AXIS Case Insight User Guide

Document last updated: February 27, 2025

Contents

1

Introduction to AXIS Case Insight

Learn about the AXIS Case Insight collaborative investigation management system.

This section includes the following topics:

About email notifications in AXIS Case Insight

To inform users or guest users about specific events in Axis Case Insight, 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 case is transferred

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

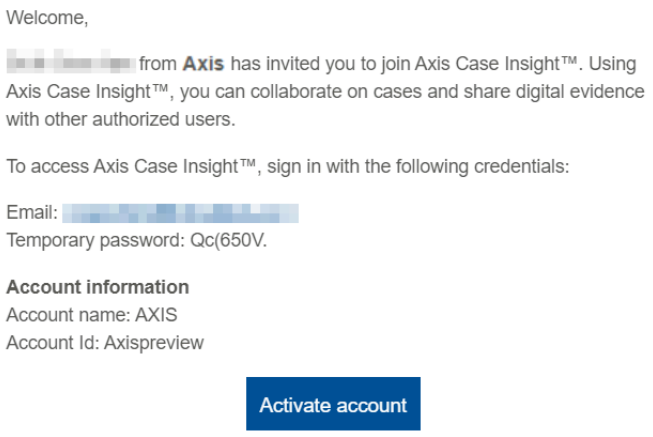
The email notification can also include one or more of the following:

- 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.

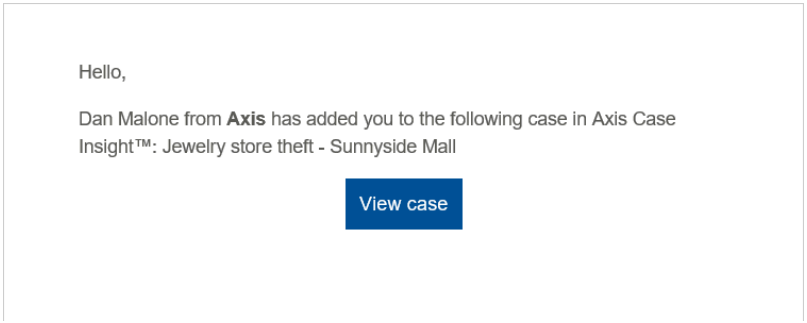
Account created

An email with the subject “Invitation to join AXIS Case Insight” is sent.



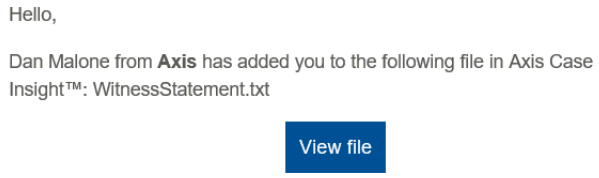
User added to a case

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



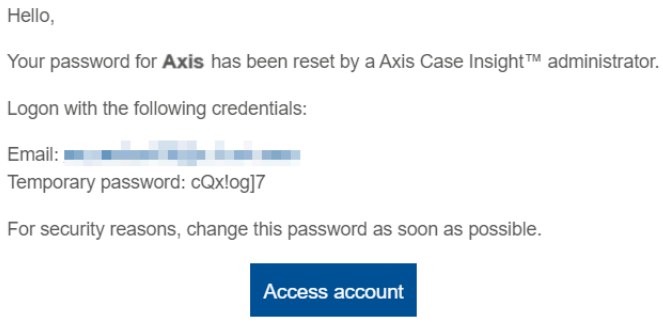
User added to a file

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



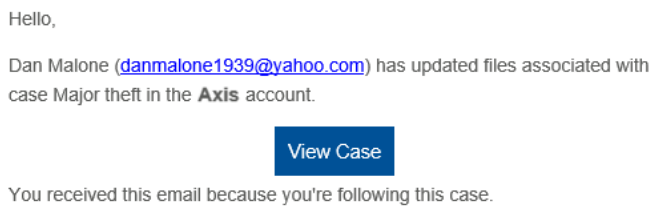
Password reset

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



Case modified

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


Hello,

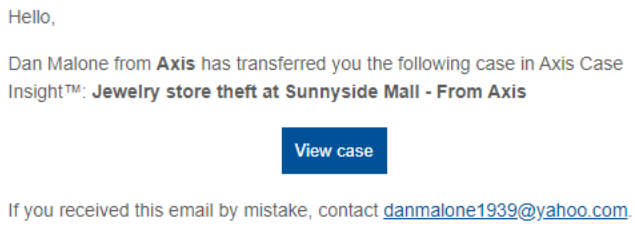
Dan Malone (danmalone1939@yahoo.com) has updated files associated with case Major theft in the **Axis** account.

View Case

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

Incoming case transfer

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


Hello,

Dan Malone from **Axis** has transferred you the following case in Axis Case Insight™: **Jewelry store theft at Sunnyside Mall - From Axis**

View case

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.

Related Topics

Activating your account on page 26
Sharing cases on page 72
Sharing files on page 112
Resetting user passwords on page 54

2

Getting started

Learn how to log on, log off, and change languages in AXIS Case Insight.

This section includes the following topics:

Deploying and using AXIS Case Insight

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

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. 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 AXIS Case Insight 2. Assign personnel to a case 3. Change access policies for cases 4. Upload files to cases 5. Preview evidence in cases
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

AXIS Case Insight videos on page 11

Logging on to AXIS Case Insight

After you have activated your user account through the activation link, you can log on to your AXIS Case Insight 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 AXIS Case Insight 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: https://us.caseinsight.axis.com or (US)
   - Host 2: https://eu.caseinsight.axis.com (Europe)
   - Host 3: https://au.caseinsight.axis.com (Australia)
   - Host 4: https://usgov.caseinsight.axis.com (US Government)
   - Host 5: https://ca.caseinsight.axis.com (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 AXIS Case Insight.

Related Topics

Activating your account on page 26

Logging off from AXIS Case Insight

To exit from AXIS Case Insight, 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 AXIS Case Insight: 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 AXIS Case Insight

To change the language in AXIS Case Insight 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.

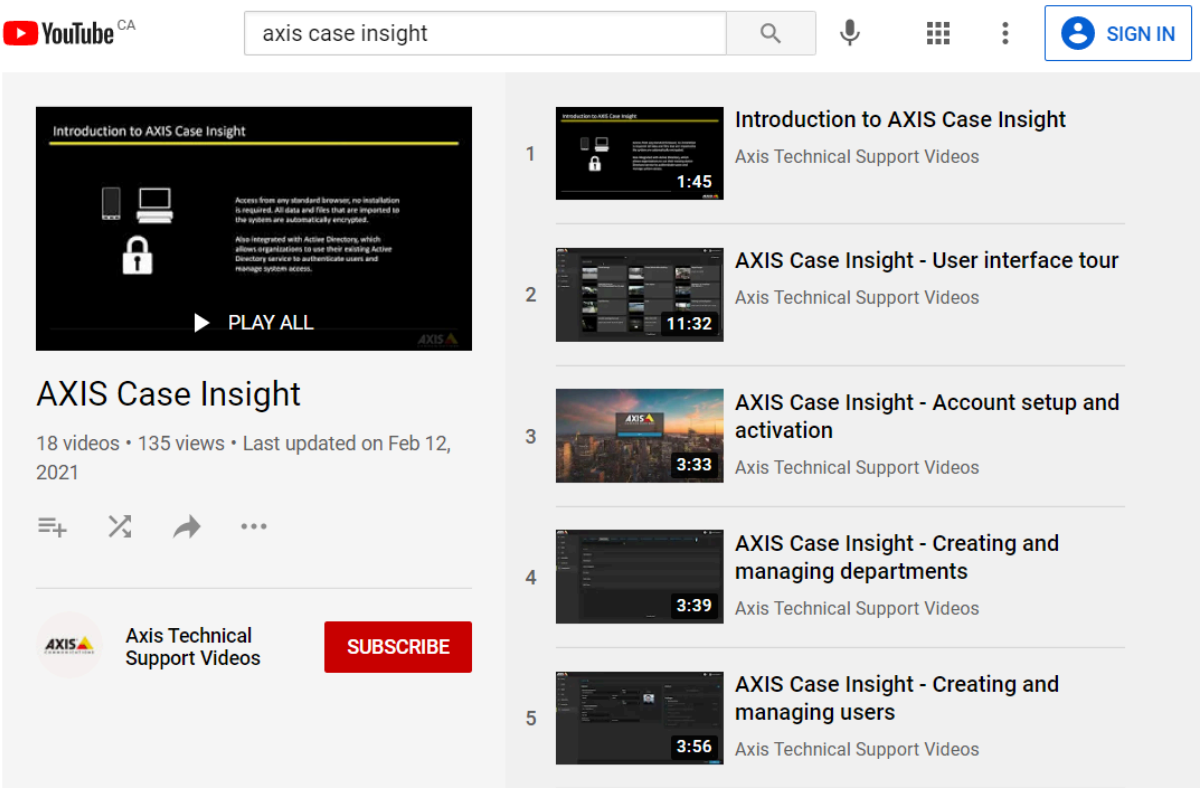
6 Click **More** (⋮) .

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

The AXIS Case Insight user interface can now be displayed in the browser language that you selected.

AXIS Case Insight videos

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



Click the image to access the AXIS Case Insight 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 AXIS Case Insight.

This section includes the following topics:

System requirements for AXIS Case Insight

For Axis Case Insight 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 AXIS Case Insight software are as follows:

Desktop Requirements

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

AXIS Case Insight 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

AXIS Case Insight 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.

What's new in AXIS Case Insight

AXIS Case Insight includes the following new features.

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 AXIS Case Insight. 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 AXIS Case Insight.

  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
  - In-car video systems
  - Public uploads
  - Video editor projects
  - Web portal uploads

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 AXIS Case Insight 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* module 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 AXIS Case Insight 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 132.

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.

- **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

- **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 more information, refer to Trimming video on page 135.

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.

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. For more information, refer to Setting a default department on page 44.

What's New: August 2023

- **Automatic case naming:** Case names can now be automatically generated when cases are created in AXIS Case Insight. 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 84.

What's New: June 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 42.

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

- **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.

What's New: September 2022

- **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: April 2022

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

February 2022

- **Automatic case ID numbers:** You can now automatically generate incident and record numbers to facilitate the classification of cases. Administrators can define the convention used to generate IDs and support the inclusion of common properties such as the date and other system properties as part of the ID template. For more information, see Configuring ID templates on page 51.
- **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 135.

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
- **Support for Internet Explorer removed:** With the upcoming end of life of Internet Explorer 11 scheduled in June 2022, the browser is no longer supported by AXIS Case Insight. For the best experience using AXIS Case Insight use Google Chrome or Microsoft Edge.

November 2021

- **Audio redaction:** Support for audio redaction has been added to the video editor in AXIS Case Insight. You can now omit sensitive audio content from video and audio recordings. For more information, see Redacting audio on page 151.

- **Disable departments:** Admins can now disable departments to remove legacy values when new cases are created. Existing cases that have the department assigned maintain it unless it is changed manually by a user with sufficient privileges.
- **Dropdown filter for custom fields:** You now have more flexibility to collect information from custom fields with the new dropdown filters using predefined values that fit your organization's needs. Admins can configure these dropdowns in the Configurations section.

October 2021

- **Notification contact email:** You can now configure the email address displayed in system notification emails. Rather than include the email of the user who shared the case, a custom support alias can be included for recipients to contact if need be. Admins can configure this email address in the Account Information page.
- **Increased user limit on a few security policies:** A limit increase, from 10 to 25, users and groups has been applied to the following security policies that concern file and case deletion and retention:
  - Delete cases and files
  - Restore cases and files from the recycle bin
  - Protect or unprotect cases and files from deletion
- **WebHelp User Guide download:** Tired of printing topics when all you want is to download the User Guide? You can now download the entire guide from the homepage of the AXIS Case Insight WebHelp.

September 2021

- **Custom fields:** Admins can now create custom fields for cases and files, allowing organizations to define their own templates and document investigations in greater detail. The feature also allows admins to change the names of existing fields to match nomenclature used within your organization. Once configured, custom fields can be used as an additional filter from the search page to refine the list of results.

August 2021

- **Export audit trail reports:** Users can now download case and file audit trails as a PDF document. The audit report includes information related to user activity, date and time of each action, and a summary of the case or file metadata.
- **Configure who can create cases:** Through the new *Create case* security policy, administrators can now configure whether users or groups have the right to create cases in AXIS Case Insight. Guest users assigned this security policy can also create cases.

June 2021

- **Capture snapshots from videos:** The snapshot tool allows you to take still images from a video, so you can preserve and share a specific element in a scene. Snapshots are logged as part of the video's audit trail and inherit the same permissions as the original evidence to maintain the chain of evidence.

  For more information, see the list of video player controls..
- **Redesigned video player:** When investigating an incident, reviewing all of the pieces of evidence collected is fundamental to recalling the events that took place. The redesigned video player allows users to playback up to six recordings in a multi-tile view to benefit from the different perspectives available. Videos can be played simultaneously or chronologically so that investigators can review different views of a scene or follow an event through successive fields of view.

  For more information, see Reviewing media on page 108.

May 2021

- **Display assigned officer:** You can now identify the officer who recorded files from body-worn cameras and in-car systems in your search results. The Officer assignment field can be toggled from the column selection menu as you configure the search fields.

April 2021

- **Configure search fields:** You can now customize and order the fields displayed in your search results to view metadata most relevant to your search. Need to find a specific case? You can list the creation date, department, and record number directly in your results. If you're searching for files, you can list the recording times, category, and name of the officer who recorded the video directly. The fields and filters you configure remain saved to your browser for the next time you run a search.

  For more information, see Searching for cases or files on page 84.

March 2021

- **Officer video security policy:** Agencies can now limit an officer's access strictly to video recorded from their own device. The new setting is configured in the security policies menu and applies to body worn camera recordings uploaded to the application.

  For more information, see Defining security policies on page 47.

February 2021

- **Files auto-save:** Files added to cases are now automatically saved as part of the case.

What's New: January 2021

- **Evidence and case dashboards:** As organizations increase the amount of data uploaded to AXIS Case Insight, they can gain a better understanding of their operations through historical trends. The new dashboard functionality provides in-app visibility of this data. Current dashboards allow you to review the number of cases created in your account, the types of file formats uploaded, your data usage, and more. The data can also easily be exported to images and spreadsheets, should it need to be shared and reviewed by others. You can manage who has access to the dashboards in your account Security Policies. For more information, see About the AXIS Case Insight dashboard on page 154.

December 2020

- **Frame-by-frame on video player:** You can now progress in a file that you are reviewing one frame at a time in the video player. This lets you analyze footage with greater precision, especially in scenes involving a lot of movement and activity.

  For more information, see the list of video player controls..

Supported languages

AXIS Case Insight is available in the following languages.

AXIS Case Insight web portal

- English
- French
- Spanish
- German
- Dutch

AXIS Case Insight public upload feature

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

4

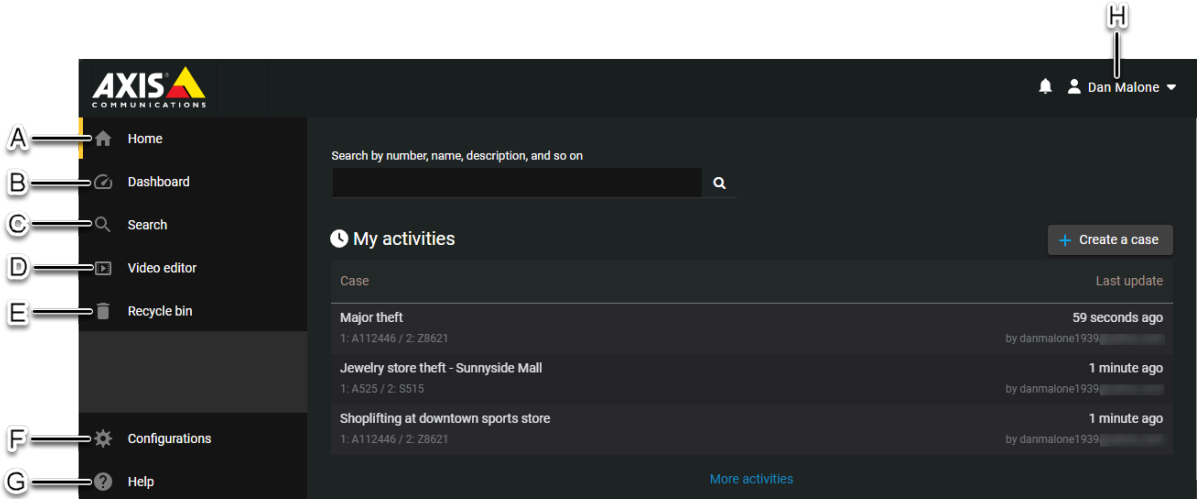
User interface tour

Get familiar with the user interface in AXIS Case Insight.

This section includes the following topics:

Overview of the menu tabs in AXIS Case Insight

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



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

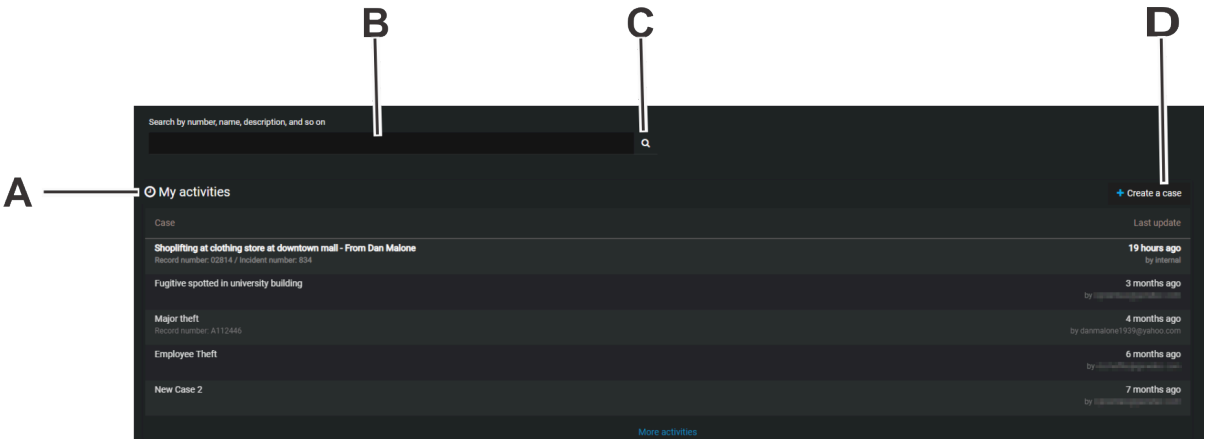
A	**Home**	Visit the homepage to use the search box, search button, news, *my activities*, and learn sections.
B	**Dashboard**	Visit the dashboard to examine storage and case data metrics.
C	**Search**	Search and filter the complete list of cases, files, and cameras in AXIS Case Insight.
D	**Video editor**	Display a list of editing projects and use it to search for, open, and modify redacted files.
E	**Recycle bin**	Display a list of cases and files in the recycle bin that can be searched and filtered.
F	**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.
G	**Help**	Open the user guide documentation or create a support ticket.
H	**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.



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	**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.
B	**Search box**	Open the *Search* page. The search results only show cases or files that contain your keywords.
C	**Search button**	Open the *Search* page. The search results only show cases or files that contain your keywords.
D	**Create a case**	Create a new case.

5

Account setup

Configure your settings in AXIS Case Insight.

This section includes the following topics:

Setting up your account

With AXIS Case Insight, 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 AXIS Case Insight 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 AXIS Case Insight 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.

Activating your account

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

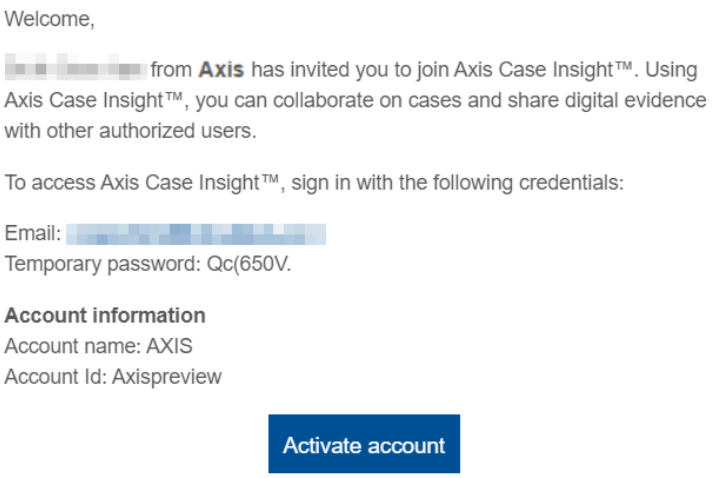
Before you begin

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

Procedure

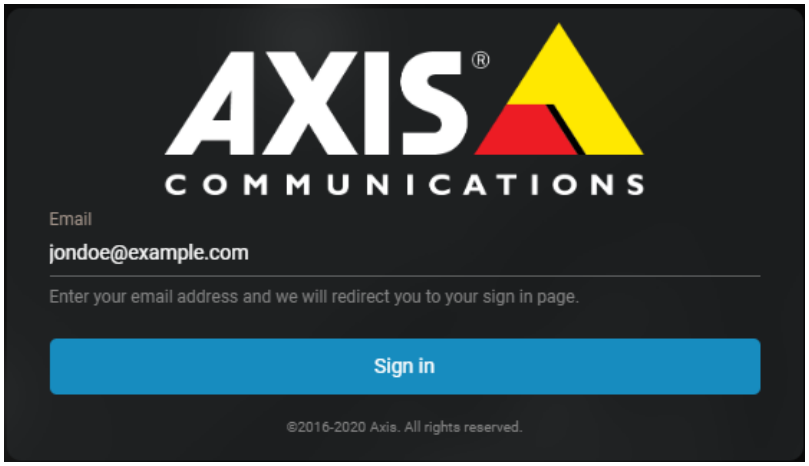
1 Sign in to your email account.

2 In your *Invitation to join AXIS Case Insight* email, click **Activate Account**.



IMPORTANT: This e-mail is sent from *info@caseinsight.axis.com* 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 AXIS Case Insight site, enter your email address and then click **Sign in**.



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

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

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

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

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

The homepage opens.

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

Example

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

Related Topics

Logging on to AXIS Case Insight on page 8
About email notifications in AXIS Case Insight on page 2

Configuring your account information

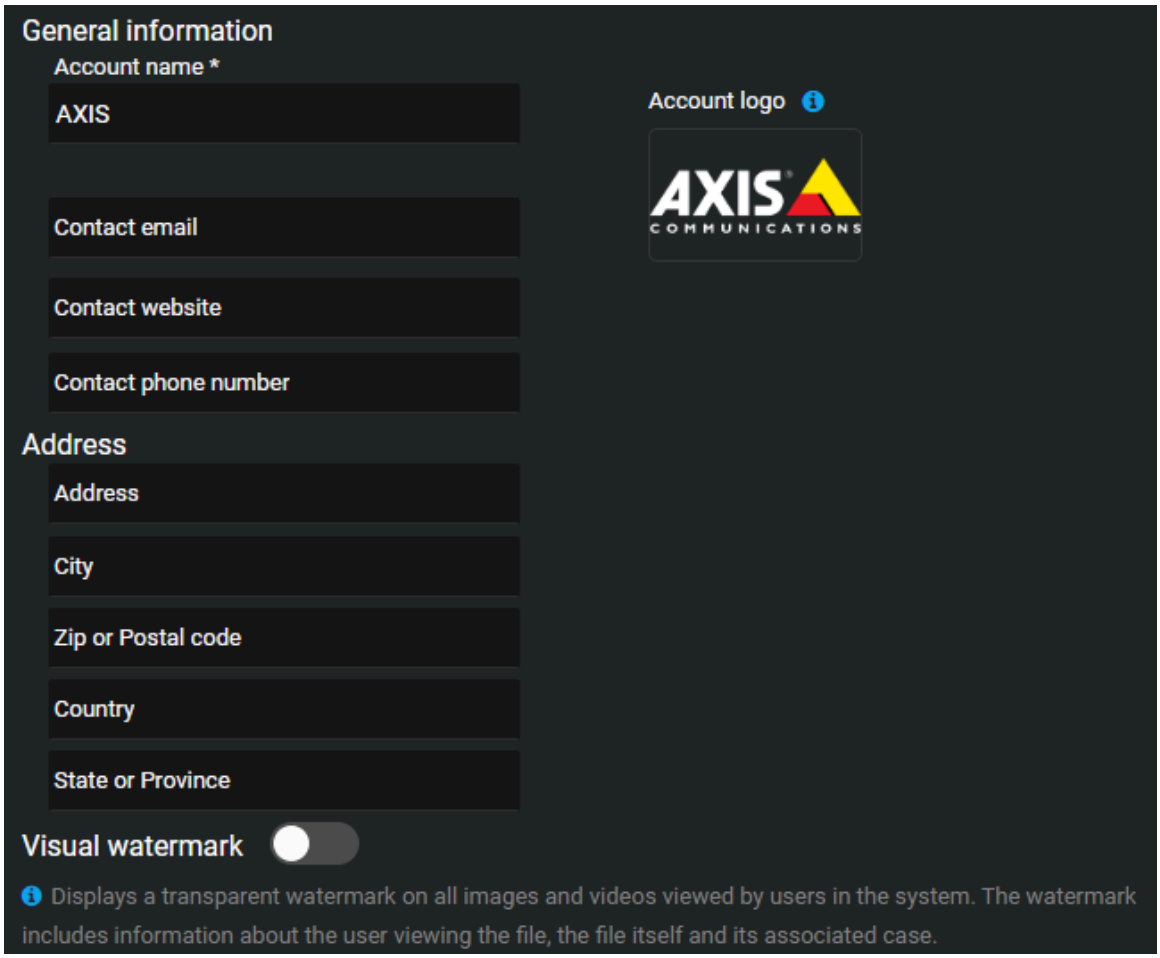
Before you can change your file request terms and conditions, create guest user terms and conditions, or apply the digital watermark feature, you must configure your account information.

Before you begin

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

Procedure

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



2 Complete the following fields:

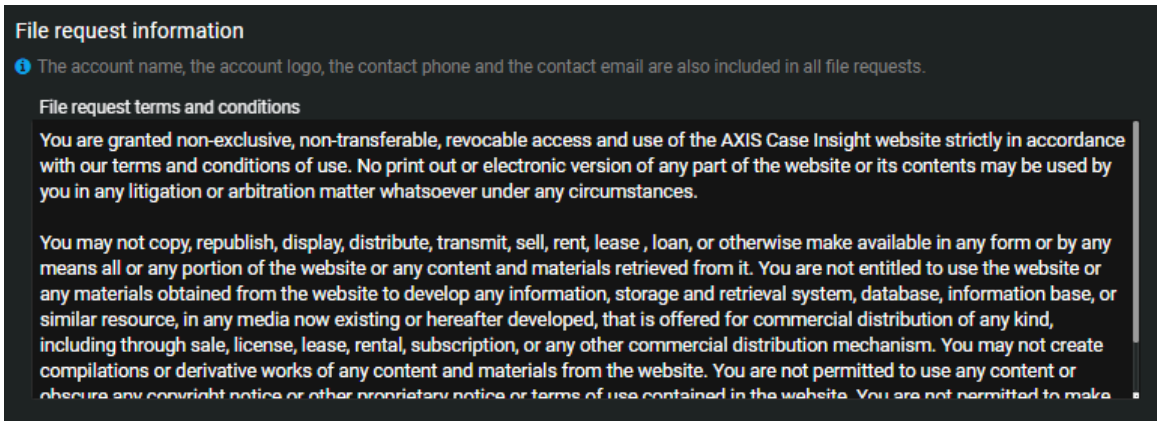
- **Account name:** The name of your organization.
- **Contact email:** An email address listed in system notification emails that can be used by parties whom you share cases and evidence with to contact your organization.
- **Contact website:** A website for your organization.
- **Contact phone number:**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

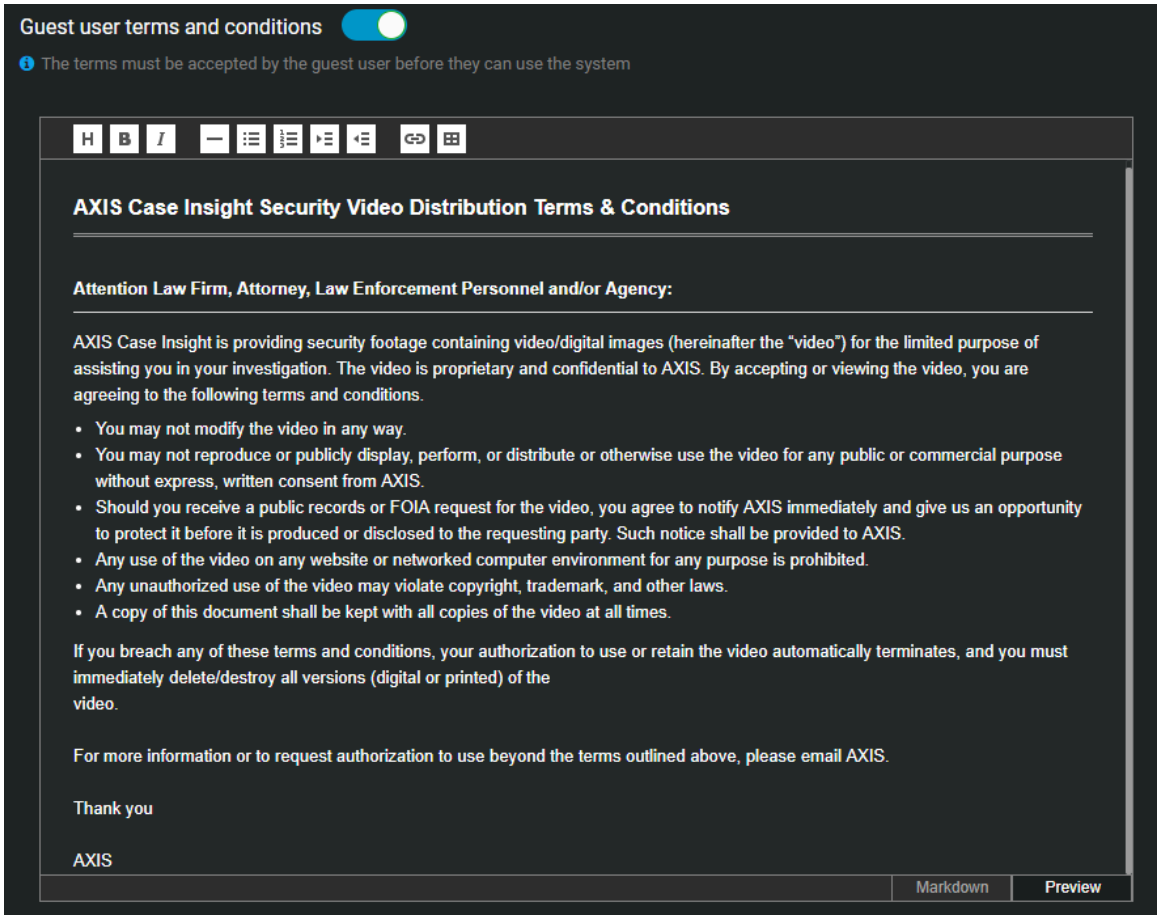


6 In the *Account logo* section, click the logo field.
a) Navigate to and select the image file to use as the logo for your account.
b) Click **Open**.

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.



8 Click **Save**.

Example

Configuring your report templates

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

Before you begin

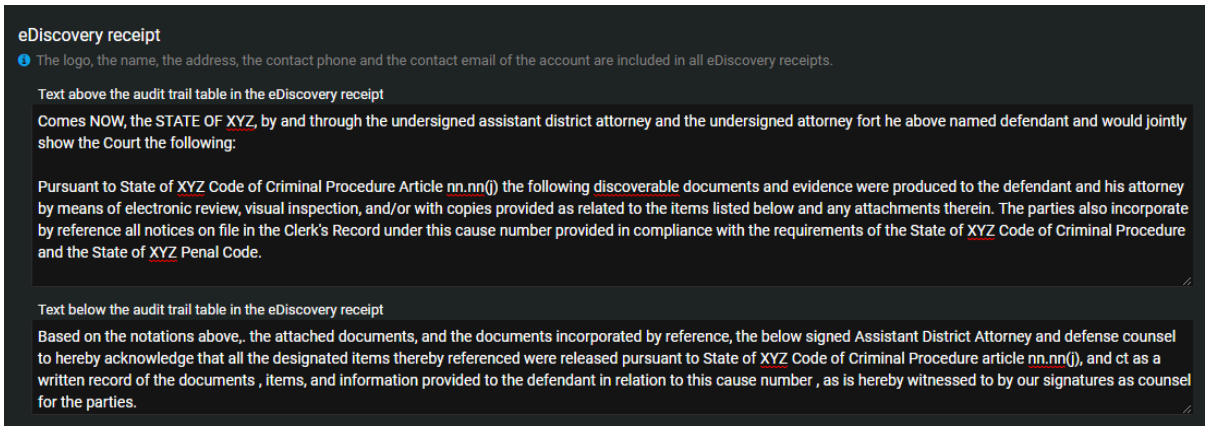
Make sure that you have a secure connection to the web.

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**.



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.

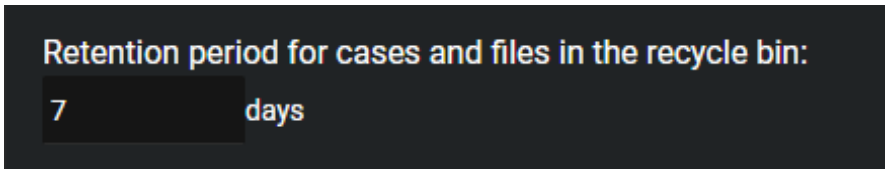
Closing and reopening cases also affects the retention period for files. For example, when a closed case is reopened, the scheduled deletion for files associated with that case is changed back to **Never delete** provided that the file is not in the recycle bin.

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.



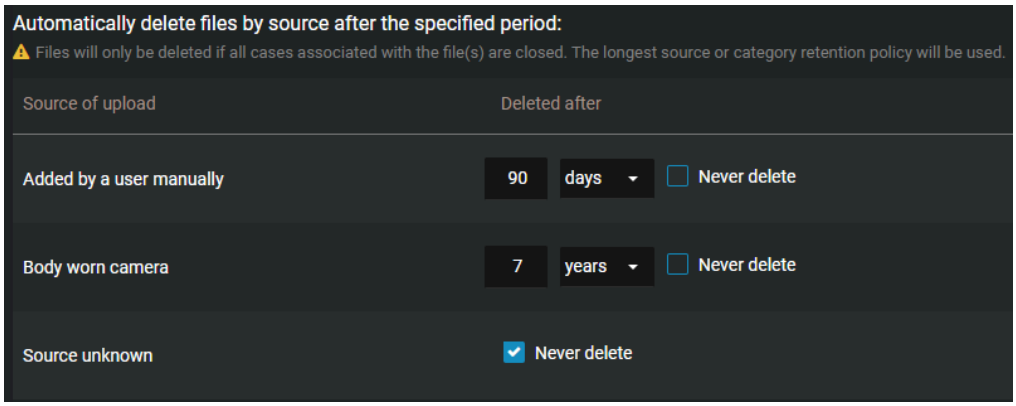
3 Click **Save**.

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**.

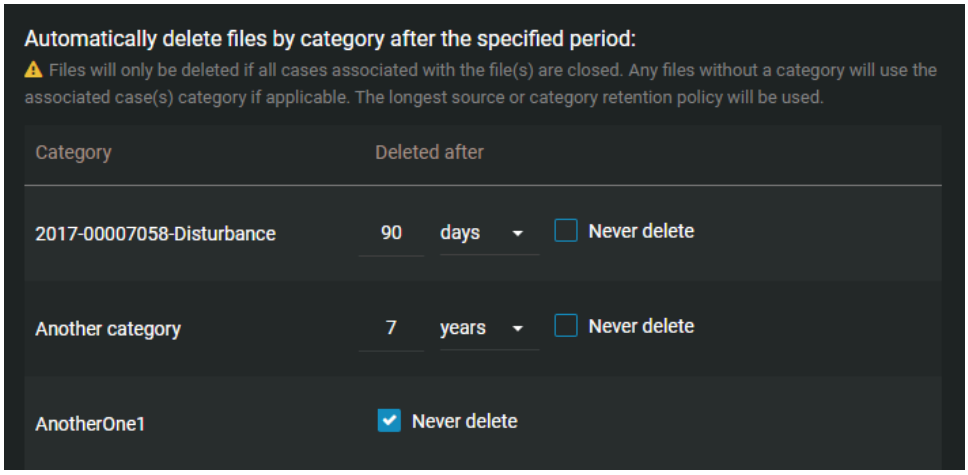
2 Specify a retention period for each source that is defined in the system.
The **Never delete** check box is selected by default, to keep your files indefinitely.
a) (Optional) To specify a retention period in days, clear the **Never delete** check box next to the source that you require and select 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.



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.



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.

Permission levels

Permission levels in AXIS Case Insight 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 AXIS Case Insight:

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 124.

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				✓
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.

Related Topics

Defining security policies on page 47
Security policy definitions list on page 47

Creating user groups

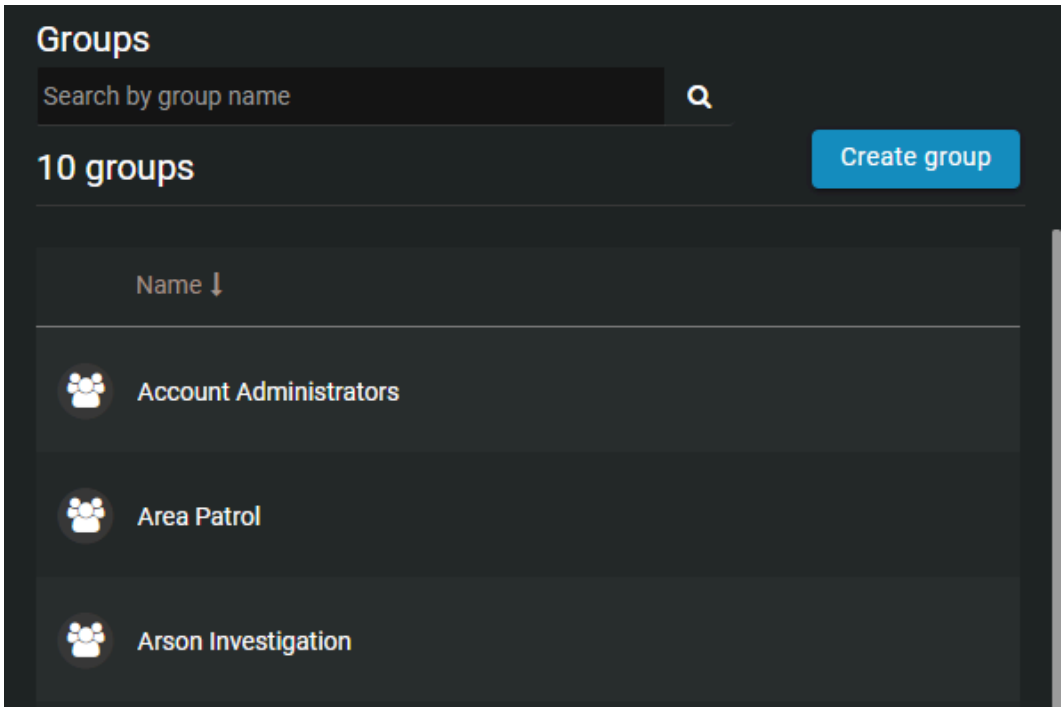
To organize users by rank or role, and to simplify the assignment of permission and security policies in the system, you can create user groups.

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 AXIS Case Insight 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 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

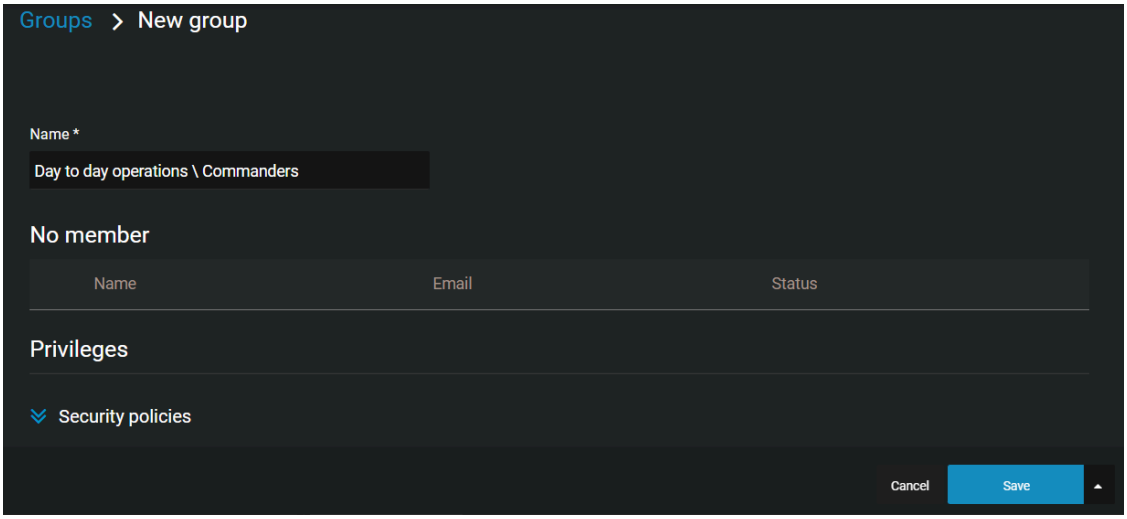
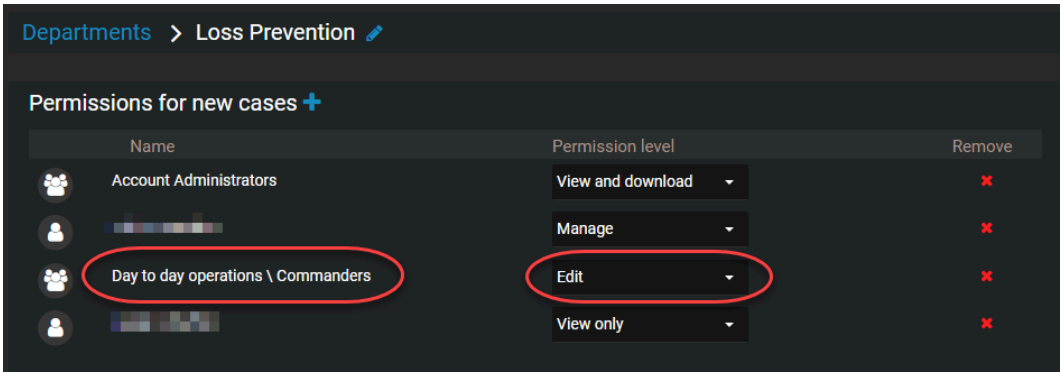


Figure B. Add group to department and assign access policies for new cases



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.

Creating user accounts

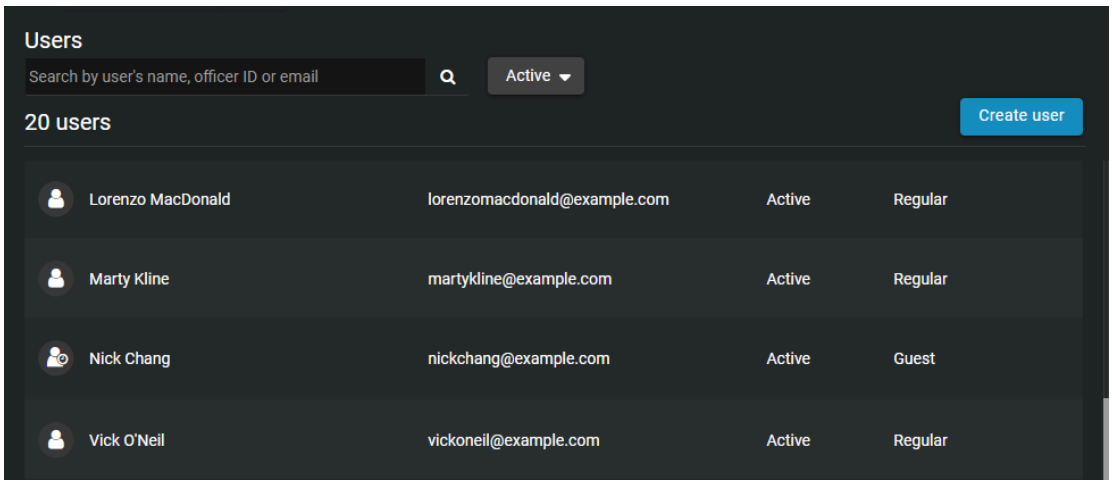
Before someone can use Axis Case Insight, you must create a user account for that person. After you have created the user's account, they can be granted access to cases and files.

What you should know

You must be an account administrator to create users in AXIS Case Insight.

Procedure

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



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 policies.

3 Click **Save**.

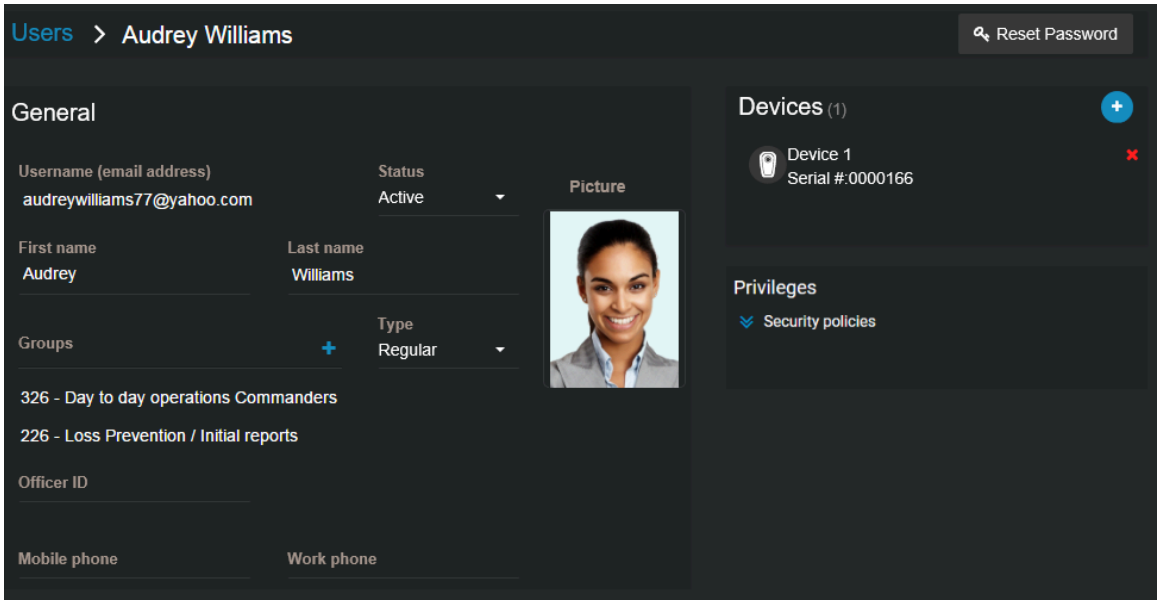
The user account is created. An email inviting the user to join AXIS Case Insight is automatically sent to the user.

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.



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

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.

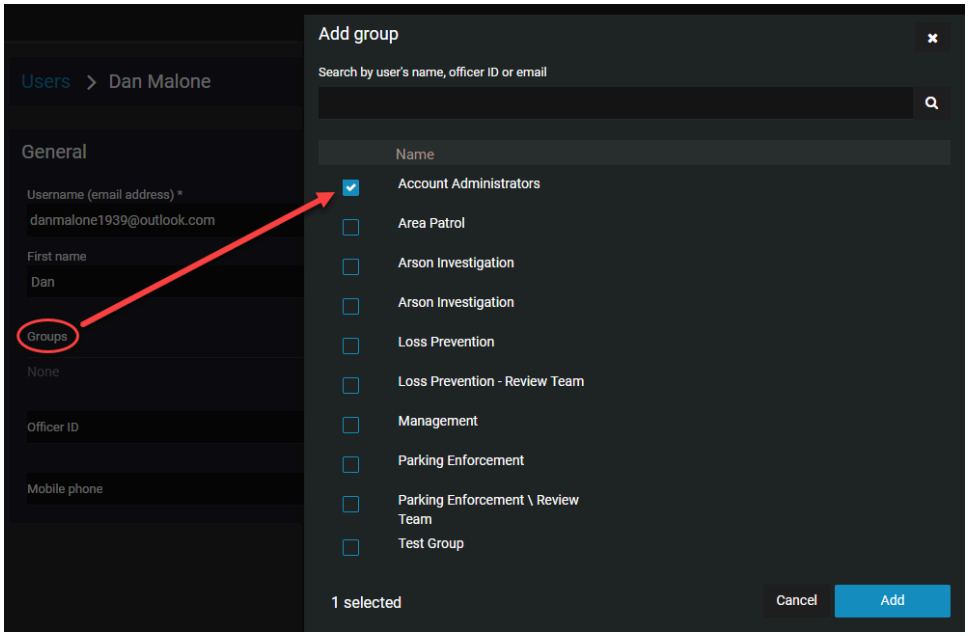
Procedure

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**.



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 departments

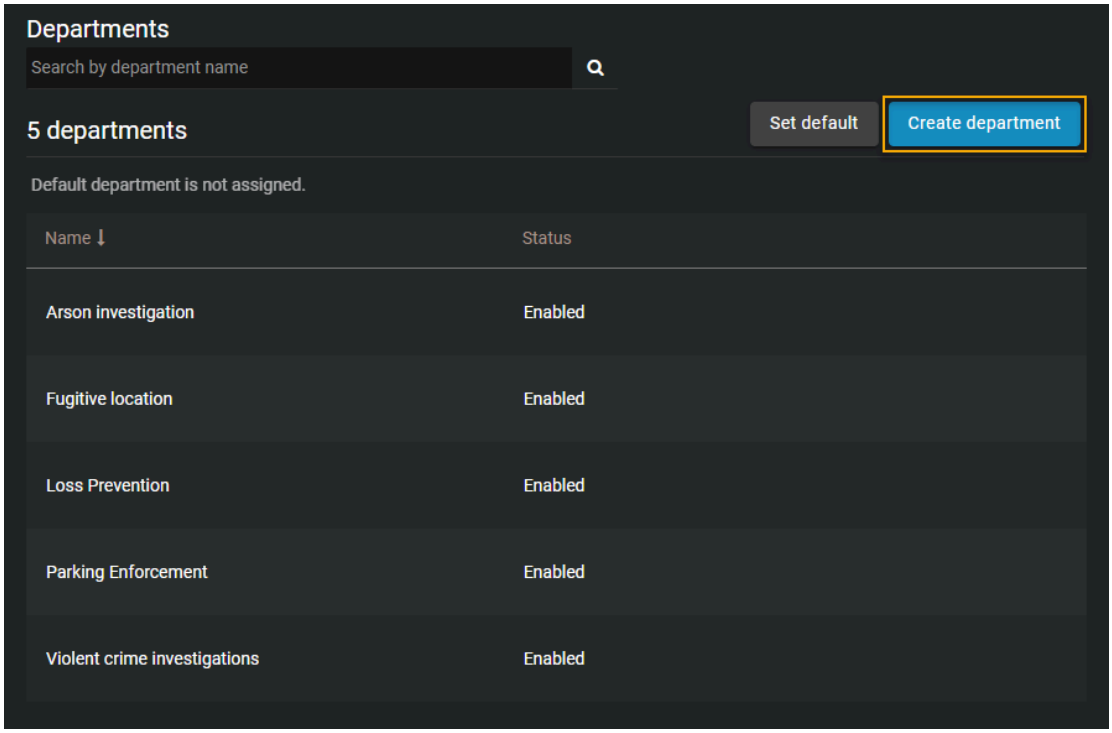
Departments act as user access templates that allow the initial permissions for users and groups to be automatically applied to cases.

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.

Procedure

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



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**.

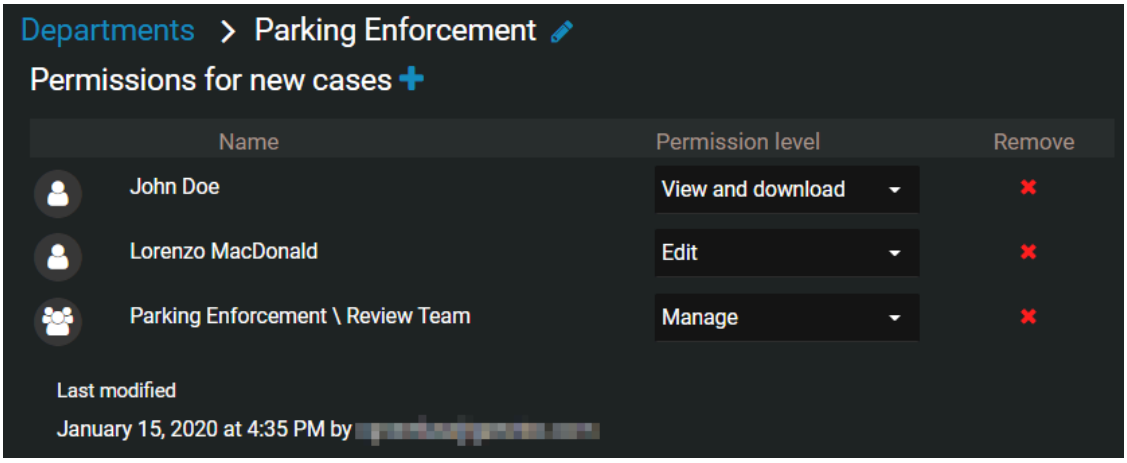
NOTE: At least one user or group must have *manage* permissions in a department. This ensures that cases are always accessible with full permissions by someone from the organization.

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.



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**.

Creating incident categories

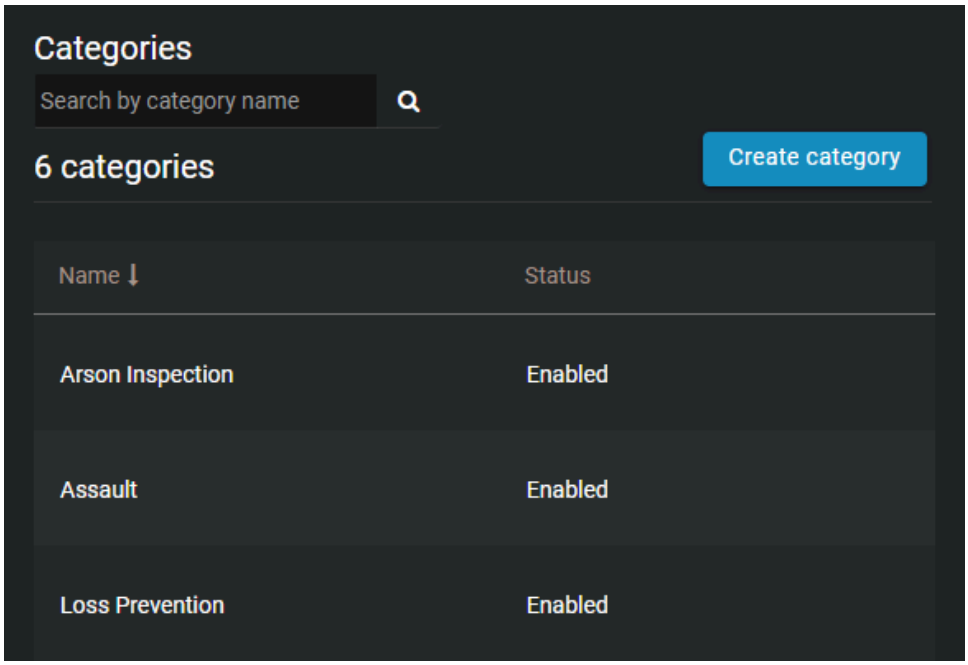
To properly classify incidents when creating cases, you can create categories for the different types of incidents.

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 **Loss Prevention** 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** > .



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 security policies

In AXIS Case Insight, 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

Related Topics

Permission levels on page 35
Security policy definitions list on page 47

Security policy definitions list

In AXIS Case Insight, 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.
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.

Security policy	Definition	Details
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.
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

Related Topics

Permission levels on page 35
Defining security policies on page 47

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 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 58

Configuring ID templates

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

3 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:

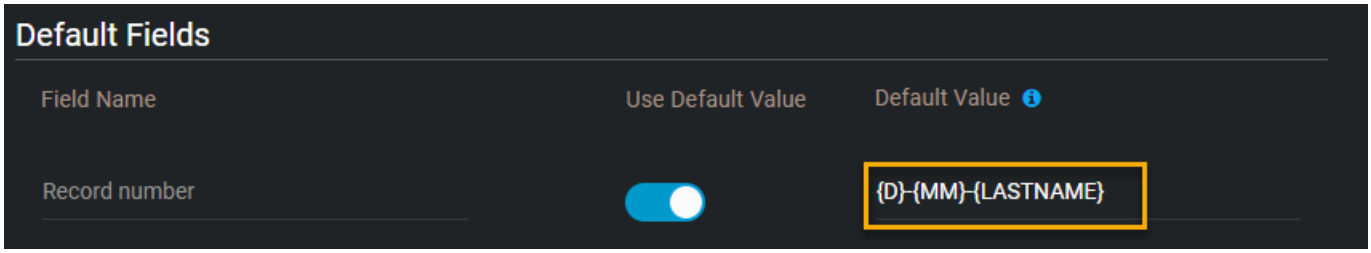
- You can also include fixed characters in the ID template by entering them in the ID template without any brackets, such as in the following example: CCN-1111-{YYYY}-{N}, which would yield the result: CCN-1111-2022-1.
- The {N} keyword is not displayed properly in the case and request views when the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

4 Click **Save**.

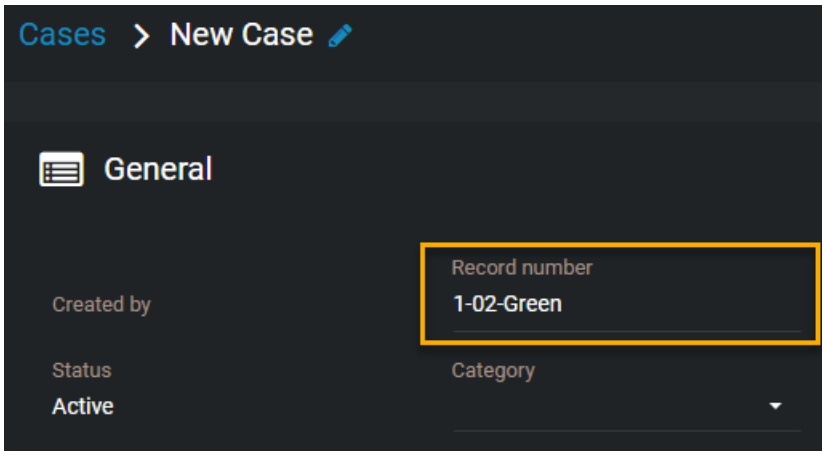
Your ID template is created.

Example

The field is configured:



The field appears in new cases:



After you finish

Create a case

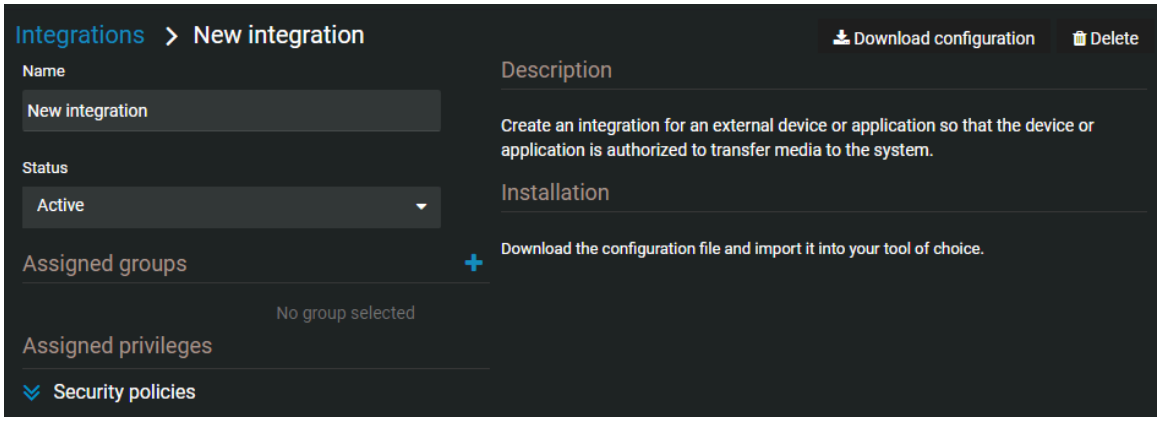
Creating integrations

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

Procedure

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

2 Select the integration that you want to create.



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.

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

Resetting user passwords

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

What you should know

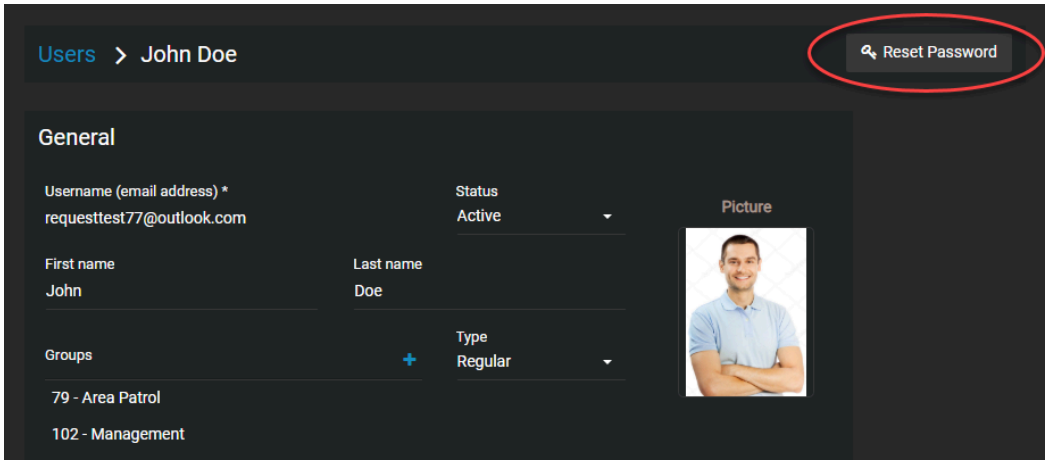
If the user's account is managed by an Active Directory, their password cannot be reset from AXIS Case Insight. They must contact their Active Directory system administrator for assistance.

Procedure

1 Click **Configurations**.

2 In the *Users* page, select a user.

3 In the user edit page, click **Reset Password**.



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 AXIS Case Insight on page 2

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.

Downloading a user list report

If you need to audit the users in your Axis Case Insight account, you can download a CSV file that lists all the users in your AXIS Case Insight 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 39.

6

Managing cases

Manage cases to record the details of an incident and link digital evidence in AXIS Case Insight.

This section includes the following topics:

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 AXIS Case Insight.
- 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:

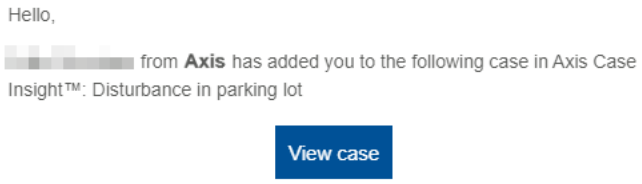
- **Record number:** A reference number for the case.
- **Incident number:** You can use this field to add external reference numbers to a case.
- **Category:** The type of incident. For example, you can categorize thefts as being either employee theft or shoplifting. You can only select one category 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.
- **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.

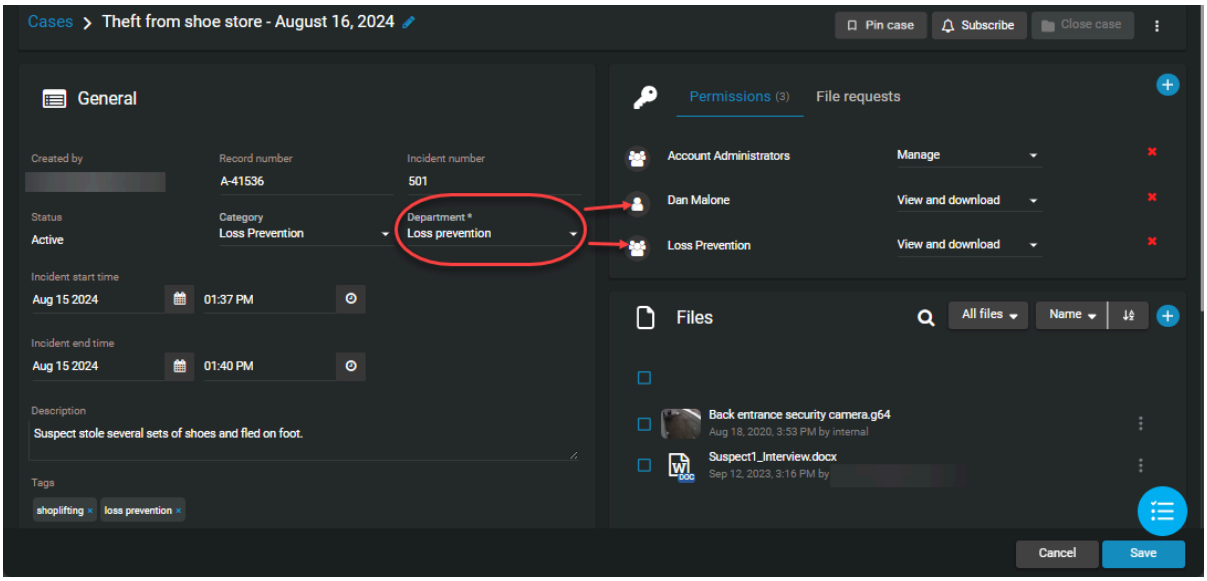
4 Click **Save**.

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



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.



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.

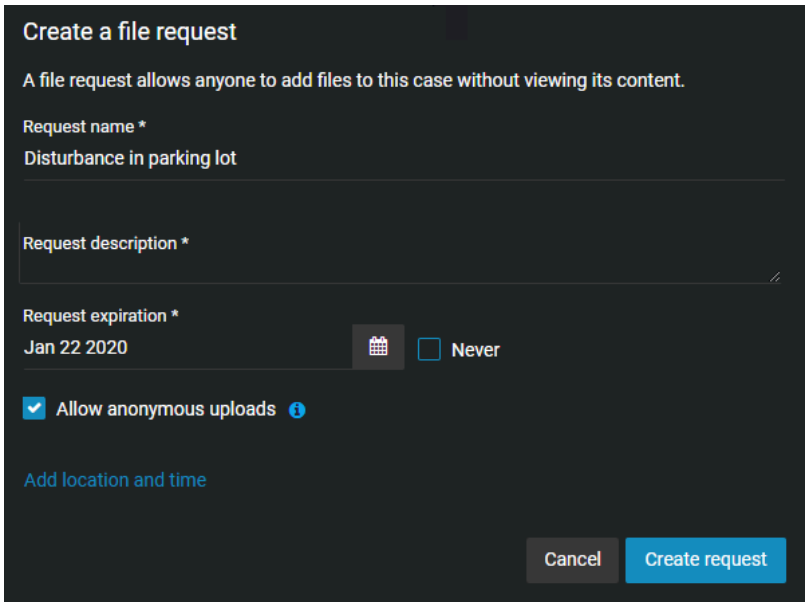
Before you begin

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 ( ).



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.

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 AXIS Case Insight, 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.

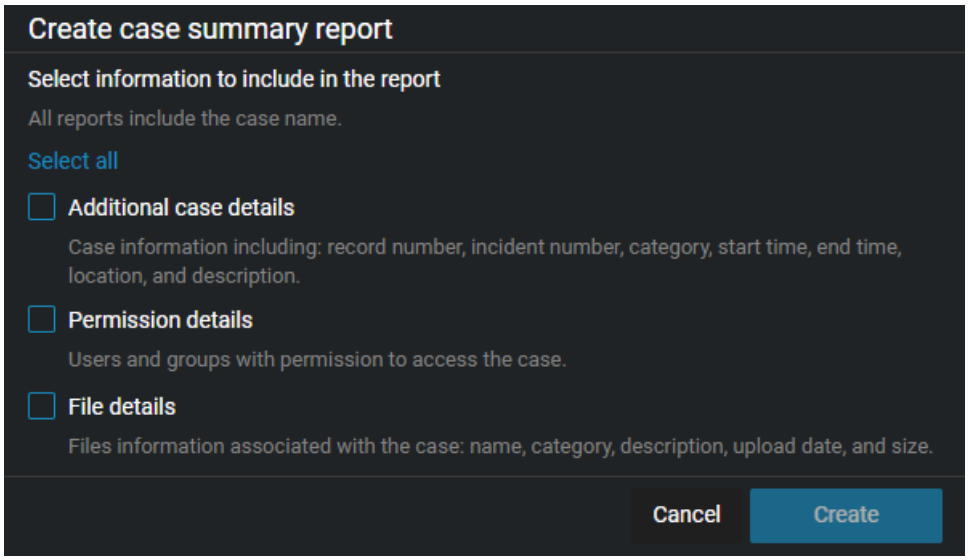
Procedure

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

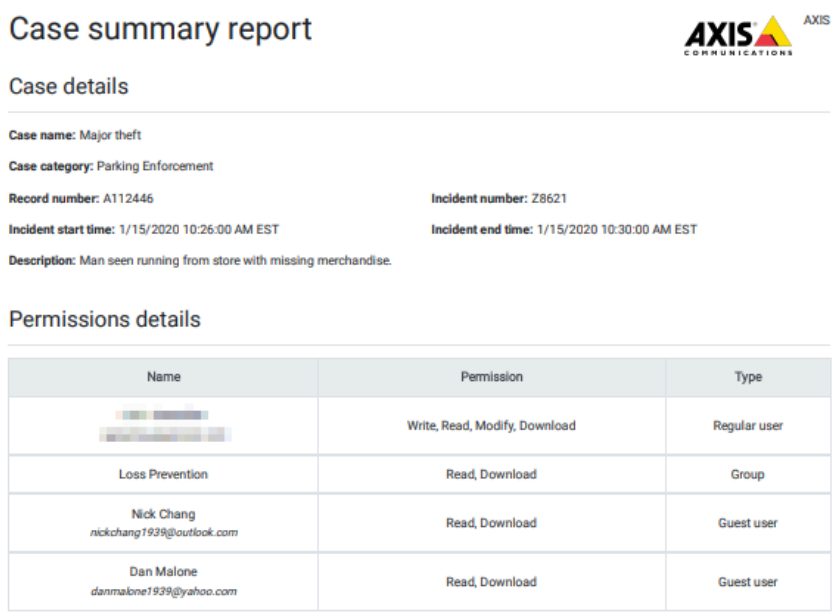
2 Click **More** (⋮) and click **Create report**.

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:



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



Case summary report

AXIS COMMUNICATIONS

Case details

Case name: Major theft

Case category: Parking Enforcement

Record number: A112446

Incident number: Z8621

Incident start time: 1/15/2020 10:26:00 AM EST

Incident end time: 1/15/2020 10:30:00 AM EST

Description: Man seen running from store with missing merchandise.

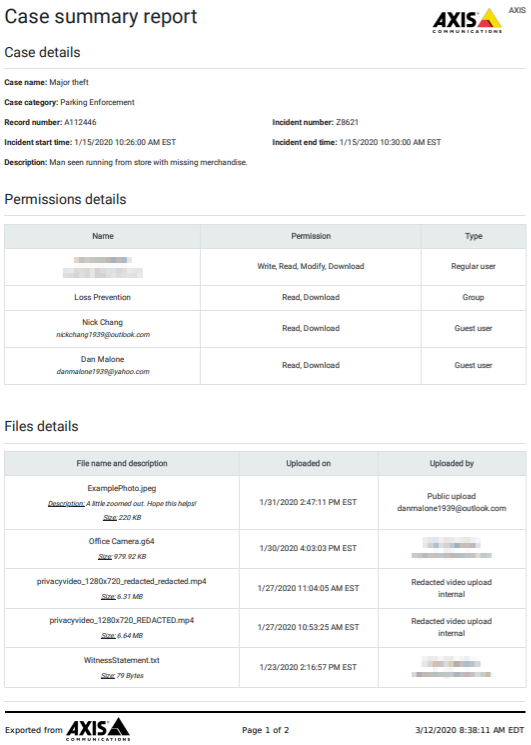
Permissions details

Name	Permission	Type
[redacted]	Write, Read, Modify, Download	Regular user
Loss Prevention	Read, Download	Group
Nick Chang nickchang1939@outlook.com	Read, Download	Guest user
Dan Malone danmalone1939@yahoo.com	Read, Download	Guest user

A copy of the case summary report PDF is stored in AXIS Case Insight.

6 Click **Download**.

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



Case summary report

AXIS COMMUNICATIONS

Case details

Case name: Major theft

Case category: Parking Enforcement

Record number: A112446

Incident number: Z8621

Incident start time: 1/15/2020 10:26:00 AM EST

Incident end time: 1/15/2020 10:30:00 AM EST

Description: Man seen running from store with missing merchandise.

Permissions details

Name	Permission	Type
[redacted]	Write, Read, Modify, Download	Regular user
Loss Prevention	Read, Download	Group
Nick Chang nickchang1939@outlook.com	Read, Download	Guest user
Dan Malone danmalone1939@yahoo.com	Read, Download	Guest user

Files details

File name and description	Uploaded on	Uploaded by
ExamplePhoto.jpeg Description: A little zoomed out. Hope this helps! Size: 220 KB	1/31/2020 2:47:11 PM EST	Public upload danmalone1939@outlook.com
Office Camera.g64 Size: 979.92 KB	1/30/2020 4:03:03 PM EST	[redacted]
privacyvideo_1280x720_redacted_redacted.mp4 Size: 6.31 MB	1/27/2020 11:04:05 AM EST	Redacted video upload internal
privacyvideo_1280x720_REDACTED.mp4 Size: 6.64 MB	1/27/2020 10:53:25 AM EST	Redacted video upload internal
WitnessStatement.txt Size: 79 Bytes	1/23/2020 2:16:57 PM EST	[redacted]

Exported from AXIS COMMUNICATIONS Page 1 of 2 3/12/2020 8:38:11 AM EDT

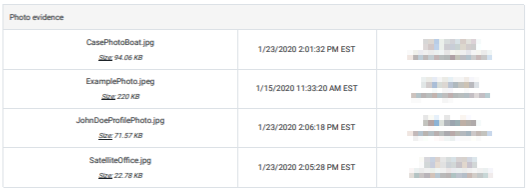
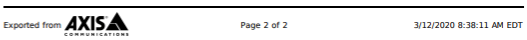


Photo evidence

CasePhotoBoat.jpg Size: 94.06 KB	1/23/2020 2:01:32 PM EST	[redacted]
ExamplePhoto.jpeg Size: 220 KB	1/15/2020 11:33:20 AM EST	[redacted]
JohnDoeProfilePhoto.jpg Size: 71.57 KB	1/23/2020 2:06:18 PM EST	[redacted]
SatelliteOffice.jpg Size: 22.78 KB	1/23/2020 2:05:28 PM EST	[redacted]



Exported from AXIS COMMUNICATIONS Page 2 of 2 3/12/2020 8:38:11 AM 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 28

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 47

What you should know

- In AXIS Case Insight, 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:

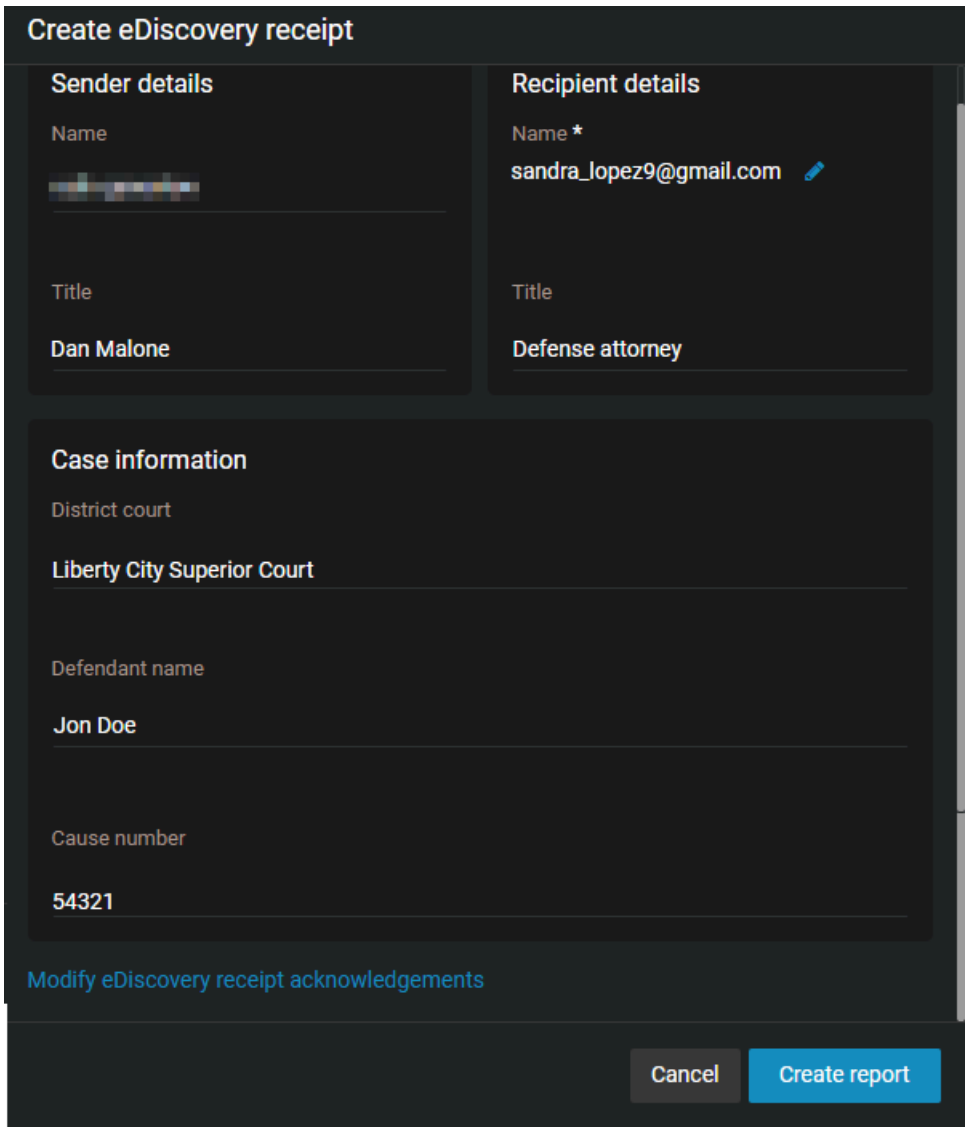
a) (Optional) In the *Sender details* section, enter a **Name** and **Title**.

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*."

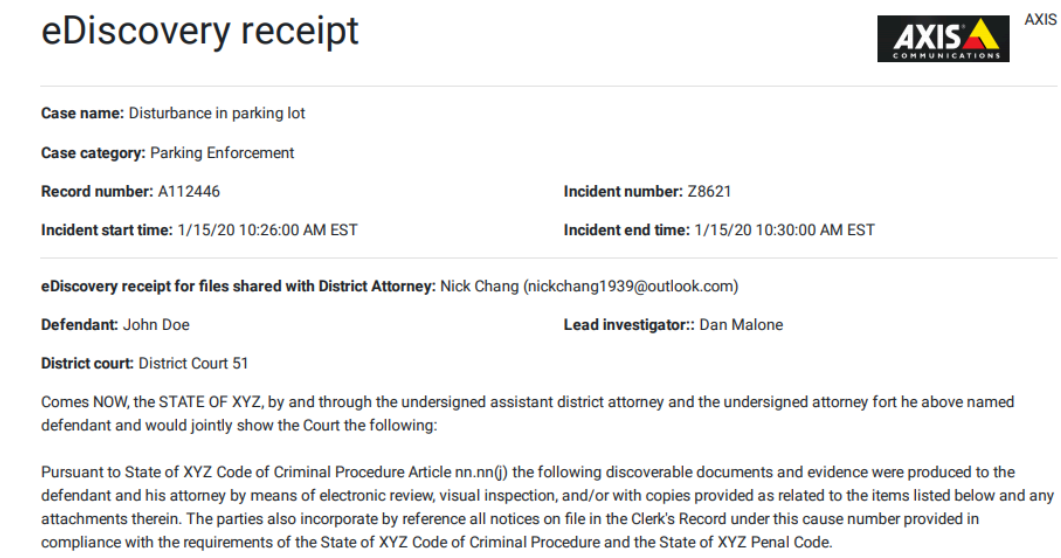
b) In the **Recipient details** section, click **Select** to choose a recipient and enter their **Title** if applicable.

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.



6 Click **Create report**.



eDiscovery receipt

AXIS

Case name: Disturbance in parking lot

Case category: Parking Enforcement

Record number: A112446 **Incident number:** Z8621

Incident start time: 1/15/20 10:26:00 AM EST **Incident end time:** 1/15/20 10:30:00 AM EST

eDiscovery receipt for files shared with District Attorney: Nick Chang (nickchang1939@outlook.com)

Defendant: John Doe **Lead investigator::** Dan Malone

District court: District Court 51

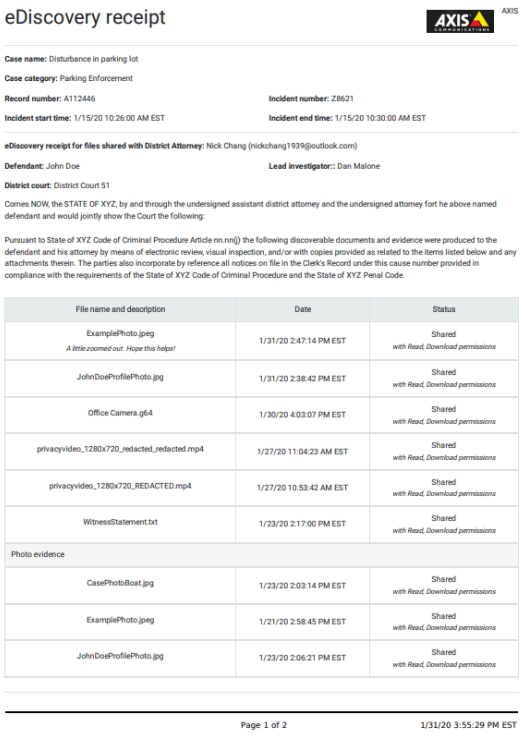
Comes NOW, the STATE OF XYZ, by and through the undersigned assistant district attorney and the undersigned attorney fort he above named defendant and would jointly show the Court the following:

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.

A copy of the eDiscovery receipt report PDF is stored in AXIS Case Insight.

7 Click **Download**.

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



eDiscovery receipt

AXIS

Case name: Disturbance in parking lot

Case category: Parking Enforcement

Record number: A112446 **Incident number:** Z8621

Incident start time: 1/15/20 10:26:00 AM EST **Incident end time:** 1/15/20 10:30:00 AM EST

eDiscovery receipt for files shared with District Attorney: Nick Chang (nickchang1939@outlook.com)

Defendant: John Doe **Lead investigator::** Dan Malone

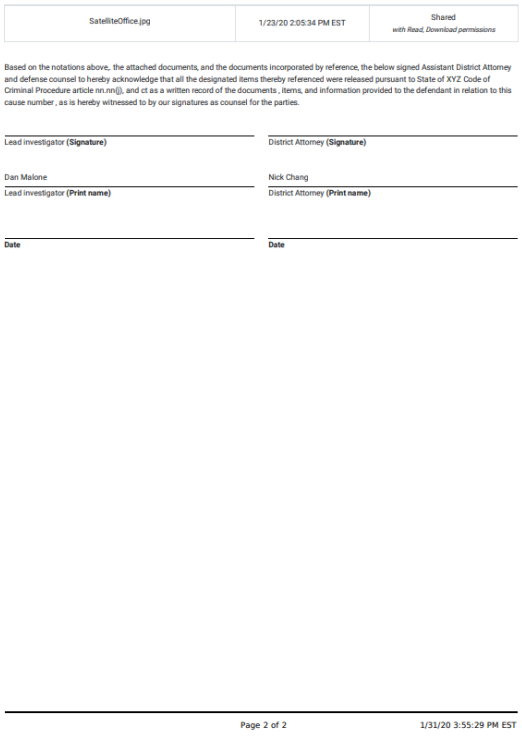
District court: District Court 51

Comes NOW, the STATE OF XYZ, by and through the undersigned assistant district attorney and the undersigned attorney fort he 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 and description	Date	Status
ExamplePhoto.jpeg *A little zoomed out. Hope this helps!*	1/31/20 2:47:14 PM EST	Shared *with Read, Download permissions*
JohnDoeProfilePhoto.jpg	1/31/20 2:38:42 PM EST	Shared *with Read, Download permissions*
Office Camera.g64	1/30/20 4:03:07 PM EST	Shared *with Read, Download permissions*
privacyvideo_1280x720_redacted_redacted.mp4	1/27/20 11:04:23 AM EST	Shared *with Read, Download permissions*
privacyvideo_1280x720_REDACTED.mp4	1/27/20 10:53:42 AM EST	Shared *with Read, Download permissions*
WitnessStatement.txt	1/23/20 2:17:00 PM EST	Shared *with Read, Download permissions*
Photo evidence		
CasePhotoBoat.jpg	1/23/20 2:03:14 PM EST	Shared *with Read, Download permissions*
ExamplePhoto.jpeg	1/21/20 2:58:45 PM EST	Shared *with Read, Download permissions*
JohnDoeProfilePhoto.jpg	1/23/20 2:06:21 PM EST	Shared *with Read, Download permissions*

Page 1 of 2 1/31/20 3:55:29 PM EST



SatelliteOffice.jpg	1/23/20 2:05:34 PM EST	Shared *with Read, Download permissions*

Based on the notations above, the attached documents, and the documents incorporated by reference, the below signed Assistant District Attorney and defense counsel to 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 ct 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.

Lead investigator **(Signature)** District Attorney **(Signature)**

Dan Malone Nick Chang

Lead investigator **(Print name)** District Attorney **(Print name)**

Date **Date**

Page 2 of 2 1/31/20 3:55:29 PM EST

After you finish

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

Related Topics

Configuring your account information on page 28
Configuring your report templates on page 31

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.

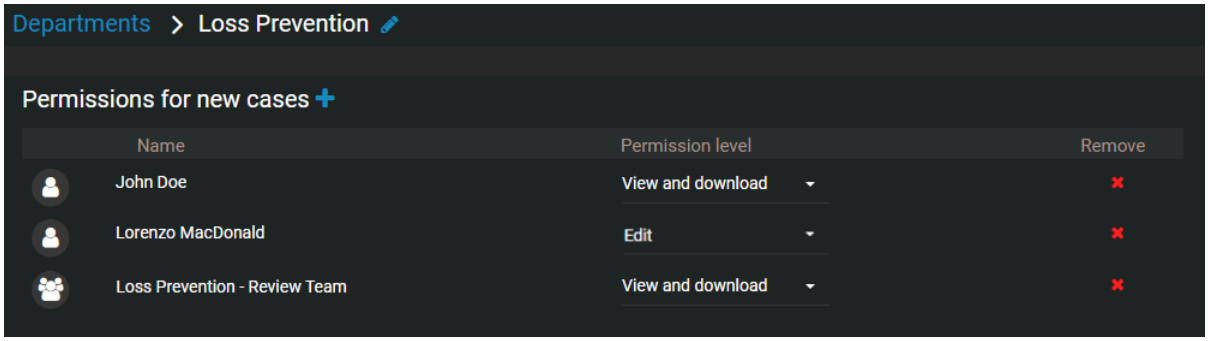
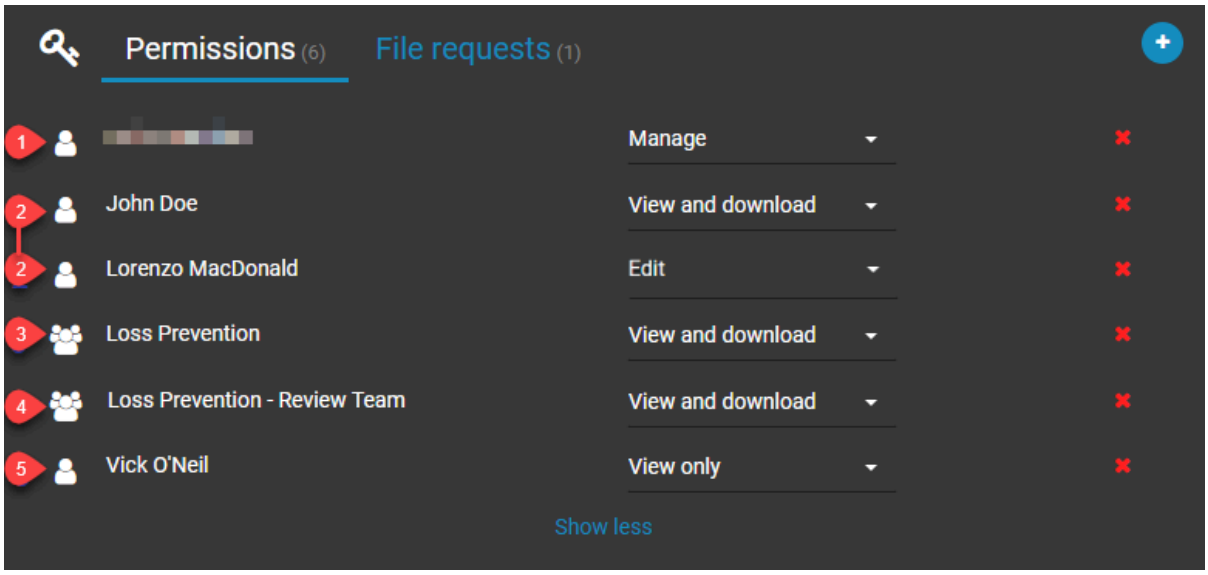


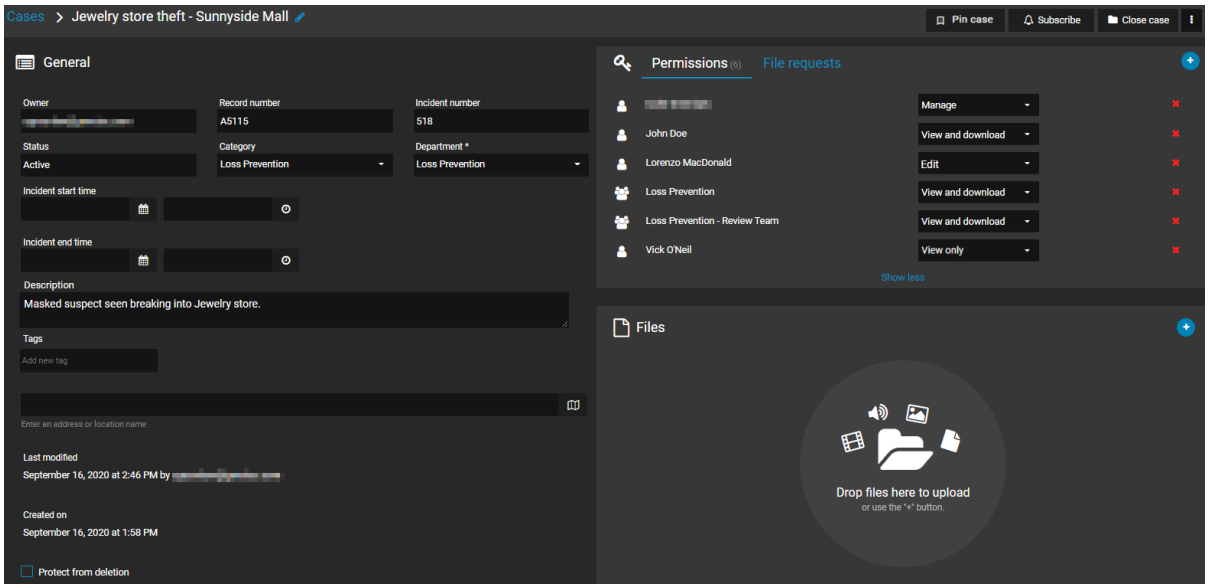
Figure B. New case assigned to the Loss Prevention Department

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.



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.



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**.

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.

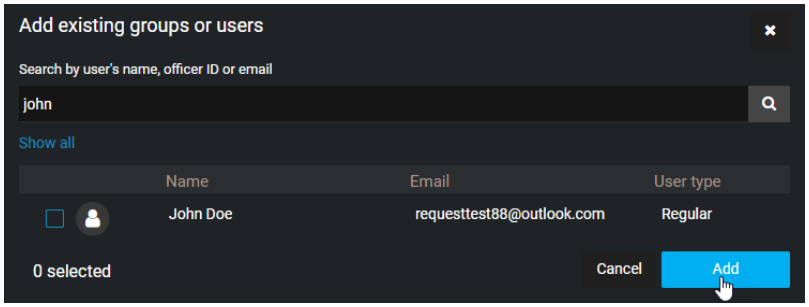
Procedure

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**.

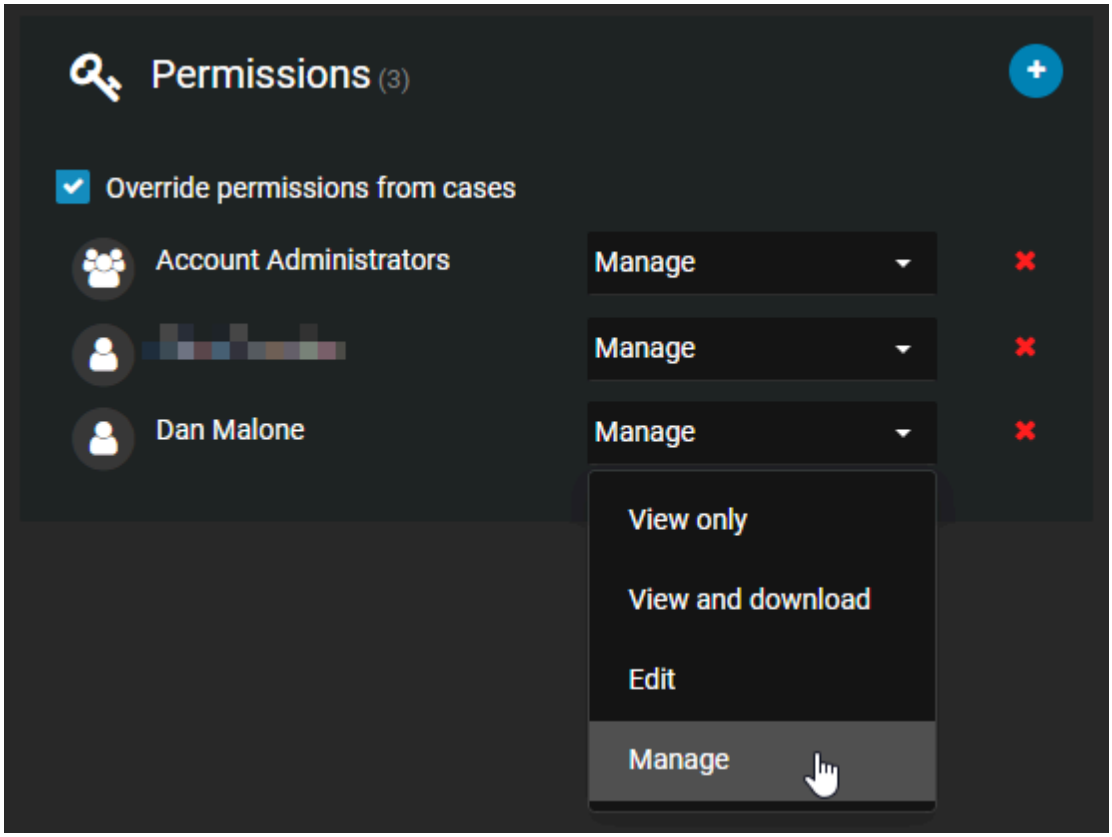


4 If you selected **Invite guest user**, enter the email of the guest user you want to share the case with.

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**.



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

Related Topics

About email notifications in AXIS Case Insight on page 2
Inviting guests to view cases on page 78

Pinning cases to the homepage

You can pin cases to the homepage in Axis Case Insight to quickly locate the ones you're working on or that require review.

What you should know

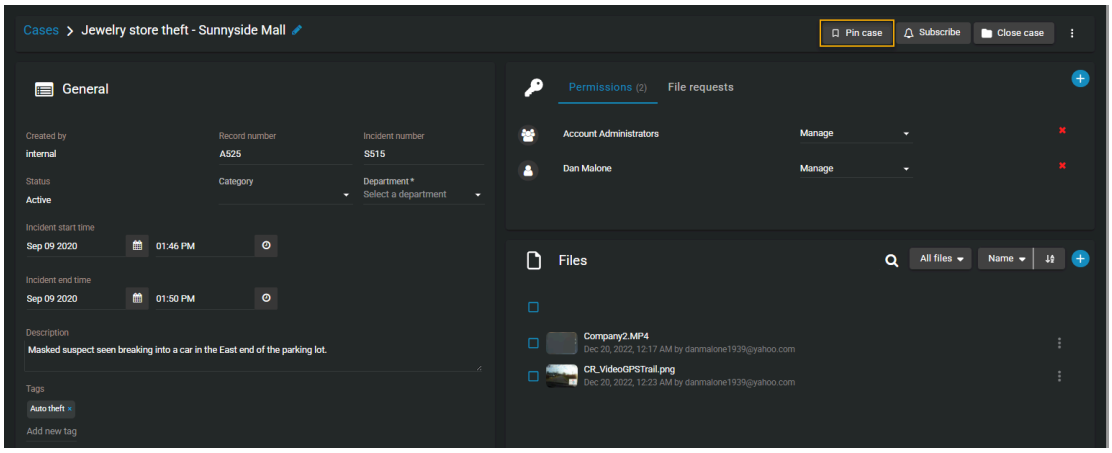
- Each AXIS Case Insight user has their own list of pinned cases.
- You can pin any case that you have access to, no matter your permission level.
- Each AXIS Case Insight user can have up to 50 cases pinned to the homepage at one time.

Procedure

To pin a case:

1 Open an existing case or create a case.

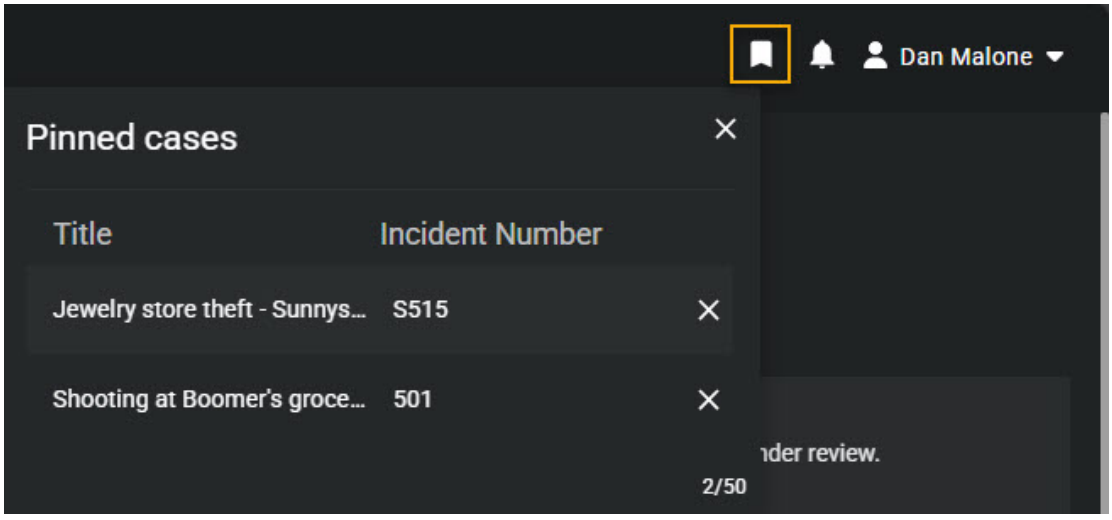
2 Click **Pin case**.



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** ( ).



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 AXIS Case Insight 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

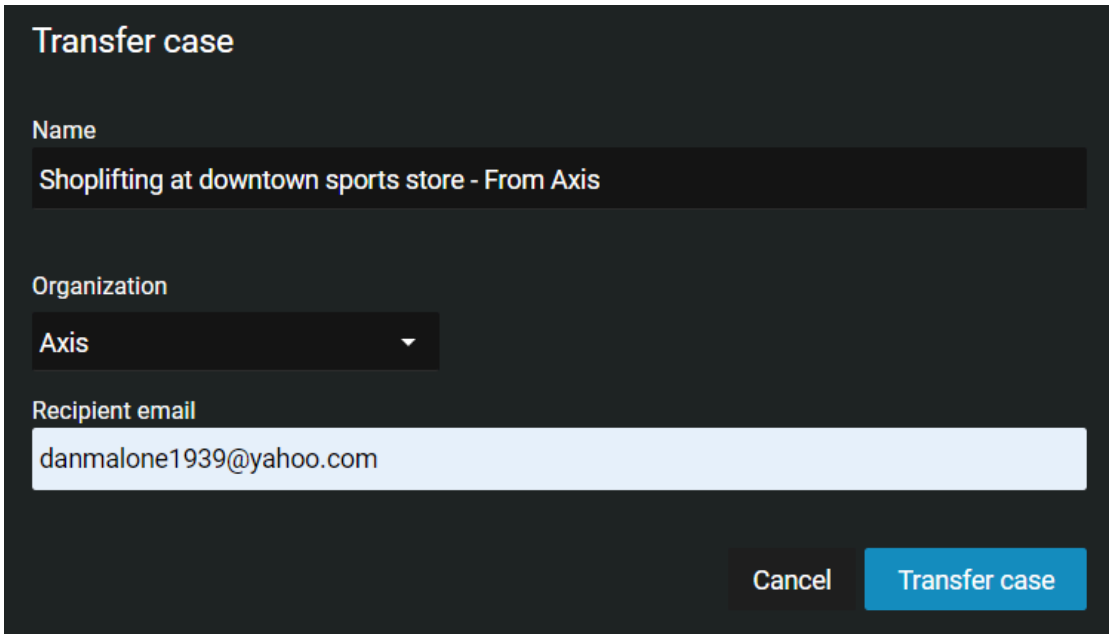
1 Select the case you want to transfer.

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 email** 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.



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.

Inviting guests to view cases

To share a specific case with someone who does not have a AXIS Case Insight 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.

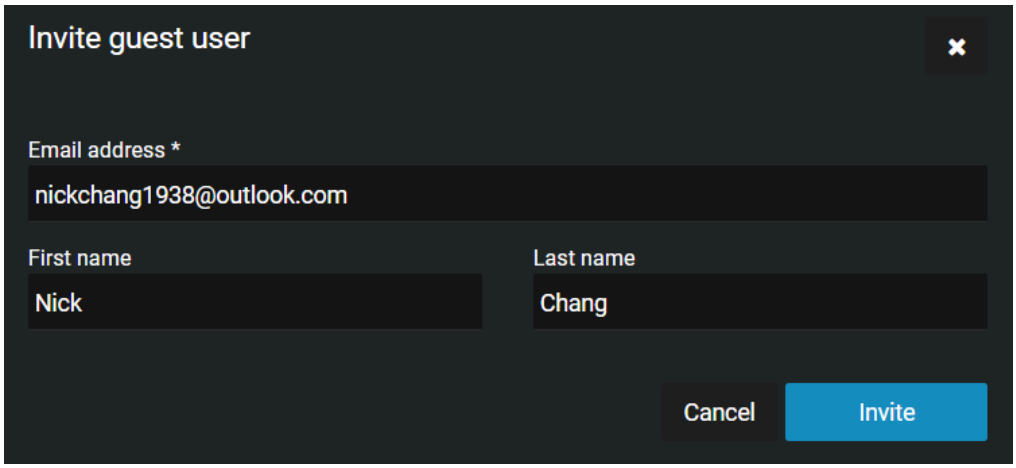
Procedure

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**.



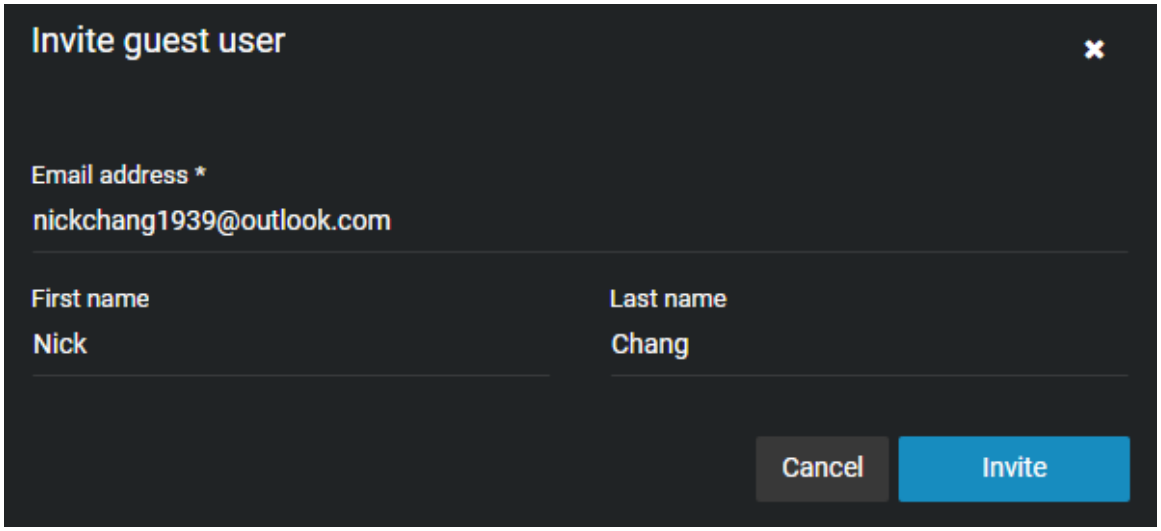
3 If you are a regular user inviting a guest user that has a AXIS Case Insight account, do the following:

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**.



   The person's email address is displayed in the *Permissions* section for the case, and an email inviting the user to join AXIS Case Insight 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**.

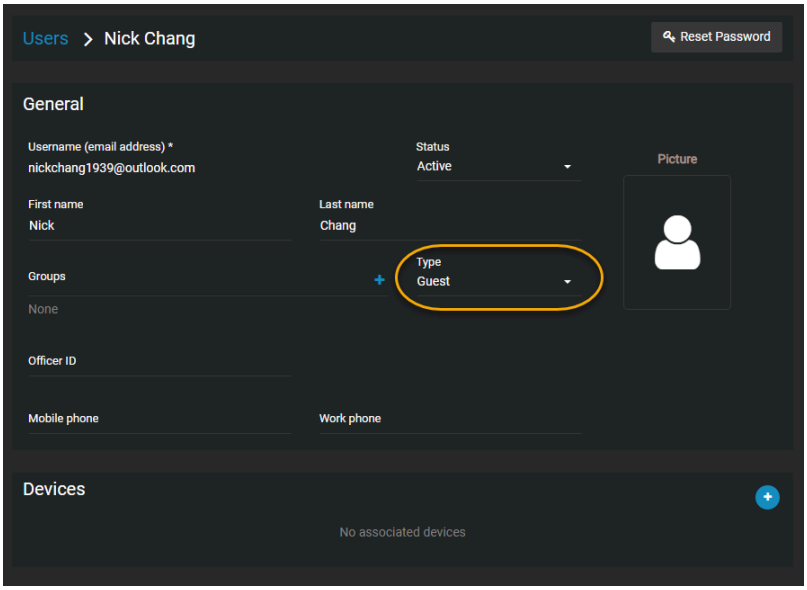
An email is automatically sent to the user, inviting the user to view the case details. After activating their account and logging on to the system, the user will only have access to the case that they were invited to view.

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.


Users > Nick Chang
Reset Password
General
Username (email address) *
nickchang1939@outlook.com
Status
Active
Picture
First name
Nick
Last name
Chang
Groups
Type
Guest
None
Officer ID
Mobile phone
Work phone
Devices
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

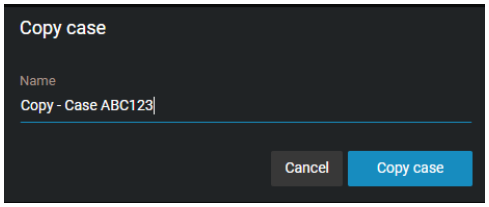
- A guest user cannot copy a case.
- Creating a copy of a case consumes one case in the plan's quota. The user that copied the case becomes the case owner.
- When a case is copied, no email notifications are sent, a unique case number is assigned, and duplicate case names are accepted.
- By default, 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`.



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.

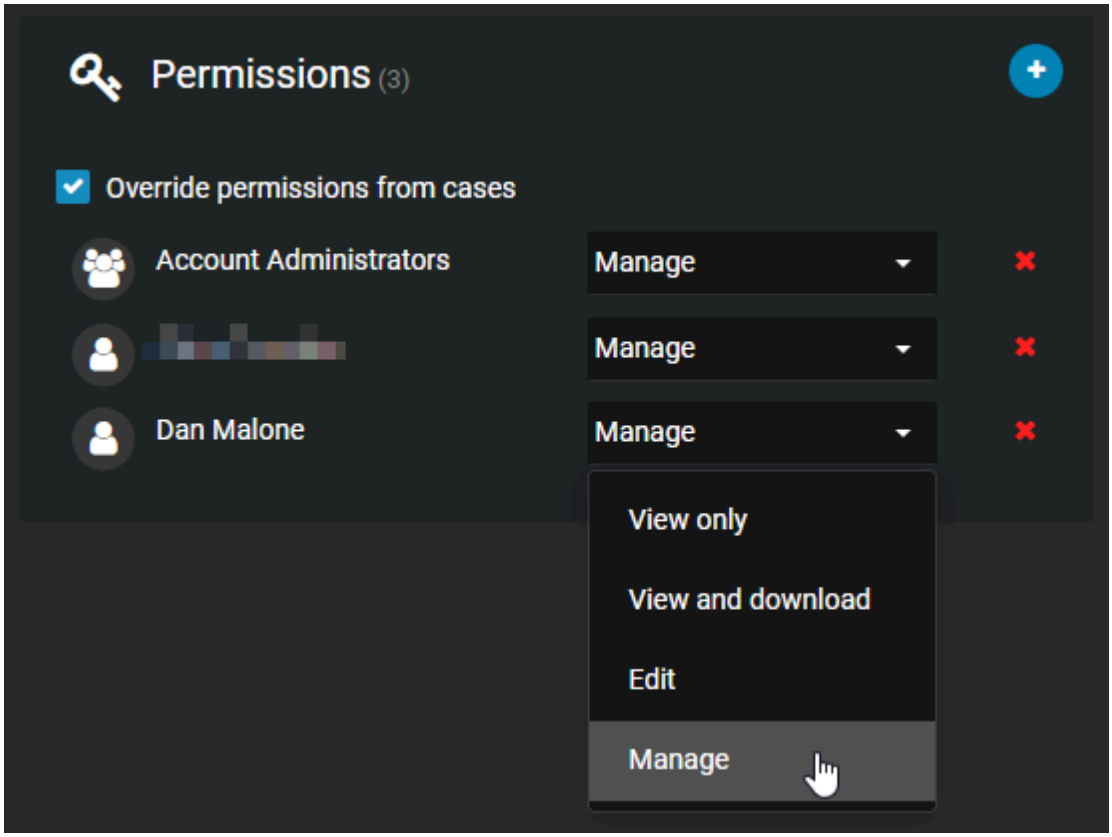
What you should know

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.



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 96
Viewing the audit trail history of files on page 130

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.

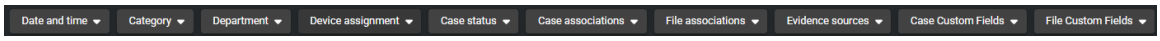
Procedure

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.

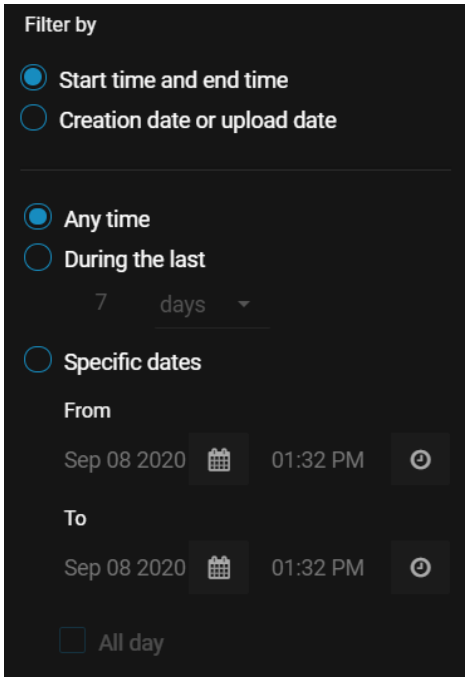


TIP: Click on the name of a column to sort it in ascending or descending order.

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.



- 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.

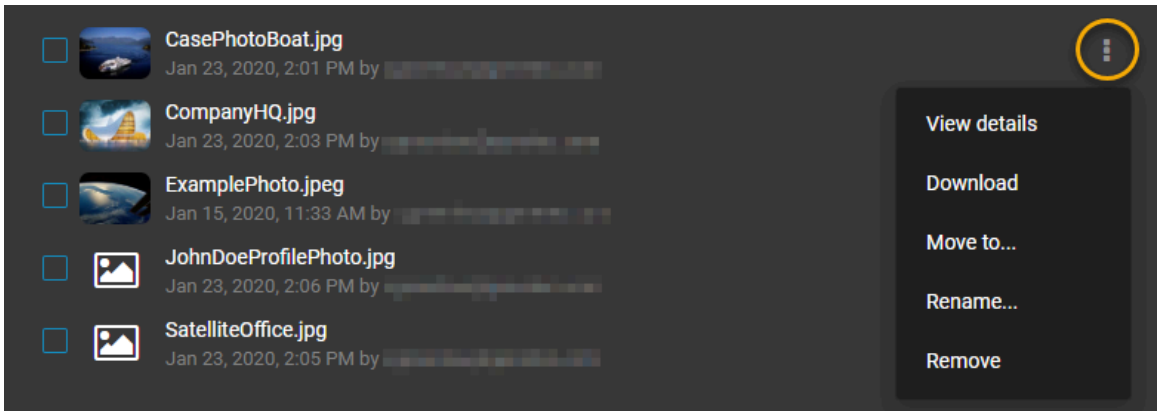
4 Select a filter from the **All files** list:

- **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.



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.

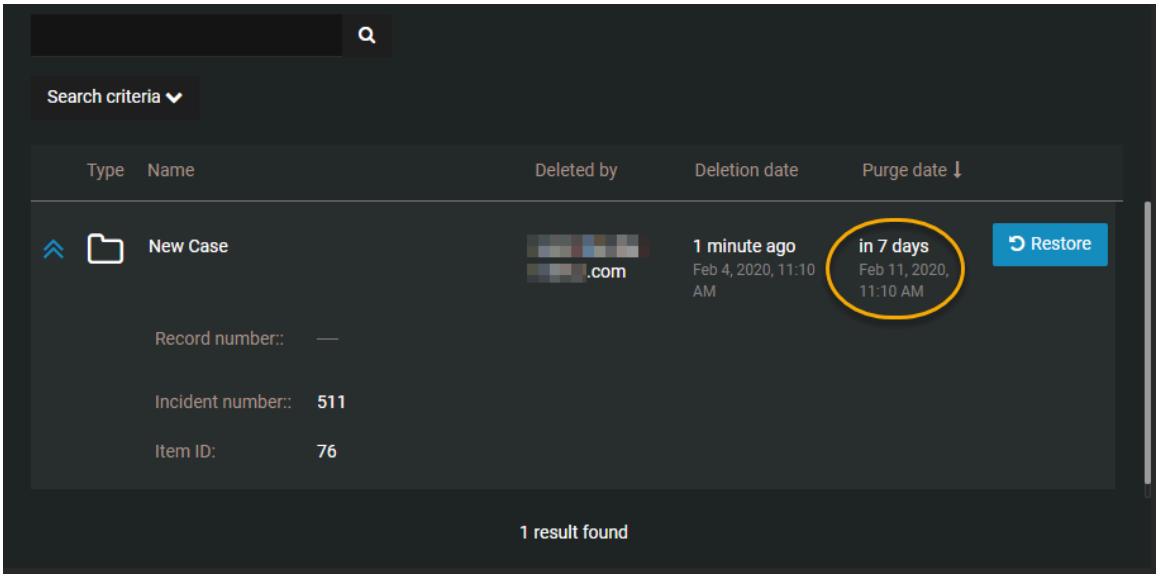
a) Clear the **Protect from deletion** check box.

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



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 AXIS Case Insight database.

Related Topics

Viewing the audit trail history of cases on page 96

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**.

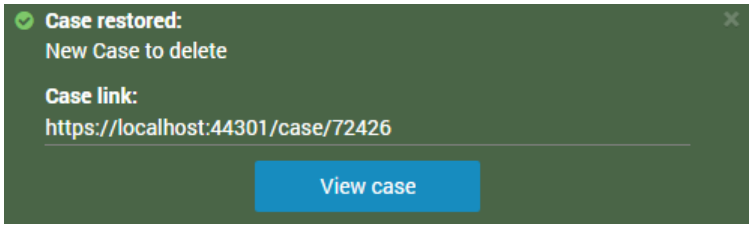
A confirmation message is displayed.

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.



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

Related Topics

Viewing the audit trail history of cases on page 96

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 AXIS Case Insight information security on page 104
Deleting cases on page 93
Restoring cases on page 95
Changing access policies for cases on page 82

7

Managing devices

Add, remove, and configure devices in AXIS Case Insight.

This section includes the following topics:

Enrolling Axis body worn cameras

You can enroll an Axis body worn camera in AXIS Case Insight by docking the camera in a docking station connected to an Axis body worn system. The Axis body worn system must be associated with AXIS Case Insight before hand.

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.
- The Axis body worn system must be installed and associated with an AXIS Case Insight account.

What you should know

The first time that you dock a new camera, the camera is automatically detected.

NOTE: New body worn cameras are visible in AXIS Case Insight, only if the Axis body worn system has been associated with AXIS Case Insight.

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**.

After you finish

You can now activate the device license.

Activating device licenses

Activate device licenses in AXIS Case Insight 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**.

The device license is now activated.

After you finish

You can now assign the device to a user.

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**.

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**.

The user is now assigned to the device.

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 AXIS Case Insight 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:

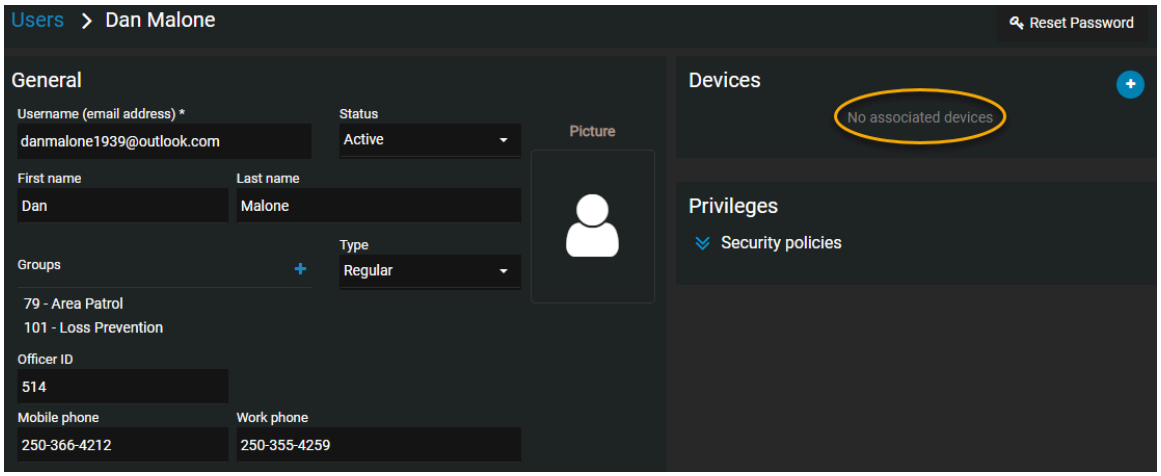
1 Click **Configurations** > **Users**.

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**.



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**.

The user is no longer assigned to the device.

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 AXIS Case Insight 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.
- AXIS Body Worn Manager must be installed and associated with an AXIS Case Insight 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:

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.

After you finish

You can now activate this device license for a new device if required.

8

Managing files

Create, share, and associate files in AXIS Case Insight.

This section includes the following topics:

About AXIS Case Insight information security

All data and files imported in AXIS Case Insight 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 AXIS Case Insight 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 AXIS Case Insight 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

AXIS Case Insight 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.

AXIS Case Insight 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 AXIS Case Insight 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 130
Viewing the audit trail history of cases on page 96

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

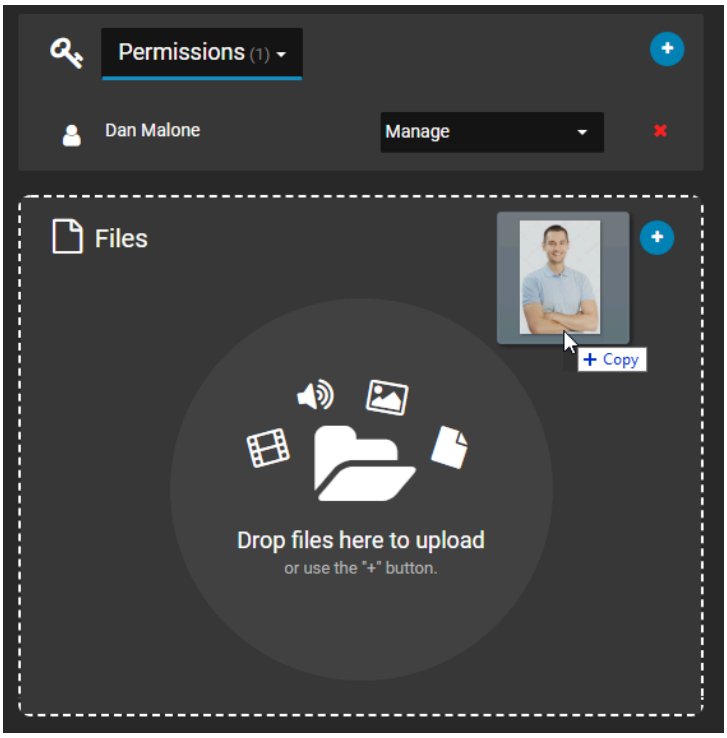
1 Open an existing case or create a case.

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

- **Add files from computer**
- **Add files from AXIS Case Insight**
- **Create folder**

NOTE: The **Add files from AXIS Case Insight** option is not available for guest users.

3 If you selected **Add files from computer**, do the following:
   a) Select the files you need using one of the following methods:
      - Select files that are saved on your local or network drive.
      - Drag files into the **Files** field of the case.



   b) After selecting the files you need, click **Open**.
   c) (Optional) To remove files that you no longer require, click **More** (⋮) and click **Remove**.
      The file is removed from the case, but remains in the system and can still be searched, edited, viewed, and downloaded.

4 If you selected **Add files from AXIS Case Insight**, 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 124
Searching for cases or files on page 84
File formats you can preview in AXIS Case Insight on page 120

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 AXIS Case Insight, click a file.
The evidence player opens.

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

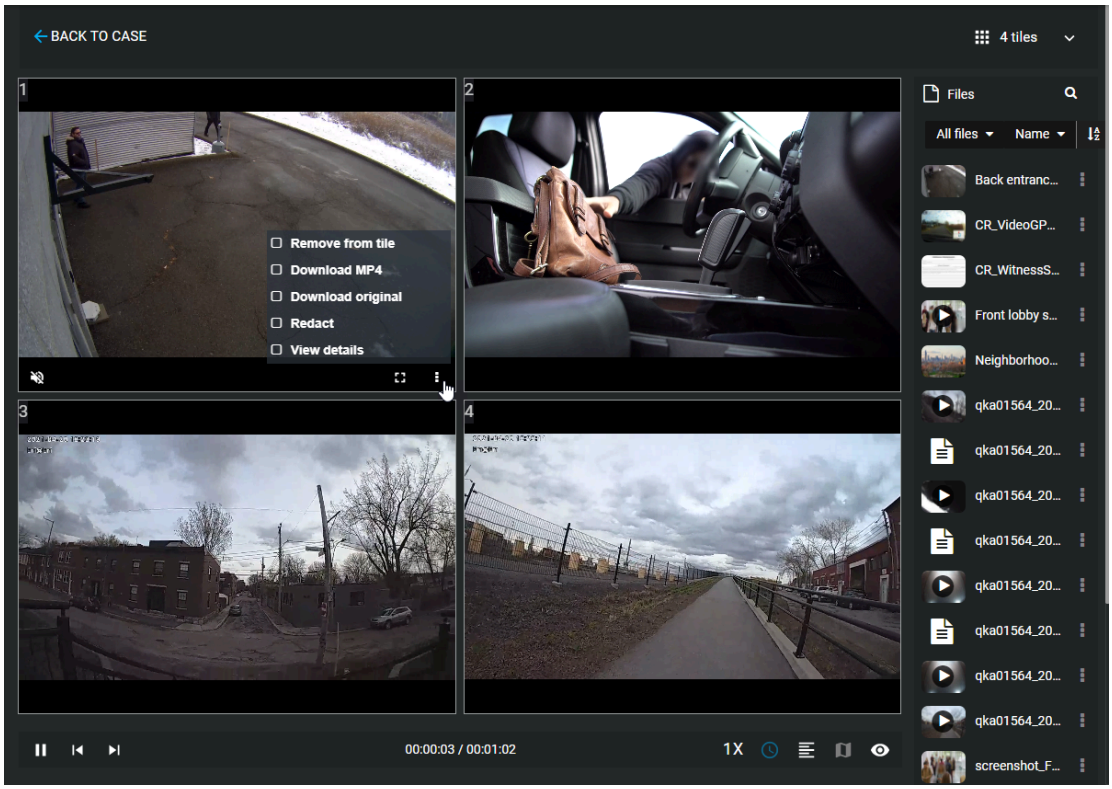
1 From the AXIS Case Insight search page, open a file.

2 Click **Play** ( ).

From the evidence player:

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

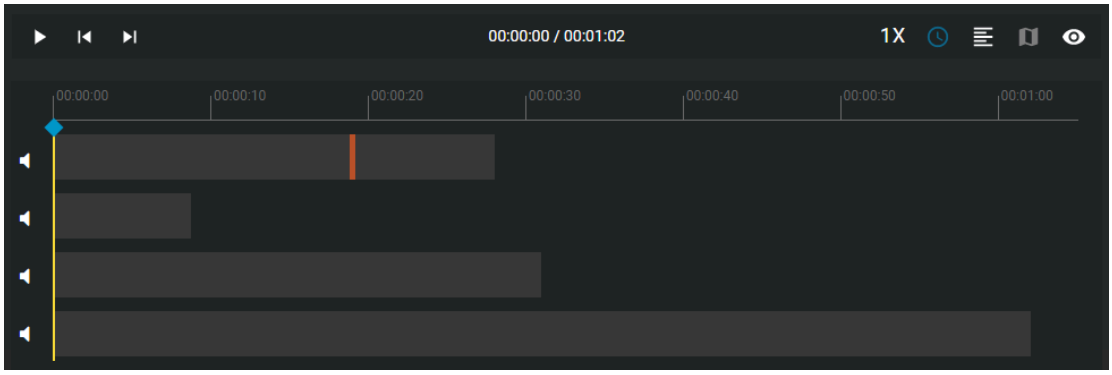
2 Click the files you want to examine, or drag and drop them into the tiles.



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

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



Example

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

After you finish

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

Video player controls

Use the video player controls in AXIS Case Insight 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.
	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.
	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.

Configuring file details

Configure file details to better classify and compare your evidence files.

Before you begin

Upload a file to a case in AXIS Case Insight.

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.

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

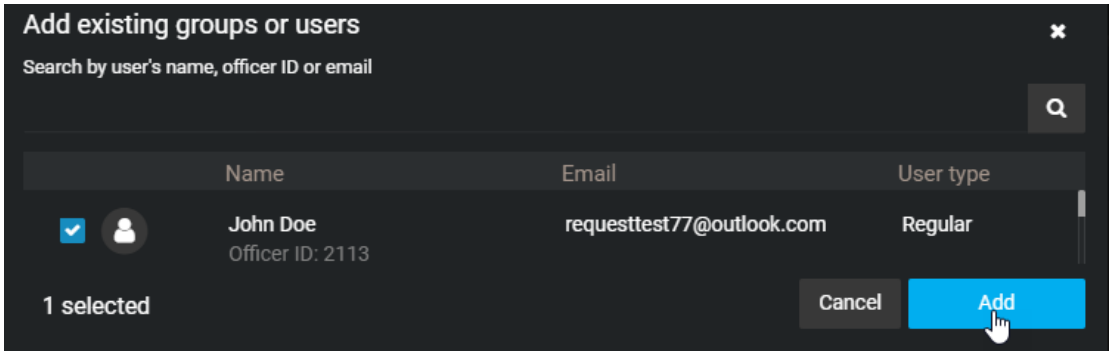
Create a user account for the user you want to share the file with.

Procedure

1 Open an existing file or Upload a file.

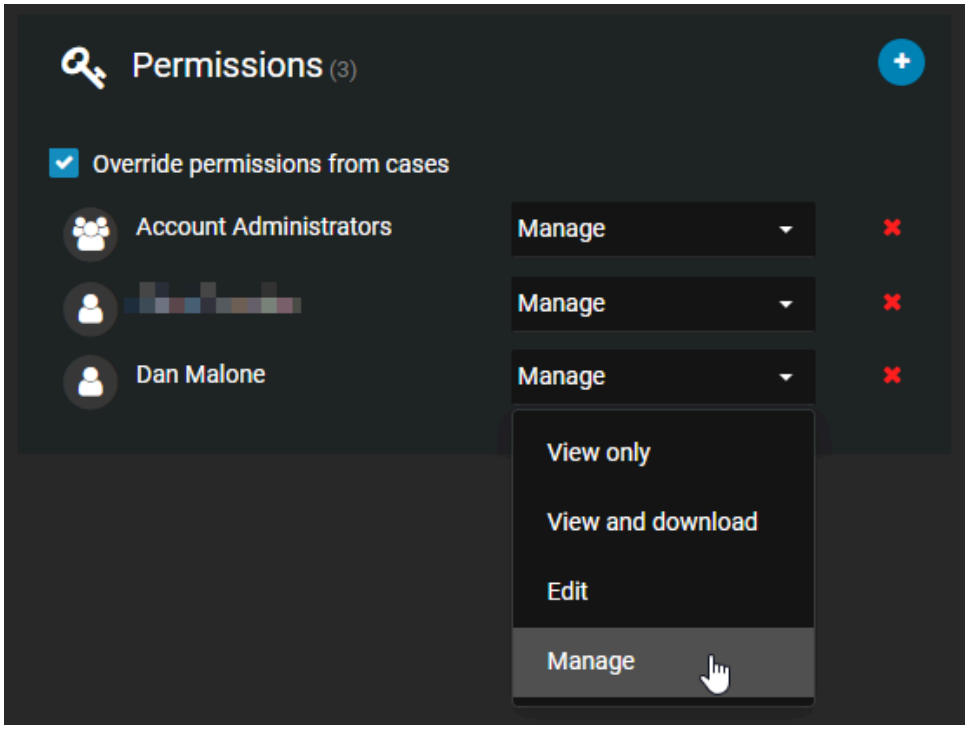
2 In the **Permissions** section, click > **Add users** .

3 In the *Add existing users* window, select the user and then click **Add**.



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**.



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

Related Topics

About email notifications in AXIS Case Insight on page 2
Inviting guests to view files on page 114

Inviting guests to view files

If you want to share a specific file with someone who does not already have a AXIS Case Insight 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.

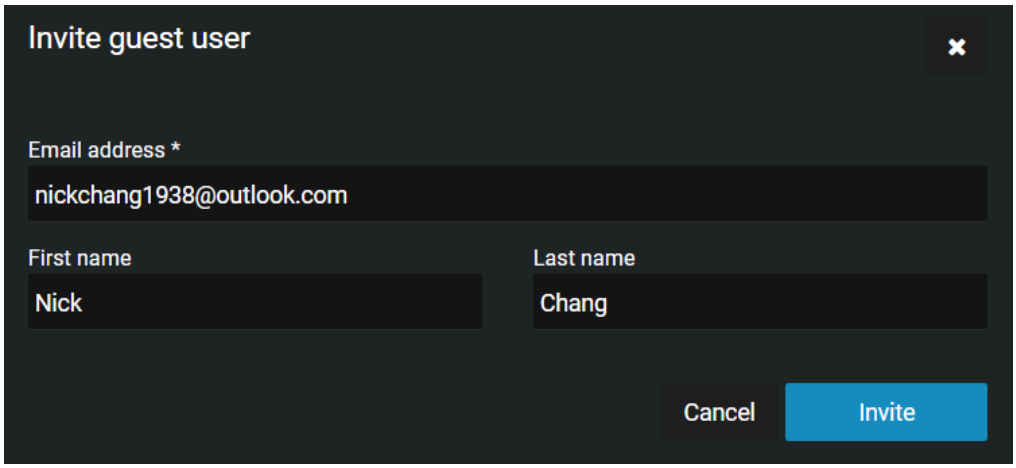
Procedure

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**.



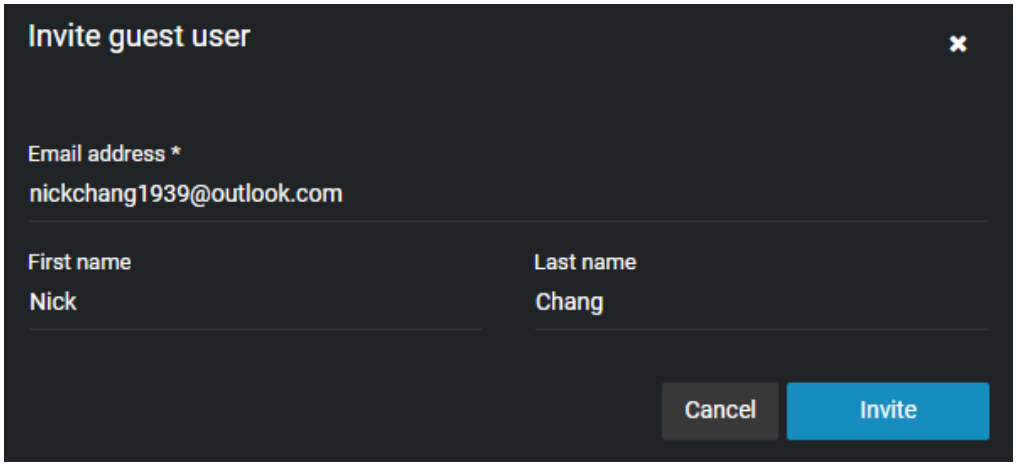
3 If you are a regular user inviting a guest user that has a AXIS Case Insight account, do the following:

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**.



   The person's email address is added to the *Permissions* section for the file, and an email inviting the user to join AXIS Case Insight 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.

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.

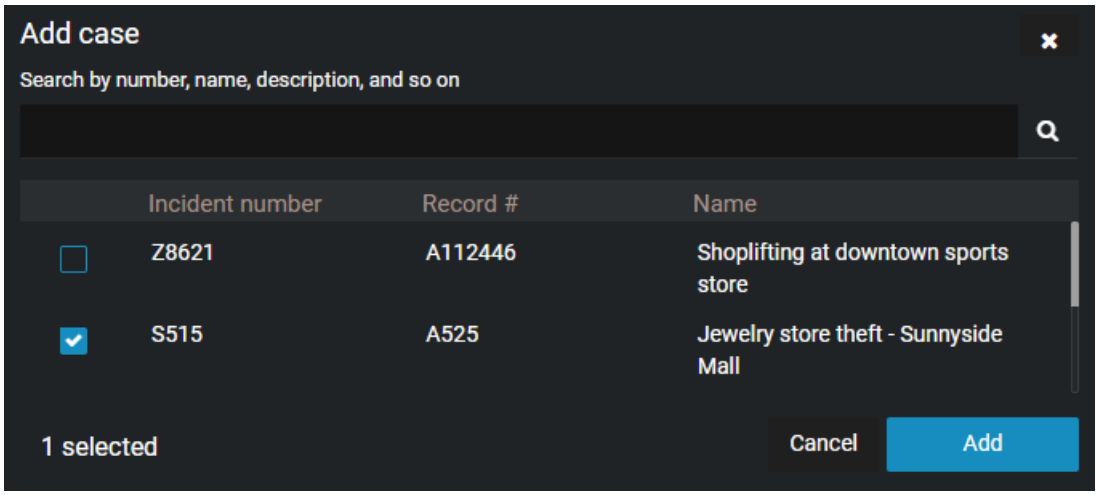
Procedure

1 Open an existing file.

2 In the *General* section of the *File edit* page, next to **Associated cases** click **Add**.

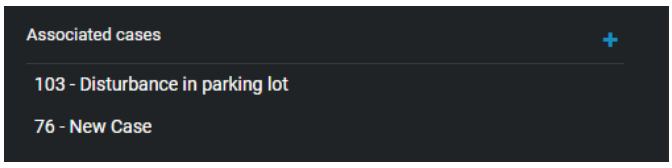
3 In the *search* box, type a case name, and press **Enter** or click the **search** button ( ).

4 Select the check box for the case that you require and click **Add**.



5 (Optional) Click **Remove** to remove any cases that are no longer required.

6 Click **Save**.



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 AXIS Case Insight.

Before you begin

Upload files to a case.

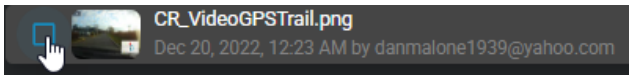
What you should know

- 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.



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.

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

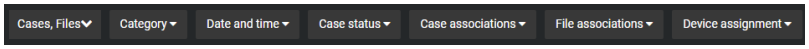
- Thumbnail previews are displayed in search results for the following files: BMP, PNG, JPEG, GIF, Icon, and MP4.
- When you select **Specific dates**, any cases or files that have at least 1 minute of their duration within the time range are displayed.
- All media recorded using an assigned device is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

Procedure

1 Click the **Files** tab or **Search** tab.

2 Click the **Search Criteria** toolbar menu.

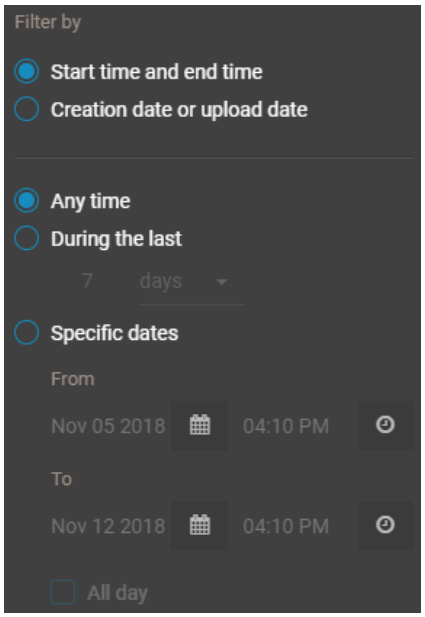
3 To filter your search for files, select **Files**.



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.

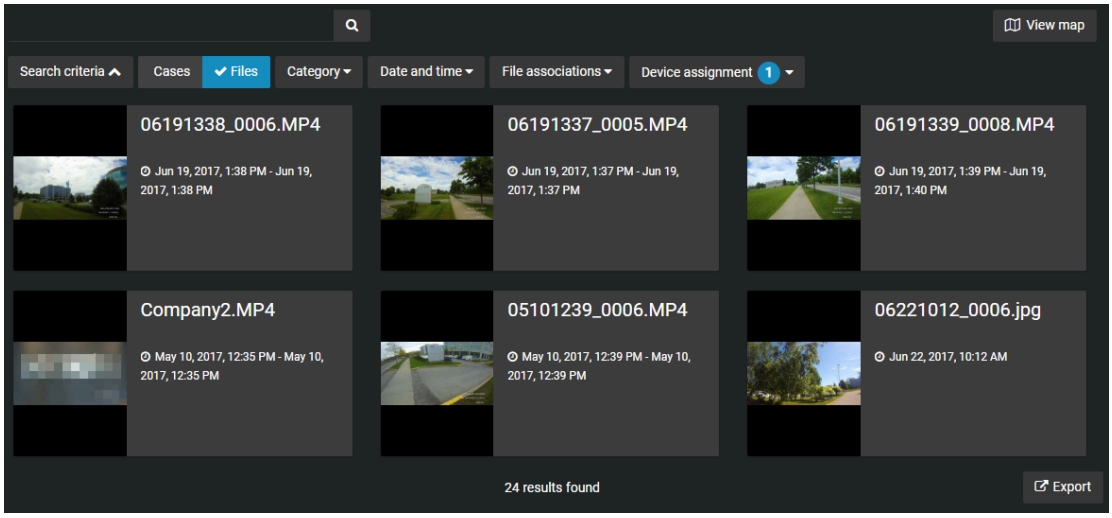
5 (Optional) To filter by date or time, click **Date and time** and select the options that you require.



- 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**.



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 AXIS Case Insight

A file in AXIS Case Insight 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 AXIS Case Insight:

- ASF (.asf)
- AVI (Uncompressed 8 bit/10 bit) (.avi)
- AV3
- FLV with H.264 and AAC codecs (.flv)
- GXF (.gxf)
- 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, 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.

Audio formats

The following audio formats can be previewed in AXIS Case Insight:

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

Image formats

The following image formats can be previewed in AXIS Case Insight:

- 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 AXIS Case Insight:

- 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 105

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.

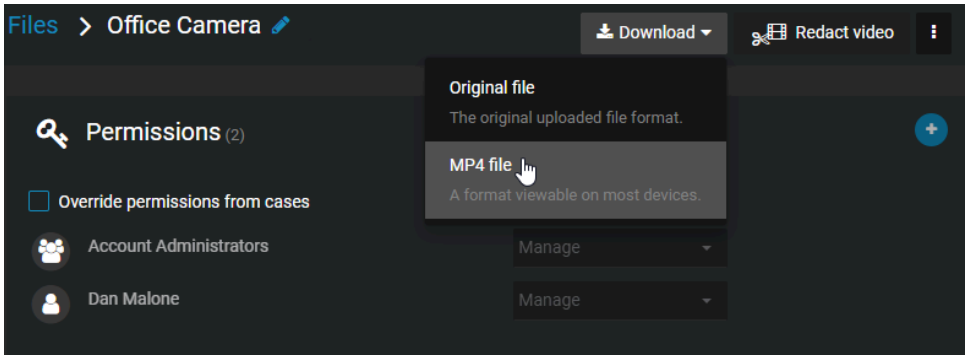
Procedure

To download a file:

1 Open an existing file.

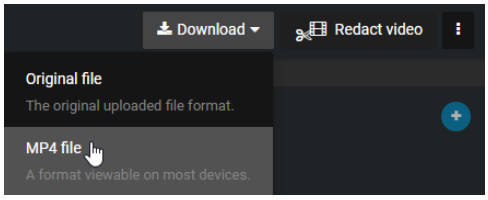
2 Click **Download**.

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



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 an MP4 file being downloaded from the File page.

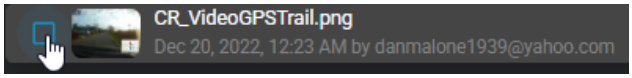


NOTE: If a malware scan flags a file as suspicious, then only users included in the *Download malicious files* security policy can download it. For more information on this security policy, refer to Security policy definitions list on page 47.

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 108

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

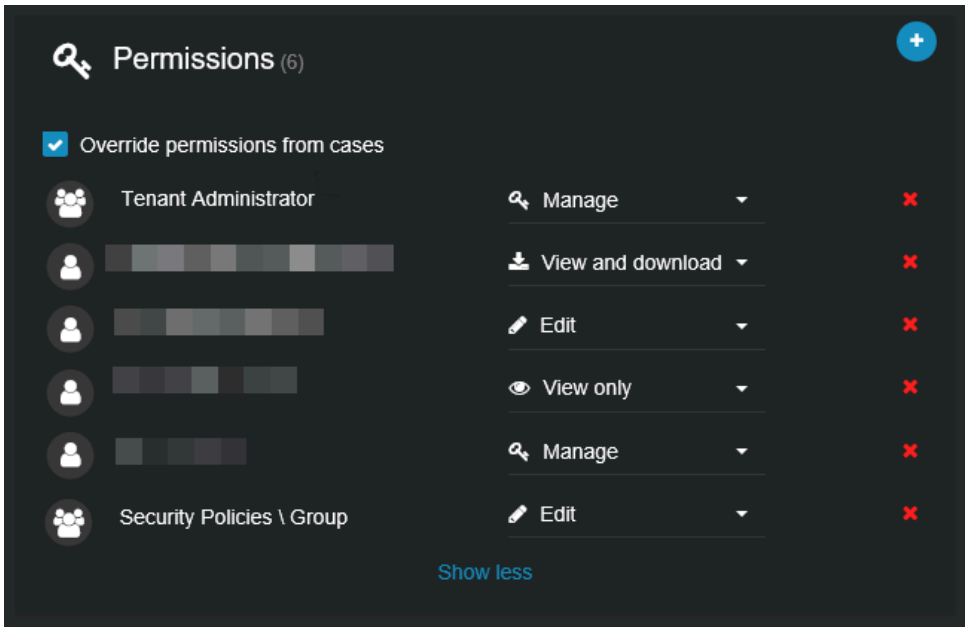
By default, a file inherits the access policy of the case with which it is associated. If a file is associated with multiple cases, user permission levels on the file are defined by the highest ranking permission level from those cases.

- 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**.



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 105

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.

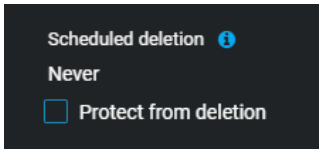
What you should know

- 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.



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.

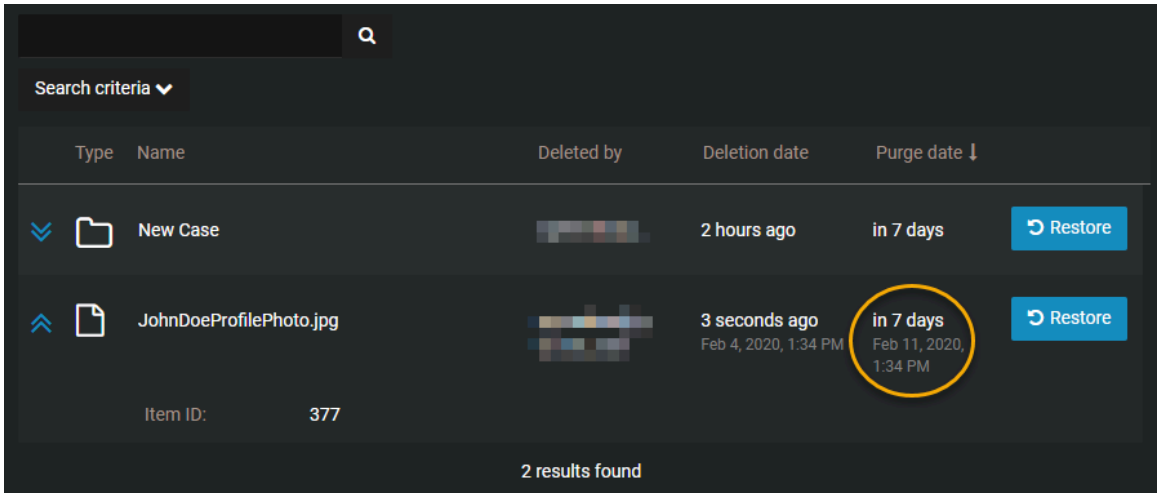
a) Clear the **Protect from deletion** check box.

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



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 AXIS Case Insight database.

Related Topics

Viewing the audit trail history of files on page 130

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.

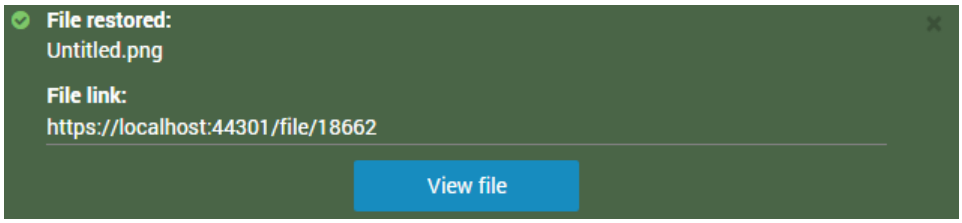
Procedure

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.



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

Related Topics

Viewing the audit trail history of files on page 130

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 AXIS Case Insight information security on page 104
Deleting files on page 127
Restoring files on page 129
Changing access policies for cases on page 82

9

Managing video editor content

Learn how to use the video editor.

This section includes the following topics:

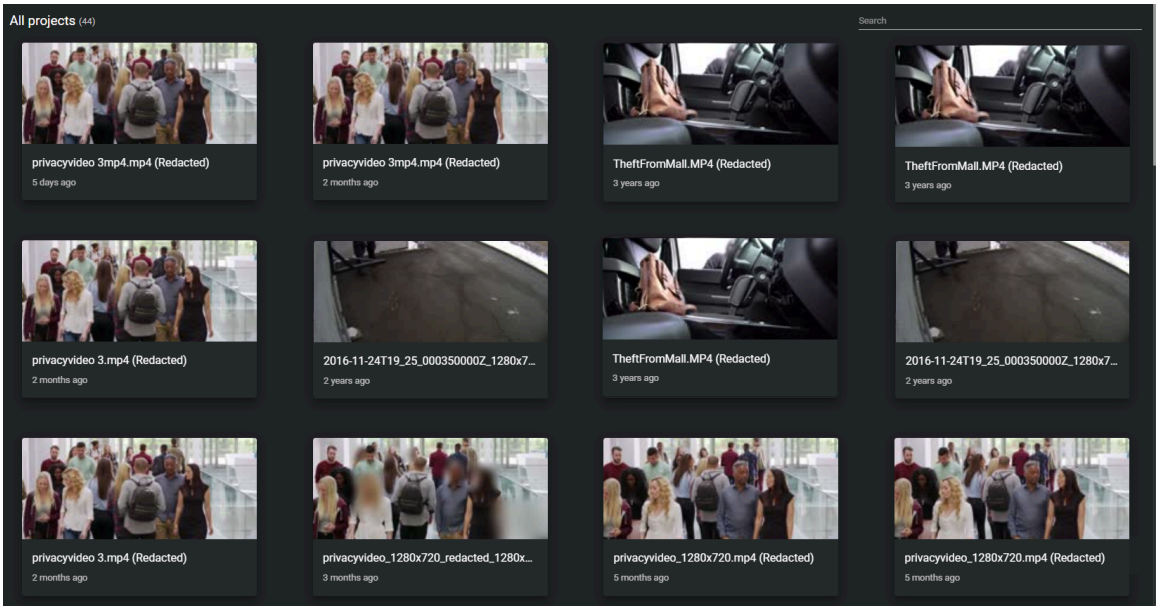
About the video editor

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 AXIS Case Insight 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.

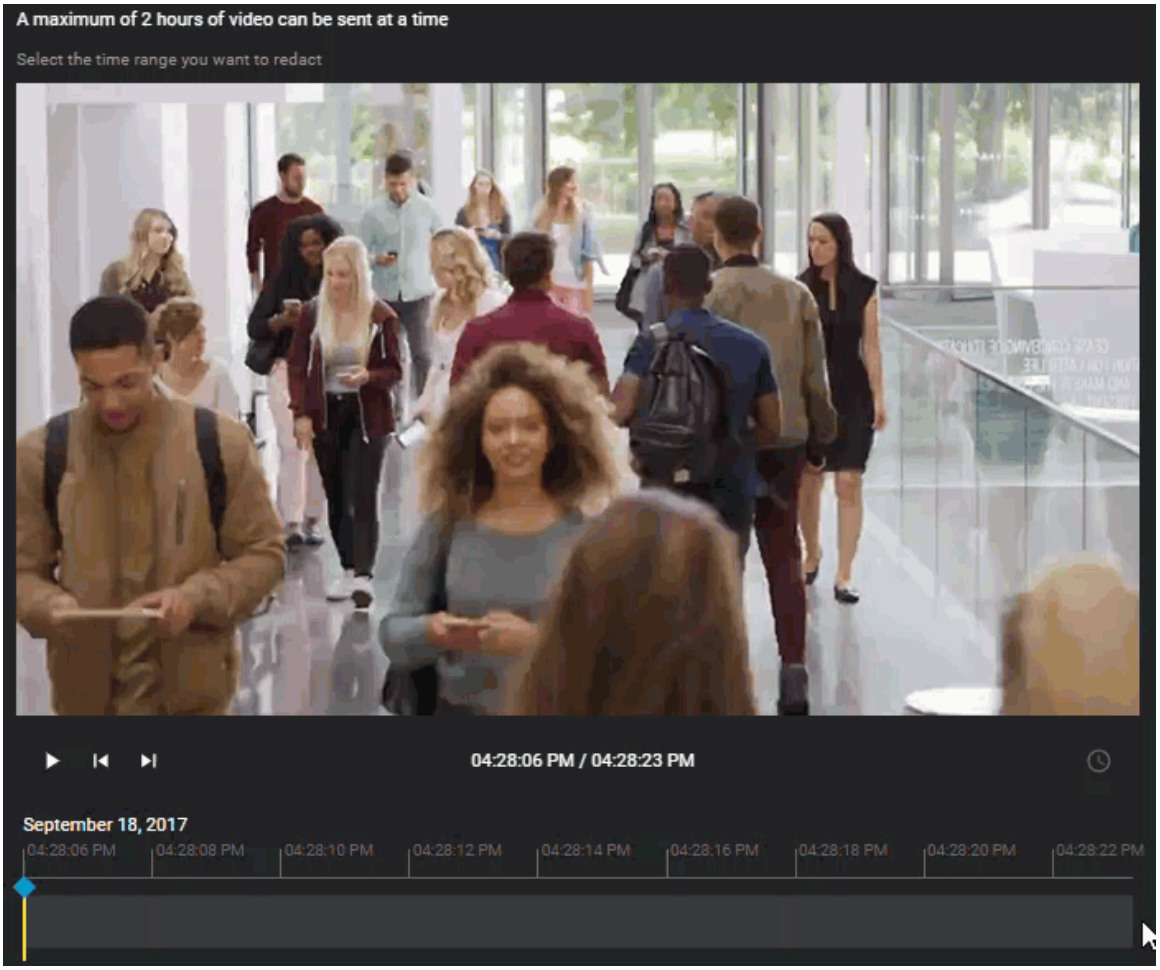
Video editor

- 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 AXIS Case Insight. Refer to the list of supported file formats for details.



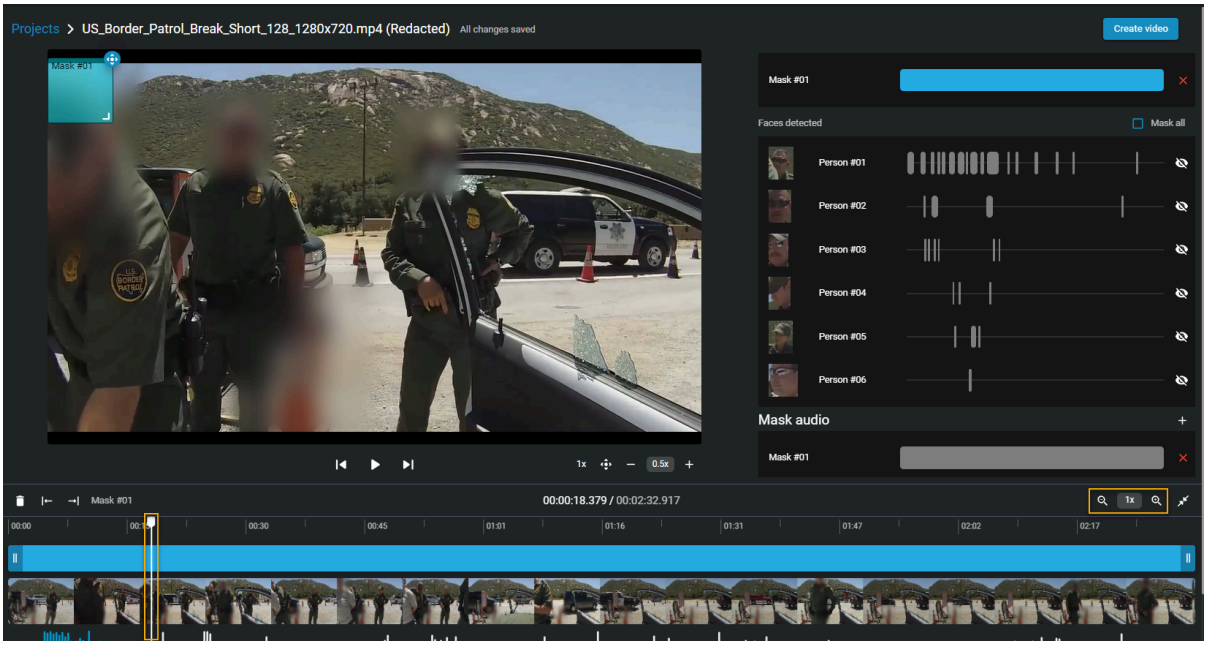
Trimming

- 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.



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 135
Redacting video in AXIS Case Insight on page 137
Redacting video manually in AXIS Case Insight on page 145
Redacting audio on page 151

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

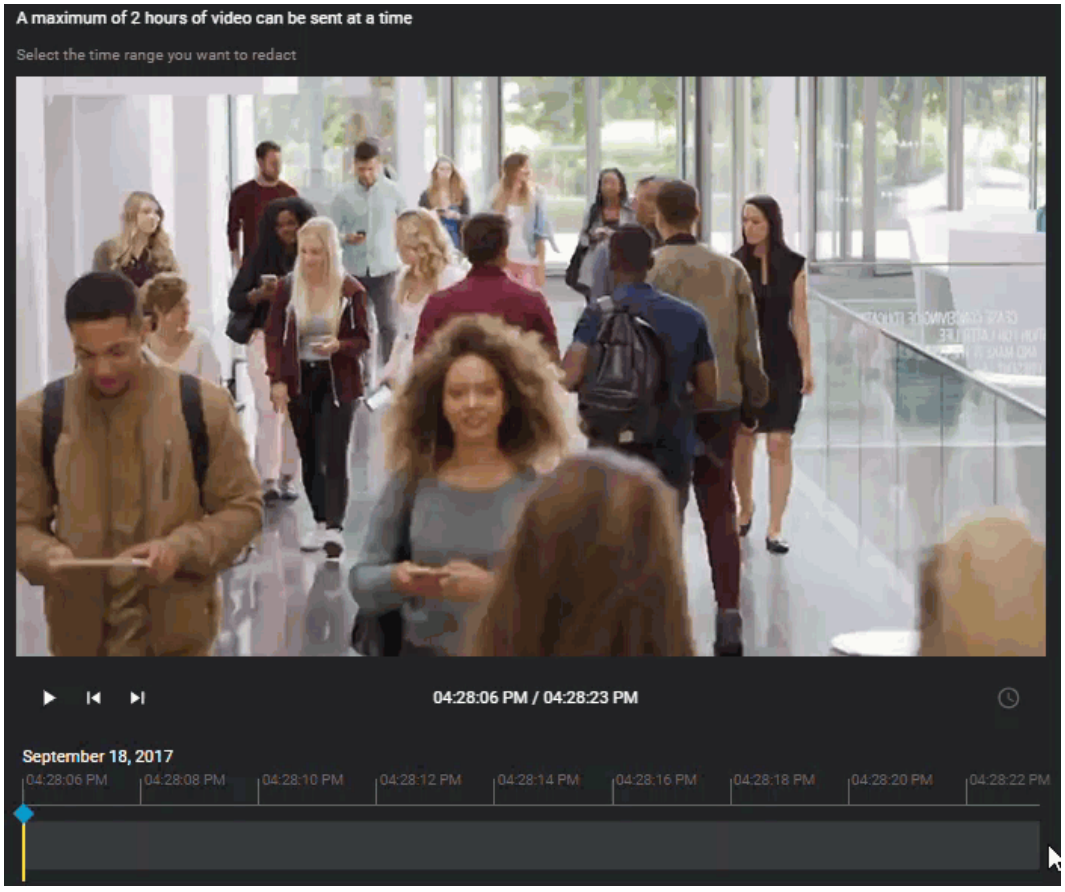
To trim a video:

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.



3 Click **Save to a case**.

The *Save to case* window opens.

4 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.

5 If you must associate the trimmed video with other cases, click **Add** ( ) and select the necessary cases.

6 (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.

7 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 AXIS Case Insight on page 137
  - Redacting video manually in AXIS Case Insight on page 145

Related Topics

About the video editor on page 132

Redacting video in AXIS Case Insight

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:

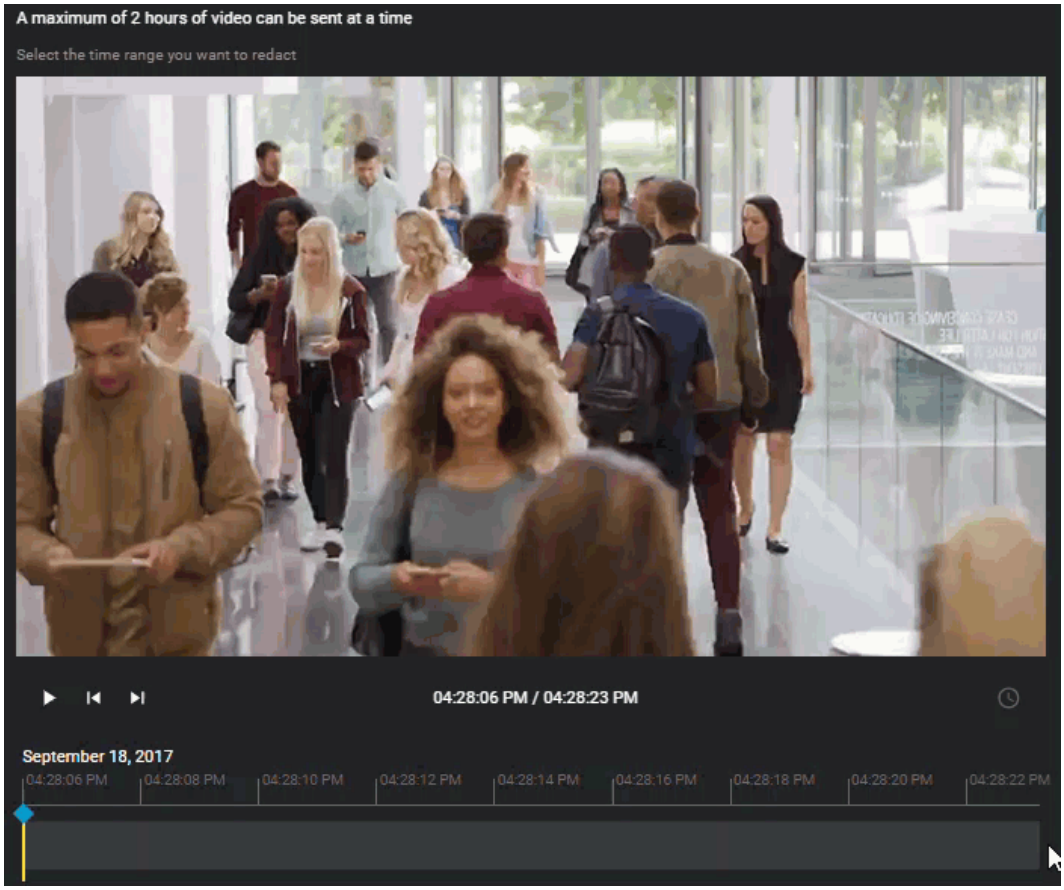
1 From a case, navigate to the file you want to redact, click **More** (⋮) in the **Files**, and then click **Trim and Redact**.

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.

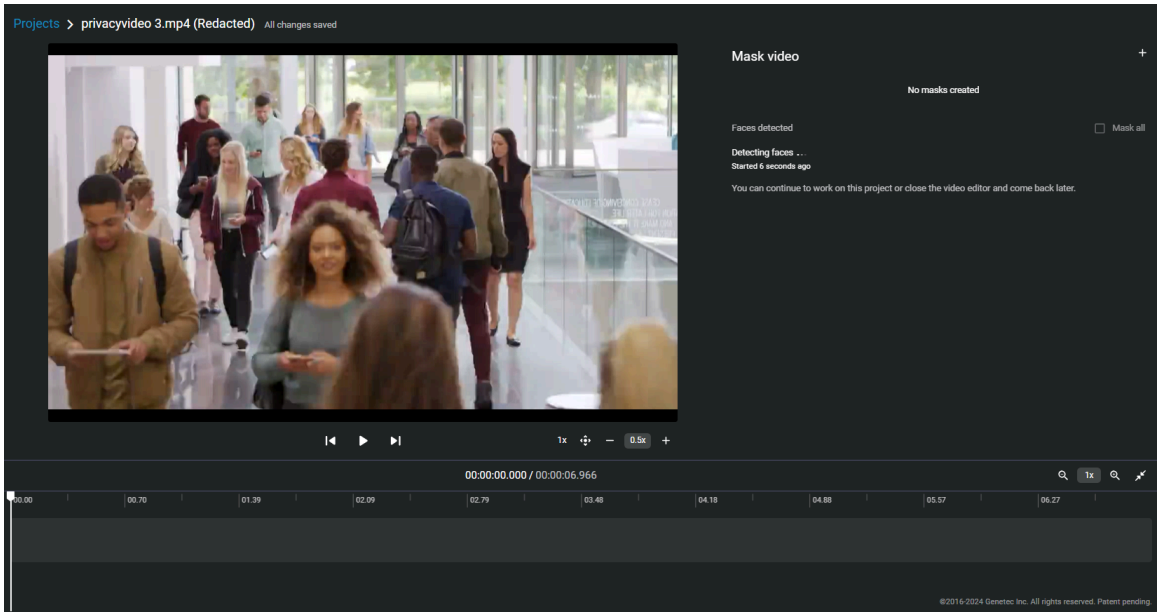
To trim a video file:

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.

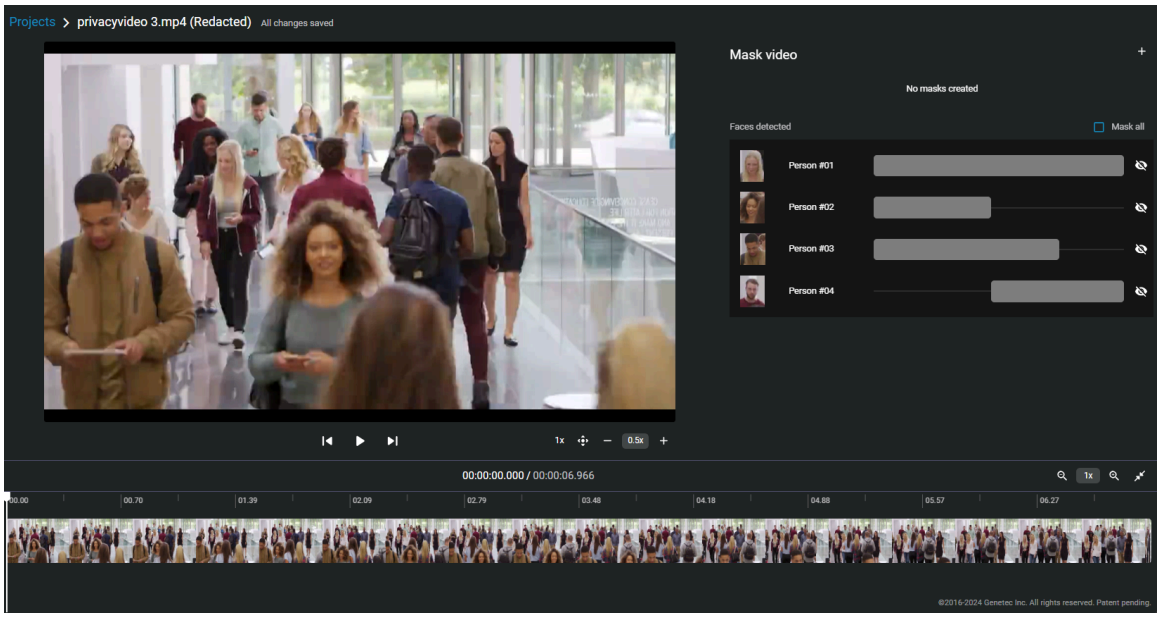


2 Click **Continue**.
The *Video editor* page opens.

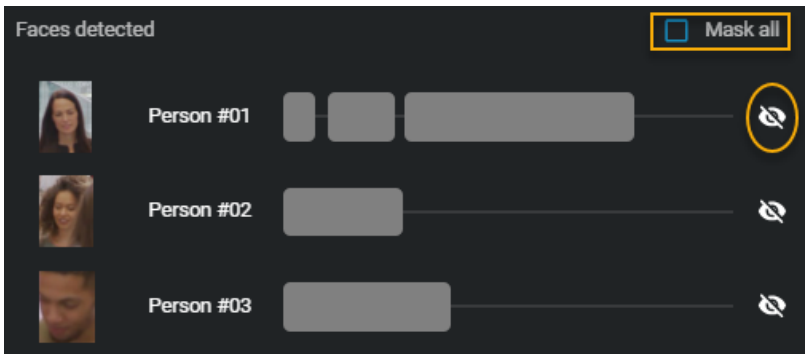
3 The face detection search begins automatically.



- 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.



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** ( ).

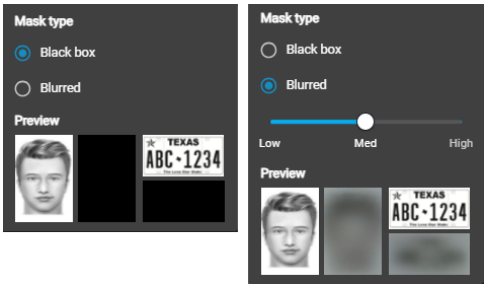
a) Use the timeline slider, zoom controls, or your mouse scroll wheel to position the timeline slider at the section of video that you want to redact.

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)

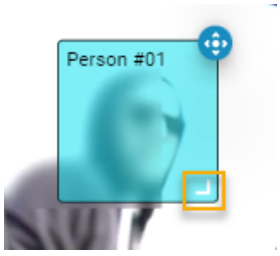
6 (Optional) Click **Mask settings** ( ) to specify the mask type that you require.

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.

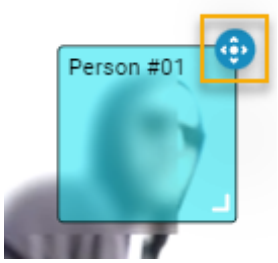


7 To resize the mask, use your mouse at the lower-right corner of the masking box.



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:

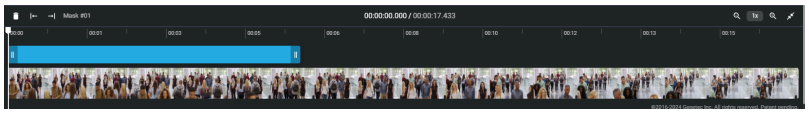
a) Next to the masking box on the video preview, click and hold the tracking button ( ).



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.

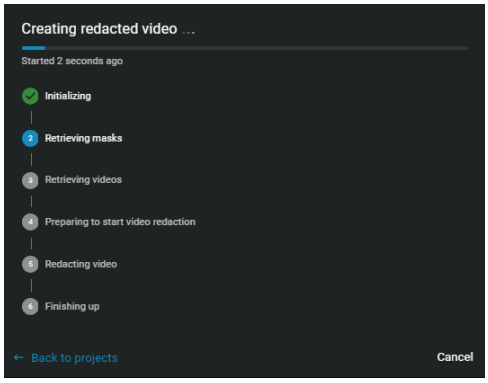
- Click delete ( ) in the mask list to remove any mask that you no longer require.
- Click **Delete mask** ( ) in the timeline controls to delete the currently selected mask.

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.



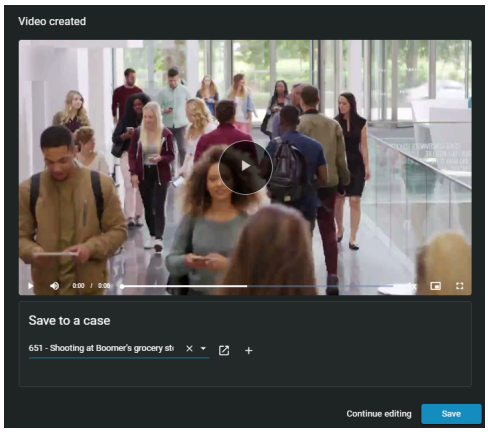
b) (Optional) Click **Back to projects** to close the progress dialog while redaction continues in the background.

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.

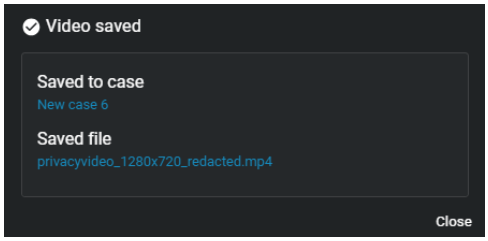
a) Enter a case ID or name in the Search field or click the menu to see a list.



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.

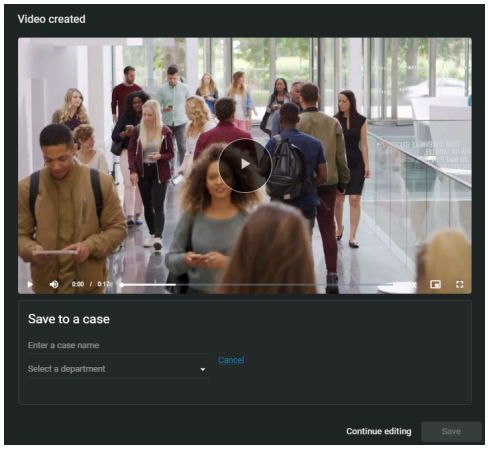


TIP: Click **View file** to change the file name before closing the dialog, so that others can easily find the file.

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**.



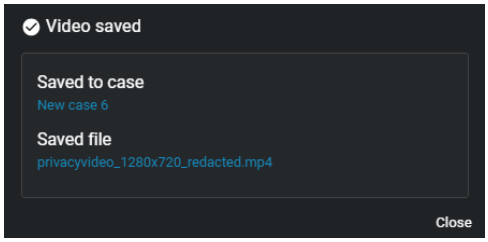
b) Enter a name for the new case.

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.



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 132

Redacting video manually in AXIS Case Insight

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:

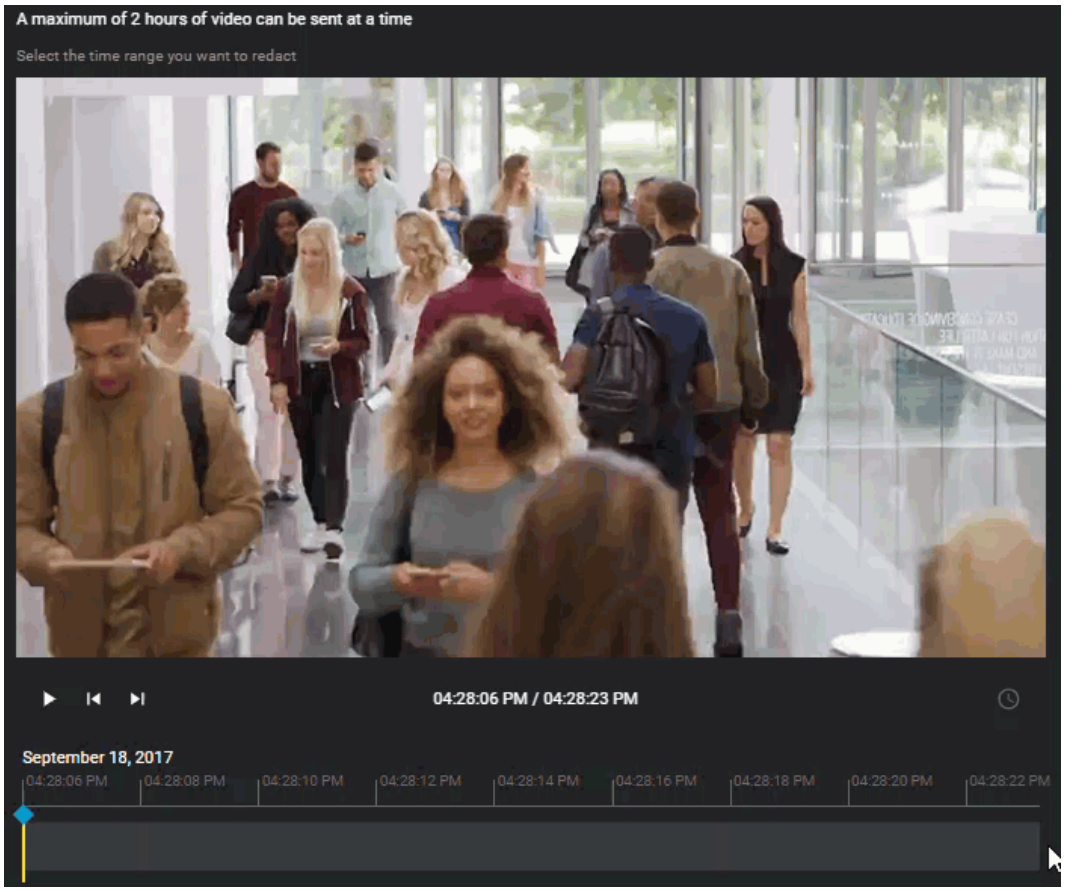
1 From a case, navigate to the file you want to redact, click **More** ( ) in the **Files**, and then click **Trim and Redact**.

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.



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.

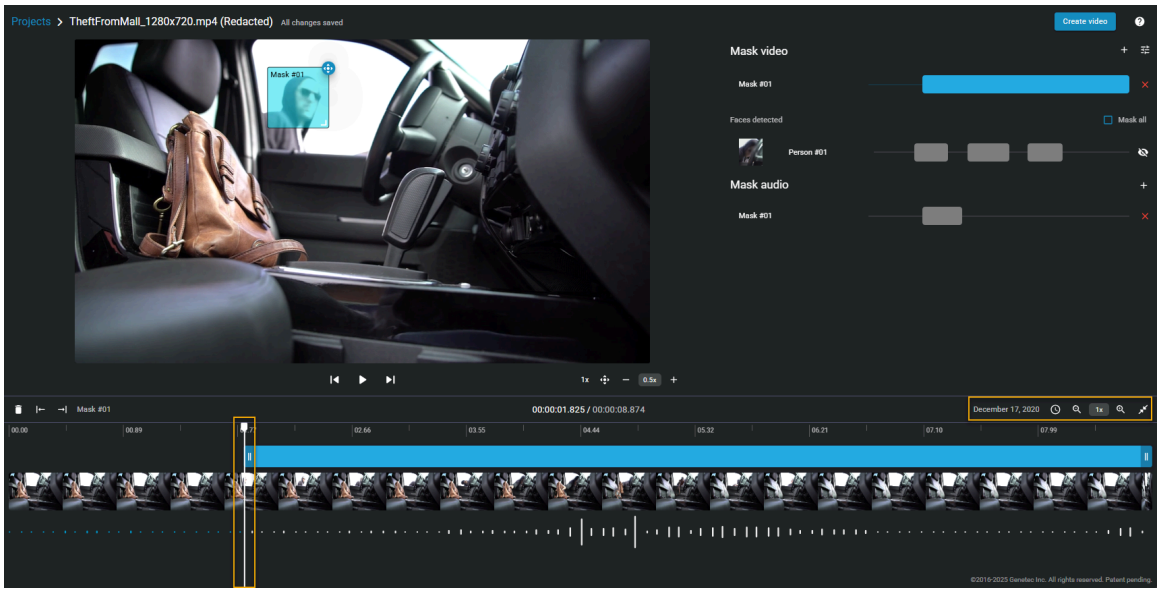
TIP: Use the thumbnail previews in the timeline to help identify the exact point in the video that you require. To zoom in or out on the timeline, click **Zoom in** or **Zoom out** (1x)

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** ( ).

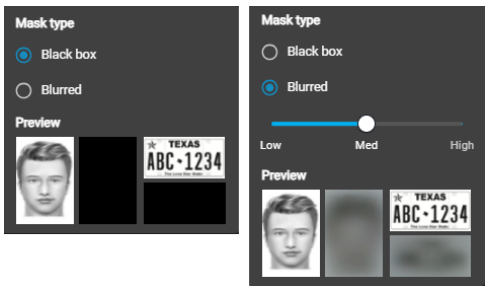
A mask layer is created on the video preview, and the duration of the mask is shown along the video timeline at the bottom of the video.



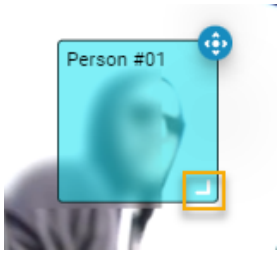
4 (Optional) Click **Mask settings** ( ) to specify the mask type that you require.

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.

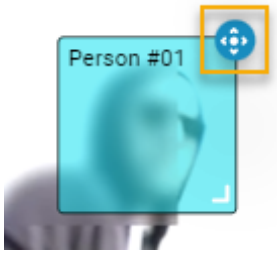


6 If the person or object you must redact is moving in the video scene, you can adjust the mask location using the tracking tool, as follows:

a) In the *Masking* pane, increase or decrease the **Tracking speed**.

You can select values in the range 0.1x to 10x.

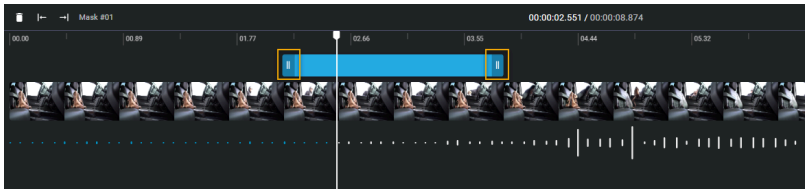
b) Next to the masking box on the video preview, click and hold the tracking button ( ).



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** ( ).

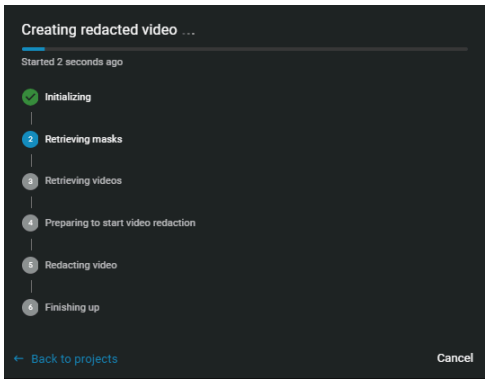
8 (Optional) Modify your masks if required.

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.



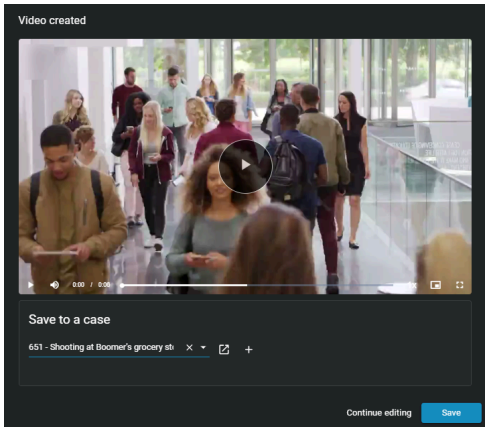
b) (Optional) Click **Back to projects** to close the progress dialog while redaction continues in the background.

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.

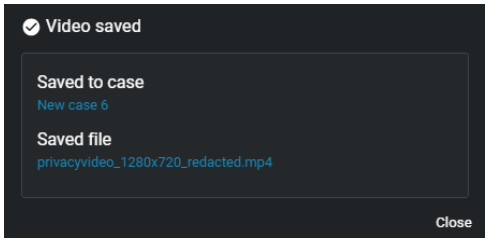
a) Enter a case ID or name in the Search field or click the menu to see a list.



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.

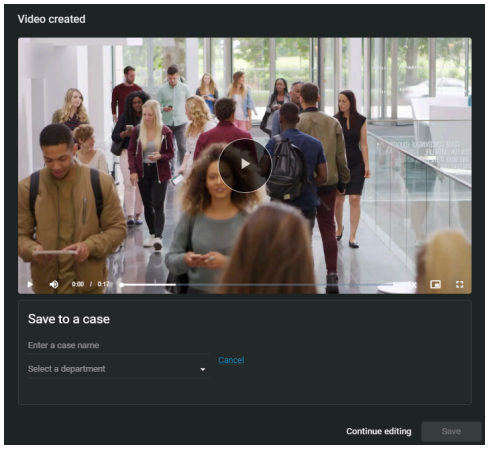


TIP: Click **View file** to change the file name before closing the dialog, so that others can easily find the file.

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**.



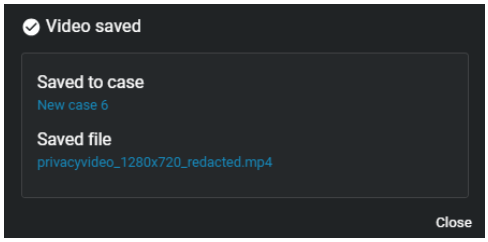
b) Enter a name for the new case.

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.



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 132

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.

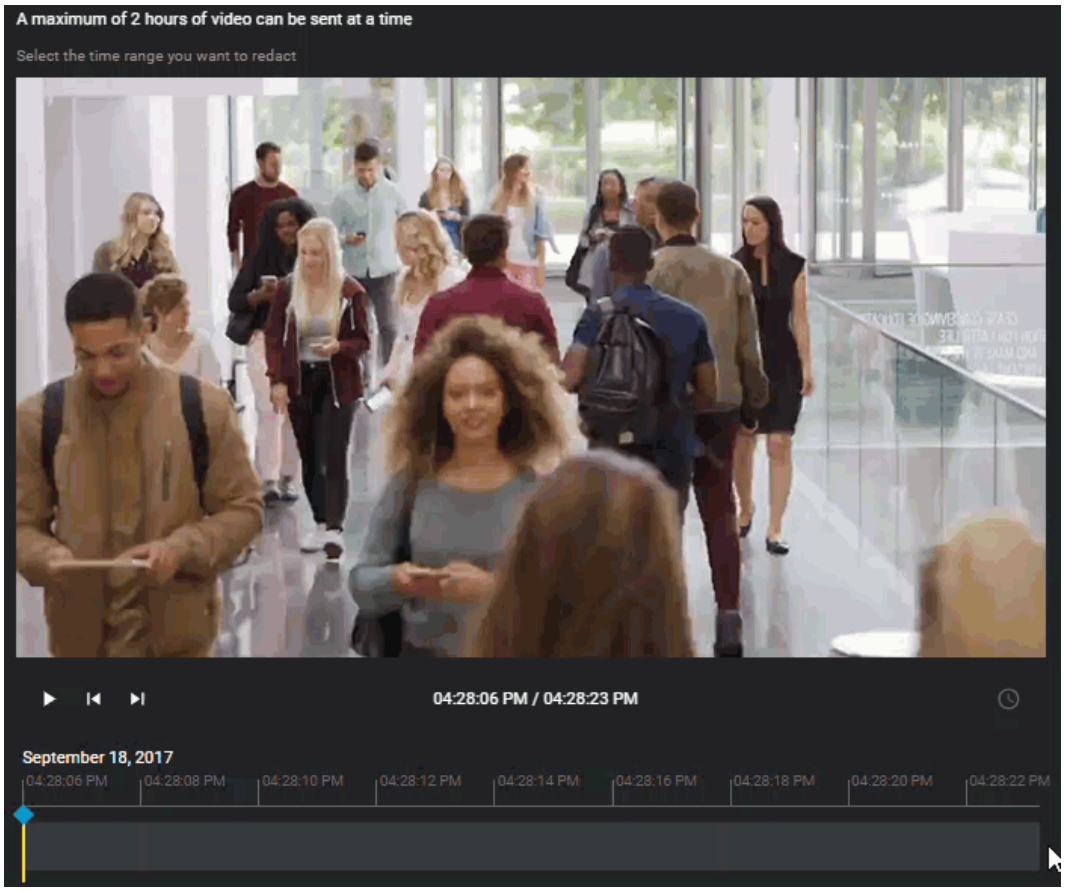
Procedure

1 From a case, navigate to the file you want to redact, click **More** ( ) in the **Files**, and then click **Trim and Redact**.

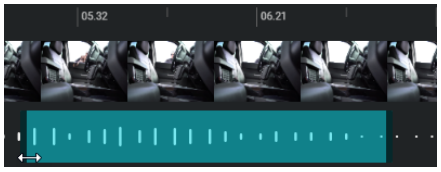
TIP: You can also start a redaction from the *File* page or from the *Evidence preview* window when previewing evidence in a case.

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.



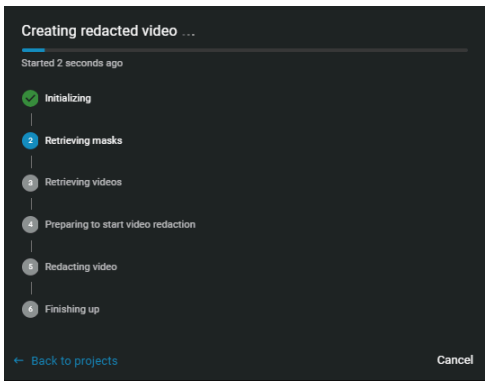
3 Click **New mask** ( ).
   a) To change the duration of the audio mask, adjust the start and end points of the mask in the timeline.



   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.



   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

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 132

10

Reviewing dashboards

Learn how use the dashboard in AXIS Case Insight.

This section includes the following topics:

About the AXIS Case Insight dashboard

You can use the AXIS Case Insight dashboard to track trends in your investigations and evaluate your subscription to ensure you get the most out of AXIS Case Insight.

The AXIS Case Insight 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.

Related Topics

Configuring the AXIS Case Insight dashboard on page 154

Configuring the AXIS Case Insight dashboard

After you have created some cases assigned them to the correct categories, you can configure the AXIS Case Insight dashboard.

What you should know

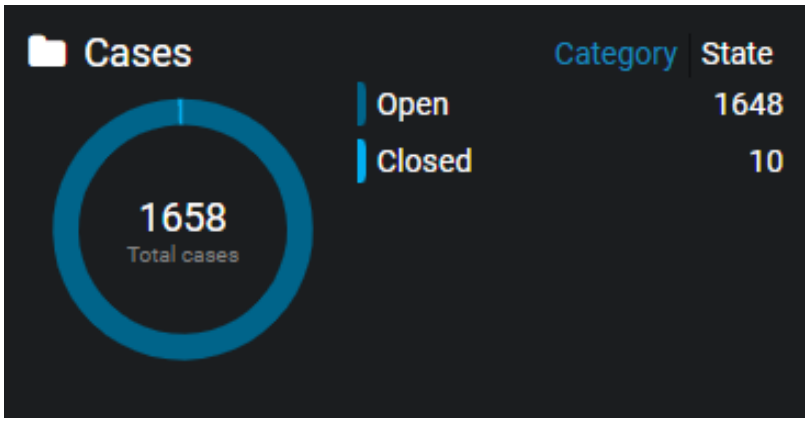
Only users included in the *View dashboard* security policy can configure the dashboard.

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.

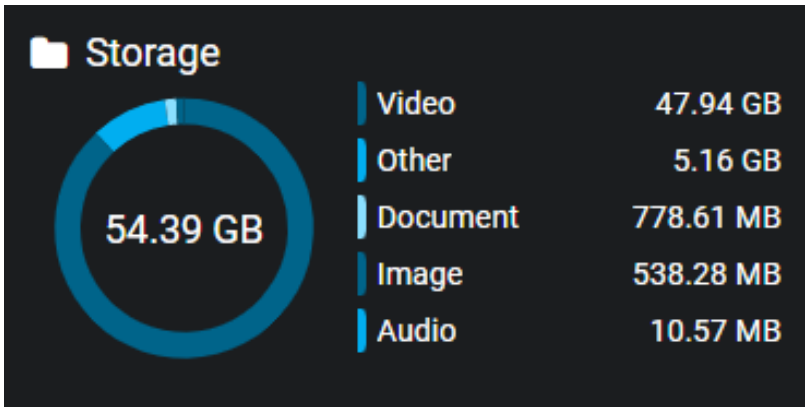
1 In the *Cases* section, examine the types and status' of investigations that your organization has handled using AXIS Case Insight. Organize total cases by:

- Category
- State



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



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

Historic section: Examine these statistics and filters give you a more detailed understanding of the data your organization has collected.

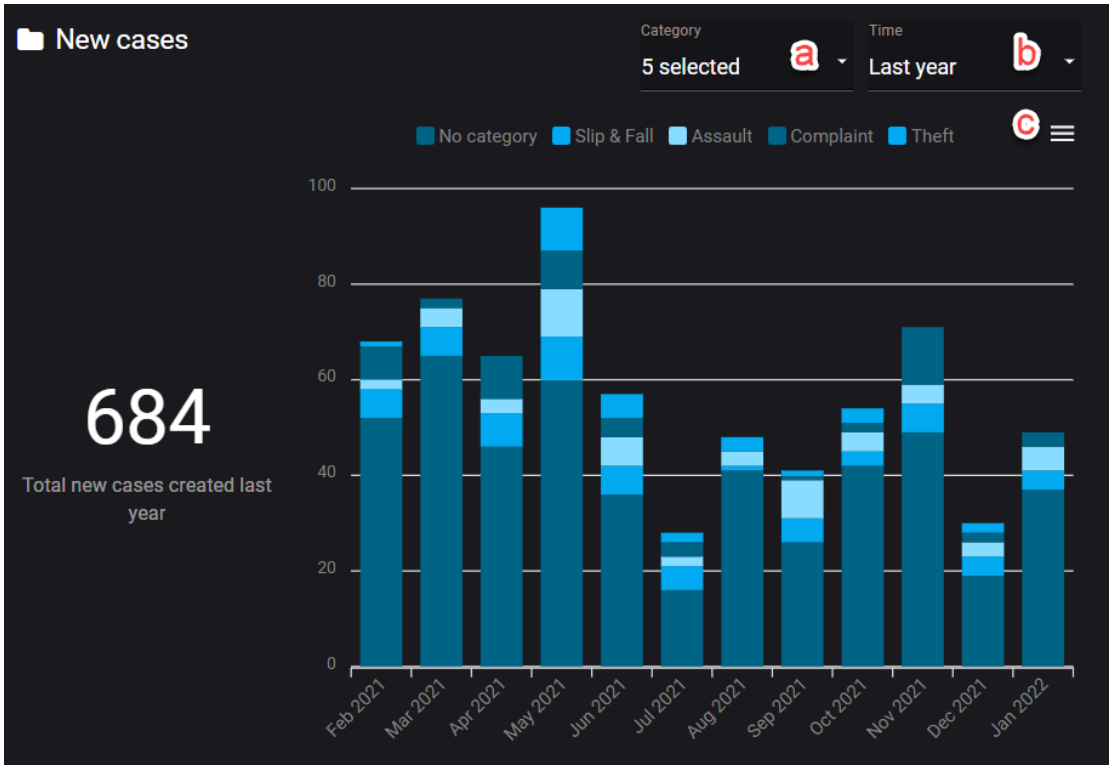
1 In the *New cases* section, gain insights into the number and types of investigations that were created over a configurable time period. Use this to identify trends over time related to different incident categories, or to assist with resource allocation for future cases. Configure the following in 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 AXIS Case Insight account.

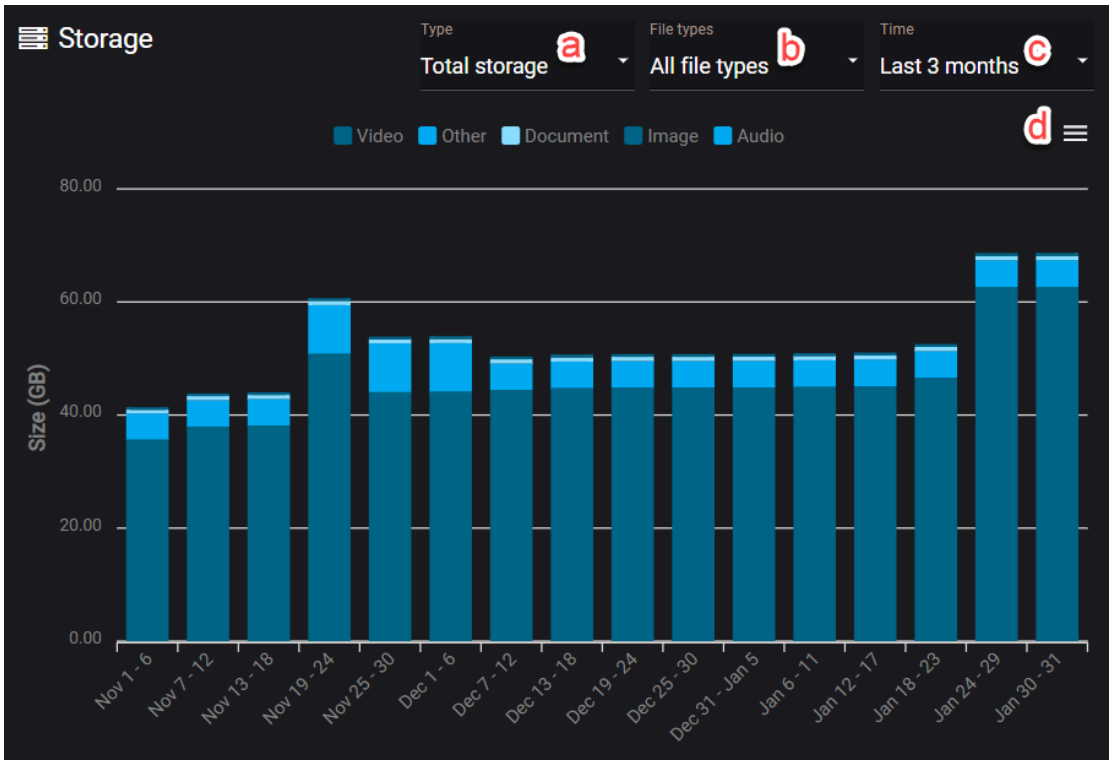
c) Optional: If you want to download the data, click **Download** ( ) and select a file type.



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.



Related Topics

About the AXIS Case Insight dashboard on page 154

11

Public upload requests

Invite anyone to add files to an incident without viewing the case contents in AXIS Case Insight.

This section includes the following topics:

Sharing files using a file request

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

Before you begin

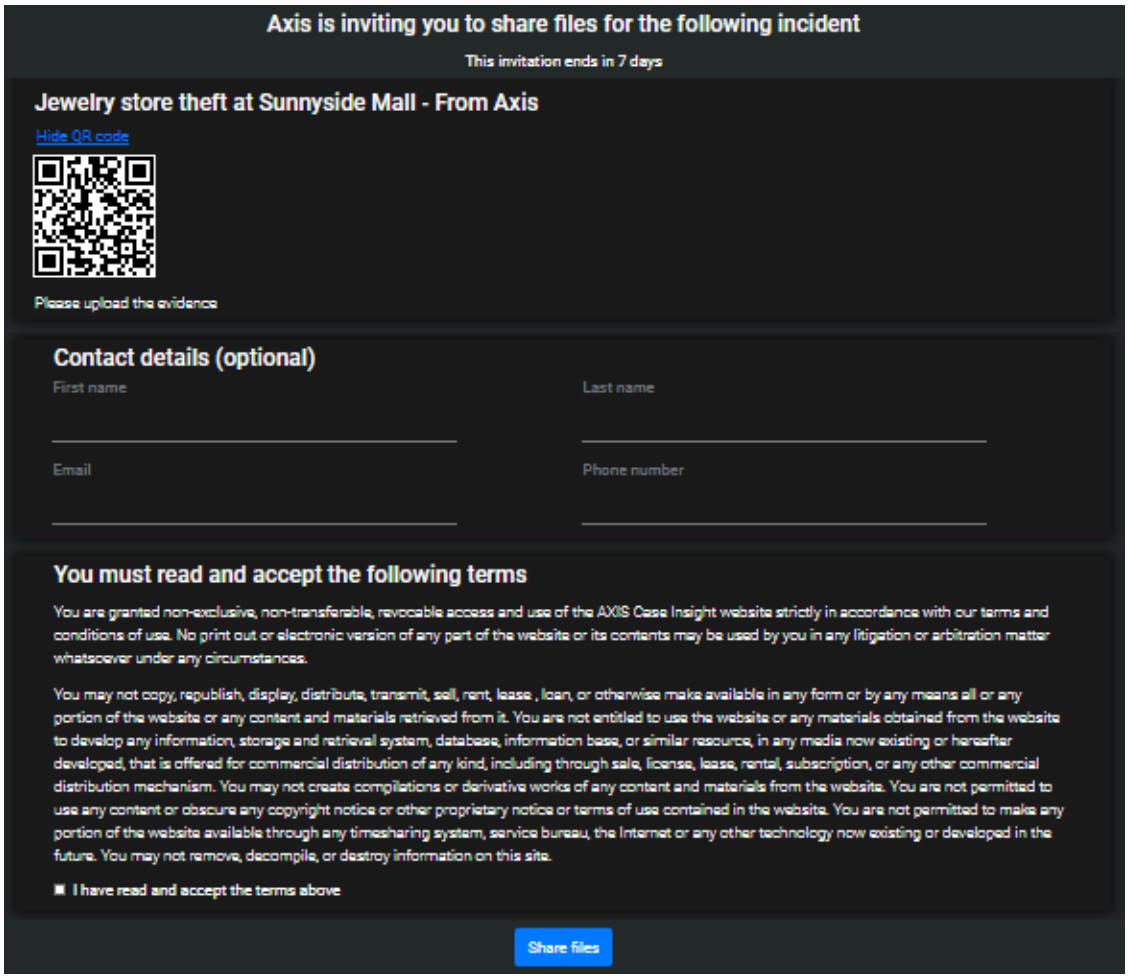
Ensure that you have received a file request containing a file request link that you can use to submit files.

What you should know

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

Procedure

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



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

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

a) Enter a **First name**.

b) Enter a **Last name**.

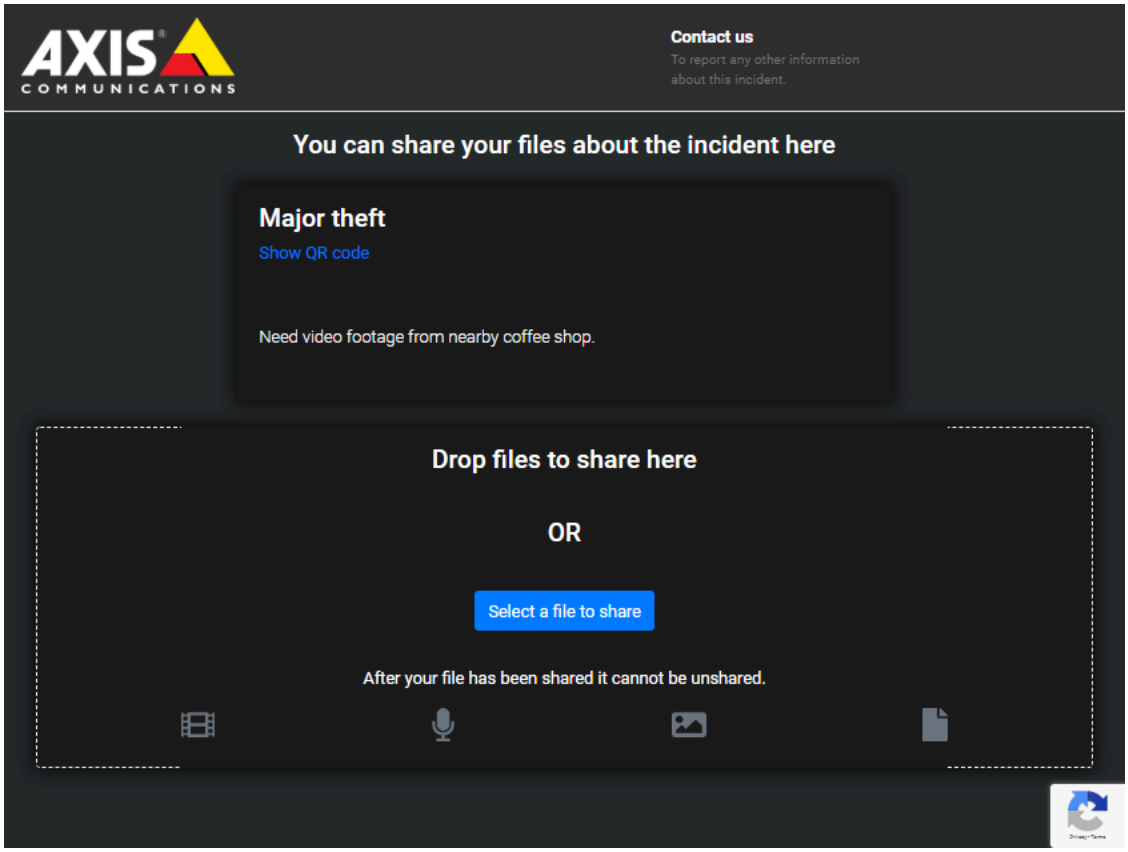
c) Enter an **Email address**.

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

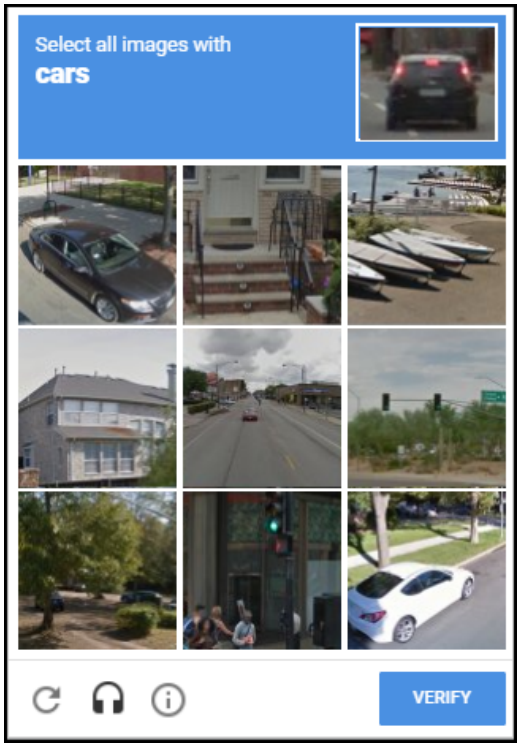
3 Read the file request terms.

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

4 Click **Share files**.

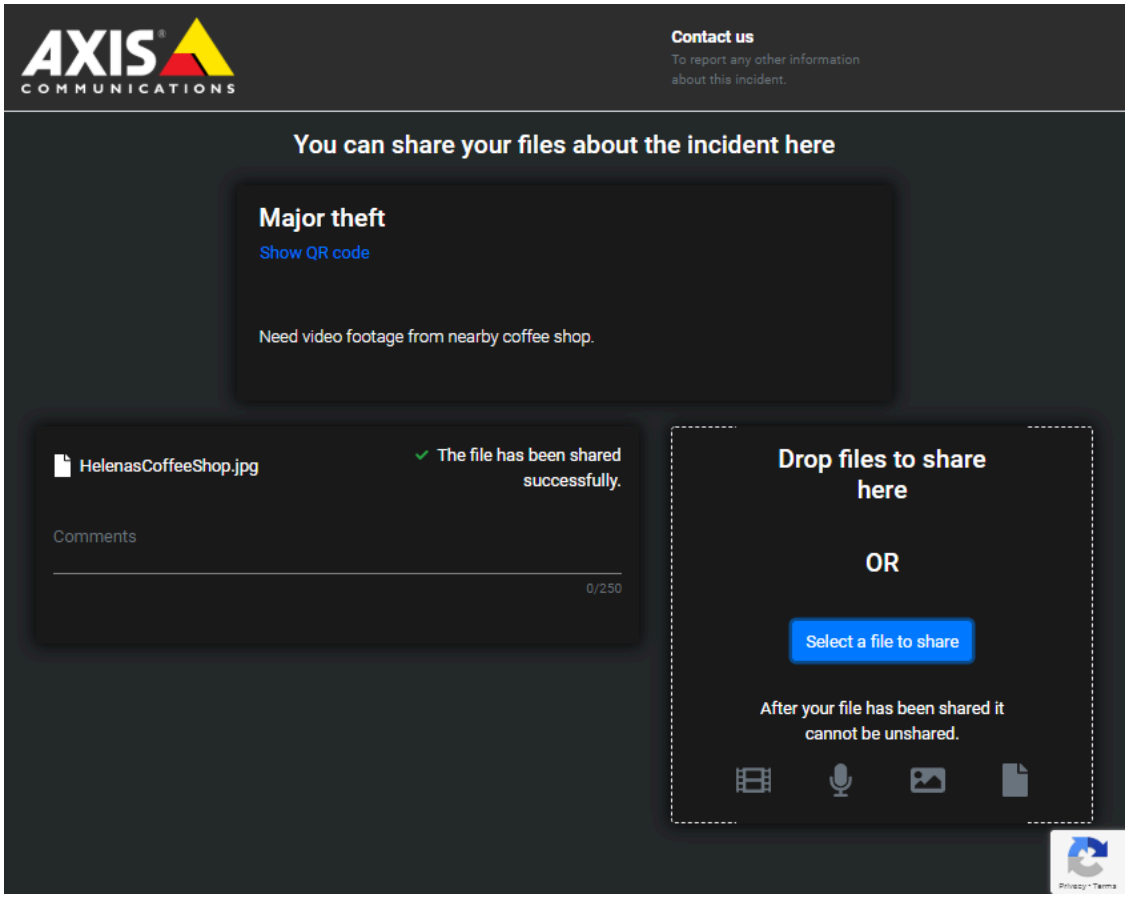


5 Drag and drop one or more files or click **Select a file to share**.



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

The shared file is immediately added to the case.


AXIS COMMUNICATIONS
Contact us
To report any other information about this incident.
You can share your files about the incident here
Major theft
Show QR code
Need video footage from nearby coffee shop.
HelenasCoffeeShop.jpg
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.

12

Frequently asked questions

Learn about common issues in AXIS Case Insight.

This section includes the following topics:

How can I create a bookmark to my AXIS Case Insight account?

If you encounter an error when you navigate to your bookmarked AXIS Case Insight 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.

Solution

Delete all bookmarked AXIS Case Insight pages that cause an error. Select the required host as detailed in your account activation email and bookmark it.

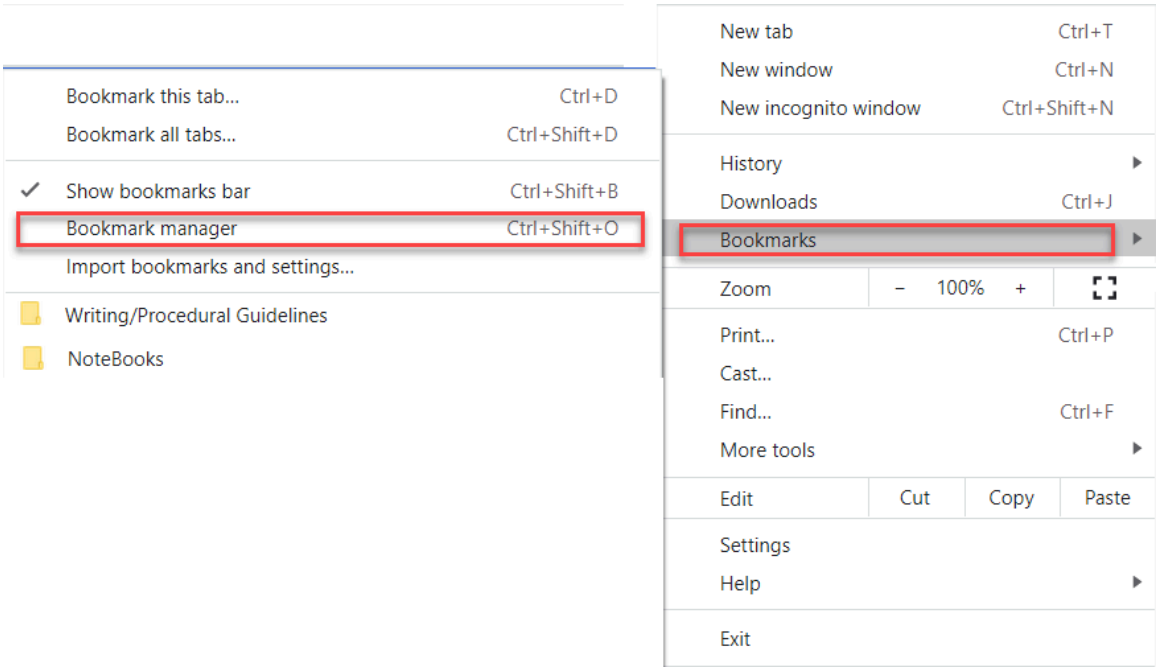
NOTE: The hostname displayed before the account ID in your account URL will vary depending on the region where your account is hosted.

Host list by region

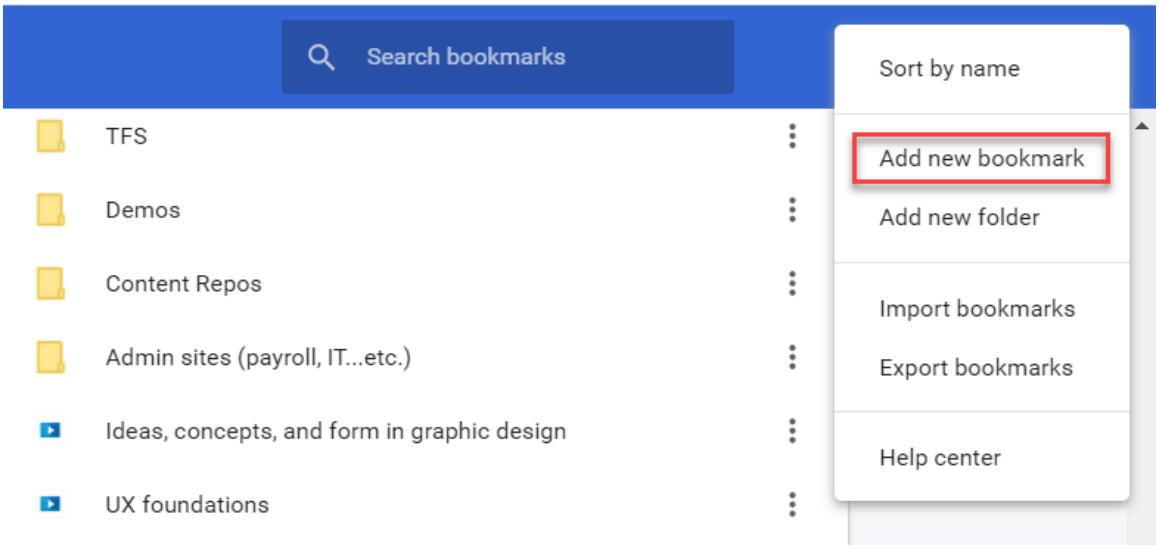
Region	Host
United States	https://us.caseinsight.axis.com
Europe	https://eu.caseinsight.axis.com
Australia	https://au.caseinsight.axis.com
US Government	https://usgov.caseinsight.axis.com
Canada	https://ca.caseinsight.axis.com

Bookmarking using Google Chrome

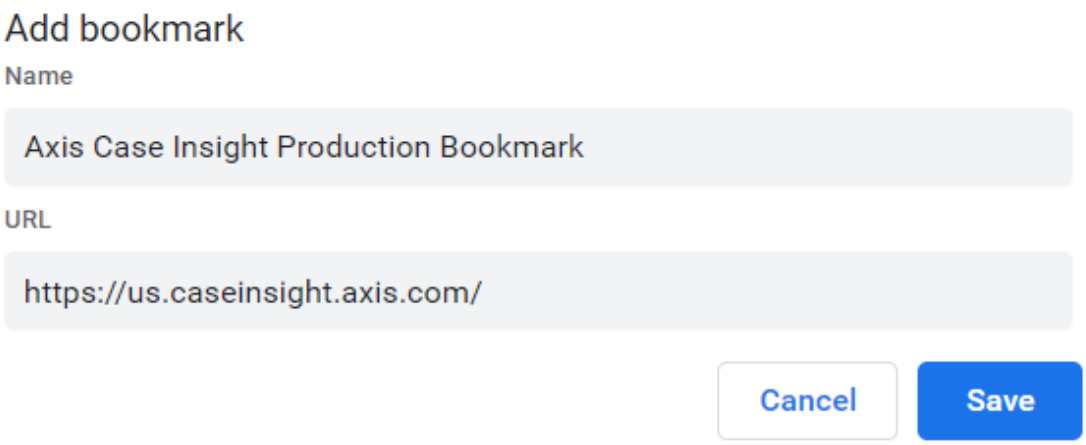
1. Open Google Chrome and, in the top right of the browser window, click **More** (⋮) to open the menu.



2. From the menu, hover over **Bookmarks** and click **Bookmark manager**.



3. From the bookmark manager page, select the three dots in the top right of the browser window and click **Add new bookmark**.



4. Add the host you need and save the bookmark.

Why is a preview of a PDF not displayed in AXIS Case Insight?

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.

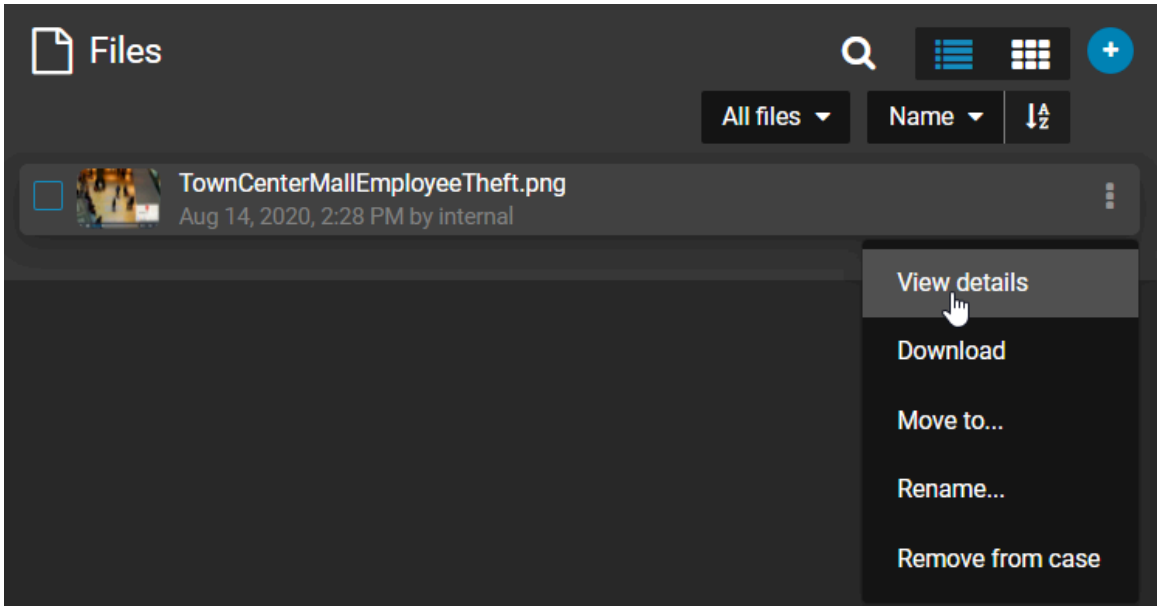
Cause

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.

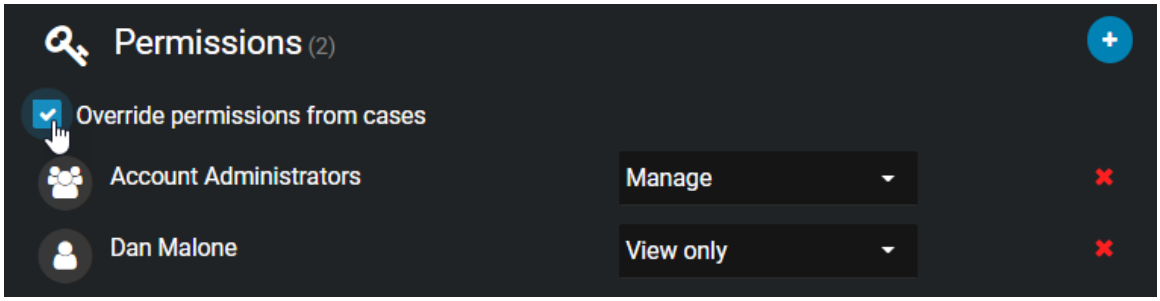
Solution

Give the user who needs to see the PDF **View and download** permission in the related case.

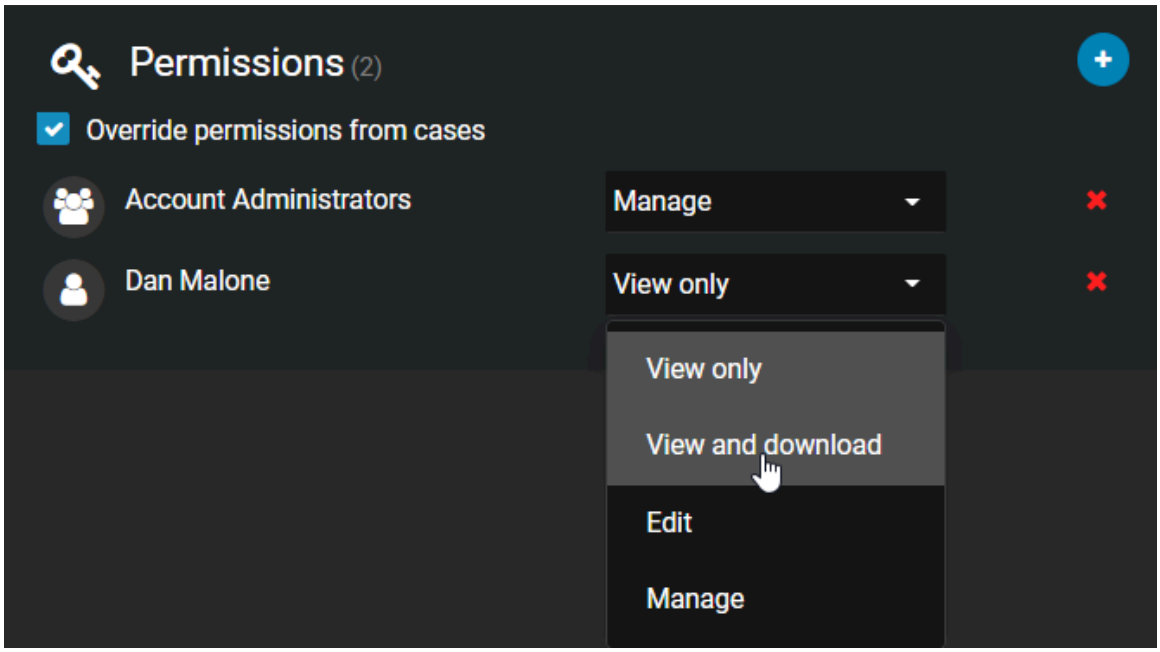
1. Select your case of choice.
2. Select the file you need the user to view and click **More** ( ).
3. Click **View details**.



4. Select **Override permissions from cases**.



5. Change the permission from **View only** to **View and download** on the PDF file you want the recipients to view and click **Save**.



NOTE: All other files on the case remain **View only**, except for the specific ones you modify.

Glossary

absolute time

In AXIS Case Insight, 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 AXIS Case Insight account.

account

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

Account Administrator

The Account Administrator in AXIS Case Insight 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.

AXIS Body Worn Manager

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

AXIS Case Insight

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

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 AXIS Case Insight 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 AXIS Case Insight are used to classify cases. Each category defines an incident type and a retention policy.

department

A department in AXIS Case Insight 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 AXIS Case Insight, 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 AXIS Case Insight, 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 AXIS Case Insight 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.

group

A group in AXIS Case Insight 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 AXIS Case Insight is an external device or application that is authorized to transfer data to the AXIS Case Insight account.

permission level

Permission levels in AXIS Case Insight 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 AXIS Case Insight is the act of obscuring faces, audio, or other sensitive information from supported video files.

relative time

In AXIS Case Insight, 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.

retention policy

A retention policy in AXIS Case Insight 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 AXIS Case Insight defines which users and groups have access to a particular system feature.

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 AXIS Case Insight 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.

visual watermarking

Visual watermarks add a transparent overlay to videos and images in AXIS Case Insight. 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.