March Networks

Command 2.18
Central Evidence Archive

USER GUIDE

MARCH networks
A Delta Group Company

North America	1 800 563 5564
Latin America	+52 55 5259 9511
Europe	+39 0362 17935
Asia	+65 6818 0963
Australia and New Zealand	+61 1300 089 419
Middle East and Africa	+971 04 399 5525

www.marchnetworks.com

Notice of Rights

Part Number

41653 Rev 1.0, November 2023

Contents

Chapter 1: Installing the Central Evidence Archive.................................. 4
Additional Documentation 5
Adding the License for the Central Evidence Archive 6
Adding the Central Evidence Archive Component.. 8
Advanced Settings in the Enterprise Console 10
Adding the Central Evidence Archive Application Rights to the User Profile 12
Access to the Central Evidence Archive.. 16
Upgrading the Central Evidence Archive Component 18

Chapter 2: Configuring the Central Evidence Archive 20
Overview 21
Configuring General Settings for the Central Evidence Archive.. 24
Configuring Triggered Tags.. 27
Configuring Scheduled Backups 31
Configuring Time Ranges 35

Chapter 3: Managing Tag, Case, and Backup Files................................ 37
Managing Tag Files.. 38
Searching for Tag Files using the Central Evidence Archive 38
Deleting a Tag File using the Central Evidence Archive 40
Managing Case Files.. 41
Searching for Case Files using the Central Evidence Archive... 41
Deleting a Case File using the Central Evidence Archive... 43
Managing Backup Files 44
Searching for Backup Files.. 44
Reviewing a Backup File... 46
Exporting a Backup File 49
Sharing a Backup File with Other Users.. 52
Changing the Owner of a Backup File.. 53
Converting a Backup File to a Case File... 54
Deleting a Backup File.. 55
Adding a Label to a Tag, Case, or Backup 56

Chapter 1

Installing the Central Evidence Archive

March Networks Central Evidence Archive is an application that when added to the Command Enterprise solution, allows you to create event-triggered video tags and automatic backups, and provides an overview and management interface for your video tags, cases, and backups. Video from tags, cases, and backups is exported from recorders and archived so that it is available for review.

Note: Your Command Enterprise solution requires a Command Media Archiver to store data for the Central Evidence Archive. For information on installing the Command Media Archiver, see the *Command Enterprise Installation Guide*.

For more information on the Command Solution, see the user guides and documentation available for download from the March Networks Partner Portal website.

This chapter describes how to install the Central Evidence Archive.
It contains the following topics:

- “Additional Documentation” on page 5
- “Adding the License for the Central Evidence Archive” on page 6
- “Adding the Central Evidence Archive Component” on page 8
- “Advanced Settings in the Enterprise Console” on page 10
- “Adding the Central Evidence Archive Application Rights to the User Profile” on page 12
- “Access to the Central Evidence Archive” on page 16
- “Upgrading the Central Evidence Archive Component” on page 18

Additional Documentation

The following table describes where to find more information on the interface that you are interested in. All the user guides are available for download from the March Networks Partner Portal website.

Interface	Purpose and Applicable Recorders	User Guide
Command Enterprise	You access Command Enterprise and the Central Evidence Archive using the Command Client interface. When Command Client is connected to Enterprise, you can view live and archive video, manage, and export video from multiple RideSafe Series recorders. When Command Client is connected to a single recorder, you can view live and archive video, manage, and export video from that recorder only.	*Command Enterprise and Client User Guide* *Command Enterprise Installation Guide*
Command Player	View exported video, snapshots, and notes from recorders.	*Command Player User Guide*
Command Config	Configure R6 recorders.	*<Recorder name> Configuration Guide*
Administrator Console	Configure R5 recorders.	*Administrator Console User Manual for Transit Recorders*

Adding the License for the Central Evidence Archive

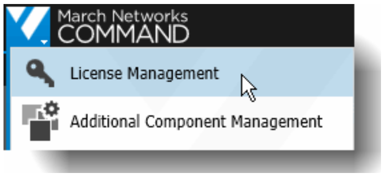
The Central Evidence Archive application requires a license to run it. In Command Enterprise, the **Additional Components** subtab of the **Licensing** tab allows you to add licenses for custom applications added to Command.

You can acquire your Central Evidence Archive license (an .xml file) from your March Networks representative or Customer Support. The Central Evidence Archive license is recorder based, you must add the license, then identify the recorders you want to use with the Central Evidence Archive.

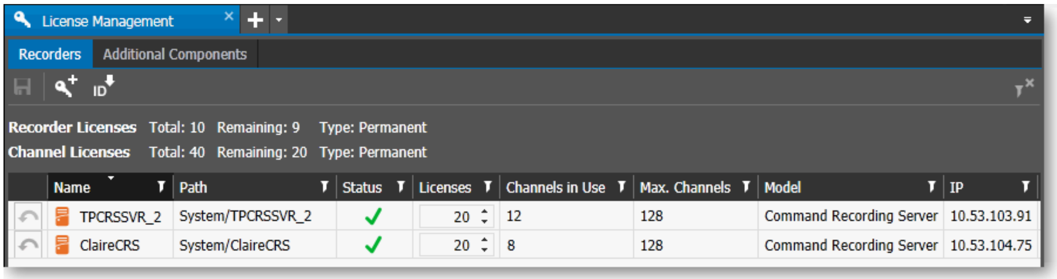
Important: You can only license R6 recorders (X-Series) or CRSs with the Central Evidence Archive. R5 recorders (8000, 9000 series) are not supported.

To add the Central Evidence Archive license to Command

1 Click the main menu and select **License Management**.



The **License Management** tab opens.

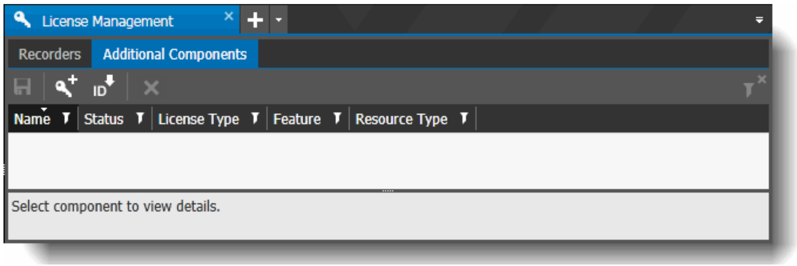


Recorder Licenses Total: 10 Remaining: 9 Type: Permanent
Channel Licenses Total: 40 Remaining: 20 Type: Permanent

Name	Path	Status	Licenses	Channels in Use	Max. Channels	Model	IP
TPCRSSVR_2	System/TPCRSSVR_2	✓	20	12	128	Command Recording Server	10.53.103.91
ClaireCRS	System/ClaireCRS	✓	20	8	128	Command Recording Server	10.53.104.75

2 Click the **Additional Components** subtab.

The **Additional Components** subtab opens.



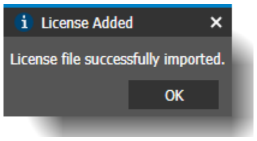
Name	Status	License Type	Feature	Resource Type

Select component to view details.

3 To import/enable the new license, click the **Add License** button.

4 Locate and select the license.xml file and click **Open**.

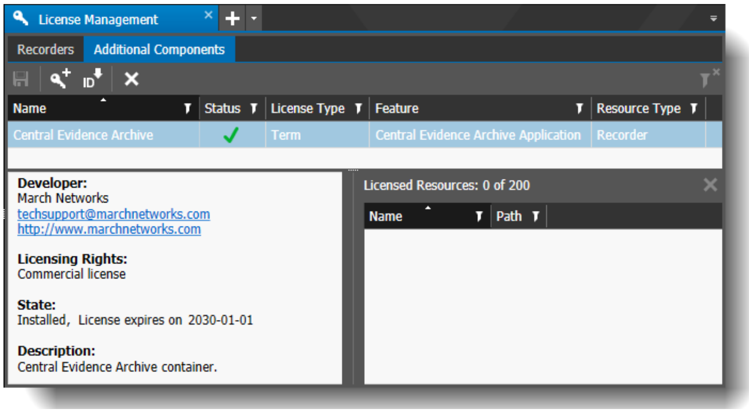
The **License Added** dialog box appears, indicating the license is applied to Command.



License file successfully imported.

5 Click **OK**.

The details of the license are added to the list. An empty **Licensed Resources** list is available.



Name	Status	License Type	Feature	Resource Type
Central Evidence Archive	✓	Term	Central Evidence Archive Application	Recorder

Developer:
March Networks
techsupport@marchnetworks.com
http://www.marchnetworks.com

Licensing Rights:
Commercial license

State:
Installed, License expires on 2030-01-01

Description:
Central Evidence Archive container.

Licensed Resources: 0 of 200

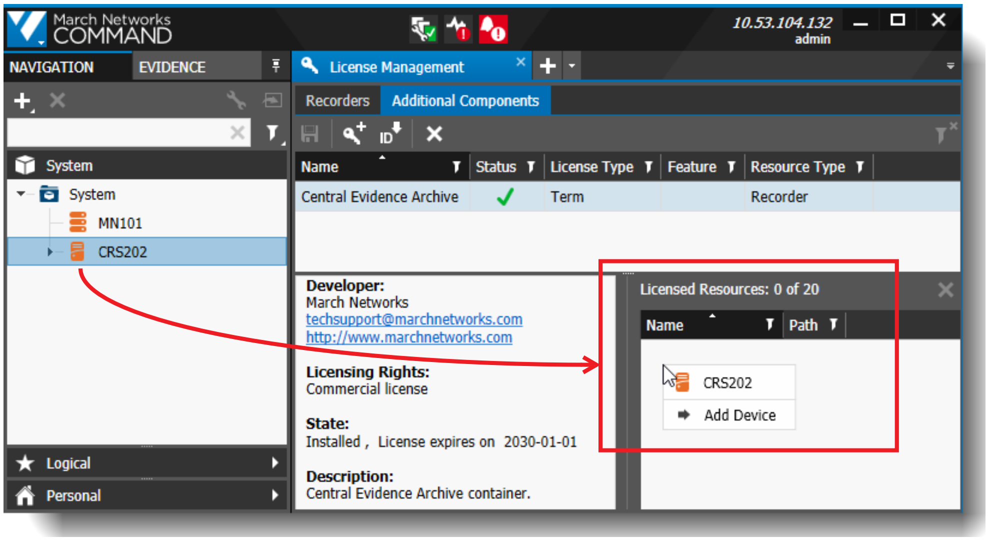
Name	Path

Note: If the license failed to import, an error message appears, indicating the reason for the failure.

6 You must add any recorders you want to use with the Central Evidence Archive application to the Licensed Resources list area.

Drag and drop recorders from the Navigation panel's **System** tree to the **Licensed Resources** area.

I**mportant:** You can only add R6 recorders (X-Series) or CRSs with the Central Evidence Archive. R5 recorders (8000, 9000 series) are not supported.



Name	Status	License Type	Feature	Resource Type
Central Evidence Archive	✓	Term		Recorder

Developer:
March Networks
techsupport@marchnetworks.com
http://www.marchnetworks.com

Licensing Rights:
Commercial license

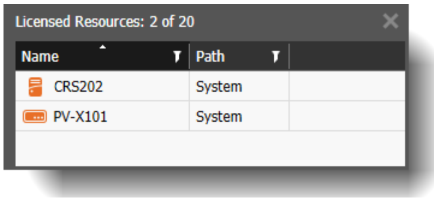
State:
Installed , License expires on 2030-01-01

Description:
Central Evidence Archive container.

Licensed Resources: 0 of 20

Name	Path

7 When you are finished, the recorders you added are displayed in the **Licensed Resources** list.



Licensed Resources: 2 of 20

Name	Path
CRS202	System
PV-X101	System

Adding the Central Evidence Archive Component

You can add the Central Evidence Archive component to Command Enterprise.

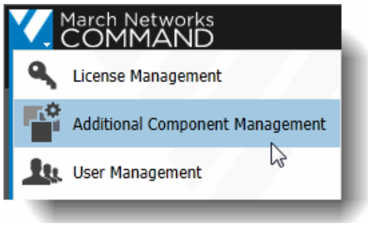
The Central Evidence Archive component adds the Central Evidence Archive tab to the Command Client interface. This new tab allows you to manage tags, cases, and backups.

You must have the **Additional Component Management** user right in your Command user profile to perform this task.

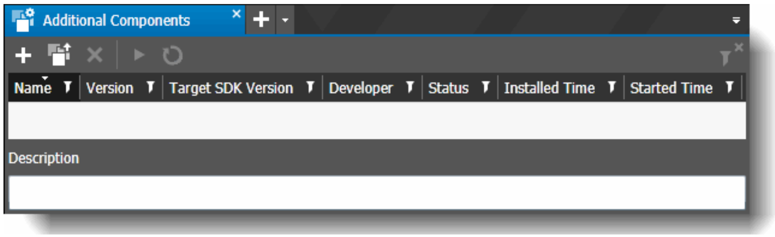
To add the Central Evidence Archive component to Command Enterprise

1 Click the button at the upper-left of Command to display the main menu.

2 Select **Additional Component Management**.



The **Additional Components** tab opens.



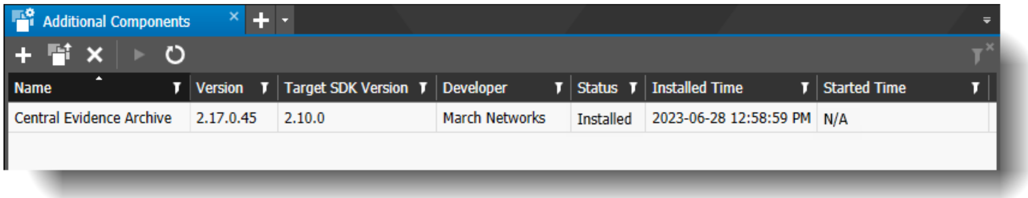
Name	Version	Target SDK Version	Developer	Status	Installed Time	Started Time

3 Click the **Load Application** + button.

A new window opens, where you can locate the Central Evidence Archive zip file.

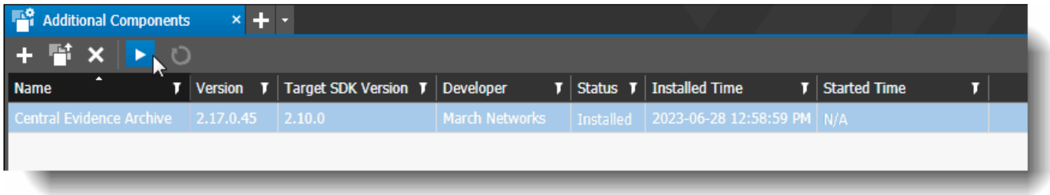
4 Select the Central Evidence Archive zip file (CommandCentralEvidenceArchive_<*version*>.zip) and click **Open**.

The application appears in the list of the Additional Components tab.



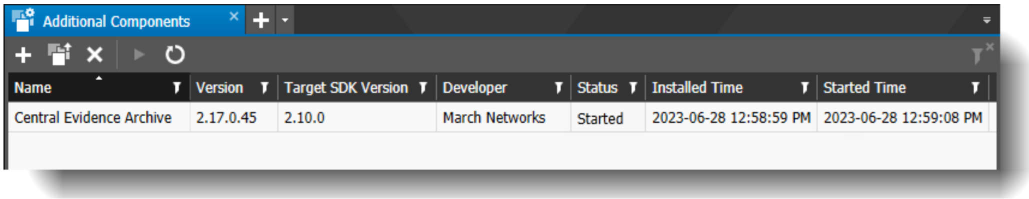
Name	Version	Target SDK Version	Developer	Status	Installed Time	Started Time
Central Evidence Archive	2.17.0.45	2.10.0	March Networks	Installed	2023-06-28 12:58:59 PM	N/A

5 In the list, select the component named Central Evidence Archive and click **Start Application** ▶.



Name	Version	Target SDK Version	Developer	Status	Installed Time	Started Time
Central Evidence Archive	2.17.0.45	2.10.0	March Networks	Installed	2023-06-28 12:58:59 PM	N/A

6 The **Status** changes to “Started” and the date and time appears in the **Started Time** column.



Name	Version	Target SDK Version	Developer	Status	Installed Time	Started Time
Central Evidence Archive	2.17.0.45	2.10.0	March Networks	Started	2023-06-28 12:58:59 PM	2023-06-28 12:59:08 PM

Notes:

- You can remove the application by selecting it in the list and clicking the **Uninstall Application** ✕ button.
- You can restart the application by selecting it in the list and clicking the **Restart Application** ↻ button.

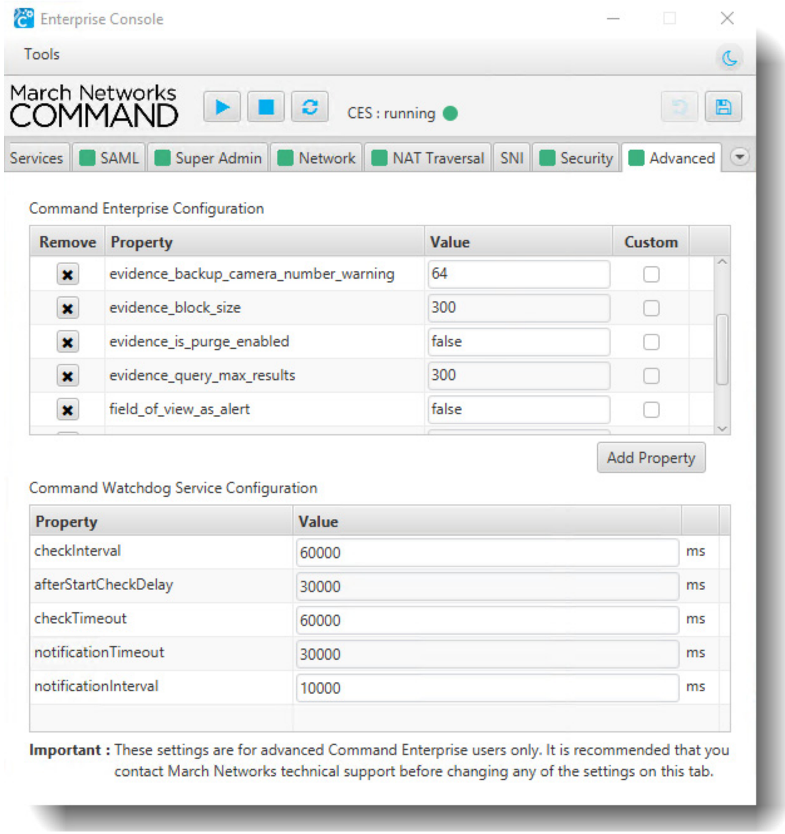
Advanced Settings in the Enterprise Console

The Enterprise Console application allows you to set up and configure various database and administration settings for Command Enterprise.

Note: The Command Enterprise Server must be stopped (offline) in order for you to save changes to the settings in the Enterprise Console. You cannot save settings while the server is running.

Complete instructions for accessing and configuring settings in the Enterprise Console are available in the *Command Enterprise Installation Guide*.

There are some settings in the **Advanced** tab that are applicable exclusively to the Central Evidence Archive.



Command Enterprise Configuration

Remove	Property	Value	Custom
☒	evidence_backup_camera_number_warning	64	☐
☒	evidence_block_size	300	☐
☒	evidence_is_purge_enabled	false	☐
☒	evidence_query_max_results	300	☐
☒	field_of_view_as_alert	false	☐

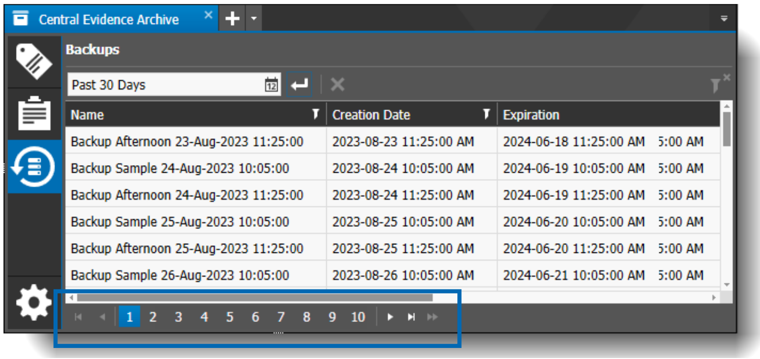
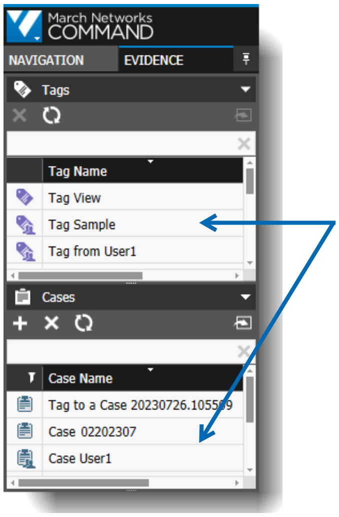
Command Watchdog Service Configuration

Property	Value	
checkInterval	60000	ms
afterStartCheckDelay	30000	ms
checkTimeout	60000	ms
notificationTimeout	30000	ms
notificationInterval	10000	ms

Important : These settings are for advanced Command Enterprise users only. It is recommended that you contact March Networks technical support before changing any of the settings on this tab.

The following table describes the advanced settings for the Central Evidence Archive.

Setting	Description
evidence_backup _camera_number _warning	The maximum number of camera channels you can add to a backup. This includes cameras on a recorder and individual cameras. See “Configuring Scheduled Backups” on page 31. The default is 64.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td><b>evidence_block_size</b></td><td>The number of results returned in a search block of the CEA tab in the Command Client, for tags/cases/backups.
The default is 300.

Central Evidence Archive
Backups
Past 30 Days
1 2 3 4 5 6 7 8 9 10
<table>
<tr><th>Name</th><th>Creation Date</th><th>Expiration</th><th></th></tr>
<tr><td>Backup Afternoon 23-Aug-2023 11:25:00</td><td>2023-08-23 11:25:00 AM</td><td>2024-06-18 11:25:00 AM</td><td>5:00 AM</td></tr>
<tr><td>Backup Sample 24-Aug-2023 10:05:00</td><td>2023-08-24 10:05:00 AM</td><td>2024-06-19 10:05:00 AM</td><td>5:00 AM</td></tr>
<tr><td>Backup Afternoon 24-Aug-2023 11:25:00</td><td>2023-08-24 11:25:00 AM</td><td>2024-06-19 11:25:00 AM</td><td>5:00 AM</td></tr>
<tr><td>Backup Sample 25-Aug-2023 10:05:00</td><td>2023-08-25 10:05:00 AM</td><td>2024-06-20 10:05:00 AM</td><td>5:00 AM</td></tr>
<tr><td>Backup Afternoon 25-Aug-2023 11:25:00</td><td>2023-08-25 11:25:00 AM</td><td>2024-06-20 11:25:00 AM</td><td>5:00 AM</td></tr>
<tr><td>Backup Sample 26-Aug-2023 10:05:00</td><td>2023-08-26 10:05:00 AM</td><td>2024-06-21 10:05:00 AM</td><td>5:00 AM</td></tr>
</table>
There are 30 results per page in the CEA tab, so the default search block has 10 pages (300 results).</td></tr>
<tr><td><b>evidence_is_purge_enabled</b></td><td><b>Note:</b> This setting is also used by Command Enterprise without the CEA installed, for tag files and case files.
If set to true, the default time evidence files are purged after a default time:
• 30 days for tag files
• 20 years for case files
• 300 days for backup files
Default is false.</td></tr>
<tr><td><b>evidence_query_max_results</b></td><td>The maximum number of results returned for the list of tags or cases in the Evidence Panel of the Command Client.
The default is 300.

March Networks COMMAND
NAVIGATION
EVIDENCE
Tags
Cases
<table>
<tr><th>Tag Name</th></tr>
<tr><td>Tag View</td></tr>
<tr><td>Tag Sample</td></tr>
<tr><td>Tag from User1</td></tr>
</table>
<table>
<tr><th>Case Name</th></tr>
<tr><td>Tag to a Case 20230726.105509</td></tr>
<tr><td>Case 02202307</td></tr>
<tr><td>Case User1</td></tr>
</table>
Maximum list size for Tags or Cases in the Evidence Panel</td></tr>
</table>

Note: These settings are for advanced Command Enterprise users only. We recommended you contact March Networks technical support before changing any of these settings. When entering a new value, you MUST press **Enter** to confirm it, or the change reverts back to the original value.

Adding the Central Evidence Archive Application Rights to the User Profile

After you have added the Central Evidence Archive component to Command Enterprise, you must allow users the right to view and use the Central Evidence Archive features. Do this by adding the Central Evidence Archive Application rights to the appropriate user profile.

Note: User rights in Command are managed through the User Profiles defined in Command Enterprise. For more information on Command User Profiles, see the *Command Enterprise and Client User Guide.*

Any user whose profile includes user management rights can modify the name, description, and set of rights associated with a profile.

When you make changes to a profile, all affected users are automatically logged out of the system and will have to log back in.

> **Note:** The steps to add the Central Evidence Archive Application rights to the user profile are slightly different if you are creating a new user profile instead of adding the rights to an existing profile. For a new profile, the additional Central Evidence Archive rights (View Tags, View Cases, View Backups, Configuration) do not appear until you save the new profile with the main Central Evidence Archive right selected. See either:
>
> - "Adding the Central Evidence Archive Rights to an Existing User Profile" on page 12
> - "Adding the Central Evidence Archive Rights to a New User Profile" on page 13

Adding the Central Evidence Archive Rights to an Existing User Profile

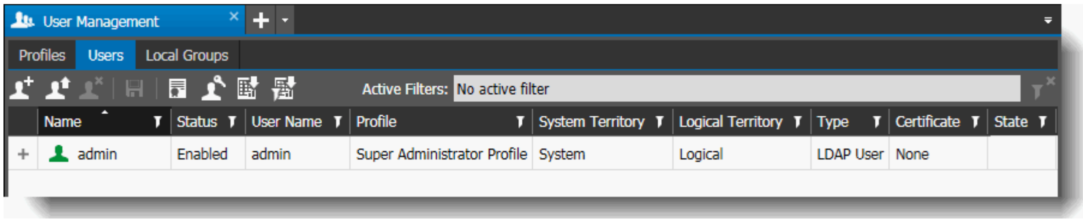
The following procedure describes how to add the Central Evidence Archive application rights to an **existing** user profile.

For a new user profile, see "Adding the Central Evidence Archive Rights to a New User Profile" on page 13.

To add the Central Evidence Archive rights to an existing user profile

1 Click the main menu and select **User Management**.

The User Management tab opens with the Users subtab open by default.



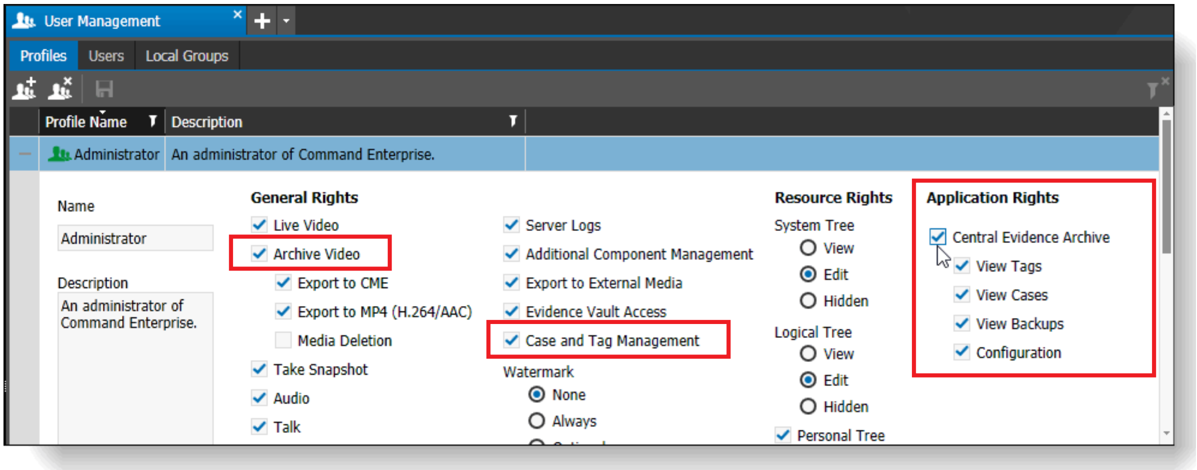
Active Filters: No active filter

Name	Status	User Name	Profile	System Territory	Logical Territory	Type	Certificate	State
admin	Enabled	admin	Super Administrator Profile	System	Logical	LDAP User	None	

2 Click the **Profiles** subtab.

3 Click the expand button to the left of the **Profile Name** of an existing profile.

The selected **Profile** page appears.



Administrator — An administrator of Command Enterprise.

Name: Administrator

Description: An administrator of Command Enterprise.

General Rights
- ☑ Live Video
- ☑ Archive Video
  - ☑ Export to CME
  - ☑ Export to MP4 (H.264/AAC)
  - □ Media Deletion
- ☑ Take Snapshot
- ☑ Audio
- ☑ Talk
- ☑ Server Logs
- ☑ Additional Component Management
- ☑ Export to External Media
- ☑ Evidence Vault Access
- ☑ Case and Tag Management

Watermark
- ● None
- ○ Always

Resource Rights

System Tree
- ○ View
- ● Edit
- ○ Hidden

Logical Tree
- ○ View
- ● Edit
- ○ Hidden

☑ Personal Tree

Application Rights
- ☑ Central Evidence Archive
  - ☑ View Tags
  - ☑ View Cases
  - ☑ View Backups
  - ☑ Configuration

4 Under **General Rights**, ensure that the **Archive Video** and the **Case and Tag Management** rights are selected.

(An existing user profile will already have rights assigned. For more information on the rights, see the *Command Enterprise and Client User Guide*.)

5 Under **Application Rights**, select the **Central Evidence Archive** check box to allow users to view the Central Evidence Archive tab.

You can further customize the Central Evidence Archive user rights with the additional rights that appear under the main right. Users require at least one of these sub-rights:

- Select the **View Tags** check box to allow users to view and manage tags (see “Managing Tag Files” on page 38).
- Select the **View Cases** check box to allow users to view and manage cases (see “Managing Case Files” on page 41).
- Select the **View Backups** check box to allow users to view and manage backups (see “Managing Backup Files” on page 44).
- Select the **Configuration** check box to allow users to view and edit Central Evidence Archive settings (see “Configuring General Settings for the Central Evidence Archive” on page 24).

Note: When you make any changes, the **Profile Name** box is highlighted in orange.

6 On the **Profiles** subtab toolbar, click the **Save All** 🖫 button.

The **Profiles** subtab refreshes to show the changes. All users affected by the changes to that profile are automatically logged out of the system. When they log back in, they have the right to access the Command Central Evidence Archive features.

Adding the Central Evidence Archive Rights to a New User Profile

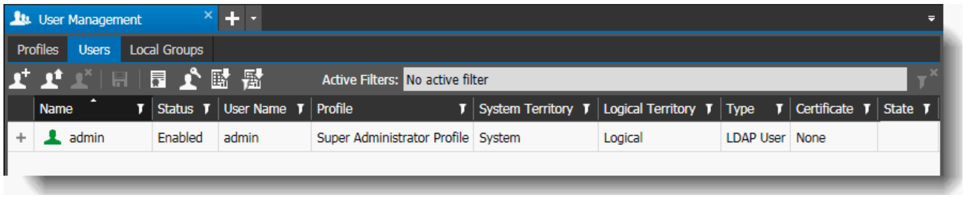
The following procedure describes how to add the Central Evidence Archive application rights to a **new** user profile.

For an existing user profile, see “Adding the Central Evidence Archive Rights to an Existing User Profile” on page 12.

To add the Central Evidence Archive right to a new user profile

1 Click the main menu and select **User Management**.

The User Management tab opens with the Users subtab open by default.



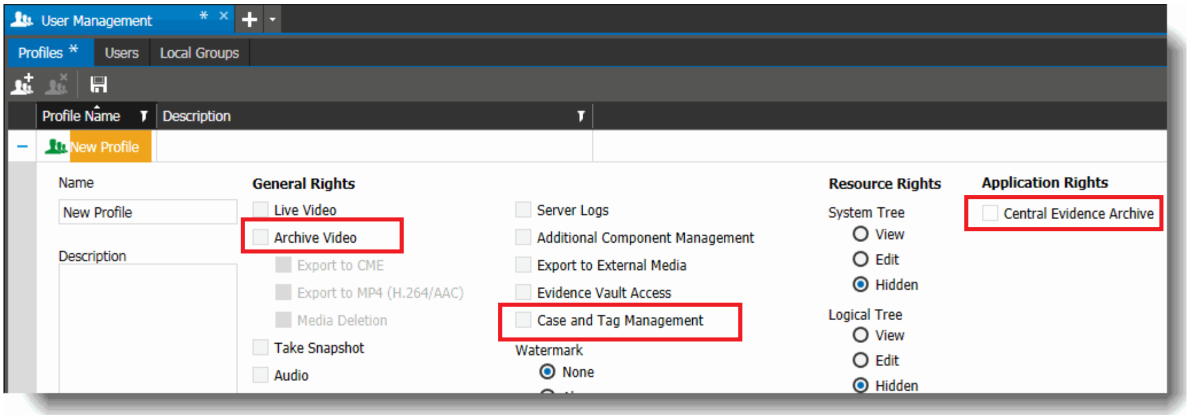
Active Filters: No active filter

Name	Status	User Name	Profile	System Territory	Logical Territory	Type	Certificate	State
admin	Enabled	admin	Super Administrator Profile	System	Logical	LDAP User	None	

2 Click the **Profiles** subtab.

3 Click the **Add a Profile** button on the **Profiles** subtab toolbar.

The new profile appears in a modified state (highlighted in orange) on the **Profiles** subtab.



New Profile

Name: New Profile

Description

General Rights
- □ Live Video
- □ Archive Video
- □ Export to CME
- □ Export to MP4 (H.264/AAC)
- □ Media Deletion
- □ Take Snapshot
- □ Audio
- □ Server Logs
- □ Additional Component Management
- □ Export to External Media
- □ Evidence Vault Access
- □ Case and Tag Management

Watermark
- ● None

Resource Rights

System Tree
- ○ View
- ○ Edit
- ● Hidden

Logical Tree
- ○ View
- ○ Edit
- ● Hidden

Application Rights
- □ Central Evidence Archive

4 Enter a new name for the profile in the **Name** box.

5 In the **Description** box, type a description of the new profile.

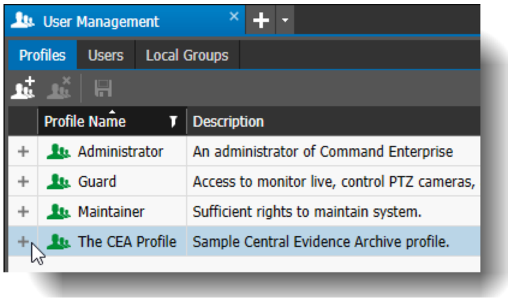
6 Under **General Rights**, ensure that the **Archive Video** and the **Case and Tag Management** rights are selected.

Select the other **General** rights, the **Resource** rights, and the **Layout** you want to assign to the new profile. For more information on the General, Resource, and Layout rights, see the *Command Enterprise and Client User Guide*.

7 Under **Application Rights**, select the **Central Evidence Archive** check box to allow users to view the Central Evidence Archive tab.

8 On the **Profiles** subtab toolbar, click the **Save All** button.

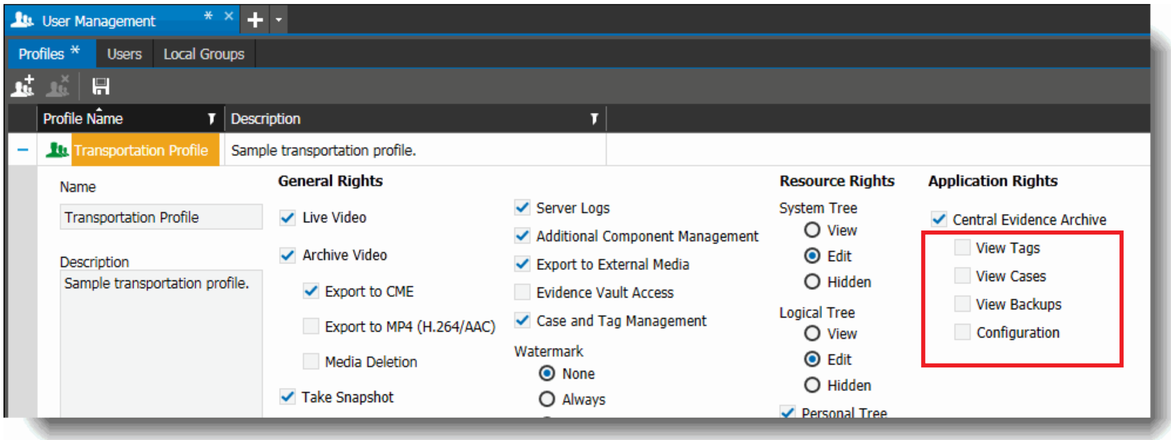
The new profile appears in the **Profile Name** column (**Profiles** subtab).



Profile Name	Description
Administrator	An administrator of Command Enterprise
Guard	Access to monitor live, control PTZ cameras,
Maintainer	Sufficient rights to maintain system.
The CEA Profile	Sample Central Evidence Archive profile.

9 Click the expand button to the left of the new **Profile Name**.

The new **Profile** page appears. Under the main **Central Evidence Archive** right, there are now four additional rights.



Transportation Profile — Sample transportation profile.

Name: Transportation Profile

Description: Sample transportation profile.

General Rights

- ☑ Live Video
- ☑ Archive Video
  - ☑ Export to CME
  - ☐ Export to MP4 (H.264/AAC)
  - ☐ Media Deletion
- ☑ Take Snapshot
- ☑ Server Logs
- ☑ Additional Component Management
- ☑ Export to External Media
- ☐ Evidence Vault Access
- ☑ Case and Tag Management
- Watermark
  - ● None
  - ○ Always

Resource Rights

- System Tree
  - ○ View
  - ● Edit
  - ○ Hidden
- Logical Tree
  - ○ View
  - ● Edit
  - ○ Hidden
- ☑ Personal Tree

Application Rights

- ☑ Central Evidence Archive
  - ☐ View Tags
  - ☐ View Cases
  - ☐ View Backups
  - ☐ Configuration

You can further customize the Central Evidence Archive user rights with these additional rights:

- Select the **View Tags** check box to allow users to view and manage tags (see “Managing Tag Files” on page 38).
- Select the **View Cases** check box to allow users to view and manage cases (see “Managing Case Files” on page 41).
- Select the **View Backups** check box to allow users to view and manage backups (see “Managing Backup Files” on page 44).
- Select the **Configuration** check box to allow users to view and edit Central Evidence Archive settings (see “Configuring General Settings for the Central Evidence Archive” on page 24).

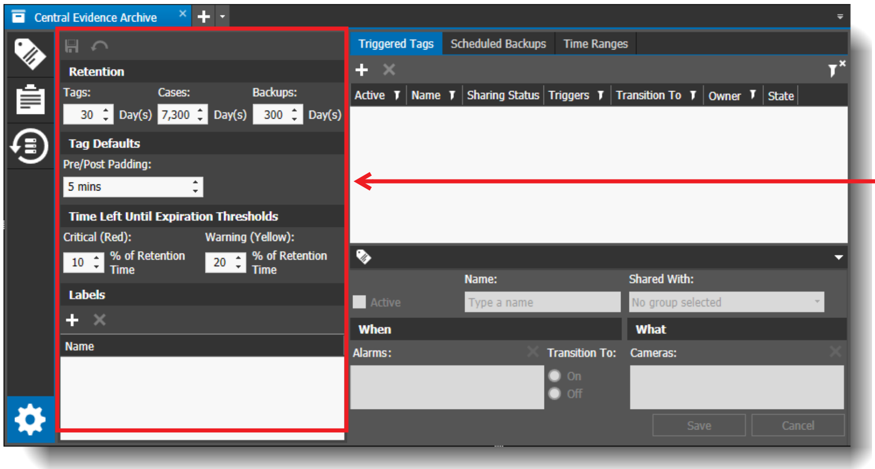
Note: When you make any changes, the **Profile Name** box is highlighted in orange.

10 On the **Profiles** subtab toolbar, click the **Save All** button.

The **Profiles** subtab refreshes to show the changes.

Access to the Central Evidence Archive

Only top-level users with the User Management right can edit the configuration settings for the Central Evidence Archive. For other users with access to the tab, the settings are view only.



Retention

Tags: 30 Day(s) Cases: 7,300 Day(s) Backups: 300 Day(s)

Tag Defaults

Pre/Post Padding: 5 mins

Time Left Until Expiration Thresholds

Critical (Red): 10 % of Retention Time Warning (Yellow): 20 % of Retention Time

Labels

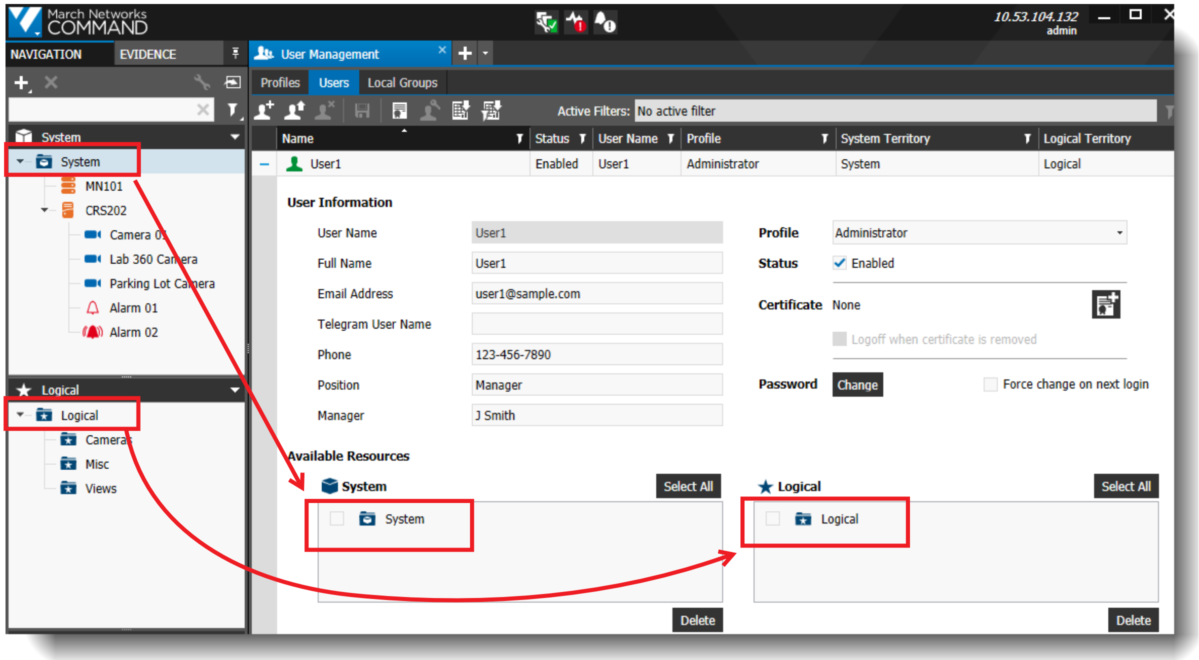
Name

General configuration settings for the Central Evidence Archive - only top-level users can edit these settings

Also, only top-level users can view and edit the configuration settings for all triggered tags, scheduled backups, and time ranges. Users without top-level access can only view and edit the configuration settings for their own triggered tags, scheduled backups, and time ranges. (See “Configuring the Central Evidence Archive” on page 20 for more information on the Configuration tab.)

A top-level user has root-level Territory access to the **System** and **Logical** trees in Command Client (full access to both trees) and the **User Management** right.

In the following example, User1 has been granted root access to the System and Logical trees.



Name	Status	User Name	Profile	System Territory	Logical Territory
User1	Enabled	User1	Administrator	System	Logical

User Information

User Name: User1

Full Name: User1

Email Address: user1@sample.com

Telegram User Name:

Phone: 123-456-7890

Position: Manager

Manager: J Smith

Profile: Administrator

Status: ☑ Enabled

Certificate: None

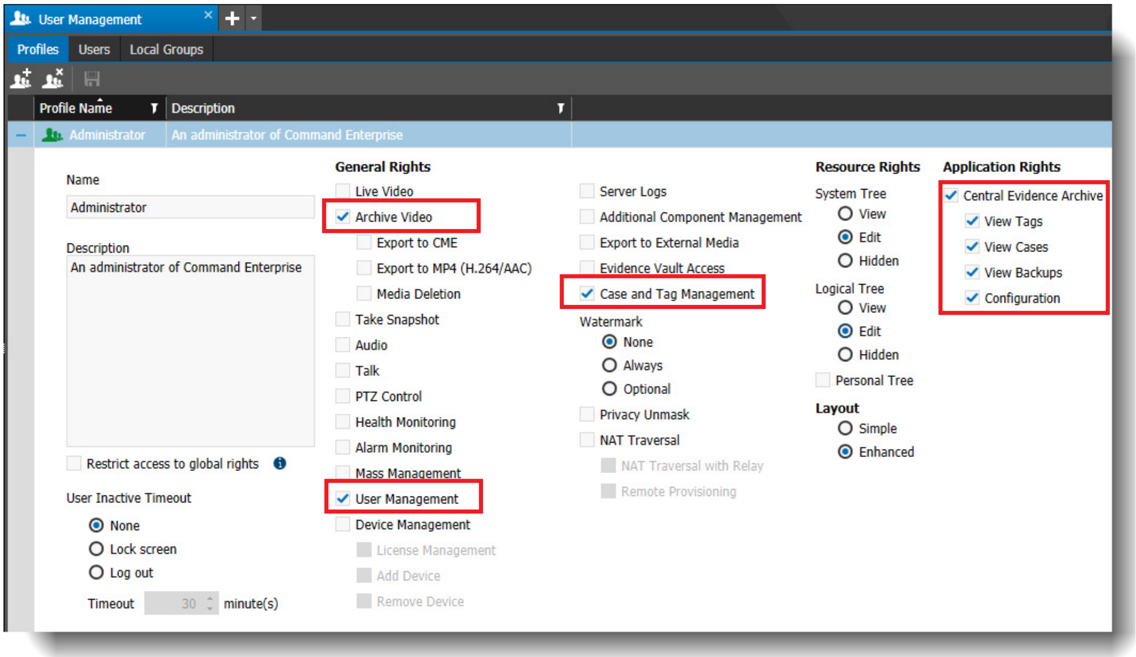
Password

Available Resources

System: □ System

Logical: □ Logical

The top-level user must also have the **User Management** right in their profile, and the required Central Evidence Archive rights, as outlined in the previous section (“Adding the Central Evidence Archive Application Rights to the User Profile” on page 12). ,



Profile Name	Description
Administrator	An administrator of Command Enterprise

Name: Administrator

Description: An administrator of Command Enterprise

□ Restrict access to global rights

User Inactive Timeout
● None
○ Lock screen
○ Log out

Timeout 30 minute(s)

General Rights
□ Live Video
☑ Archive Video
□ Export to CME
□ Export to MP4 (H.264/AAC)
□ Media Deletion
□ Take Snapshot
□ Audio
□ Talk
□ PTZ Control
□ Health Monitoring
□ Alarm Monitoring
□ Mass Management
☑ User Management
□ Device Management
□ License Management
□ Add Device
□ Remove Device

□ Server Logs
□ Additional Component Management
□ Export to External Media
□ Evidence Vault Access
☑ Case and Tag Management

Watermark
● None
○ Always
○ Optional

□ Privacy Unmask
□ NAT Traversal
□ NAT Traversal with Relay
□ Remote Provisioning

Resource Rights

System Tree
○ View
● Edit
○ Hidden

Logical Tree
○ View
● Edit
○ Hidden

□ Personal Tree

Layout
○ Simple
● Enhanced

Application Rights
☑ Central Evidence Archive
☑ View Tags
☑ View Cases
☑ View Backups
☑ Configuration

For more information on top-level users, user profiles, and user accounts in Command Enterprise, see the *Command Enterprise and Client User Guide*, available from the March Networks Partner Portal website.

Upgrading the Central Evidence Archive Component

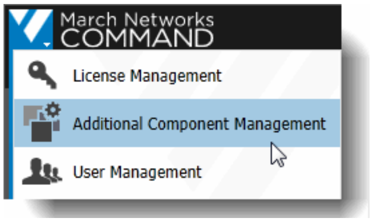
You can upgrade the Central Evidence Archive component if a new version is available to you.

Note: You must have the **Additional Component Management** user right in your Command user profile to perform this task.

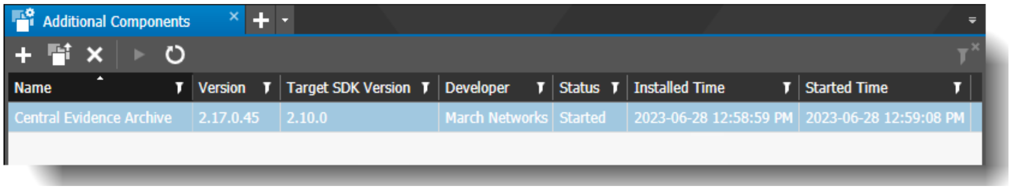
Important: After a Command Enterprise software upgrade, the Central Evidence Archive application may no longer be compatible with Command Enterprise. If this occurs, the Central Evidence Archive application is automatically stopped and an **Upgrade Required** notification appears in the **Additional Components** tab. You must upgrade the Central Evidence Archive application and manually start it again.

To upgrade the Central Evidence Archive component

1 Click the main menu and select **Additional Component Management**.



The **Additional Components** tab opens. The current release of the Central Evidence Archive application is displayed in the list.



Name	Version	Target SDK Version	Developer	Status	Installed Time	Started Time
Central Evidence Archive	2.17.0.45	2.10.0	March Networks	Started	2023-06-28 12:58:59 PM	2023-06-28 12:59:08 PM

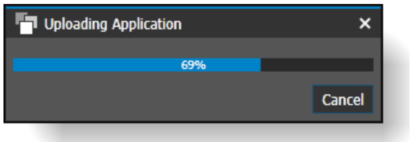
Note: You can upgrade when the Central Evidence Archive application is in either Started or Installed status.

2 Click the **Upgrade Application** button.

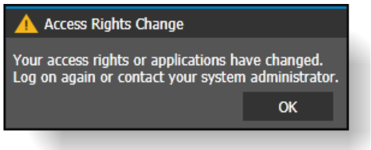
A new window opens, where you can locate the Central Evidence Archive zip file for the new version of the application.

3 Select the new version of the Central Evidence Archive application zip file (CommandCentralEvidenceArchive_<*version*>.zip) and click **Open**.

The Uploading Application dialog appears. This dialog displays the progress of the upgrade.



When the application finishes uploading, the **Access Rights Change** dialog appears to indicate that there has been a change in an application.



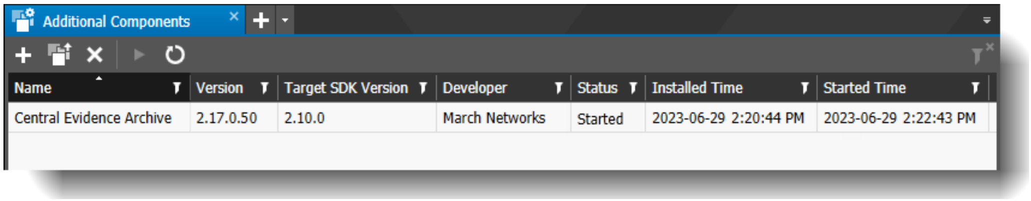
Your access rights or applications have changed.
Log on again or contact your system administrator.

4 Click **OK**.

Command Enterprise automatically logs you out.

5 Enter your user name and password to log in and open the Additional Components tab again.

The **Version** column displays the new release that you just upgraded to.



Name	Version	Target SDK Version	Developer	Status	Installed Time	Started Time
Central Evidence Archive	2.17.0.50	2.10.0	March Networks	Started	2023-06-29 2:20:44 PM	2023-06-29 2:22:43 PM

Chapter 2

Configuring the Central Evidence Archive

This chapter describes how to configure the settings for the Central Evidence Archive.

It contains the following topics:

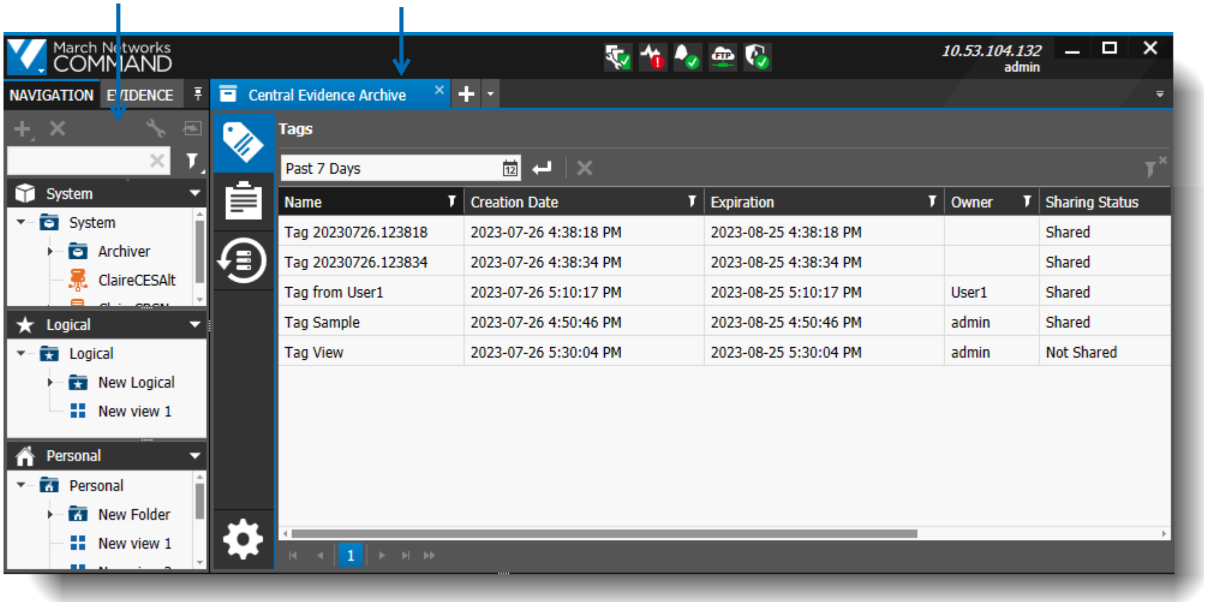
- “Overview” on page 21
- “Configuring General Settings for the Central Evidence Archive” on page 24
- “Configuring Triggered Tags” on page 27
- “Configuring Scheduled Backups” on page 31
- “Configuring Time Ranges” on page 35

Overview

The user interface of the Command Central Evidence Archive application consists of an additional tab within the Command Client (when connected to Enterprise). This tab allows you to manage your tags, cases, and backups.

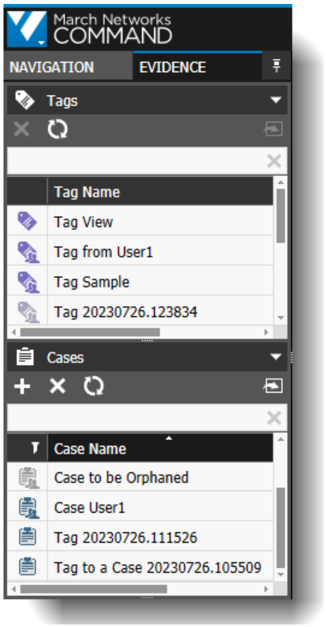
Navigation & Evidence Panels

CEA tab, displaying Tag management



Name	Creation Date	Expiration	Owner	Sharing Status
Tag 20230726.123818	2023-07-26 4:38:18 PM	2023-08-25 4:38:18 PM		Shared
Tag 20230726.123834	2023-07-26 4:38:34 PM	2023-08-25 4:38:34 PM		Shared
Tag from User1	2023-07-26 5:10:17 PM	2023-08-25 5:10:17 PM	User1	Shared
Tag Sample	2023-07-26 4:50:46 PM	2023-08-25 4:50:46 PM	admin	Shared
Tag View	2023-07-26 5:30:04 PM	2023-08-25 5:30:04 PM	admin	Not Shared

The **Evidence** panel is the right tab of the Navigation Panel, on the left under the **Main Menu** button. This panel is available in Command Enterprise without the Central Evidence Archive.



Tag Name
Tag View
Tag from User1
Tag Sample
Tag 20230726.123834

Case Name
Case to be Orphaned
Case User1
Tag 20230726.111526
Tag to a Case 20230726.105509

In the **Evidence** panel, you can view your current tags and case files. For more information on the evidence panel, see the *Command Enterprise and Client User Guide*.

Case Files

Case files are available in Command Enterprise without the Central Evidence Archive installed, but the Central Evidence Archive allows you to centrally manage them, and add labels.

Cases are files that can include multiple video files, snapshots and notes, allowing you to organize your video evidence. A case file allows you to queue multiple files before exporting. The video files that you add to a case are exported from the recorder and saved on the Archiver, so that they are retained for a longer period of time than video on the recorder and are always available to you when you want to review the evidence in a case file.

Without the Central Evidence Archive installed, you can still create cases, but they are only available from the Evidence panel. With the Central Evidence Archive, you can still create cases, but you can also manage and filter cases in a central location (see “Managing Case Files” on page 41).

You can add and edit notes to a case file to provide more information for the video evidence. Notes allow you to provide details about the video and snapshots in the case file. With the Central Evidence Archive installed, you can add labels. You can share case files with other users so that multiple users can view, edit, and export the information in the case.

Tag Files

Like case files, tag files are available in Command Enterprise without the Central Evidence Archive installed, but the Central Evidence Archive allows you to centrally manage them, create them automatically, and add labels.

Tags are video clips configured to save automatically from an event (for example, an alarm), or created manually when a user sees a point of interest in a video.

Without the Central Evidence Archive installed, you can create manual tags, which are available from the Evidence panel. With the Central Evidence Archive, you can still create manual tags, but you can also set up tags that are automatically created when an event is triggered — see “Configuring Triggered Tags” on page 27. Triggered tags are only supported for R6 recorders and CRS, not R5 recorders.

You can add notes, export, share, change the owner, and convert the tag file to a case file. With the Central Evidence Archive installed, you can add labels.

Note:

When configuring an automatic triggered tag:

- You must ensure that the recorder will be recording when the event triggers, so that video is available for extraction. For example, if the trigger for the tag is an alarm that could be triggered after business hours, ensure that the recorder is configured to record video after business hours.
- If the Alarm/Event is from the same recorder as the Camera selected for the tag, we recommend that you configure the “On Condition Recording Retention” for the camera, to ensure that the required recording is retained until the tag can extract it. Recorded video not related to the tag Alarm/Event can be configured with a lower retention or not retained, saving storage on the recorder.

Backup Files

Backup files are only available when you have the Central Evidence Archive installed. They are created when you set up scheduled backups (see “Configuring Scheduled Backups” on page 31).

Backup files consist of the video and data from the recorder or cameras selected for backup, during the scheduled time period. You can add notes, add labels, export, share, change the owner, and convert the backup file to a case file.

Additional Information for Tag Files and Case Files

The *Command Enterprise and Client User Guide* has more information on creating Cases and Tags. You can create cases and tags in Command Enterprise without the Central Evidence Archive, but the Central Evidence Archive allows you to manage them in a central location.

See the *Command Enterprise and Client User Guide* for more information on:

- creating Cases
- creating Tags manually
- reviewing the content of a Case or Tag file
- sharing Cases and Tags (also applies to Backups)
- exporting Case and Tag files (also applies to Backups)

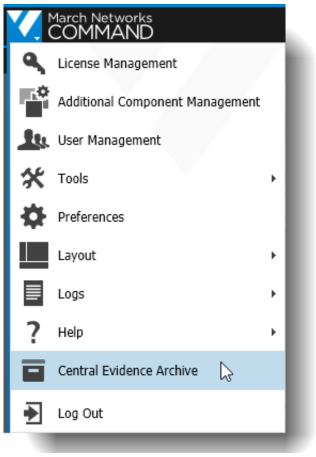
Configuring General Settings for the Central Evidence Archive

You can configure retention for tags, cases, and backups, pre and post padding for tags, expiration thresholds, and labels.

Important: Only top-level users can edit the general settings (top-level users have full access to the root System tree and the root Logical tree, and the User Management right). For users without top-level access, the fields in the general settings area (Retention, Tag Defaults, Time Left Until Expiration Thresholds, and Labels) are unavailable to edit, they can only be viewed.

To configure general settings for the Central Evidence Archive

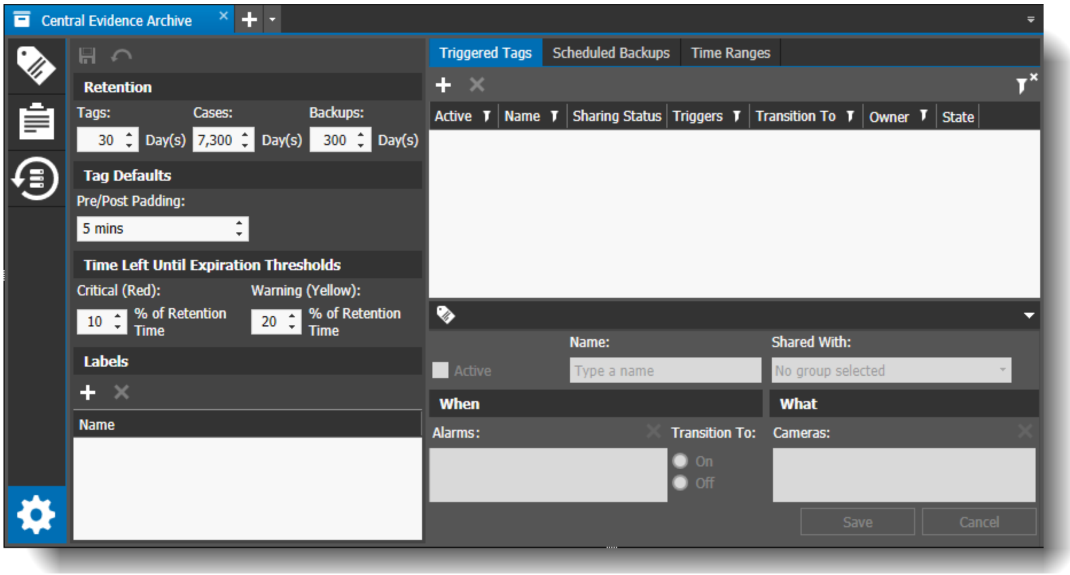
1 From the main menu button select **Central Evidence Archive**.



The Central Evidence Archive tab opens, with the Tags subtab open by default.

2 Select the **Configuration** subtab.

The Configuration subtab opens.



Retention

Tags: 30 Day(s) Cases: 7,300 Day(s) Backups: 300 Day(s)

Tag Defaults

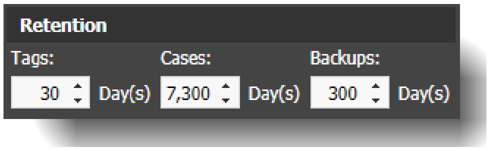
Pre/Post Padding: 5 mins

Time Left Until Expiration Thresholds

Critical (Red): 10 % of Retention Time Warning (Yellow): 20 % of Retention Time

3 Set the **Retention** period for central evidence. This is the number of days that evidence is saved before it is automatically deleted.

Tags, cases, and backups all have individual retention settings.



Retention

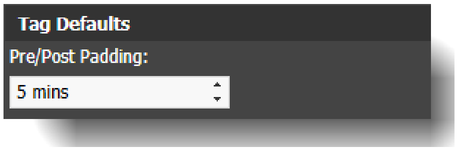
Tags: 30 Day(s) Cases: 7,300 Day(s) Backups: 300 Day(s)

4 Set the **Tag Defaults**. The **Pre/Post Padding** is the amount of time added before and after the point at which the tag is created.

By default, the tag is set to give you 5 minutes before and 5 minutes after the time selected (manually or triggered by an event).

For example, at the default of 5 minutes:

- For **manual** tags, if you are viewing archive video from 1:00 pm and manually create a tag, the video defaults to start at 12:55 pm and ends at 1:05 pm. If you create the tag from live video, the current time is displayed and there is no future video — if you create the tag while viewing live video from 1:00 pm, the video defaults to start at 12:55 pm and ends at 1:00 pm (the current time).
- For **automatic** tags triggered by an event, the system saves video from 5 minutes before and 5 minutes after the event trigger (the tag is created after the required video is available).

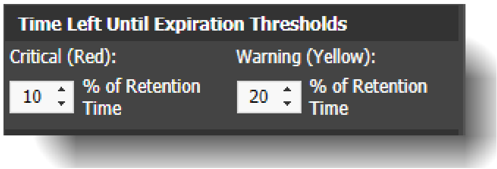


Tag Defaults

Pre/Post Padding: 5 mins

5 Set the **Time Left Until Expiration Thresholds**. This controls when the warning colors are implemented: red for critical and yellow for warning.

Set the percentage of retention time remaining when the warning colors appear.



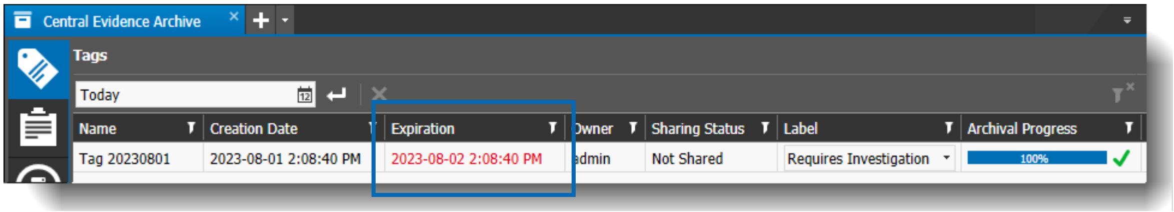
Time Left Until Expiration Thresholds

Critical (Red): 10 % of Retention Time

Warning (Yellow): 20 % of Retention Time

For example, if the retention time is 30 days, and the critical threshold is set to 10%, the critical threshold is triggered when there are 3 days left before the item is deleted.

The Expiration date/time in the Central Evidence Archive changes color to notify you when the expiration threshold is at the critical or warning level.



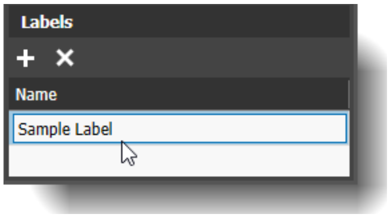
Tags

Today

Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Tag 20230801	2023-08-01 2:08:40 PM	2023-08-02 2:08:40 PM	admin	Not Shared	Requires Investigation	100% ✓

6 Add **Labels**, to assist in filtering and searching.

Select the **Add Label** ✚ button, then double-click the new label to change the name.

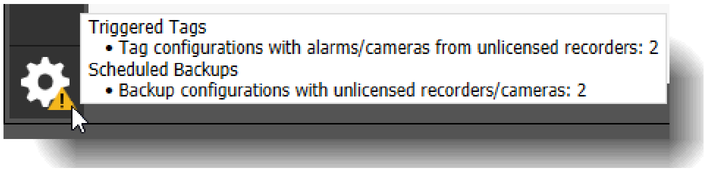


You can select a Label then the **Remove Label** ✖ button to delete it.

7 Select **Save** 💾.

You can select the **Revert** ↶ button if you do not want to keep your changes.

Note: If there are any issues with the settings for the Central Evidence Archive, a warning appears on the **Configuration** icon (this warning is visible to top-level users with the User Management right). When you hover your mouse over it, a message appears. You can find more details in the **State** column of the Triggered Tags and the Scheduled Backups.



Triggered Tags
- Tag configurations with alarms/cameras from unlicensed recorders: 2

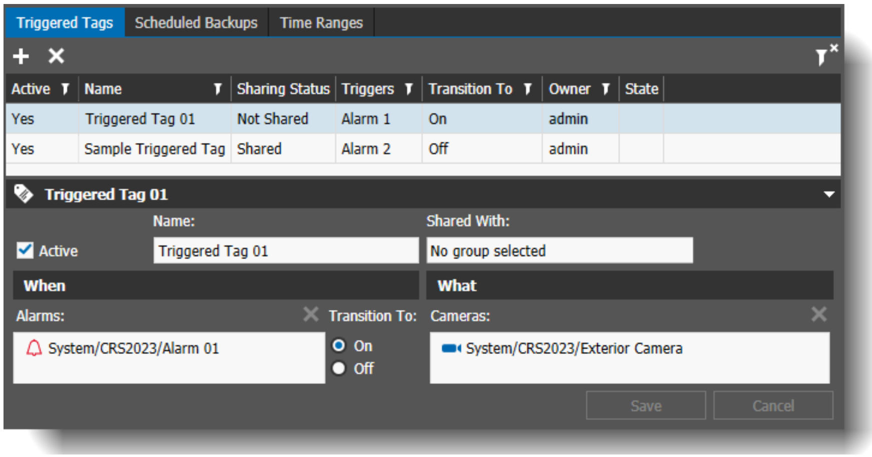
Scheduled Backups
- Backup configurations with unlicensed recorders/cameras: 2

Configuring Triggered Tags

In the **Triggered Tags** tab of the Central Evidence Archive, you can configure the system to create a tag when an event is triggered. You can also edit the triggered tag if required.

Important: Only top-level users can view and edit all triggered tags in the **Configuration > Triggered Tags** tab (top-level users have full access to the root System tree and the root Logical tree, and the User Management right). Users without top-level access can only view and edit their own triggered tags.

Note: For triggered tags, the event and camera must be from an R6 recorder (X-Series) or a CRS. R5 recorders (8000, 9000 series) do not support triggered tags, only manual tags.



Active	Name	Sharing Status	Triggers	Transition To	Owner	State
Yes	Triggered Tag 01	Not Shared	Alarm 1	On	admin	
Yes	Sample Triggered Tag	Shared	Alarm 2	Off	admin	

Triggered Tag 01

☑ Active

Name: Triggered Tag 01

Shared With: No group selected

When

Alarms: System/CRS2023/Alarm 01

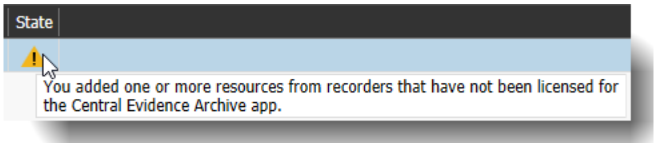
Transition To: ● On ○ Off

What

Cameras: System/CRS2023/Exterior Camera

The following settings are listed for triggered tags.

Option	Description
Active	The triggered tag is active or not. When set to **Yes**, the tag is active and created on event trigger. When set to **No**, the tag is not created.
Name	Name for the triggered tag.
Sharing Status	Whether the triggered tag is shared with any local groups or not. **Note:** Before you can share a tag, you must have some local user groups available to share the tag with, set up in the **User Management > Local Groups** tab. Users can only share with local groups that they are a member of. For instructions on setting up local groups, see the *Command Enterprise and Client User Guide*.
Triggers	The event that triggers the creation of the tag (for example, an alarm).
Transition To	Whether the triggered tag is created when the state of the event turns to **On** or when it turns to **Off**.
Owner	The owner of the triggered tag.

Option	Description
State	The state of the triggered tag. If there is a problem with the tag, a warning icon appears here, with a message when you hover your mouse over the icon. For example, a warning appears if you add a resource (alarm or camera) from a recorder that is unlicensed from the Central Evidence Archive.  State You added one or more resources from recorders that have not been licensed for the Central Evidence Archive app. **Note:** Ensure that your triggered tag does not display any warnings, as the tag may not be triggered if there is a problem.

To set up triggered tags

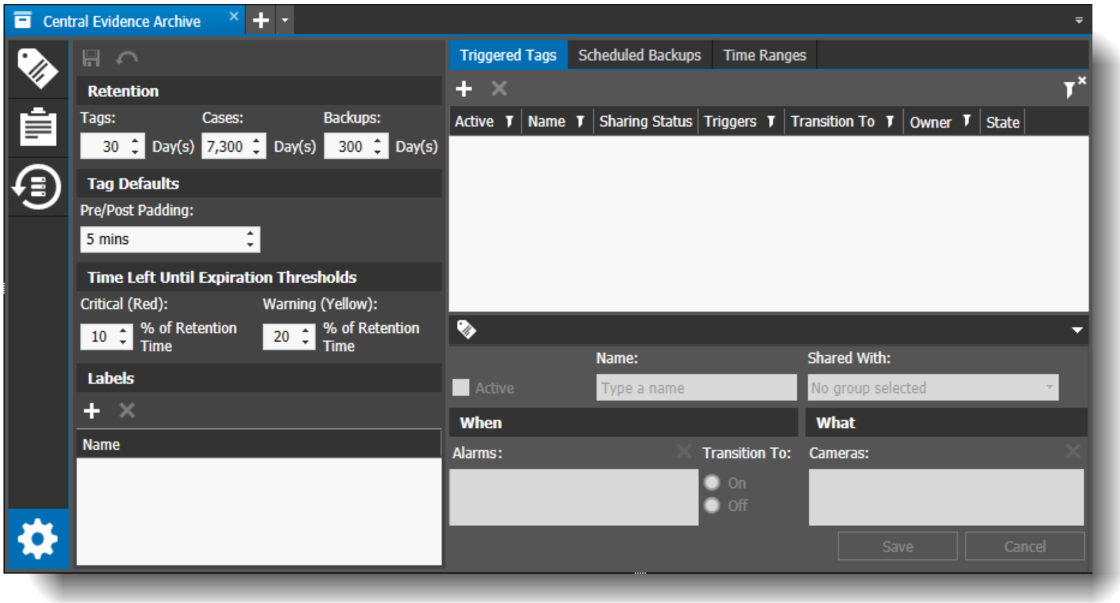
1 From the main menu button select **Central Evidence Archive**.

The Central Evidence Archive tab opens, with the Tags subtab open by default.

2 Select the **Configuration** subtab.

The Configuration subtab opens.

At the right, the **Triggered Tags** tab is open by default.



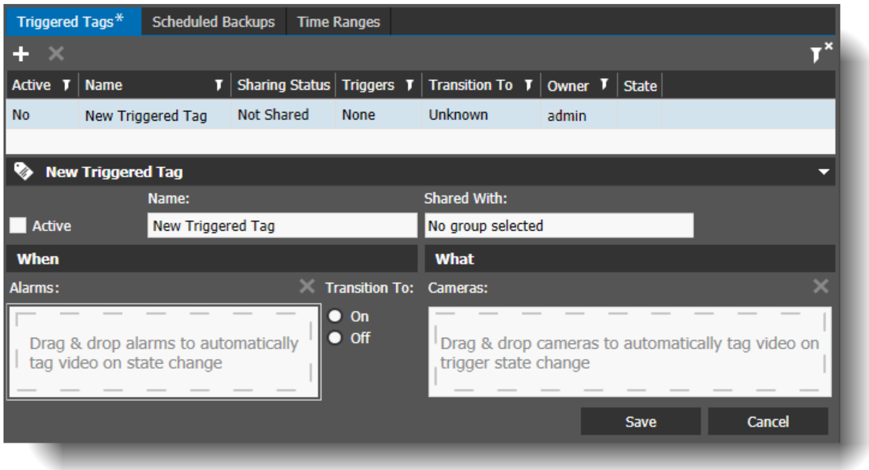
Tags: 30 Day(s) Cases: 7,300 Day(s) Backups: 300 Day(s)

Pre/Post Padding: 5 mins

Critical (Red): 10 % of Retention Time Warning (Yellow): 20 % of Retention Time

3 In the **Triggered Tags** tab at the right, select the **Add** ➕ button.

A new tag is added to the list.



Active	Name	Sharing Status	Triggers	Transition To	Owner	State
No	New Triggered Tag	Not Shared	None	Unknown	admin	

New Triggered Tag

☐ Active

Name: New Triggered Tag

Shared With: No group selected

When

Alarms: Drag & drop alarms to automatically tag video on state change

Transition To: ○ On ○ Off

What

Cameras: Drag & drop cameras to automatically tag video on trigger state change

4 Select the **Active** check box to activate the creation of the triggered tag.

Note: You can create the triggered tag and activate it at a later time.

5 Enter a **Name** for the triggered tag.

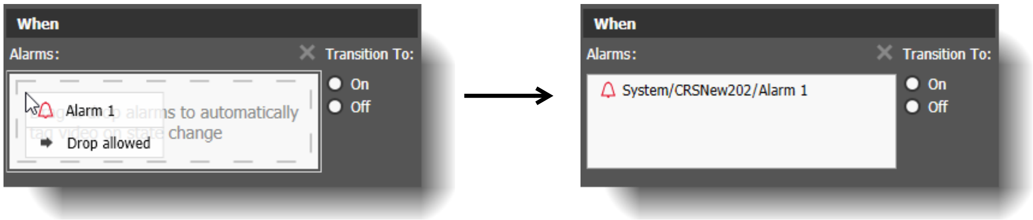
6 In **Shared With**, select a local group to share the tag with.

Note: If there are no local user groups available, the Shared With field is not available. Local groups are set up in the **User Management > Local Groups** tab. Only groups that you are a member of are available for you to share with. For more information on creating local groups, see the *Command Enterprise and Client User Guide*.

Any user with the right to view the triggered tag settings can edit the **Shared With** field.

7 In **Alarms**, drag and drop an alarm from the Navigation panel (System, Logical, or Personal tree) to the list to trigger the creation of the tag.

The alarm must be from an R6 recorder (X-Series) or a CRS. R5 recorders (8000, 9000 Series) do not support triggered tags.

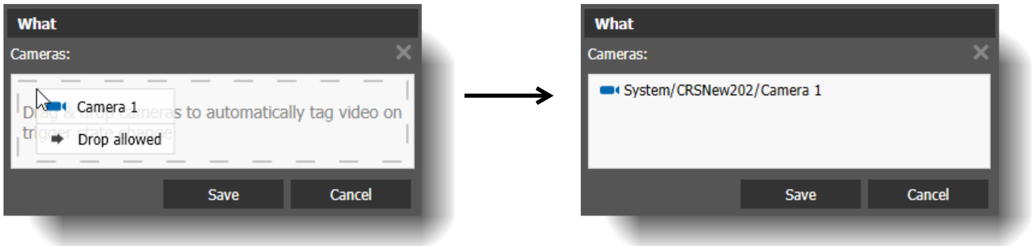


8 For **Transition To**, select **On** or **Off**, to configure whether the tag is created when the state of the alarm changes to On or when it changes to Off.

9 In **Cameras**, drag and drop a camera from the Navigation panel (System, Logical, or Personal tree) to the list. Video from this camera is automatically tagged when the alarm is triggered on

or off (including the pre and post padding time, see “Configuring General Settings for the Central Evidence Archive” on page 24).

The camera must be from an R6 recorder (X-Series) or a CRS. R5 recorders (8000, 9000 Series) do not support triggered tags.



10 Select **Save**.

If the tag is set to active, it is triggered when the alarm state changes.

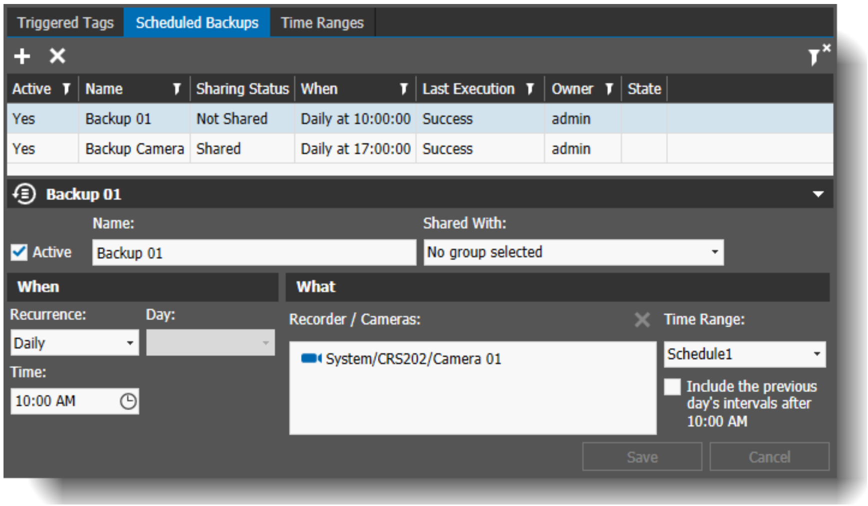
Configuring Scheduled Backups

In the **Scheduled Backups** tab of the Central Evidence Archive, you can configure the system to create a backup at a scheduled time. You can also edit the scheduled backup if required.

Important: Only top-level users can view and edit all scheduled backups in the **Configuration > Scheduled Backups** tab (top-level users have full access to the root System tree and the root Logical tree, and the User Management right). Users without top-level access can only view and edit their own scheduled backups.

Note: For scheduled backups, the recorder/cameras must be from an R6 recorder (X-Series) or a CRS. R5 recorders (8000, 9000 series) do not support scheduled backups.

At maximum, each Scheduled Backup includes video from a single day (24 hours).



Active	Name	Sharing Status	When	Last Execution	Owner	State
Yes	Backup 01	Not Shared	Daily at 10:00:00	Success	admin	
Yes	Backup Camera	Shared	Daily at 17:00:00	Success	admin	

Backup 01

Name: Backup 01

☑ Active

Shared With: No group selected

When

Recurrence: Daily

Day:

Time: 10:00 AM

What

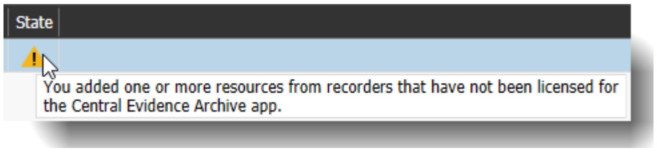
Recorder / Cameras: System/CRS202/Camera 01

Time Range: Schedule1

□ Include the previous day's intervals after 10:00 AM

The following settings are listed for scheduled backups.

Option	Description
Active	The scheduled backup is active or not. When set to **Yes**, the backup is active and created on schedule. When set to **No**, the backup is not created.
Name	Name for the scheduled backup.
Sharing Status	Whether the scheduled backup is shared with any local groups or not. **Note:** Before you can share a backup, you must have some local user groups available to share the tag with, set up in the **User Management > Local Groups** tab. Users can only share with local groups that they are a member of. For instructions on setting up local groups, see the *Command Enterprise and Client User Guide*.
When	When the scheduled backup is scheduled to occur.
Last Execution	Whether the most recent scheduled backup was successful or not.
Owner	The owner of the scheduled backup.

Option	Description
State	The state of the scheduled backup. If there is a problem with the backup, a warning appears here, with a message when you hover your mouse over the icon. For example, a warning appears if you add a resource (recorder or camera) from a recorder that is unlicensed from the Central Evidence Archive.  State You added one or more resources from recorders that have not been licensed for the Central Evidence Archive app. **Note:** Ensure that your scheduled backup does not display any warnings, as the backup may not be generated if there is a problem.

To set up scheduled backups

Note: At least one **Time Range** must be created before you can create a scheduled backup. See “Configuring Time Ranges” on page 35.

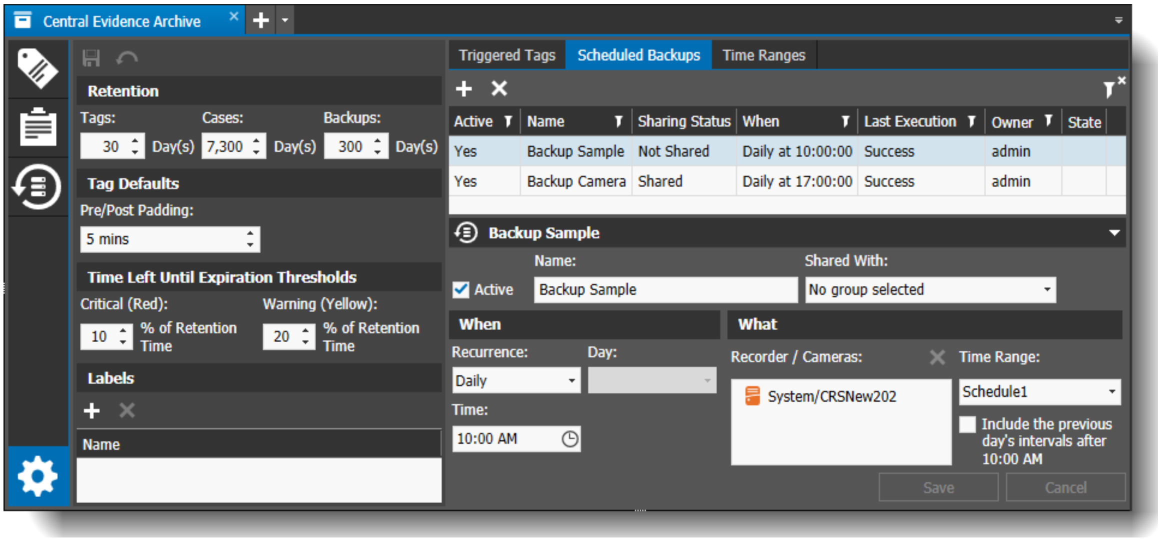
1 From the main menu button select **Central Evidence Archive**.

The Central Evidence Archive tab opens, with the Tags subtab open by default.

2 Select the **Configuration** subtab.

The Configuration subtab opens.

3 At the right, select the **Scheduled Backups** tab.



Retention

Tags: 30 Day(s) Cases: 7,300 Day(s) Backups: 300 Day(s)

Tag Defaults

Pre/Post Padding: 5 mins

Time Left Until Expiration Thresholds

Critical (Red): 10 % of Retention Time

Warning (Yellow): 20 % of Retention Time

Labels

Name

Active	Name	Sharing Status	When	Last Execution	Owner	State
Yes	Backup Sample	Not Shared	Daily at 10:00:00	Success	admin	
Yes	Backup Camera	Shared	Daily at 17:00:00	Success	admin	

Backup Sample

☑ Active

Name: Backup Sample

Shared With: No group selected

When

Recurrence: Daily

Day:

Time: 10:00 AM

What

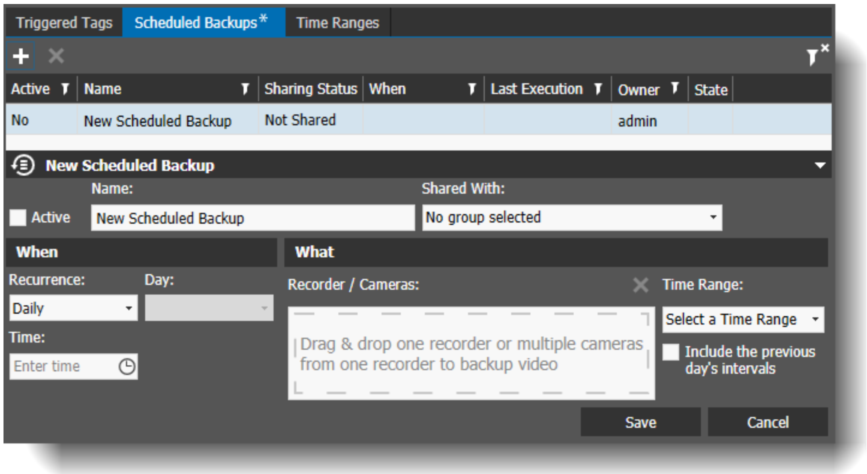
Recorder / Cameras: System/CRSNew202

Time Range: Schedule1

□ Include the previous day's intervals after 10:00 AM

4 In the **Scheduled Backups** tab, select the **Add** ➕ button.

A new scheduled backup is added to the list.



Active	Name	Sharing Status	When	Last Execution	Owner	State
No	New Scheduled Backup	Not Shared			admin	

□ Active

Name: New Scheduled Backup

Shared With: No group selected

Recurrence: Daily

Day:

Time: Enter time

Recorder / Cameras: Drag & drop one recorder or multiple cameras from one recorder to backup video

Time Range: Select a Time Range

□ Include the previous day's intervals

5 Select the **Active** check box to activate the creation of the scheduled backup.

Note: You can create the scheduled backup and activate it at a later time.

6 Enter a **Name** for the scheduled backup.

7 In **Shared With**, select a local group to share the backup with.

Note: If there are no local user groups available, the Shared With field is not available. Local groups are set up in the **User Management > Local Groups** tab. Only groups that you are a member of are available for you to share with. For more information on creating local groups, see the *Command Enterprise and Client User Guide*.

Any user with the right to view the scheduled backup settings can edit the **Shared With** field.

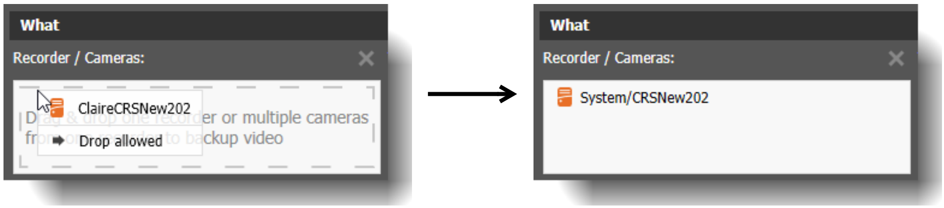
8 In **Recurrence**, select whether you want the backup to occur Daily or Weekly.

9 The **Day** option is only available if you selected a Weekly recurrence for the schedule. Select the day of the week that you want the backup to occur.

10 For **Time**, select the time of day that you want the backup to occur.

Tip: You can select the clock icon to open a quick time selection.

11 In **Recorder/Cameras**, drag and drop one recorder, or multiple cameras belonging to the same recorder, from the Navigation panel to the list. Video from all the cameras on the recorder or from the selected cameras is automatically included in the backup.



12 In **Time Range**, select a pre-created time range for the backup.

Note: At least one Time Range be created before you can select one here. See “Configuring Time Ranges” on page 35.

This time range defines which data is collected for the backup. For example, a backup that occurs weekly on a Sunday could be scheduled to back up all the data from a time range of

8AM to 8PM. A backup that occurs daily could be scheduled to collect data from different time ranges each day.

13 Select **Include the previous day's intervals after <*time*>** if you want the backup to include data from the previous day, if the backup is scheduled to start after the time range set for the data.

Example 1:

A **Daily** recurrence starting at 11AM with a **Time Range** from 8AM to 8PM.

- Check box not selected — each day the backup archives data from 8AM (beginning of schedule) to 11AM (time backup is scheduled to start) of that day.
- Check box is selected — each day the backup archives data from 11AM (time backup is scheduled to start) to 8PM (end of schedule) of the previous day and from 8AM (beginning of schedule) to 11AM (time of backup) of the current day.

Example 2:

A **Weekly** recurrence starting at 11AM on Tuesday, with a **Time Range** from 8AM to 8PM.

- Check box not selected — each Tuesday the backup archives data from 8AM (beginning of schedule) to 11AM (time backup is scheduled to start) of Tuesday.
- Check box is selected — each Tuesday the backup archives data from 11AM (time backup is scheduled to start) to 8PM (end of schedule) of Monday (the previous day) and from 8AM (beginning of schedule) to 11AM (time of backup) of Tuesday (the current day).

14 Select **Save**.

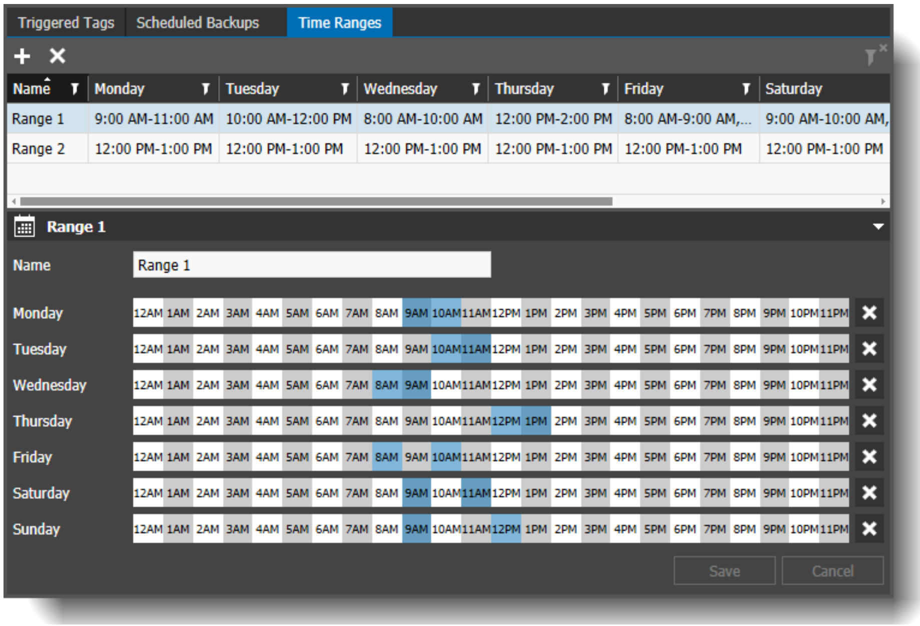
If the backup is set to active, it occurs when scheduled.

Configuring Time Ranges

You create time range schedules to determine when activities occur, such as when backups collect the data they are backing up.

Important: Only top-level users can view and edit all time ranges in the **Configuration > Time Ranges** tab (top-level users have full access to the root System tree and the root Logical tree, and the User Management right). Users without top-level access only view and edit their own time ranges.

You must set up at least one time range before you can create a scheduled backup.



Name	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Range 1	9:00 AM-11:00 AM	10:00 AM-12:00 PM	8:00 AM-10:00 AM	12:00 PM-2:00 PM	8:00 AM-9:00 AM,...	9:00 AM-10:00 AM,
Range 2	12:00 PM-1:00 PM	12:00 PM-1:00 PM	12:00 PM-1:00 PM	12:00 PM-1:00 PM	12:00 PM-1:00 PM	12:00 PM-1:00 PM

Name: Range 1

	12AM	1AM	2AM	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	10PM	11PM	
Monday										■	■														✕
Tuesday											■	■													✕
Wednesday									■	■															✕
Thursday													■	■											✕
Friday									■		■														✕
Saturday										■		■													✕
Sunday										■			■												✕

The following settings are listed for time ranges.

Option	Description
Name	Name for the time range.
Monday - Sunday	The time range (or ranges) for the selected day. Each day can have multiple time ranges, if desired.
Owner	The owner of the time range.

To set up time ranges

Note: At least one **Time Range** must be created before you can create a backup.

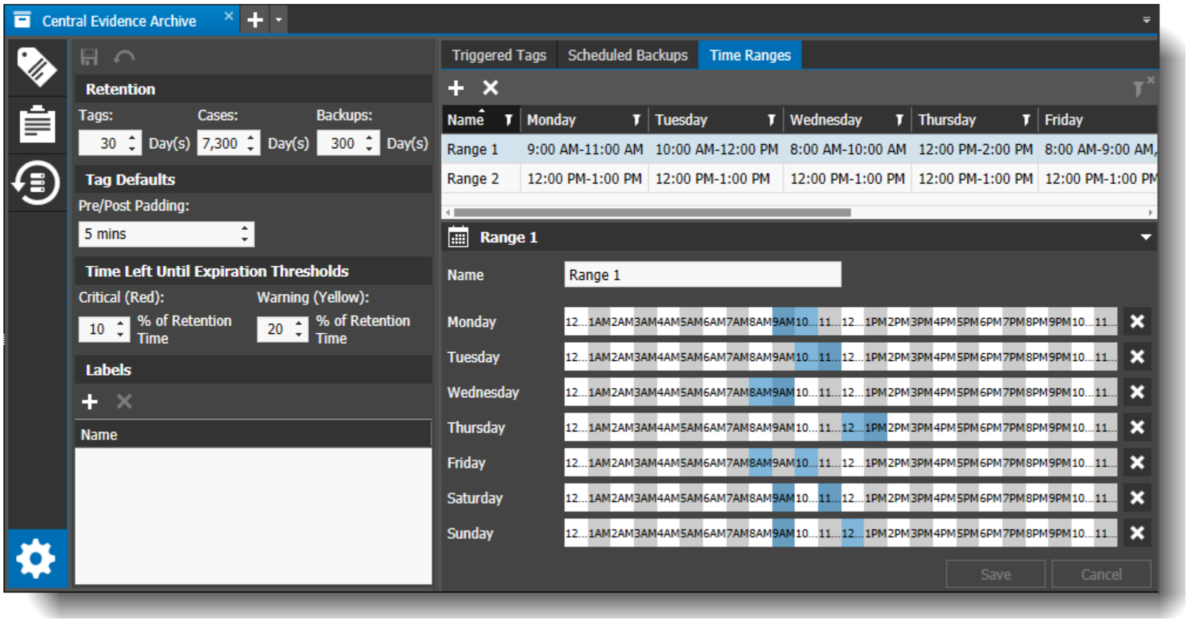
1 From the main menu button select **Central Evidence Archive**.

The Central Evidence Archive tab opens, with the Tags subtab open by default.

2 Select the **Configuration** ⚙ subtab.

The Configuration subtab opens.

3 At the right, select the **Time Ranges** tab.



Retention

Tags: 30 Day(s) Cases: 7,300 Day(s) Backups: 300 Day(s)

Tag Defaults

Pre/Post Padding: 5 mins

Time Left Until Expiration Thresholds

Critical (Red): 10 % of Retention Time

Warning (Yellow): 20 % of Retention Time

Labels

Name

Name	Monday	Tuesday	Wednesday	Thursday	Friday
Range 1	9:00 AM-11:00 AM	10:00 AM-12:00 PM	8:00 AM-10:00 AM	12:00 PM-2:00 PM	8:00 AM-9:00 AM,
Range 2	12:00 PM-1:00 PM	12:00 PM-1:00 PM	12:00 PM-1:00 PM	12:00 PM-1:00 PM	12:00 PM-1:00 PM

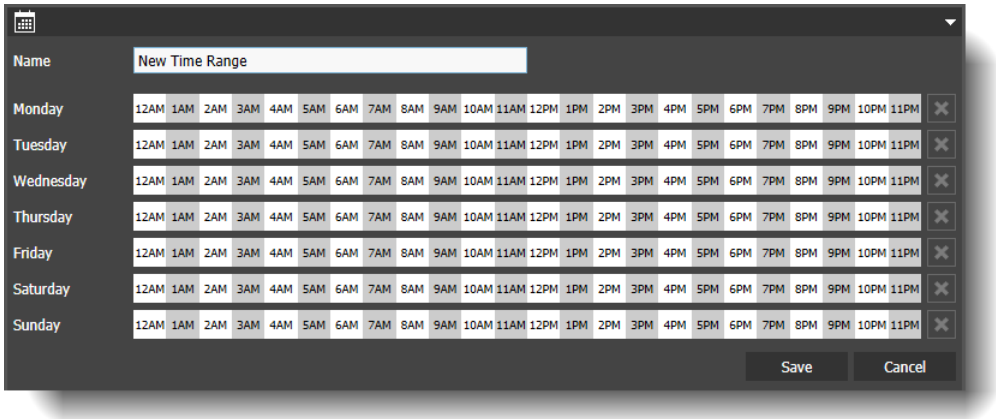
Range 1

Name: Range 1

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday: 12... 1AM 2AM 3AM 4AM 5AM 6AM 7AM 8AM 9AM 10... 11... 12... 1PM 2PM 3PM 4PM 5PM 6PM 7PM 8PM 9PM 10... 11...

4 In the **Time Ranges** tab, select the **Add Time Range** ✚ button.

The time range settings section (below the time range list) becomes available..



Name: New Time Range

Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday: 12AM 1AM 2AM 3AM 4AM 5AM 6AM 7AM 8AM 9AM 10AM 11AM 12PM 1PM 2PM 3PM 4PM 5PM 6PM 7PM 8PM 9PM 10PM 11PM

5 Enter a **Name** for the new time range.

6 For each day of the week, click to select the hours you want included in the schedule, or click and drag to highlight multiple hours.

Tip: Select the **Clear Time Range** ✖ button at the end of the row to remove the hour selections from a day.

7 When you have the desired hours highlighted, select **Save**.

The new time range is added to the list.

Note: You can edit a time range by selecting it in the list and changing the hours. You can also delete a time range by selecting it in the list and clicking **Remove Time Range** ✖ (a warning prompts you that removing the schedule may affect backups).

Chapter 3

Managing Tag, Case, and Backup Files

This chapter describes how to manage tags, cases, and backup files using the Central Evidence Archive.

Management of tag and case files does not require the Central Evidence Archive — you can create and manage manual tags and cases in Command Enterprise without the Central Evidence Archive.

You can only create triggered tags and scheduled backups when the Central Evidence Archive is installed. The Central Evidence Archive also provides a better way to search and filter all your tags, cases and backups, and it provides the ability to add labels to your files.

It contains the following topics:

- “Managing Tag Files” on page 38
- “Managing Case Files” on page 41
- “Managing Backup Files” on page 44
- “Adding a Label to a Tag, Case, or Backup” on page 56

Managing Tag Files

Tags are automatically triggered or manually generated video clips saved from an event or a user-defined point in time.

An automatically triggered tag is created when an event (such as an alarm) turns on or off (configured in the tag settings). By default, five minutes of pre and post padding time is added to the tag, so that the final tag video is ten minutes. (You can change the duration of the padding, as described in “Configuring General Settings for the Central Evidence Archive” on page 24.)

The Central Evidence Archive allows you to manage all your tag files in one area.

Managing Tags in Command Enterprise without the Command Evidence Archive

Manual tags can be created in Command Enterprise without the Central Evidence Archive. For more information about creating tags manually and managing tags in the Command Client, see the *Command Enterprise and Client User Guide.*

The following procedures are described in the *Command Enterprise and Client User Guide*:

- Adding a Tag File (manual tag file)
- Reviewing a Tag File
- Exporting a Tag File
- Sharing a Tag File with Other Users
- Changing the Owner of a Tag File
- Converting a Tag File to a Case File

Note: If the Central Evidence Archive is not installed, manual tags have a pre and post padding time of 5 minutes. When the Central Evidence Archive is installed, you can edit the padding duration, as described in “Configuring General Settings for the Central Evidence Archive” on page 24.

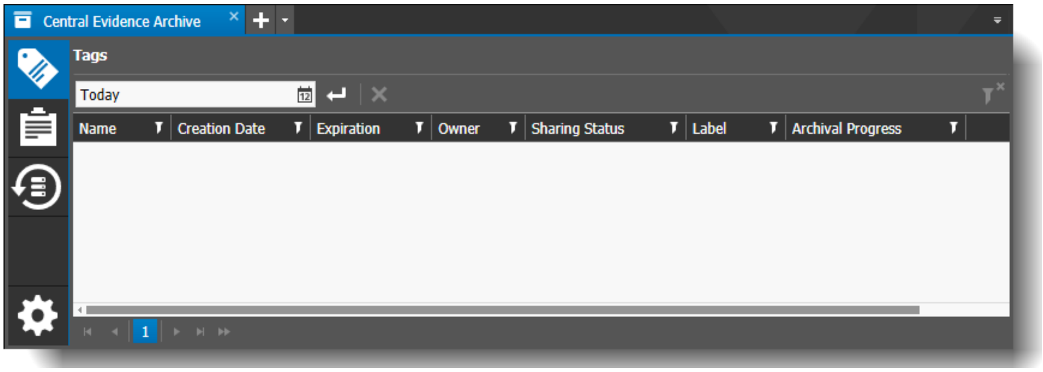
Searching for Tag Files using the Central Evidence Archive

You can search for manual and automatic tag files, filter them, and quickly view all the available tag file information using the Central Evidence Archive.

To search for tag files in the Central Evidence Archive

1 From the main menu button select **Central Evidence Archive**.

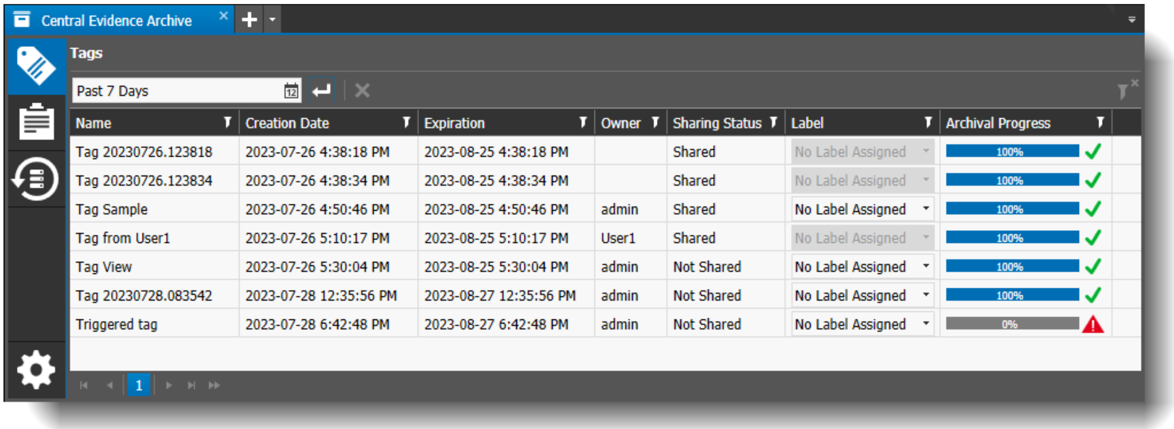
The Central Evidence Archive tab opens, with the **Tags** subtab open by default.



2 Select a time period from the list provided, or choose **Select Range** to open a calendar and set your own time period.

3 Select **Search**. ↵

The results of the search appear.

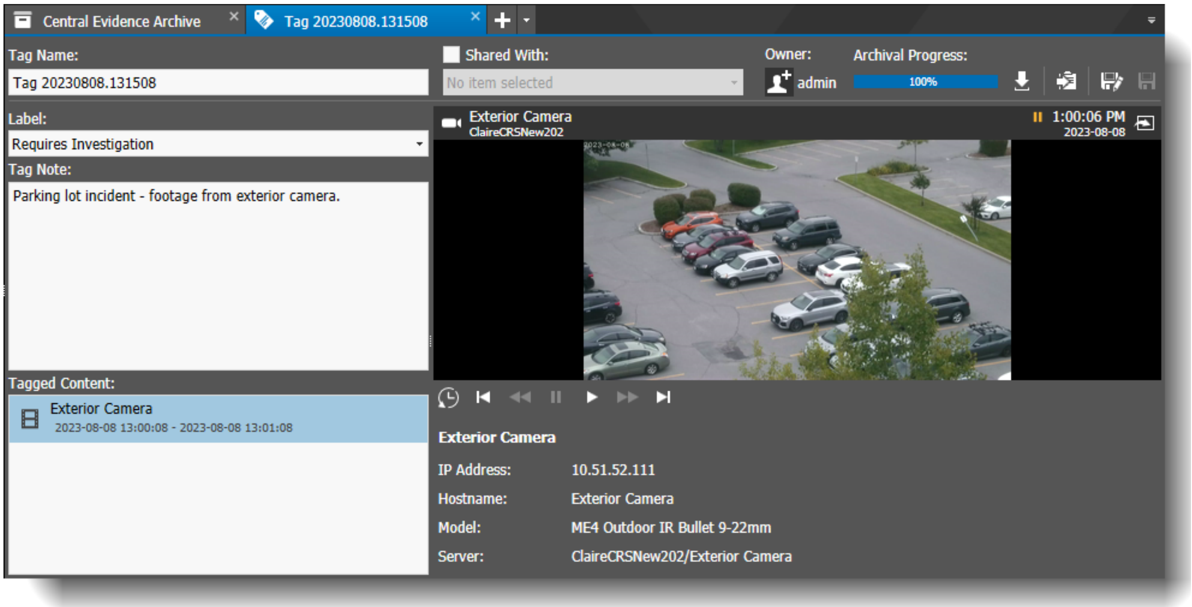


Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Tag 20230726.123818	2023-07-26 4:38:18 PM	2023-08-25 4:38:18 PM		Shared	No Label Assigned	100% ✓
Tag 20230726.123834	2023-07-26 4:38:34 PM	2023-08-25 4:38:34 PM		Shared	No Label Assigned	100% ✓
Tag Sample	2023-07-26 4:50:46 PM	2023-08-25 4:50:46 PM	admin	Shared	No Label Assigned	100% ✓
Tag from User1	2023-07-26 5:10:17 PM	2023-08-25 5:10:17 PM	User1	Shared	No Label Assigned	100% ✓
Tag View	2023-07-26 5:30:04 PM	2023-08-25 5:30:04 PM	admin	Not Shared	No Label Assigned	100% ✓
Tag 20230728.083542	2023-07-28 12:35:56 PM	2023-08-27 12:35:56 PM	admin	Not Shared	No Label Assigned	100% ✓
Triggered tag	2023-07-28 6:42:48 PM	2023-08-27 6:42:48 PM	admin	Not Shared	No Label Assigned	0% ⚠

The following settings are listed for tags.

Option	Description
Name	Name of the tag.
Creation Date	Date the tag was created.
Expiration	Date the tag expires and will be removed from the system.
Owner	Owner of the tag.
Sharing Status	Whether the tag is shared with any local groups or not.
Label	Any labels assigned to the tag. Labels are created in the CEA settings, see “Configuring General Settings for the Central Evidence Archive” on page 24. You can assign a label to a tag, see “Adding a Label to a Tag, Case, or Backup” on page 56.
Archival Progress	Shows the percent of the tag saved to the archiver. A symbol after the progress bar indicates the status: 100% ✓ **Success** - The tag is successfully saved to the archiver. 0% ✱ **Pending** - The save to the archiver is pending - waiting for resolution of an issue. The recorder may be offline, or no Media Archiver associated. 100% ⚠ **Warning** - The tag is saved but there may be an issue. Open the tag for more details. 0% ⚠ **Failed** - A problem has occurred and the tag is not saved to the archiver.

4 You can double-click to open any of the tags in the list and view them in more detail.



Tag Name: Tag 20230808.131508

☐ Shared With: No item selected

Owner: admin

Archival Progress: 100%

Label: Requires Investigation

Tag Note: Parking lot incident - footage from exterior camera.

Exterior Camera ClaireCRSNew202 1:00:06 PM 2023-08-08

Tagged Content: Exterior Camera 2023-08-08 13:00:08 - 2023-08-08 13:01:08

Exterior Camera

IP Address: 10.51.52.111

Hostname: Exterior Camera

Model: ME4 Outdoor IR Bullet 9-22mm

Server: ClaireCRSNew202/Exterior Camera

You can rename the tag, add a label, add notes, view the video, share the tag, export the tag, convert the tag to a case file, and save the tag.

For more information on tags, see the *Command Enterprise and Client User Guide.*

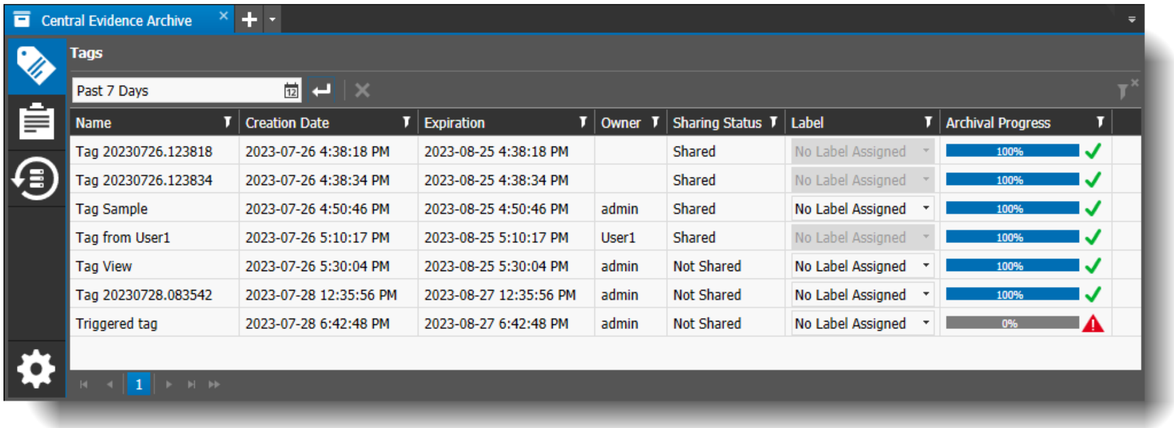
Deleting a Tag File using the Central Evidence Archive

Any user with the right to view a tag file can delete it (a user can view a tag file that they own, or one that is shared with them).

To delete a tag file in the Central Evidence Archive

1 Search for the tag file you want to delete, as described in “Searching for Tag Files using the Central Evidence Archive” on page 38.

The results of the search appear.



Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Tag 20230726.123818	2023-07-26 4:38:18 PM	2023-08-25 4:38:18 PM		Shared	No Label Assigned	100% ✓
Tag 20230726.123834	2023-07-26 4:38:34 PM	2023-08-25 4:38:34 PM		Shared	No Label Assigned	100% ✓
Tag Sample	2023-07-26 4:50:46 PM	2023-08-25 4:50:46 PM	admin	Shared	No Label Assigned	100% ✓
Tag from User1	2023-07-26 5:10:17 PM	2023-08-25 5:10:17 PM	User1	Shared	No Label Assigned	100% ✓
Tag View	2023-07-26 5:30:04 PM	2023-08-25 5:30:04 PM	admin	Not Shared	No Label Assigned	100% ✓
Tag 20230728.083542	2023-07-28 12:35:56 PM	2023-08-27 12:35:56 PM	admin	Not Shared	No Label Assigned	100% ✓
Triggered tag	2023-07-28 6:42:48 PM	2023-08-27 6:42:48 PM	admin	Not Shared	No Label Assigned	0% ⚠

2 Select the tag file in the list and select the **Delete Tag** ☒ button.

Managing Case Files

Cases are files that can include multiple video files, snapshots and notes, allowing you to organize your video evidence. A case file allows you to queue multiple files before exporting. The video files that you add to a case are exported from the recorder and saved on the Archiver, so that they are retained for a longer period of time than video on the recorder and are always available to you when you want to review the evidence in a case file.

The Central Evidence Archive allows you to manage all your case files in one area.

Managing Cases in Command Enterprise without the Command Evidence Archive

Case files can be created in Command Enterprise without the Central Evidence Archive. For more information about creating and managing case files, see the *Command Enterprise and Client User Guide.*

The following procedures are described in the *Command Enterprise and Client User Guide*:

- Creating a Case File from the Evidence Panel
- Reviewing the Contents of a Case File and Adding Notes
- Exporting a Case File
- Sharing a Case File with Other Users
- Changing the Owner of a Case File
- Deleting Selected Video from a Case File
- Viewing Available Space on the Media Archiver
- Ensuring the Media Archiver has Enough Space

Searching for Case Files using the Central Evidence Archive

You can search for case files, filter them, and quickly view all the available case file information using the Central Evidence Archive.

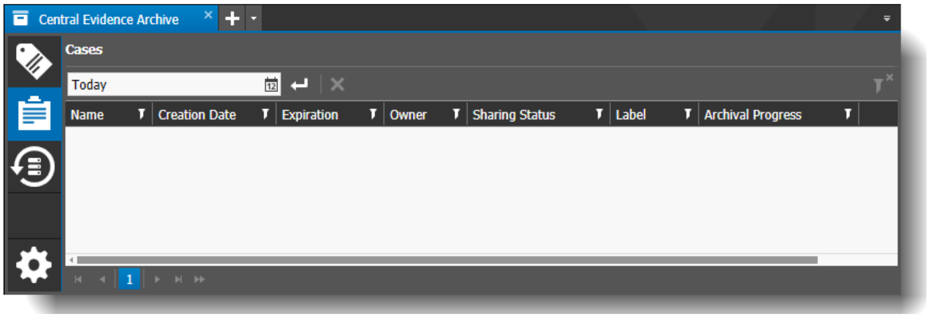
To search for case files in the Central Evidence Archive

1 From the main menu button select **Central Evidence Archive**.

The Central Evidence Archive tab opens, with the **Tags** subtab open by default.

2 Select the **Cases** subtab.

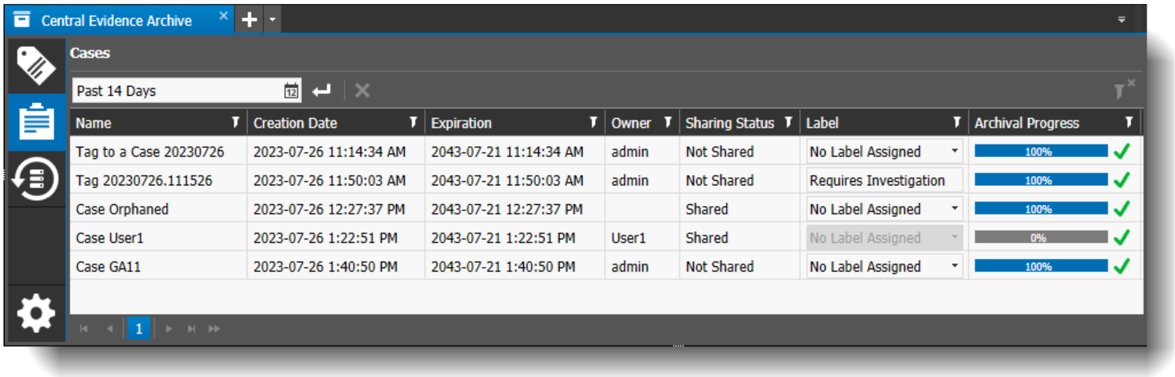
The Cases subtab opens.



3 Select a time period from the list provided, or choose **Select Range** to open a calendar and set your own time period.

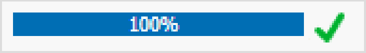
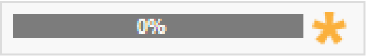
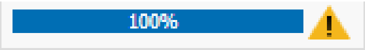
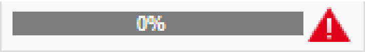
4 Select **Search**.

The results of the search appear.

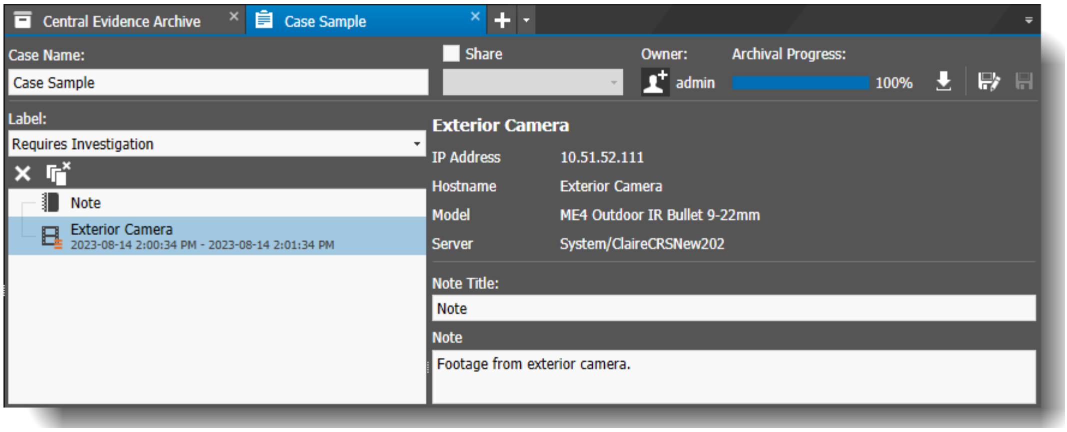


Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Tag to a Case 20230726	2023-07-26 11:14:34 AM	2043-07-21 11:14:34 AM	admin	Not Shared	No Label Assigned	100% ✓
Tag 20230726.111526	2023-07-26 11:50:03 AM	2043-07-21 11:50:03 AM	admin	Not Shared	Requires Investigation	100% ✓
Case Orphaned	2023-07-26 12:27:37 PM	2043-07-21 12:27:37 PM		Shared	No Label Assigned	100% ✓
Case User1	2023-07-26 1:22:51 PM	2043-07-21 1:22:51 PM	User1	Shared	No Label Assigned	0% ✓
Case GA11	2023-07-26 1:40:50 PM	2043-07-21 1:40:50 PM	admin	Not Shared	No Label Assigned	100% ✓

The following settings are listed for cases.

Option	Description
Name	Name of the case.
Creation Date	Date the case was created.
Expiration	Date the case expires and will be removed from the system.
Owner	Owner of the case.
Sharing Status	Whether the case is shared with any local groups or not.
Label	Any labels assigned to the case. Labels are created in the CEA settings, see “Configuring General Settings for the Central Evidence Archive” on page 24.
Archival Progress	Shows the percent of the case saved to the archiver. A symbol after the progress bar indicates the status:  **Success** - The case is successfully saved to the archiver.  **Pending** - The save to the archiver is pending - waiting for resolution of an issue. The recorder may be offline, or no Media Archiver associated.  **Warning** - The case is saved but there may be an issue. Open the tag for more details.  **Failed** - A problem has occurred and the case is not saved to the archiver.

5 You can double-click to open any of the cases in the list and view them in more detail.



Case Name: Case Sample

□ Share

Owner: admin

Archival Progress: 100%

Label: Requires Investigation

- Note
- Exterior Camera 2023-08-14 2:00:34 PM - 2023-08-14 2:01:34 PM

Exterior Camera

IP Address	10.51.52.111
Hostname	Exterior Camera
Model	ME4 Outdoor IR Bullet 9-22mm
Server	System/ClaireCRSNew202

Note Title: Note

Note: Footage from exterior camera.

You can rename the case, add a label, add notes, view the video, share the case, export the case, add evidence (video, snapshots) to the case, and save the case.

For more information on cases, see the *Command Enterprise and Client User Guide.*

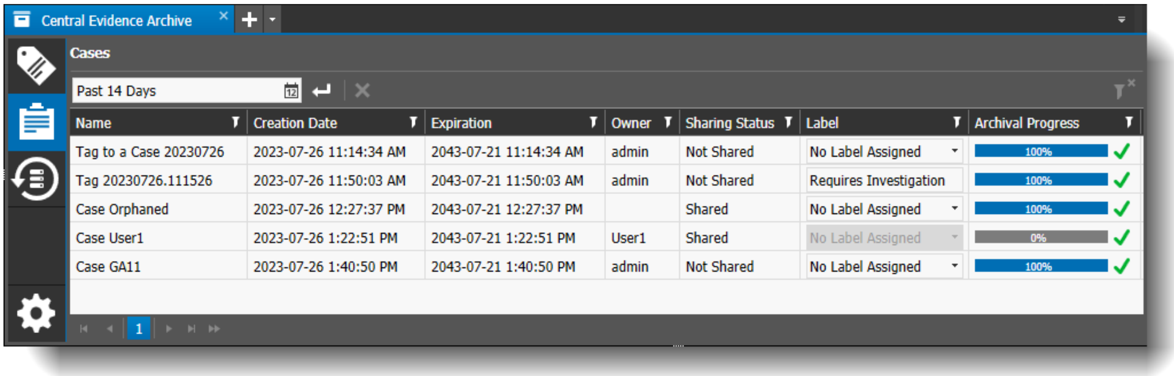
Deleting a Case File using the Central Evidence Archive

Any user with the right to view a case file can delete it (a user can view a case file that they own, or one that is shared with them).

To delete a case file in the Central Evidence Archive

1 Search for the case file you want to delete, as described in “Searching for Case Files using the Central Evidence Archive” on page 41.

The results of the search appear.



Past 14 Days

Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Tag to a Case 20230726	2023-07-26 11:14:34 AM	2043-07-21 11:14:34 AM	admin	Not Shared	No Label Assigned	100% ✓
Tag 20230726.111526	2023-07-26 11:50:03 AM	2043-07-21 11:50:03 AM	admin	Not Shared	Requires Investigation	100% ✓
Case Orphaned	2023-07-26 12:27:37 PM	2043-07-21 12:27:37 PM		Shared	No Label Assigned	100% ✓
Case User1	2023-07-26 1:22:51 PM	2043-07-21 1:22:51 PM	User1	Shared	No Label Assigned	0% ✓
Case GA11	2023-07-26 1:40:50 PM	2043-07-21 1:40:50 PM	admin	Not Shared	No Label Assigned	100% ✓

2 Select the case file in the list and select the **Delete Case** ☒ button.

Managing Backup Files

With the Central Evidence Archive, you can schedule backups for your recorders and cameras, as described in “Configuring Scheduled Backups” on page 31.

Important: Scheduled backup files are only available with the Central Evidence Archive installed. You cannot create or manage scheduled backup files without the Central Evidence Archive.

The following procedures for backup files are described in this section:

- “Searching for Backup Files” on page 44
- “Reviewing a Backup File” on page 46
- “Exporting a Backup File” on page 49
- “Sharing a Backup File with Other Users” on page 52
- “Changing the Owner of a Backup File” on page 53
- “Converting a Backup File to a Case File” on page 54
- “Deleting a Backup File” on page 55

Searching for Backup Files

You can search for backup files, filter them, and quickly view all the available backup file information using the Central Evidence Archive.

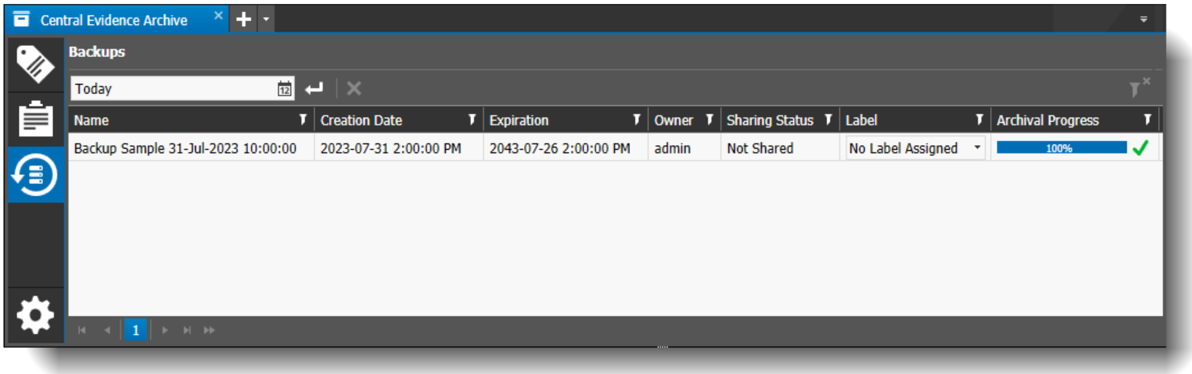
To search for backup files

1 From the main menu button select **Central Evidence Archive**.

The Central Evidence Archive tab opens, with the **Tags** subtab open by default.

2 Select the **Backups** subtab.

The Backups subtab opens.

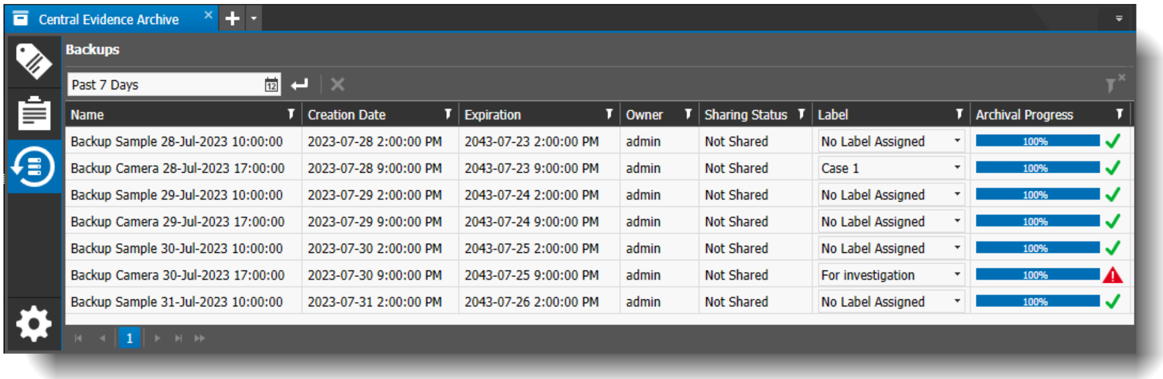


Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Backup Sample 31-Jul-2023 10:00:00	2023-07-31 2:00:00 PM	2043-07-26 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓

3 Select a time period from the list provided, or choose **Select Range** to open a calendar and set your own time period.

4 Select **Search**. ↵

The results of the search appear.



Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Backup Sample 28-Jul-2023 10:00:00	2023-07-28 2:00:00 PM	2043-07-23 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Camera 28-Jul-2023 17:00:00	2023-07-28 9:00:00 PM	2043-07-23 9:00:00 PM	admin	Not Shared	Case 1	100% ✓
Backup Sample 29-Jul-2023 10:00:00	2023-07-29 2:00:00 PM	2043-07-24 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Camera 29-Jul-2023 17:00:00	2023-07-29 9:00:00 PM	2043-07-24 9:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Sample 30-Jul-2023 10:00:00	2023-07-30 2:00:00 PM	2043-07-25 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Camera 30-Jul-2023 17:00:00	2023-07-30 9:00:00 PM	2043-07-25 9:00:00 PM	admin	Not Shared	For investigation	100% ⚠
Backup Sample 31-Jul-2023 10:00:00	2023-07-31 2:00:00 PM	2043-07-26 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓

The following settings are listed for backups.

Option	Description
Name	Name of the backup.
Creation Date	Date the backup was created.
Expiration	Date the backup expires and will be removed from the system.
Owner	Owner of the backup.
Sharing Status	Whether the backup is shared with any local groups or not.
Label	Any labels assigned to the backup. Labels are created in the CEA settings, see “Configuring General Settings for the Central Evidence Archive” on page 24.
Archival Progress	Shows the percent of the backup saved to the archiver. A symbol after the progress bar indicates the status: 100% ✓ — **Success** - The backup is successfully saved to the archiver. 0% ✱ — **Pending** - The save to the archiver is pending - waiting for resolution of an issue. The recorder may be offline, or no Media Archiver associated. 100% ⚠ — **Warning** - The backup is saved but there may be an issue. Open the backup for more details. 0% ⚠ — **Failed** - A problem has occurred and the backup is not saved to the archiver.

5 You can use the labels and column filters ⊤ to refine your search.

6 You can double-click to open any of the backups in the list and view them in more detail, as described in the next section.

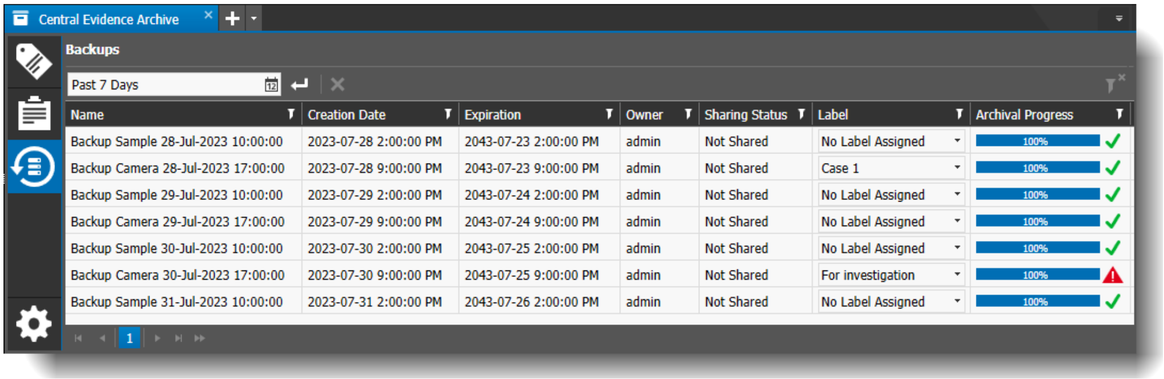
Reviewing a Backup File

Once backup files have been created, you can view the associated video and add notes to the file.

To review a backup file

1 Search for the backup file you want to review, as described in “Searching for Backup Files” on page 44.

The results of the search appear.

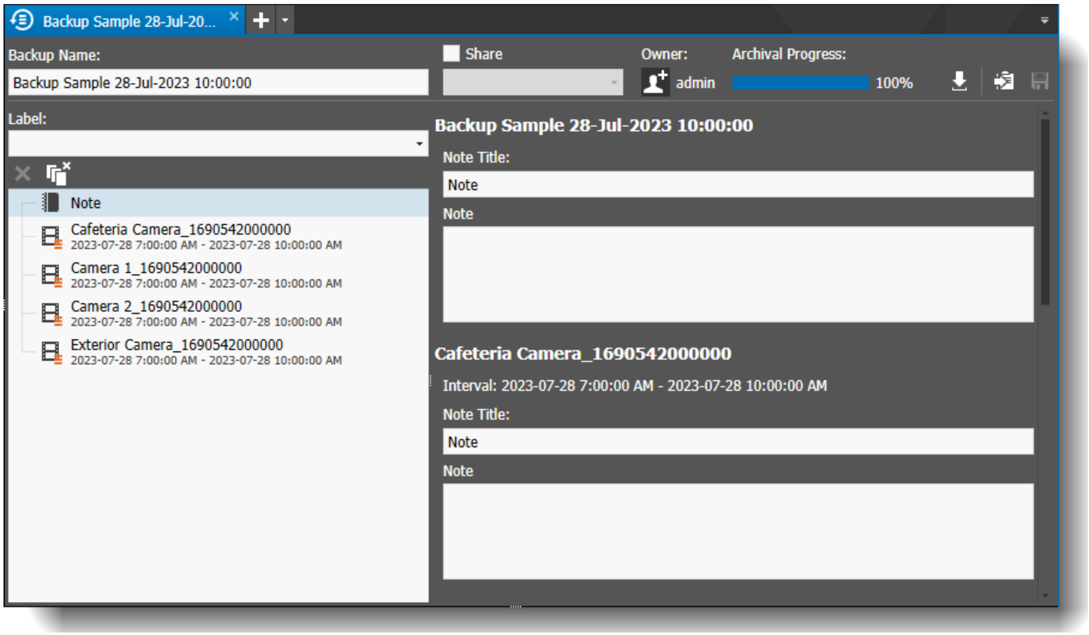


Past 7 Days

Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Backup Sample 28-Jul-2023 10:00:00	2023-07-28 2:00:00 PM	2043-07-23 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Camera 28-Jul-2023 17:00:00	2023-07-28 9:00:00 PM	2043-07-23 9:00:00 PM	admin	Not Shared	Case 1	100% ✓
Backup Sample 29-Jul-2023 10:00:00	2023-07-29 2:00:00 PM	2043-07-24 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Camera 29-Jul-2023 17:00:00	2023-07-29 9:00:00 PM	2043-07-24 9:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Sample 30-Jul-2023 10:00:00	2023-07-30 2:00:00 PM	2043-07-25 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Camera 30-Jul-2023 17:00:00	2023-07-30 9:00:00 PM	2043-07-25 9:00:00 PM	admin	Not Shared	For investigation	100% ⚠
Backup Sample 31-Jul-2023 10:00:00	2023-07-31 2:00:00 PM	2043-07-26 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓

2 To open a backup file, select the backup from the list, right-click and select **Open**, or double-click.

The backup file opens in the workspace.



Backup Name: Backup Sample 28-Jul-2023 10:00:00

□ Share

Owner: admin

Archival Progress: 100%

Label:

- Note
- Cafeteria Camera_1690542000000
  2023-07-28 7:00:00 AM - 2023-07-28 10:00:00 AM
- Camera 1_1690542000000
  2023-07-28 7:00:00 AM - 2023-07-28 10:00:00 AM
- Camera 2_1690542000000
  2023-07-28 7:00:00 AM - 2023-07-28 10:00:00 AM
- Exterior Camera_1690542000000
  2023-07-28 7:00:00 AM - 2023-07-28 10:00:00 AM

Backup Sample 28-Jul-2023 10:00:00

Note Title: Note

Note

Cafeteria Camera_1690542000000

Interval: 2023-07-28 7:00:00 AM - 2023-07-28 10:00:00 AM

Note Title: Note

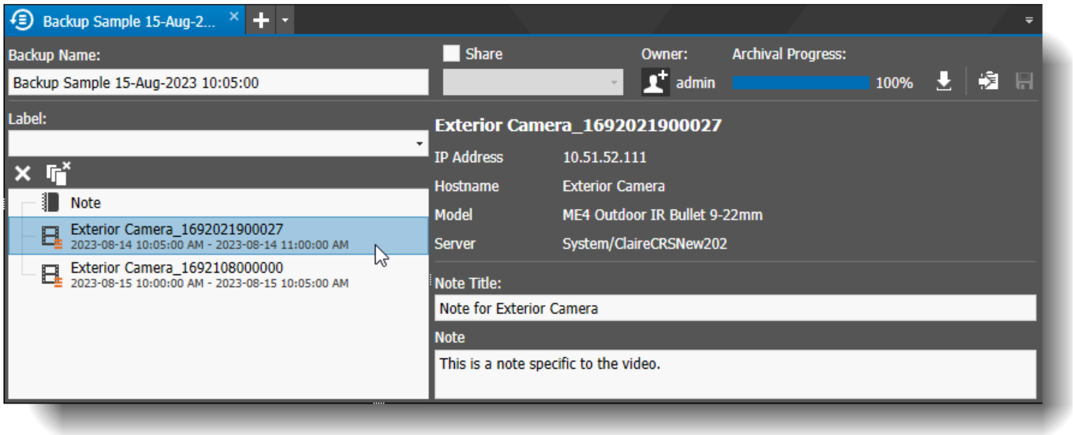
Note

A backup tab contains a list of the video files in the left panel, and displays the file details and notes in the right panel. You can add a note about the backup in general, or notes for each specific video file.

Tip: When you select the general backup note at the top of the list, all the notes for the backup are displayed in the right panel.

3 You can click on the name of a video file to see the information stored about the video file. At the bottom are boxes for the note to go with that video file. You can enter a note title and content to add information about the video to the backup.

Tip: You can double-click on the name of a video file to open and play the video in a new tab.



Backup Sample 15-Aug-2...

Backup Name: Backup Sample 15-Aug-2023 10:05:00

□ Share

Owner: admin

Archival Progress: 100%

Label:

Note

Exterior Camera_1692021900027
2023-08-14 10:05:00 AM - 2023-08-14 11:00:00 AM

Exterior Camera_1692108000000
2023-08-15 10:00:00 AM - 2023-08-15 10:05:00 AM

Exterior Camera_1692021900027

IP Address	10.51.52.111
Hostname	Exterior Camera
Model	ME4 Outdoor IR Bullet 9-22mm
Server	System/ClaireCRSNew202

Note Title: Note for Exterior Camera

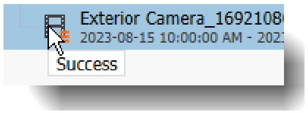
Note

This is a note specific to the video.

When a video file is added to a backup, the video is downloaded from the recorder and saved on the Archiver. This ensures that the video is available to the backup file even if the recorder is offline, and the video is retained as long as the backup file, not lost if the retention settings on the recorder purge it. The **Archival Progress** bar shows the percent completion of this process.

When a video file is saved to the Archiver, a symbol appears on the video icon in the backup file, to indicate the status of the save to the Archiver, as described in the following table.

Note: Tooltip text also appears when you move your mouse over the black part of the video icon.



Exterior Camera_1692108
2023-08-15 10:00:00 AM - 202

Success

Icon	Description
🎞≡	**Success** The video file including all data is successfully saved to the Archiver.
🎞⚠	**Success, missing some data** The video file is saved to the Archiver, but there is some data missing, for example, the video is saved but the audio information is missing, or there are gaps in the video.
🎞▲	**No data available** The video file is saved to the Archiver, but there is no data.
🎞✖	**Failed**, **Failed (local storage)**, or **Failed (timeout)** The video file is not saved to the Archiver, the save has failed. If the tool tip indicates local storage, the operation to save the video to the Archiver failed because the storage on the archiver is full. See the *Command Enterprise and Client User Guide* for tips on ensuring that the Archiver has enough space. If the tool tip indicates timeout, the operation to save the video to the Archiver timed out before it could be completed.

Icon	Description
🎞	**No Archiver available** The video file is saved to the backup file, but not to an Archiver. If your Command system is not using an Archiver, the video file icon does not show any additional symbols. In this situation, when playing back the video added to the backup, the system retrieves the video file from the recorder instead of an Archiver.

4 You can enter a different name for the backup in the **Backup Name** box. This is the name that the CME file is assigned if you export the backup file.

For example, if you enter “Sample Backup 1”, the file is saved as “Sample Backup 1.cme”.

5 You can remove:

- A video from the backup by selecting the file in the evidence list and clicking the **Remove Selected Items** ✕ button.
- All the files from the backup by clicking the **Remove All Items** button.

6 Select **Save** 💾.

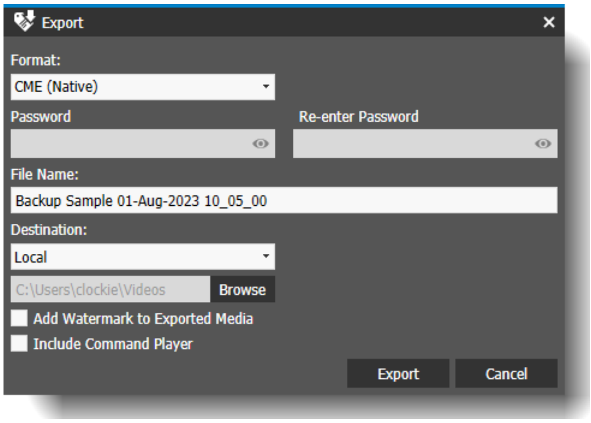
Exporting a Backup File

When you are finished reviewing and editing the backup file, you can export it to a folder location or removable media (such as a USB drive) so that you can distribute the evidence file to investigators, authorities, or whoever needs to see it.

To export a backup file

1 Open the Backup tab in the workspace, and select the **Export to file** button.

The **Export** dialog box appears.



Export

Format: CME (Native)

Password

Re-enter Password

File Name: Backup Sample 01-Aug-2023 10_05_00

Destination: Local

C:\Users\clockie\Videos Browse

□ Add Watermark to Exported Media

□ Include Command Player

Export Cancel

2 From the **Format** drop-down list, select the file type:

- **CME (Native)**: Command Multimedia Evidence. This is a March Networks proprietary video file format which can only be played using the Command Player. The fact that this file format can only be viewed using the Command Player ensures that sensitive video evidence cannot be easily shared over the Internet or posted for public view.
- **CME (Encrypted)**: Command Multimedia Evidence. This the same as the CME Native format, but it is in an encrypted format, so that a password is required to play it.
  If you select this option, you must specify a password that the end user must enter to play the video after it is exported.
- **PDF:** If you select this option, you can download the notes, but video files are not included. Video files are represented in the PDF as a single image with text details such as start time, end time, recorder name, and camera name.

3 If you selected the CME (Encrypted) format type, enter and re-enter a **Password** for the exported video file. The exported video remains encrypted and the end user cannot view the file until they enter the password that you specify here.

Note: Click the eye icon to display the characters of the password in the dialog instead of the password masking dots.

4 If you selected the CME (Native or Encrypted) format type, you can change the name of the file in the **File Name** box.

5 From the **Destination** drop-down list select from:

- **Local** — The path to the local folder where you want to save your video. For example, C:\Users\<*username*>\Videos.

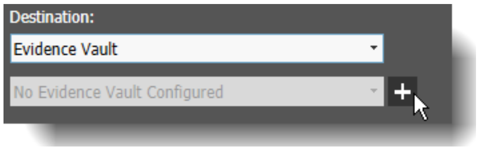
  Click the **Browse** button to select a different folder. You can browse to a local folder on the computer or a removable drive, for example, a USB drive. If you change the local folder destination, the system remembers the new location the next time (per user).

  Note: To save to a CD or a DVD, select the CD/DVD drive option button (described below).

The option button allows Command to manage the CD/DVD burning procedure. Browsing to the CD or DVD drive is not recommended.

- **CD/DVD drive** — Enables a drop-down list of the available CD and/or DVD drives, if available. You can burn to a CD or DVD if you select an available RW Drive or connected burner. For the CD/DVD burning procedure, see the *Command Enterprise and Client User Guide*.

  Note: You cannot save a backup file saved as PDF to the CD/DVD drive.
- **Evidence Vault** — Export your backup file to the cloud-based Evidence Vault application, accessible through Command Client. You can then share the backup file with external users, who can log in and download the backup file from the Evidence Vault through a web browser.
  - If one or more vaults are available, select the name of the Evidence Vault you want to export to, from the list of vaults that appears.
  - If there are no Evidence Vaults added to Command Client yet, you can click the **Add Evidence Vault** ➕ button to add one.

    Destination:

    Evidence Vault

    No Evidence Vault Configured

    The Add New Evidence Vault dialog appears for you to add a vault, as described in the *Command Enterprise and Client User Guide*. After adding the vault you can return to the Export dialog. The newly added vault is selected.

  For more information about Evidence Vaults, see the *Evidence Vault User Guide*, available from the March Networks Partner Portal website.

6 If you want to apply a watermark over the video and/or snapshots in the exported backup file, select the **Add Watermark to Exported Media** check box.

If you selected the PDF export option, the watermark is applied over the snapshot and video images in the PDF.

The appearance of the watermark is configured on the Command Enterprise Software server. You cannot modify it in Command Client.

Note: This check box only appears if your user profile has the Watermark General Right set to Optional (see “Watermark” on page 90).

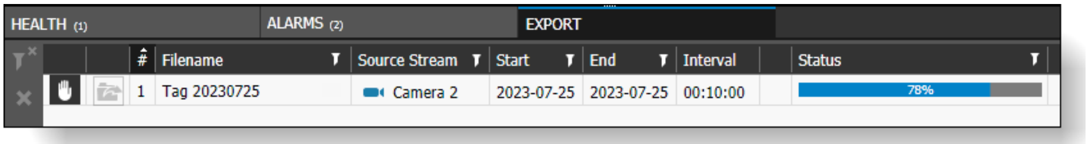
7 If you selected the CME (Native or Encrypted) format type and you want to include the executable file for the portable Command Player with the exported file, select the **Include Command Player** check box.

Command Player is a playback tool that allows others to view video, snapshots, notes, tags and case files in the proprietary CME format.

8 Click **Export**.

The result of the export depends on the format type and destination you selected:

- If you selected the CME format type and saved to a local folder or an Evidence Vault, you can view the progress of the export by clicking the **Export** tab in the dashboard.

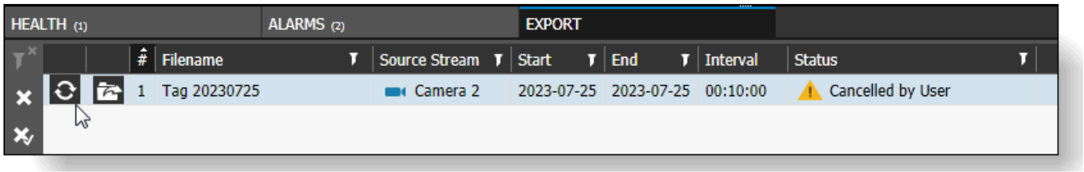


#	Filename	Source Stream	Start	End	Interval	Status
1	Tag 20230725	Camera 2	2023-07-25	2023-07-25	00:10:00	78%

The CME file is saved to the **Local** folder you selected or to the **Evidence Vault** you selected in the destination section of the export dialog. You can open the Evidence Vault in Command Client and view/share the exported files.

If you saved to a **CD/DVD drive**, see the *Command Enterprise and Client User Guide* for details on how to burn a CD/DVD in Command.

Tip: To stop the export while still in progress, click the **Cancel Video Export** button. The file in progress is deleted. Click **Restart Video Export** to begin the export again.



#	Filename	Source Stream	Start	End	Interval	Status
1	Tag 20230725	Camera 2	2023-07-25	2023-07-25	00:10:00	Cancelled by User

- If you selected the PDF format type and saved to a local folder on the computer, a **Save As** window opens. Browse to the location where you want to save the PDF file, enter a file name for the PDF, and click **Save**.
  The PDF file is saved to the location you selected in the Save As window.
- If you selected the PDF format type and saved to an Evidence Vault, the file is saved to the selected Evidence Vault. You can open the Evidence Vault in Command Client and view the exported PDF.

Note: If you are using Windows 10 or 11 with Controlled Folder Access enabled, you may get a warning or be prevented from saving a backup file to the default Windows Videos folder. If this occurs, you can configure Windows to “Allow an app through Controlled folder access” in Windows settings. When you add the CommandClient.exe as an allowed app, you are able to save Command Client files to Windows protected folders.

9 After the video clip is successfully exported, you can click the **Close Export Video** button to remove the entry from the **Dashboard**.

Depending on the selected destination, successfully exported files are available:

- in the local folder (select the **Open Export Destination** button or double-click the table row to open the folder on your computer)
- on the CD/DVD (see the *Command Enterprise and Client User Guide* for details)
- in the selected Evidence Vault - (select the **Open Export Destination** button or double-click the table row to open the Evidence Vault in Command Client and view/share the exported files (see the *Command Enterprise and Client User Guide* for more information)

Note: Entries in the **Export** panel are cleared when you log out of Command Client.

Sharing a Backup File with Other Users

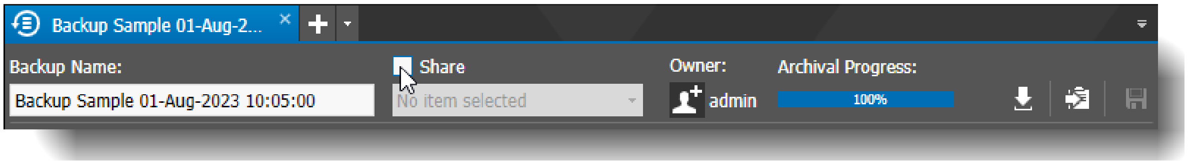
You can choose to share a backup file with other users so that they can view, edit, and export the information in the backup.

When you share a backup, other selected users can access the backup, but only other top-level users you share with can edit the sharing by adding or removing local groups or change the owner (top-level users have full access to the root System tree and the root Logical tree, and the User Management right).

Important: Before you can share a backup file, you must have some local user groups available to share the backup with. Local groups are set up in the **User Management > Local Groups** tab. Only groups that you are a member of are available for you to share with. For instructions on setting up local groups, see the *Command Enterprise and Client User Guide.*

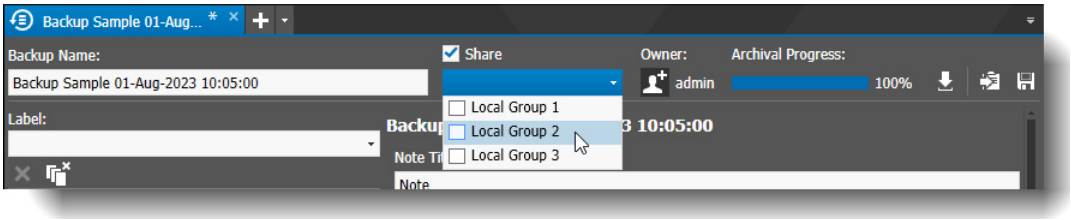
To share a backup file

1 Open the Backup tab in the workspace, and select the **Share** check box.



Note: If there are no local user groups available, the **Share** check box is not available. Local groups are set up in the **User Management > Local Groups** tab. Only groups that you are a member of are available for you to share with. See the *Command Enterprise and Client User Guide* for instructions on creating local groups.

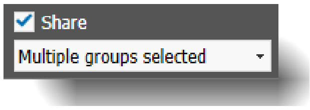
2 Select the field under the **Share** check box to view the list of available groups.



3 Select the group or groups you want to share the backup with.

Note: This list only contains groups that you are a member of.

If you select one group, the name of the group is displayed. If you select more than one group, “**Multiple groups selected**” is displayed.



4 Select **Save** 🖫.

When a backup is shared, the **Sharing Status** column in the Central Evidence Archive changes to show that the file is shared.

When a member of the Local Group opens a shared backup, if that user is not the creator/ owner of the backup, they can view and export the backup information, but they must be a top-level user to share the backup or set the backup to private (the **Share** check box and group list is unavailable unless they are a top-level user).

Changing the Owner of a Backup File

If you are a top-level user (top-level users have full global access to the root System folder and the root Logical folder, and the User Management right), you can change the owner of a backup file.

If the backup file is shared, only users that belong to a shared Local Group are available to re-assign it to. If it is not shared, you can re-assign it to any eligible user, but you will not be able to view the backup file after you change the owner.

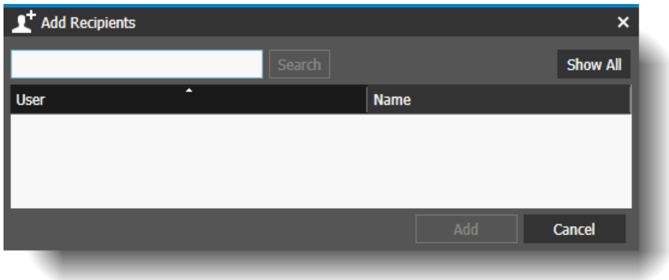
To change the owner of a backup file

1 As a top-level user, from the **Evidence** panel, open a backup file in a tab by selecting the backup from the list and clicking the **Open in Tab** button (or right-click and select **Open,** or double-click the backup name).

The backup management tab opens.

2 Select the Re-assign button. If the backup file is shared, only users that belong to a shared Local Group are available to re-assign it to. If it is not shared, you can re-assign it to any eligible user, but you will not be able to see it after you change the owner.

The **Add Recipients** dialog appears.



3 Do one of the following:

- To view a complete list of all eligible recipients, select **Show All**.
- To search for a specific recipient, type a portion of the user name and select **Search**.

The users that fit the search criteria appear in the list.

4 From the list, select the user that you want to re-assign the backup file to, and click **Add**.

The new user is now displayed as the owner of the backup file.

Note: Ensure that the user you assign the backup file to has the Central Evidence Archive **View Backups** application right, or they will not be able to see the backup file (See “Adding the Central Evidence Archive Application Rights to the User Profile” on page 12).

5 Click **Save** .

If the backup file is not shared, a warning informs you that you will not be able to access the backup anymore. The backup is removed from your backup list and only the new owner can access it.

If the backup file is shared, the backup is saved with the new owner, but is still available for you to access in the backup list.

Converting a Backup File to a Case File

You can convert your backup file to a case file. You can add more video and snapshot evidence to a case file.

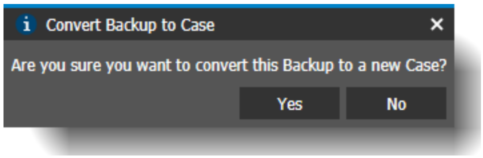
Any user with the right to view a backup file can convert it to a case file (a user can view a backup file that they own, or one that is shared with them).

Important: When you convert a backup file to a case file, the backup file is removed from the list of backups. You cannot convert the new case file back to a backup file. Any user that the backup file is shared with can convert it to a case.

To convert a backup file to a case file

1 To convert the backup file, on the Backup management tab, click the **Convert to Case** button.

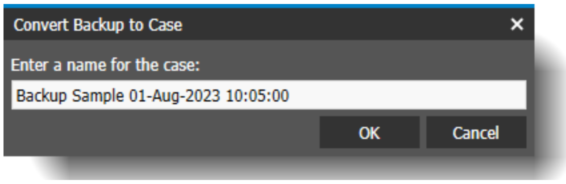
The initial dialog appears, to ensure that you want to convert the backup to a case.



Are you sure you want to convert this Backup to a new Case?

2 Select **Yes**.

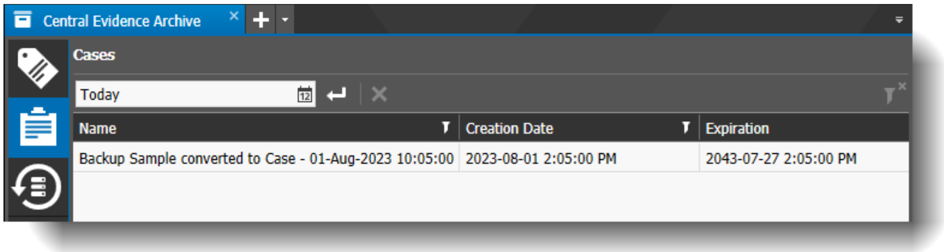
The second **Convert Backup to Case** dialog appears, where you can enter a new name for the file, if desired.



Enter a name for the case: Backup Sample 01-Aug-2023 10:05:00

3 Select **OK**.

In the Central Evidence Archive, the backup file is removed from the list of **Backups**, and appears in the list of **Cases**.



Name	Creation Date	Expiration
Backup Sample converted to Case - 01-Aug-2023 10:05:00	2023-08-01 2:05:00 PM	2043-07-27 2:05:00 PM

4 You can now manage the case as desired (see “Managing Case Files” on page 41).

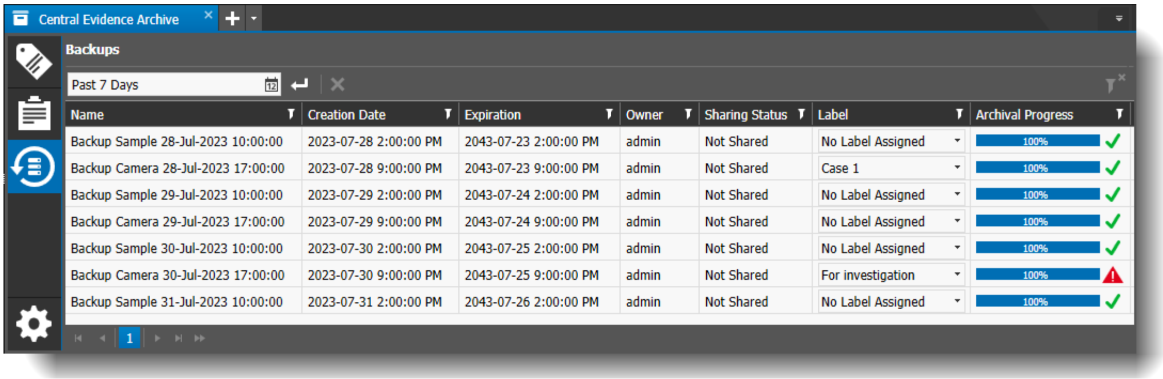
Deleting a Backup File

Any user with the right to view a backup file can delete it (a user can view a backup file that they own, or one that is shared with them).

To delete a backup file

1 Search for the backup file you want to delete, as described in “Searching for Backup Files” on page 44.

The results of the search appear.



Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Backup Sample 28-Jul-2023 10:00:00	2023-07-28 2:00:00 PM	2043-07-23 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Camera 28-Jul-2023 17:00:00	2023-07-28 9:00:00 PM	2043-07-23 9:00:00 PM	admin	Not Shared	Case 1	100% ✓
Backup Sample 29-Jul-2023 10:00:00	2023-07-29 2:00:00 PM	2043-07-24 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Camera 29-Jul-2023 17:00:00	2023-07-29 9:00:00 PM	2043-07-24 9:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Sample 30-Jul-2023 10:00:00	2023-07-30 2:00:00 PM	2043-07-25 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓
Backup Camera 30-Jul-2023 17:00:00	2023-07-30 9:00:00 PM	2043-07-25 9:00:00 PM	admin	Not Shared	For investigation	100% ⚠
Backup Sample 31-Jul-2023 10:00:00	2023-07-31 2:00:00 PM	2043-07-26 2:00:00 PM	admin	Not Shared	No Label Assigned	100% ✓

2 Select the backup file in the list and select the **Delete Backup** ☒ button.

Adding a Label to a Tag, Case, or Backup

The Central Evidence Archive allows you to add labels to your tags, cases and backup files.

Labels help you to organize and filter the files you want to manage.

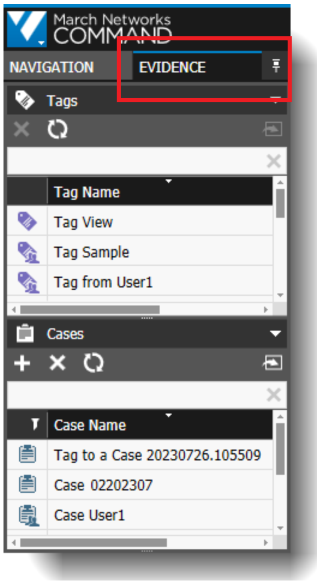
Notes:

- Before you can add a label to a tag, case, or backup file, one or more labels must have been created in the Central Evidence Archive. To create labels, see “Configuring General Settings for the Central Evidence Archive” on page 24.
- You can only add one label at a time to a tag, case, or backup file.

Adding a label

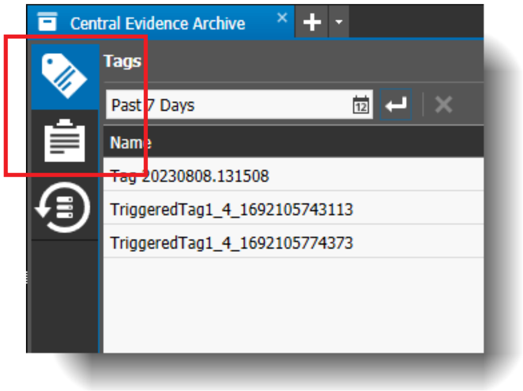
1 Find the file you want to add a label to.

- You can find **Tags** and **Cases** in the Evidence Panel, or in the Central Evidence Archive tab (see “Managing Tag Files” on page 38 and “Managing Case Files” on page 41).



Tag Name
Tag View
Tag Sample
Tag from User1

Case Name
Tag to a Case 20230726.105509
Case 02202307
Case User1

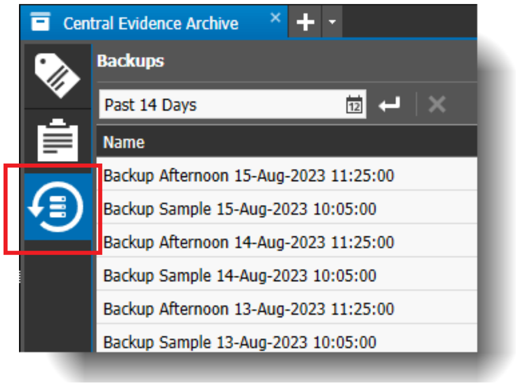


Name
Tag 20230808.131508
TriggeredTag1_4_1692105743113
TriggeredTag1_4_1692105774373

Tags and Cases in
Central Evidence Archive

Tags and Cases
in Evidence Panel

- You can find **Backups** in the Central Evidence Archive tab (see “Managing Backup Files” on page 44).

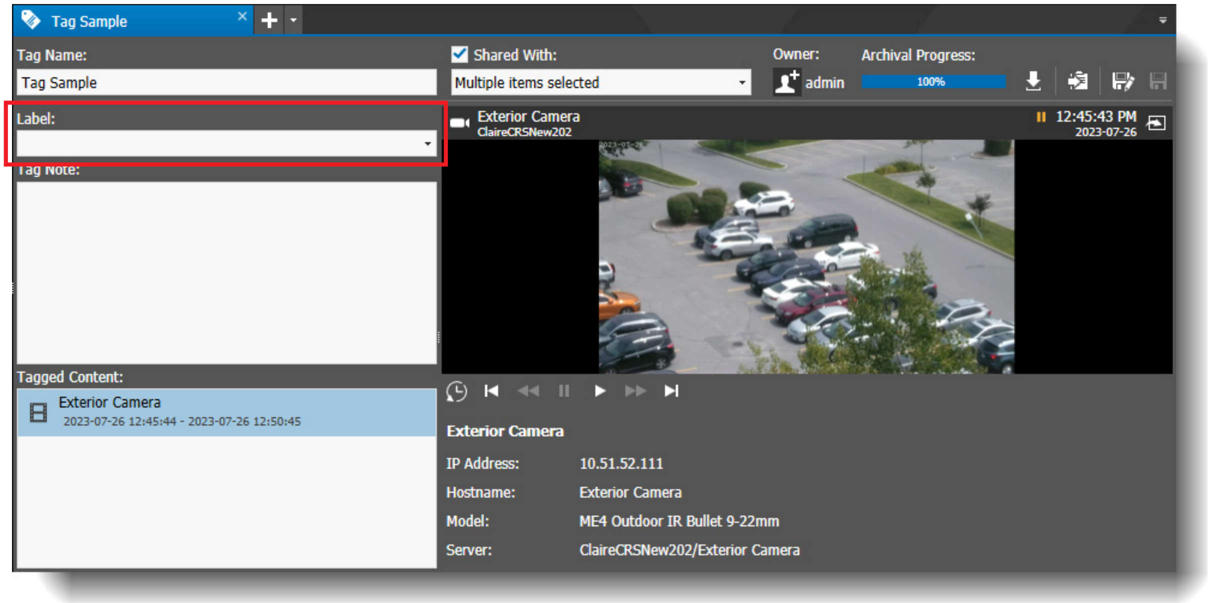


Name
Backup Afternoon 15-Aug-2023 11:25:00
Backup Sample 15-Aug-2023 10:05:00
Backup Afternoon 14-Aug-2023 11:25:00
Backup Sample 14-Aug-2023 10:05:00
Backup Afternoon 13-Aug-2023 11:25:00
Backup Sample 13-Aug-2023 10:05:00

Backup files in
Central Evidence Archive

2 You can add a label by opening the tag, case, or backup file in the workspace of the Command Client by double-clicking a tag or case in the Evidence Panel or double-clicking a tag or case, or backup in the Central Evidence Archive tab.

The file opens in the workspace.



Tag Name: Tag Sample

☑ Shared With: Multiple items selected

Owner: admin

Archival Progress: 100%

Label:

Tag Note:

Tagged Content: Exterior Camera 2023-07-26 12:45:44 - 2023-07-26 12:50:45

Exterior Camera ClaireCRSNew202 12:45:43 PM 2023-07-26

Exterior Camera

IP Address: 10.51.52.111

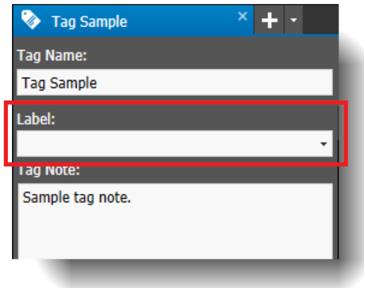
Hostname: Exterior Camera

Model: ME4 Outdoor IR Bullet 9-22mm

Server: ClaireCRSNew202/Exterior Camera

When the Central Evidence Archive is present in Command Enterprise, the label option appears for tag, case, and backup files.

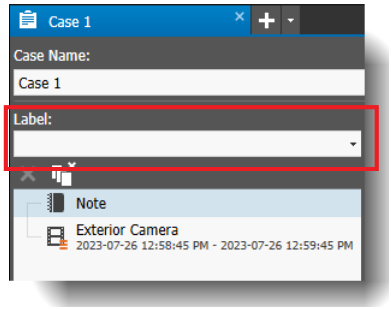
Note: If the Central Evidence Archive is not installed, the Label option is not available.



Tag Name: Tag Sample

Label:

Tag Note: Sample tag note.

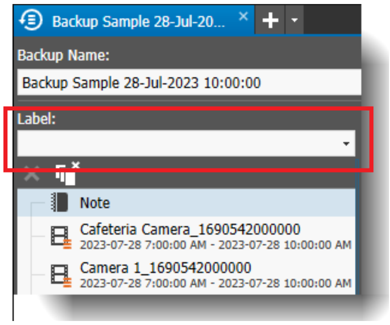


Case Name: Case 1

Label:

Note

Exterior Camera 2023-07-26 12:58:45 PM - 2023-07-26 12:59:45 PM



Backup Name: Backup Sample 28-Jul-2023 10:00:00

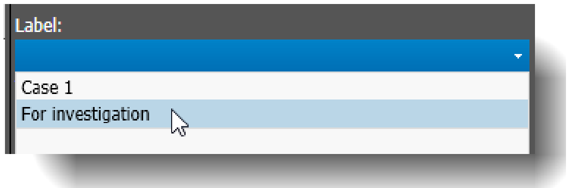
Label:

Note

Cafeteria Camera_1690542000000 2023-07-28 7:00:00 AM - 2023-07-28 10:00:00 AM

Camera 1_1690542000000 2023-07-28 7:00:00 AM - 2023-07-28 10:00:00 AM

From the **Label** list, select a label for the file.



Label:

Case 1

For investigation

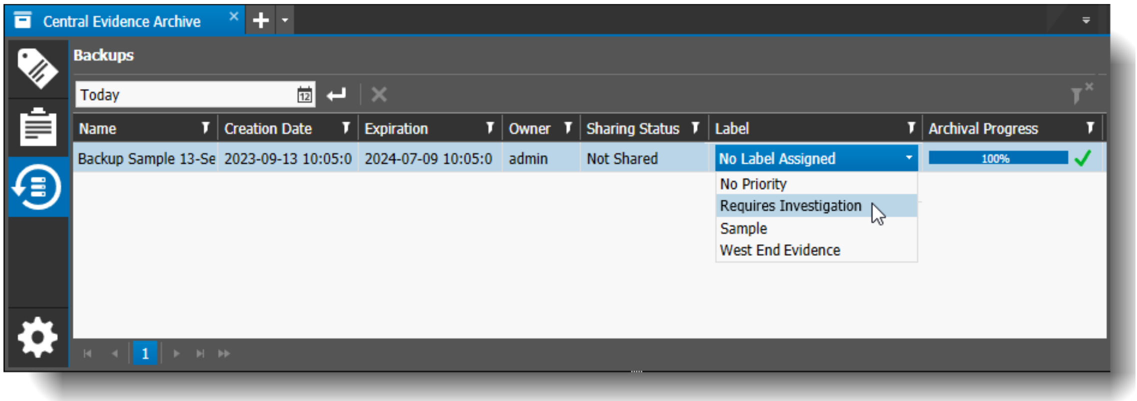
Note: There must be one or more labels configured in the Central Evidence Archive to populate this list. To create labels, see “Configuring General Settings for the Central Evidence Archive” on page 24.

Select **Save**.

3 You can also add a label in the Central Evidence Archive, by opening one of the Tags, Cases, or Backup subtabs.

For example, to add a label to a backup file, open the Central Evidence Archive tab, select the **Backups** subtab, and search for the backup you want to add a label to.

In the **Label** column, select a label from the list to apply it.



Name	Creation Date	Expiration	Owner	Sharing Status	Label	Archival Progress
Backup Sample 13-Se	2023-09-13 10:05:0	2024-07-09 10:05:0	admin	Not Shared	No Label Assigned	100% ✓

- No Priority
- Requires Investigation
- Sample
- West End Evidence

Note: There must be one or more labels configured in the Central Evidence Archive to populate this list. To create labels, see “Configuring General Settings for the Central Evidence Archive” on page 24.

4 You can now use the labels you have applied to help identify files and filter your searches.

Company Overview

March Networks® helps organizations transform video into business intelligence through the integration of surveillance video, analytics, and data from business systems and IoT devices. Companies worldwide use our software solutions to improve efficiency and compliance, reduce losses and risk, enhance customer service and compete more successfully. With deep roots in video security and networking, March Networks is also recognized as the leader in scalable, enterprise-class video management and hosted services. We are proud to work with many of the world's largest financial institutions, retail brands, cannabis operators and transit authorities, and deliver our software and systems through an extensive distribution and partner network in more than 70 countries. Founded in 2000, March Networks is headquartered in Ottawa, Ontario, Canada. For more information, please visit *www.marchnetworks.com*.

Customer Support and Assistance

Certified partners can telephone our Technical Support team Monday to Friday during business hours or email at any time.

North America, South America, & Asia Pacific

Telephone – 1 613 591 1441
Toll Free (US & Canada) – 1 800 472 0116
Email – techsupport@marchnetworks.com

Europe, Middle East, & Africa

Telephone – +39 0362 17935 extension 3
Email – supporteurope@marchnetworks.com

If you have purchased a March Networks solution through one of our Certified Partners, please contact your representative directly for first level technical support and assistance with RMA services.