameras in the *Map* view:

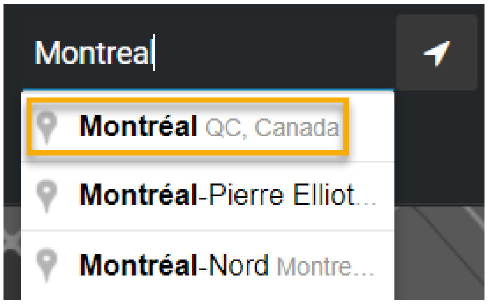
1 Click **Registry** ().

2 Click **View map**.



● Any time
○ Specific dates
From
Jun 05 2023 02:00 PM
To
Jun 05 2023 02:00 PM
□ All day

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



Montreal

- Montréal QC, Canada
- Montréal-Pierre Elliot...
- Montréal-Nord Montre...

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.

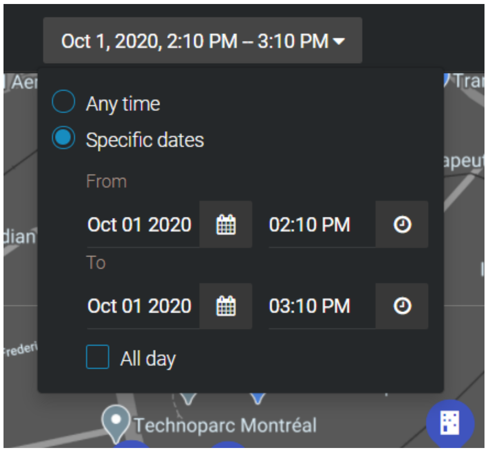
7 (Optional) Filter for cameras, participants, vehicles, or all three.

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.



Oct 1, 2020, 2:10 PM – 3:10 PM

○ Any time
● Specific dates

From
Oct 01 2020 02:10 PM

To
Oct 01 2020 03:10 PM

□ All day

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** (➤).

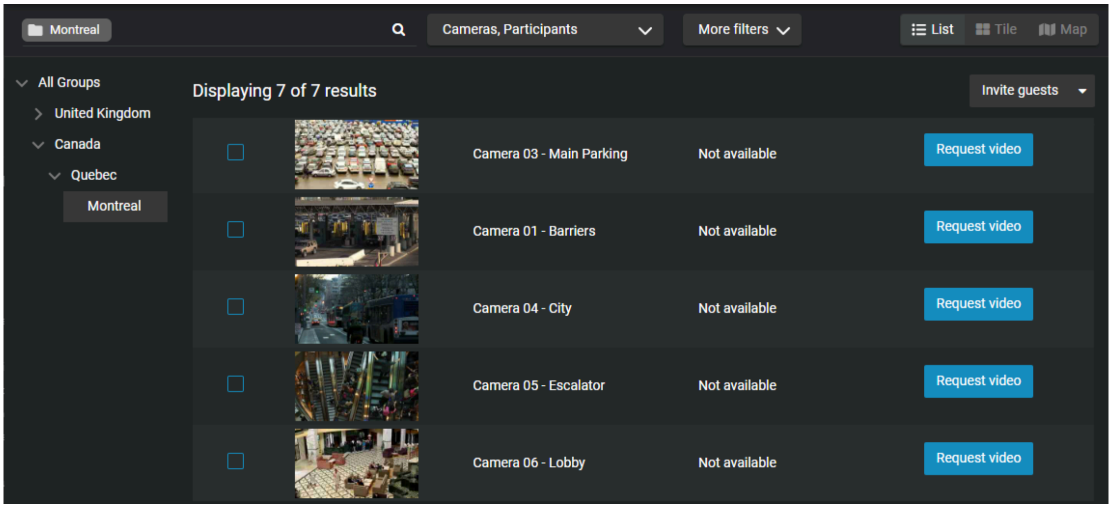
12 To select multiple cameras from the map:

- 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** (▭).

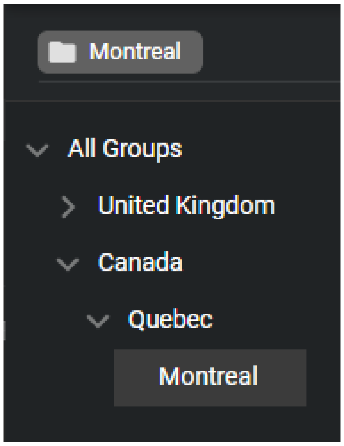
2 Click **List view** (☰).



Displaying 7 of 7 results

□	Camera 03 - Main Parking	Not available	Request video
□	Camera 01 - Barriers	Not available	Request video
□	Camera 04 - City	Not available	Request video
□	Camera 05 - Escalator	Not available	Request video
□	Camera 06 - Lobby	Not available	Request video

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.

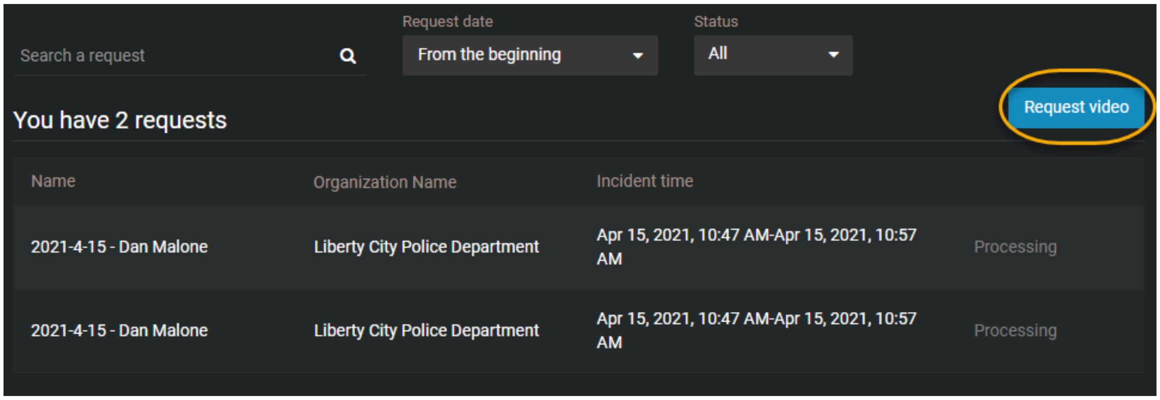
What you should know

- 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**.



Request date: From the beginning

Status: All

You have 2 requests

Name	Organization Name	Incident time	
2021-4-15 - Dan Malone	Liberty City Police Department	Apr 15, 2021, 10:47 AM-Apr 15, 2021, 10:57 AM	Processing
2021-4-15 - Dan Malone	Liberty City Police Department	Apr 15, 2021, 10:47 AM-Apr 15, 2021, 10:57 AM	Processing

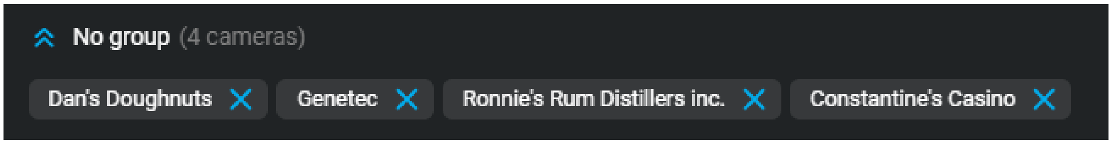
2 From the **Request video** menu, select a type of request form.

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

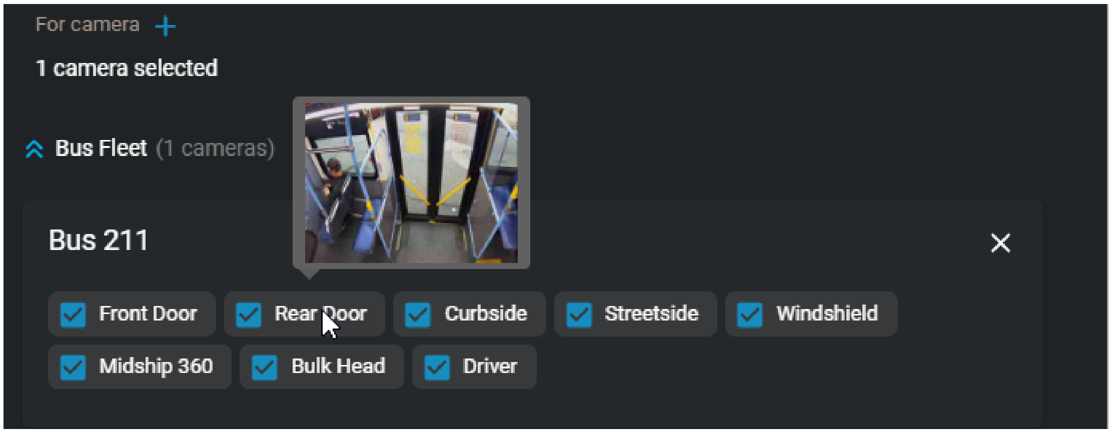
- Click **Add** (✚) to associate the request with a camera, vehicle, or participant from the list.
- Click **Map** (🗺) to select the geographical location you need video from.
  - Click **Enter location** (➤) to locate a specific address on the map.
  - Click **Rectangle selection** (⬚) to select multiple 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.

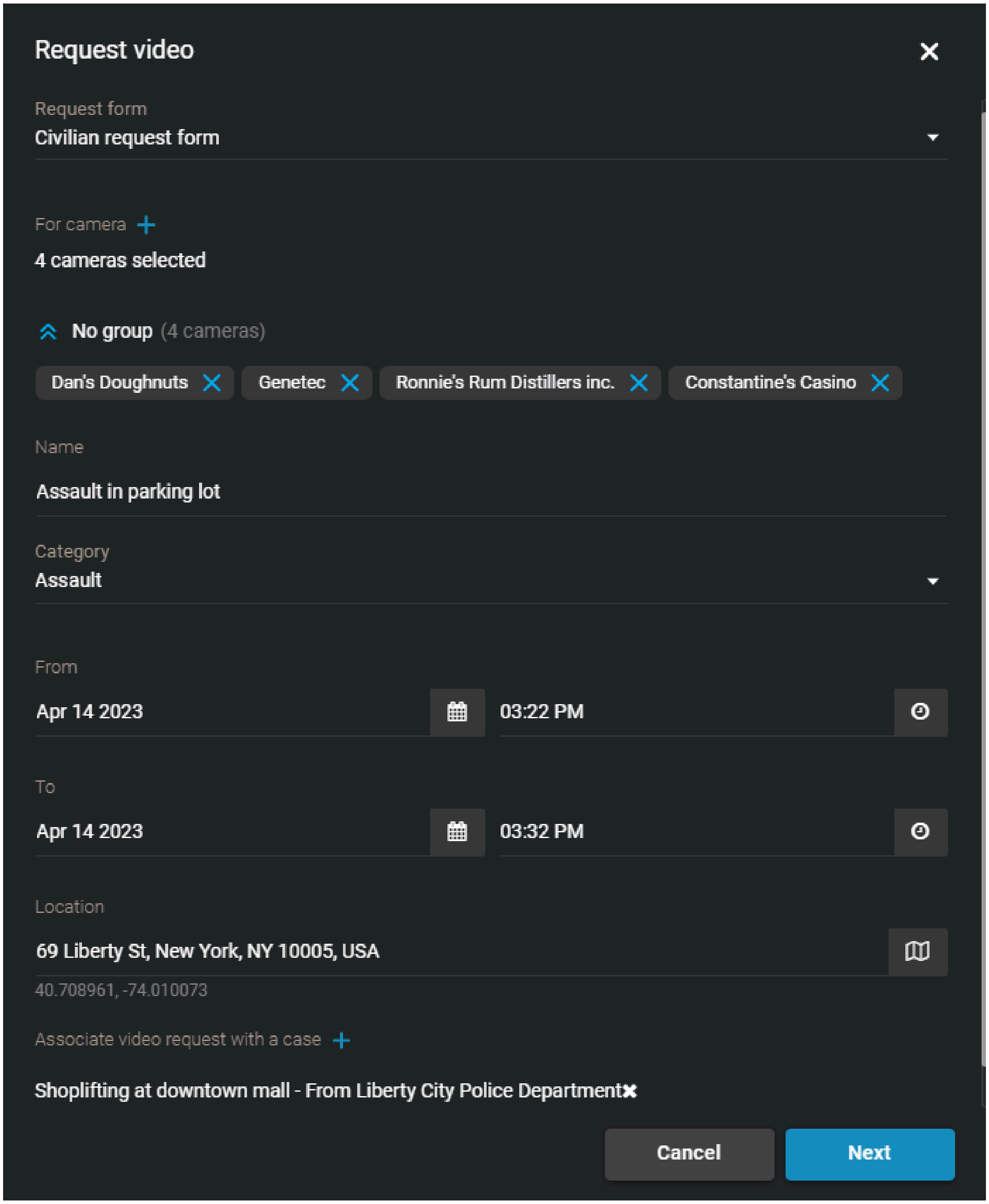
5 Choose a category for the request.

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.



Request video

Request form
Civilian request form

For camera +
4 cameras selected

No group (4 cameras)

Dan's Doughnuts ✕ | Genetec ✕ | Ronnie's Rum Distillers inc. ✕ | Constantine's Casino ✕

Name
Assault in parking lot

Category
Assault

From
Apr 14 2023 03:22 PM

To
Apr 14 2023 03:32 PM

Location
69 Liberty St, New York, NY 10005, USA
40.708961, -74.010073

Associate video request with a case +
Shoplifting at downtown mall - From Liberty City Police Department✖

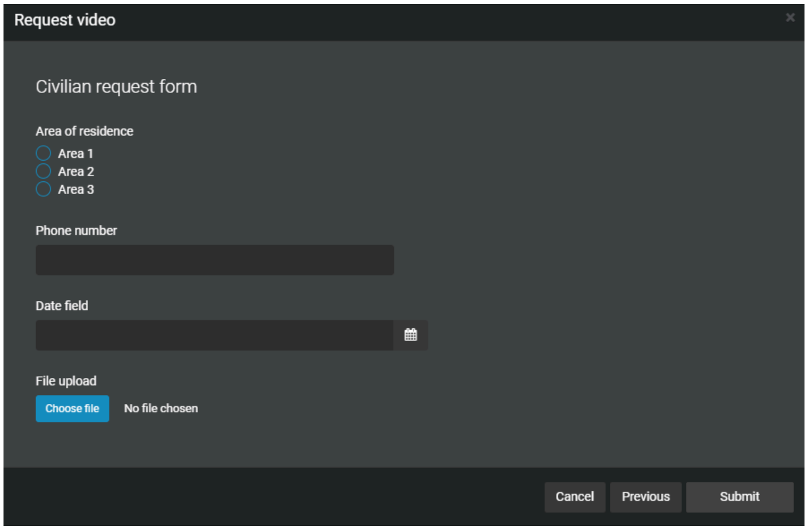
NOTE:

- 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.



Request video

Civilian request form

Area of residence

○ Area 1
○ Area 2
○ Area 3

Phone number

Date field

File upload

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.

Inviting guests to submit video requests

For guest users to submit video requests, a user included in the *Manage and invite requesters* video request policy must invite them to submit video requests.

Before you begin

Define your video request policies.

What you should know

- Only users included in the *Manage and invite requesters* video request policy can invite guest users to submit video requests.

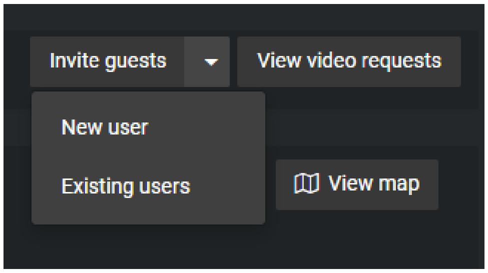
Procedure

To invite a user to submit video requests from the Registry page:

1 Click **Registry** (▭).

2 Click **Invite guests** and choose one of the following:

- New user
- Existing users

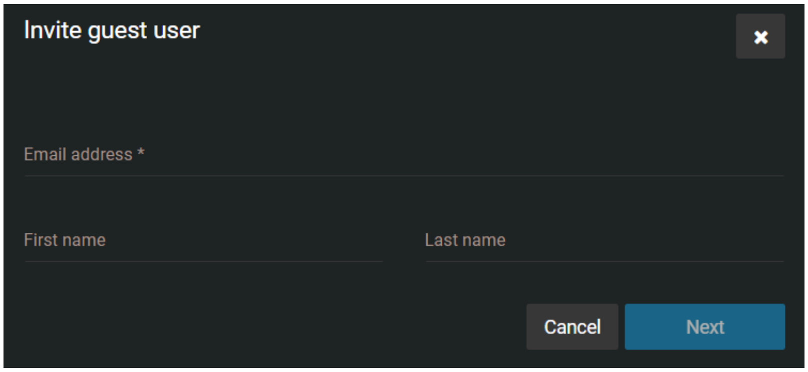


3 If you selected new user, complete the following fields:

a) Enter an email address.

b) (Optional) Enter a first name.

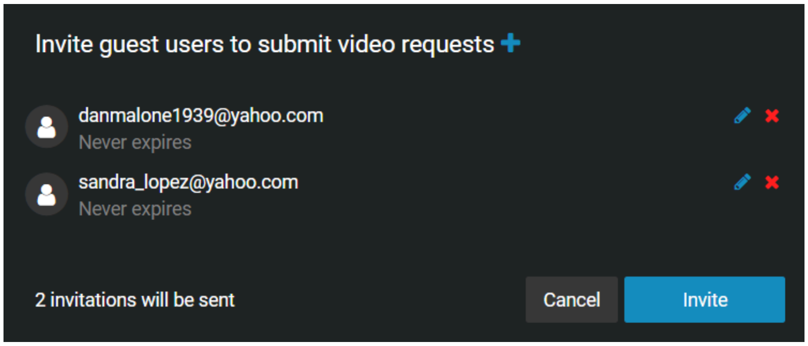
c) (Optional) Enter a last name.



d) Click **Next**.

e) (Optional) Click **Edit** (✎) to modify the expiration date for each invitation.

f) (Optional) Click **Add** (+) to invite additional new or existing users.



danmalone1939@yahoo.com
Never expires

sandra_lopez@yahoo.com
Never expires

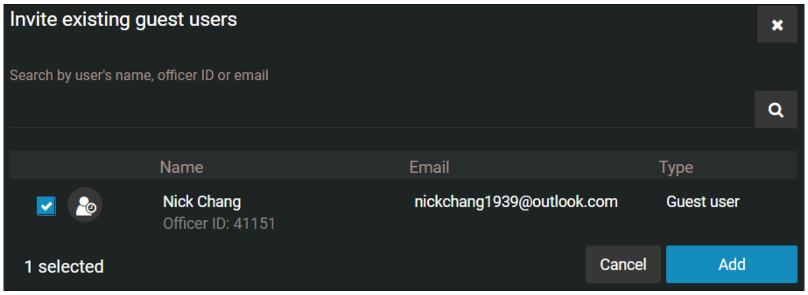
2 invitations will be sent

g) Click **Invite** to send the guest user invitation.

4 If you selected existing users, do the following:

a) In the *Invite existing guest users* dialog, enter the email address or name of the guest user you want to invite, and click **Search** (🔍).

b) Select the users that you require from the list and click **Add**.


Invite existing guest users
✖
Search by user's name, officer ID or email
Cancel
Add

	Name	Email	Type
☑	Nick Chang Officer ID: 41151	nickchang1939@outlook.com	Guest user

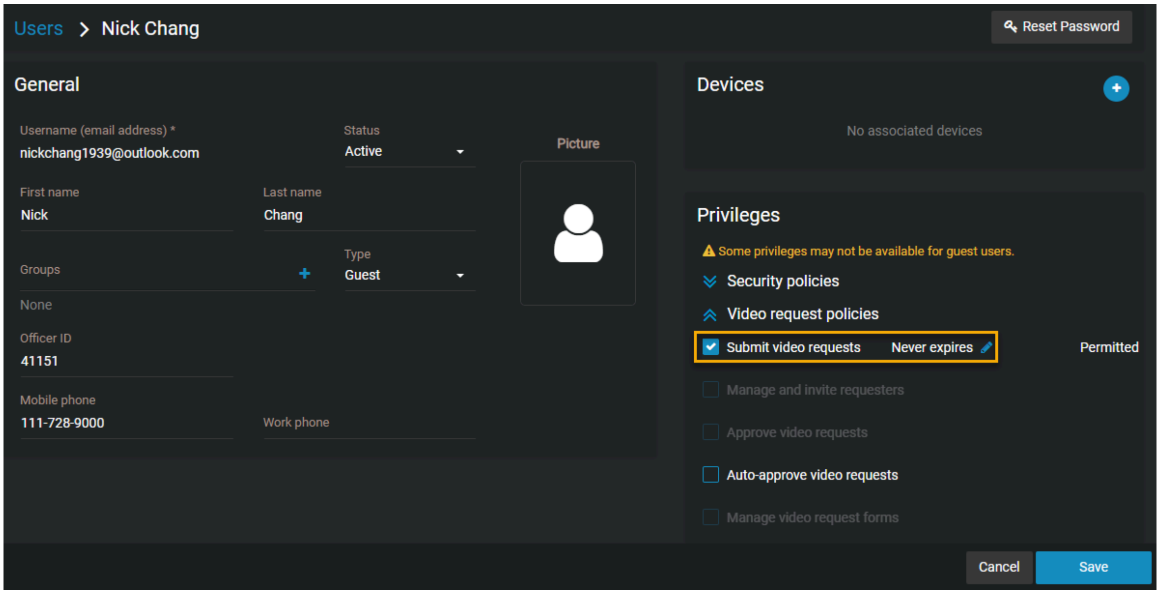
1 selected

To invite a guest user to submit video requests from the Configurations page:

1 Click **Configurations** > **Users**.

TIP: Use the search field to find a specific guest user in a long list.

2 In the *Privileges* section, select the **Submit video requests** check box.



Users > Nick Chang

Reset Password

General

Username (email address) *: nickchang1939@outlook.com

Status: Active

First name: Nick

Last name: Chang

Groups: None

Type: Guest

Officer ID: 41151

Mobile phone: 111-728-9000

Work phone:

Picture

Devices

No associated devices

Privileges

⚠ Some privileges may not be available for guest users.

Security policies

Video request policies

☑ Submit video requests Never expires ✎ Permitted

□ Manage and invite requesters

□ Approve video requests

□ Auto-approve video requests

□ Manage video request forms

Cancel Save

3 (Optional) Click **Edit** (✎) to modify the expiration date.

a) Clear the **Never** check box and follow the on-screen prompts.

b) Click **Modify** to confirm your changes.

4 Click **Save**.

The guest user is now authorized to submit video requests.

Example

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

Reviewing video requests

To perform an audit or check the history of video requests, you can review video requests using search filters for request date and status.

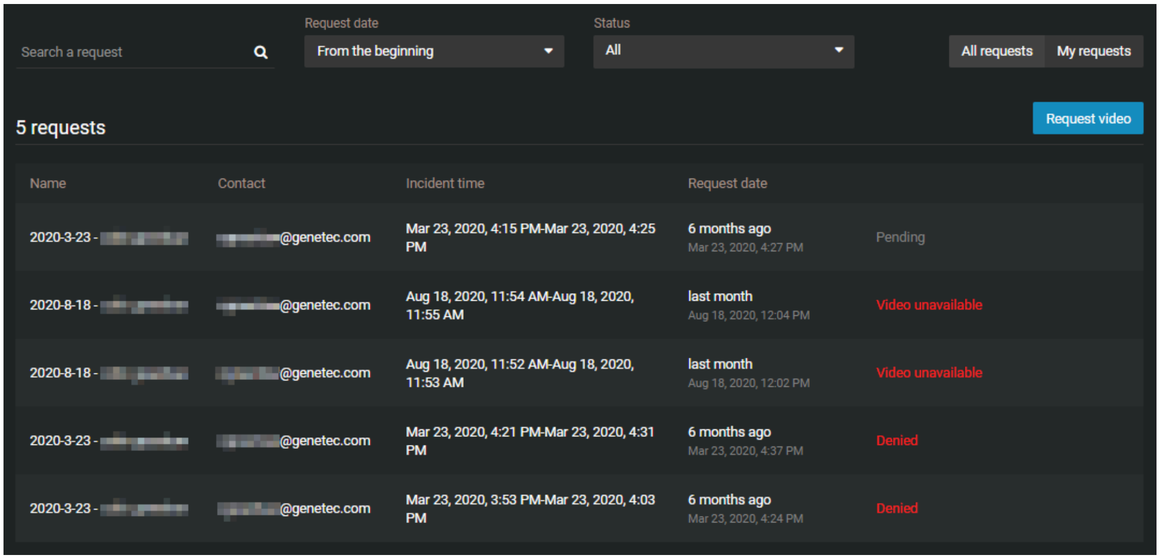
What you should know

Only a user with *Approve video requests* permissions can audit all video requests and check their history.

Procedure

To review all video requests:

1 Click **Requests** (▣).



Request date: From the beginning

Status: All

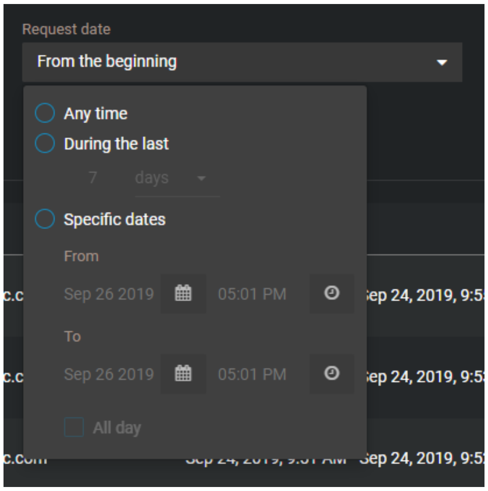
5 requests

Name	Contact	Incident time	Request date	
2020-3-23 - [redacted]	[redacted]@genetec.com	Mar 23, 2020, 4:15 PM-Mar 23, 2020, 4:25 PM	6 months ago Mar 23, 2020, 4:27 PM	Pending
2020-8-18 - [redacted]	[redacted]@genetec.com	Aug 18, 2020, 11:54 AM-Aug 18, 2020, 11:55 AM	last month Aug 18, 2020, 12:04 PM	Video unavailable
2020-8-18 - [redacted]	[redacted]@genetec.com	Aug 18, 2020, 11:52 AM-Aug 18, 2020, 11:53 AM	last month Aug 18, 2020, 12:02 PM	Video unavailable
2020-3-23 - [redacted]	[redacted]@genetec.com	Mar 23, 2020, 4:21 PM-Mar 23, 2020, 4:31 PM	6 months ago Mar 23, 2020, 4:37 PM	Denied
2020-3-23 - [redacted]	[redacted]@genetec.com	Mar 23, 2020, 3:53 PM-Mar 23, 2020, 4:03 PM	6 months ago Mar 23, 2020, 4:24 PM	Denied

2 Click **All requests**.

3 In the search box, enter search criteria to narrow the search results.

4 From the **Request date** list, select the period of requests that you are looking for.



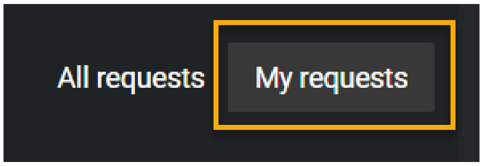
5 Use the **Status** list options to filter results:
   - **All:** Display all video requests.
   - **Pending:** Display requests waiting for review and approval.
   - **Processing:** Display requests that have been approved and are in the process of being uploaded.
   - **Completed:** Display requests that have been approved and uploaded.
   - **Partially completed:** Display requests where multiple videos have been requested and some of the uploads are still being processed.
   - **Denied:** Display requests that were denied.
   - **Canceled:** Display pending requests that were canceled by the requester.
   - **Video unavailable:** Display requests that have been approved but video for the specified period was unavailable. For example: camera offline, archived video not available.

6 Select a video request from the list and review the details:
   - **Incident time:** The time period that was requested.
   - **Comments:** An approver can add a comment to describe why a request was approved or denied, or additional details related to the request.
   - **Associated case:** Cases associated with the video request.
   - **Camera to review:** Shows a list of cameras from which video has been requested. Also displays whether or not the camera is part of a Security Center integration.
   - **Request details:** Shows details such as the overseeing department, incident or cause number, subpoena, and date needed by.

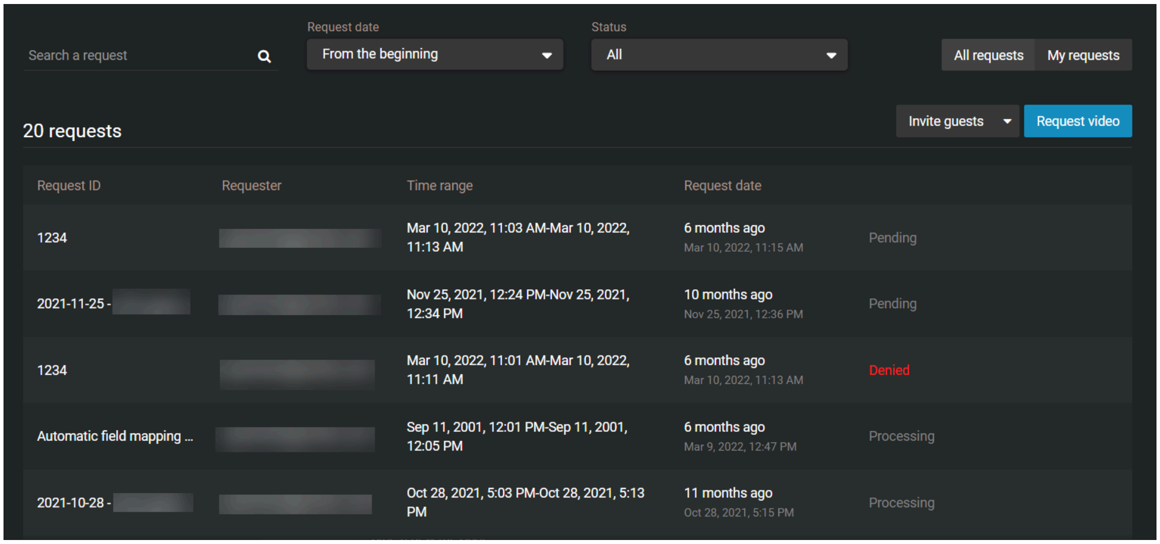
To review My requests:

1 Click **Requests** (📹).

2 Click **My requests**.



NOTE: The **My requests** button is only displayed for users with *Approve video requests* permission. Users who lack the *Approve video requests* permission are automatically shown only their requests.



Request date: From the beginning

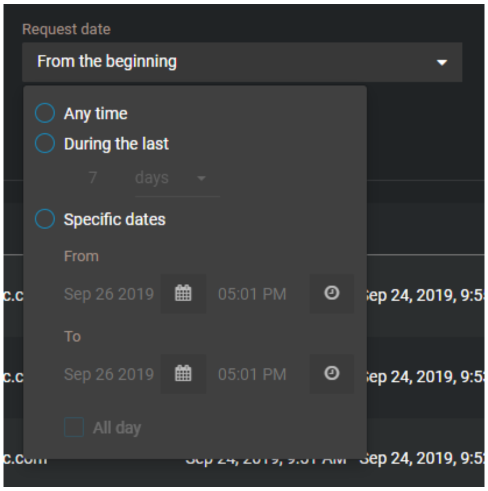
Status: All

20 requests

Request ID	Requester	Time range	Request date	
1234	[redacted]	Mar 10, 2022, 11:03 AM-Mar 10, 2022, 11:13 AM	6 months ago Mar 10, 2022, 11:15 AM	Pending
2021-11-25 - [redacted]	[redacted]	Nov 25, 2021, 12:24 PM-Nov 25, 2021, 12:34 PM	10 months ago Nov 25, 2021, 12:36 PM	Pending
1234	[redacted]	Mar 10, 2022, 11:01 AM-Mar 10, 2022, 11:11 AM	6 months ago Mar 10, 2022, 11:13 AM	Denied
Automatic field mapping ...	[redacted]	Sep 11, 2001, 12:01 PM-Sep 11, 2001, 12:05 PM	6 months ago Mar 9, 2022, 12:47 PM	Processing
2021-10-28 - [redacted]	[redacted]	Oct 28, 2021, 5:03 PM-Oct 28, 2021, 5:13 PM	11 months ago Oct 28, 2021, 5:15 PM	Processing

3 In the search box, enter search criteria to narrow the search results.

4 From the **Request date** list, select the period of requests that you are looking for.



Request date

From the beginning

5 Use the **Status** list options to filter results as required.

6 Select a video request from the list and review the details:

7 Review your request details:

   a) Check reviewer comments in any reviewed request if provided.

   b) Check all information that you provided in your request for accuracy.

Example

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

Approving video requests

Before an investigator can access a requested video, you must review and approve the request.

Before you begin

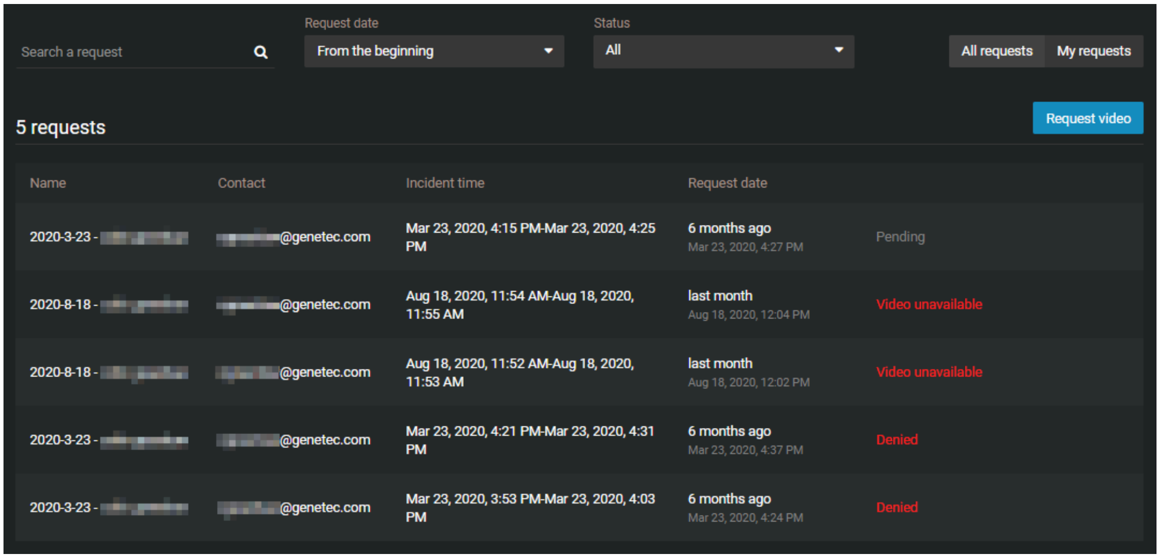
- Define request approvers.
- Review video requests.

What you should know

- Only approvers can approve requests. Approvers are listed in the *Approve video requests* section of the *Video request policies* page.
- When a request is approved, recordings are sent to the user who requested the video.
- Approval happens immediately for users or groups with the *Auto-approve video requests* permission specified on the *Video request policies* page.

Procedure

1 Click **Requests** (📹).



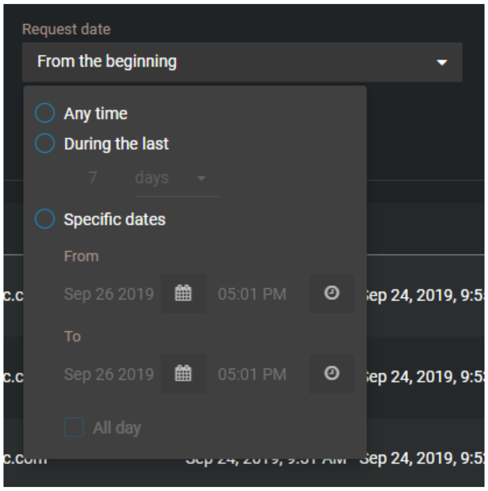
5 requests

Name	Contact	Incident time	Request date	
2020-3-23 - [redacted]	[redacted]@genetec.com	Mar 23, 2020, 4:15 PM-Mar 23, 2020, 4:25 PM	6 months ago Mar 23, 2020, 4:27 PM	Pending
2020-8-18 - [redacted]	[redacted]@genetec.com	Aug 18, 2020, 11:54 AM-Aug 18, 2020, 11:55 AM	last month Aug 18, 2020, 12:04 PM	Video unavailable
2020-8-18 - [redacted]	[redacted]@genetec.com	Aug 18, 2020, 11:52 AM-Aug 18, 2020, 11:53 AM	last month Aug 18, 2020, 12:02 PM	Video unavailable
2020-3-23 - [redacted]	[redacted]@genetec.com	Mar 23, 2020, 4:21 PM-Mar 23, 2020, 4:31 PM	6 months ago Mar 23, 2020, 4:37 PM	Denied
2020-3-23 - [redacted]	[redacted]@genetec.com	Mar 23, 2020, 3:53 PM-Mar 23, 2020, 4:03 PM	6 months ago Mar 23, 2020, 4:24 PM	Denied

2 Click **All requests**.

3 In the search box, enter search criteria to narrow the search results.

4 From the **Request date** list, select the period of requests that you are looking for.



Request date

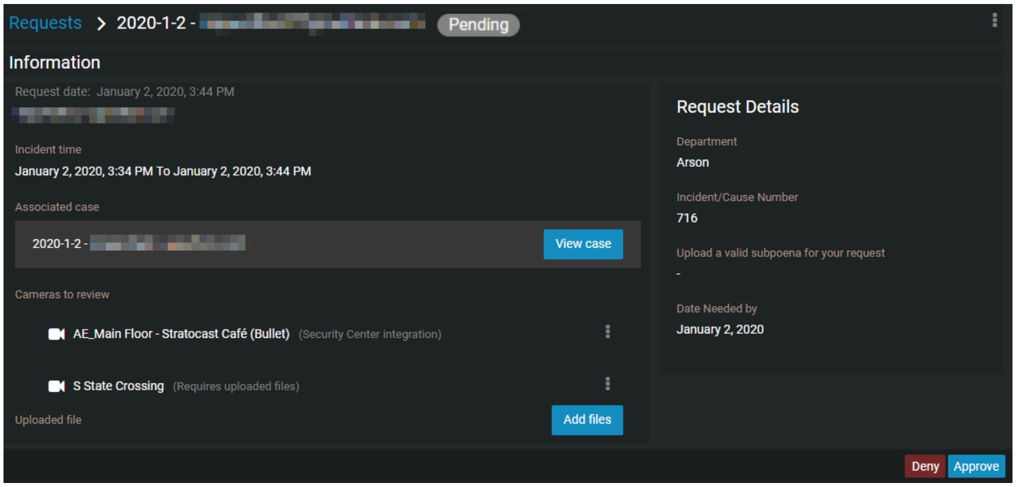
From the beginning

5 To filter requests waiting for review and approval, select **Pending** from the **Status** list.

6 Review a video request.

a) Select a request from the list.

b) Review the details of the request.



Requests > 2020-1-2 - [redacted] Pending

Information

Request date: January 2, 2020, 3:44 PM

[redacted]

Incident time

January 2, 2020, 3:34 PM To January 2, 2020, 3:44 PM

Associated case

2020-1-2 - [redacted]

Cameras to review

AE_Main Floor - Stratocast Café (Bullet) (Security Center integration)

S State Crossing (Requires uploaded files)

Uploaded file

Request Details

Department

Arson

Incident/Cause Number

716

Upload a valid subpoena for your request

-

Date Needed by

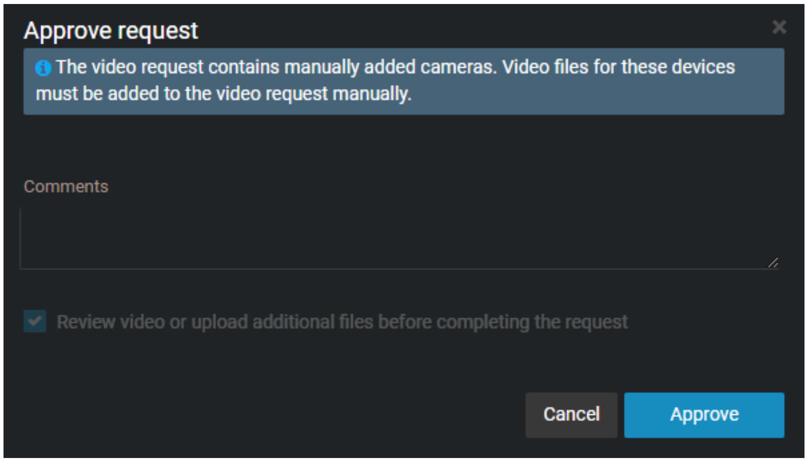
January 2, 2020

c) (Optional) If your request was associated with a case, click **View case** to validate that the correct case has been associated.

d) If the request is valid, click **Approve**.

e) (Optional) Add a comment in the **Comments** field.

f) (Optional) To review the video manually before it is uploaded to the case, select the **Review video or upload additional files before completing the request** check box.



Approve request

The video request contains manually added cameras. Video files for these devices must be added to the video request manually.

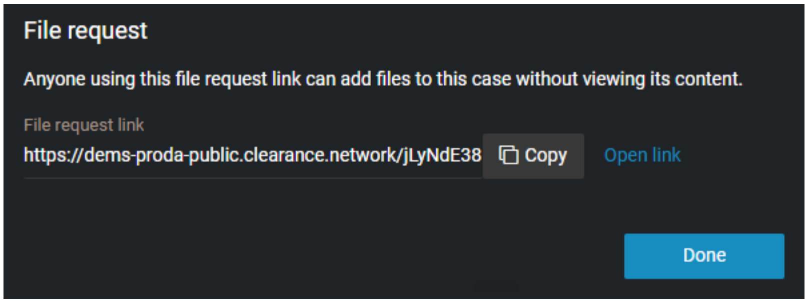
Comments

☑ Review video or upload additional files before completing the request

7 If a camera is not enrolled in the **Registry** or if the video request was not associated with a camera, files must be uploaded manually:

a) Click **Add files**.

b) Copy and paste the link or click **Open link**.



File request

Anyone using this file request link can add files to this case without viewing its content.

File request link

https://dems-proda-public.clearance.network/jLyNdE38

If the request is approved, one of the following happens:

- If you associate the request with a case, the video is automatically added to that case. The access policy for that case remains unchanged after the request is approved.
- If you do not associate the request with a case, a case is automatically created. The case uses the name provided when the request was submitted. The video is uploaded and will include the access policy that was defined in the video request policies.

For more information, see Sharing files using a file request.

c) If there are issues with the request, click **Deny**.

Example

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

Related Topics

About Clearance Plugin for Security Center on page 250

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

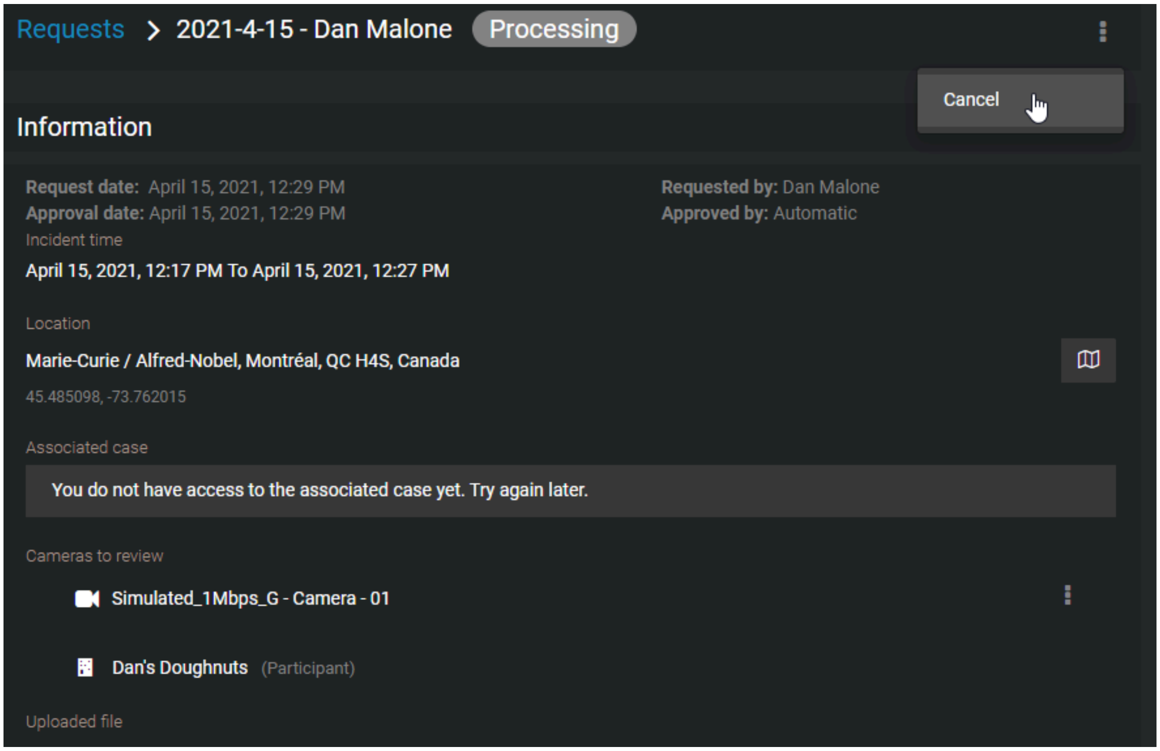
- Only a requester can cancel their request.
- Requests cannot be canceled after they have been approved.

Procedure

1 Click **Requests** (▣).

2 Select the pending request that you want to cancel.

3 Click ⋮.



Request date: April 15, 2021, 12:29 PM
Approval date: April 15, 2021, 12:29 PM
Incident time
April 15, 2021, 12:17 PM To April 15, 2021, 12:27 PM

Requested by: Dan Malone
Approved by: Automatic

Location
Marie-Curie / Alfred-Nobel, Montréal, QC H4S, Canada
45.485098, -73.762015

Associated case
You do not have access to the associated case yet. Try again later.

Cameras to review
Simulated_1Mbps_G - Camera - 01
Dan's Doughnuts (Participant)

Uploaded file

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.

11

Managing video editor content

Learn how to use the video editor in Clearance.

This section includes the following topics:

- "About the video editor" on page 215
- "Trimming video" on page 218
- "Redacting video in Clearance" on page 220
- "Redacting video manually in Clearance" on page 228
- "Redacting audio" on page 234

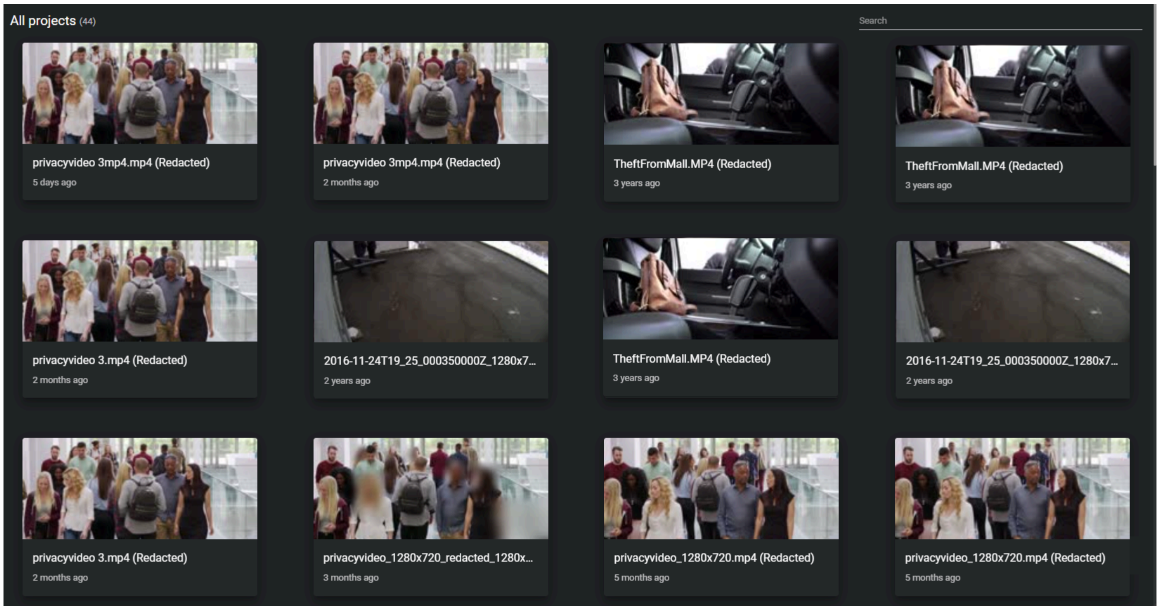
About the video editor

Before sharing a video file with others, you can use the video editor to trim or redact it.

- 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. Use trimming to shorten the recording and keep only the relevant sequence of a longer video to accelerate the review of the recording.
- Redaction in Clearance is the act of obscuring faces, audio, or other sensitive information from supported video files. Use redaction to conceal a persons face, voice, or other sensitive or identifiable information.

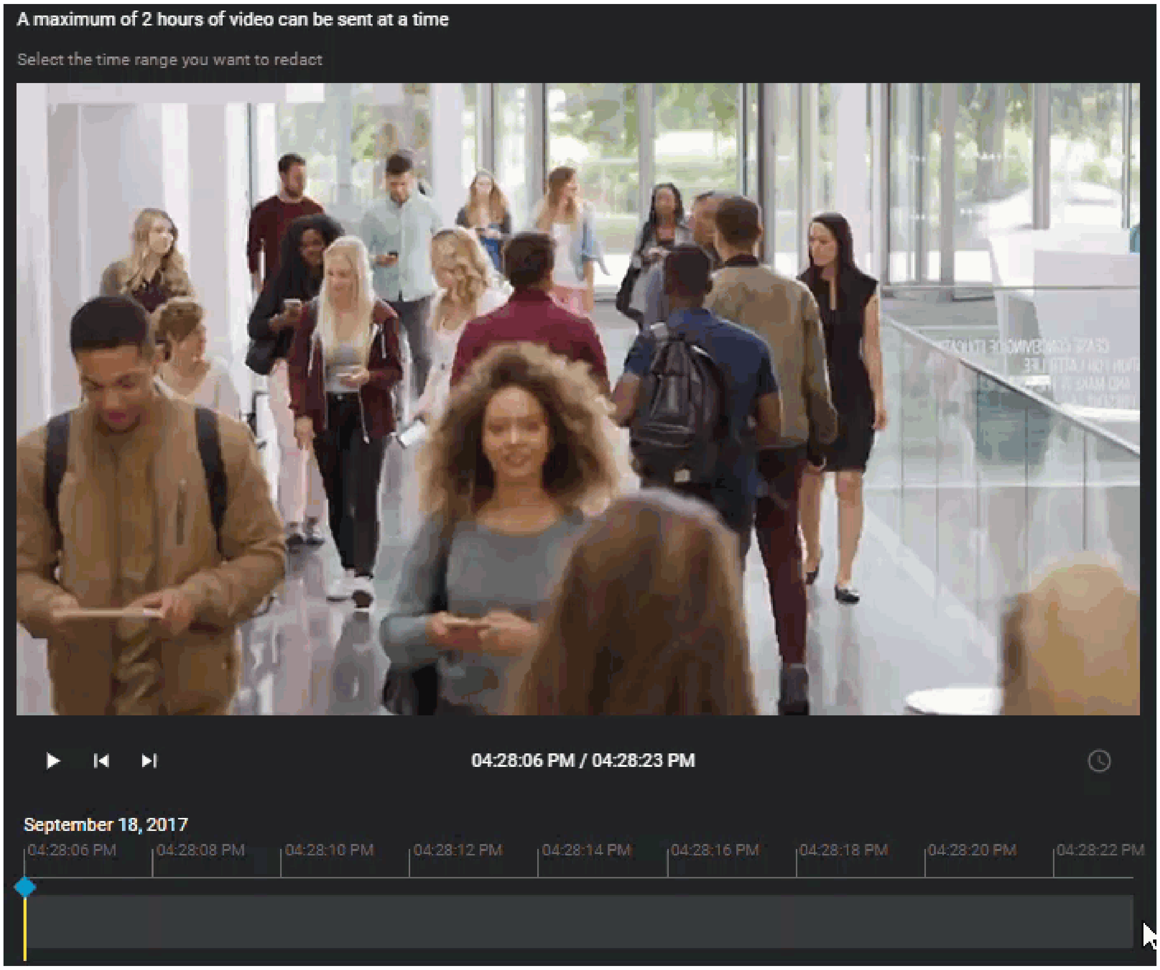
Video editor

- Each user's ongoing redaction and trimming projects are shown in the video editor.
  - If you exit the video while editing or saving a video, it is saved in the list of video editor projects.
  - A copy of the original file is saved when a file is trimmed or redacted. You can create multiple trimmed or redacted versions of the same file.
  - **NOTE:** You can only trim and redact video files that are supported in Clearance. Refer to the list of supported file formats for details.


All projects (44)
Search
privacyvideo 3mp4.mp4 (Redacted)
5 days ago
privacyvideo 3mp4.mp4 (Redacted)
2 months ago
TheftFromMall.MP4 (Redacted)
3 years ago
TheftFromMall.MP4 (Redacted)
3 years ago
privacyvideo 3.mp4 (Redacted)
2 months ago
2016-11-24T19_25_000350000Z_1280x7...
2 years ago
TheftFromMall.MP4 (Redacted)
3 years ago
2016-11-24T19_25_000350000Z_1280x7...
2 years ago
privacyvideo 3.mp4 (Redacted)
2 months ago
privacyvideo_1280x720_redacted_1280x...
3 months ago
privacyvideo_1280x720.mp4 (Redacted)
5 months ago
privacyvideo_1280x720.mp4 (Redacted)
5 months ago

Trimming

- You can trim a file without redacting it.
- If a video is longer than 30 minutes, the first 30 minutes is automatically selected for trimming. You can adjust this selection.
- If a video is longer than 3 hours, the maximum size you can trim it to is 02:59:00.



A maximum of 2 hours of video can be sent at a time

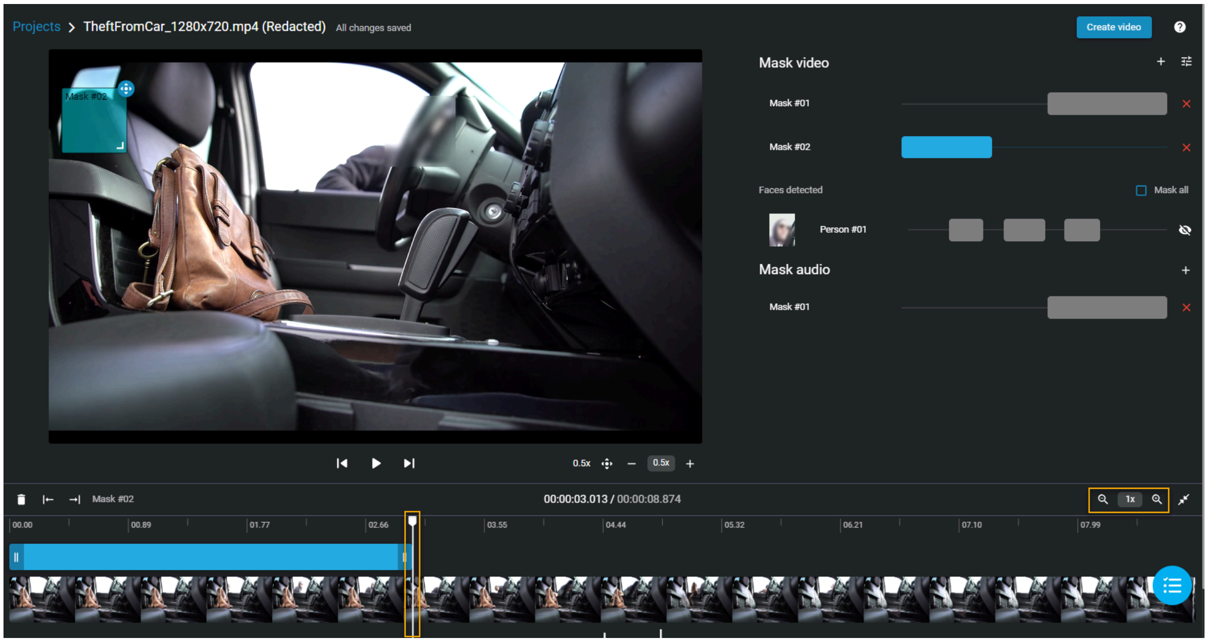
Select the time range you want to redact

04:28:06 PM / 04:28:23 PM

September 18, 2017

Redaction

- You can redact video automatically or manually.
- You can redact visual areas of a video, or audio segments of a video recording.



Related Topics

Trimming video on page 218
Redacting video in Clearance on page 220
Redacting video manually in Clearance on page 228
Redacting audio on page 234

Trimming video

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. Choose to keep only the relevant sequence of a longer video to accelerate the review of the recording.

Before you begin

Upload a file.

Procedure

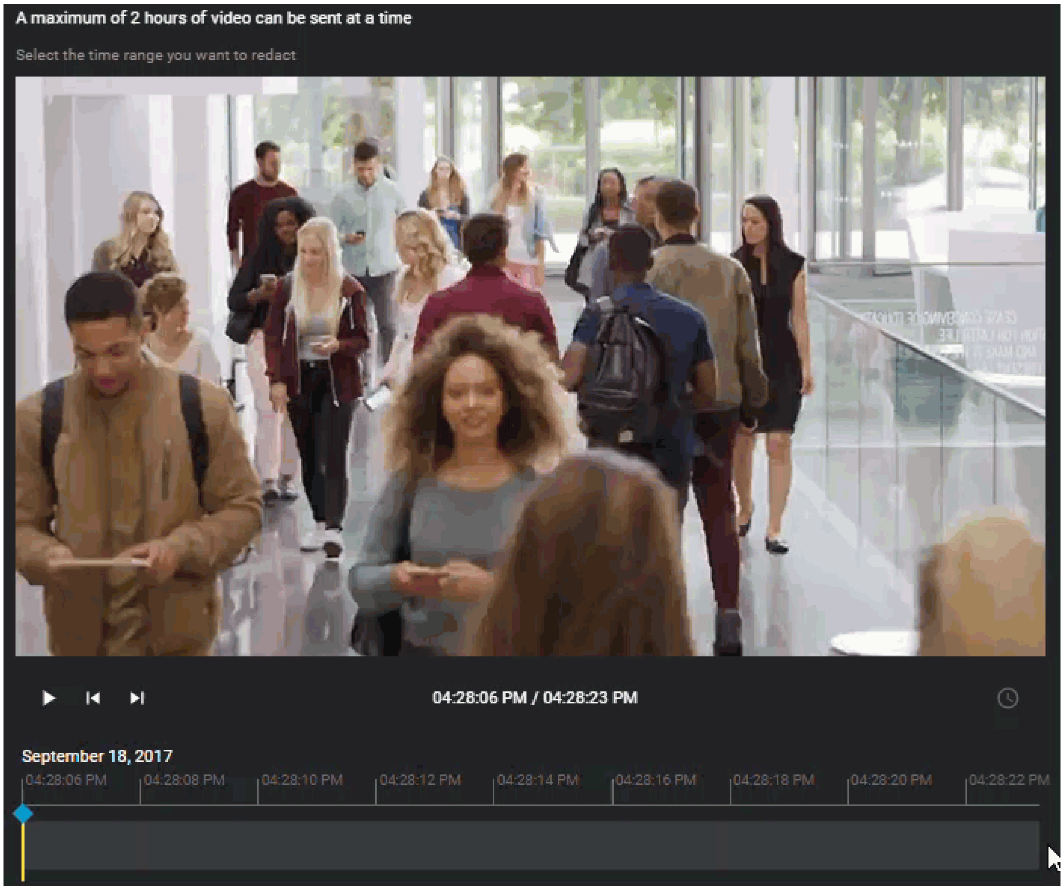
To trim a video:

1 From a case, navigate to the file you want to redact, click **More** (⋮) in the **Files**, and then click **Trim and Redact**.

TIP: You can also start a redaction from the *File* page or from the *Evidence preview* window when previewing evidence in a case.

The *Trim video* window opens.

2 (Optional) Move your cursor over the start or end of the file timeline and drag the its borders to fit your desired time range or adjust the **From** and **To** time values.



A maximum of 2 hours of video can be sent at a time

Select the time range you want to redact

3 If an i-PRO in-car system with multiple microphones associated with it recorded the video, you can choose the audio channel that best suits your needs.

4 Click **Save to a case**.

The *Save to case* window opens.

5 Modify the name of the video as necessary.

TIP: Include identifying information in the name of the video that indicates it is a trimmed copy.

6 If you must associate the trimmed video with other cases, click **Add** (➕) and select the necessary cases.

7 (Optional) If you want to copy the field information, including location, category, and tags from the original video to the trimmed copy, select the **Copy evidence field information** check box.

8 Click **Save**.

To redact the video after trimming:

1 From the *Edit video* window, click **Redact**.

After you finish

- Before sharing the case with third parties or guests, restrict access to the original file by changing the access policy for the file.
- If you need to conceal sensitive or identifiable information in the recording, refer to the following:
  - Redacting video in Clearance on page 220
  - Redacting video manually in Clearance on page 228

Related Topics

About the video editor on page 215

Redacting video in Clearance

To reduce the time required to redact videos, use the face detection function to detect faces, then manually adjust the masks if required.

What you should know

The analytic process begins to search and detect faces whenever a new redaction process is started.

- When the process is complete, a thumbnail image of each detected face is then displayed, these thumbnails can be used to select the individuals that should be redacted from the scene.
- Masks are applied to all parts of the scene where a face is identified.

The processing time for auto face detection can vary depending on the video file size and will be affected by the resolution, length, frame rate, and other factors related to video. The success of the auto face detection can vary depending on the quality of the video and whether the subject is facing to the front or the side.

Performing video *redaction* (Auto Face Detection) on a mobile device is not supported.

Procedure

To redact a video file:

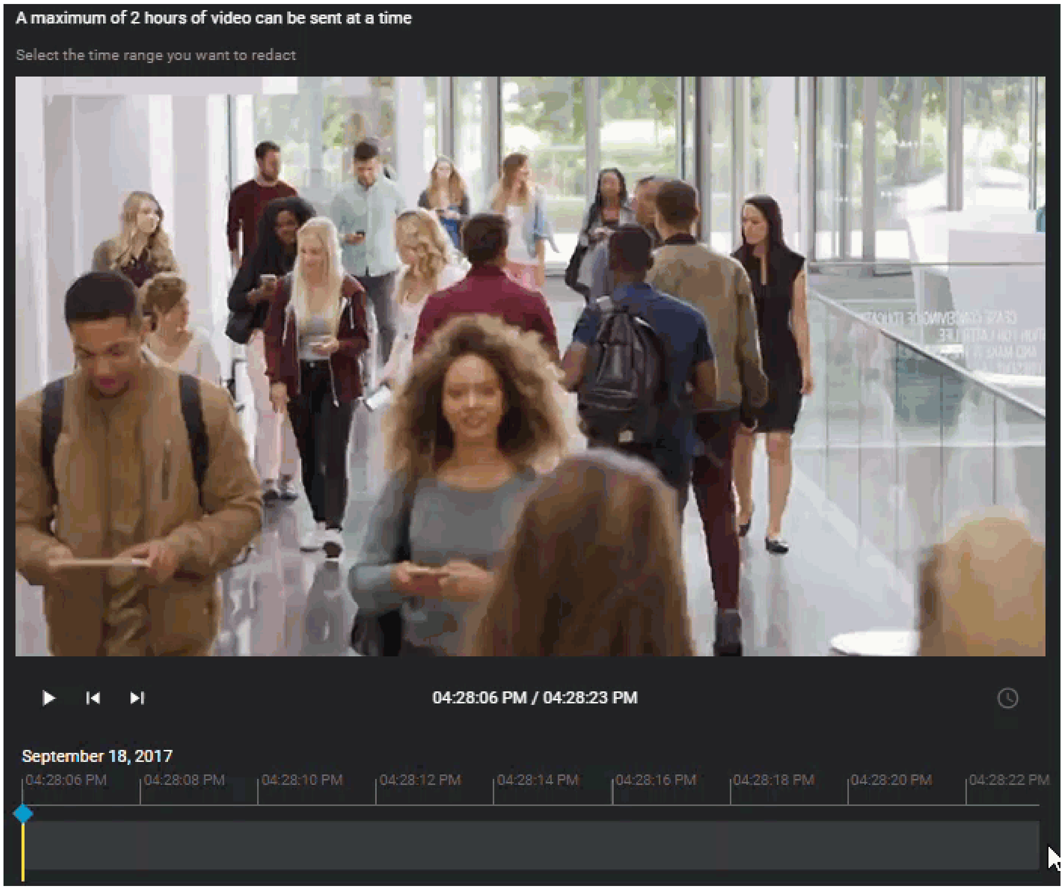
1 From a case, navigate to the file you want to redact, click **More** (⋮) in the **Files**, and then click **Trim and Redact**.

TIP: You can also start a redaction from the *File* page or from the *Evidence preview* window when previewing evidence in a case.

The *Trim video* window opens.

To trim a video file:

1 (Optional) Move your cursor over the start or end of the file timeline and drag the its borders to fit your desired time range or adjust the **From** and **To** time values.



A maximum of 2 hours of video can be sent at a time

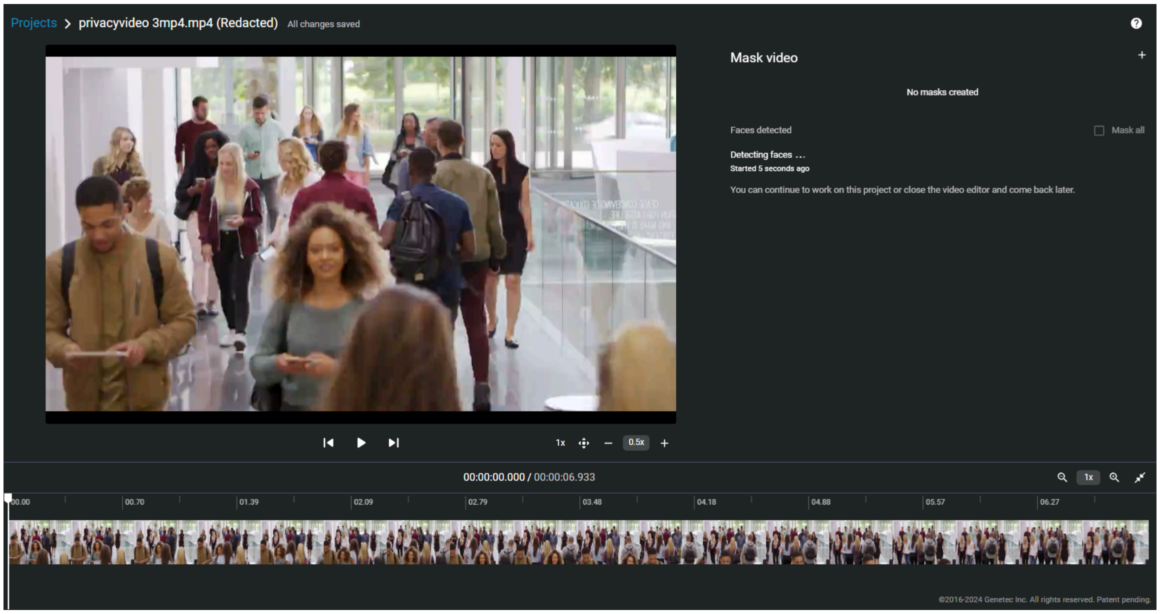
Select the time range you want to redact

04:28:06 PM / 04:28:23 PM

September 18, 2017

2 Click **Continue**.
The *Video editor* page opens.

3 The face detection search begins automatically.



No masks created

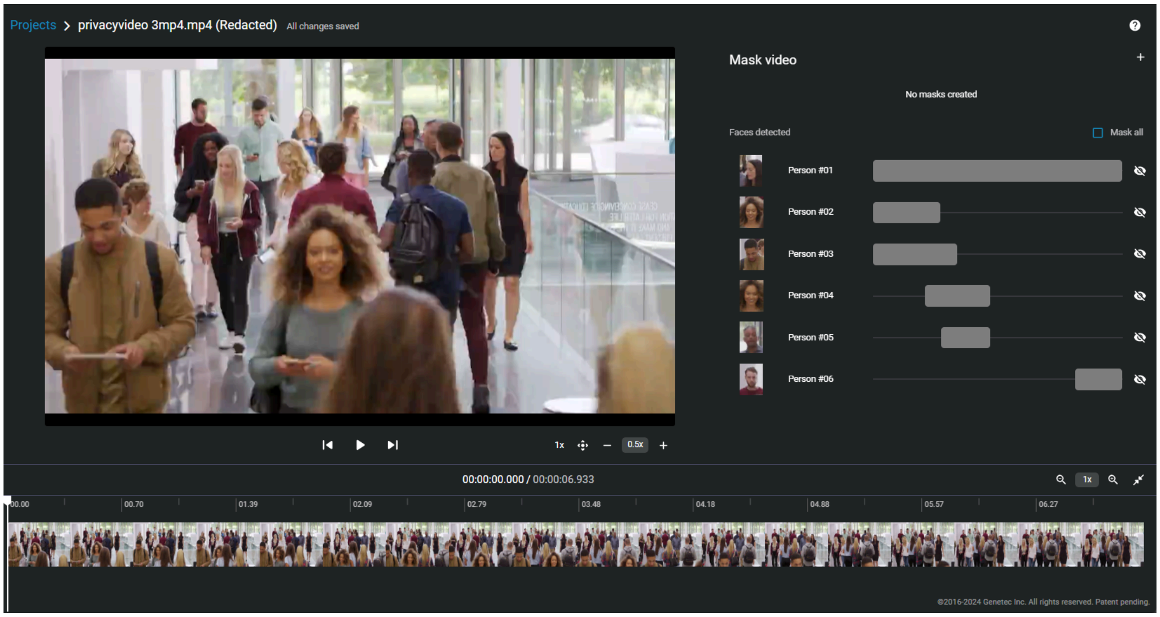
Detecting faces ...
Started 5 seconds ago

You can continue to work on this project or close the video editor and come back later.

00:00:00.000 / 00:00:06.933

©2016-2024 Genetec Inc. All rights reserved. Patent pending.

- Detected faces are displayed as thumbnails in the **Mask faces** section of the **Faces** tab.
- Detected faces are assigned a unique identifier to help identify them and assign masks individually. For example, Person #01.

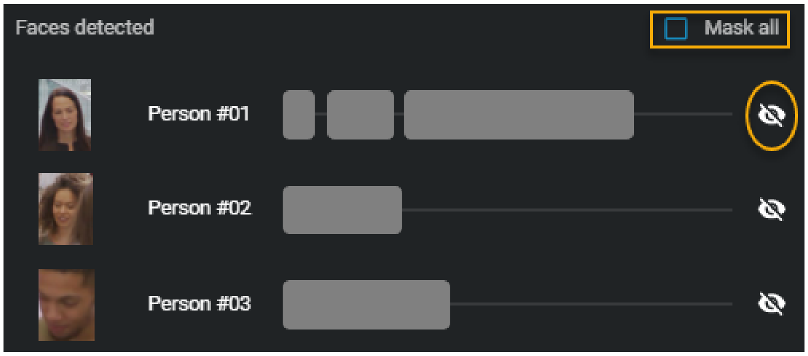


No masks created

00:00:00.000 / 00:00:06.933

©2016-2024 Genetec Inc. All rights reserved. Patent pending.

4. In the *Mask video* section, select one or mores face that you want to mask by clicking the **Mask face** icon or select **Mask all**.



TIP: Clicking a mask in the list immediately identifies where in the scene that person was detected. This helps you navigate to and review the required segment more efficiently.

5. Select a mask in the list and click **Play video** (▶).

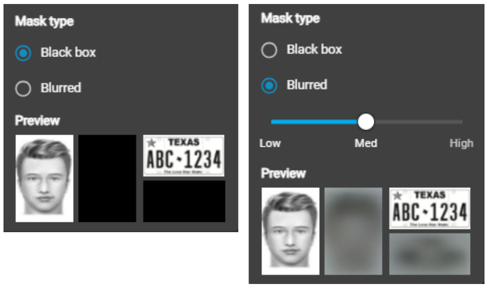
   a) Use the timeline slider, zoom controls, or your mouse scroll wheel to position the timeline slider at the section of video that you want to redact.

   TIP: Use the thumbnail previews in the timeline to help identify the exact point in the video that you require. To zoom in or out on the timeline, click **Zoom in** or **Zoom out** (🔍 1x 🔍)

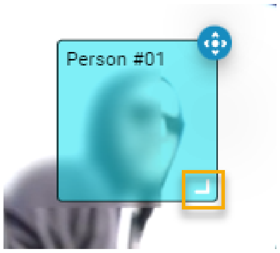
6. (Optional) Click **Mask settings** (☰) to specify the mask type that you require.

   a) Select either **Black box** or **Blurred**.

   b) If you specified **Blurred**, select a blur level. Click or drag the slider to either **Low**, **Medium**, or **High** to preview the blur level.

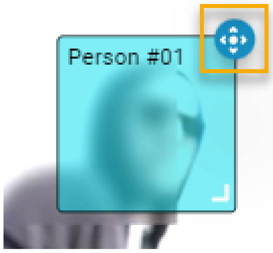


7. To resize the mask, use your mouse at the lower-right corner of the masking box.



8 If the person or object you must redact is moving in the video scene, you can adjust the mask location using the tracking tool, as follows:

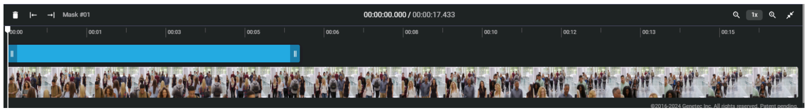
a) Next to the masking box on the video preview, click and hold the tracking button (✥).



b) As the video plays, move the masking box to keep the mask covering the person's face, the object, and so on.

c) When the mask is no longer required on the video, release the tracking button (✥).

9 To change the duration of the mask, adjust the start and end points of the mask in the timeline.



TIP: You can also adjust the start and end points by dragging the timeline bar to a specific point in the video and clicking **Start mask at current time** (|←) or **End mask at current time** (→|).

10 (Optional) Delete masks.

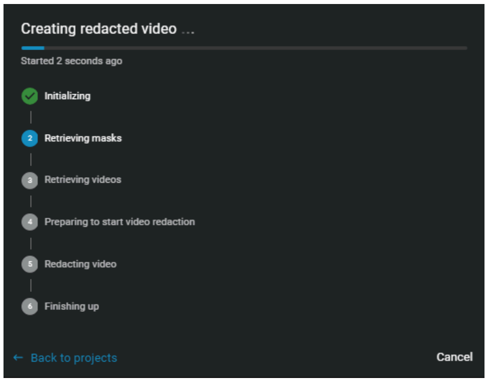
- Click delete (✖) in the mask list to remove any mask that you no longer require.
- Click **Delete mask** (🗑) in the timeline controls to delete the currently selected mask.

11 (Optional) Click **New mask** to create additional masks as required.

This function is typically used to redact a person missed by the face detection, or to redact an object or other content in the scene that needs to be redacted.

12 Click **Create video** to generate the redacted file.

a) (Optional) Click **View details** to track the progress.



Creating redacted video ...

Started 2 seconds ago

✓ Initializing

2 Retrieving masks

3 Retrieving videos

4 Preparing to start video redaction

5 Redacting video

6 Finishing up

← Back to projects

Cancel

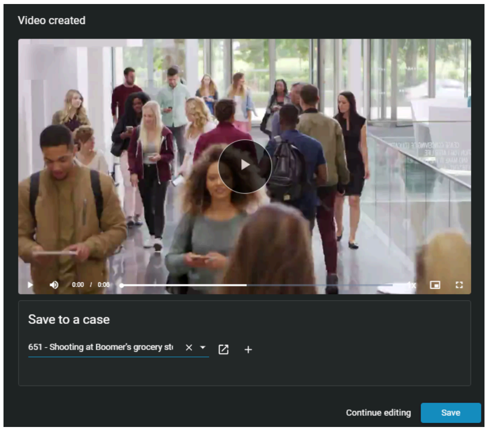
b) (Optional) Click **Back to projects** to close the progress dialog while redaction continues in the background.

13 After the redacted video is created, choose one of the following:

- Save the redacted video to an existing case.
- Save the redacted video to a new case.

14 (Optional) To save the redacted video to an existing case.

a) Enter a case ID or name in the Search field or click the menu to see a list.



Video created

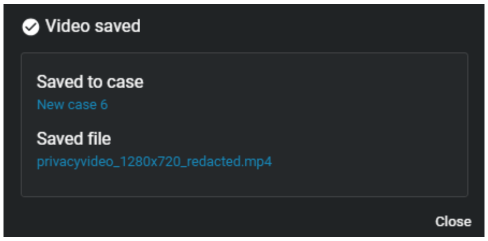
Save to a case

651 - Shooting at Boomer's grocery st

b) (Optional) To check that you have the correct case click **View case** (↗).

c) (Optional) Click **Continue editing** to return to the video editor and make more changes.

d) Click **Save** to create a redacted copy of the video file.



✓ Video saved

Saved to case

New case 6

Saved file

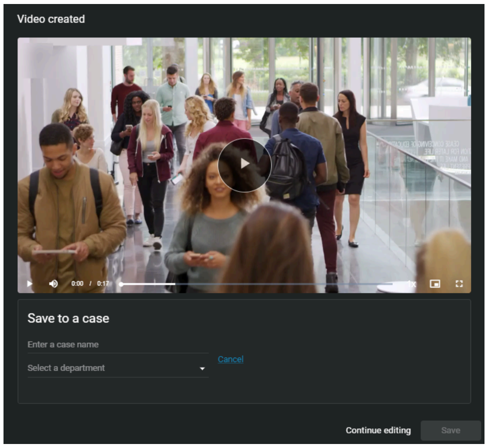
privacyvideo_1280x720_redacted.mp4

TIP: Click **View file** to change the file name before closing the dialog, so that others can easily find the file.

e) Click **Close**.

15 (Optional) To save the redacted video to a new case. For example, when you want to share redacted evidence with someone who must not have access to the original case.

a) Click **Create a case**.



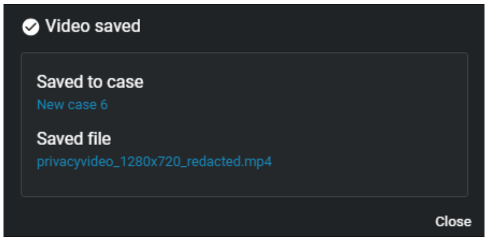
b) Enter a name for the new case.

c) Select a department from the **Department** list.

d) (Optional) Click **Cancel** to return to the previous dialog panel.

e) (Optional) Click **Continue editing** to return to the video editor and make more changes.

f) Click **Save** to create a redacted copy of the video file.



Video saved

Saved to case
New case 6

Saved file
privacyvideo_1280x720_redacted.mp4

TIP: Click **View file** to change the file name before closing the dialog, so that others can easily find the file.

g) Click **Close**.

The edited clip is saved as a separate video file. The original file and the edited file are both associated with the case.

Example

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

Although we do our best to keep our videos current, the information presented in this video might become outdated with each new release. If you find anything wrong with this video, feel free to contact us.

After you finish

Before sharing the case with third parties or guests, restrict access to the original file by changing the access policy for the file.

Related Topics

About the video editor on page 215

Redacting video manually in Clearance

You can manually mask or redact faces or other sensitive content in a video file scene to conceal a person's face or other identifiable information. You can also remove all audio from a video to mask sensitive audio content before generating a redacted video clip.

What you should know

- If the source file contains audio, audio is on by default.
- The timeline contains thumbnail previews of the complete evidence file.

Procedure

To redact a video file manually:

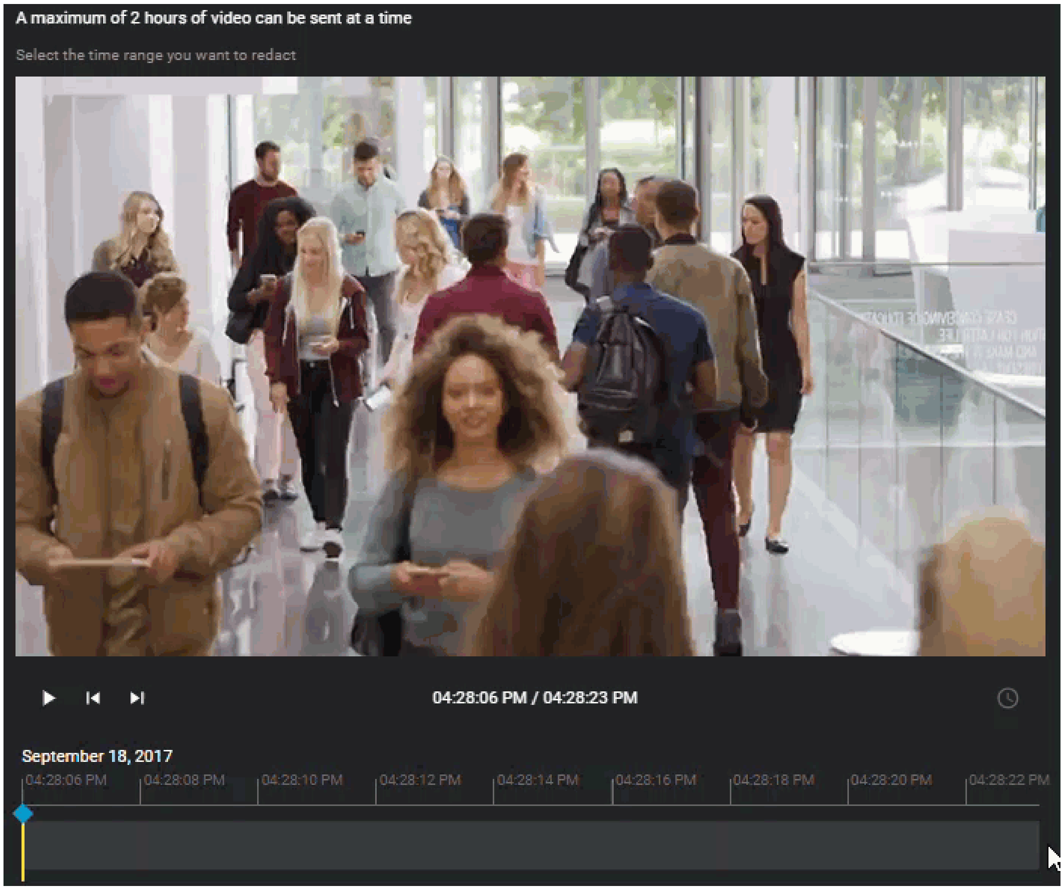
1 From a case, navigate to the file you want to redact, click **More** (⋮) in the **Files**, and then click **Trim and Redact**.

TIP: You can also start a redaction from the *File* page or from the *Evidence preview* window when previewing evidence in a case.

The *Trim video* window opens.

To trim a video file:

1 (Optional) Move your cursor over the start or end of the file timeline and drag the its borders to fit your desired time range or adjust the **From** and **To** time values.



A maximum of 2 hours of video can be sent at a time

Select the time range you want to redact

04:28:06 PM / 04:28:23 PM

September 18, 2017

2 Click **Continue**.

The *Video editor* page opens.

3 From the *Video editor*, do the following:

a) Use the timeline slider, zoom controls, or your mouse scroll wheel to position the timeline slider at the section of video that you want to redact.

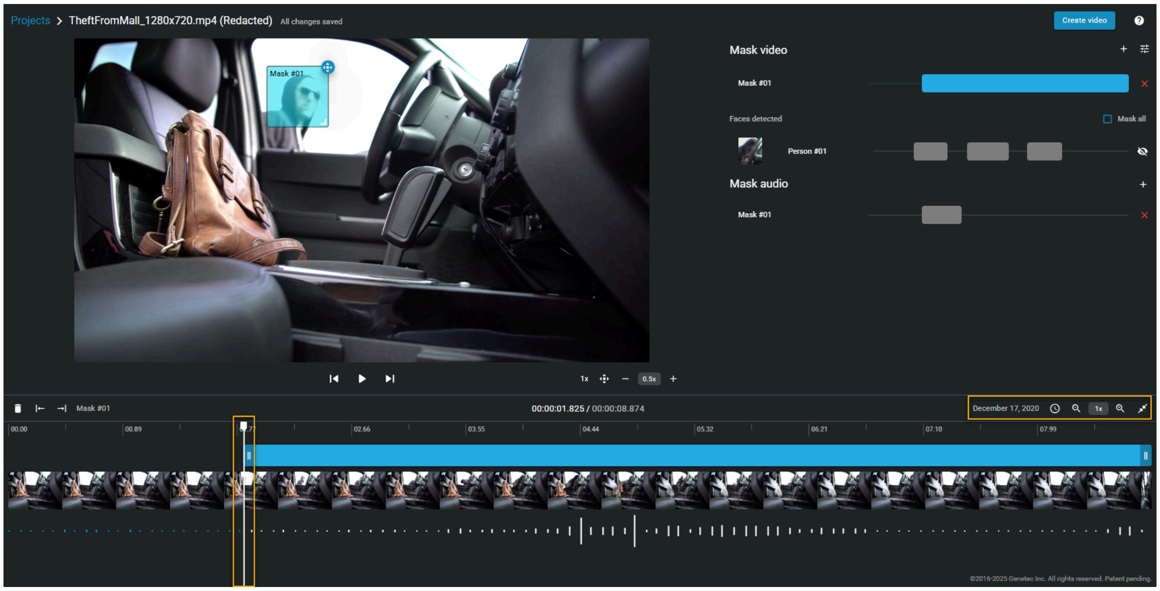
TIP: Use the thumbnail previews in the timeline to help identify the exact point in the video that you require. To zoom in or out on the timeline, click **Zoom in** or **Zoom out** (🔍 1x 🔍)

b) (Optional) Click 🕓 to toggle between *absolute time* and *relative time*.

c) In the video editor, click **Mask video** (👁).

d) In the *Additional masks* section, click **New mask** (+).

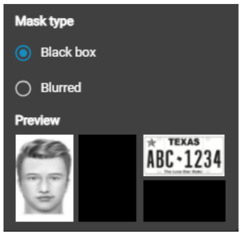
A mask layer is created on the video preview, and the duration of the mask is shown along the video timeline at the bottom of the video.

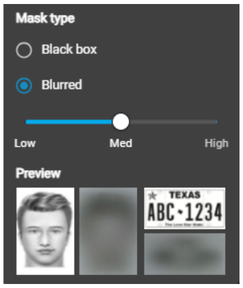


4 (Optional) Click **Mask settings** (☰) to specify the mask type that you require.

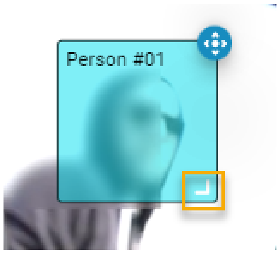
a) Select either **Black box** or **Blurred**.

b) If you specified **Blurred**, select a blur level. Click or drag the slider to either **Low**, **Medium**, or **High** to preview the blur level.





5 To resize the mask, use your mouse at the lower-right corner of the masking box.

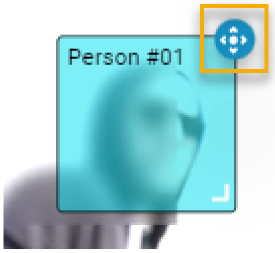


6 If the person or object you must redact is moving in the video scene, you can adjust the mask location using the tracking tool, as follows:

a) In the *Masking* pane, increase or decrease the **Tracking speed**.

You can select values in the range 0.1x to 10x.

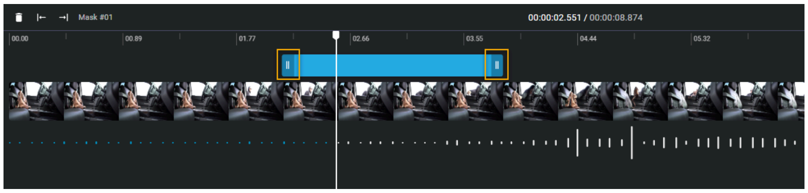
b) Next to the masking box on the video preview, click and hold the tracking button (✥).



c) As the video plays, move the masking box to keep the mask covering the person's face, the object, and so on.

d) When the mask is no longer required on the video, release the tracking button (✥).

7 To change the duration of the mask, adjust the start and end points of the mask in the timeline.



TIP: You can also adjust the start and end points by dragging the timeline bar to a specific point in the video and clicking **Start mask at current time** (|←) or **End mask at current time** (→|).

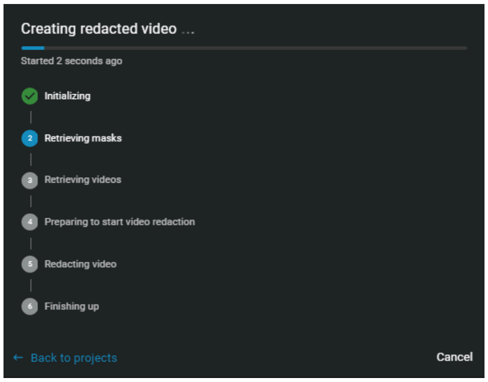
8 (Optional) Modify your masks if required.

a) Click **New mask** (✚) to create additional masks.

b) Click delete (✖) to remove any masks that you no longer require.

9 Click **Create video** to generate the redacted file.

a) (Optional) Click **View details** to track the progress.



Creating redacted video ...

Started 2 seconds ago

Initializing

2 Retrieving masks

3 Retrieving videos

4 Preparing to start video redaction

5 Redacting video

6 Finishing up

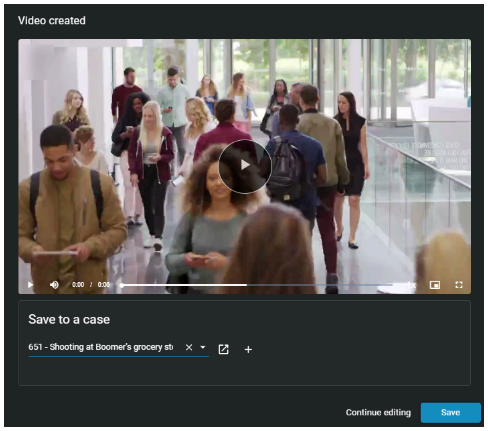
b) (Optional) Click **Back to projects** to close the progress dialog while redaction continues in the background.

10 After the redacted video is created, choose one of the following:

- Save the redacted video to an existing case.
- Save the redacted video to a new case.

11 (Optional) To save the redacted video to an existing case.

a) Enter a case ID or name in the Search field or click the menu to see a list.



Video created

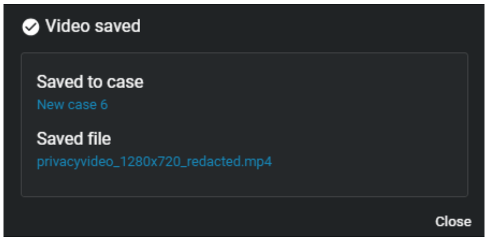
Save to a case

651 - Shooting at Boomer's grocery st

b) (Optional) To check that you have the correct case click **View case** (⧉).

c) (Optional) Click **Continue editing** to return to the video editor and make more changes.

d) Click **Save** to create a redacted copy of the video file.



Video saved

Saved to case

New case 6

Saved file

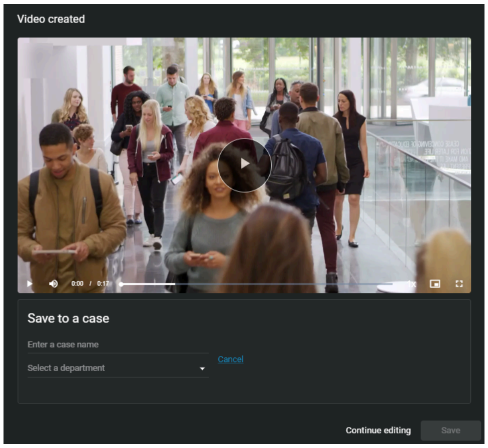
privacyvideo_1280x720_redacted.mp4

TIP: Click **View file** to change the file name before closing the dialog, so that others can easily find the file.

e) Click **Close**.

12 (Optional) To save the redacted video to a new case. For example, when you want to share redacted evidence with someone who must not have access to the original case.

  a) Click **Create a case**.



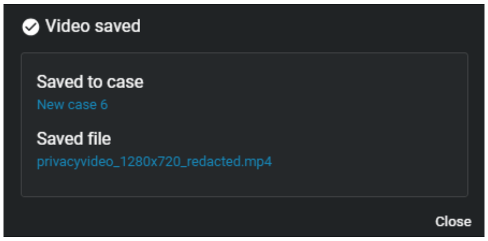
Video created

Save to a case

Enter a case name

Select a department

  b) Enter a name for the new case.
  c) Select a department from the **Department** list.
  d) (Optional) Click **Cancel** to return to the previous dialog panel.
  e) (Optional) Click **Continue editing** to return to the video editor and make more changes.
  f) Click **Save** to create a redacted copy of the video file.



Video saved

Saved to case

New case 6

Saved file

privacyvideo_1280x720_redacted.mp4

  TIP: Click **View file** to change the file name before closing the dialog, so that others can easily find the file.

  g) Click **Close**.

13 (Optional) Click **Continue editing** to return to the video editor and make more changes.

14 (Optional) From the video editor, click **View created video** to return to the redacted video.

The redacted video is saved as a separate video file.

Example

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

NOTE: Although we do our best to keep our videos current, the information presented in this video might become outdated with each new release. If you find anything wrong with this video, feel free to contact us.

After you finish

Before sharing the case with third parties or guests, restrict access to the original file by changing the access policy for the file.

Related Topics

About the video editor on page 215

Redacting audio

You can apply masks to redact voices, noises, or other audio content in a video file.

Before you begin

Upload a file to a case.

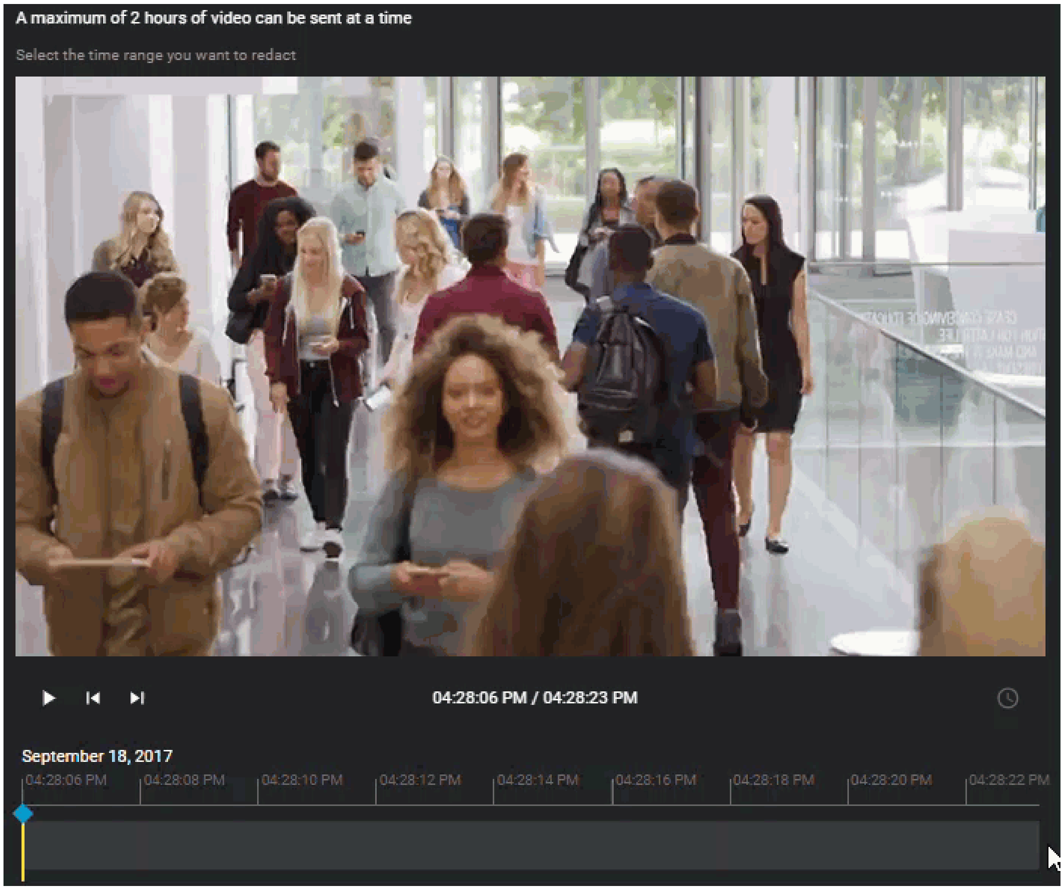
Procedure

1 From a case, navigate to the file you want to redact, click **More** (⋮) in the **Files**, and then click **Trim and Redact**.

TIP: You can also start a redaction from the *File* page or from the *Evidence preview* window when previewing evidence in a case.

The *Trim video* window opens.

2 (Optional) Move your cursor over the start or end of the file timeline and drag the its borders to fit your desired time range or adjust the **From** and **To** time values.



A maximum of 2 hours of video can be sent at a time

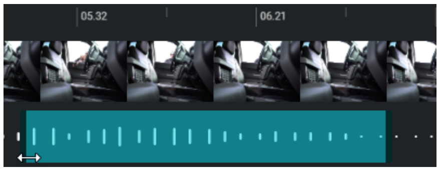
Select the time range you want to redact

04:28:06 PM / 04:28:23 PM

September 18, 2017

3 Click **New mask** (+).

   a) To change the duration of the audio mask, adjust the start and end points of the mask in the timeline.



TIP: To zoom in or out on the timeline, click **Zoom in** or **Zoom out** (🔍 1x 🔍)

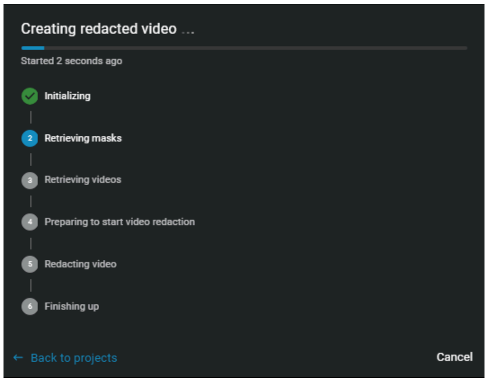
4 (Optional) Modify your masks if required.

   a) Click **New mask** (+) to create additional masks.

   b) Click delete (✖) to remove any masks that you no longer require.

5 Click **Create video** to generate the redacted file.

   a) (Optional) Click **View details** to track the progress.



Creating redacted video ...

Started 2 seconds ago

✓ Initializing

2 Retrieving masks

3 Retrieving videos

4 Preparing to start video redaction

5 Redacting video

6 Finishing up

← Back to projects

Cancel

   b) (Optional) Click **Back to projects** to close the progress dialog while redaction continues in the background.

The redacted video or audio clip is saved as a separate file.

Example

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

▶

Although we do our best to keep our videos current, the information presented in this video might become outdated with each new release. If you find anything wrong with this video, feel free to contact us.

After you finish

Before sharing the case with third parties or guests, restrict access to the original file by changing the access policy for the file.

Related Topics

About the video editor on page 215

12

Reviewing dashboards

Learn how use the dashboard in Clearance.

This section includes the following topics:

- "About the Clearance dashboard " on page 237

About the Clearance dashboard

You can use the Clearance dashboard to track trends in your investigations and evaluate your subscription to ensure you get the most out of Clearance.

The Clearance dashboard consists of the following:

Case dashboards:

- View total cases by category or state.
- Track creation of cases over time and filter by category.
- Track which categories of investigations occur most frequently.

Storage dashboards:

- View total storage used by file type.
- Track data storage over time and filter this information by file type, and total storage or new storage.
  NOTE: New storage is defined as the change in storage in a given time period. The value displayed for new storage in a given time period will be negative if more data was deleted than added.

Requests dashboards:

- View total file requests by status.
- Measure requests over time organized by their status.
- Measure requests by average processing time.
- Measure requests and approvals by user

NOTE: The requests dashboards are only available in accounts that have the Registry module enabled.

Related Topics

Configuring the Clearance dashboard on page 237

Configuring the Clearance dashboard

After you have created some cases assigned them to the correct categories, you can configure the Clearance dashboard.

What you should know

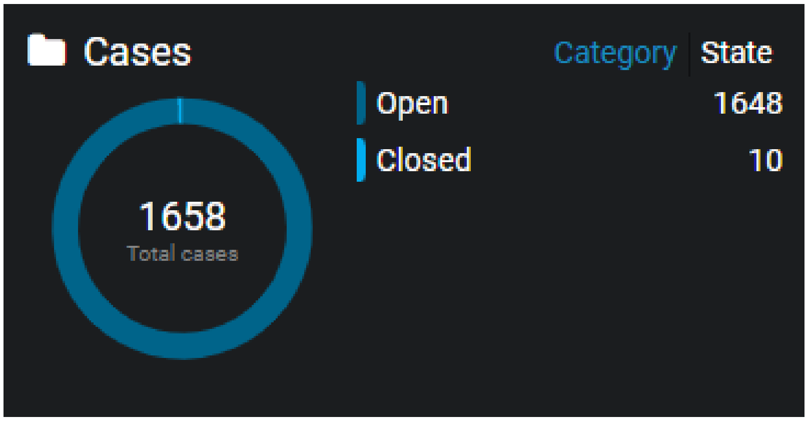
Only users included in the *View dashboard* security policy can configure the dashboard.

Procedure

To date section: This section gives an overview of data added since the creation of the account. Total data storage is can be organized by category or state.

1 In the *Cases* section, examine the types and status’ of investigations that your organization has handled using Clearance. Organize total cases by:

- Category
- State

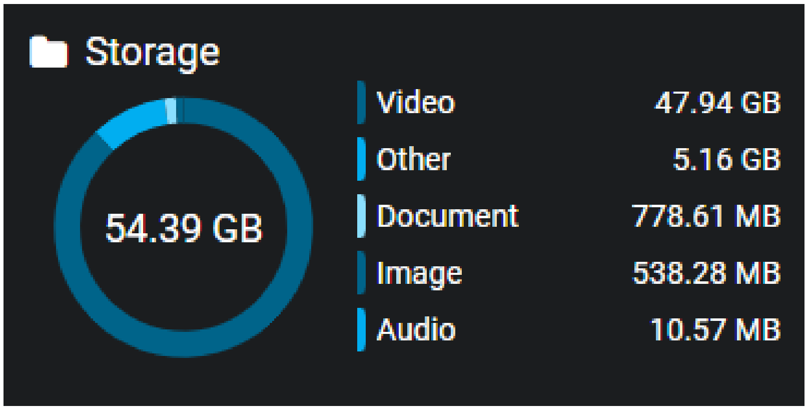


Cases

Open	1648
Closed	10

2 In the *Storage* section, you can assess how your organization has used storage between the following media types since the creation of your account:

- Video
- Document
- Image
- Audio
- Other

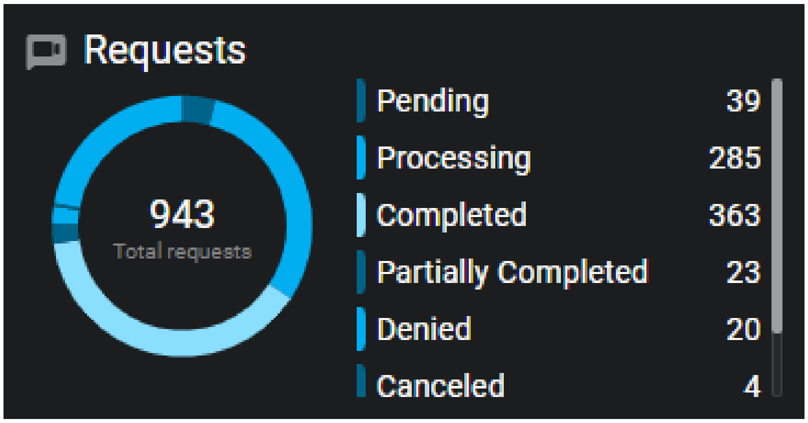


Storage

Video	47.94 GB
Other	5.16 GB
Document	778.61 MB
Image	538.28 MB
Audio	10.57 MB

3 In the *Requests* section, you can examine the total number of requests, organized by request status, that your organization has handled. It can be an indicator of the overall health of your organization's request process. Examine requests by the following status':

- Pending
- Processing
- Completed
- Partially Completed
- Denied
- Canceled
- Video Unavailable



Requests

943
Total requests

Pending	39
Processing	285
Completed	363
Partially Completed	23
Denied	20
Canceled	4

Historic section: Examine these statistics and filters give you a more detailed understanding of the data your organization has collected.

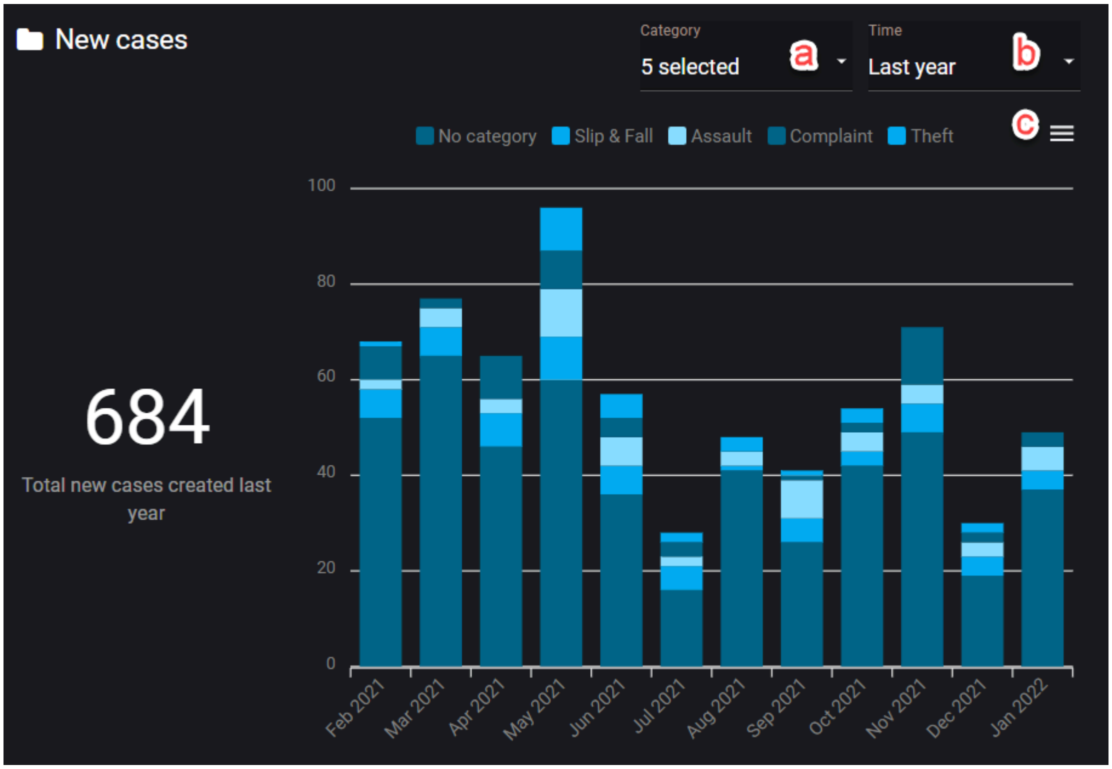
1 In the *New cases* section, gain insights into the number and types of investigations that were created over a configurable time period. Use this to identify trends over time related to different incident categories, or to assist with resource allocation for future cases. Configure the following in the **New cases** section:

a) Click **Category** and select the categories you require.

b) Click **Time** and select the time period you require.

NOTE: To see your all time stats, you must click **Time** and then click **Custom**. Then, select the day you opened your Clearance account.

c) Optional: If you want to download the data, click **Download** (≡) and select a file type.



2 In the *Storage* section, discover how storage is allocated between the different types of evidence used in your investigations. Assess your storage needs over time and examine how much of each specific

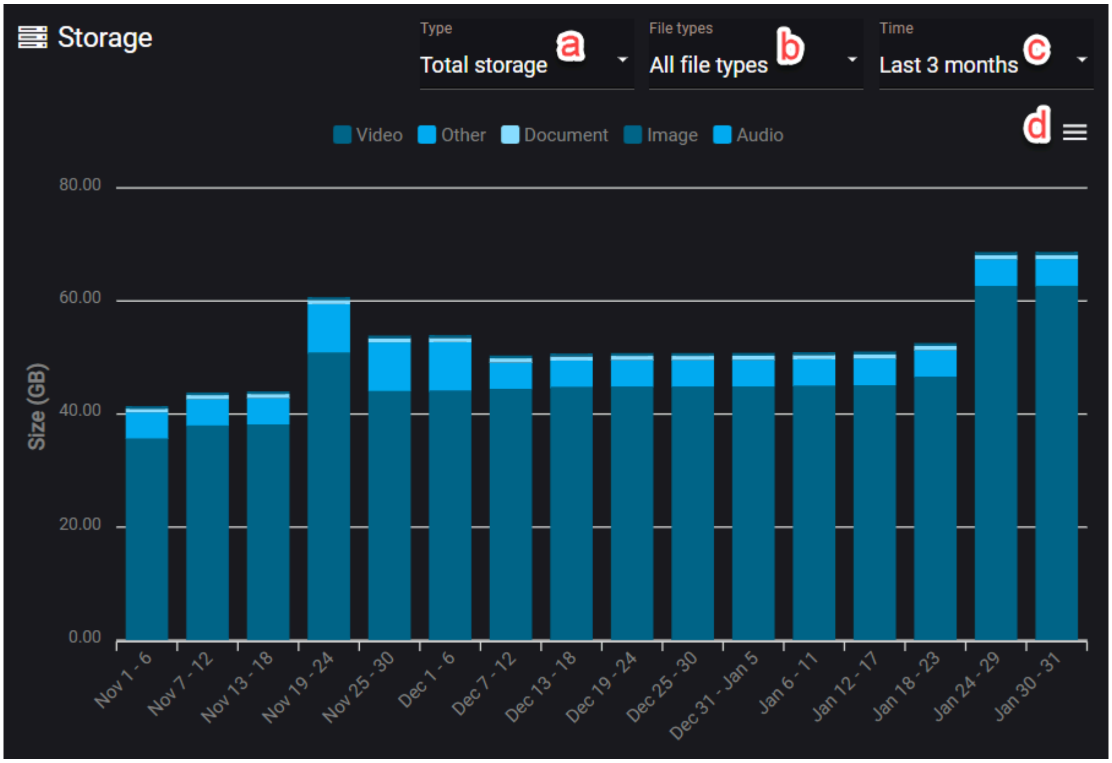
media type your organization has added in the past week, month, or other period of time. Configure the following storage settings:

a) Click **Type** and select **New storage** or **Total storage**.

b) Click **File types** and select the file type that you want to examine.

c) Click **Time** and select the time period you want to examine.

d) Optional: If you want to download the data, click (≡) and select a file type.



Storage

Type: Total storage

File types: All file types

Time: Last 3 months

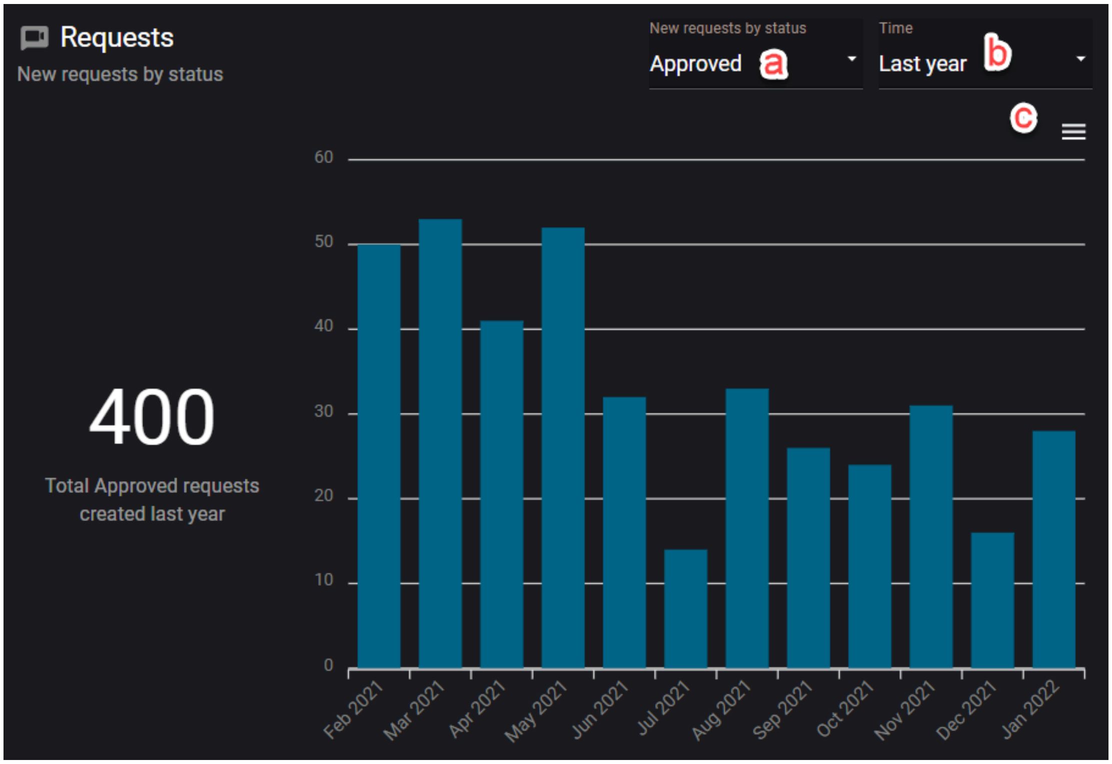
3 In the **Requests: New requests by status** section, you can gain a better understanding of the level of efficiency of your request process. These metrics can help your organization identify potential bottlenecks

and trends in the number of submitted and completed requests. In this section, configure the following settings:

a) Click **New requests by status** and select a request status state.

b) Click **Time** and select the time period you want to examine.

c) Optional: If you want to download the data, click (≡) and select a file type.



Requests

New requests by status

New requests by status: Approved

Time: Last year

400

Total Approved requests created last year

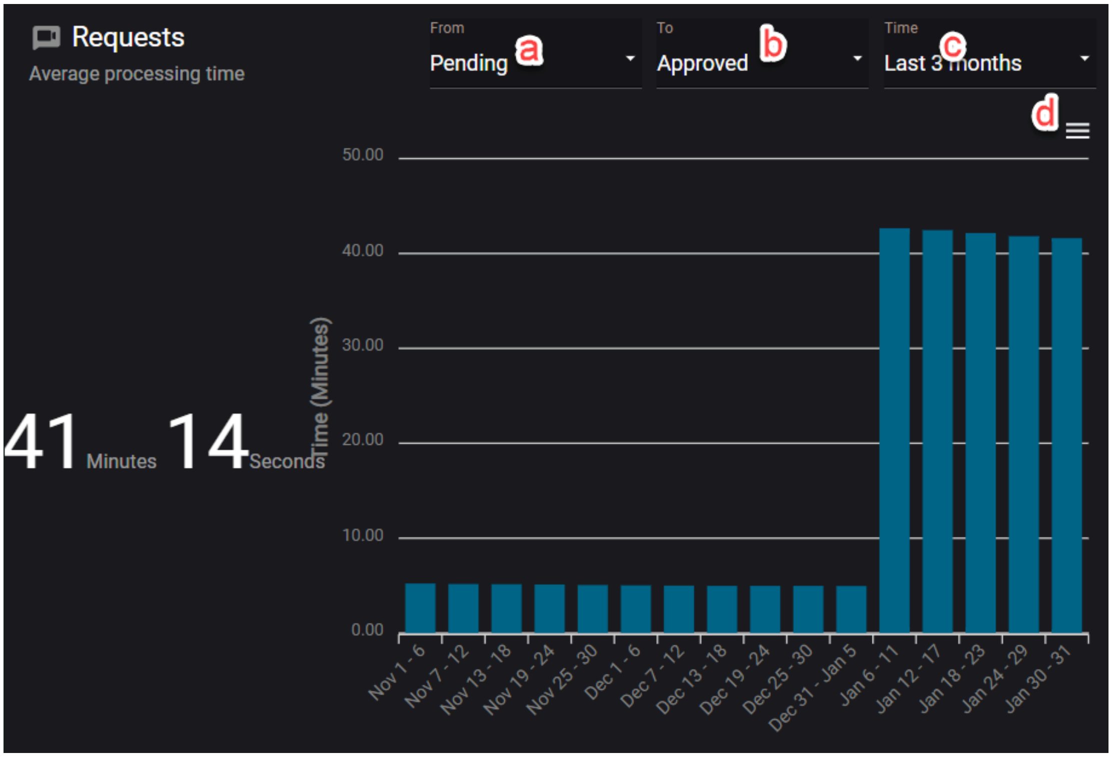
4 In the **Requests: Average processing time** section, assess how long it takes to complete the request process and determine whether it is improving, worsening, or remaining consistent. Configure the following settings:

a) Click **From** and select a starting status for the average processing time measurement.

b) Click **To** and select an ending status measurement.

c) Click **Time** and select the time period you want to examine.

d) Optional: If you want to download the data, click (≡) and select a file type.



Requests

Average processing time

From: Pending

To: Approved

Time: Last 3 months

41 Minutes 14 Seconds

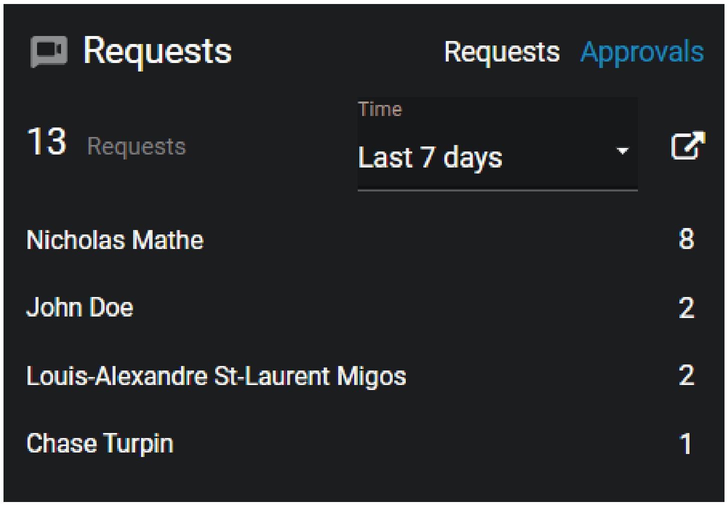
5 In the **Requests: requests/approvals** section, examine how many requests have been submitted and approved over time by specific users by configuring the following settings:

a) Click **Requests** for a list of users organized by the number of requests they have made.

b) Click **Approvers** for a list of users organized by the number of requests they have approved.

c) Click **All time** and select the time period you want to examine.

d) Optional: If you want to download the data as a .CSV file, click (↗).



Requests

Requests Approvals

13 Requests

Time: Last 7 days

Nicholas Mathe	8
John Doe	2
Louis-Alexandre St-Laurent Migos	2
Chase Turpin	1

Related Topics

About the Clearance dashboard on page 237

13

Public upload requests

Invite anyone to add files to an incident without viewing the case contents in Clearance.

This section includes the following topics:

- "Sharing files using a file request" on page 246

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

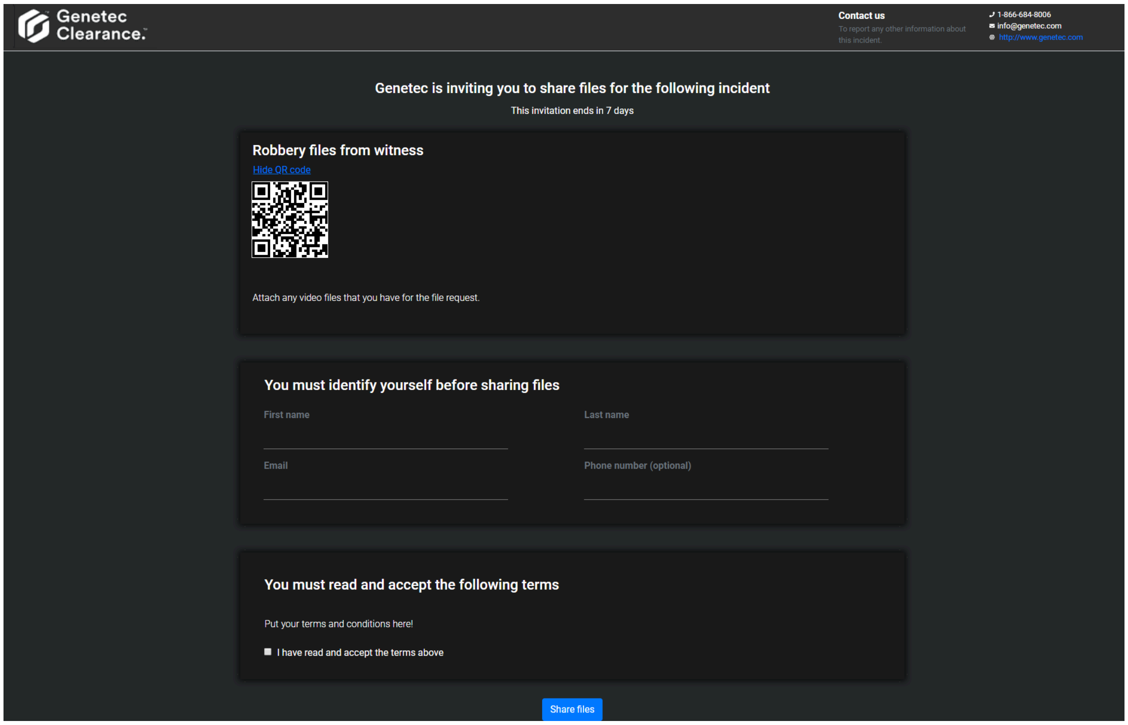
Ensure that you have received a file request containing a file request link that you can use to submit files.

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.



Contact us

To report any other information about this incident.

1-866-684-8006

info@genetec.com

http://www.genetec.com

Genetec is inviting you to share files for the following incident

This invitation ends in 7 days

Robbery files from witness

Hide QR code

Attach any video files that you have for the file request.

You must identify yourself before sharing files

First name

Last name

Email

Phone number (optional)

You must read and accept the following terms

Put your terms and conditions here!

■ I have read and accept the terms above

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**.

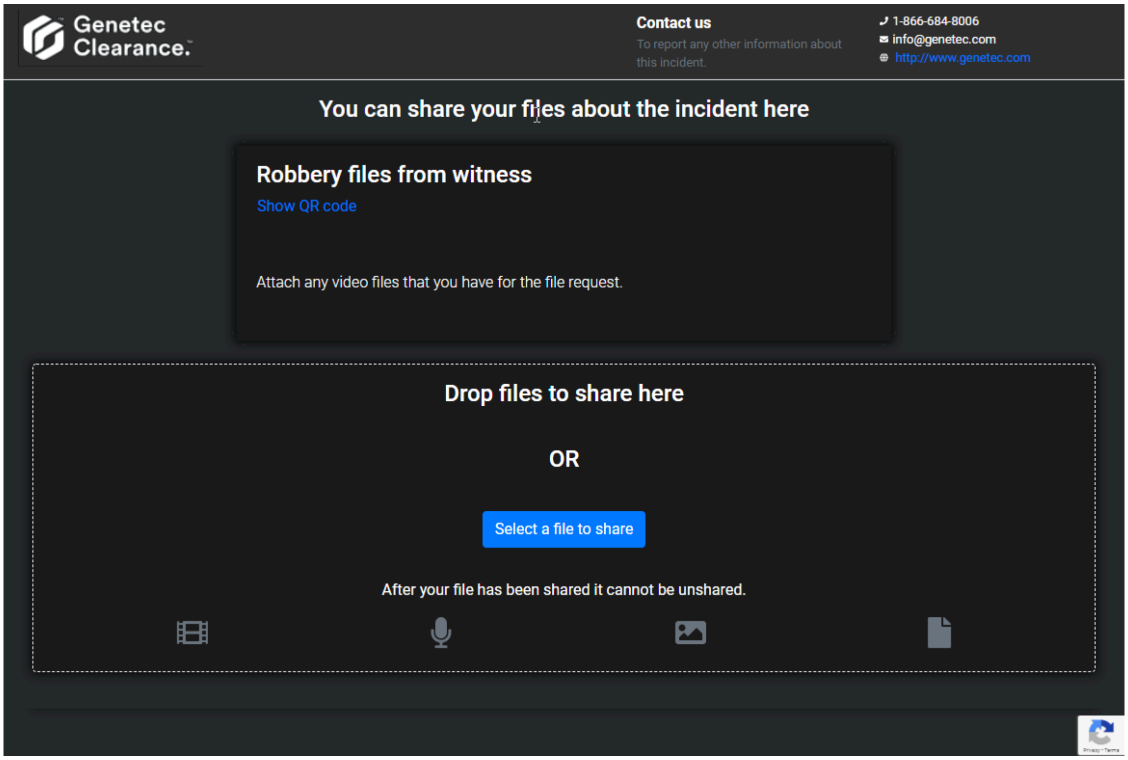
   c) Enter an **Email address**.

   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**.



To report any other information about this incident.

You can share your files about the incident here

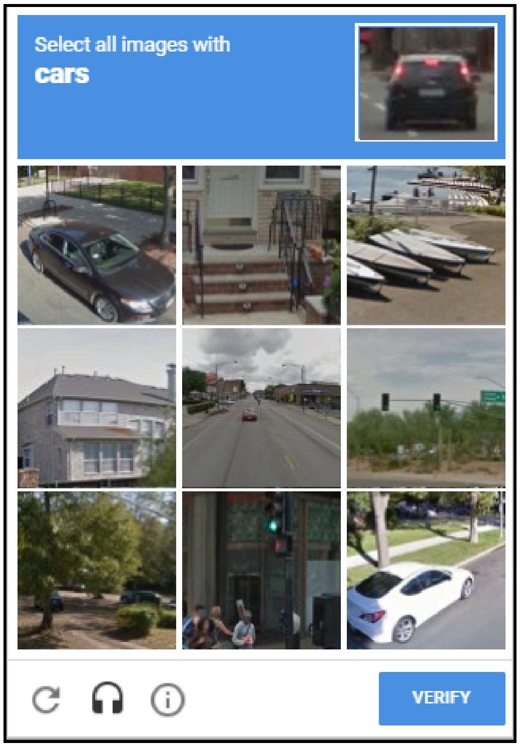
Robbery files from witness

Attach any video files that you have for the file request.

Drop files to share here

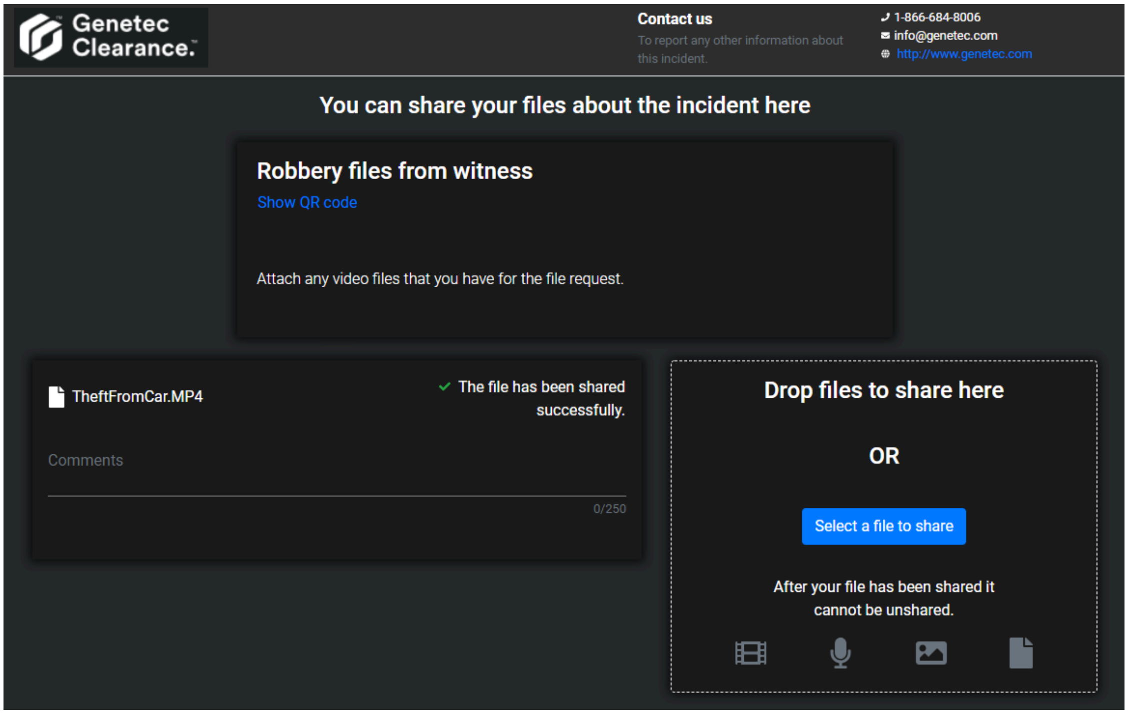
After your file has been shared it cannot be unshared.

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.



Contact us
To report any other information about this incident.
1-866-684-8006
info@genetec.com
http://www.genetec.com

You can share your files about the incident here

Robbery files from witness
Show QR code

Attach any video files that you have for the file request.

TheftFromCar.MP4
✓ The file has been shared successfully.
Comments
0/250

Drop files to share here
OR
Select a file to share
After your file has been shared it cannot be unshared.

14

Clearance plugin

Export Security Center video as evidence to an account in the Clearance system.

This section includes the following topics:

- "About Clearance Plugin for Security Center" on page 250

About Clearance Plugin for Security Center

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.

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

To link the Genetec Clearance™ Plugin for Security Center with your Clearance account, you must Create an integration and download the configuration file.

For more information, see the latest Clearance Plugin Guide. To download the Clearance plugin for Security Center, click **here**.

Related Topics

Creating integrations on page 54

Approving video requests on page 209

15

Clearance Drive

Manage file transfers to and from Clearance.

This section includes the following topics:

- "About Clearance Drive" on page 252
- "Installing Clearance Drive" on page 253
- "Clearance Drive user interface tour" on page 256
- "Managing cases using Clearance Drive" on page 258
- "Transferring files using Clearance Drive" on page 261
- "Configuring settings in Clearance Drive" on page 262

About Clearance Drive

Clearance Drive is an application used to transfer files, such as those generated by VMS, in-car systems, cellphones or body cameras, to Clearance. Clearance Drive uses Windows File Explorer to facilitate mass transfer of files to and from Clearance. You can also create cases using Clearance Drive.

Clearance Drive includes the following components:

- **Clearance Drive agent:** The Clearance Drive agent is the user interface component of the application that is used to manage media uploads.

Example

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

▶

Related Topics

Installing Clearance Drive on page 253

Installing Clearance Drive

Before you can transfer files or create cases using Clearance Drive, you must complete the installation procedure.

Before you begin

The following prerequisites apply when installing the Clearance Drive application.

- A user with Windows Admin access to install the application.
- Windows 10 is the minimum version supported with Clearance Drive.
- To login with Clearance Drive, you must have a user account in Clearance.
- You must have an active internet connection.

What you should know

- The program and associated files are installed in the current users Windows profile.
- Clearance Drive software updates occur automatically after the initial installation.

Procedure

1. Download the application install package.
2. Select the *ClearanceDrive* installer *.exe* file and click **RUN**.
   The Clearance *Drive Setup* window opens.
3. Accept the terms of the installer and finish the installation.

4 Connect Clearance Drive with your Clearance account.

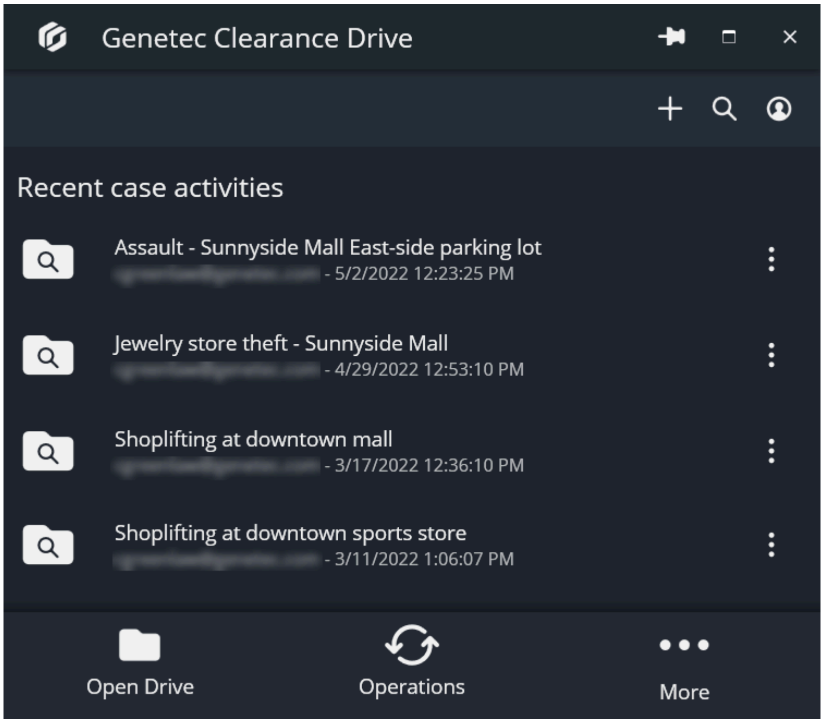
a) Select the data center where your Clearance account is hosted.

b) Sign in using your email address and password.

c) Select the Clearance account you require.

NOTE: To open the Clearance Drive, click the **Clearance Drive** icon ( ) located in the Windows system tray.

- Clearance Drive opens.



Genetec Clearance Drive

Recent case activities

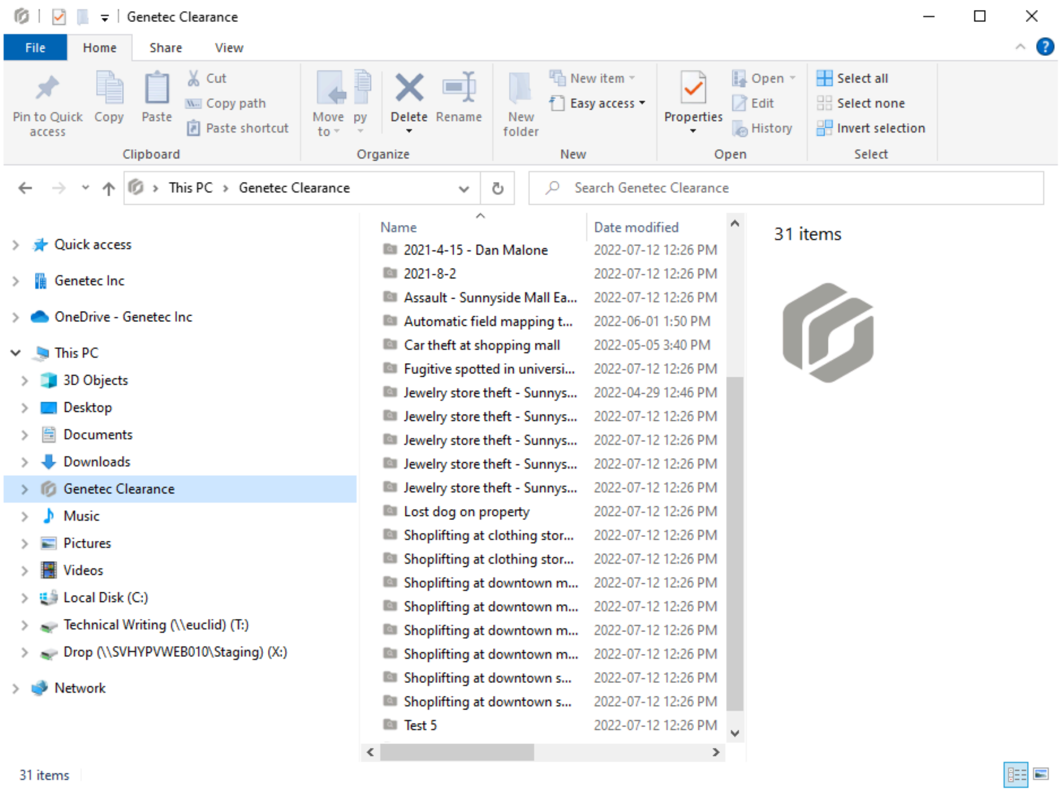
Assault - Sunnyside Mall East-side parking lot
[redacted] - 5/2/2022 12:23:25 PM

Jewelry store theft - Sunnyside Mall
[redacted] - 4/29/2022 12:53:10 PM

Shoplifting at downtown mall
[redacted] - 3/17/2022 12:36:10 PM

Shoplifting at downtown sports store
[redacted] - 3/11/2022 1:06:07 PM

- Clearance Drive is shown when you navigate to the file explorer.



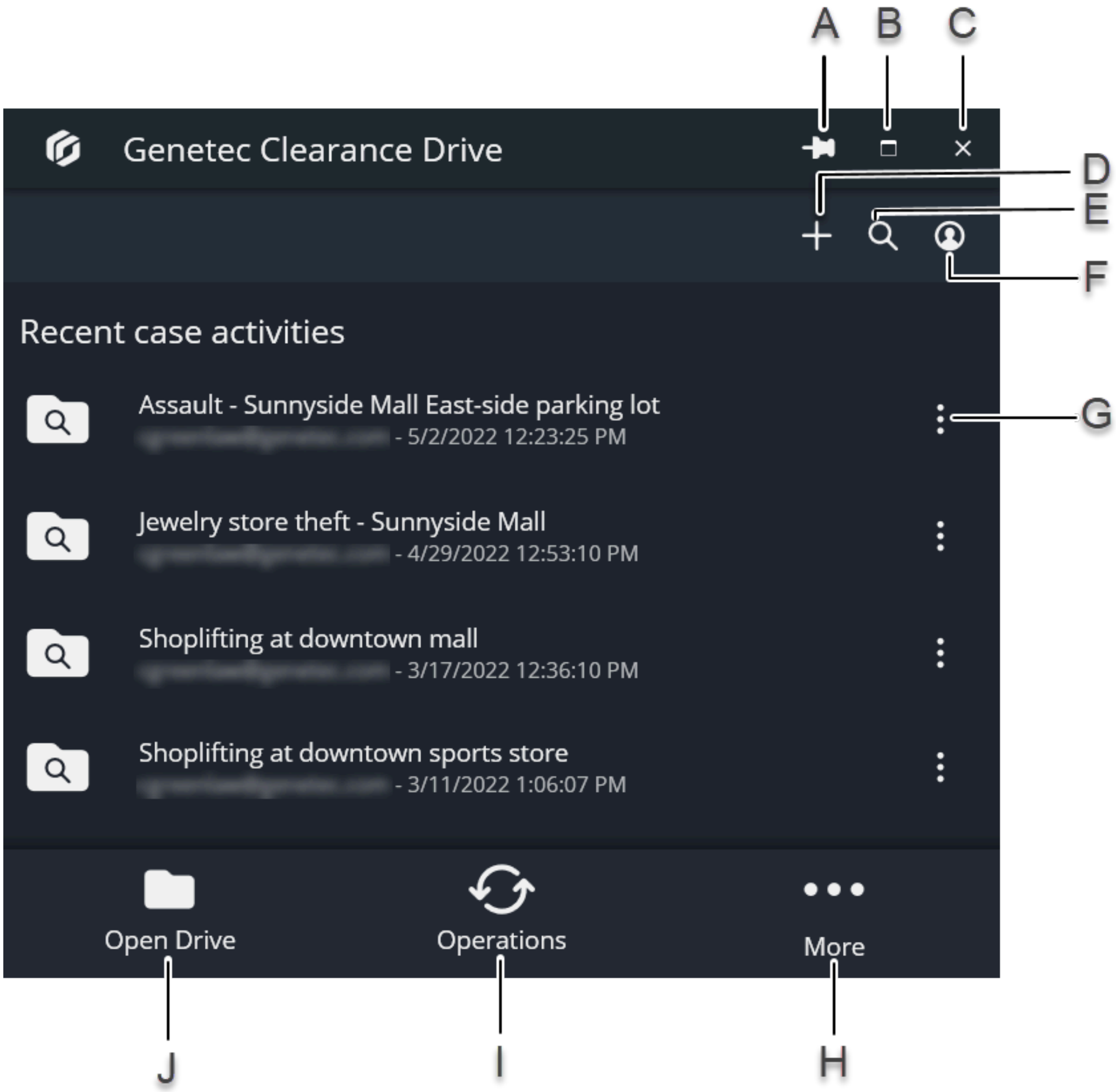
Name	Date modified
2021-4-15 - Dan Malone	2022-07-12 12:26 PM
2021-8-2	2022-07-12 12:26 PM
Assault - Sunnyside Mall Ea...	2022-07-12 12:26 PM
Automatic field mapping t...	2022-06-01 1:50 PM
Car theft at shopping mall	2022-05-05 3:40 PM
Fugitive spotted in universi...	2022-07-12 12:26 PM
Jewelry store theft - Sunnys...	2022-04-29 12:46 PM
Jewelry store theft - Sunnys...	2022-07-12 12:26 PM
Jewelry store theft - Sunnys...	2022-07-12 12:26 PM
Jewelry store theft - Sunnys...	2022-07-12 12:26 PM
Jewelry store theft - Sunnys...	2022-07-12 12:26 PM
Lost dog on property	2022-07-12 12:26 PM
Shoplifting at clothing stor...	2022-07-12 12:26 PM
Shoplifting at clothing stor...	2022-07-12 12:26 PM
Shoplifting at downtown m...	2022-07-12 12:26 PM
Shoplifting at downtown m...	2022-07-12 12:26 PM
Shoplifting at downtown m...	2022-07-12 12:26 PM
Shoplifting at downtown m...	2022-07-12 12:26 PM
Shoplifting at downtown s...	2022-07-12 12:26 PM
Shoplifting at downtown s...	2022-07-12 12:26 PM
Test 5	2022-07-12 12:26 PM

Related Topics

Clearance Drive user interface tour on page 256

Clearance Drive user interface tour

Get to know Clearance Drive's layout and feature set using the following user interface description.



A	**Pin**	Lock the Clearance Drive to the desktop.
B	**Expand**	Expand the Clearance Drive to occupy the entire screen.
C	**Exit**	Close the Clearance Drive window.
D	**New case**	Create a new case from Clearance Drive. For more information about creating cases, see Managing cases using Clearance Drive on page 258.

E	**Search**	Search for cases in Clearance Drive. For more information about creating cases, see Managing cases using Clearance Drive on page 258.
F	**Account options**	View your account name, the area your data center is located in, change your account, or sign out.
G	**Case options**	Open the case in a file explorer window or download the case to your local drive. For more information about creating cases, see Managing cases using Clearance Drive on page 258.
H	**More**	Configure settings, cancel ongoing operations, consult the Clearance Drive help, or close Clearance Drive. For more information about configuring settings, see Configuring settings in Clearance Drive on page 262.
I	**Operations**	Monitor in-progress file transfers and downloads.
J	**Open drive**	Open the Clearance Drive in a file explorer window.

Related Topics

Managing cases using Clearance Drive on page 258

Managing cases using Clearance Drive

Create cases in Clearance Drive and review them in Clearance later.

Before you begin

Install Clearance Drive.

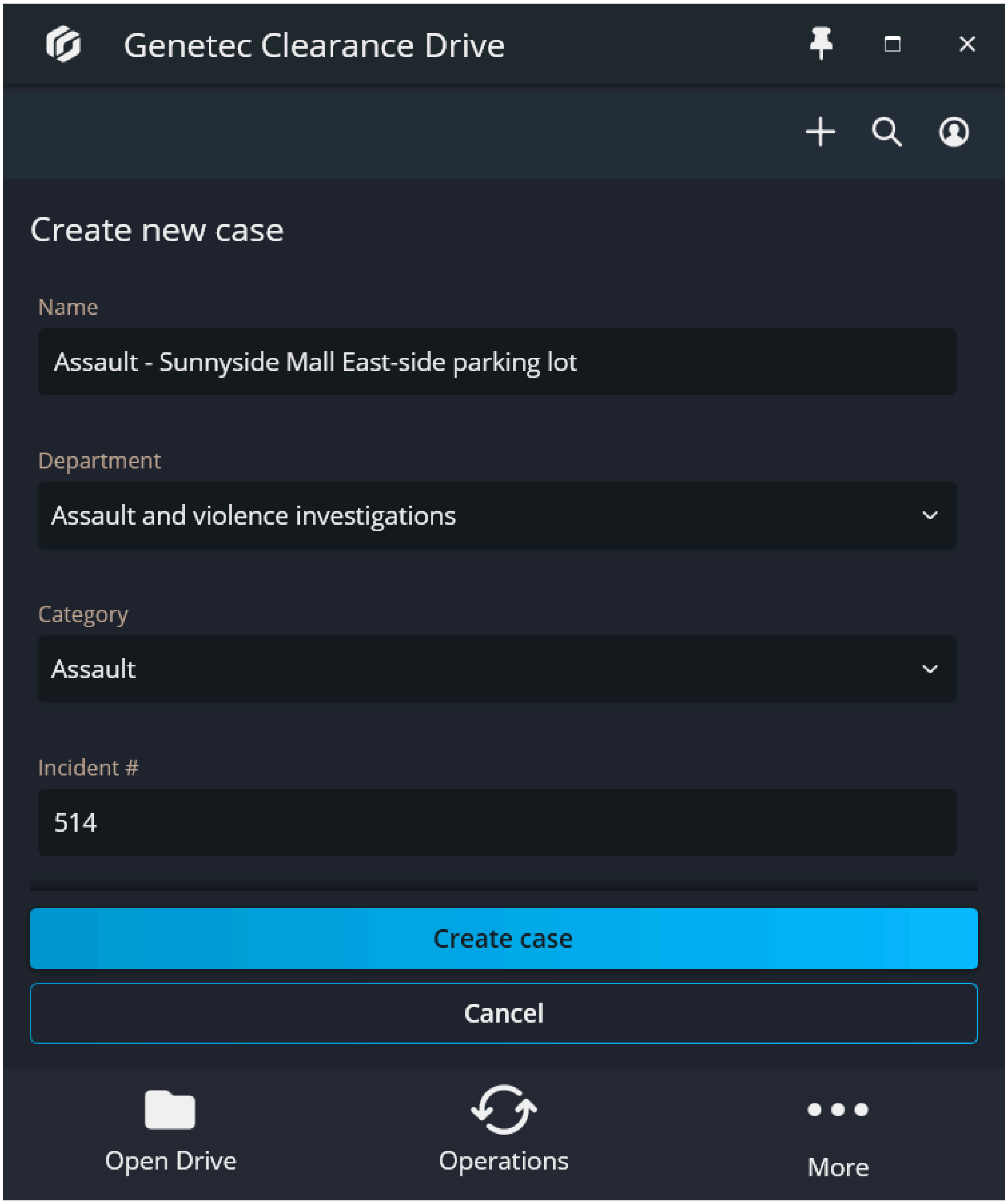
Procedure

To create a case in Clearance Drive:

1 From the Clearance Drive header, click **Create case** (+).

2 Click **Create new case**.

3 Enter information into the case fields:
   a) Enter a name for the case.
   b) Assign the case to a department.
   c) Assign a category to the case.
   d) Enter an incident number for the case.



Genetec Clearance Drive

Create new case

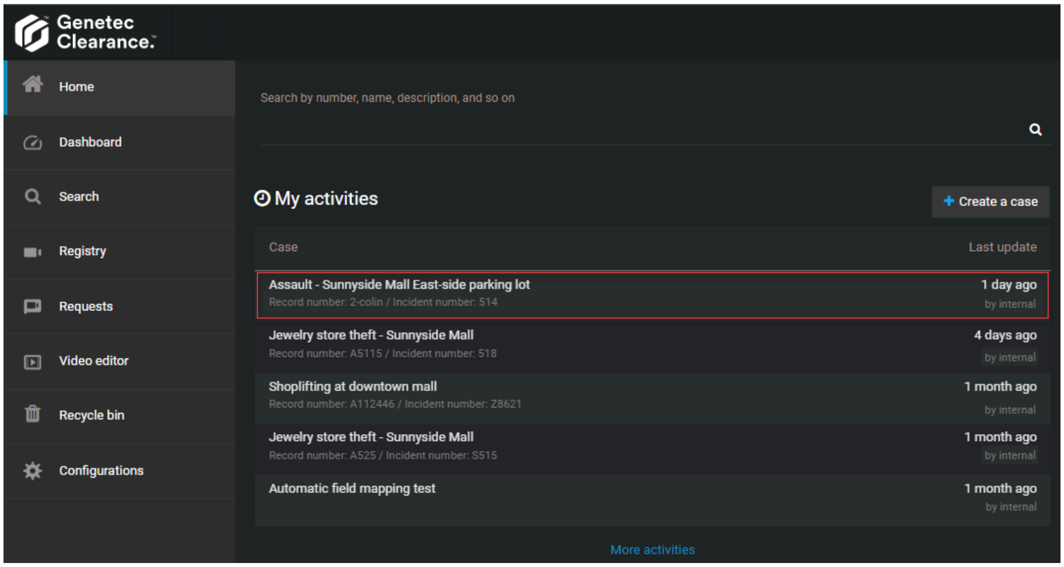
Name: Assault - Sunnyside Mall East-side parking lot

Department: Assault and violence investigations

Category: Assault

Incident #: 514

4 Click **Create case**.
   The case is created.
   NOTE:



Case	Last update
Assault - Sunnyside Mall East-side parking lot Record number: 2-colin / Incident number: 514	1 day ago by internal
Jewelry store theft - Sunnyside Mall Record number: A5115 / Incident number: 518	4 days ago by internal
Shoplifting at downtown mall Record number: A112446 / Incident number: Z8621	1 month ago by internal
Jewelry store theft - Sunnyside Mall Record number: A525 / Incident number: S515	1 month ago by internal
Automatic field mapping test	1 month ago by internal

You can view the case in Clearance and add further field information and metadata to it there.

To search for a case using Clearance Drive:

1 From the Clearance Drive header, click **Search** (🔍).

2 Click **Search**.

3 Enter the search terms you require.

4 Double click the relevant case to view the files.

After you finish

Log in to Clearance and add further information to the case. For more information, see Creating cases in Clearance.

Related Topics

Transferring files using Clearance Drive on page 261

Transferring files using Clearance Drive

You can use Clearance Drive to transfer files to and from cases in your Clearance account.

Before you begin

Create cases using Clearance Drive.

Procedure

To download files from a case using Clearance Drive:

1 Search for a case, or select a case from the homepage.

2 Find the file you want to download, click **More** (⋮).

3 Choose to download the original or a converted MP4 version of the file.

NOTE: MP4 is a widely supported file format, but you can also download the original version for use in Security Center and to ensure information security.

4 Select a folder to download the file to.

The file is downloaded.

To transfer a large number of files simultaneously using the file explorer view starting from Clearance Drive:

1 From the Clearance Drive homepage, select the case you require.

2 Click **Open folder**.

3 Browse or search for the case you require and select it.

4 Browse the files located in the case - select the file you want to download, and choose to download the original file, or a converted MP4 version.

5 To upload files to the case, drag and drop the file on the case into the Windows Explorer window.

To transfer a large number of files simultaneously starting from the file explorer view:

1 Open file explorer and navigate to Clearance, located under **This PC**.

2 Browse or search for the case you require and select it.

3 Browse the files located in the case - select the file you want to download, and choose to download the original file, or a converted MP4 version.

4 To upload files to the case, drag and drop the file on the case into the Windows Explorer window.

TIP: You can monitor the status of in-progress file transfers from the **Operations page**.

Related Topics

Configuring settings in Clearance Drive on page 262

Configuring settings in Clearance Drive

Configure drive location, network settings, and delete files using the Clearance Drive settings menu.

Before you begin

Install Clearance Drive.

Procedure

To configure settings in Clearance Drive:

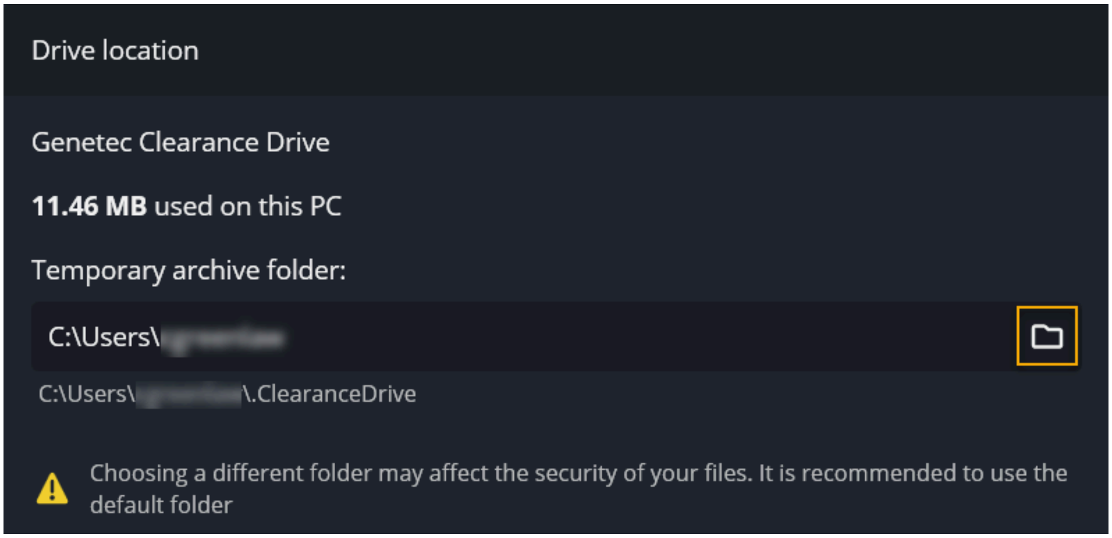
1 From the Clearance Drive homepage, click **More** (⋯).

2 From the drop-down menu, click **Settings**.

To configure general settings:

1 If you want Clearance drive to launch automatically upon starting your computer, check the **Start Clearance Drive automatically when I sign in to Windows** checkbox.

2 In the **Temporary archive folder** field, click **Browse** (🗀) and select a location for Clearance Drive, or enter a file path in the field.



Drive location

Genetec Clearance Drive

11.46 MB used on this PC

Temporary archive folder:

C:\Users\[redacted]

C:\Users\[redacted]\.ClearanceDrive

⚠ Choosing a different folder may affect the security of your files. It is recommended to use the default folder

3 If you need to delete all the temporary files that were downloaded from Clearance Drive, click **Delete all files from local drive**.

NOTE: This action does not delete all associated files from Clearance Drive. It only deletes the local files you have downloaded.

To configure network settings:

1 From the Clearance Drive homepage, click **More** (⋯).

2 From the drop-down menu, click **Settings**.

3 Click the **Network** tab.

4 From the **Upload rate** section, choose how much bandwidth to dedicate to uploads by selecting the **Limit to** option and setting an upload rate limit in megabytes per second.

5 From the **Download rate** section, choose how much bandwidth to dedicate to downloads by selecting the **Limit to** option and setting a download rate limit in megabytes per second.

16

Clearance Uploader application

Automatically upload media from devices to Clearance, or a Security Center video archive.

This section includes the following topics:

- "About Clearance Uploader" on page 264
- "Installing the Clearance Uploader" on page 266
- "Configuring the Clearance Uploader" on page 268
- "Uploading media using the Clearance Uploader" on page 270
- "Monitoring Clearance Uploader activities" on page 273
- "Viewing Clearance Uploader event logs" on page 276

About Clearance Uploader

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.

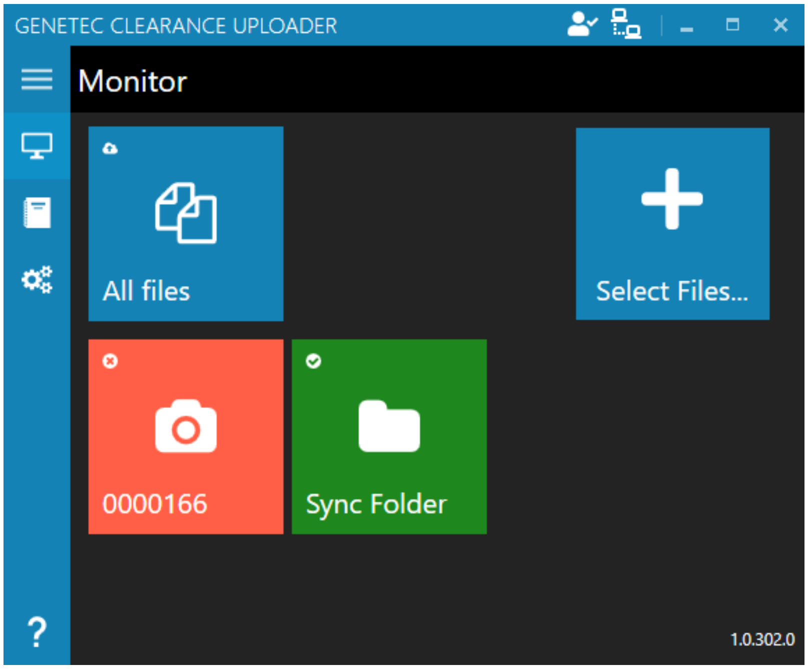
The Clearance Uploader application includes the following components:

- **Clearance Uploader agent:** The Clearance Uploader agent (*Genetec.SaaS.Dems.Uploader.Agent.exe*) is the user interface component of the application that is used to check the status of media uploads.
- **Clearance Uploader integration:** The Clearance Uploader integration (*Genetec.SaaS.Dems.Uploader.Integration.exe*) is the Windows integration component of the application that performs media uploads automatically in the background. To link the Clearance Uploader with your Clearance account, you must create an integration.

  TIP: Scheduled uploads can help you avoid using bandwidth during office hours by deferring uploads to a more convenient time. Scheduled uploads are also useful if you are using a multi-dock or are uploading media from multiple devices, which might consume excessive bandwidth.

  The Clearance Uploader supports a maximum of 26 concurrent cameras per workstation or server when using a multi-dock.

Use the Clearance Uploader to view and manage media uploads.



The Genetec Clearance™ Uploader application menu includes the following controls:

Menu items	Description
✓ Ready Status	Displays the current status of the Clearance Uploader application. For example, **Not configured**, **Ready** and so on.
≡ Menu	Expands the sidebar menu items.

Menu items	Description
Monitor	**All files** displays the status of files being downloaded to the client workstation. **Select Files** opens a dialog to add files to an existing case, create a case and upload, or skip case selection and upload evidence. **NOTE:** The uploader must have *Manage* permissions for a case to upload files to cases. **Connected device** displays the status of connected devices. **Sync folder** displays the status of files being uploaded to Clearance. **NOTE:** The Sync folder tile is only available when the Sync folder option has been enabled in **Settings**.
Event logs	Displays event log information and error messages.
Settings	Specifies account setup information, upload schedule, application log settings, and bandwidth settings. **NOTE:** You must have Windows Administrator access to view or change these settings.
? About	Displays Clearance Uploader application version information.

Example

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

Installing the Clearance Uploader

Before you can use the Genetec Clearance™ Uploader, you must install and configure the application.

Before you begin

The following prerequisites apply when installing the Clearance Uploader application.

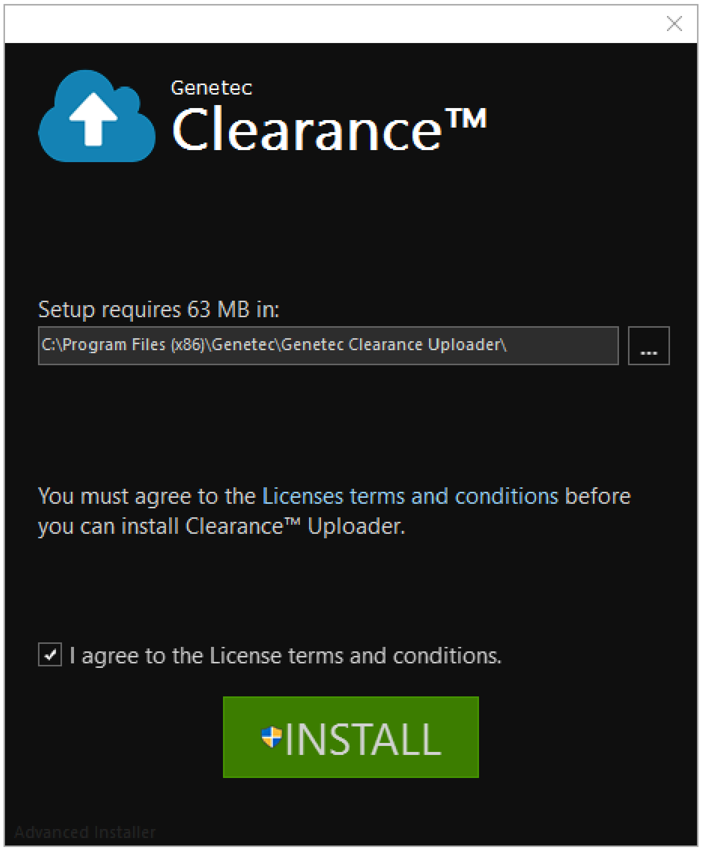
- A user with Windows Admin access might be required for installation, access to the **Settings** menu items, and auto updates.
- The Clearance Uploader must be associated with a Clearance account to upload media to that account.
- You must have an active internet connection.
- You must create a Clearance Uploader integration if one is not already set up.

What you should know

The program and associated files are installed in *C:\Program Files (x86)\Genetec\Clearance Uploader*.

Procedure

1. Download the application install package.
2. Select the *GenetecClearanceUploader* installer *.exe* file and click **RUN**.
3. Select the **I agree to the License terms and conditions.** check box and click **Install** to begin the installation.



Setup requires 63 MB in:

C:\Program Files (x86)\Genetec\Genetec Clearance Uploader\

You must agree to the Licenses terms and conditions before you can install Clearance™ Uploader.

☑ I agree to the License terms and conditions.

4. Click **Finish**.

5 Set up your Clearance Uploader account:

The Clearance Uploader account setup wizard opens.

NOTE: The first time that you configure your account the wizard is automatically started.

a) On the Account Setup wizard welcome screen, click **Next**.

b) Select the Clearance account that you want to upload files to. Click **Browse** and select a Clearance Uploader configuration file. For example, select *config.json* and then click **Open**.

c) Click **Next** > **Complete**.

The Clearance Uploader application is now ready to use.

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

You can change the Clearance Uploader settings at any time from the *settings* section in the Clearance Uploader.

NOTE: If you need to uninstall the Clearance Uploader application, follow the standard Windows uninstall process for programs and features.

Related Topics

Creating integrations on page 54

Enrolling Axis and Reveal body-worn cameras on page 136

Activating device licenses on page 129

Configuring the Clearance Uploader

Before you can use the Genetec Clearance™ Uploader application, configure the application settings. This includes account setup information, upload schedule, application log settings, bandwidth and sync folder settings.

Before you begin

Create a Clearance Uploader integration if one is not already set up.

What you should know

You can set up your account during installation using the Clearance Uploader account setup wizard. However, you can change your account settings at any time. For example, you can change account information, add or change an upload schedule, send logs to Clearance, or limit bandwidth.

Procedure

1 Click **Settings** > **Set up Your Account**.

The Clearance Uploader account setup wizard opens.

NOTE: The first time that you configure your account the wizard is automatically started.

a) On the Account Setup wizard welcome screen, click **Next**.

b) Select the Clearance account that you want to upload files to. Click **Browse** and select a Clearance Uploader configuration file. For example, select *config.json* and then click **Open**.

c) Click **Next** > **Complete**.

2 (Optional) Define an Upload Schedule.

a) Specify a start time.

b) Specify an end time.

These deferred upload schedule settings define a time range when the Clearance Uploader can upload media to the Clearance account. Media is uploaded immediately if the fields are left blank.

NOTE: Scheduled uploads can help you avoid using bandwidth during office hours by deferring uploads to a more convenient time. Scheduled uploads are also useful if you are using a multi-dock or are uploading media from multiple devices, which might consume excessive bandwidth.

3 (Optional) Send application logs to support. Slide the **Send application log** to **On** when you want to send anonymous logs to us for support purposes.

4 (Optional) Set a bandwidth limit. Slide the **Limit Bandwidth** to **On** when you want to specify a bandwidth limit in MB/s.

This setting specifies the maximum bandwidth the Clearance Uploader agent can use during media upload.

5 (Optional) Define a Sync folder. Set the **Sync folder** to **On** if you want to automatically upload files in the folder to Clearance.

IMPORTANT: Changing the **Sync folder** setting requires a manual restart of the Clearance Uploader. The **Sync folder** that you defined is automatically created for you after the Clearance Uploader is restarted.

6 (Optional) Define a Storage folder. Set the **Storage folder** to **On** if you want to change the default storage path to specify where files should be stored before uploading to Clearance.

IMPORTANT: Changing the **Storage folder** setting requires a manual restart of the Clearance Uploader. The **Storage folder** that you defined is automatically created for you after the Clearance Uploader is restarted.

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

You can change the Clearance Uploader settings at any time from the *settings* section.

Related Topics

Creating integrations on page 54
Enrolling Axis and Reveal body-worn cameras on page 136
Activating device licenses on page 129

Uploading media using the Clearance Uploader

You can use the Genetec Clearance™ Uploader application to automatically upload videos, media, and other file types without manually logging into Clearance. Uploaded files are searchable and can be added to cases. The Uploader automatically resumes the upload process after an interruption, making it a great solution when uploading larger files or a large selection of files.

Before you begin

The following prerequisites apply when uploading media using the Clearance Uploader.

- The Clearance Uploader must be associated with a Clearance account to upload media to that account.
- You must have an active internet connection.

What you should know

To simplify importing files to Clearance, you can use the Clearance Uploader application to transfer large files or a selection of files directly from your desktop.

The media files are then uploaded from your client to your Clearance account. Deferred schedule uploads can optimize this process by performing the upload activities at a more convenient time.

Scheduled uploads can help you avoid using bandwidth during office hours by deferring uploads to a more convenient time. Scheduled uploads are also useful if you are using a multi-dock or are uploading media from multiple devices, which might consume excessive bandwidth.

The Clearance Uploader supports a maximum of 26 concurrent cameras per workstation or server when using a multi-dock.

Logs are also kept to provide details about media uploads. These event logs can be found in *C:\ProgramData\AppData\Local\Genetec Clearance\logs*.

Procedure

To download media from a body-worn Camera:

1 Download the files to your client workstation by completing the following steps:

a) (Optional) Click the ☁ icon to start the Clearance Uploader agent.

b) Dock your body-worn Camera.

Media files are automatically downloaded from the camera and saved to your client workstation. (The media files can be found in *C:\ProgramData\AppData\Local\Genetec Clearance\data\files*).

TIP: Status LEDs on the dock indicate when download activities are in progress.

After the download completes, the media files are deleted from the camera.

NOTE: The camera tile in the *Monitor* page turns green after the download completes to indicate that the camera can be removed from the dock.

To automatically upload media to your Clearance account:

1 The media files are uploaded from your client to your Clearance account.

Depending on your defined settings, one of the following occurs:

- If no schedule is specified, the media files are uploaded immediately to your Clearance account. During upload the following states can occur: Uploading, In Progress, Completing, Completed, Calculating, and Pending.
- If an upload schedule is specified, the media files are automatically uploaded to the Clearance account at the deferred schedule time. Scheduled uploads are useful when using a multi-dock or when uploading media from multiple devices.
- If a sync folder is enabled in the configuration settings, any files put in the sync folder are uploaded immediately.

After the media files upload completes, the media files are deleted from the client workstation.

NOTE: You can set up or change an **Upload schedule** or **Sync folder** in the ⚙ *Settings* section of the Clearance Uploader agent. You must have administrator access to view or change these settings.

To manually upload media to your Clearance account:

1 Click **Select files**.

2 Select the file or files that you want to upload and click **Open**.

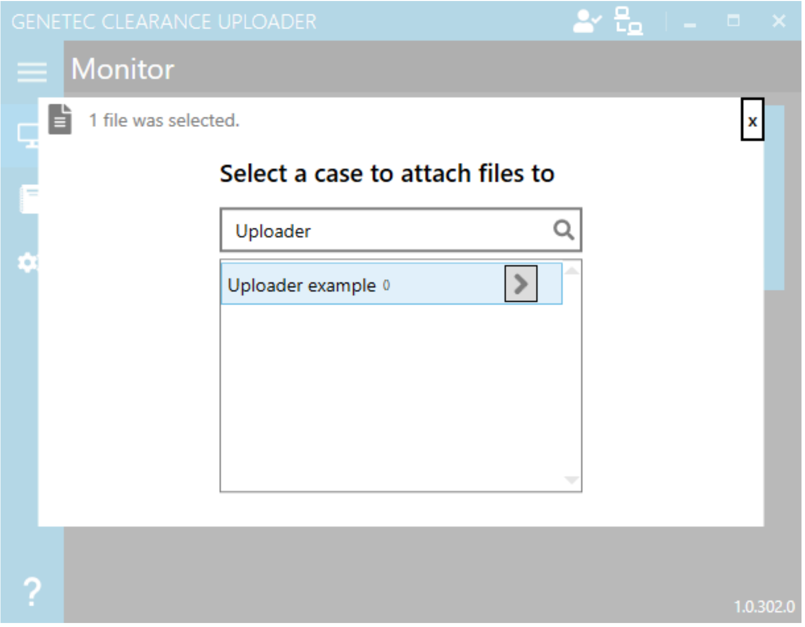
3 Select a case association or upload option.

- Select existing case
- Create a new case
- Skip and upload evidence

4 If you clicked **Select existing case**, do the following:

a) Enter the case title, record number, or incident number in the search field and click **Search**.

b) Select the case that you need and click > to upload the file to the selected case.



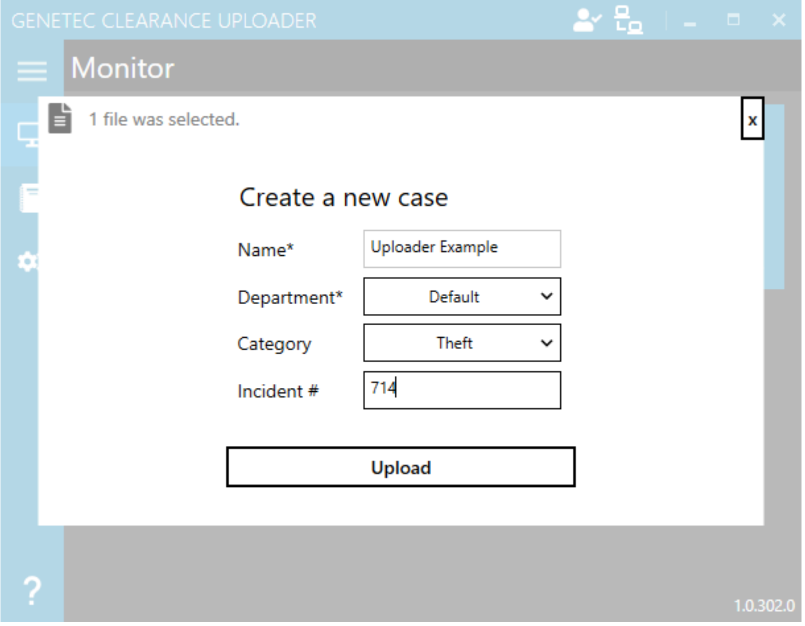
1 file was selected.

Select a case to attach files to

Uploader

Uploader example 0

5 If you clicked **Create a new case**, do the following:
   a) Enter a name.
   b) Select a department from the **Department** drop-down list.
   c) Select a category from the **Category** drop-down list.
   d) Enter an incident number.
   e) Click **Upload**.



1 file was selected.

Create a new case

Name* Uploader Example

Department* Default

Category Theft

Incident # 714

6 If you clicked **Skip and upload evidence**, the file is uploaded with no case association.

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

You can now add the media files to their respective cases.

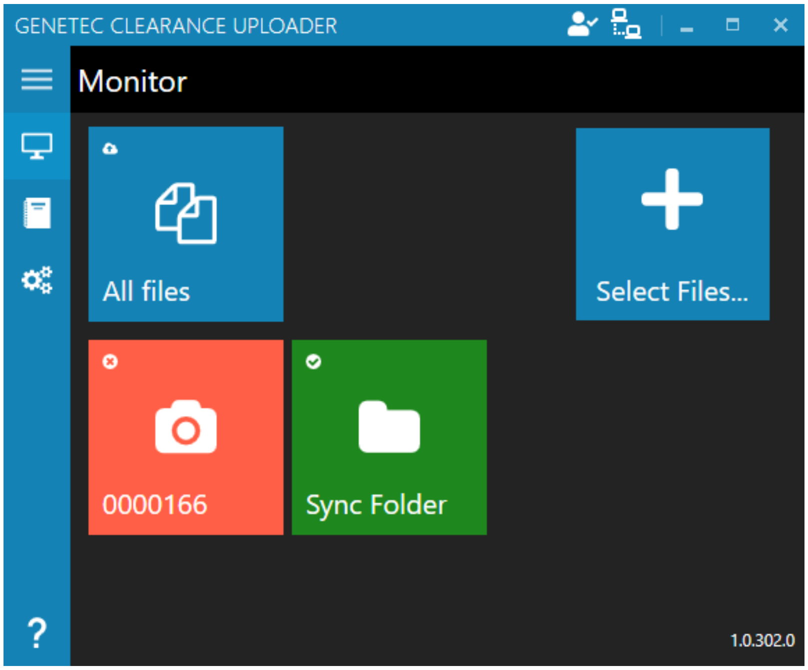
Monitoring Clearance Uploader activities

To view and manage the status of connected devices, files being downloaded to the client workstation, and files being uploaded to Genetec Clearance™ Uploader, use the Clearance Uploader *Monitor* page.

Procedure

1 In the applica application, click **Monitor** 🖥.

2 Choose a monitoring activity.



a) Click the **Camera** tile to display the status of files to download from the camera to client workstation including the file name, device, progress, rate, and state.

Camera tile status icons include the following:

- A device is connected.
- Downloads to the client workstation are in progress.
- Downloads to the client workstation are complete.
- Camera is disconnected.
- An error is encountered. For example, the device stops responding or is removed from the dock while an activity is in progress.

NOTE: The camera tile remains visible for 60 minutes after the camera is disconnected.

b) Click the **All files** tile to display the status of files to upload to Genetec Clearance™ including the file name, device, progress, rate, and state.

All files tile status icons include the following:

- Uploads to Clearance are in progress.
- Uploads are complete.

c) Click the **Sync folder** tile to display the status of files to upload to Clearance including the file name, device, progress, rate, and state.

NOTE: The **Sync folder** tile is only available when the Sync folder option has been enabled in **Settings**.

Sync folder tile status icons include the following:

- Uploads to Clearance are complete.
- There are no files to upload.

Example

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

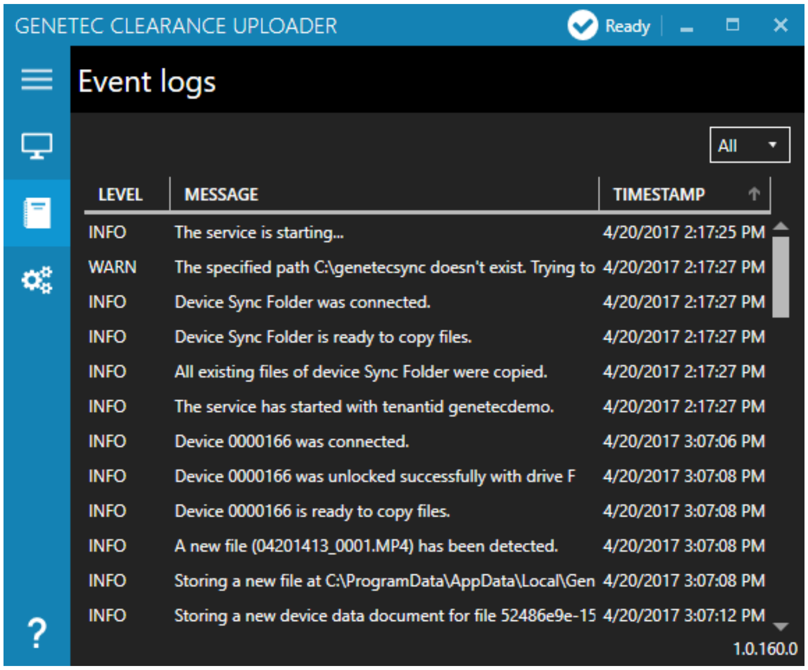
Viewing Clearance Uploader event logs

You can investigate the files being downloaded to the client workstation, files being uploaded to Genetec Clearance™ Uploader, or the status of a connected device by viewing the Clearance Uploader event logs.

Procedure

1 In the applica application, click **Event logs** .

2 View the **Event logs** history.



GENETEC CLEARANCE UPLOADER

Ready

Event logs

All

LEVEL	MESSAGE	TIMESTAMP
INFO	The service is starting...	4/20/2017 2:17:25 PM
WARN	The specified path C:\genetecsync doesn't exist. Trying to	4/20/2017 2:17:27 PM
INFO	Device Sync Folder was connected.	4/20/2017 2:17:27 PM
INFO	Device Sync Folder is ready to copy files.	4/20/2017 2:17:27 PM
INFO	All existing files of device Sync Folder were copied.	4/20/2017 2:17:27 PM
INFO	The service has started with tenantid genetecdemo.	4/20/2017 2:17:27 PM
INFO	Device 0000166 was connected.	4/20/2017 3:07:06 PM
INFO	Device 0000166 was unlocked successfully with drive F	4/20/2017 3:07:08 PM
INFO	Device 0000166 is ready to copy files.	4/20/2017 3:07:08 PM
INFO	A new file (04201413_0001.MP4) has been detected.	4/20/2017 3:07:08 PM
INFO	Storing a new file at C:\ProgramData\AppData\Local\Gen	4/20/2017 3:07:08 PM
INFO	Storing a new device data document for file 52486e9e-15	4/20/2017 3:07:12 PM

1.0.160.0

- Click the **Level** column header to sort the events by level in ascending or descending order.
- Click the **Message** column header to sort the events by message in ascending or descending alphabetical order.
- Click the **Timestamp** column to sort the events by date and time in ascending or descending order.

3 (Optional) Click the drop-down menu in the upper right corner to filter the events by event level. Select one of the following: **All**, **Info**, or **Error** events.

Example

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

17

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.

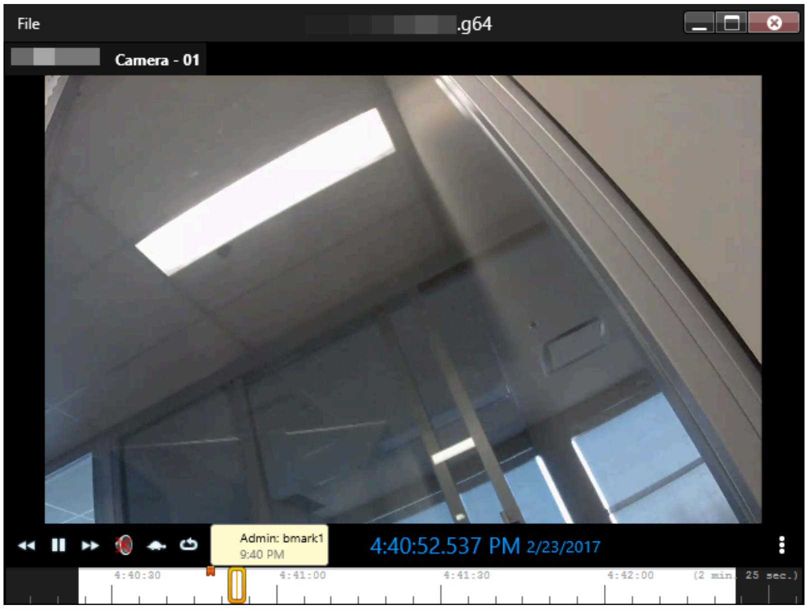
This section includes the following topics:

- "About Genetec™ Video Player" on page 278
- "Downloading Genetec™ Video Player" on page 279
- "Viewing G64 or G64x video files in the Genetec™ Video Player" on page 280

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

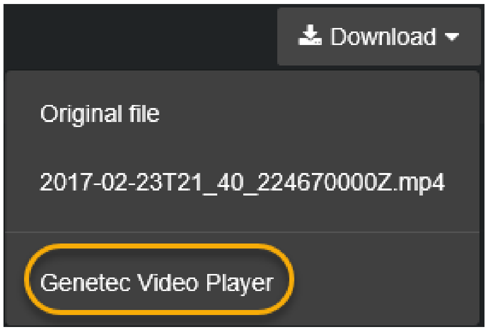
When a *G64* or *G64x* video file has been uploaded into Clearance, users can download the Genetec™ Video Player so that they can download, share, and playback the original files.

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.

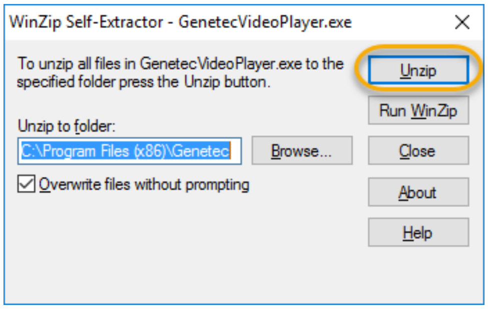
2 Click **Download** and then click **Genetec™ Video Player**.



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**.



To unzip all files in GenetecVideoPlayer.exe to the specified folder press the Unzip button.

Unzip to folder: C:\Program Files (x86)\Genetec

☑ Overwrite files without prompting

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.

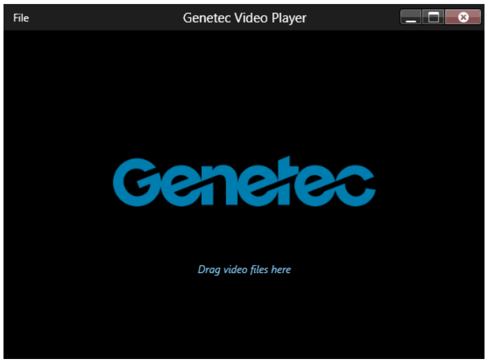
What you should know

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.

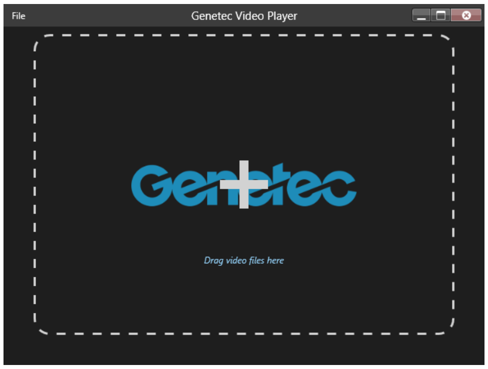
Procedure

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

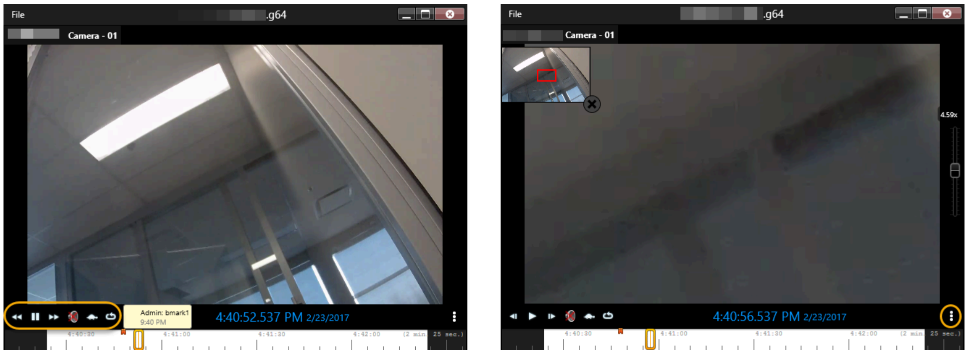
For example, double-click the *Genetec Video Player.exe* in *C:\Program Files (x86)\Genetec\GenetecVideoPlayer*



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.

Related Topics

File formats you can preview in Clearance on page 180
Reviewing media on page 168
Downloading files on page 182

18

Clearance Seen

Capture videos, images, and audio recordings from your phone and upload evidence directly to your Clearance account.

This section includes the following topics:

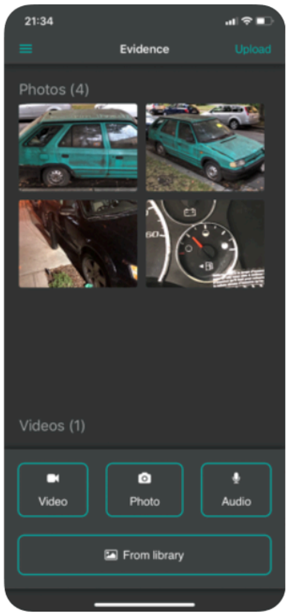
- "About Clearance™ Seen" on page 283

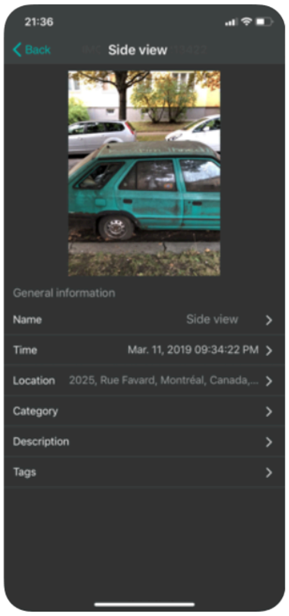
About Clearance™ Seen

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.

With Genetec Clearance™ Seen, you can do the following:

- Send videos, photos, and audio recordings to Genetec Clearance™ accounts
- Assign evidence directly to cases
- Assign a case directly to a department
- Include additional information, like notes and GPS coordinates, and assign categories
- Add tags to quickly find evidence in future searches





General information

Name: Side view

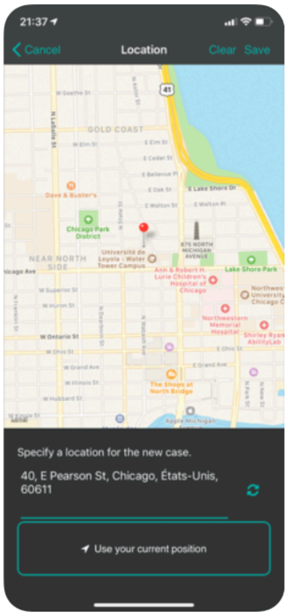
Time: Mar. 11, 2019 09:34:22 PM

Location: 2025, Rue Favard, Montréal, Canada,...

Category

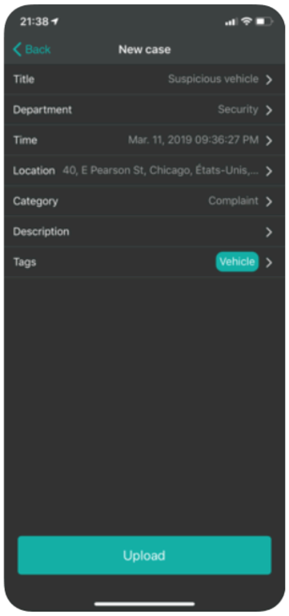
Description

Tags



Specify a location for the new case.

40, E Pearson St, Chicago, États-Unis, 60611



Title: Suspicious vehicle

Department: Security

Time: Mar. 11, 2019 09:36:27 PM

Location: 40, E Pearson St, Chicago, États-Unis,...

Category: Complaint

Description

Tags: Vehicle

NOTE: To download Genetec Clearance™ Seen, visit Google Play or the App Store.

Example

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

19

Frequently asked questions

Learn about common issues in Clearance.

This section includes the following topics:

- "How can I create a bookmark to my Clearance account?" on page 285
- "Why is a preview of a PDF not displayed in Clearance?" on page 288
- "How can I avoid errors when accessing my Clearance account through my browser history?" on page 290
- "Why does my file fail to upload to Clearance?" on page 292
- "Why does the download link fail to work in Google Chrome?" on page 293
- "Change to Clearance login" on page 294

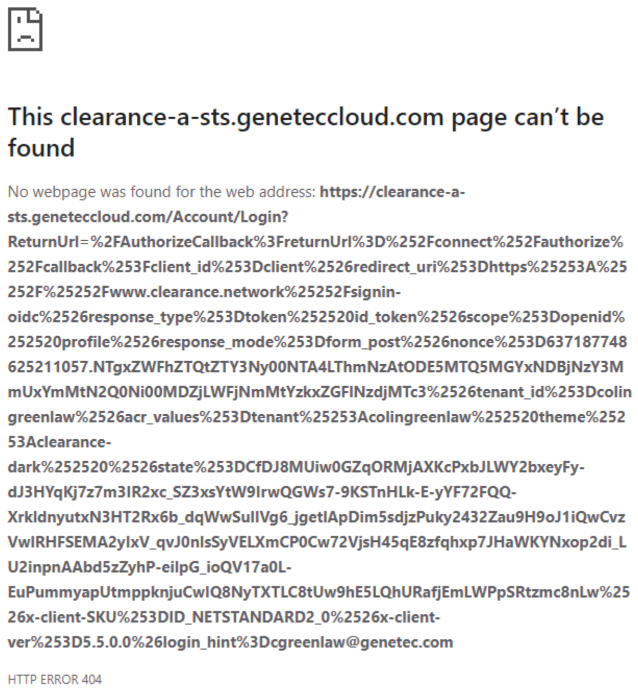
How can I create a bookmark to my Clearance account?

If you encounter an error when you navigate to your bookmarked Clearance account page or have bookmarked the incorrect account, you can fix this by setting up a new bookmark.

Causes

- You bookmarked the URL provided by the **Activate account** button in your confirmation email.
- You bookmarked an incorrect account, such as a testing account instead of your organization's production account.

Example of the error message:



This clearance-a-sts.geneteccloud.com page can’t be found

No webpage was found for the web address: **https://clearance-a-sts.geneteccloud.com/Account/Login?ReturnUrl=%2FAuthorizeCallback%3FreturnUrl%3D%252Fconnect%252Fauthorize%252Fcallback%253Fclient_id%253Dclient%2526redirect_uri%253Dhttps%25253A%25252F%25252Fwww.clearance.network%25252Fsignin-oidc%2526response_type%253Dtoken%252520id_token%2526scope%253Dopenid%252520profile%2526response_mode%253Dform_post%2526nonce%253D637187748625211057.NTgxZWFhZTQtZTY3Ny00NTA4LThmNzAtODE5MTQ5MGYxNDBjNzY3MmUxYmMtN2Q0Ni00MDZjLWFjNmMtYzkxZGFlNzdjMTc3%2526tenant_id%253Dcolingreenlaw%2526acr_values%253Dtenant%25253Acolingreenlaw%252520theme%25253Aclearance-dark%252520%2526state%253DCfDJ8MUiw0GZqORMjAXKcPxbJLWY2bxeyFy-dJ3HYqKj7z7m3IR2xc_SZ3xsYtW9IrwQGWs7-9KSTnHLk-E-yYF72FQQ-XrkldnyutxN3HT2Rx6b_dqWwSullVg6_jgetlApDim5sdjzPuky2432Zau9H9oJ1iQwCvzVwIRHFSEMA2yIxV_qvJ0nlsSyVELXmCP0Cw72VjsH45qE8zfqhxp7JHaWKYNxop2di_LU2inpnAAbd5zZyhP-eilpG_ioQV17a0L-EuPummyapUtmppknjuCwIQ8NyTXTLC8tUw9hE5LQhURafjEmLWPpSRtzmc8nLw%2526x-client-SKU%253DID_NETSTANDARD2_0%2526x-client-ver%253D5.5.0.0%26login_hint%3Dcgreenlaw@genetec.com**

HTTP ERROR 404

Solution

Delete all bookmarked Clearance pages that cause an error. Select the required host as detailed in your account activation email and bookmark it.

NOTE: The hostname displayed before the account ID in your account URL will vary depending on the region where your account is hosted.

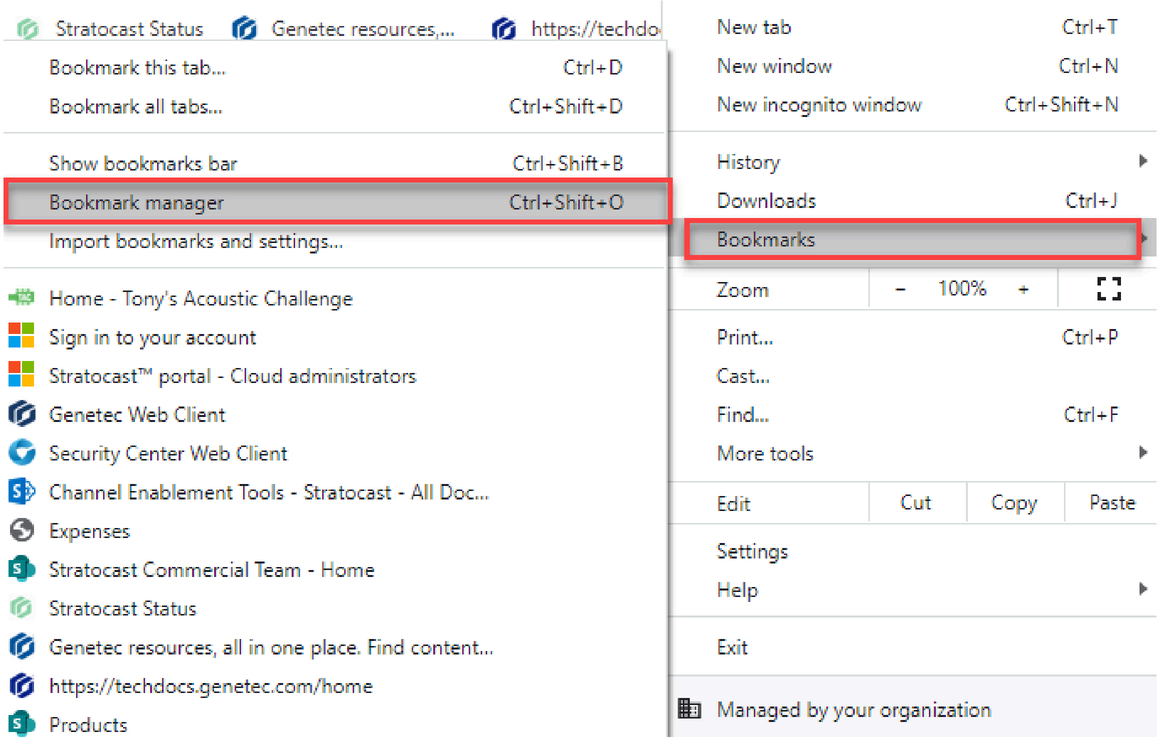
Host list by region

Region	Host
United States	https://www.clearance.network
Europe	https://eu.clearance.network
Australia	https://au.clearance.network

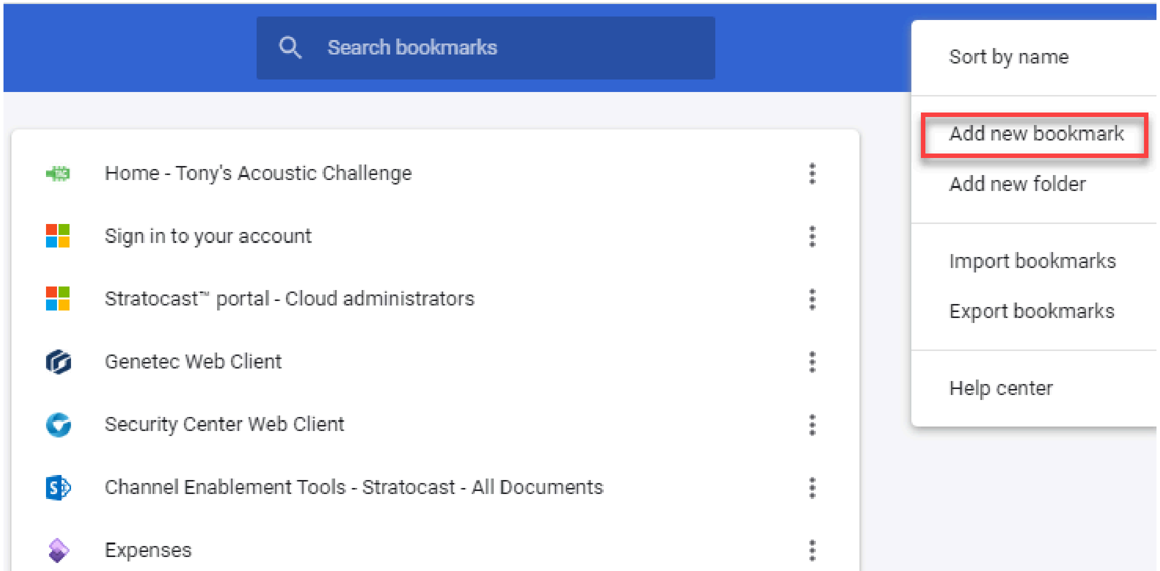
Region	Host
US Government	https://usgov.clearance.network
Canada	https://ca.clearance.network

Bookmarking using Google Chrome

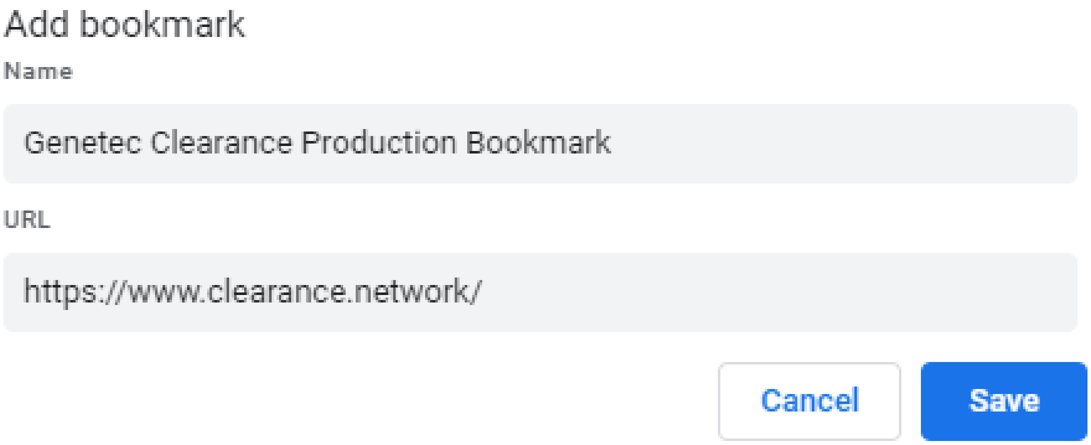
1. Open Google Chrome and, in the top right of the browser window, click **More** (⋮) to open the menu.


Stratocast Status
Genetec resources,...
https://techdo
Bookmark this tab... Ctrl+D
Bookmark all tabs... Ctrl+Shift+D
Show bookmarks bar Ctrl+Shift+B
Bookmark manager Ctrl+Shift+O
Import bookmarks and settings...
Home - Tony's Acoustic Challenge
Sign in to your account
Stratocast™ portal - Cloud administrators
Genetec Web Client
Security Center Web Client
Channel Enablement Tools - Stratocast - All Doc...
Expenses
Stratocast Commercial Team - Home
Stratocast Status
Genetec resources, all in one place. Find content...
https://techdocs.genetec.com/home
Products
New tab Ctrl+T
New window Ctrl+N
New incognito window Ctrl+Shift+N
History
Downloads Ctrl+J
Bookmarks
Zoom – 100% +
Print... Ctrl+P
Cast...
Find... Ctrl+F
More tools
Edit Cut Copy Paste
Settings
Help
Exit
Managed by your organization

2. From the menu, hover over **Bookmarks** and click **Bookmark manager**.


Search bookmarks
Home - Tony's Acoustic Challenge
Sign in to your account
Stratocast™ portal - Cloud administrators
Genetec Web Client
Security Center Web Client
Channel Enablement Tools - Stratocast - All Documents
Expenses
Sort by name
Add new bookmark
Add new folder
Import bookmarks
Export bookmarks
Help center

3. From the bookmark manager page, select the three dots in the top right of the browser window and click **Add new bookmark**.



Add bookmark

Name: Genetec Clearance Production Bookmark

URL: https://www.clearance.network/

4. Add the host you need and save the bookmark.

Why is a preview of a PDF not displayed in Clearance?

If a user is unable to view a PDF file in a case, you need to make sure that they have **View and download** permissions on the PDF file.

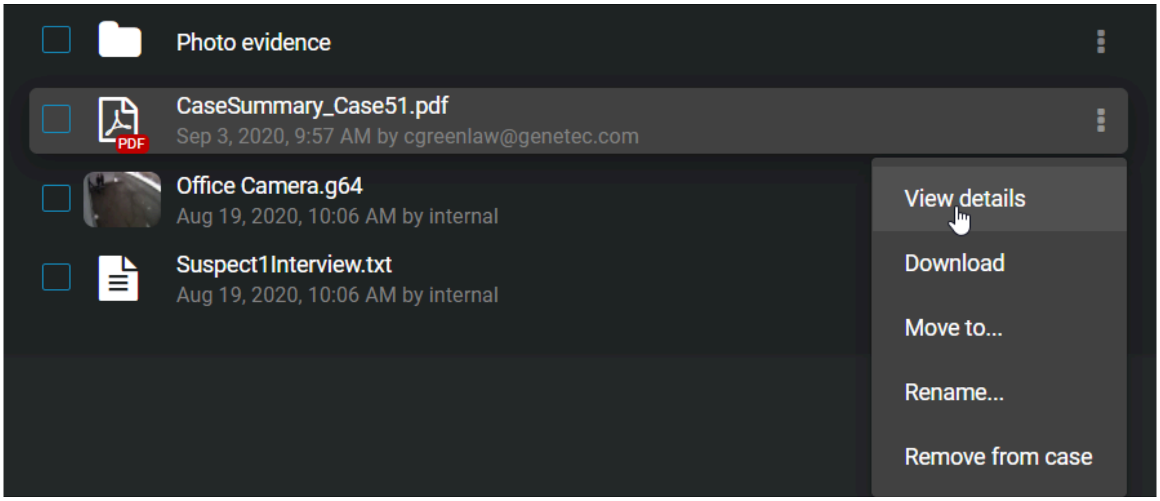
Cause

When a user generates a preview of a PDF file, it is possible for the user to go to their browser console to download it because a download of the file is generated each time you open it for preview. To mitigate this workaround, users who have **View** permissions for a case cannot view PDF files because they would also be able to download the PDF files without the **View and download** permission using this method.

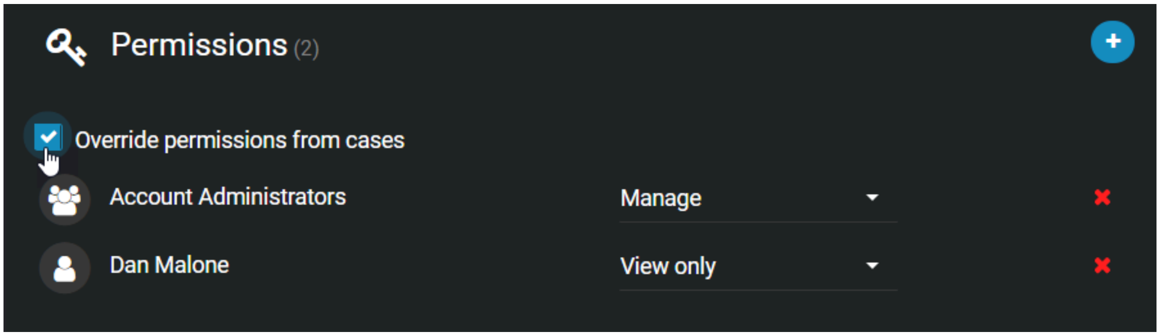
Solution

Give the user who needs to see the PDF **View and download** permission in the related case.

1. Select your case of choice.
2. Select the file you need the user to view and click **More** (⋮).
3. Click **View details**.



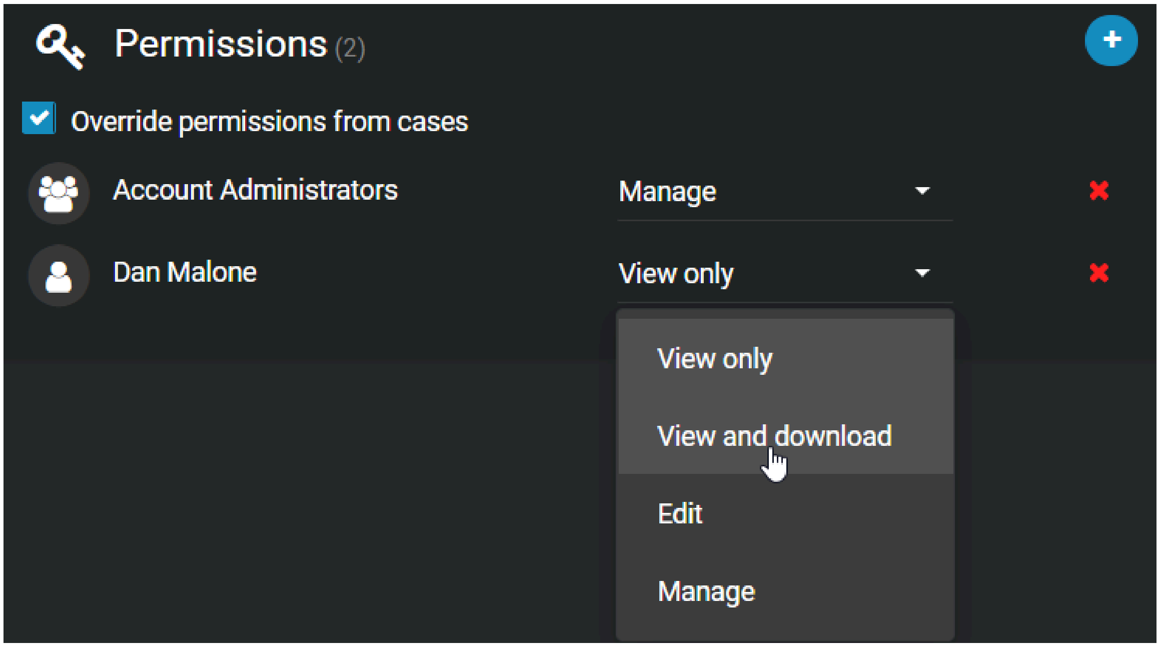
4. Select **Override permissions from cases**.


Permissions (2)

☑ Override permissions from cases

Account Administrators	Manage
Dan Malone	View only

5. Change the permission from **View only** to **View and download** on the PDF file you want the recipients to view and click **Save**.

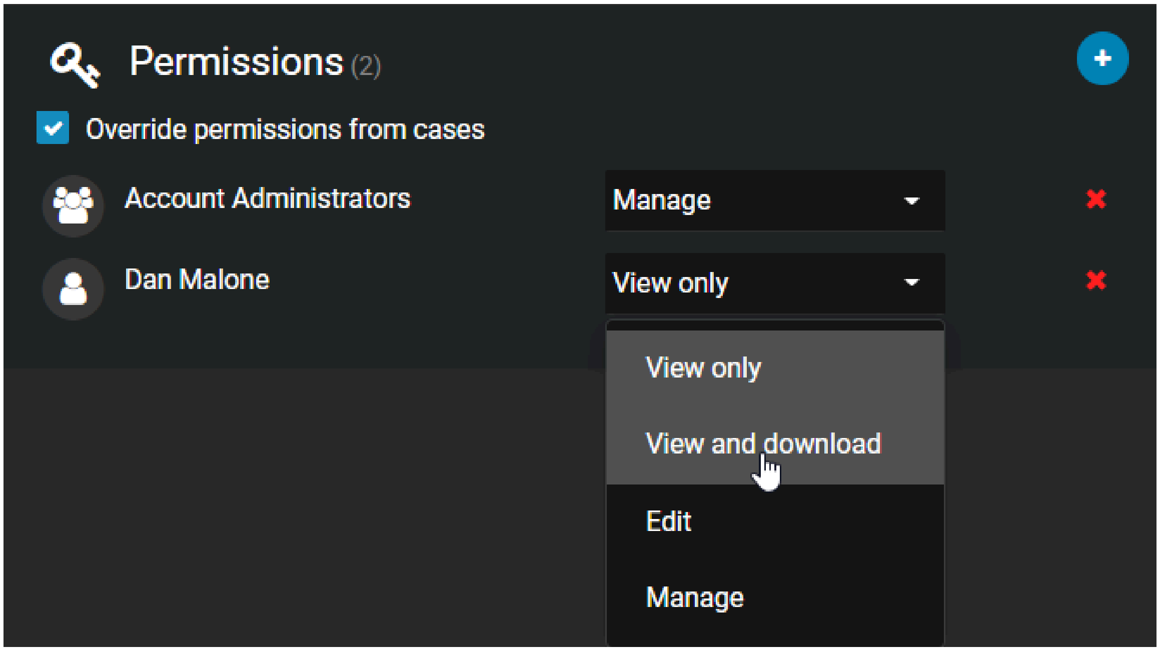


Permissions (2)

☑ Override permissions from cases

Account Administrators — Manage

Dan Malone — View only



Permissions (2)

☑ Override permissions from cases

Account Administrators — Manage

Dan Malone — View only

NOTE: All other files on the case remain **View only**, except for the specific ones you modify.

How can I avoid errors when accessing my Clearance account through my browser history?

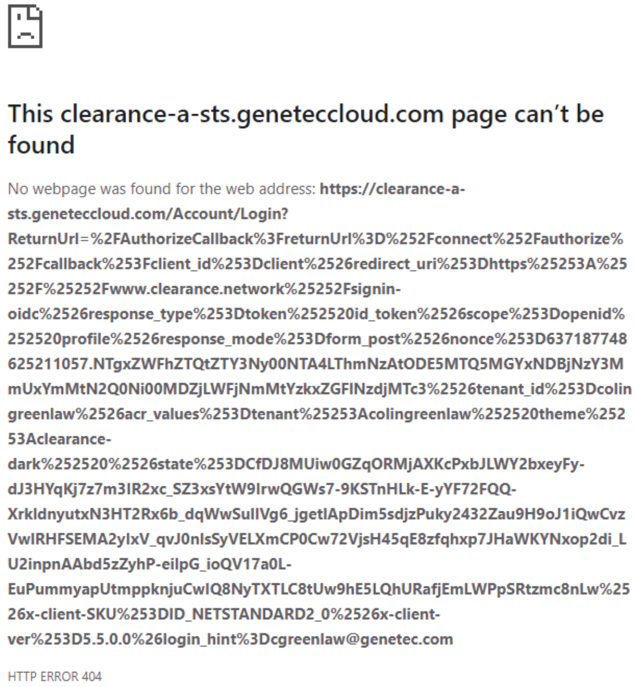
If you encounter an error when you navigate to your Clearance account through your browser history, you can fix this by setting up a bookmark to your Clearance account and using it to access your account moving forward.

Cause

- You navigated to your Clearance through your browser history.

  NOTE: The link to your Clearance account in your browser history expires after four hours. This is to ensure that users validate their credentials and prevent unauthorized individuals from accessing your Clearance account through your browser history.

Example of the error message:



This clearance-a-sts.geneteccloud.com page can’t be found

No webpage was found for the web address: **https://clearance-a-sts.geneteccloud.com/Account/Login?ReturnUrl=%2FAuthorizeCallback%3FreturnUrl%3D%252Fconnect%252Fauthorize%252Fcallback%253Fclient_id%253Dclient%2526redirect_uri%253Dhttps%25253A%25252F%25252Fwww.clearance.network%25252Fsignin-oidc%2526response_type%253Dtoken%252520id_token%2526scope%253Dopenid%252520profile%2526response_mode%253Dform_post%2526nonce%253D637187748625211057.NTgxZWFhZTQtZTY3Ny00NTA4LThmNzAtODE5MTQ5MGYxNDBjNzY3MmUxYmMtN2Q0Ni00MDZjLWFjNmMtYzkxZGFlNzdjMTc3%2526tenant_id%253Dcolingreenlaw%2526acr_values%253Dtenant%25253Acolingreenlaw%252520theme%25253Aclearance-dark%252520%2526state%253DCfDJ8MUiw0GZqORMjAXKcPxbJLWY2bxeyFy-dJ3HYqKj7z7m3IR2xc_SZ3xsYtW9IrwQGWs7-9KSTnHLk-E-yYF72FQQ-XrkldnyutxN3HT2Rx6b_dqWwSullVg6_jgetlApDim5sdjzPuky2432Zau9H9oJ1iQwCvzVwlRHFSEMA2ylxV_qvJ0nlsSyVELXmCP0Cw72VjsH45qE8zfqhxp7JHaWKYNxop2di_LU2inpnAAbd5zZyhP-eilpG_ioQV17a0L-EuPummyapUtmppknjuCwlQ8NyTXTLC8tUw9hE5LQhURafjEmLWPpSRtzmc8nLw%2526x-client-SKU%253DID_NETSTANDARD2_0%2526x-client-ver%253D5.5.0.0%26login_hint%3Dcgreenlaw@genetec.com**

HTTP ERROR 404

Solution

Select the required URL as detailed in your account activation email and bookmark it. Use the bookmark to access your Clearance account.

NOTE: The hostname displayed before the account ID in your account URL will vary depending on the region where your account is hosted.

Host list by region

Region	Host
United States	https://www.clearance.network
Europe	https://eu.clearance.network

Region	Host
Australia	https://au.clearance.network
US Government	https://usgov.clearance.network
Canada	https://ca.clearance.network

Why does my file fail to upload to Clearance?

Cause

If you are unable to upload a file to Clearance, it might be because some of the necessary domains are blocked, resulting in certain Clearance functionalities being restricted.

NOTE:

- Uploading a file to Clearance requires access to the internet.
- All communication is outbound over HTTPS.
- A list of the domains that must be accessible for Clearance to work can be found here.

Solution

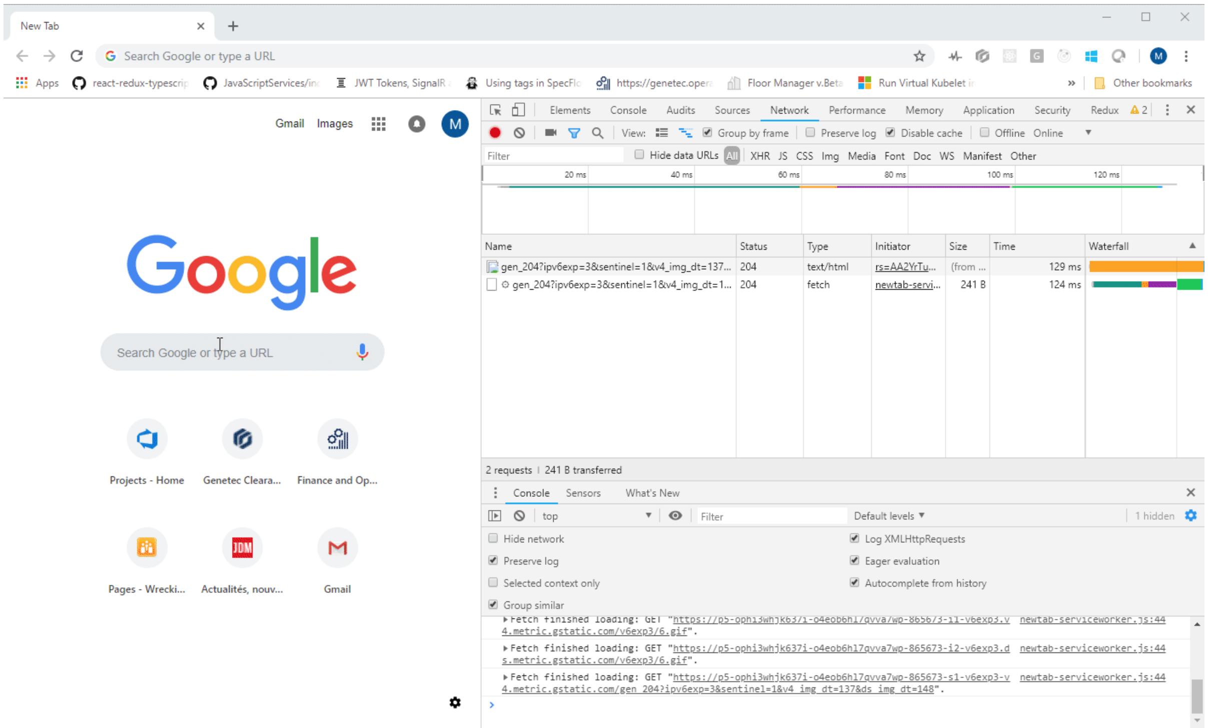
Should a file fail to upload, it might indicate that one of the required domains is restricted on your network. To resolve this, do the following:

- Attempt to upload the file from a different internet connection.
- Request your IT department to white list the required domains.

Steps to identify which domains are restricted

To identify if your connection is restricted, you can run the following example from Google Chrome to generate a network trace:

1. Press the F12 key on your keyboard, and select the **Network** tab.
2. Click the **Preserve log** check box.
3. Log into Clearance to generate the error message.
4. Right click any of the links on the Network view and click **Save all as HAR with content**.
5. Send the exported HAR file to the Clearance account administrator.



☑ Group by frame ☐ Preserve log ☑ Disable cache ☐ Offline Online

Name	Status	Type	Initiator	Size	Time	Waterfall
gen_204?ipv6exp=3&sentinel=1&v4_img_dt=137...	204	text/html	rs=AA2YrTu...	(from ...	129 ms	
gen_204?ipv6exp=3&sentinel=1&v4_img_dt=1...	204	fetch	newtab-servi...	241 B	124 ms	

2 requests | 241 B transferred

☐ Hide network ☑ Log XMLHttpRequests
☑ Preserve log ☑ Eager evaluation
☐ Selected context only ☑ Autocomplete from history
☑ Group similar

```
▸Fetch finished loading: GET "https://p5-ophi3whjk637i-o4eob6hl7qvva7wp-865673-i1-v6exp3.v  newtab-serviceworker.js:44
4.metric.gstatic.com/v6exp3/6.gif".
▸Fetch finished loading: GET "https://p5-ophi3whjk637i-o4eob6hl7qvva7wp-865673-i2-v6exp3.d  newtab-serviceworker.js:44
s.metric.gstatic.com/v6exp3/6.gif".
▸Fetch finished loading: GET "https://p5-ophi3whjk637i-o4eob6hl7qvva7wp-865673-s1-v6exp3-v  newtab-serviceworker.js:44
4.metric.gstatic.com/gen_204?ipv6exp=3&sentinel=1&v4_img_dt=137&ds_img_dt=148".
>
```

Why does the download link fail to work in Google Chrome?

If a download link found in Clearance or the Clearance User Guide for a tool such as the Clearance Uploader, Genetec Video Player, or Clearance plugin does not work when you are using Chrome, you must change your site settings to allow insecure content.

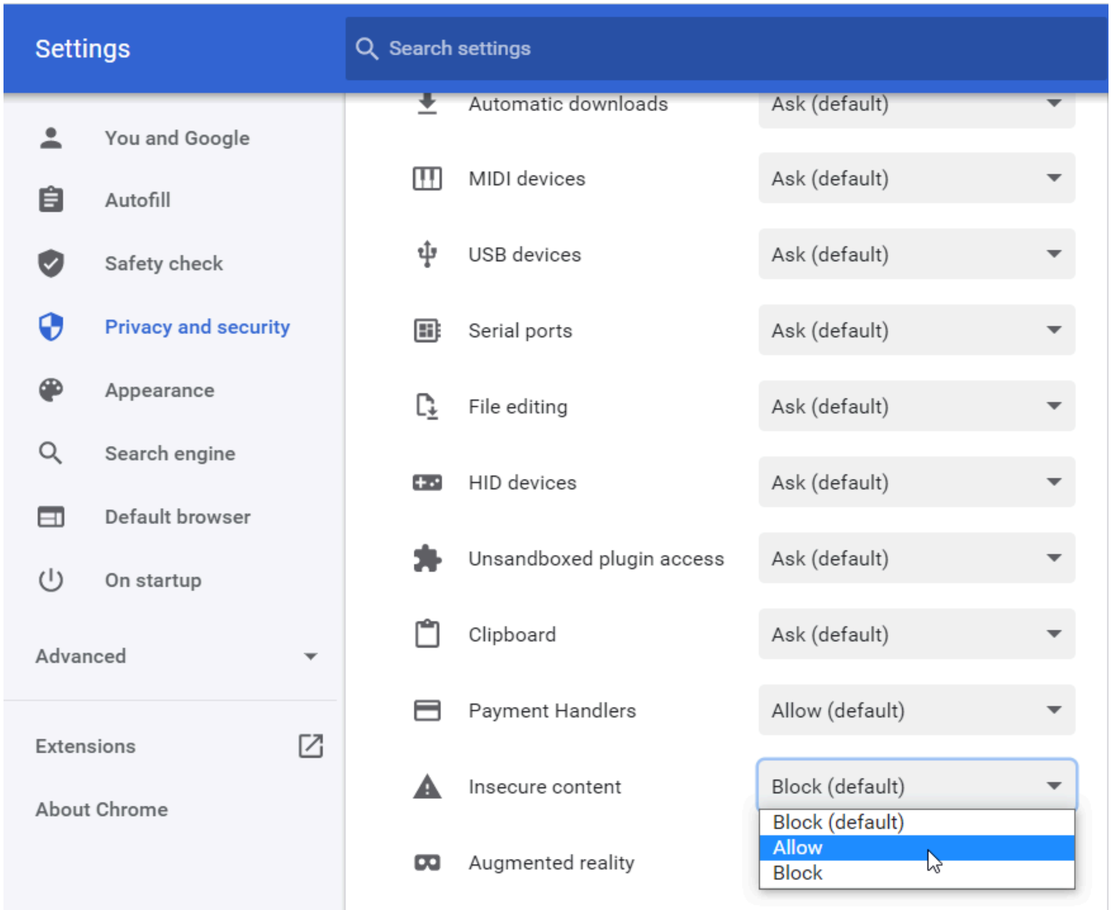
Cause

Your site settings are configured to block insecure content in Clearance or the Clearance online help.

Solution

You must change your site settings to allow insecure content on the site you want to download content from.

1. In your browser, click **View site information** (🔒).
2. Click **Site settings** (▤).
3. Scroll down the list of permissions and change the **Insecure content** permission to **Allow**.



Automatic downloads Ask (default)
MIDI devices Ask (default)
USB devices Ask (default)
Serial ports Ask (default)
File editing Ask (default)
HID devices Ask (default)
Unsandboxed plugin access Ask (default)
Clipboard Ask (default)
Payment Handlers Allow (default)
Insecure content Block (default)
Block (default)
Allow
Block
Augmented reality

NOTE: Only change this site setting for secure websites that you trust.

Change to Clearance login

Beginning in April 2024, users who do not use a SSO (Single Sign On) integration will need to reset their passwords the first time they login to Genetec Clearance™.

Cause

Clearance will transition users to the Genetec Login authentication system in April 2024. Genetec Login is used across Genetec web applications and ensures a single identity is used across all Genetec products.

Solution

Following the change, users must reset their passwords the first time they log into Clearance. As part of the transition, Multifactor authentication (MFA) is mandatory for all users that sign into Genetec applications. The second factor is a pin that is sent to the email address associated with the user's account.

NOTE: Users from organizations that integrate their corporate identity system with Clearance will not be affected by this change. These users will continue to use the SSO functionality that is administered by their organization.

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.

Clearance Uploader

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.

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™ 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.