Important Notice

Copyright © 2019 WatchGuard, Inc. All rights reserved. This document and supporting data are the exclusive property of WatchGuard, Inc. and may not be copied and/or reproduced without permission.

Software updates
WatchGuard is committed to the continual testing and improvement of our software. As new software revisions become available, these updates will be made available to your agency; fees may apply depending on your licensing agreement.

Contact information
WatchGuard, Inc.
415 East Exchange Parkway
Allen, Texas 75002
Customer Service: 800-605-6734
Customer Service web portal: https://support.watchguardvideo.com/hc/en-us

Send us your suggestions
Tell us about your experience and how you are using Evidence Library 4 Web. We will do our best to accommodate suggestions you may have in future revisions.

U.S. customers, call Customer Service or submit a ticket through the Customer Service web portal. International customers, contact your local distributor or submit a ticket through the Customer Service web portal.

Trademark notices
Microsoft, Windows, Windows Media, Windows Server, SQL Server, Active Directory, Azure, Visual C++, Edge, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Intel Xeon is a trademark of Intel Corporation in the U.S. and/or other countries.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions.

Google Chrome is a trademark of Google, Inc.

Wi-Fi® is a registered trademark of Wi-Fi Alliance.

Rimage® and Catalyst™ are registered trademarks or trademarks of the Rimage Corporation.

All other marks, names, and logos mentioned herein are the property of their respective owners.
# Contents

**Introduction** ........................................................................................................................................................................... 13  
  About this document ................................................................................................................................................................. 13  
  Related documents and information ........................................................................................................................................... 13

**Chapter 1. About Evidence Library 4 Web** .......................................................................................................................... 15  
  Introduction to Evidence Library 4 Web ........................................................................................................................................ 16  
  What's New in Evidence Library 4 Web ......................................................................................................................................... 17  
  What's new in version 4.4: ................................................................................................................................................................. 17  
  What's new in version 4.3: ................................................................................................................................................................. 17  
  What's new in version 4.2: ................................................................................................................................................................. 18  
  What's new in version 4.1.2: ............................................................................................................................................................... 18  
  What's new in version 4.1: ................................................................................................................................................................. 19  
  What's new in version 4.0: ................................................................................................................................................................. 20  
  Using Evidence Library 4 Web .......................................................................................................................................................... 22  
    Evidence Library 4 Web client .......................................................................................................................................................... 22  
    Accessing Evidence Library 4 Web ................................................................................................................................................. 23  
  Evidence Library Administrator .......................................................................................................................................................... 24  
    Accessing Evidence Library Administrator ..................................................................................................................................... 25  
  Evidence Library Transfer Agent .......................................................................................................................................................... 26

**Chapter 2. Importing Evidence** .................................................................................................................................................. 29  
  Overview .............................................................................................................................................................................................. 30  
  Automatic Import from Ethernet-Connected Devices ..................................................................................................................... 31  
    4RE DVR .......................................................................................................................................................................................... 31  
    VISTA camera .................................................................................................................................................................................. 31  
  Automatic Import from USB-Connected Devices .......................................................................................................................... 32  
  Manually Importing from USB-Connected Devices ......................................................................................................................... 34  
    Using the Import Events dialog box ................................................................................................................................................. 36  
    Preview ............................................................................................................................................................................................ 39  
    Secondary event tags ......................................................................................................................................................................... 39  
  Using the USB Dashboard .................................................................................................................................................................. 40  
  Removing a USB thumb drive safely from a 4RE DVR ..................................................................................................................... 41
# Contents

Using the Transfer function ......................................................... 41
Using the Stop button ................................................................. 43
Creating a VISTA Record-After-the-Fact® Event ................................ 44

**Chapter 3. Working with Recorded Events** .................................. 47

Overview ....................................................................................... 48
Searching for Recorded Events ..................................................... 49
  Recorded event search fields ...................................................... 50
  Complex searches ....................................................................... 51
    Saving complex searches ......................................................... 51
  Auto Update checkbox ............................................................... 51
Working with search results ......................................................... 52
Search results rows ..................................................................... 53
Changing the recorded event list view ........................................... 56
  Large view ................................................................................ 56
  Medium view ............................................................................ 56
  Small view ................................................................................ 56
  Table view ................................................................................ 56
  Sorting search results ............................................................... 57
Actions menus .............................................................................. 57
  Single event Actions menu ....................................................... 58
  Multiple event Group Actions menu ......................................... 59
Manually Linking and Unlinking Events ......................................... 60
  Selecting one event to link to another ...................................... 60
  Selecting two events to link together ....................................... 61
  Unlinking events ...................................................................... 61
Playing Back Recorded Events ..................................................... 62
  Single event playback .............................................................. 63
  Synchronized event playback with 1-Up .................................... 66
    Sync Export ........................................................................... 70
      Using Sync Export ............................................................... 71
  Synchronized event playback with 2-Up .................................... 73
Playing back a camera view with an audio track from a different device ......................................................... 77
Playing back two camera views and an audio track from different devices ............................................................ 79
Viewing recorded event metadata .................................................. 82
Contents

Metadata graph ........................................................................................................... 83
Event video trim ........................................................................................................... 84
Trimming event video ................................................................................................. 86
Viewing and Editing Event Details ........................................................................... 91
Basic event details section ......................................................................................... 92
Import Properties ....................................................................................................... 94
Viewing linked event detail information ................................................................... 95
Viewing case event detail information ....................................................................... 96
Viewing the event audit log ....................................................................................... 97
Manually Archiving Events ....................................................................................... 98
Restoring archived events ......................................................................................... 99
Manually Purging Events ............................................................................................ 100

**Chapter 4. Working with Cases** ........................................................................ 101
Overview .................................................................................................................. 102
Creating a Case ........................................................................................................ 103
Deleting a case ......................................................................................................... 105
Adding a Recorded Event to an Existing Case ........................................................ 106
Removing a recorded event from a case .................................................................. 108
Adding Other Files to a Case .................................................................................. 109
Deleting non-event files from a case ....................................................................... 110
Adding Links to a Case ............................................................................................ 111
Deleting a link from a case ...................................................................................... 112
Searching for a Case ............................................................................................... 113
Viewing Case Attachments .................................................................................... 114
Adding Case Workers to a Case ............................................................................. 115
Using the Case Workers tab .................................................................................... 117

**Chapter 5. Exporting Evidence** .................................................................... 119
Overview ................................................................................................................ 120
Exporting a Recorded Event .................................................................................... 121
Exporting Multiple Recorded Events ...................................................................... 124
Exporting a Sync Export Video/Audio Combination ............................................. 127
Exporting a Trimmed Video .................................................................................... 131
Exporting Cases ..................................................................................................... 134
Export Worksheet and My Exports ......................................................................... 136
Contents

Export Worksheet ........................................................................................................ 137
My Exports tab ........................................................................................................ 138
Select Items to Export ............................................................................................ 138
Sync Export video/audio combinations .................................................................. 139
Linked events ............................................................................................................ 139
Trimmed video ........................................................................................................ 139
Cases and case attachments .................................................................................... 140
Camera views .......................................................................................................... 140
Choose a Format for Media Export ........................................................................ 140
Video formats .......................................................................................................... 141
Including on-screen text ........................................................................................ 142
Subtitles .................................................................................................................. 142
Embedded text ........................................................................................................ 142
Select a Destination for Media Export ..................................................................... 143
Local computer or network folder .......................................................................... 143
Individual optical disc burner ............................................................................... 144
DVD robot ................................................................................................................ 145
Media export destination preferences ..................................................................... 146
Export Using CLOUD-SHARE .............................................................................. 148
CLOUD-SHARE configuration ............................................................................ 150
Setting up CLOUD-SHARE in EL4 Web ................................................................. 151
Export Summary ...................................................................................................... 155
Using the My Exports tab ....................................................................................... 156
Actions menu ......................................................................................................... 157
Filtering .................................................................................................................... 157
WatchGuard Single Event Player ........................................................................... 158
Snapshots list .......................................................................................................... 159
Video player controls ............................................................................................ 159
Playing back exported video with the single event player .................................... 161
Exported Audit Log ................................................................................................ 162
WatchGuard Synchronized Event Player ................................................................ 164
Installing the WatchGuard Video Player for synchronized event playback .......... 165
Accessing exported video using the WatchGuard Video Player ......................... 169
Single event playback ............................................................................................. 172
Synchronized event playback with 1-Up ................................................................. 175
Synchronized event playback with 2-Up ................................................................. 178
Playing back a camera view with an audio track from a different device .............. 180
Playing back two camera views and an audio track from different devices .......... 182

Chapter 6. Checking Out VISTA Cameras ............................................................... 185
Overview .................................................................................................................. 186
Checking Out VISTA Cameras from the USB Dashboard ........................................ 187
Checkout Using the VISTA Dashboard ................................................................. 192
Checking out individual VISTA cameras from the VISTA Dashboard ................. 193
Checking out using Rapid Checkout ..................................................................... 197
Printing a Checkout Report .................................................................................. 199
From the VISTA Dashboard ................................................................................. 199
From the Rapid Checkout dialog box .................................................................. 199
Checkout Using Kiosk Mode .................................................................................. 200
Checking out VISTA cameras from the Kiosk ...................................................... 201
Setting up Kiosk Mode ......................................................................................... 204
VISTA SmartConnect Preferences: Using VISTA with SmartConnect ........ ........ 208
Using the VISTA Dashboard ................................................................................. 210

Chapter 7. Managing Evidence Storage ................................................................. 213
Overview .................................................................................................................. 214
Accessing Evidence Management ....................................................................... 215
Setting up evidence storage and retention workflow .......................................... 216
Managing Storage Locations ................................................................................ 217
Shared folders ....................................................................................................... 219
User and group account permissions ................................................................. 219
Setting up a shared folder .................................................................................... 219
Setting up Online Video storage ........................................................................ 222
Setting up the first tier ......................................................................................... 223
Adding an on-premise video storage tier ............................................................ 228
Adding a storage location to an on-premise tier ................................................. 230
Adding a cloud video storage tier ....................................................................... 234
Adding a storage location to a cloud tier ............................................................ 236
Editing a video storage tier .................................................................................. 237
Editing a storage location for an on-premise tier .............................................. 238
## Contents

Editing a storage location for a cloud tier .......................................................... 239
About Online Video storage ................................................................................. 240
  Tiers .................................................................................................................. 240
  Storage locations .............................................................................................. 241
On-premise versus cloud storage ......................................................................... 242
Rollover versus round-robin usage ...................................................................... 242
Moving events to the next tier automatically ....................................................... 243
Online Video storage examples ........................................................................... 244
Video Processing storage .................................................................................... 245
  Setting up a Video Processing storage location .............................................. 246
Import storage ...................................................................................................... 250
  Setting up an Import storage location ............................................................. 250
Export storage ..................................................................................................... 251
  Setting up an Export storage location ............................................................. 251
Offline Archive storage ....................................................................................... 252
  Setting up an Offline Archive storage location .............................................. 253
Case storage ......................................................................................................... 253
  Setting up a Case storage location ................................................................. 254
Storage status notifications .................................................................................. 255
Managing Evidence Retention and Cleanup ......................................................... 257
  Setting up evidence retention rules ................................................................. 258
Evidence retention rules ...................................................................................... 259
    Default rule .................................................................................................... 260
    Exceptions to the Default rule ...................................................................... 261
Scheduling automatic evidence cleanup ............................................................... 262
Evidence cleanup ................................................................................................ 263
    Automatic ..................................................................................................... 264
    Manual .......................................................................................................... 264
**Chapter 8. Managing Devices** .......................................................................... 265
Overview .............................................................................................................. 266
  Accessing Device Management ...................................................................... 267
Using Device Management ................................................................................... 268
  Single configurations for smaller agencies ...................................................... 268
  Multiple configurations for larger agencies ...................................................... 268
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting Up System Settings</td>
<td>269</td>
</tr>
<tr>
<td>Configuring the 4RE DVR</td>
<td>270</td>
</tr>
<tr>
<td>Accessing 4RE Management</td>
<td>270</td>
</tr>
<tr>
<td>Recommended workflow for configuring a 4RE DVR</td>
<td>271</td>
</tr>
<tr>
<td>Setting up agency 4RE settings</td>
<td>272</td>
</tr>
<tr>
<td>All Vehicles list</td>
<td>274</td>
</tr>
<tr>
<td>Adding a new 4RE DVR to the All Vehicles list</td>
<td>275</td>
</tr>
<tr>
<td>Editing properties for an existing 4RE DVR</td>
<td>277</td>
</tr>
<tr>
<td>4RE configurations</td>
<td>278</td>
</tr>
<tr>
<td>Creating a new 4RE configuration</td>
<td>279</td>
</tr>
<tr>
<td>Copying an existing 4RE configuration</td>
<td>280</td>
</tr>
<tr>
<td>Assigning a 4RE DVR to a configuration</td>
<td>281</td>
</tr>
<tr>
<td>Assigning a user group to a 4RE configuration</td>
<td>282</td>
</tr>
<tr>
<td>Setting the 4RE Recording Properties</td>
<td>284</td>
</tr>
<tr>
<td>4RE video quality settings</td>
<td>287</td>
</tr>
<tr>
<td>Front camera</td>
<td>287</td>
</tr>
<tr>
<td>Secondary camera</td>
<td>288</td>
</tr>
<tr>
<td>Panoramic camera</td>
<td>289</td>
</tr>
<tr>
<td>4RE user permissions settings</td>
<td>290</td>
</tr>
<tr>
<td>4RE pre-event</td>
<td>290</td>
</tr>
<tr>
<td>Setting the 4RE DVR Behavior properties</td>
<td>291</td>
</tr>
<tr>
<td>Shutdown timers</td>
<td>294</td>
</tr>
<tr>
<td>Ignition shutdown timer</td>
<td>294</td>
</tr>
<tr>
<td>Wireless transfer shutdown timer</td>
<td>294</td>
</tr>
<tr>
<td>Setting the 4RE Import Properties</td>
<td>295</td>
</tr>
<tr>
<td>Deployment</td>
<td>297</td>
</tr>
<tr>
<td>Deploying a configuration</td>
<td>298</td>
</tr>
<tr>
<td>Deploying a configuration manually</td>
<td>298</td>
</tr>
<tr>
<td>Deploying a configuration to a 4RE DVR</td>
<td>301</td>
</tr>
<tr>
<td>Deploying a configuration automatically</td>
<td>302</td>
</tr>
<tr>
<td>Deploying a 4RE DVR software update</td>
<td>303</td>
</tr>
<tr>
<td>Deploying a 4RE DVR software update manually</td>
<td>303</td>
</tr>
<tr>
<td>Deploying a 4RE DVR software update automatically</td>
<td>304</td>
</tr>
<tr>
<td>Setting your In-Car Supervisor Password</td>
<td>306</td>
</tr>
</tbody>
</table>
Contents

Configuring the VISTA Camera ................................................................. 307
  Accessing VISTA Management ............................................................ 307
Recommended workflow for configuring a VISTA camera ...................... 308
Setting the VISTA New Officer Preferences ........................................... 308
  Enabling VISTA Other Options .......................................................... 309
VISTA configurations ........................................................................... 310
  Creating a new VISTA configuration ................................................... 311
  Copying an existing VISTA configuration ............................................ 312
Assigning a user group to a VISTA configuration .................................. 312
Setting the VISTA Recording Properties .............................................. 314
VISTA video quality settings ............................................................... 318
VISTA pre-event .................................................................................... 319
Setting the VISTA Device Properties ................................................... 319
Setting the VISTA Import Settings ....................................................... 321
Setting the VISTA Network Settings .................................................... 323
Deploying a VISTA firmware update .................................................... 325
  Deploying a VISTA firmware upgrade automatically .......................... 325
  Deploying a VISTA firmware update manually .................................. 326
Requesting a VISTA state capture ....................................................... 329
Setting Up Event Tags .......................................................................... 331
  Creating secondary event tags ............................................................ 332
  Marking an answer Critical ................................................................. 332
    On the 4RE ...................................................................................... 332
    On VISTA ..................................................................................... 333
  Marking an answer Retired ................................................................. 333
  Making an event tag required ............................................................. 333
    On the 4RE ...................................................................................... 333
    On VISTA ..................................................................................... 333
Setting up the EventCategory event tag .............................................. 334
Setting up secondary event tags .......................................................... 337
  Drop-down selection list form ............................................................ 337
  Short text answer form ...................................................................... 337
Adding a drop-down list event tag using a template ............................. 338
Adding a custom drop-down list event tag ............................................ 341
Chapter 9. Managing Security

Overview ................................................................. 352
Accessing Security Management .................................. 352
Security Management Roles ........................................ 354
Setting Up Security in an AD Environment ...................... 358
Best practices for working with AD ................................ 358
Before installing EL4 Web ........................................... 358
Creating EL4 Web user groups in AD .............................. 358
Adding AD user groups ............................................. 359
Assigning roles to AD user groups ................................. 360
Setting Up Security in an AD LDS Environment ............... 361
Users, user groups, and roles ..................................... 361
Setup process ........................................................ 361
Creating and setting up an LDS administrator account ........ 362
Adding LDS user groups and assigning roles .................. 367
Adding LDS user accounts ....................................... 369
Assigning LDS users to user groups .............................. 370
Assigning users to groups on the Edit User Group dialog box .............................................. 371
Assigning users to groups on the Edit User dialog box ........ 373
This page intentionally left blank.
Introduction

Welcome to the WatchGuard® Evidence Library 4 Web User Guide. This guide is designed to walk you through the basics of using Evidence Library 4 Web (EL4 Web) to manage your WatchGuard® 4RE® DVRs and VISTA® Body Cameras, as well as evidence imported from them.

Note: This document covers versions 4.0 through 4.4 of EL4 Web.

About this document

The Evidence Library 4 Web User Guide covers the most common operations in EL4 Web including:

- Importing recorded events captured by a WatchGuard 4RE DVR or VISTA Body Camera
- Managing WatchGuard recorded events and cases
- Exporting evidence using media or CLOUD-SHARE
- Managing evidence storage
- Setting up and assigning configurations to WatchGuard 4RE DVRs or VISTA Body Cameras
- Managing user security

The images in this document represent what you could see on your screen. They are meant to serve as a guide. What you see on your screen will not exactly match the images in this guide.

Important! This user guide covers the basic use of EL4 Web. It is not a comprehensive manual for every possible action or situation in Evidence Library. If you have a question about EL4 Web that is not covered in the user guide, contact your WatchGuard representative.

Related documents and information

For subjects related to your WatchGuard system that are not covered by the Evidence Library 4 Web User Guide, see the following documents:

- VISTA HD Wearable Camera User Guide
- 4RE In-Car Video User Guide
- CLOUD-SHARE User Guide
- Evidence Library 4 Web Installation Guide
Introduction

This page intentionally left blank.
Chapter 1. About Evidence Library 4 Web

In this chapter...

- Introduction to Evidence Library 4 Web (EL4 Web) (page 16)
- What’s new in EL4 Web (page 17)
  - Version 4.4 (page 17)
  - Version 4.3 (page 17)
  - Version 4.2 (page 18)
  - Version 4.1.2 (page 18)
  - Version 4.1 (page 19)
- Using EL4 Web (page 22)
- Using the Evidence Library Administrator (EL Administrator) (page 24)
- Using the Evidence Library Transfer Agent (page 26)
Introduction to Evidence Library 4 Web

**Note:** This document covers versions 4.0 through 4.4 of EL4 Web.

Evidence Library 4 Web (EL4 Web) is the WatchGuard® software component for managing:

- Your fleet of WatchGuard 4RE® in-car DVRs (digital video recorders)
- Your set of WatchGuard VISTA® Body Cameras
- The evidence produced by and imported from the 4RE DVRs and VISTA Body Cameras

EL4 Web includes the following major features:

- Video evidence management, including
  - Import (page 29)
  - Search (page 49)
  - Playback (page 62)
  - Export (page 119)
- Case management (page 101)
- Evidence storage management (page 213)
- Device management, including
  - 4RE DVR configuration (page 270)
  - VISTA Body Camera configuration (page 307)
- Security management (page 351)

EL4 Web gives you the ability to configure your 4RE DVRs and VISTA Body Cameras as well as manage the video recorded by and imported from those devices.

*For more information about...*

What's new in EL4 Web, see *What’s New in Evidence Library 4 Web* on page 17.

Using EL4 Web, see *Using Evidence Library 4 Web* on page 22.
What's New in Evidence Library 4 Web

- Version 4.4 (below)
- Version 4.3 (below)
- Version 4.2 (page 18)
- Version 4.1.2 (page 18)
- Version 4.1 (page 19)
- Version 4.0 (page 20)

What's new in version 4.4:

- **Sync Export** (page 70)
  Version 4.4 gives you the ability to export some video and audio streams together, even when they come from different events or devices.

- **Video Processing storage location** (page 245)
  Version 4.4 provides a new storage/processing location to improve newly imported evidence processing. Each Video Processing location corresponds to a local Job Queue Worker Service.

- Performance and security enhancements
- Bug fixes

What's new in version 4.3:

- **Bulk addition and deletion of non-event files for cases** (page 109)
  Version 4.3 gives you the ability to upload multiple non-event files to a case at one time, by browsing or drag-and-drop. With version 4.3, you can also delete multiple non-event files from a case at one time.

- **Faster event search by exact event ID** (page 50)
  Version 4.3 speeds up a search for an exact match to a full recorded event ID when you check the **Match Exact Event ID** checkbox.

- VISTA battery metrics improvements
- Performance and security enhancements
- Bug fixes
What's new in version 4.2:

- **Support for export to Rimage® robots** (page 145)
  
  Version 4.2 gives you the option to export to any of three Rimage robots: 2000i, 5400 series, or Catalyst™.

- **Support for auto-start record settings for the VISTA Vehicle Kit** (page 314)
  
  Version 4.2 gives you the ability to configure VISTA WiFi (as part of the VISTA Vehicle Kit) to automatically start recording an event when certain external inputs are activated.

  *Note: For the VISTA Vehicle Kit, external inputs are connected to the Smart Power Switch.*

- **Support for disabling VISTA audio capture** (page 314)

  Version 4.2 gives you the option to completely disable audio on the VISTA camera.

- **Security Management role to Edit Recorded Event Tags** (page 354)

  Version 4.2 gives you the ability to assign user permissions to edit only the tag on a recorded event rather than all the event details.

- **Event search by a location radius of less than 1 mile** (page 50)

  Version 4.2 gives you the ability to search your database for recorded events within a mile radius (down to .1 mile radius) of a set Location.

- **Support for CA (Canada) date format**, including:
  
  - Dates showing in the EL4 Web Client, EL Administrator, EL Transfer Agent, and WatchGuard Video Player 4.1.0/4.1.1
  
  - Configuration (page 291)

  Version 4.2 gives you the ability to configure your instance of EL4 Web and your 4RE DVRs to use and display a Canada date format.

- **Support for Google Chrome version 58 and higher** (page 22)

  Version 4.2 supports the certificate implementation that Google Chrome requires in version 58 (and higher).

  - Reliability improvements

What's new in version 4.1.2:

- **Support for UK (United Kingdom) date format**, including:
  
  - Dates showing in the EL4 Web Client, EL Administrator, EL Transfer Agent, and WatchGuard Video Player 4.1.0/4.1.1
  
  - Configuration (page 291)

  Version 4.2 gives you the ability to configure your instance of EL4 Web and your 4RE DVRs to use and display a UK date format.
What's new in version 4.1:

- **Automatic deployment of new configurations to VISTA when docked**, including:
  - Configuration (page 309)
  - Support for devices docked in the VISTA USB Base or Transfer Station
  Version 4.1.2 gives you the ability to automatically deploy new configurations to docked VISTA Body Cameras (in the USB Base or Transfer Station) without the need to check them out again.

- **Addition of badge numbers to the list of officer names at VISTA checkout**, including:
  - Checkout from the USB Dashboard (page 187)
  - Checkout from the VISTA Dashboard (page 192)
  - Checkout from the Kiosk (page 201)
  Version 4.1.2 allows you to add badge numbers to the list of officer names that shows at VISTA checkout.

- **Addition of Import Date to the list of sort criteria on the Events tab** (page 57)
  Version 4.1.2 gives you the ability to sort search results on the Events tab (Large, Medium, and Small Views) by Import Date.

What's new in version 4.1:

- **Web-based Evidence Management** (page 213)
  Version 4.1 provides access to evidence storage management through the EL4 Web client as well as new options in managing your storage locations, including:
  - Tiered storage locations
  - Round-robin storage method
  - Support for Microsoft Azure Government cloud storage

- **New single event playback experience and support for synchronized event playback** (page 62)
  Version 4.1 gives you the ability to play back video and/or audio from up to three events recorded at the same time using different devices.

- **Support for the Wi-Fi/GPS version of the VISTA camera**, including:
  - Configuration (page 307)
  - VISTA Dashboard monitoring (page 210)
  - Device type selection at checkout (page 185)
  Version 4.1 gives you the ability to manage your set of VISTA WiFi cameras alongside your existing set of non-Wi-Fi VISTAs and your fleet of 4RE DVRs.

- **Support for VISTA event import from the vehicle using the VISTA WiFi Base**, including:
  - Configuration (page 323)
  - VISTA Dashboard monitoring (page 31)
  Version 4.1 gives you the option to use the VISTA WiFi Base in the vehicle for importing VISTA events automatically through the same wireless network that the 4RE DVR uses for its wireless transfer.
Chapter 1. About Evidence Library 4 Web

- **Support for recording groups and group events** (VISTA WiFi/4RE integration), including:
  - 4RE DVR configuration (page 284)
  - VISTA WiFi configuration (page 314)
  - Automatic linking of events in a group event on import

  Version 4.1 gives you the ability to set up your 4RE DVRs and VISTA WiFi cameras to work together to perform group events.

  **Note:** For more information about recording groups and group events, see the VISTA HD Wearable Camera User Guide or the 4RE In-Car Video User Guide.

- **Support for power and network management in the vehicle using the Smart Power Switch**, including:
  - 4RE DVR configuration (page 275)
  - VISTA configuration (page 319)

  Version 4.1 gives you the ability to set up your 4RE DVRs and VISTA cameras to be managed automatically (power and network) in the vehicle by the Smart Power Switch.

  **Note:** For more information about using the Smart Power Switch as part of your vehicle network, see the VISTA HD Wearable Camera User Guide or the 4RE In-Car Video User Guide.

- **Support for blanking the 4RE Display Screen on vehicle movement** (page 291)

  Version 4.1 gives you the ability to configure this setting for your 4RE DVR.

- **Support for the VISTA SmartConnect iPhone® application**, including:
  - VISTA WiFi configuration (page 323)
  - Wi-Fi credential assignment (page 208)

  Version 4.1 gives you the ability to set up VISTA WiFi to connect to the VISTA SmartConnect iPhone application.

**What's new in version 4.0:**

- **Web client** (page 22)

  Version 4 provides access through a web browser on your local computer to much of Evidence Library’s evidence management functionality.

- **Support for the VISTA camera**, including:
  - Configuration (page 307)
  - Checkout (page 185)
  - Import of VISTA recorded events (page 29)

  Version 4 gives you the ability to manage your set of VISTA Body Cameras and their recorded events alongside your fleet of 4RE DVRs and their events.
What's new in version 4.0:

- **Support for VISTA Transfer Station** *(page 210)*
  Version 4 gives you the ability to monitor and work with your set of VISTA Body Cameras using the VISTA Transfer Station.

- **Automatic import from USB-connected devices** *(page 32)*
  Version 4 gives you the ability to configure your USB-connected devices to automatically import recorded events.

- **Support for additional 4RE DVR options**, including:
  - **HD Panoramic Camera** *(page 289)*
  - **Programmable automatic record start delay** *(page 284)*
  - **Recording Reminder Alerts** *(page 284)*
  - **Maximum Recorded Event Time** *(page 284)*
  - **Automatic event stop when Ignition Shutdown Timer expires** *(page 291)*
  Version 4 gives you the ability to configure the additional 4RE DVR options and features offered with 4RE DVR firmware version 3.6.

- **Automatic** *(page 269)* and **manual** *(page 60)* **event linking**
  Version 4 gives you the ability to set up EL4 Web to automatically link events at import. It also gives you the ability to manually link events from the list of recorded events.

- **Previewing video and viewing/editing event details at manual import** *(page 36)*
  Version 4 gives you the option to preview images of the event video as well as to view and/or edit certain details about an event before import.

- **Support for WatchGuard CLOUD-SHARE** *(page 148)*
  Version 4 gives you the ability to export to the secure cloud using CLOUD-SHARE.
Using Evidence Library 4 Web

The Evidence Library 4 Web (EL4 Web) system has three major parts:

- Evidence Library 4 Web (EL4 Web) client (below)
- Evidence Library Administrator (EL Administrator) (page 24)
- Evidence Library Transfer Agent (page 26)

Evidence Library 4 Web client

The Evidence Library 4 Web (EL4 Web) client is the piece of EL4 Web that you use to work with and manage evidence and evidence storage. You also use the web client to monitor any devices connected to EL4 Web and to check out VISTA Body Cameras from the system.

You use your web browser to access the EL4 Web client. For instructions how to access the EL4 Web client, see Accessing Evidence Library 4 Web on page 23.

Important! EL4 Web supports the following web browsers: Google Chrome version 45 or higher, Windows Internet Explorer version 11, and Edge.

From the EL4 Web client, you can perform the following functions:

- Import recorded events (page 29)
- Work with recorded events including:
  - Search for events (page 49)
  - Play back event video (page 62)
  - Trim event video for export (page 86)
  - View and edit event details (page 91)
- Manually link events (page 60)
- Manually archive (page 98) and purge (page 100) events

- Work with cases (page 101)
- Export evidence (page 119)
- Check out VISTA Body Cameras (page 185)
- Monitor USB-connected devices (page 40)
- Monitor VISTA Transfer Stations and WiFi Bases (page 210)
- Manage evidence storage (page 213)
  - Set up storage locations (page 217)
  - Manage evidence cleanup (page 257)

**Accessing Evidence Library 4 Web**

You can access Evidence Library 4 Web (EL4 Web) using a browser on any computer in your agency's network.

---

**Important!** EL4 Web supports the following web browsers: Google Chrome version 45 or higher, Internet Explorer version 11, and Edge.

---

Before you can sign in to EL4 Web, you must know the web address (URL) for the EL4 Web client.

---

**Note:** If you do not know the URL for the EL4 Web client, contact your system administrator.

---

To access the EL4 Web client:

1. Open your web browser.
Chapter 1. About Evidence Library 4 Web

2. Enter the EL4 Web client’s URL in the browser address bar then press **Enter**.
   The EL4 Web **Secure Sign In** page opens.

3. Enter your **User Name** and **Password**, then click **Sign In**.
   EL4 Web opens to the **Events** tab.
   For information about managing events in EL4 Web, see Chapter 3. **Working with Recorded Events** on page 47.

Evidence Library Administrator

Evidence Library Administrator (EL Administrator) is the piece of Evidence Library 4 Web (EL4 Web) that you use to manage some of EL4 Web's administrative functions.

You access EL Administrator on the computer where it was installed. For instructions how to access EL Administrator, see **Accessing Evidence Library Administrator** on page 25.
From EL Administrator, you perform the following administrative functions:

- Manage devices (page 265)
  - Configure (page 270) and deploy (page 297) 4RE DVRs
  - Configure VISTA Body Cameras (page 307)
- Manage user security (page 351)
  - Active Directory® (AD) (page 358)
    - Or
  - AD Lightweight Directory Services (page 361)
- Set up a label for exported evidence DVDs burned by a DVD robot (page 145)

**Accessing Evidence Library Administrator**

You must access Evidence Library Administrator (EL Administrator) on the computer where it is installed.

---

**Note:** To access EL Administrator, you must be assigned the correct permissions by your system administrator.

---

To access EL Administrator:

1. On the desktop where EL Administrator is installed, double-click the **Evidence Library Administrator** icon.

   ![Evidence Library Administrator icon](image)

   The **Evidence Library Administrator Sign In** dialog box opens.

2. Enter your **Username** and **Password**, then click **Sign In**.
The **Evidence Library Administrator** dialog box opens, showing tabs for the management functions that you have permissions to access.

![Evidence Library Administrator dialog box](image)

**Note:** *EL Administrator opens to the management tab you have permissions to access. You will not see the above EL Administrator screen unless you have Device Management permissions.*

### Evidence Library Transfer Agent

The Evidence Library Transfer Agent is the piece of Evidence Library 4 Web (EL4 Web) that runs on the local computer.

![Evidence Library Transfer Agent](image)

The Transfer Agent must be installed for the local computer to use all of the EL4 Web import and export functionality. If it is not yet installed, you can download the Transfer Agent from the Manage tab in EL4 Web:

- Move your mouse over the **Manage** tab, select **Download the Transfer Agent**, then follow the prompts.
For in-depth instructions for installing the Transfer Agent, see the *Evidence Library 4 Web Installation Guide*.

Most of the time, the Transfer Agent runs in the background. However, if you need to, you can access it from the Windows notification area (system tray):

- Right-click the *Evidence Library Transfer Agent* icon in the system tray, then select **Show Window**.

From the Transfer Agent, you can also perform the following administrative functions:

- Manually update VISTA firmware (page 326)
- Request a VISTA state capture (page 329)
- Set up media export preferences (page 146)
Chapter 1. About Evidence Library 4 Web

This page intentionally left blank.
Chapter 2. Importing Evidence

In this chapter...

- Automatic import from Ethernet-connected devices (page 31)
- Automatic import from USB-connected devices (page 32)
- Manually importing events from USB-connected devices (page 34)
- Using the Import Events dialog box (page 36)
- Using the USB Dashboard (page 40)
- Removing a USB thumb drive safely from the 4RE DVR (page 41)
- Creating a VISTA Record-After-the-Fact® (RATF) event (page 44)
Overview

With Evidence Library 4 Web (EL4 Web), you can import recorded events from a 4RE DVR or a VISTA Body Camera, automatically or manually.

**Important!** You must have the Evidence Library Transfer Agent installed on your computer in order to access some of the import functionality. You can download the Transfer Agent from the Manage tab in EL4 Web.

EL4 Web **automatically** imports events for:

- Ethernet-connected devices (page 31)
  - 4REs that connect to EL4 Web through a wireless network
  - VISTAs docked in VISTA WiFi Bases that connect to EL4 Web through a wireless network
  - VISTAs that connect to EL4 Web through the Transfer Station
  
  For information about monitoring VISTA WiFi Bases or Transfer Stations in EL4 Web, see Using the VISTA Dashboard on page 210.

**Note:** With 4RE version 4.0.6 and VISTA version 3.0.4, WatchGuard supports cellular upload from the vehicle to EL4 Web. For more information, contact WatchGuard Customer Service.

- USB-connected devices, if designated for automatic import in the device configuration (page 32)

  **Tip:** For EL4 Web, devices that are considered **USB-connected** are: a USB thumb drive removed from a 4RE DVR; a VISTA Body Camera docked in a USB Base.

  If your agency does NOT connect wirelessly to its 4RE DVRs or if your agency does NOT use the WiFi Base or Transfer Station with its VISTA Body Cameras, your agency connects to those devices using a USB connection.

EL4 Web allows you to **manually** import events only from USB-connected devices, and only when manual import has been designated in the device configuration. When you import events manually, you can preview the event video and edit certain event details before the event is actually imported into EL4 Web. For instructions how to manually import events, see Manually Importing from USB-Connected Devices on page 34.

When you import events from USB-connected devices, whether automatically or manually, the devices appear and can be monitored on the **USB Dashboard**. For information about the **USB Dashboard**, see Using the USB Dashboard on page 40.
Automatic Import from Ethernet-Connected Devices

Recorded events are imported automatically from the following Ethernet-connected devices:

- 4RE DVRs that connect to Evidence Library 4 Web (EL4 Web) through a wireless network
- VISTA Body Cameras docked in VISTA WiFi Bases that connect to EL4 Web through a wireless network
- VISTA Body Cameras that connect to EL4 Web through the VISTA Transfer Station

**Note:** With 4RE version 4.0.6 and VISTA version 3.0.4, WatchGuard supports cellular upload from the vehicle to EL4 Web. For more information, contact WatchGuard Customer Service.

When import happens automatically, you cannot preview the video or edit the event details before import. If you need to view the video or make changes to any of the event details, you must wait until after the event has been imported into EL4 Web. You can then view the event video on the Recorded Event Playback page and edit its details on the Event Details page.

*For more information about...*

Playing back event video, see Playing Back Recorded Events on page 62.

Editing event details, see Viewing and Editing Event Details on page 91.

**4RE DVR**

If your agency chooses to import evidence from in-car 4REs using wireless transfer, import happens automatically through the wireless network when the 4RE-equipped vehicle drives into range of a wireless hotspot at the agency. The 4RE system automatically connects to EL4 Web and begins to transfer its recorded events. The 4RE Display Screen shows the wireless transfer status as the wireless import happens.

With 4RE wireless import, in-car officers do not need to physically transport the USB thumb drive from the 4RE to the EL4 Web server.

**VISTA camera**

If your agency chooses to import evidence from in-car VISTA Body Cameras that are docked in VISTA WiFi Bases, import happens automatically through the same wireless network that the 4RE DVR uses for its wireless transfer. Both use the wireless hotspot at the agency. VISTA, through the WiFi Base, automatically connects to EL4 Web and begins to transfer its recorded events. The 4RE Display Screen shows VISTA's wireless transfer status as the wireless import happens. For more information about 4RE and what its Display Screen shows for VISTA, see the 4RE In-Car Video User Guide.

If your agency chooses to connect its VISTA Body Cameras to EL4 Web using the VISTA Transfer Station, evidence import happens automatically through the Transfer Station.
Chapter 2. Importing Evidence

When you dock VISTA in the Transfer Station, it automatically connects to EL4 Web and begins to transfer its recorded events.

Each VISTA shows its importing status on the **VISTA Dashboard**, available from the **Manage** tab in EL4 Web.

For more information about monitoring VISTA in Transfer Stations or WiFi Bases using the **VISTA Dashboard**, see *Using the VISTA Dashboard* on page 210.

### Automatic Import from USB-Connected Devices

**Tip:** For Evidence Library 4 Web (EL4 Web), devices that are considered **USB-connected** are: a USB thumb drive removed from a 4RE DVR; a VISTA Body Camera docked in a USB Base.

*If your agency does NOT connect wirelessly to its 4RE DVRs or if your agency does NOT use the Transfer Station or WiFi Base with its VISTA Body Cameras, your agency connects to those devices using a USB connection.*

EL4 Web can automatically import recorded events from a USB-connected device if the device was configured for automatic import.

**Note:** USB-connected 4RE DVRs and VISTA Body Cameras are configured for automatic import separately. For information on setting up a USB-connected 4RE DVR for automatic import, see *Setting the 4RE Import Properties* on page 295. For information on setting up a USB-connected VISTA for automatic import, see *Setting the VISTA Import Settings* on page 321.

If automatic import is configured for a device, when you connect the device to EL4 Web using a USB connection, EL4 Web automatically begins to import any events present on the device. The import takes place in the background so you can work in other areas of EL4 Web while your
recorded events are being imported. As needed, you can monitor the status of the import on the USB Dashboard. For more information about the USB Dashboard, see Using the USB Dashboard on page 40.

On the USB Dashboard, you see each individual device that is configured for automatic import move through the import process. As soon as the device appears on the dashboard, you see the system start the import: Ready becomes Staging, the progress bar shows the status of the import, and the Events show as Importing, one by one.

Tip: Click Cancel Import at any time to cancel the import. If the system is in the middle of processing an event when you cancel the import, it finishes processing that event, then stops. No further events are imported.

Once it finishes, EL4 Web automatically ejects the device.

Important! Once EL4 Web has finished automatically importing events from your USB-connected device, it automatically ejects the device from EL4 Web and the computer. The device disappears from the USB Dashboard and can be safely removed from either the USB port on the computer or the VISTA USB Base.

When your device is configured for automatic import, you cannot preview the video or edit the event details before import. If you need to view the video or make changes to any of the event details, you must wait until after the event has been imported into EL4 Web. You can then view the event video on the Recorded Event Playback page and edit its details on the Event Details page. For information about playing back event video, see Playing Back Recorded Events on page 62. For information about editing event details, see Viewing and Editing Event Details on page 91.
Manually Importing from USB-Connected Devices

Tip: For Evidence Library 4 Web (EL4 Web), devices that are considered USB-connected are: a USB thumb drive removed from a 4RE DVR; a VISTA Body Camera docked in a USB Base.

If your agency does NOT connect wirelessly to its 4RE DVRs or if your agency does NOT use the Transfer Station or WiFi Base with its VISTA Body Cameras, your agency connects to those devices using a USB connection.

To import recorded events manually to EL4 Web from a USB-connected device:

1. If you are importing events from a 4RE USB thumb drive, safely remove the USB thumb drive containing the stored recorded events from the 4RE DVR.
   
   For instructions how to safely remove a USB thumb drive from a 4RE, see Removing a USB thumb drive safely from a 4RE DVR on page 41.

   Warning! It is critical that you only remove a USB thumb drive from a 4RE DVR when it is safe to do so. Removing the USB thumb drive too early can result in loss of evidence or other unexpected results when data is imported from the USB thumb drive.

2. Connect the device containing the events to import to the EL4 Web computer.

3. Access the USB Dashboard on the EL4 Web computer.

   For instructions how to access the USB Dashboard and information about the USB Dashboard, see Using the USB Dashboard on page 40.

   The device you connected to the EL4 Web computer appears on the USB Dashboard.
4. Click **Import Events** for the device whose events you want to import.

   The **Import Events** dialog box opens listing the recorded events available for import.

![Import Events dialog box](image)

5. Preview an event or edit any event details on the **Import Events** dialog box, as needed.

   For information about the features available on the **Import Events** dialog box, see *Using the Import Events dialog box* on page 36.

   **Note:** If your agency requires that events be categorized and/or assigned to an officer before they are imported, the **Process Events** button will be inactive until you categorize any uncategorized events or assign any unassigned events.

6. Click **Process Events**.

   The **Import Events** dialog box closes and you see the system start the import process.

![USB Dashboard](image)

   As the import process progresses, the progress bar shows the status of the import, and the **Events** show as **Importing**, one by one. When the events have finished transferring from the device into EL4 Web, the device status area on the **USB Dashboard** reads **Staging Complete** and **Events** shows the number of events you selected to import in the **Importing** field.
Chapter 2. Importing Evidence

**Tip:** Click **Cancel Import** at any time to cancel the import. If the system is in the middle of processing an event when you cancel the import, it finishes processing that event, then stops. No further events are imported.

The newly transferred events are in the process of being added to the EL4 Web database.

**Important!** How fast a newly transferred event is available to be searched for on the **Events** tab depends on its size. Larger events take longer to be processed.

Using the Import Events dialog box

In Evidence Library 4 Web (EL4 Web), you manually import recorded events from a 4RE DVR USB thumb drive or a VISTA Body Camera using the **Import Events** dialog box. The **Import Events** dialog box lists all the non-imported events currently on the device you selected on the **USB Dashboard**.

From the **Import Events** dialog box you can:

- Categorize or change the categorization of an event (depending on your agency's settings)
- View and/or edit any secondary event tags for an event
- Assign or change the assignment of the officer for an event (depending on your agency's settings)
- Learn information about each recorded event to be imported, for example, date and time the event was recorded
- Identify the device where an event was recorded
- Preview a recorded event before importing it
- Delete an event from the device before importing it (depending on your agency's settings)

For instructions how to manually import recorded events into EL4 Web, see *Manually Importing from USB-Connected Devices* on page 34.

**Note:** Depending on your permissions level and your agency's settings, you may only be able to edit or preview your own events on import.
The **Import Events** dialog box contains the following elements:

- **Process n of n Events**: Indicates the number of recorded events on the list to be imported
- **Total Import Size**: Shows the total combined size of all of the events to be imported
- **Preview thumbnail image**: Click a thumbnail image to show preview images for the event
  
  For more information about previewing event images prior to import, see *Preview* on page 39.

**Note**: Events recorded on a 4RE DVR with a firmware version prior to 3.6 do not display a thumbnail image and do not have preview images available.

- **Event category**: Shows the event category applied to the recorded event on the device
  
  Depending on your agency’s settings, you can edit the contents of this field. Click the event category field, then select a new event category from the drop-down list.

- **Officer**: Shows the name of the officer who recorded the event
  
  Depending on your agency’s settings, you can edit the contents of this field. Double-click the officer field to select the contents, then begin entering the new officer name. When the new officer name you want appears in the drop-down list, select it.

  **Tip**: You must enter three characters before the system shows you a list of matching names. You can enter the first or last name of the officer. The system finds any name that matches the name you enter.

- **Recorded on**: Shows the start date and time of the recorded event
- **Duration**: Shows the length of the recorded event
- **Event size**: Shows the size of the recorded event
- **Device type**: Indicates the type of device used to record the event (4RE or VISTA)
Chapter 2. Importing Evidence

- **Vehicle/Device**: Shows the agency-assigned name of the device where the event was recorded; for VISTA, the field shows the **Device ID**, for 4RE, the field shows the **Vehicle ID**

- **View Secondary Tags button**: If active, click **View Secondary Tags** to view and/or edit secondary event tags
  
  For more information about viewing/editing secondary event tags prior to import, see **Secondary event tags** on page 39.

- **Mark Event for Delete button**: If active, click **Mark Event for Delete** to mark the event for deletion from the device prior to import; the button is inactive by default

  **Note**: For the **Mark Event for Delete** button to be active, the device configuration must allow events to be deleted prior to import and you must have the correct permissions assigned to you.

The event you marked for deletion is shaded red.

If an event on the import list is marked for deletion, it is NOT imported into EL4 Web. The event that is marked for deletion is deleted from VISTA as soon as the camera is undocked and deleted from the 4RE USB thumb drive as soon as the thumb drive is replaced in the 4RE DVR.

To restore the event to the list of events to be imported, click the button again (**Unmark Event for Delete**) BEFORE you click **Process Events**.

**Warning!** You must restore the event **BEFORE** you click **Process Events**. In most cases, an event that you marked for deletion is unrecoverable once you click **Process Events** to import the selected events.

- **Close button**: Click **Close** to discard any changes and close the **Import Events** dialog box WITHOUT importing the events

- **Process Events button**: Click **Process Events** to begin processing the recorded events for import
**Preview**

On the **Import Events** dialog box, you can preview an event to see whether you want to import it into EL4 Web. To preview an event:

- Click an event record's thumbnail image.

The event's preview images appear at the top of the dialog box. The event you selected to preview is shaded green.

The images are from the event video, taken at regular intervals. You can scroll to see all of the preview images, if applicable.

- Click **Close** in the upper right corner of the preview area to close the preview images.

**Secondary event tags**

On the **Import Events** dialog box, you can view and/or edit any secondary event tags for an event before you import it into EL4 Web. To open secondary event tag fields for viewing/editing:

- Click the **View Secondary Tags** button.

If present, the secondary event tag fields appear below the event record.
Chapter 2. Importing Evidence

Depending on the type of event tag, you can either click the field and select a value from the drop-down list, or click the field and enter a value.

**Important!** The secondary event tags present (or not) for an event depend on your agency’s configuration and event tag settings in Evidence Library Administrator (EL Administrator) Device Management.

Using the USB Dashboard

If your agency does NOT connect wirelessly to its 4RE DVRs or if your agency does NOT use the VISTA WiFi Base or Transfer Station with its VISTA Body Cameras, your agency connects to these devices using a USB connection.

In Evidence Library 4 Web (EL4 Web), devices that are considered USB-connected are:

- USB thumb drive removed from a 4RE DVR
- VISTA Body Camera docked in a USB Base

When these devices are USB-connected to an EL4 Web computer, you can monitor and work with them using the **USB Dashboard**.

**Important!** To work with USB-connected devices on the **USB Dashboard**, you must have the Evidence Library Transfer Agent installed on your local computer. If the system notifies you that you need to install the Transfer Agent, follow the prompts to download and install it.

To access the **USB Dashboard**:

- Move your mouse over the **Manage** tab, then select **USB Dashboard**.

When you connect a device into your EL4 Web computer using a USB connection, the device appears on the **USB Dashboard**.
Removing a USB thumb drive safely from a 4RE DVR

From the **USB Dashboard**, you can:

- Initiate import, if the device is configured for manual import (**page 34**)
- Create a Record-After-the-Fact® (RATF) event from a VISTA Body Camera (**page 44**)
- Check out a VISTA Body Camera (**page 187**)
- Eject the device

If the device is configured for automatic import (**page 32**), as soon as the device appears on the dashboard, you see the system start the import process automatically.

---

**Removing a USB thumb drive safely from a 4RE DVR**

---

**Warning!** *It is critical that you only remove a USB thumb drive from a 4RE DVR when it is safe to do so. Removing the USB thumb drive too early can result in loss of evidence or other unexpected results when data is imported from the USB thumb drive.*

There are two ways to safely remove the USB thumb drive from the 4RE DVR. The first uses the **Transfer** function (below) on the display's **Main Menu**. The second uses the **Stop** button (**page 43**).

---

**Using the Transfer function**

To safely remove a USB thumb drive from a 4RE DVR using the **Transfer** function:

1. If the door on the front of the 4RE DVR is closed and locked, insert the key and turn it clockwise.
   
   The door opens and the USB thumb drive pops out.
Chapter 2. Importing Evidence

2. On the 4RE Display Screen’s **Main Menu**, touch **Transfer**.

![Transfer](image)

The **Status** screen appears.

3. Touch **USB**.

The **USB** screen appears.

![USB Screen](image)

4. Touch **Safely Remove**.

If it is not yet safe to remove the USB thumb drive, the **The system is currently writing...** message appears.

![System is Writing](image)

5. Touch **OK**.

When it is safe to remove the USB thumb drive, the **It is now safe...** message appears.

![Safe to Remove](image)

6. Touch **OK** and remove the USB thumb drive from the 4RE DVR.
Using the Stop button

To safely remove a USB thumb drive from a 4RE DVR using the Stop button:

1. If the door on the front of the 4RE DVR is closed and locked, insert the key and turn it clockwise.
   The door opens and the USB thumb drive pops out.

2. On the 4RE Display Control Panel, press and hold the Stop button for three seconds, then release it.
   The Do you wish to safely remove... message appears.

   Do you wish to safely remove the USB?
   - Yes
   - No

3. Touch Yes.
   The It is now safe... message appears.

   It is now safe to remove the USB device.
   - OK

4. Touch OK and remove the USB thumb drive from the 4RE DVR.
Chapter 2. Importing Evidence

Creating a VISTA Record-After-the-Fact® Event

The Record-After-the-Fact® (RATF) feature, when enabled, allows the VISTA Body Camera to continuously capture and save video. You can use this video to create an RATF event by sending the VISTA camera a manual request from Evidence Library 4 Web (EL4 Web).

An RATF event typically includes video that was not originally part of a recorded event.

**Note:** You can create an RATF event from any video that the VISTA camera has saved. If the RATF feature is not enabled, the available video is limited to recorded events (protected video/audio/metadata segments between manual or automatic event starts and stops) plus any pre-event video added to the events.

When you request a VISTA RATF event, you give the camera a date and time range (from oldest to newest). The camera uses all the saved video available during that range to create the RATF event.

You send the manual RATF request to the VISTA camera using the **USB Dashboard**. For information about the **USB Dashboard**, see *Using the USB Dashboard* on page 40.

The VISTA camera creates the RATF event after you undock the camera. The RATF event is available for import the next time you dock the camera with EL4 Web.

To create an RATF event:

1. On the **USB Dashboard**, click the **Actions** menu for the VISTA Body Camera whose video you want to use to create an RATF event, then select **Record-After-the-Fact®**.
Creating a VISTA Record-After-the-Fact® Event

The Record-After-the-Fact dialog box opens.

2. Click the calendar icon (📅) next to the Start Time field and select the starting date of the range you want the RATF event to include.

3. Click the clock icon (⏰) next to the Start Time field and select the starting time on the starting date of the range you want the RATF event to include.

4. Click the calendar and clock icons next to the Stop Time field and select the ending date and time of the range you want the RATF event to include.

Note: The drop-down calendar only allows you to select days where video is available. Days on the calendar before the Start Time and after the Stop Time dates are blank.
Chapter 2. Importing Evidence

5. Click **Create Event**.

   The **Record-After-the-Fact Created** message box opens.

   ![Record-After-The-Fact Created]
   A new recorded event request was created and the VISTA device was ejected.
   To import the event, or manage the device, please **undock** and **re-dock** the VISTA device.

6. Click **OK**.

   EL4 Web automatically ejects the VISTA Body Camera.

---

**Important!** VISTA creates the RATF event only after you undock the camera.  
The RATF event can be imported the next time you dock VISTA with EL4 Web.
Chapter 3. Working with Recorded Events

In this chapter...

- Searching for events (page 49)
- Working with search results (page 52)
- Manually linking events together (page 60)
- Playing back event video (page 62)
- Viewing event metadata (page 82)
- Trimming event video (page 86)
- Viewing and editing event details (page 91)
- Viewing event audit information (page 97)
- Manually archiving events (page 98)
- Restoring events from archive (page 99)
- Manually purging events (page 100)
Chapter 3. Working with Recorded Events

Overview

Once you have imported recorded events into Evidence Library 4 Web (EL4 Web), you can work with the recorded events in a number of ways including:

- Searching for a specific recorded event (page 49)
- Sorting event search results (page 57)
- Manually linking events (page 60)
- Playing back event video (page 62)
- Viewing event metadata (page 82)
- Trimming event video (page 86)
- Viewing and editing event details (page 91)
- Viewing event audit information (page 97)
- Manually archiving events (page 98)
- Restoring events from archive (page 99)
- Manually purging events (page 100)
Searching for Recorded Events

**Note:** Depending on your permissions level, you may only be able to search for your own events.

Once recorded events have been imported into Evidence Library 4 Web (EL4 Web), you can search for them using the fields on the **Event Search** pane (the left pane of the **Events** tab). For information on the fields where you set your search criteria, see *Recorded event search fields* on page 50.

To search for recorded events:

- Select or enter your search criteria in the **Event Search** fields, then click **Search**.

EL4 Web produces a list of recorded events that fit the criteria you entered for the search. The search results appear in the right pane of the **Events** tab. For more information on the search results, see *Working with search results* on page 52.

**Note:** Depending on your permissions, you may only see your own events on the **Events** tab, and you may not see the **Cases**, **My Exports**, or **Manage** tabs.
Chapter 3. Working with Recorded Events

Recorded event search fields

**Note:** Depending on your permissions level, you may only be able to search for your own events.

You search for recorded events using the fields on the **Event Search** pane (the left pane of the **Events** tab):

- **Date:** Click the **Date** field to select the range of dates when the event was recorded
- **Officers:** Click the **Officers** field to select the name of the officer who recorded the event
- **Vehicles/Devices:** Click the **Vehicles/Devices** field to select the identifier of the vehicle (4RE DVR) or device (VISTA) that recorded the event
- **Category:** Click the **Category** field to select the category assigned to the recorded event (for example, assault, traffic accident, DUI)
- **Additional search fields:** Click an additional drop-down list to access further search criteria fields
  - **Secondary Tags:** Click **Secondary Tags** to search for recorded events using tags (other than category) set up for both 4RE and VISTA configurations
  - **Evidence Size:** Click **Evidence Size** to search for recorded events of a certain size or duration
  - **Event Status:** Click **Event Status** to search for recorded events with a certain status (online, archived, in a case) or with a specific recorded event ID

Check the **Match Exact Event ID** checkbox to speed up your search using a full, exact **Recorded Event ID**. Your search will return the one event whose ID matches exactly what you entered.

Clear the **Match Exact Event ID** checkbox when you search with a partial event ID. Your search will return all events whose full **Recorded Event ID** contains the partial event ID you entered.

- **Vehicle Dynamics:** Click **Vehicle Dynamics** to search for recorded events using certain vehicle-related attributes including where **Crash** or **Aux** was triggered, a specific **Location**, or **Speed**
Complex searches

You can use combinations and multiples of the fields on the Event Search pane to perform a more complex search. For example, you can search for events recorded by any of a list of officers, tagged with any of a list of event categories, over a custom date range.

To search by a list of officers, vehicles/devices, or event categories:

- Click the search field, select the Multiple option, then follow the prompts on the Select Multiple dialog box.

To search by a custom date range:

- Click the Date field, select Date Range, then click the Custom Date Range field to bring up the date range calendar where you can choose the custom date range.

Saving complex searches

If you find that you use some complex searches regularly, you can save the search to use again later. To save a search:

- Set all of your search criteria, click Save This Search, then enter a name for the search on the Save Search dialog box.

To search by a saved search at a later date:

- Select the appropriate saved search from the Saved Searches drop-down list just above the Event Search pane.

Auto Update checkbox

Each time you change or add a search criteria and click the Search button, a new search request is sent to EL4 Web. If you want EL4 Web to automatically refine the search results as you update your criteria (without having to click the Search button each time):

- Check the Auto Update checkbox just above the Search button.

In essence, EL4 Web clicks the Search button for you and updates your search results as soon as you change one of the search criteria.
Chapter 3. Working with Recorded Events

Working with search results

In Evidence Library 4 Web (EL4 Web), when you search for recorded events using the Event Search pane, your search results appear in the right pane of the Events tab. For information about using the fields on the Event Search pane to search for recorded events, see Recorded event search fields on page 50.

### Note:
Depending on your permissions, you may only see your own events on the Events tab, and you may not see the Cases, My Exports, or Manage tabs.

Each row of the search results represents one recorded event. You can change the way the search results display in the Events tab:

- Change the view of the list of recorded events by changing the size of the thumbnail image or removing it from the view (page 56)
- Sort the list of recorded events (page 57)

For information about the event data contained in a row of search results, see Search results rows below.
Search results rows

Each row in the search results contains one recorded event's data. To select one or multiple recorded events:

- Check the checkbox on the left end of each row that you want to select.

The selected rows change from white to blue.

Each row of the search results can contain the following elements:

- **Thumbnail image**: Shows a frame from the recorded event video as a reference; when you move the mouse over the thumbnail image, the Playback and Event Details icons appear, layered on top of the image.
  - **Playback icon**: Click the Playback icon on the thumbnail image to open the event player in the browser window and start playing back the event video; if there is more than one available camera view, the playback starts with the front camera view.
  
  **Note**: If there is no available front camera view, the playback starts with the first secondary camera view on the list, then goes to the next on the list, etc.

  For information about playing back video, see *Playing Back Recorded Events* on page 62.
  - **Event Details icon**: Click the Event Details icon on the thumbnail image to open the event details in the browser window.
    
    For information about viewing and/or editing event details, see *Viewing and Editing Event Details* on page 91.

- **Duration**: Shows the length (in hours, minutes, and seconds) of the recorded event.
- **Date**: Shows the date and time that the recorded event was started.
- **Vehicle/Device**: Shows the agency-assigned name of the device where the event was recorded; for VISTA, the field shows the Device ID, for 4RE, the field shows the Vehicle ID.
Chapter 3. Working with Recorded Events

- **Event ID**: Shows the system-defined unique identifier for the recorded event
- **Officer**: Shows the name of the officer who recorded the event
- **Event Category**: Shows the event category assigned by the officer when the event was recorded or when it was imported
- **Device type**: Indicates the type of device used to record the event, either 4RE or VISTA
- **Camera Views Captured**: Shows the number of camera views included in the recorded event
- **Badge**: Shows the badge number of the officer who recorded the event, if applicable
- **Imported on**: Lists the date and time that the recorded event was imported to Evidence Library

**Note:** If the event has been archived, the **Imported on** date will show when the event was restored to Evidence Library.

- **Event Size**: Shows the storage size, MB or GB, of the recorded event
- **Restricted**: Indicates whether the recorded event has had its access restricted; only users who have been assigned the correct permissions in the system can access a restricted event

  For information on roles and permissions in Evidence Library 4 Web (EL4 Web), see *Security Management Roles* on page 354.

- **Prevent Archive**: Indicates whether the recorded event was marked to prevent it from being archived

  **Note:** If an event was marked to prevent it from being archived, it cannot be purged either.

  For information on your system’s archive and purge criteria, see *Managing Evidence Retention and Cleanup* on page 257.

- **Event Tags**: Indicates that tags other than **Event Category** were entered by the officer when the event was recorded or when it was imported; when you move your mouse over the **Event Tags** icon, a tooltip shows you which secondary tags were applied

  For information on setting up secondary tags, see *Creating secondary event tags* on page 332.

- **Split Event**: If present, indicates that the recorded event was part of a larger recorded event that was split into smaller events by the device that recorded the event; the indicator shows the part number of the split event out of the total number of parts that were created from the original large event

  **Note:** Once a large event is split by the device, it cannot be put back together either by the device or by EL4 Web.

EL4 Web treats a split event just as it does any other event. You can import it, search for it, play it back, export it, etc. like you can any recorded event in EL4 Web.
Tip: If you do not see all the split event parts listed on the Events tab, verify that you imported all the parts and that your search parameters include all the parts.

- **Linked Event icon ( )**: If present, indicates that the recorded event has been linked to other recorded events, either automatically or manually; click the Linked Event icon to open the appropriate event details screen and move directly to the Linked Events tab. For information about the Linked Events tab on event details, see Viewing linked event detail information on page 95.

- **Case icon ( )**: If present, indicates that the recorded event is part of a case in Case Management; click the Case icon to view a list of cases that the recorded event has been assigned to, then select a case on the list to open that case in the browser window. For information on cases and Case Management, see Chapter 4. Working with Cases on page 101.

- **Actions menu icon ( )**: Click the Actions menu icon to show the Actions menu for the corresponding recorded event. For information about the Actions menu, see Actions menus on page 57.

Note: The actions that are available on the Actions menu depend on the permissions you are assigned in the Security Management module in Evidence Library Administrator (EL Administrator). For information about roles and permissions in Security Management, see Security Management Roles on page 354.

- **Importing banner**: If present across the thumbnail image, indicates that the recorded event is still being processed for import and may not be accessible for immediate playback or event-details editing; once the event has been fully processed, the banner disappears. For more information on importing recorded events, see Chapter 2. Importing Evidence on page 29.

- **Partial banner**: If present across the thumbnail image, indicates that only part of a recorded event was imported from the device before the device was removed from the system. If an event is marked with the Partial banner, the system has waited 72 hours for the rest of the files associated with the event to be imported, but they have not been imported. If the rest of the files are imported at some point in the future, the system will then process the full recorded event and remove the Partial banner.
Chapter 3. Working with Recorded Events

Changing the recorded event list view

You can change the way information is displayed on the Events tab by selecting a different option in the View field. The options are:

- Large
- Medium
- Small
- Table

The Large, Medium, and Small options refer to the size of the thumbnail image, but they also affect how much data is displayed in a recorded event row. The Table option has no thumbnail image, and all the data is displayed in columns. Large is the default option.

To change your view of the recorded events list:

- On the Events tab, click the View field and select the option you want.

Large view

Medium view

Small view

Table view
Sorting search results

You can sort a list of recorded events, in ascending or descending order, using some of the recorded events’ data elements.

You can only sort by one element at a time using any of the following elements:

- **Date**, from newest to oldest or vice versa
- **Import Date**, from newest to oldest or vice versa
- **Officer**, from A to Z or vice versa
- **Duration**, from shortest to longest or vice versa
- **Vehicle/Device**, from A to Z or vice versa
- **Category**, from A to Z or vice versa
- **Event Size**, from smallest to largest or vice versa
- **Badge #**, from A to Z and vice versa

**Note:** The active sort order button (ascending or descending) is depressed (light gray).

To sort a list of recorded events:

- Click the **Sort By** field and select the element you want to sort by, then click the appropriate ascending or descending order button.

Actions menus

Evidence Library 4 Web (EL4 Web) has two **Actions** menus available on the **Events** tab, one for single event actions, one for multiple event actions.

- The **Actions** menu for single events is available from each row of the search results (below)
- The **Group Actions** menu appears near the top right of the **Events** tab when you select more than one event (page 59)

The actions that are available on the **Actions** or **Group Actions** menu depend on the permissions you are assigned in the Security Management module in Evidence Library.
Chapter 3. Working with Recorded Events


Note: The available actions can change depending on the current state of the event you selected; for example, if the event you selected has been archived, you only see those actions that are allowed for an archived event.

Single event Actions menu

When you click the Actions menu icon on a recorded event, the single event Actions menu appears. The single event Actions menu contains the following actions:

- **Event Playback**: Select Event Playback to open the event player in the browser window and start playing back the event video; if there is more than one available camera view, the playback starts with the front camera view.
  
  If there is no available front camera view, the playback starts with the first secondary camera view on the list, then goes to the next on the list, etc.
  
  For information about playing back video, see Playing Back Recorded Events on page 62.

- **Event Details**: Select Event Details to open the event details in the browser window.
  
  For information about viewing and/or editing event details, see Viewing and Editing Event Details on page 91.

- **Export Event**: Select Export Event to open the Export Worksheet tab and start the export process for the recorded event you selected.
  
  For information about exporting a recorded event, see Exporting a Recorded Event on page 121.

- **Add to Case**: Select Add to Case to open the Add Event to Case dialog box and start the process to add a recorded event to a case in Case Management.
  
  For information about adding events to cases and Case Management, see Chapter 4. Working with Cases on page 101.

- **Link to Event**: Select Link to Event to open the Link to Event dialog box and enter the Event ID of the recorded event you want to manually link with the selected event.
  
  Note: When manually linking one recorded event to another single event, you must know the Event ID of the recorded event you want to link to.

For instructions how to manually link or unlink recorded events, see Manually Linking and Unlinking Events on page 60.
Multiple event Group Actions menu

- **Archive Event**: Select **Archive Event** to manually archive a recorded event to your system archive storage location
  For information about manually archiving a recorded event, see *Manually Archiving Events* on page 98.

- **Purge Event**: Select **Purge Event** to manually purge a recorded event from your system storage
  For information about manually purging a recorded event, see *Manually Purging Events* on page 100.

Multiple event Group Actions menu

With two or more recorded events selected on the search results, the **Group Actions** menu appears near the top right of the **Events** tab.

The **Group Actions** menu contains the following actions:

- **Export Selected Events**: Select **Export Selected Events** to open the **Export Worksheet** tab and start the export process for the recorded events you selected
  For information about exporting multiple recorded events at the same time, see *Exporting Multiple Recorded Events* on page 124.

- **Add Selected to Case**: Select **Add Selected to Case** to open the **Add Event to Case** dialog box and start the process to add the selected recorded events to a case in Case Management
  For information about adding events to cases and Case Management, see *Chapter 4. Working with Cases* on page 101.

- **Link Selected Events**: Select **Link Selected Events** to manually link the selected events together

  **Note**: The **Link Selected Events** action is only available when exactly two events are selected.

For instructions how to manually link or unlink recorded events, see *Manually Linking and Unlinking Events* below.

- **Archive Selected Events**: Select **Archive Selected Events** to manually archive the selected recorded events to your system archive storage location
  For information about manually archiving recorded events, see *Manually Archiving Events* on page 98.
Chapter 3. Working with Recorded Events

- **Purge Selected Events**: Select **Purge Selected Event** to manually purge the selected recorded events from your system storage.
  
  For information about manually purging recorded events, see *Manually Purging Events* on page 100.

### Manually Linking and Unlinking Events

**Note:** If configured in Device Management, events are automatically linked together if they meet the following criteria: same officer name, overlapping event times. *(page 270)*

In Evidence Library 4 Web (EL4 Web), from the **Events** tab, you can manually link recorded events two ways:

- Select one event and search for an event to link to it (below)
- Select two events and link them together *(page 61)*

**Important!** One event can be linked to multiple events, but you can only link two events together at a time.

If an event is linked to another event, each linked event record on the **Events** tab shows the **Linked Event** icon ( ). The **Linked Events** tab (under **Event Details**) for the applicable event shows the events that are linked to it.

For information about event records on the **Events** tab, see *Search results rows* on page 53. For information about **Event Details**, see *Viewing and Editing Event Details* on page 91.

You can manually unlink any events that have been linked together automatically or manually *(page 61).*

### Selecting one event to link to another

To search for an event and link it to a selected event:

1. On the **Events** tab, select the initial recorded event you want to link to another event.
2. Click the **Actions** menu icon and select **Link to Event**.
   
   The **Link to Event** dialog box opens.

   ![Link to Event dialog box](image)

   For information on the **Actions** menu, see *Single event Actions menu* on page 58.
3. Enter the **Event ID** of the event you want to link to the initial event, then click **Save**.

**Tip:** As you enter an **Event ID** in the **Search by** field, the system gives you a list of events with event IDs that match what you entered. You can enter any part of the event ID; for example, enter **821**, and the system will find the ID **00:1d:96:00:7b:70-187197821** (among others) that you wanted.

The events are linked together: the **Linked Event** icon shows on both event records on the **Events** tab and each event shows on the **Linked Events** tab (under **Event Details**) for the other event.

---

### Selecting two events to link together

To link two selected events together:

1. On the **Events** tab, select the two events you want to link together.
2. Click **Group Actions**, then select **Link Selected Events**.

   For information on the **Group Actions** menu, see **Multiple event Group Actions menu** on page 59.

   The events are linked together: the **Linked Event** icon shows on both event records on the **Events** tab and each event shows on the **Linked Events** tab (under **Event Details**) for the other event.

---

### Unlinking events

To unlink events:

1. On the **Events** tab, click the **Linked Events** icon for one of the events you want to unlink. The **Linked Events** tab (under **Event Details**) for the applicable event opens.
2. Click the **Actions** menu icon for the event you want to unlink, then select **Unlink This Event**.

   The events are unlinked.
Chapter 3. Working with Recorded Events

Playing Back Recorded Events

**Note:** The actions that are available to you from Recorded Event Playback depend on your assigned permissions.

In Evidence Library 4 Web (EL4 Web), you play back recorded events using the **Recorded Event Playback** pages:

- Single event playback (page 63)
- Synchronized event playback
  - **1-Up** (page 66)
    - The 1-Up player shows one video screen.
  - **2-Up** (page 73)
    - The 2-Up player can show two video screens.

When you initially access playback for any event, the Recorded Event Playback page opens as single event playback. Single event playback allows you to play back individual events in WatchGuard's standard web video player.

From single event playback, you can move to synchronized event playback, if the event you selected contains synchronization (sync) data. Synchronized event playback allows you to simultaneously play back video and/or audio from events recorded at the same time using different devices.

**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.

For two common examples of playing back events synchronized, see:

- Playing back a camera view with an audio track from a different device (page 77)
- Playing back two camera views and an audio track from different devices (page 79)

From Recorded Event Playback, you can also:

- View or edit event details (page 91)
- Export an event (page 119)
- Export an event using Sync Export (page 70)
  - Sync Export is available from the 1-Up player page if the video and audio streams you are playing back meet the criteria.
- Add the event to a case (page 101)
- Archive the event (page 98)
- View event metadata (page 82)
- Trim event video (page 86)
Single event playback

When you initially access playback for any event in Evidence Library 4 Web (EL4 Web), the **Recorded Event Playback** page opens as single event playback. Single event playback allows you to play back individual events in WatchGuard’s standard web video player.

**Tip:** If the event you select to play back has been in your Evidence Library system for some time, it may not have been converted yet to the EL4 Web native video format (MP4). If this is the case, the system shows you a message that the **video cannot be played in its current format**. Follow the prompts on the message to convert the video so you can play it back in EL4 Web.

To access **Recorded Event Playback** for single event playback from the **Events** tab:

- Click the **Play** icon on the thumbnail image for the event you want to play back.
  
  Or

- Click the **Actions** menu icon for the event you want to play back, then select **Event Playback**.

The **Recorded Event Playback** page for single event playback opens in the browser window with the event playing back.

**Note:** The look of the playback controls depends on which browser you use to play back the recorded event.
Chapter 3. Working with Recorded Events

The **Recorded Event Playback** page for single event playback includes the following elements:

- **Event category**: Shows the event category (for the selected event) assigned by the officer when the event was recorded or when it was imported.

  The **Event category** and the rest of the event metadata listed above the playback screen always correspond to the event in the **Selected event** section of the **Camera Views Panel**. Even when a **Linked Events** view is playing back, the metadata above the screen remains that of the event in the **Selected event** section.

- **Event start date and time**: Shows the date and time that the recorded event started.

- **Officer name**: Shows the name of the officer who recorded the event.

- **Vehicle/Device ID**: Shows the name of the 4RE DVR or VISTA Body Camera that recorded the event.

- **Device type**: Indicates the type of device used to record the event, either 4RE or VISTA.

- **Options**: Click the **Options** icon to open the **Options** menu:
  - **Export**: Click **Export** to open the **Export Worksheet** for the event that is playing back.
    
    For information on exporting an event and the **Export Worksheet**, see **Export Worksheet and My Exports** on page 136.
  - **Add to Case**: Click **Add to Case** to open the **Add Event to Case** dialog box for the event that is playing back.
    
    For information on adding a recorded event to a case in Case Management, see **Adding a Recorded Event to an Existing Case** on page 106.
  - **Archive Events**: Click **Archive Event** to move the event that is playing back to the **Offline Archive** storage location.
    
    For information on archiving an event, see **Manually Archiving Events** on page 98.

- **Event Details button**: Click **Event Details** to move to the **Recorded Event Details** page for the event that is playing back.

  For information about viewing and editing event details, see **Viewing and Editing Event Details** on page 91.

- **Toggle Thumbnails**: Click the **Toggle Thumbnails** control to hide or show the **Camera Views Panel**.

- **Camera Views Panel**: Shows all the camera views included with the recorded event that you selected, as well as any events linked to the selected event.
  - **Selected event section**: Shows the camera views that make up the recorded event that you initially selected on the **Events** tab.
  - **Linked Events section**: Shows a list of events that are linked to the selected event; each linked event shows the camera views that make up the event.
    
    - **Event category**: Click the **Event category** link to make the corresponding linked event into the selected event.
      
      When you click the linked event category, the corresponding event moves up into the **Selected event** section of the **Camera Views Panel**. The event that was in the **Selected event** section moves into the **Linked Events** section. The metadata above the playback screen becomes the metadata from the new selected event.
Single event playback

- **Thumbnail images**: Click a thumbnail image to start playing back the associated camera view.
  The camera view that is currently playing back is outlined and shaded in yellow.
- **Camera views metadata**: Shows information about each camera view and event listed in the **Camera Views Panel**.
  Each camera view shows the view name (for example, **Front, Secondary**) and the video duration.
- **Audio track buttons**: Click an audio track button to play back that audio track with the video.
  The button for the audio track that is currently playing back is yellow.

  Available audio tracks for a camera view show as buttons on the thumbnail image. For single event playback, only the currently playing event thumbnail image shows audio track buttons.

---

**Important!** You must have the Evidence Library Transfer Agent installed to see all available audio tracks for a camera view.

---

**Note:** Each camera view includes at least one audio track; however, the availability of an audio track does not necessarily mean that audio was recorded on that track for the camera view. For example, if no microphone was on, no audio was recorded. The audio track is still present but with no audio recorded.

---

- **Go to Start** ![Icon]: Click the **Go to Start** icon to restart the video from the beginning.
- **Play/Pause** ![Icon]: Click the **Play/Pause** icon to start or stop playback of the video.
- **Playback Progress bar**: Indicates how much of the video has been played back and how much is remaining.
  The **Playback Progress** bar changes to orange as a video plays back. Click and drag the end of the orange part of the bar to a new position to start the video playback from that point.
- **Time Elapsed/Duration**: Shows how much of the video has been played and how long the video is.
- **Captions** ![Icon]: Click the **Captions** icon to turn on or off the on-screen text.
  For information about the on-screen text included for a recorded event, see **Viewing recorded event metadata** on page 82.
- **Snapshot** ![Icon]: Click the **Snapshot** icon to take a still image of the current video frame that you can save as a separate image file.
  When you click the **Snapshot** icon, the still image appears in a dialog box in the video player. Click **Save** to save the image file to your browser **Downloads** folder.
- **Actual Size** ![Icon]: Click **Actual Size** to play back the video in a size that is a completely accurate view of the captured video; if the monitor cannot accommodate the actual video size, the player provides scroll bars to move as needed.
Chapter 3. Working with Recorded Events

For information about 4RE DVR video quality settings, see 4RE video quality settings on page 287. For information about VISTA Body Camera video quality settings, see VISTA video quality settings on page 318.

- **Full Screen (F):** Click the Full Screen icon to show the video on the full monitor screen; press Esc or click the Full Screen icon again to exit full-screen mode

- **Trim (T):** Click the Trim icon to open the trim tool for the camera view that is playing back For information about trimming video, see Event video trim on page 84.

- **Volume Control/Mute (M):** Click the Volume Control icon to mute or unmute the audio; click and drag the control to adjust the volume of the video playback

- **Metadata button:** Click Metadata to show or hide the recorded event's metadata, in graphical form, below the playback screen

  If there is no metadata available for an event, the Metadata button is inactive.

  For information about the metadata included in a recorded event, see Viewing recorded event metadata on page 82.

- **Sync button:** Click Sync to move to the Recorded Event Playback for synchronized events page with 1-Up

  If there is no synchronizing (sync) data available for an event, the Sync button is inactive (gray).

_**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher._

For information about synchronized playback with 1-Up, see Synchronized playback with 1-Up below. For information about synchronized playback with 2-Up, see Synchronized event playback with 2-Up on page 73.

### Synchronized event playback with 1-Up

In Evidence Library 4 Web (EL4 Web), synchronized event playback with 1-Up allows you to simultaneously play back video and audio from events recorded at the same time using different devices. You access synchronized event playback through single event playback, if the event you initially selected to play back contains sync data.

_**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher._

Using the 1-Up player, you can play back video from one device and audio from another device at the same time (page 77). The 1-Up player shows at most one video screen.

**Sync Export** is available from the 1-Up player page if the events you are playing back meet the criteria. You access **Sync Export** through the **Options** menu, if applicable.
To access **Recorded Event Playback** for synchronized event playback (1-Up) from the **Events** tab:

1. Click the **Play** icon on the thumbnail image for the event you want to play back.
   Or
   Click the **Actions** menu icon for the event you want to play back, then select **Event Playback**.
2. Click **Sync** on the right end of the playback controls for single event playback.

   The single event playback player changes to the synchronized event playback player with **1-Up**.

   **Note:** The look of the playback controls depends on which browser you use to play back the recorded event.

The **Recorded Event Playback** page for synchronized event playback with **1-Up** includes the following elements:

- **Event category**: Shows the event category (for the selected event) assigned by the officer when the event was recorded or when it was imported

  The **Event category** and the rest of the event metadata listed above the playback screen always correspond to the event in the **Selected event** section of the **Camera Views Panel**.
Chapter 3. Working with Recorded Events

Even when a **Linked Events** view is playing back, the metadata above the screen remains that of the event in the **Selected event** section.

- **Event start date and time**: Shows the date and time that the recorded event started
- **Officer name**: Shows the name of the officer who recorded the event
- **Vehicle/Device ID**: Shows the name of the 4RE DVR or VISTA Body Camera that recorded the event
- **Device type**: Indicates the type of device used to record the event, either 4RE or VISTA
- **Options** (/png): Click the Options icon to open the **Options** menu:
  - **Export**: Click **Export** to open the **Export Worksheet** for the event that is playing back
    For information on exporting an event and the **Export Worksheet**, see [Export Worksheet and My Exports on page 136](#).
  - **Sync Export**: Click **Sync Export** to open the **Export Worksheet** for the **Sync Export** video/audio combination that is playing back
    For information on setting up a video/audio combination for **Sync Export**, see [Sync Export on page 70](#).
  - **Add to Case**: Click **Add to Case** to open the **Add Event to Case** dialog box for the event that is playing back
    For information on adding a recorded event to a case in Case Management, see [Adding a Recorded Event to an Existing Case on page 106](#).
  - **Archive Events**: Click **Archive Event** to move the event that is playing back to the **Offline Archive** storage location
    For information on archiving an event, see [Manually Archiving Events on page 98](#).
- **Event Details button**: Click **Event Details** to move to the **Recorded Event Details** page for the event that is playing back
  For information about viewing and editing event details, see [Viewing and Editing Event Details on page 91](#).
- **Toggle Thumbnails** (/png): Click the **Toggle Thumbnails** control to hide or show the Camera Views Panel
- **Camera Views Panel**: Shows all the camera views included with the recorded event that you selected, as well as any events linked to the selected event
  - **Selected event section**: Shows the camera views that make up the recorded event that you initially selected on the **Events** tab
  - **Linked Events section**: Shows a list of events that are linked to the selected event; each linked event shows the camera views that make up the event
    - **Event category**: Click the **Event category** link to make the corresponding linked event into the selected event
      When you click the **Event category** for a linked event, the corresponding event moves up into the **Selected event** section of the Camera Views Panel. The event that was in the **Selected event** section moves into the **Linked Events** section. The metadata above the playback screen becomes the metadata from the new selected event.
    - **Thumbnail images**: Click a thumbnail image to start playing back the associated camera view
      The camera view that is currently playing back is outlined and shaded in yellow.
Synchronized event playback with 1-Up

- **Camera views metadata:** Shows information about each camera view and event listed in the **Camera Views Panel**
  Each camera view shows the view name (for example, **Front, Secondary**) and the video duration.

- **Audio track buttons:** Click an **audio track button** from any camera view to play back that audio track with the video
  Available audio tracks for a camera view show as buttons on the thumbnail image. The button for the audio track that is currently playing back is yellow.

  ![Important! You must have the Evidence Library Transfer Agent installed to see all available audio tracks for a camera view.]

  **Note:** Each camera view includes at least one audio track; however, the availability of an audio track does not necessarily mean that audio was recorded on that track for the camera view. For example, if no microphone was on, no audio was recorded. The audio track is still present but with no audio recorded.

- **Timeline:** Shows each of the camera views listed in the **Camera Views Panel** as a horizontal bar or series of bars over time; all available camera views are listed together on the timeline in the same order as they appear on the **Camera Views Panel**

  The camera view bars are synchronized on the timeline. If a bar is present for a camera view, video from that camera view exists for that time frame.
  The bar for the camera view that is currently playing back is yellow. A **Playback Progress** indicator shows where in time the video playback is. You can move the playback to a different location in the video by dragging the handle at the top of the **Playback Progress** indicator. You can change which camera view is playing back by clicking the bar belonging to the new view.
  When you move your mouse over any of the camera view bars, a popup box appears showing information about the view.

  - **Go to Start ( ):** Click the **Go to Start** icon to restart the video from the beginning
  - **Play/Pause:** Click the **Play/Pause** icon to start or stop playback of the video
  - **Elapsed Time/Video Duration:** Shows how much of the current video has been played back and how long the video is
  - **Captions ( ):** Click the **Captions** icon to turn on or off the on-screen text
    For information about the on-screen text included for a recorded event, see **Viewing recorded event metadata** on page 82.

  - **Snapshot ( ):** Click the **Snapshot** icon to take a still image of the current video frame that you can save as a separate image file
Chapter 3. Working with Recorded Events

When you click the **Snapshot** icon, the still image appears in a dialog box in the video player. Click **Save** to save the image file to your browser **Downloads** folder.

- **Actual Size** (\): Click **Actual Size** to play back the video in a size that is a completely accurate view of the captured video; if the monitor cannot accommodate the actual video size, the player provides scroll bars to move as needed

  For information about 4RE DVR video quality settings, see *4RE video quality settings* on page 287; for information about VISTA Body Camera video quality settings, see *VISTA video quality settings* on page 318.

- **Full Screen** (\): Click the **Full Screen** icon to show the video on the full monitor screen; press **Esc** or click the **Full Screen** icon again to exit full-screen mode

- **Trim** (\): Click the **Trim** icon to open the trim tool for the camera view that is playing back

  For information about trimming video, see *Event video trim* on page 84.

- **Volume Control/Mute** (\ / \): Click the **Volume Control** icon to mute or unmute the audio; click and drag the control to adjust the volume of the audio playback

- **Toggle Timeline** (\): Click the **Toggle Timeline** control to hide or show the timeline

- **1-Up button**: When yellow, shows that the 1-Up player is active; when gray, shows that the 1-Up player is inactive

  Click 1-Up when the button is gray to move to synchronized event playback with 1-Up.

- **2-Up button**: When gray, shows the 2-Up player is inactive; when yellow, shows that the 2-Up player is active

- **Sync button**: Click **Sync** to move back to the **Recorded Event Playback** for single event page

  For information about single event playback, see *Single event playback* on page 63.

**Sync Export**

You can export some video and audio streams together, even when they come from different events or devices, with the **Sync Export** feature.

**Sync Export** is available from the 1-Up player page if the video and audio streams you are playing back meet the following criteria:

- Come from different camera views
- Have no gaps
- Overlap in time

You access **Sync Export** through the **Options** menu on the 1-Up player page. If the streams you selected meet the criteria, **Sync Export** shows on the **Options** menu.

**Note**: You cannot trim a **Sync Export** video/audio combination.
Using Sync Export

To set up video and audio streams for **Sync Export**:  

1. On the **Events** tab, click the **Play** icon on the thumbnail image for the event whose video you want to include in the **Sync Export**. 

   The **Recorded Event Playback** page for single event playback opens.

2. Click **Sync** on the right end of the playback controls. 

   The single event playback page changes to the synchronized event playback page with **1-Up**.
Chapter 3. Working with Recorded Events

3. On the **Camera Views Panel**, locate the event whose audio you want to export with the video, then click the appropriate audio track button.

4. Select **Sync Export** from the **Options** menu.
The *Export Worksheet* for the *Sync Export* opens.

For information and instructions how to finish the *Sync Export*, see *Exporting a Sync Export Video/Audio Combination* on page 127.

**Synchronized event playback with 2-Up**

In Evidence Library 4 Web (EL4 Web), synchronized event playback allows you to simultaneously play back video and/or audio from events recorded at the same time using different devices. You access synchronized event playback through single event playback, if the event you initially selected to play back contains sync data.

---

**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.

---

Using the 2-Up player, you can play back video from two devices and audio from another device at the same time (page 79). The 2-Up player shows at most two video screens.

To access *Recorded Event Playback* for synchronized event playback (2-Up) from the *Events* tab:

1. Click the *Play* icon on the thumbnail image for the event you want to play back.
   Or
   Click the *Actions* menu icon for the event you want to play back, then select *Event Playback*.

2. Click *Sync* on the right end of the playback controls for single event playback.

   The single event playback player changes to the synchronized event playback player with 1-Up.
3. Click **2-Up**.

   The **1-Up** player changes to the **2-Up** player. The event you selected moves to the left video screen.

4. Click the thumbnail for a second camera view

   The view you selected opens in the right video screen.

---

**Note:** The look of the playback controls depends on which browser you use to play back the recorded event.

The **Recorded Event Playback** page for synchronized event playback with **2-Up** includes the following elements:

- **Event category:** Shows the event category (for the selected event) assigned by the officer when the event was recorded or when it was imported

  The **Event category** and the rest of the event metadata listed above the playback screen always correspond to the event in the **Selected event** section of the **Camera Views Panel**. Even when a **Linked Events** view is playing back, the metadata above the screen remains that of the event in the **Selected event** section.

- **Event start date and time:** Shows the date and time that the recorded event started

- **Officer name:** Shows the name of the officer who recorded the event
- **Vehicle/Device ID**: Shows the name of the 4RE DVR or VISTA Body Camera that recorded the event
- **Device type**: Indicates the type of device used to record the event, either 4RE or VISTA
- **Options**: Click the Options icon to open the Options menu:
  - **Export**: Click Export to open the Export Worksheet for the event that is playing back
    For information on exporting an event and the Export Worksheet, see Export Worksheet and My Exports on page 136.
  - **Add to Case**: Click Add to Case to open the Add Event to Case dialog box for the event that is playing back
    For information on adding a recorded event to a case in Case Management, see Adding a Recorded Event to an Existing Case on page 106.
  - **Archive Events**: Click Archive Event to move the event that is playing back to the Offline Archive storage location
    For information on archiving an event, see Manually Archiving Events on page 98.
- **Event Details button**: Click Event Details to move to the Recorded Event Details page for the event that is playing back
  For information about viewing and editing event details, see Viewing and Editing Event Details on page 91.
- **Toggle Thumbnails**: Click the Toggle Thumbnails control to hide or show the Camera Views Panel
- **Camera Views Panel**: Shows all the camera views included with the recorded event that you selected, as well as any events linked to the selected event
  - **Selected event section**: Shows the camera views that make up the recorded event that you initially selected on the Events tab
  - **Linked Events section**: Shows a list of events that are linked to the selected event; each linked event shows the camera views that make up the event
  - **Event category**: Click the Event category link to make the corresponding linked event into the selected event
    When you click the linked event category, the corresponding event moves up into the Selected event section of the Camera Views Panel. The event that was in the Selected event section moves into the Linked Events section. The metadata above the playback screen becomes the metadata from the new selected event.
  - **Thumbnail images**: Click a thumbnail image to start playing back the associated camera view; you can play back up to two camera views at a time on the 2-Up player
    The camera views that are currently playing back are outlined and shaded in yellow.
  - **Camera views metadata**: Shows information about each camera view and event listed in the Camera Views Panel
    Each camera view shows the view name (for example, Front, Secondary) and the video duration.
  - **Audio track buttons**: Click an audio track button from any camera view to play back that audio track with the camera views' video
    Available audio tracks for a camera view show as buttons on the thumbnail image. The button for the audio track that is currently playing back is yellow.
Chapter 3. Working with Recorded Events

**Important!** You must have the Evidence Library Transfer Agent installed to see all available audio tracks for a camera view.

**Note:** Each camera view includes at least one audio track; however, the availability of an audio track does not necessarily mean that audio was recorded on that track for the camera view. For example, if no microphone was on, no audio was recorded. The audio track is still present but with no audio recorded.

- **Timeline:** Represents each of the camera views listed in the Camera Views Panel as a horizontal bar or series of bars over time; all available camera views are listed together on the timeline in the same order as they appear on the Camera Views Panel.

  The camera view bars are synchronized on the timeline. If a bar is present for a camera view, video from that camera view exists for that time frame.

  The bars for the camera views that are currently playing back are yellow. A Playback Progress indicator shows where in time the video playback is. You can move the playback to a different video location by dragging the handle at the top of the Playback Progress indicator.

  You can change which camera views are playing back by clicking a bar belonging to a new view. Only two camera views can play back at one time.

  When you move your mouse over any of the camera view bars, a popup box appears showing information about the view.

- **Go to Start (i):** Click the **Go to Start** icon to restart the video from the beginning.

- **Play/Pause:** Click the **Play/Pause** icon to start or stop playback of the video.

- **Elapsed Time/Video Duration:** Shows how much of the current video has been played back and how long the video is.

- **Captions (gu):** Click the **Captions** icon to turn on or off the on-screen text.

  For information about the on-screen text included for a recorded event, see *Viewing recorded event metadata* on page 82.

- **Volume Control/Mute (ııı)/ııı:** Click the **Volume Control** icon to mute or unmute the audio; click and drag the control to adjust the volume of the video playback.

- **Toggle Timeline (ııı):** Click the **Toggle Timeline** control to hide or show the timeline.

- **1-Up button:** When gray, shows that the **1-Up** player is inactive; when yellow, shows that the **1-Up** player is active.

- **2-Up button:** When yellow, shows that the **2-Up** player is active; when gray, shows the **2-Up** player is inactive.

  Click **2-Up** when the button is gray to move to synchronized event playback with **2-Up**.

- **Sync button:** Click **Sync** to move back to the **Recorded Event Playback** for single event page.

  For information about single event playback, see *Single event playback* on page 63.
Playing back a camera view with an audio track from a different device

You can play back video from one device with audio from another device (for example, 4RE DVR video with VISTA WiFi audio) if the events occurred in the same time frame and both have synchronization (sync) data.

**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.

The events must be linked so they show on the synchronized event playback page together.

**Tip:** If the events you want to play back together have not been linked automatically, you can link them manually. For more information, see Manually Linking and Unlinking Events on [page 60](#).

To play back video from one device with audio from another device:

1. On the **Events** tab, click the **Play** icon on the thumbnail image for the event whose video you want to play back.

   The **Recorded Event Playback** page for single event playback opens.
Chapter 3. Working with Recorded Events

2. Click **Sync** on the right end of the playback controls.
   
The single event playback page changes to the synchronized event playback page with **1-Up**.

3. On the **Camera Views Panel**, locate the event whose audio you want to play back with the video, then click the appropriate audio track button.

4. Use the playback controls as needed.
Playing back two camera views and an audio track from different devices

You can play back video from two devices with audio from a third device (for example, video from a 4RE DVR and a VISTA WiFi with audio from a second VISTA WiFi) if the three events occurred in the same time frame and all have synchronization (sync) data.

**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.

The three events must be linked so they show on the synchronized event playback page together.

**Tip:** If the events you want to play back together have not been linked automatically, you can link them manually. For more information, see Manually Linking and Unlinking Events on page 60.

To play back video from two devices with audio from a third device:

1. On the **Events** tab, click the **Play** icon on the thumbnail image for one of the events whose video you want to play back.

   The **Recorded Event Playback** page for single event playback opens.
Chapter 3. Working with Recorded Events

2. Click Sync on the right end of the playback controls.
   The single event playback page changes to the synchronized event playback page with 1-Up.

3. Click 2-Up near the right end of the playback controls.
   The 1-Up synchronized event playback page changes to the 2-Up playback page with the selected video in the left video position.

4. On the Camera Views Panel, locate the second event whose video you want to play back, then click the appropriate thumbnail image.
Playing back two camera views and an audio track from different devices

The second video opens in the right video position.

5. On the **Camera Views Panel**, locate the event whose audio you want to play back with the video, then click the appropriate audio track button.

6. Use the playback controls as needed.
Chapter 3. Working with Recorded Events

Viewing recorded event metadata

Recorded events captured by WatchGuard devices (4RE DVRs and VISTA Body Cameras) contain metadata. Metadata is the information that is collected and included with the video and audio, for example, the name of the officer who recorded the event and when the recorded event started and stopped. The 4RE collects a significant amount of metadata, while VISTA, currently, collects a smaller subset of that metadata.

For both the 4RE and VISTA, some of the metadata can appear as captions or subtitles on the screen during video playback.

For the 4RE, some of the captured metadata includes:

- Patrol car speed
- When the patrol car brakes were depressed
- When the emergency siren and/or lights were turned on
- Radar target speed
- GPS coordinates
- Which cameras were active and when they became active
- Which microphones were active and when they became active

On the Recorded Event Playback page for single event playback, you can also view the 4RE metadata on a graph.
**Metadata graph**

For an event recorded by the 4RE DVR, you can view much of the common event metadata on a graph. To access the metadata graph for a recorded event:

- Click **Metadata** on the **Recorded Event Playback** page for single event playback.

For information about the elements on the **Recorded Event Playback** page for single event playback, see **Single event playback** on page 63.

---

**Note:** The metadata graph is only available from the single event playback page.

---

A portion of the metadata graph slides up just above the playback controls. If you need to see more of the metadata graph:

- Click and drag the dividing handle (.Itoa) up until you see more of the graph.

When the graph appears, a **Playback Progress** indicator provides a cross reference between the video playback screen and the metadata graph. The **Playback Progress** indicator on the graph is synchronized with the video playback.

You can move the playback and metadata graph to a different location in the video by dragging the handle at the top of the metadata graph **Playback Progress** indicator.

The metadata graph has two basic sections:

- Inputs
- Speed data

---

**Important!** The elements, data, and their order on the metadata graph depend on the equipment your agency uses and how each device is set up or configured.
Chapter 3. Working with Recorded Events

The **inputs** section shows metadata that only has two possible states: ON or OFF. On the metadata graph, inputs are shown with a horizontal bar. If the bar is visible, the input device represented is turned ON; otherwise, the input device is OFF. For example, the system can track the patrol car brakes; they are either on or off. On the metadata graph, the horizontal bar representing the brakes only appears when the brakes are on.

The **speed data** section shows the following speed information tracked by the system, as applicable:

- GPS patrol speed
- Radar patrol speed
- Radar lock speed
- Radar fastest/target speed

The speed metadata is plotted on the graph as connected points showing speed over time.

When you move your mouse over any of the input or speed data points, a popup box appears showing more information about that plotted point.

### Event video trim

*Note:* You must have permissions to export recorded events to have access to the video trim tool.

You use the video trim tool to trim a video to just the section you want to export. The trim tool allows you to view the video so you can see exactly where to make the edits. You can click and drag the starting point and the ending point of the section, or enter the start and end points or times and the tool trims the video for you.

For instructions how to trim an event video, see *Trimming event video* on page 86.

*Note:* Trimming a video does not delete the parts you trimmed from Evidence Library 4 Web (EL4 Web). The entire video is still part of the recorded event in EL4 Web.

To access the trim tool for a camera view:

- In the playback controls of the **Recorded Event Playback** page, click the **Trim** icon ( ).

*Note:* You can only access the trim tool when playing back the originally selected event as a single event or as a **1-Up** synchronized event. For more information about playback options, see *Playing Back Recorded Events* on page 62.
The trim tool opens showing the video playback for the camera view you want to trim. If you are trimming an event that was recorded by the 4RE DVR, the metadata graph also opens below the video playback screen.

Once you set your start and end points for the trimmed section, the starting frame and ending frame of the trimmed section appear as two smaller images to the right of the playback screen.

The trim tool contains the following sections and elements:

- **Playback screen**: Functions as a smaller version of the Recorded Event Playback page for a single event or for 1-Up synchronized playback

  For information on Recorded Event Playback, see Playing Back Recorded Events on page 62.

  You can use playback on the trim tool to view the video and help you determine where you want your trimmed section to start and end.

- **Subtitles**: Shows the metadata that appears as captions or subtitles on the screen during video playback

- **Start and end images, points, or times**: Shows the first and last frames of the trimmed section, as well as the start point or time and end point or time in the full video

  You can enter values in the fields below the images to set either:

  - **Duration**: Click Duration, then enter the start and end points of the section you want to keep and export

    For example, your original video lasts one hour. You need to export the middle half hour. Under the first image, you enter the start point as 15 minutes, meaning the trimmed video starts at 15 minutes into the original video. Under the second image, you enter the end point as 45 minutes, meaning the trimmed video ends at 45 minutes from the start of the original video.
Chapter 3. Working with Recorded Events

- **Date/Time**: Click **Date/Time**, then enter the start and end dates and times of the section you want to keep and export

  For example, your original video starts at 11:43 P.M. (23:43) and ends at 12:43 A.M. (00:43). You need to export the middle half hour. Under the first image, you select the earlier date from the date drop-down list, then enter the start time as 23:58:00. Under the second image, you select the later date from the date drop-down list, then enter the end time as 00:28:00.

  **Important!** Click the green **save button** next to each set of start and end point/time fields to accept the values you entered. When you click the save button, the corresponding video frame appears as the image and the start or end point handle moves to that position over the metadata graph.

- **Start and end point handles**: (4RE DVR events only) Click and drag the start and end point handles to the beginning and the end of the section of the video you want to keep and export; once you have moved the handles, the start and end images (and associated start and end points or times) change to match the locations of the handles within the video

  **Note**: If no metadata is included with the event, the start and end point handles are not available.

- **Trimmed video shaded area**: (4RE DVR events only) Shows the area of the trimmed video laid over the metadata graph for the whole, original video

- **Metadata graph**: (4RE DVR events only) Shows the metadata graph corresponding to the view you selected to trim

  For information on the metadata graph, see *Viewing recorded event metadata* on page 82.

- **Play Selection button**: Click **Play Selection** to play back the section of the video between the start and end point handles

- **Export Video button**: Click **Export Video** to open the **Export Worksheet** for the video you just trimmed

  For information on exporting trimmed video, see *Exporting a Trimmed Video* on page 131.

- **Cancel Trim button**: Click **Cancel Trim** to cancel any activities you performed during the current trim session

  **Trimming event video**

  **Note**: You must have permissions to export recorded events to have access to the video trim tool.

If you want to export a piece of video from a recorded event, you can use the video trim tool to trim the video to just the section you want to export.

For information about the video trim tool, see *Event video trim* on page 84.
To trim an event video:

1. On the **Events** tab, click the **Play** icon on the thumbnail image for the event you want to trim. The **Recorded Event Playback** page opens for the event you selected.

![Recorded Event Playback](image1)

2. If the camera view that you want to trim is playing back, click the **Trim** icon ( sliders) in the playback controls.

   If the camera view that you want to trim is NOT playing back, in the selected event section of the **Camera Views Panel**, click the camera view that you want to trim, then click the **Trim** icon ( sliders) in the playback controls.

   **Important!** You can only trim camera views that are part of an event you selected from the **Events** tab.

The trim tool opens for the camera view you selected. A 4RE DVR event includes the metadata graph with trim handles.

![Trim Tool](image2)
Chapter 3. Working with Recorded Events

A VISTA event does not include the metadata graph.

3. **For a 4RE DVR event**, click and drag the start point handle to the place in the video where you want to start the trimmed section.
For a VISTA event, with **Duration** selected, enter the start point of the section of video you want to export, for example, 30 seconds into the original video, then click the green save button.

---

**Important!** Click the green save button next to each set of start and end point/time fields to accept the values you entered.

---

4. **For a 4RE DVR event,** click and drag the end point handle to the place in the video where you want to end the trimmed section.
Chapter 3. Working with Recorded Events

For a VISTA event, with Duration still selected, enter the end point of the section of video you want to export, for example, 2 minutes into the original video, then click the green save button. (A start point of 30 seconds into the video and an end point of 2 minutes into the video produce a trimmed section in the middle of the video that is 1 minute and 30 seconds in duration.)

Important! Click the green save button next to each set of start and end point/time fields to accept the values you entered.

5. Click Play Selection to verify that you have the video you want in the trimmed section.
6. Adjust the start or end points as needed to include the video you want in the trimmed section.
7. Click Export Video.

The Export Worksheet opens for the trimmed video.

For information about exporting trimmed video, see Exporting a Trimmed Video on page 131.

Tip: To save a trimmed video, export it to a folder, navigate to the folder, then save the file where you want it.

If needed, you can then attach the file containing the trimmed video to a case, as a non-event file. For instructions how to attach a non-event file to a case, see Adding Other Files to a Case on page 109.
Viewing and Editing Event Details

**Note:** Depending on your system permissions, you may be able to view event details but not edit them. If you have permissions to edit details, you may only have permissions to edit the event tags.

In Evidence Library 4 Web (EL4 Web), you can view and edit recorded event details using the Recorded Event Details page. When Recorded Event Details opens, the basic event details (page 92) and Import Properties (page 94) show for the event you selected. Only the Event Notes field is editable. You can edit other event details fields in the basic details section, if you have the correct permissions.

From Recorded Event Details, you can also:

- Play back recorded events
- Export an event
- Add the event to a case
- Archive the event
- View an event that is linked to the current event or unlink it from the current event
  For information on the event details Linked Events tab, see Viewing linked event detail information on page 95.
- View and work with any cases that are associated with the event or remove the event from a case
  For information on the event details Cases tab, see Viewing case event detail information on page 96.
- View the audit log for the event
  For information on the event audit log, see Viewing the event audit log on page 97.

**Note:** The actions that are available to you from Recorded Event Details depend on your assigned permissions. Not all of the above actions will be available to every user. For more information on roles and permissions in EL4 Web, see Security Management Roles on page 354.

To access Recorded Event Details:

- On the Events tab, click the Event Details icon on the thumbnail image for the event whose details you want to view.
  Or
- On the Events tab, click the Actions menu icon for the event whose details you want to view, then select Event Details.
Chapter 3. Working with Recorded Events

The **Recorded Event Details** page opens in the browser window.

![Recorded Event Details Page](image)

**Basic event details section**

The fields in the basic event details section are the only fields that can be edited. You must have the correct permissions assigned to you to edit event details.

**Note:** If you have edit permissions, you may only be able to edit the **Event Category** and **Secondary Event Tags** fields.

To open the fields for editing in basic event details:

- **On Recorded Event Details**, click **Edit Details**.

The editable fields in the basic event details section open for editing and the **Edit Details** button changes to **Cancel** and **Save Changes**.

![Basic Event Details](image)

The basic event details section of the **Recorded Event Details** page includes the following elements:

- **Event Playback button**: Click **Event Playback** to move to **Recorded Event Playback** for the event whose details are displayed
  - For information about playing back a recorded event, see Playing Back Recorded Events on page 62.
- **Event start date and time**: Shows the date and time that the recorded event started
- **Vehicle/Device name**: Shows the name of the 4RE DVR or VISTA Body Camera that recorded the event
- **Officer name**: Shows the name of the officer who recorded the event
- **Event category**: Shows the event category assigned by the officer when the event was recorded or when it was imported
- **Export**: Click **Export** to open the **Export Worksheet** for the event whose details are displayed. For information about exporting events and the **Export Worksheet**, see *Export Worksheet and My Exports* on page 136.
- **Add to Case**: Click **Add to Case** to open the **Add Event to Case** dialog box for the event whose details are displayed. For information on adding a recorded event to a case in Case Management, see *Adding a Recorded Event to an Existing Case* on page 106.
- **Archive Event**: Click **Archive Event** to move the event whose details are displayed to the archive storage location. For information on archiving an event, see *Manually Archiving Events* on page 98.
- **Event ID**: Shows the system-defined unique identifier for the recorded event
- **Date**: Shows the date and time that the recorded event started
- **Officer**: Shows the name of the officer who recorded the event; this field is editable. To edit the **Officer** field, with the fields open for editing, click the field and select the name of the officer who recorded the event.
- **Vehicle/Device**: Shows the name of the 4RE DVR or VISTA Body Camera that recorded the event; this field is editable. To edit the **Vehicle/Device** field, with the fields open for editing, click the field and select the name of the 4RE or VISTA that recorded the event.
- **Event Category**: Shows the event category assigned by the officer when the event was recorded or when it was imported; the field is editable. To edit the **Event Category** field, with the fields open for editing, click the field and select the event category that should be assigned to the recorded event.
- **Prevent Archive**: Indicates whether the recorded event is marked to prevent it from being archived; the field is editable. For information on your system’s archive and purge criteria, see *Managing Evidence Retention and Cleanup* on page 257. To edit the **Prevent Archive** field, with the fields open for editing, click the field to change between **No** (the event will be archived as normal) and **Yes** (the event will not be allowed to be archived).

  **Note**: If you mark an event to prevent it from being archived, it cannot be purged either.

- **Restrict Access**: Indicates whether the recorded event has its access restricted to only users who have been assigned the correct permissions in the system; the field is editable.
For information on roles and permissions in Evidence Library 4 Web (EL4 Web), see Security Management Roles on page 354.

To edit the Restrict Access field, with the fields open for editing, click the field to change between No (access to the event will not be restricted) and Yes (access to the event will be restricted).

- Prevent Purge: Indicates whether the recorded event is marked to prevent it from being purged; the field is editable

For information on your system's archive and purge criteria, see Managing Evidence Retention and Cleanup on page 257.

To edit the Prevent Purge field, with the fields open for editing, click the field to change between No (the event will be purged as normal) and Yes (the event will not be allowed to be purged).

- Secondary Event Tags: Shows the event tags other than Event Category that were entered by the officer when the event was recorded or when it was imported; the fields are editable

For information on setting up secondary tags, see Creating secondary event tags on page 332.

To edit the Secondary Event Tag fields, with the fields open for editing, click the field you want to edit and either select the new answer or enter the new answer for the secondary event tag.

- Edit Details button: Click Edit Details to open the basic event details fields for editing

- Event Notes: Shows any notes entered about the recorded event; the field is editable

To edit the Event Notes field, click in the field, enter a new note or edit an existing note, then click Save Note.

Import Properties

The Import Properties section of the event details shows information about the import of the recorded event.

The Import Properties section includes the following fields:

- Import Date: Shows the date and time that the recorded event was imported to Evidence Library 4 Web (EL4 Web)
- Import Source: Shows the method used to import the recorded event (Wireless, USB, etc.)
- Tick Range: Shows the internal 4RE DVR or VISTA Body Camera system tracking values that indicate when the event begins and ends
Viewing linked event detail information

**Note:** Each tick is one-half second, so the tick range provides a time reference for the video.

- **Event ID**: Shows the system-defined unique identifier for the recorded event
- **Size**: Shows the storage size, MB or GB, of the recorded event
- **Location**: Shows the path to the storage location that the recorded event was imported into

**Note:** Other fields may be present in the Import Properties, depending on your system setup. If you have questions about the information you see in Import Properties, contact WatchGuard customer service.

Viewing linked event detail information

From the bottom of the Recorded Event Details, you can view any events that are linked to the current event.

To see a list of events that are linked to the current event:

- At the bottom of Recorded Event Details, click the Linked Events tab.

![Linked Events](image)

The linked event record shows some of the basic event information for a linked event:

- Linked event start date and time
- Name of the officer who recorded the linked event
- Name of the device where the linked event was recorded
- Event category assigned to the linked event

You can also perform some basic functions for the linked event using the linked event Actions menu icon:

- Play back the linked event
  For information on playing back a recorded event, see Playing Back Recorded Events on page 62.
- View the details for the linked event
  For information on viewing and editing event details, see Viewing and Editing Event Details on page 91.
- Unlink the event from the current event
  For information on unlinking events, see Unlinking events on page 61.
Chapter 3. Working with Recorded Events

**Note:** Depending on your permissions, if the linked event is not yours, you may not be able to view or work with it.

### Viewing case event detail information

If you have the correct permissions, from the bottom of the **Recorded Event Details**, you can view any cases that are associated with the current event.

To see a list of cases that are associated with the current event:

- At the bottom of **Recorded Event Details**, click the **Cases** tab.

![Associated Cases](image)

The case record shows some of the basic information for the case associated with the current event:

- Case number
- Name of the user who created the case
- When the case was created
- How many events are included in the case
- How many links are included in the case
- How many other files are included in the case

You can also perform some basic functions for the associated case using the cases **Actions** menu icon:

- Open and view the associated case and its attachments in Case Management
  
  For information on cases in Case Management, see Chapter 4. Working with Cases on page 101.

- Export the case
  
  For information on exporting cases, see Exporting Cases on page 134.

- Remove the current recorded event from the associated case
  
  For information on removing an event from a case, see Removing a recorded event from a case on page 108

**Note:** Depending on your permissions, if the case is not yours, you may not be able to view or work with it.
Viewing the event audit log

If you have the correct permissions, from the bottom of the **Recorded Event Details**, you can view the **Audit Log** for the current event. The **Audit Log** lists all the historical information about the current recorded event, including:

- When it was imported into Evidence Library 4 Web (EL4 Web) and the details of that import
- When it was exported and by whom
- When it was played back and by whom
- When its properties were modified and by whom

To view the audit log for an event:

- At the bottom of **Recorded Event Details**, click the **Audit Log** tab.

To view the details about each high-level action:

- Click the + sign next to the action you want to view in depth.

You can filter the list of high-level actions if you want to view only one type of action:

- Click the **Filter By** field and select which type of action you want to view.

The possible high-level actions recorded in the audit log include (in alphabetical order):

- **Archived**: Lists the details about the archiving of the recorded event
- **Created**: Lists the details about the initial transfer of the recorded event from the device to the EL4 Web system
- **Downloaded**: Lists the details about the downloading of the export package
- **Exported**: Lists the details about the packaging of the recorded event export
- **Imported**: Lists the details about the transfer of the recorded event into the EL4 Web database and video storage location
- **Modified**: Lists the details about any modifications made to the recorded event and its event details
- **Move**: Lists the details about the movement of an event into and through the EL4 Web storage locations
- **Restored**: Lists the details about the restoration of the recorded event from an archive storage location
- **Shared**: Lists the details about sharing the recorded event on EvidenceLibrary.com using CLOUD-SHARE
Chapter 3. Working with Recorded Events

- **Uploaded**: Lists the details about the staging of the recorded event in the EL4 Web system for import to the video storage location
- **Viewed**: Lists the details about the playback and review of the recorded event

Manually Archiving Events

**Note**: If you have access to the Evidence Management module, you can set up your system to automatically archive recorded events after a certain time period. For information on automatically archiving recorded events, see Managing Evidence Retention and Cleanup on page 257.

If you have the correct permissions, you can manually archive a recorded event to the Evidence Library 4 Web (EL4 Web) **Offline Archive** storage location. When you archive an event, you move its video and some associated data files to the archive storage location. A record of the archived event, including its metadata, remains in the database; an event search can find the archived event database record.

To view any of the archived event’s video or data, you must restore the event from the archive storage location to the video storage location. For instructions how to restore an archived event, see **Restoring archived events** on page 99.

On the **Events** tab, an archived event's record has a placeholder for the thumbnail image and shows a crosshatched pattern as its background.

To manually archive recorded events:

1. On the **Events** tab, locate the event you want to manually archive.
2. Click the **Actions** menu icon for the event you want to manually archive and select **Archive Event**.

   ![Archive Event Menu]

   The **Confirm** dialog box opens asking you to confirm that you want to archive the event.
3. Click **Yes**.

The event you selected for archive is added to the archive queue.

---

**Note:** The system periodically runs a process that moves any events in the archive queue to the **Offline Archive** storage location.

---

Once the event has been successfully moved to the archive storage location, the event record shows a placeholder thumbnail image and a crosshatched background.

---

**Restoring archived events**

If you have the correct permissions, you can restore an event that has been archived either manually or automatically.

---

**Tip:** You cannot restore an event until it has been moved to the **Offline Archive** storage location. The system periodically runs the archive process. If the event you want to restore is still waiting for that archive process to run, you cannot restore the event until the process has finished with it.

---

To restore events from the **Offline Archive** storage location:

1. On the **Events** tab, locate the event you want to restore.
2. Click the **Actions** menu icon for the event you want to restore and select **Restore Event**.

The system starts the restore process. When the system has finished restoring the event, the event appears on the **Events** tab as normal.
Manually Purging Events

Note: If you have access to the Evidence Management module, you can set up your system to automatically purge recorded events after a certain time period. For information on automatically purging recorded events, see Managing Evidence Retention and Cleanup on page 257.

If you have the correct permissions, you can manually purge a recorded event from Evidence Library 4 Web (EL4 Web) storage. When you purge an event, you remove it and any associated data from the database completely.

Warning! A recorded event that has been purged from the EL4 Web database cannot be recovered or restored from EL4 Web.

To manually purge recorded events from the EL4 Web database:

1. On the Events tab, select the event or events you want to purge.
2. Click the Actions menu icon for one selected event, or Group Actions for multiple selected events, then select the Purge option from the applicable menu.
   For information on both the Actions and the Group Actions menus, see Actions menus on page 57.
   The Confirm dialog box opens.

3. Click Yes.
   The events you selected are purged.

Important! You cannot purge a recorded event that is part of a case in Case Management. For information about Case Management, see Chapter 4. Working with Cases on page 101.
Chapter 4. Working with Cases

In this chapter...

- Creating a new case (page 103)
- Adding a recorded event to a case (page 106)
- Adding other files to a case (page 109)
- Adding links to a case (page 111)
- Searching for a case (page 113)
- Viewing case attachments (page 114)
- Adding a caseworker to a case (page 117)
Overview

A case, in Evidence Library 4 Web (EL4 Web), is a mechanism to help you associate media and other files that relate to each other. For example, if two different vehicles recorded the same event, you can add both recorded events to the same case to associate them.

You can also add related links, images, documents, audio, or other types of files to the case. EL4 Web Case Management supports most file formats.

EL4 Web Case Management includes the following functions:

- Creating a new case (page 103)
- Adding recorded events to a case (page 106)
- Adding other files to a case (page 109)
- Adding links to a case (page 111)
- Searching for a case (page 113)
- Viewing case attachments (page 114)
- Adding a caseworker to a case (page 115)
- Exporting cases (page 134)

**Note:** To work with cases or assign case workers to a case, you must have the correct permissions assigned by your system administrator in EL Administrator Security Management. If you need access to Case Management, contact your system administrator.
Creating a Case

When you create a new case, typically you start with a recorded event from the Events tab and build the case around it.

**Important!** When you include a recorded event in a case, any purge and archive rules that would normally apply to the event no longer apply. For example, you add a recorded event that has a category of Traffic Warning to a case. Even though Traffic Warning events are normally purged after 30 days, the event will not be purged, as long as it is part of the case.

Once the event is no longer part of a case, it is again subject to purge and archive rules. If the event is older than 30 days, it will be automatically purged the next time data cleanup is run on the system. For information on purge and archive rules and data cleanup, see Evidence retention rules on page 259.

To create a new case:

1. On the Events tab, click the Actions menu icon for the recorded event you want to create a new case with, then select Add to Case.

   ![Add Event to Case](image)

   **Tip:** You can add more than one recorded event to a case at the same time. Select the events you want to add to a case, then click Group Actions (near the top right of the Events tab) and select Add Selected to Case.

   The Add Event to Case dialog box opens.
Chapter 4. Working with Cases

2. On the **New Case** tab, enter the new **Case Number** and any applicable **Case Notes**, then click **Save Changes**.

![Add Event to Case](image)

The system creates the new case with the selected recorded event. The **Case** icon (●) is added to the event listing on the **Events** tab, showing that the event is part of a case.

3. Navigate to the **Cases** tab.

4. Locate the case you just created, click the **Actions** menu icon for that case, and then select **View Case**.

**Tip:** You can also click the large **Case** icon on the left of the case record to view the **Case Details**.

**Note:** If the case you just created does not show on the **Cases** tab, click **Search** on the **Cases** tab.
Deleting a case

The **Case Details** open for the case you just created, showing the attached recorded event you started with.

![Case Details screenshot](image)

**Tip:** You can also create a new case without a recorded event. On the **Cases** tab, click **Create New Case**. Once the case is created, you can add recorded events and other items as you would for an existing case.

Once you have created the case, you can add:

- Other files (page 109) and links (page 111) from the **Case Details**
- Other recorded events (page 106) from the **Events** tab

### Deleting a case

A case in EL4 Web is a mechanism to associate recorded events and other files. When you delete a case, you remove the association between case items and delete the non-recorded event files and links. Any events that were part of the case are not deleted.

To delete a case:

- On **Case Details**, click **Delete Case**.

![Delete Case screenshot](image)
Chapter 4. Working with Cases

Adding a Recorded Event to an Existing Case

You can add a recorded event to an existing case, even if there is already a recorded event associated with the case. When you add a recorded event to a case, you start with the recorded event you want to add (rather than from the case you want to add it to).

**Note:** You must know the case number of the case that you want to add the event to.

To add a recorded event to an existing case:

1. On the **Events** tab, click the **Actions** menu icon for the recorded event you want to add to a case.

   ![Actions menu icon](image)

   **Tip:** You can add more than one recorded event to a case at the same time. Select the events you want to add to a case, then click **Group Actions** (near the top right of the **Events** tab) and select **Add Selected to Case**.

   The **Add Event to Case** dialog box opens.

2. Click the **Existing Case** tab, then start entering the number of the case you want to add the event to.

   ![Add Event to Case dialog box](image)

3. Select the applicable case number from the drop-down list, then click **Save Changes**.

   The system adds the recorded event to the existing case you selected. The **Case** icon ( ) is added to the event record on the **Events** tab, showing that the event is part of a case.
Adding a Recorded Event to an Existing Case

**Important!** When you include a recorded event in a case, any purge and archive rules that would normally apply to the event no longer apply. For example, you add a recorded event that has a category of Traffic Warning to a case. Even though Traffic Warning events are normally purged after 30 days, the event will not be purged, as long as it is part of the case.

Once the event is no longer part of a case, it is again subject to purge and archive rules. If the event is older than 30 days, it will be automatically purged the next time Data Cleanup is run on the system. For information on purge and archive rules and data cleanup, see Evidence retention rules on page 259.

4. Navigate to the **Cases** tab.

**Tip:** You can click the **Case** icon on the event record to take you directly to the **Case Details** for the case you added the event to.

5. Locate the case you just added an event to, click the **Actions** menu icon for that case, and then select **View Case**.

**Tip:** You can click the large **Case** icon on the left of the case record to view the **Case Details**.

![Found 10 Cases - 0 records selected](image)

**Note:** If the case you just added an event to does not show on the **Cases** tab, click **Search** on the **Cases** tab.
Chapter 4. Working with Cases

The Case Details open for the case you just added an event to, showing that the recorded event you just added is attached.

Removing a recorded event from a case

You can remove a recorded event from a case. Removing events from a case does not delete the events; it removes the association between those events and the rest of the items in the case.

To remove a recorded event from a case:

- **On Case Details**, click the Actions menu icon for the event you want to remove from the case and select Remove Attachment.

To remove multiple events from a case, on the Case Details page:

- Select the attachments you want to remove, click Group Actions, then select Delete Selected Attachments.
Adding Other Files to a Case

You can add any image, document, audio, or other type of file to a case, one or multiple at a time. Case Management supports most file formats.

You use the **Add New Attachment(s)** button on the Case Details page to add non-event files to the case.

To add non-event files to a case, on the Case Details page:

1. Click **Add New Attachment(s)**.

The **Add Case Attachment(s)** dialog box opens.

![Add Case Attachment(s) dialog box](image-url)
Chapter 4. Working with Cases

2. Perform one of these actions:
   - Click the central area of the **Case Attachment(s)** dialog box, navigate to, then select the files you want to attach to the case.
   - Or
   - Navigate to the files you want to attach, select them, then drag and drop them into the central area of the **Case Attachment(s)** dialog box.

![Add Case Attachment(s)](image)

3. Click **Add Attachment(s)**.

The **Case Details** reappear, showing the additional attachment.

![Case Details](image)

Deleting non-event files from a case

You can delete files that are not recorded events from a case. When you delete a non-event file from a case, the file is deleted from Evidence Library 4 Web (EL4 Web) storage. To access it again from within EL4 Web, you must re-add the file to the case.
Adding Links to a Case

To delete a single non-event file from a case, on the **Case Details** page:

- Click the **Actions** icon for the file you want to delete and select **Delete Attachment**.

To delete multiple non-event files from a case, on the **Case Details** page:

- Select the attachments you want to delete, click **Group Actions**, then select **Delete Selected Attachments**.

Adding Links to a Case

You can add a link to a file or a web page to a case.

You use the **Add Link Attachment** button on the **Case Details** to add a link to the case.

To add a file or web-page link to a case, on the **Case Details** page:

1. Click **Add Link Attachment**.
Chapter 4. Working with Cases

The **Add Case Link** dialog box opens.

2. Enter the **Link URL** in the field, then click **Add Case Link**.

---

**Note:** Click outside the field if the **Add Case Link** button does not become active when you enter or paste a URL in the **Link URL** field.

---

The **Case Details** reappear, showing the additional attachment.

Deleting a link from a case

You can delete a link from a case. When you delete a link from a case, the link reference is deleted from Evidence Library 4 Web (EL4 Web) storage. To access the link again from within EL4 Web, you must re-add the link to the case.

To delete a link from a case, on the **Case Details** page:

- Click the **Actions** icon for the link you want to delete and select **Delete Link**.
To delete multiple links from a case, on the **Case Details** page:

- Select the attachments you want to delete, click **Group Actions**, then select **Delete Selected Attachments**.

### Searching for a Case

You can search for cases just as you do for recorded events using the **Case Search** pane on the **Cases** tab. When you run a search in Evidence Library 4 Web (EL4 Web) Case Management, the system produces a list of cases that fit the criteria you entered for the search.

To search for a case in EL4 Web:

1. Navigate to the **Cases** tab.

   The **Cases** tab appears showing the **Case Search** pane on the left and the empty **Found Cases** pane on the right.

2. Enter your case search criteria then click **Search**.

   The cases fitting your search criteria appear in the **Found Cases** pane.
Viewing Case Attachments

You can view, open, or access any of the items (recorded events, other files, links) you attached to a case from the Cases tab.

To work with items attached to a case:

1. On the Cases tab, locate the case whose attachments you want to work with.
2. Click the Actions menu icon for that case, and then select View Case.

   **Tip:** You can also click the large Case icon on the left of the case record to view the Case Details.

3. The Case Details open for the case you selected.
4. Locate the attachment you want to work with.

   1. Click the Actions menu icon for that attachment, and then select the applicable option.

      **Tip:** You can also click the large attachment icon on the left of the record to access the attachment.

If the attachment is an event, the event opens in the playback or details page, as selected. If the attachment is a non-event file, the file is downloaded to the browser Downloads folder. If the attachment is a link, the link opens in a new browser tab.
Adding Case Workers to a Case

**Note:** To create and work with cases or assign case workers to a case, you must have the correct permissions assigned by your system administrator in EL Administrator Security Management. If you do not see the Cases tab in EL4 Web, or do not have all of the Case Management functionality, contact your system administrator to verify your assigned permissions.

If you have permissions, the Case Workers tab allows you to add case workers to a case and assign them case-specific permissions.

To add case workers to a case:

1. On the Cases tab, locate the case you want to add case workers to.
2. Click the Actions menu icon for that case, and then select View Case.

**Tip:** You can also click the large Case icon on the left of the case record to view the Case Details.

The Case Details open for the case you selected.
Chapter 4. Working with Cases

3. Click the **Case Workers** tab.

   The **Case Workers** tab appears, showing any case workers that have already been assigned.

   !important! The case creator, as well as users with the **Case Manager** or **Administrator** role, can always access and work with the case. They do not need to be assigned to the case as case workers.

4. Click **Add Case Workers**.

   The **Add Case Worker** dialog box opens

5. Click the **Select Case Worker** field and select the case worker you want to give permission to view and/or work with the case.

   **Tip:** You do not need to add the case creator or any **Case Manager** or **Administrator** users.

6. Click the **Assign Permissions** field and select the case-specific permissions level you want to assign to the case worker you selected.
7. Click **Save Changes**.

The case worker you selected is added to the list of **Assigned Case Workers** with the case-specific permissions level you selected.

**Tip:** To edit the **Assigned Case Workers** record, click the pencil icon (✍️), then on the **Edit Case Worker** dialog box, select a different name or case-specific permissions level. Click the **X** to remove the case worker from the case.

8. Repeat steps 4 through 7 as needed to add case workers to the case.

**Using the Case Workers tab**

The **Case Workers** tab under **Case Details** shows you which case workers are assigned to the case and what their case-specific permission level is. If you have permissions, the **Case Workers** tab also allows you to add case workers to a case and assign them case-specific permissions. For instructions how to add case workers to a case as well as assign them case-specific permissions, see *Adding Case Workers to a Case* on page 115.

The case creator, as well as users with the **Case Manager** or **Administrator** role, can always access and work with the case. You do not need to add them to the case as case workers.

**Tip:** Because users who have the **Case Manager** or **Administrator** user role automatically have full access to all cases, you do not need to add them to any case. For more information about user roles and associated permissions, see *Security Management Roles* on page 354.
Chapter 4. Working with Cases

When you add other case workers to a case (NOT the case creator or Case Manager/Administrator users), you assign them case-specific permissions at the same time. The Assigned Case Workers permission level options are:

---

**Important!** The permission levels assigned to a case worker on the Case Workers tab are applicable only for the current case.

---

- **Read-Only**: Allows the assigned case workers to view the list of case attachments and workers for the current case, as well as play back any recorded events in the case.
- **Add Attachments**: Gives the assigned case workers all of the Read-Only permissions AND allows them to add attachments to the case.
- **Full Access**: Allows the assigned case workers full access to view all case attachments, add and delete attachments, or delete the case itself; allows the assigned case workers to add or remove other case workers to the case and change their permission levels.

---

**Note:** If an assigned case worker has the Case Manager or Administrator user role, you cannot remove that case worker or change his permission level.
Chapter 5. Exporting Evidence

In this chapter...

- Exporting a recorded event (page 121)
- Exporting multiple recorded events (page 124)
- Exporting a Sync Export video/audio combination (page 127)
- Exporting a trimmed video (page 131)
- Exporting cases (page 134)
- Using the Export Worksheet and My Exports tab (page 136)
- Exporting to media destination types (page 143)
- Configuring media export preferences (page 146)
- Exporting using CLOUD-SHARE (page 148)
- Configuring the CLOUD-SHARE export options (page 150)
- Using the WatchGuard single event export player (page 161)
- Using the WatchGuard synchronized event export player (page 164)
Overview

To view a video, a recorded event, or other Evidence Library 4 Web (EL4 Web) item outside of EL4 Web, you must export it. All the parameters for exporting from EL4 Web are set on the Export Worksheet and tracked on the My Exports tab. For information on the Export Worksheet and the My Exports tab, see Export Worksheet and My Exports on page 136.

**Important!** You must have the Evidence Library Transfer Agent installed on your computer in order to access some of the export functionality. You can download the Transfer Agent from the Manage tab in EL4 Web.

When exporting evidence, you can:

- Export a single recorded event (page 121)
- Export multiple recorded events (page 124)
- Export a Sync Export video/audio combination (page 127)
- Export a trimmed video (page 131)
- Export cases (page 134)
- Configure (page 146) and export (page 143) to multiple media destinations
- Configure (page 150) and export (page 148) using CLOUD-SHARE

Once exported, under certain conditions, you can view the exported video with the WatchGuard Video Player for single events (page 158) or the WatchGuard Video Player for synchronized events (page 164).

**Note:** To export from EL4 Web, you must have the correct permissions. If you do not see the options for export, contact your system administrator.
Exporting a Recorded Event

To export a single recorded event:

1. On the Events tab, click the Actions menu icon for the event you want to export, then select Export Event from the Actions menu.
   
   For information about events listed on the Events tab, see Working with search results on page 52.
   
   The Export Worksheet opens for the event you selected.
   
   For information about the sections on the Export Worksheet, see Export Worksheet on page 137.

   ![Export Worksheet](image)

   **Note:** If the recorded event you selected to be exported is linked to other events, by default the linked events are included in the export. The export then works like a multiple event export. If you do not want to include a linked event in the export, clear the selection checkbox for the linked event that you do not want to include. For information about exporting multiple events, see Exporting Multiple Recorded Events on page 124.

2. If you do not want to export all the available camera views, clear the checkboxes in the Cameras section for the views that you do NOT want to export.

   **Note:** All the camera views are checked for inclusion in the export by default.
Chapter 5. Exporting Evidence

3. On the Media Export tab, if you want to export in Original Format, go to step 5.

   Note: WatchGuard’s Original Format is MP4.

If you want to export to the secure cloud using CLOUD-SHARE, go to step 8.
If you want to export to media using a different video format than the WatchGuard Original Format, click Change.
The drop-down list of available video formats opens.

4. Select the format you want to use to export the recorded event, then enter any applicable export parameters for the format you selected.
   For information about the video format options, see Choose a Format for Media Export on page 140.

5. Confirm whether you want to include the WatchGuard Player with the export.
   For information about the WatchGuard Player, see WatchGuard Single Event Player on page 158.

6. Confirm whether you want to include subtitles with the exported video, and how you want to include them.
   For information about including subtitles in the exported video, see Including on-screen text on page 142.

7. Select the export destination, then enter any applicable export parameters for the destination you selected.
   For information about media export destinations, see Select a Destination for Media Export on page 143.
   After you have finished entering information about your export destination, go to step 10.

8. Click the CLOUD-SHARE tab.
   The CLOUD-SHARE tab appears.
9. On the **CLOUD-SHARE** tab, enter:
   a. The recipients for your shared evidence
   b. The number of days you want the shared evidence to be available on the CLOUD-SHARE site
   c. The type of security the recipients must use to access the shared evidence

   !important! Depending on the type of security you select, there may be other fields you need to fill in.

d. Whether you want to include subtitles in your exported shared evidence

For information about the fields on the **CLOUD-SHARE** tab, see *Export Using CLOUD-SHARE* on page 148.

10. Enter a **Reference Label** for the export, then click **Prepare Export**.

For information about the label for the export, see *Export Summary* on page 155.

The **Export Worksheet** for the export closes. The export appears on the **My Exports** tab, its status showing where it is in the export process.

For information about the **My Exports** tab, see *Using the My Exports tab* on page 156.

How long the export takes depends on the size of the recorded event, whether you export using media or CLOUD-SHARE, and any options you select for the media export.

**Note:** If a local computer is involved in the export (for a local-computer or burn-to-disc destination), the local computer’s performance will also affect the speed of the export.
Chapter 5. Exporting Evidence

Exporting Multiple Recorded Events

You can export multiple events together, but all the recorded events must use the same export parameters.

To export multiple recorded events together:

1. On the Events tab, select all of the events that you want to export together, click Group Actions, then select Export Selected Events.

The Export Worksheet opens for the events you selected.

For information about the sections on the Export Worksheet, see Export Worksheet on page 137.

2. If you do not want to export all the available camera views for any of the events, clear the checkboxes in the Cameras sections for the views that you do NOT want to export.

Note: All the camera views are checked for inclusion in the export by default.
3. On the **Media Export** tab, if you want to export in **Original Format**, go to **step 5**.

   **Note:** WatchGuard’s **Original Format** is MP4.

If you want to export to the secure cloud using CLOUD-SHARE, go to **step 8**.
If you want to export to media using a different video format than the WatchGuard **Original Format**, click **Change**.

The drop-down list of available video formats opens.

4. Select the format you want to use to export the recorded events, then enter any applicable export parameters for the format you selected.
   
   For information about the video format options, see *Choose a Format for Media Export* on page 140.

5. Confirm whether you want to include the WatchGuard Player with the export.
   
   For information about the WatchGuard Player, see *WatchGuard Single Event Player* on page 158.

6. Confirm whether you want to include subtitles with the exported video, and how you want to include them.
   
   For information about including subtitles in the exported video, see *Including on-screen text* on page 142.

7. Select the export destination, then enter any applicable export parameters for the destination you selected.
   
   For information about media export destinations, see *Select a Destination for Media Export* on page 143.

   After you have finished entering information about your export destination, go to **step 10**.

8. Click the **CLOUD-SHARE** tab.
   
   The **CLOUD-SHARE** tab appears.
Chapter 5. Exporting Evidence

9. On the CLOUD-SHARE tab, enter:
   a. The recipients for your shared evidence
   b. The number of days you want the shared evidence to be available on the CLOUD-SHARE site
   c. The type of security the recipients must use to access the shared evidence

   **Important!** Depending on the type of security you select, there may be other fields you need to fill in.

   d. Whether you want to include subtitles in your exported shared evidence

   For information about the fields on the CLOUD-SHARE tab, see Export Using CLOUD-SHARE on page 148.

10. Enter a Reference Label for the export, then click Prepare Export.

    For information about the label for the export, see Export Summary on page 155.

    The Export Worksheet for the export closes. The export appears on the My Exports tab, its status showing where it is in the export process.

    ![Export Worksheet](image)

    For information about the My Exports tab, see Using the My Exports tab on page 156.

    How long the export takes depends on the size of the included recorded events, whether you export using media or CLOUD-SHARE, and any options you select for the media export.

    **Note:** If a local computer is involved in the export (for a local-computer or burn-to-disc destination), the local computer’s performance will also affect the speed of the export.
Exporting a Sync Export Video/Audio Combination

When you export a Sync Export video/audio combination, the synced combination appears on the worksheet showing the Sync flag. The full events that contain the video and audio streams that make up the Sync Export are included on the worksheet as well. You can choose not to include the full events when you export.

You can export multiple Sync Export combinations together. You can export Sync Export combinations, recorded events, and trimmed videos together. All items exported together are exported using the same export parameters.

To export a Sync Export video/audio combination:

1. On the 1-Up player page, select the video and audio streams you want for the Sync Export, then select Sync Export from the Options menu.

For information about setting up a Sync Export video/audio combination for export, see Sync Export on page 70.
Chapter 5. Exporting Evidence

The Export Worksheet opens for the Sync Export. For information about the sections on the Export Worksheet, see Export Worksheet on page 137.

1. If you do not want to export the full events that contain the video and audio streams that make up the Sync Export are included in the list of items to export, by default. If you do not want to include the full events in the export package, clear the checkboxes for the full events.

Note: The full events that contain the video and audio streams that make up the Sync Export are included in the list of items to export, by default. If you do not want to include the full events in the export package, clear the checkboxes for the full events.

2. If you do not want to export all the available camera views for the full events, clear the checkboxes in the Cameras sections for the views that you do not want to export.

Note: All the camera views are checked for inclusion in the export by default.

3. On the Media Export tab, if you want to export in Original Format, go to step 5.

Note: WatchGuard’s Original Format is MP4.

If you want to export to the secure cloud using CLOUD-SHARE, go to step 8. If you want to export to media using a different video format than the WatchGuard Original Format, click Change.
The drop-down list of available video formats opens.

4. Select the format you want to use to export the audio/video combination, then enter any applicable export parameters for the format you selected.

For information about the video format options, see Choose a Format for Media Export on page 140.

5. Confirm whether you want to include the WatchGuard Player with the export.

For information about the WatchGuard Player, see WatchGuard Single Event Player on page 158.

6. Confirm whether you want to include subtitles with the exported video, and how you want to include them.

For information about including subtitles in the exported video, see Including on-screen text on page 142.

7. Select the export destination, then enter any applicable export parameters for the destination you selected.

For information about media export destinations, see Select a Destination for Media Export on page 143.

After you have finished entering information about your export destination, go to step 10.

8. Click the CLOUD-SHARE tab.

The CLOUD-SHARE tab appears.
Chapter 5. Exporting Evidence

9. On the CLOUD-SHARE tab, enter:
   a. The recipients for your shared evidence
   b. The number of days you want the shared evidence to be available on the CLOUD-SHARE site
   c. The type of security the recipients must use to access the shared evidence

   **Important!** Depending on the type of security you select, there may be other fields you need to fill in.

   d. Whether you want to include subtitles in your exported shared evidence

   For information about the fields on the CLOUD-SHARE tab, see Export Using CLOUD-SHARE on page 148.

10. Enter a Reference Label for the export, then click Prepare Export.

    For information about the label for the export, see Export Summary on page 155.

    The Export Worksheet for the export closes. The export appears on the My Exports tab, its status showing where it is in the export process.

    ![Export Worksheet](image)

    For information about the My Exports tab, see Using the My Exports tab on page 156.

    How long the export takes depends on the size of the included video and audio streams (as well as full events if applicable), whether you export using media or CLOUD-SHARE, and any options you select for the media export.

    **Note:** If a local computer is involved in the export (for a local-computer or burn-to-disc destination), the local computer’s performance also affects the speed of the export.
Exporting a Trimmed Video

Once you have finished trimming a video, you export it to save it in its new length. You can export multiple trimmed videos and recorded events together. For information about trimming video, see Trimming event video on page 86.

To export a trimmed video:

1. On the video trim tool, after you have finished trimming the video, click Export Video.

The Export Worksheet opens for the trimmed video. For information about the sections on the Export Worksheet, see Export Worksheet on page 137.
Tip: You can export multiple trimmed videos together. Leave the Export Worksheet open, trim another video, then click Export Video on the video trim tool. The additional trimmed video is added to the Export Worksheet. Just as for multiple recorded events exported together, multiple trimmed videos exported together must all use the same export parameters.

2. On the Media Export tab, if you want to export in Original Format, go to step 4.

Note: WatchGuard's Original Format is MP4.

If you want to export to the secure cloud using CLOUD-SHARE, go to step 7.

If you want to export to media using a different video format than the WatchGuard Original Format, click Change.

The drop-down list of available video formats opens.

3. Select the format you want to use to export the trimmed video, then enter any applicable export parameters for the format you selected.

   For information about the video format options, see Choose a Format for Media Export on page 140.

4. Confirm whether you want to include the WatchGuard Player with the export.

   For information about the WatchGuard Player, see WatchGuard Single Event Player on page 158.

5. Confirm whether you want to include subtitles with the exported video, and how you want to include them.

   For information about including subtitles in the exported video, see Including on-screen text on page 142.

6. Select the export destination, then enter any applicable export parameters for the destination you selected.

   For information about media export destinations, see Select a Destination for Media Export on page 143.

After you have finished entering information about your export destination, go to step 9.
7. Click the CLOUD-SHARE tab.

   The CLOUD-SHARE tab appears.

![Image of the CLOUD-SHARE tab]

8. On the CLOUD-SHARE tab, enter:
   a. The recipients for your shared evidence
   b. The number of days you want the shared evidence to be available on the CLOUD-SHARE site
   c. The type of security the recipients must use to access the shared evidence

   **Important!** Depending on the type of security you select, there may be other fields you need to fill in.

   d. Whether you want to include subtitles in your exported shared evidence

   For information about the fields on the CLOUD-SHARE tab, see Export Using CLOUD-SHARE on page 148.

9. Enter a Reference Label for the export, then click Prepare Export.

   For information about the label for the export, see Export Summary on page 155.

   The Export Worksheet for the export closes. The export appears on the My Exports tab, its status showing where it is in the export process.

   ![Image of the My Exports tab]

   For information about the My Exports tab, see Using the My Exports tab on page 156.

   How long the export takes depends on the size of the trimmed video, whether you export using media or CLOUD-SHARE, and any options you select for the media export.

   **Note:** If a local computer is involved in the export (for a local-computer or burn-to-disc destination), the local computer's performance will also affect the speed of the export.
Chapter 5. Exporting Evidence

Exporting Cases

When you export a case, all items appear on the Export Worksheet together, but you can choose not to include an item when you export.

Recorded event videos in a case can only be exported in the WatchGuard Original Format. Other format options are not available when you export a case.

**Tip:** If you need a video in the case to be in another video format, export the recorded event separately in the needed video format, then add the exported video file to the case as a new file (non-event file). When you export the case, the video in the format you need is exported with the case.

You can export multiple cases at a time, but you cannot add other recorded events or trimmed videos to the export outside of the case.

To export a case:

1. On the Cases tab, click the Actions menu icon for the case you want to export, then select Export Case from the Actions menu.
   
   For information about the cases that appear on the Cases tab, see Searching for a Case on page 113.

   The Export Worksheet opens for the case you selected.

   For information about the sections on the Export Worksheet, see Export Worksheet on page 137.
2. If you do not want to export all of the attachments included in the case, clear the checkboxes for the attachments that you do NOT want to export.

   **Note:** All of the case attachments are checked for inclusion in the export by default.

3. If you do not want to export all the available camera views for any of the events included in the case, clear the checkboxes in the **Cameras** section for the views that you do NOT want to export.

   **Note:** All the camera views are checked for inclusion in the export by default.

4. If you want to export to media, on the **Media Export** tab, select the export destination, enter any applicable export parameters for the destination you selected, then go to **step 7**.

   **Note:** If a non-event case attachment is larger than the size of the selected export destination (for example, a CD), the attachment will not be exported with the case.

For information about media export destinations, see *Select a Destination for Media Export* on page 143.

If you want to export to the secure cloud using CLOUD-SHARE, click the **CLOUD-SHARE** tab. The **CLOUD-SHARE** tab appears.

5. On the **CLOUD-SHARE** tab, enter:
   a. The recipients for your shared evidence
   b. The number of days you want the shared evidence to be available on the CLOUD-SHARE site
   c. The type of security the recipients must use to access the shared evidence

   **Important!** Depending on the type of security you select, there may be other fields you need to fill in.

   d. Whether you want to include subtitles on the event videos in your exported shared evidence
Chapter 5. Exporting Evidence

For information about the fields on the CLOUD-SHARE tab, see Export Using CLOUD-SHARE on page 148.

6. Enter a Reference Label for the export, then click Prepare Export.

For information about the label for the export, see Export Summary on page 155.

The Export Worksheet for the export closes. The export appears on the My Exports tab, its status showing where it is in the export process.

The Export Worksheet and My Exports

Note: If a local computer is involved in the export (for a local-computer or burn-to-disc destination), the local computer's performance will also affect the speed of the export.

You export recorded events from EL4 Web using the Export Worksheet. You monitor the status of exports on the My Exports tab.
Export Worksheet

After you select what you want to export, you set all the parameters of your export on the Export Worksheet.

**Important!** All of the selected items will be exported in the same export package using the same parameters. If a selected item needs to be exported using a different set of parameters, you must export it separately.

You can access the Export Worksheet from multiple locations in EL4 Web, depending on what you want to export:

- To export recorded events, on the Events tab, select the export option from either the Actions menu or the Group Actions menu.
  
  Or
  
  From Event Playback or Event Details, select Export from the Options menu.

- To export a Sync Export video/audio combination, on the 1-Up player page, select Sync Export from the Options menu.

- To export a trimmed video, on the trim tool, click Export Video.

- To export cases, on the Cases tab, select the export option from either the Actions menu or the Group Actions menu.
  
  Or
  
  With a case open, click Export near the top right.

**Note:** You can select multiple recorded events (at the same time or individually) and/or trimmed videos to export together in a package. You can select multiple cases (at the same time or individually) to export together. You cannot export a recorded event or trimmed video and a case together unless that event/trimmed video is a part of the case.
Chapter 5. Exporting Evidence

The Export Worksheet has multiple sections. These sections either let you select parameters for the export or give you information about your selections:

- Select Items to Export (below)
- Choose a Format for Media Export (page 140)
- Select a Destination for Media Export (page 143)
- Export using CLOUD-SHARE (page 148)
- Export Summary (page 155)

My Exports tab

Once you click Prepare Export on the Export Worksheet, a record of the export appears on the My Exports tab.

The My Exports tab shows you the status of your export in the Exported Evidence Queue.

For more information about the My Exports tab, see Using the My Exports tab on page 156.

Select Items to Export

The Select Items to Export section of the Export Worksheet shows the items you selected to export together in an export package.

**Important!** All of the checked items in the section will be exported in the same export package using the same parameters. If an item on the list needs to be exported using a different set of parameters, you must export it separately.
The section includes an individual record for each item to be exported together. The item types include:

- Recorded events
- **Sync Export** video/audio combinations
- Linked events
- Trimmed video
- Cases
- Case attachments

Each record contains information specific to the item, for example, an individual event record shows much of what is listed for the event on the **Events** tab, including event start date and time, the officer name, vehicle or device ID, and the event category assigned to the event.

For more information on the data that is listed for a recorded event on the **Events** tab, see *Working with search results* on page 52.

**Sync Export video/audio combinations**

If any of the items to export is a **Sync Export** video and audio combination, the primary record shows the **Sync** flag. The full events that contain the video and audio streams that make up the **Sync Export** are also included in the list of items to export, by default. If you do not want to include the full events in the export package, clear the checkboxes for the full events.

For more information on **Sync Export**, see *Sync Export* on page 70.

**Linked events**

If any of the recorded events to export is linked to other events, the primary event record shows the **Linked Events** flag, and the linked event record is included in the list of items to export, by default. If you do not want to include the linked event in the export package, clear the checkbox for the linked event.

For more information on linked events, see *Manually Linking and Unlinking Events* on page 60.

**Trimmed video**

If any of the items to export is trimmed video, the item record shows the **Trimmed Camera** flag, and indicates the camera view that was trimmed.

For more information on trimmed video, see *Event video trim* on page 84.
Chapter 5. Exporting Evidence

Cases and case attachments

**Note:** You cannot export a recorded event or trimmed video and a case together unless that event/trimmed video is attached to the case.

For a case, each attachment (recorded event, file, or link) is listed as an individual item record under the case, and is included in the export package by default. If you do not want to include a case attachment in the export package, clear the checkbox for the attachment you do not want to include.

For more information on cases and case attachments, see *Chapter 4. Working with Cases* on page 101.

Camera views

Each record for a recorded event item includes a list of the Camera views available with that event. Each available view has its own checkbox. You can choose to export one or all of the camera views for each event by checking or clearing the associated checkboxes. All camera views are checked to be exported by default.

Choose a Format for Media Export

**Note:** This selection only applies to an export to media, not an export using CLOUD-SHARE. For information about exporting using CLOUD-SHARE, see *Export Using CLOUD-SHARE* on page 148.

The Choose a Format section on the Media Export tab of the Export Worksheet allows you to select which video format you want to use to export recorded events, Sync Export video/audio combinations, or trimmed video that are not part of a case.

**Note:** Any recorded events or Sync Export combinations that are attached to a case are automatically exported in Original Format.

You can choose whether you want to include the on-screen text in the exported video, and how you want to include it (subtitles or embedded text).

**Note:** Selecting any format other than Original Format requires that the video be transcoded. This process increases the export time. Choosing to embed the on-screen text in the video substantially increases the export time.
You can also choose to include the WatchGuard Video Player in the export package. For information about the WatchGuard Video Player, see WatchGuard Single Event Player on page 158.

**Video formats**

All of the supported video formats are different ways of compressing video, and as WatchGuard uses them, produce video files of comparable quality. The major differences are file size and the amount of time needed to package the export because of transcoding (changing the Original Format into a different format). The transcoding process increases the export packaging time.

To change the export video format:

- Click Change in the Choose a Format section.

WatchGuard supports five video formats for export:

- **Original Format**: Select Original Format to export using WatchGuard's format (MP4); Original Format is the default option and the Recommended Video Format. Original Format uses h.264 video compression, one of the standards used in Blu-ray Discs. Exporting using the Original Format is the fastest method, comparatively.
  
  **Tip**: When an exported video spans discs, it means that the single exported video is too large to fit on a single disc.

- **MPEG-2**: Select MPEG-2 to export to a folder or an optical disc in the MPEG-2 format. MPEG-2 is used for digital television signals and for DVD and other optical media.

- **WMV**: Select WMV to export to a folder or an optical disc in the WMV format. WMV is a Microsoft format originally designed for Internet streaming applications. It is one of the default file formats for Windows Media Player.

- **DVD-Video**: Select DVD-Video to export to an optical disc for a standard DVD player. The standard DVD format is a variation of the MPEG-2 format. When you export in DVD-Video format, you can also select the Quality: High, Medium, or Low. High is the default option. Selecting a higher quality increases the quality of the resulting video, but also increases the exported file size. Exporting using the DVD-Video format is the slowest method, comparatively.
  
  **DVD-Video** format supports spanning discs.

- **AVI**: Select AVI to export to a folder or an optical disc in the AVI format. AVI is an older Microsoft format.
Chapter 5. Exporting Evidence

Including on-screen text

You can include the on-screen metadata text in the exported video, as:

- Subtitles (default and recommended)
- Embedded text

**Note:** The metadata text is the text that shows as captions over the video during playback.

Subtitles

Subtitles are the captions that show on the screen during playback. The captions come from a file that is included by default in the exported recorded event. The video player picks up the file and lays its contents over the video. Subtitles are not permanent; when you use the WatchGuard Video Player to play back the video, you can turn the subtitles off and on using the Captions button.

WatchGuard recommends that you choose to include Subtitles in every export; they are included by default. Including subtitles does not significantly affect either the size or speed of the export.

If you choose NOT to include subtitles:

- Clear the Include Subtitles checkbox.

In this case, NO on-screen metadata text will be included in the export unless you check the Permanently Embed On-screen Text in the Video checkbox.

**Important!** Choosing to permanently embed text into the exported video significantly increases export time.

For more information on embedding text in the video, see **Embedded text** below.

Embedded text

Embedded text uses the same metadata text as Subtitles (see above)—the text comes from the same file as the captions—but embedded text is burned into the exported video. Embedded text is permanent; it cannot be turned off. Embedded text will be visible using any video player.

WatchGuard does not recommend choosing to permanently embed text in the exported video. The option to embed text is disabled by default.

**Important!** Choosing to permanently embed text into the exported video significantly increases export time.
Select a Destination for Media Export

If you choose to embed text in the exported video:

- Clear the **Include Subtitles** checkbox, then check the **Permanently Embed On-screen Text in the Video** checkbox.

**Select a Destination for Media Export**

*Note: This selection only applies to an export to media, not an export to CLOUD-SHARE. For information about exporting using CLOUD-SHARE, see Export Using CLOUD-SHARE on page 148.*

The **Select a Destination** section on the **Media Export** tab of the **Export Worksheet** allows you to select which destination you want to export to:

- Folder on the local computer or network
- Individual optical disc burner
- DVD robot, if installed in your system

*Important! You must have the Evidence Library Transfer Agent installed on your computer in order to access some of the export functionality. You can download the Transfer Agent from the **Manage** tab in EL4 Web.*

You can set default export preferences for a media export to the local computer, network, or individual optical disc burner. For information on setting the default destination values, see **Media export destination preferences** on page 146.

**Local computer or network folder**

Select **Local Computer** to export to a folder on your computer or in your network.
Chapter 5. Exporting Evidence

When you choose to export to a local computer or network folder, you can either accept the Default Download Location (if applicable) or browse to and select the folder you want this export to download to.

To select a folder other than the default:

- Click Change Location to open the Export to Folder dialog box and navigate to the folder you want this export to download to.

The Download Location changes to the selected folder.

If you want the export to download automatically to the Download Location after it has been packaged, make sure the Automatically download switch is set to Yes. Yes is the default option.

You can choose to manually download the export package from the My Exports tab. To choose to manually download an export package:

- Click the Automatically download switch to change it to No.

For information on the My Exports tab, see Using the My Exports tab on page 156.

**Individual optical disc burner**

Select Burn to Disc to export to a disc using an individual optical disc burner.

[Image of disc burner selection interface]

**Note:** If there are multiple individual disc burners connected to your system, the system uses the device that is set as default in the export preferences. If no default is set, it automatically selects the most efficient device.

When you choose to export to an individual disc burner, you select which Media Type you want to burn.

**Note:** If you select a disc type that is not valid for your burner device, EL4 Web alerts you that the media type is not compatible with your system.

Each Media Type option shows you approximately how many discs of that type you need for the export.
If the export requires more than one disc, you must use the same type of disc for all parts of the export. For example, if you start with a CD, you must use a CD for each of the follow-up discs as well.

One recorded event can span multiple discs, depending on its size and duration. If you export multiple recorded events, each event is burned on its own disc or set of discs; even if the size and duration of all the recorded events exported together could fit on one disc, they will not be burned on one disc together.

**Tip:** When an exported event spans discs, it means that the single exported event is too large to fit on a single disc. **Original Format** and **DVD-Video** are the only formats that support spanning discs. For information on video formats, see Video formats on page 141.

If you want the export to automatically burn to disc after it has been packaged, make sure the **Automatically Burn to Disc** switch is set to **Yes**. **Yes** is the default option.

You can choose to manually burn the export package to disc from the **My Exports** tab. To choose to manually burn an export package to disc:

- Click the **Automatically Burn to Disc** switch to change it to **No**.

For information on the **My Exports** tab, see Using the **My Exports** tab on page 156.

**DVD robot**

Select **DVD Robot** to export to a DVD robot in your network.

**Note:** You must have a DVD robot installed in your system for the **DVD Robot** destination to be available for export.

When you select this option, you select which robot in the network you want to use (if multiple robots are installed). You also select how many copies of the evidence DVD you want the robot to burn.
Chapter 5. Exporting Evidence

For more information on installing a robot in your network, see the Evidence Library 4 Web Installation Guide.

**Tip:** The robot can print the label for the DVD as well, either a WatchGuard basic label or a custom image label that uses an image you upload. You set up the label for your evidence DVDs on the Label Maker tab in Evidence Library Administrator (EL Administrator). For information about EL Administrator, see Evidence Library Administrator on page 24.

### Media export destination preferences

You can set default export destination preferences for a media export to the local computer, network, or individual optical disc burner. The default export destinations you set will apply to every media export from Evidence Library 4 Web (EL4 Web), unless you select a different, one-time destination for an individual export on the Export Worksheet. For information about setting a one-time export destination, see Select a Destination for Media Export on page 143.

You use the Evidence Library Transfer Agent to set the default export destination preferences. The Evidence Library Transfer Agent is the piece of EL4 Web that runs on your local computer. You can access it from the Windows notification area (system tray).

To set the media export destination preferences:

1. Right-click the Evidence Library Transfer Agent icon in the system tray, then select Show Window.

   ![Show Window](image1)

   The Evidence Library Transfer Agent opens.

   ![Evidence Library Transfer Agent](image2)
2. Select **Preferences** from the **File** menu.
   The **Preferences** dialog box opens.

   ![Preferences dialog box](image)

3. Click the **Media Burner** field and select the media burner you want to set as the default.
   The media burner you selected populates the **Media Burner** field.

4. Click **Browse** next to the **Export Folder Location** field and navigate to the folder location you want to use as the default.

5. Click **Select Folder**.
   The location you selected populates the **Export Folder Location** field.

6. Click **OK**.
Chapter 5. Exporting Evidence

Export Using CLOUD-SHARE

**Important!** CLOUD-SHARE is a subscription service offered by WatchGuard that allows you to export, store, share, and access evidence using the secure cloud.

For more information on WatchGuard CLOUD-SHARE, see the CLOUD-SHARE user documentation. For more information on your agency’s CLOUD-SHARE subscription, contact your CLOUD-SHARE administrator.

The CLOUD-SHARE tab on the Export Worksheet allows you to export evidence to secure cloud storage using WatchGuard CLOUD-SHARE.

![CLOUD-SHARE tab](image)

**Note:** The contents of the fields that appear on the CLOUD-SHARE tab are set up by your CLOUD-SHARE administrator on the CLOUD-SHARE Configuration page available from the Manage tab in Evidence Library 4 Web (EL4 Web). For information on setting up the CLOUD-SHARE tab, see CLOUD-SHARE configuration on page 150.

On the CLOUD-SHARE tab, you set:

- **Recipients:** Click the Recipients field and enter the email addresses and/or group mailing lists for the people or groups who you want to allow to access the shared evidence in the export.

  The email addresses or group mailing lists allowed as recipients of shared evidence can be limited by a whitelist set up by your CLOUD-SHARE administrator on the CLOUD-SHARE Configuration page. When the whitelist is enabled, you cannot export using CLOUD-SHARE if you entered a recipient who is NOT on the whitelist.

  **Tip:** Group mailing lists are set up in the CLOUD-SHARE application. Each list contains a set of recipients that you frequently share evidence with; often all the recipients on the list are from the same organization. For example, the group mailing list HCDA#Highwater refers to a group of people from the Highwater County DA’s office who need to receive shared evidence from you at Highwater PD.

- **Share Expiration:** Click the Share Expiration field and select how long you want this exported evidence to remain available in the secure cloud.

  The maximum number of days that an evidence share can remain available in the secure cloud is determined by your agency’s CLOUD-SHARE subscription.
• **Share Security**: Click the Share Security field and select the type of security the recipient must use to access the exported evidence in the secure cloud.

  **Note**: The security type you select for exported evidence cannot be downgraded once the evidence is in the CLOUD-SHARE application. For example, evidence shared with the Secured type cannot be downgraded later to Access Code or Unsecured.

When a notification is sent to the recipients in the Recipients field that shared evidence is available, the recipients also receive instructions regarding which type of security has been applied to this shared evidence, and what they need to do to access it. The security type options are:

- **Unsecured**: Select Unsecured to allow access to anyone possessing the web storage link to the shared evidence.
- **Access Code**: Select Access Code to allow access only to those recipients who know the access code as well as have the web storage link to the shared evidence.
- **Secured**: Select Secured to allow access only to those recipients who are registered users on EvidenceLibrary.com; the recipient must log in to EvidenceLibrary.com to access the shared evidence.

  **Note**: The security types available in the Share Security field depend on how your administrator configured the CLOUD-SHARE tab in EL4 Web as well as your agency’s CLOUD-SHARE subscription level.

Evidence shared using any of the three access types can be viewed by a registered user on EvidenceLibrary.com, provided that the shared evidence has been sent or forwarded to that particular user.

• **Include Subtitles checkbox**: Clear the Include Subtitles checkbox to NOT include the on-screen captions as part of the exported evidence package; the checkbox is checked by default. Subtitles are the captions that show on the screen during playback. The captions come from a file that is included by default in the exported recorded event. The video player picks up the file and lays its contents over the video. Subtitles are not permanent; when you use the WatchGuard Video Player to play back the video, you can turn the subtitles off and on using the Captions button. WatchGuard recommends that you include captions with any exported evidence.

  **Note**: The WatchGuard Video Player is available as a one-time download when you export using CLOUD-SHARE. See the CLOUD-SHARE user documentation for more information.

• **Access Code Hint**: Click the Access Code Hint field and select the hint you want to send to the recipients with the shared-evidence notification; the hint should help recipients remember the predetermined code needed to access the shared evidence.
Chapter 5. Exporting Evidence

The Access Code Hint field only appears when you select AccessCode in the Share Security field.

- **Access Code**: Click the Access Code field and enter the predetermined code that recipients need to enter to access the shared evidence; what you enter as an Access Code should directly relate to what you selected in the Access Code Hint field.

The Access Code field only appears when you select AccessCode in the Share Security field.

- **Allow Recipients to Forward this Share switch**: If Yes, allows recipients who are registered users of EvidenceLibrary.com to forward the shared evidence from their CLOUD-SHARE inbox; if No, keeps recipients who are registered users of EvidenceLibrary.com from forwarding the shared evidence.

The default value for this switch is set by your CLOUD-SHARE administrator. Click the switch to change its value. Changing the value overrides the default value only for the current Export Worksheet.

The Allow Recipients to Forward this Share switch only appears when you select Secured in the Share Security field.

- **Allow Playback switch**: If Yes, allows recipients who are registered users of EvidenceLibrary.com to play back the shared evidence from their CLOUD-SHARE inbox; if No, keeps recipients who are registered users of EvidenceLibrary.com from playing back the shared evidence from their CLOUD-SHARE inbox.

Note: Recipients can always play back evidence once they have downloaded it from EvidenceLibrary.com to their local computer.

The default value for this switch is set by your CLOUD-SHARE administrator. Click the switch to change its value. Changing the value overrides the default value only for the current Export Worksheet.

The Allow Playback switch only appears when you select Secured in the Share Security field.

**CLOUD-SHARE configuration**

**Important!** CLOUD-SHARE is a subscription service offered by WatchGuard that allows you to export, store, share, and access evidence using the secure cloud.

For more information on WatchGuard CLOUD-SHARE, see the CLOUD-SHARE user documentation. For more information on your agency’s CLOUD-SHARE subscription, contact your CLOUD-SHARE administrator.

If your agency uses the CLOUD-SHARE service, you set up the connection between Evidence Library 4 Web (EL4 Web) and CLOUD-SHARE on the CLOUD-SHARE Configuration page. On the configuration page, you can also set up the default options for the CLOUD-SHARE tab on the Export Worksheet. For more information about the CLOUD-SHARE tab on the Export Worksheet, see Export Using CLOUD-SHARE on page 148.
On the **CLOUD-SHARE Configuration** page you can:

- Enter the connection string that connects EL4 Web to CLOUD-SHARE

**Important!** The **Share Connection String** is **REQUIRED** to connect to CLOUD-SHARE as well as to configure the rest of the settings on the configuration page.

- Set up the default types of security the share recipient must use to access the exported evidence in the secure cloud
- Set up the default number of days you want the exported evidence to remain available in the secure cloud
  
  You can assign different default expiration periods for each event category.
- Set up and enable a list of valid email domains for shared evidence recipients

**Setting up CLOUD-SHARE in EL4 Web**

To set up CLOUD-SHARE for sharing EL4 Web evidence:

1. In the CLOUD-SHARE application, access your **Organization Configuration** page.
   
   For instructions how to access the CLOUD-SHARE configuration page for your organization, see the CLOUD-SHARE user documentation.

   ![Organization Configuration](image)

   
   2. Copy all of the text, including the braces, in the **Share Connection String** field.
   3. Log in to EL4 Web.

   For instructions how to log in to EL4 Web, see *Accessing Evidence Library 4 Web on page 23.*
Chapter 5. Exporting Evidence

4. Move your mouse over the Manage tab and select CLOUD-SHARE Setup.

The CLOUD-SHARE Configuration page opens.

5. In the orange Share Connection String field, paste the connection string that you copied from the Organization Configuration page in the CLOUD-SHARE application.

   **Tip:** You may need to tab out of the field for the system to read the string correctly.

6. Click Test Connection.

   The system reads the connection string you entered and tests whether it correctly connects EL4 Web to the CLOUD-SHARE application. When it is finished testing the connection, if the connection has been made successfully, the Successfully connected to CLOUD-SHARE message appears.

   **Important!** If a message appears that the connection was not successful, try clicking Test Connection again. If you continue to see an error, contact your WatchGuard Technical Services representative.

7. Click the Allowed Share Types field and select a share type that you want to be available in the Share Security field on the CLOUD-SHARE tab of the Export Worksheet.

   For information on share security types, see Share Security on page 149.

   **Note:** The share type determines the type of security the recipient must use to access the exported evidence in the secure cloud.

8. Repeat step 7 as needed to select all the share types that you want to be available on the CLOUD-SHARE tab for export.
Note: The security types that are ultimately available for use at your agency depend on your agency’s CLOUD-SHARE subscription level.

9. Set the default settings for enabling Share Forwarding and allowing Video Playback.

Tip: Enabling Share Forwarding allows registered users of EvidenceLibrary.com to forward the shared evidence from their CLOUD-SHARE inbox. Allowing Video Playback allows registered users of EvidenceLibrary.com to play back the shared evidence from their CLOUD-SHARE inbox.

10. Click the Default Expiration field and select the default number of days you want the exported evidence to remain available in the secure cloud.

11. If you want to set a different default expiration period for evidence categorized with certain event categories, click the Expiration field next to the Category you want to set differently, and select the default number of days you want exported evidence with that categorization to remain available in the secure cloud.

12. If you want to enable a list of valid email domains for shared evidence recipients, click the Enable Domain Whitelist switch to change the value to Yes, then enter the valid email domains in the Domain Whitelist field.
Chapter 5. Exporting Evidence

**Important!** Enabling the **Domain Whitelist** limits the valid recipients of shared evidence to only those email domains on the whitelist.

**Note:** The whitelist you set up in EL4 Web limits the list of people you can initially share evidence with. There is also a whitelist in the CLOUD-SHARE application that limits the list of people you can forward evidence to once the evidence is in the secure cloud.

13. If you selected **AccessCode** as one of your **Allowed Share Types**, set up the access code options you want to be available from the **Access Code** fields on the CLOUD-SHARE tab of the Export Worksheet.
   
a. Click the field in the **Hint** column and enter an **Access Code Hint**, for example, Case Number, Birthday, Birth City.

   **Tip:** The **Access Code** is the predetermined code that shared-evidence recipients need to enter to access the shared evidence. The **Access Code Hint** should help recipients remember the predetermined code needed to access the shared evidence.

   b. Click the **Format** field and select the format the access code should follow, for example, for a Case Number hint, select **AlphaNumeric**.

   c. Click the green + (i+) button to add another hint to the list, as needed.

   d. Repeat step a through step c as needed to add access code hint options to the **Access Code** fields on the Export Worksheet.

   For information on access codes and hints, see **Access Code Hint** and **Access Code** on page 149.

14. Click **Save Changes**.

   Your connection to CLOUD-SHARE is saved, and your CLOUD-SHARE configuration setup and/or changes are saved to the CLOUD-SHARE tab on the Export Worksheet.
Export Summary

The Export Summary section of the Export Worksheet shows you basic information about the export. It requires you to label the export package with a name that will help you identify the package while it is going through the export process.

The elements in the Export Summary section of the Export Worksheet include:

- **Estimated Size**: Shows the estimated size of the all the files included in the export, with the video files in the selected format.
  
  The Estimated Size changes depending on whether you choose to include all the camera views and which video format you select.
  
  For information on including camera views in the export, see Camera views on page 140. For information on the video format, see Video formats on page 141.

- **Relative export speed**: For a media export, shows the speed of the export relative to other exports that use a different video format or embed text in the video.
  
  The relative export speed changes (Fast, Slow, Slowest) depending on which video format you select and whether you choose to embed the on-screen text in the video. Original Format with no embedded text is the fastest; any format with embedded text is the slowest.
  
  For information on embedding the on-screen text in the exported video, see Including on-screen text on page 142.

- **Reference Label**: Click the Reference Label field and enter a label for the export that will identify it for you (and any others as needed) throughout the export process; the text you enter in this field becomes part of the official file name of the export package.

  **Important!** The Reference Label field is REQUIRED for any export.

- **Prepare Export button**: Click Prepare Export to start the export packaging process.
  
  After you click Prepare Export, the Export Worksheet closes and the record and status of your export shows on the My Exports tab.
  
  For information on the My Exports tab, see Using the My Exports tab on page 156.

- **Cancel Export button**: Click Cancel Export to close the Export Worksheet without exporting.
  
  When you click Cancel Export, any entries that you made on the Export Worksheet as well as any record of the export are discarded.
Chapter 5. Exporting Evidence

Using the My Exports tab

**Note:** To export from Evidence Library 4 Web (EL4 Web), you must have the correct permissions assigned to you. Contact your system administrator to verify your assigned permissions.

The **My Exports** tab contains the **Exported Evidence Queue**; it shows you information about each export you initiated.

**Note:** If you are an administrator for EL4 Web, the queue contains all the exports initiated by any user in the system.

**Note:** The exports listed on the **My Exports** tab age off over time, depending on your agency’s settings for the **Export** storage location in the Evidence Management module. For information about the amount of time exports stay on the **My Exports** tab, see Export storage on page 251.
The information for each export in the queue includes:

- **Priority**: Shows the export's priority for processing in the queue; if you have exports waiting in the queue, you can change which of the waiting exports will be processed first.

To change the priority of an export with a **Status** of **Waiting**, click the **Actions** menu icon and select the option to change the priority.

- **Status**: Shows the export's status in the export process.

- **Label**: Shows the **Reference Label** you entered for the export on the **Export Worksheet**.

For an export using CLOUD-SHARE, the system appends a reference number that uniquely identifies the shared evidence package. Just after the reference number, CLOUD-SHARE also adds a list of recipients.

- **Export To**: Shows the destination for the export.

- **Total Size**: Shows the size of the total contents of the export.

- **Export Type**: Shows the type of item that was exported.

- **Submitted On**: Shows the date the export was initiated.

- **Submitted By**: Shows the username of the person who initiated the export.

**Actions menu**

The options on the **Actions** menu change depending on the status of the export. The following actions can show as options on the **Actions** menu:

- **Increase Priority**: If the **Status** of the export is **Waiting**, allows you to change the export's priority in the export queue.

- **Cancel from Queue**: If the **Status** of the export is **Waiting**, allows you to cancel the export.

- **Burn to Disc**: If the export destination was **Burn to Disc** originally, allows you to burn the export package to an optical disc again.

- **Download Package**: If the export has been successfully packaged, downloaded, or burned to disc, allows you to download (for the first time or again) the export package to the **Downloads** folder on your local computer.

- **Show Error Message**: If the **Status** of the export is **System Error**, allows you to view the error message.

- **Remove from Queue**: Allows you to remove the export from the export queue.

- **Unshare from CLOUD-SHARE**: If the **Status** of the export is **Shared**, allows you to remove the shared evidence from the secure cloud.

**Note**: The options do not all appear on the **Actions** menu at the same time.

**Filtering**

You can filter the list of exports by any of the column values using the filter feature:

- Click the **Filter** icon (★) in the column you want to filter by, then enter the values you want to use for the filter.
WatchGuard Single Event Player

In Evidence Library 4 Web (EL4 Web), when you export video to media (rather than using CLOUD-SHARE), you can choose to include the WatchGuard Video Player for single events with the exported files. Double-clicking the video player file opens the video player ready to play whatever videos were included in the export.

**Important!** The WatchGuard Video Player for single events does NOT support synchronized event playback. You must install the WatchGuard Video Player for synchronized events to play back multiple events synchronized. For more information, see WatchGuard Synchronized Event Player on page 164.

**Note:** The WatchGuard Video Player for single events is available as a separate download for use with shared evidence exported using CLOUD-SHARE. When a recipient is notified that shared evidence is available, the notification includes a link to download the WatchGuard Video Player for single events.

The elements on the WatchGuard Video Player for single events include:

- **Videos list:** Lists all the available videos in the export; double-click any Video-n item to start playing that video
  
  The list includes the name of the officer who recorded the video, when it was imported to EL4 Web, and the stream (camera view) the video captured.

- **Videos accordion tab:** Click Videos to show the Videos list; the video player opens with the Videos accordion tab active, showing the Videos list, by default

- **Snapshots accordion tab:** Click Snapshots to show the Snapshots list (page 159)
Snapshots list

The Snapshots list shows all of the still images, from the included videos, that were taken using the Take Snapshot button on the video player controls.

Each still image has five icons next to it:

- **Save Snapshot**: Click Save Snapshot to open Windows Explorer and navigate to where you want to save the still image
- **Preview Snapshot**: Click Preview Snapshot to open a larger version of the still image
- **Print Snapshot**: Click Print Snapshot to open the Print dialog box
- **Enter Notes on Snapshot**: Click Enter Notes on Snapshot to open the SnapShot Notes dialog box
  On the SnapShot Notes dialog box, you can enter details about the still image. You can also print the image, with your notes, from this dialog box.
- **Delete Snapshot**: Click Delete Snapshot to delete the still image from the list

Video player controls

The video player controls allow you to control playback of the exported video.
Chapter 5. Exporting Evidence

The **WatchGuard Video Player** for single events includes the following controls:

- **Toggle Left Pane**: Click **Toggle Left Pane** to hide the **Videos** or **Snapshots** pane; click the button again to show the pane
- **Toggle Full Screen**: Click **Toggle Full Screen** to show the selected video on the full monitor screen
  
  To return to playing back on the partial screen, move the cursor to the bottom of the screen to show the video player controls, then click **Toggle Full Screen**.
- **Toggle Captions**: Click **Toggle Captions** to turn off the on-screen text; click the button again to show the captions
- **Mute**: Click **Mute** to turn the video sound off; click the button again to turn the video sound back on
- **Volume**: Click and drag the **Volume** control to adjust the volume of the video playback
- **Audio Source**: Click and drag the **Audio Source** balance control to isolate either the **Wireless** microphone or the **Cabin** microphone audio
  
  If you are using two wireless microphones with Evidence Library 4 Web (EL4 Web), the audio source balance for the front camera moves between the two wireless microphones. The audio source balance for any secondary cameras remains between the wireless and the cabin microphones.
- **Play Rate**: Shows the current speed of the video playback
  
  Click **Play Rate** and select another option from the drop-down list to change the current playback speed. The speed options range from 0.25X to 4X.
- **Reverse Play**: Click **Reverse Play** to jump the video back a short distance then resume forward video playback
- **Play**: Click **Play** to start forward video playback
- **Stop**: Click **Stop** to stop forward video playback and reset the **Video Position** back to the beginning of the video
- **Pause**: Click **Pause** to stop forward video playback on the current frame; click **Play** to restart forward video playback from the current frame
- **Advance by Frame**: Click **Advance by Frame** to move forward one frame of video, then pause video playback
- **Take Snapshot**: Click **Take Snapshot** to take a still image of the current video frame; the still image appears on the **Snapshots** list *(page 159)*
- **Video Position**: Shows how much of the video has been played back
  
  The **Video Position** control moves as the video plays back. Click and drag the control to a new position to start the video playback from that point.
Playing back exported video with the single event player

If you exported to media, and chose to include the **WatchGuard Video Player** with your export, you can view the exported videos using the **WatchGuard Video Player** for single events included with the export.

If you exported using CLOUD-SHARE, your recipients were given the option to download and install the **WatchGuard Video Player** for single events separately.

For information about the **WatchGuard Video Player** for single events, see *WatchGuard Single Event Player* on page 158.

To view videos using the **WatchGuard Video Player** for single events:

1. For evidence that was exported to media, locate, then double-click, the *WGVPlayer.exe* file in the folder or on the disc that was the export destination.

   **Note:** The **WatchGuard Video Player** for single events may launch automatically when you insert an exported evidence disc in the computer’s disc drive.

   For a shared evidence package that was exported using CLOUD-SHARE, unzip the evidence package, then double-click the *.wgplayer* file.

   The **WatchGuard Video Player** for single events opens showing a list of available videos.
Chapter 5. Exporting Evidence

2. Double-click **Video-n** for the video you want to view.

   The video you selected begins playing back.

3. Use the video player controls to adjust the playback as needed.

   For a description of the controls on the **WatchGuard Video Player** for single events, see Video player controls on page 159.

**Exported Audit Log**

From the WatchGuard Player for single events, you can view an exported version of the audit log that is available from event details in Evidence Library 4 Web (EL4 Web).

In EL4 Web, the audit log from event details lists the historical information to date about the current recorded event. The exported version of the audit log lists similar information, but in a different format.

For information about the audit log available from event details, see Viewing the event audit log on page 97.

---

**Important!** WatchGuard recommends that you work with your WatchGuard Technical Services representative if you need an in-depth analysis and/or audit of a recorded event.

---

The information available in the exported version of the audit log includes:

- When the event was imported into EL4 Web and the details of the import
- When the event was exported and by whom
- When the event was viewed and by whom
- When the event's properties were modified and by whom
To view the exported version of the audit log:

- On the **WatchGuard Video Player** for single events, click **View Audit Log** just above the playback screen.

The **Audit Log** dialog box opens.

![Audit Log dialog box]

To view a section's details:

- Click the + next to the section name.

To view all the details on the exported version of the audit log:

- Click **Expand All**.

Once you click **Expand All**, the button changes to **Collapse All**. To collapse all the details on the exported version of the audit log:

- Click **Collapse All**.

You can also print the exported version of the audit log if you need to:

- Click **Print** to open the **Print** dialog box.
WatchGuard Synchronized Event Player

With version 4.1 (and above) of Evidence Library 4 Web (EL4 Web), WatchGuard provides a player that supports synchronized event playback for exported events.

The **WatchGuard Video Player** for synchronized event playback supports:

- Single event playback *(page 172)*
- Synchronized event playback
  - **1-Up** *(page 175)*
    The **1-Up** player shows one video screen.
  - **2-Up** *(page 178)*
    The **2-Up** player can show two video screens.

When you initially access playback for an exported event, the **WatchGuard Video Player** for synchronized event playback opens as single event playback. Single event playback allows you to play back individual events.

From single event playback, you can move to synchronized event playback, if the event you selected contains synchronization (sync) data. Synchronized event playback allows you to simultaneously play back video and/or audio from events recorded at the same time using different devices.

**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.

The **WatchGuard Video Player** for synchronized event playback is a stand-alone application that must be installed on each computer where you want to play back exported video. For instructions how to install the WatchGuard Video Player for synchronized event playback, see *Installing the WatchGuard Video Player for synchronized event playback* on page 165.

For two common examples of playing back events synchronized, see:

- Playing back a camera view with an audio track from a different device *(page 180)*
- Playing back two camera views and an audio track from different devices *(page 182)*
Installing the WatchGuard Video Player for synchronized event playback

With version 4.1 (and above) of Evidence Library 4 Web (EL4 Web), WatchGuard provides a player that supports synchronized event playback for exported events.

You must install the synchronized event player on each computer where you want to use it to play back exported events.

Note: The WatchGuard Video Player for single event playback, available in previous versions of EL and ELX, is still included in the export package with each individual exported event. For information on using the previous exported event player, see WatchGuard Single Event Player on page 158.

The WatchGuard Video Player for synchronized event playback is available to download from the WatchGuard website: https://support.watchguardvideo.com/hc/en-us.

Note: Contact your system administrator for more information or help downloading the player.

To install the WatchGuard Video Player for synchronized event playback of exported events:

1. On the computer where you want to install the player, download the WatchGuard Video Player executable file.
2. Locate the file in your browser Downloads folder, then run it.

The Preparing to Install dialog box opens then closes.
Chapter 5. Exporting Evidence

If your computer already has all the prerequisites installed, the License Agreement dialog box opens. Go to step 4.

If your computer does NOT have all the prerequisites installed, the Requirements dialog box opens.

3. Click **Install**.

Any prerequisites are installed, then the **License Agreement** dialog box opens.

![License Agreement dialog box](image)

4. Read the **End User License Agreement**, select the **I accept the terms...** option, then click **Next**.

The **Destination Folder** dialog box opens.

![Destination Folder dialog box](image)

5. To accept the default folder location for the player files, click **Next**.

**Tip:** To change the folder location for the player files, click **Change**, then navigate to the new location.
Chapter 5. Exporting Evidence

The Ready to Install... dialog box opens.

6. Check the Create desktop shortcut for Player checkbox to place a shortcut on your computer desktop, then click Install.

When the player installation has finished, the InstallShield Wizard Completed dialog box opens.

7. Click Finish.
Accessing exported video using the WatchGuard Video Player

To access exported event video using the synchronized event player:

1. If needed, extract the contents of the zipped export package.

   **Note:** Some export packages from Evidence Library 4 Web (EL4 Web) are in a ZIP file format. You must extract the files before the player can access them.

2. Locate the **WatchGuard Video Player** shortcut on your computer desktop and double-click it to open the player.

   ![WatchGuard Video Player](image)

   The **WatchGuard Video Player** opens showing its initial screen.

3. Click **Open File**.

   The **Select File** dialog box opens.
4. Navigate to the export package whose video you want to play back.

5. Open the export package folder whose video you want to play back.

6. Open the .wgplayer file.

Tip: If the export package does NOT contain a .wgplayer file, click Cancel to close the Select File dialog box and return to the initial player screen. Click Open Folder on the initial screen, then navigate to the export package. Select the export package folder then click Select Folder.
The **WatchGuard Video Player** opens to single event playback.
Single event playback

When you initially access the **WatchGuard Video Player** to play back an exported event, the player opens for single event playback. Single event playback allows you to play back individual exported events.

For instructions how to access the WatchGuard Video Player and start playing back an exported event, see *Accessing exported video using the WatchGuard Video Player* on page 169.

The **WatchGuard Video Player** for single event playback includes the following elements:

- **File menu**: Click File to navigate to another export package and play back its video
- **Event category**: Shows the event category assigned by the officer when the event that is playing back was recorded
- **Event start date and time**: Shows the date and time that the recorded event started
- **Vehicle/Device ID**: Shows the name of the 4RE DVR or VISTA Body Camera that recorded the event
- **Officer name**: Shows the name of the officer who recorded the event
- **Device type**: Indicates the type of device used to record the event, either 4RE or VISTA
- **Audit Log button**: Click Audit Log to open the Audit Log for the event that is playing back
  
  If no audit log was included in the export package, the Audit Log button is inactive. For information about the Audit Log, see *Viewing the event audit log* on page 97.
- **Event Details button**: Click Event Details to open the Event Details popup for the event that is playing back
**Toggle Thumbnails**: Click the **Toggle Thumbnails** control to hide or show the **Camera Views Panel**

**Camera Views Panel**: Shows all the camera views that you included with the recorded events that were exported together; each event has its own section on the panel

- **Thumbnail images**: Click an image to start playing back the associated camera view
  The camera view that is currently playing back is outlined and shaded in yellow.

- **Camera views metadata**: Shows information about each event and camera view listed in the **Camera Views Panel**
  Each event shows the category, device type, start data and time, officer name, and device ID. Each camera view shows the view name (for example, **Camera 1**) and the video duration.

- **Audio track buttons**: Click an audio track button to play back that track with the video
  The button for the audio track that is currently playing back is yellow.
  Available audio tracks for a camera view show as buttons on the thumbnail image. For single event playback, only the currently playing event image shows audio track buttons.

---

**Note**: Each camera view includes at least one audio track; however, the availability of an audio track does not necessarily mean that audio was recorded on that track for the camera view. For example, if no microphone was on, no audio was recorded. The audio track is still present but with no audio recorded.

---

- **Go to Start**: Click the **Go to Start** icon to restart the video from the beginning
- **Play/Pause**: Click the **Play/Pause** icon to start or stop playback of the video
- **Playback Speed**: Click the **Playback Speed** icon to increase the playback speed to two times normal speed (2x)
  Click the 2x icon to increase to four times normal speed (4x). Click the 4x icon to increase to eight times normal (8x). Click the 8x icon to return to normal speed.
- **Playback Progress bar**: Indicates how much of the video has been played back and how much is remaining
  The **Playback Progress** bar changes to orange as a video plays back. Click anywhere on the progress bar (orange or black part) to start the video playback from that point.
- **Time Elapsed/Duration**: Shows how much of the video has been played back and how long the video is
- **Volume**: Click and drag the **Volume** control to adjust the volume of the video playback
- **Captions**: Click the **Captions** icon to turn on or off the on-screen text
  The **Captions** icon is inactive if no subtitles were included in the export, or the subtitles were embedded in the video during export packaging.
  For information about the on-screen text included in an exported event, see **Including on-screen text on page 142**.
- **Snapshot**: Click the **Snapshot** icon to take a still image of the current video frame that you can save as a separate image file
Chapter 5. Exporting Evidence

When you click the **Snapshot** icon, the still image appears in a dialog box separate from the video player. Click **Save** to navigate to the location where you want to save the image file.

- **Full Screen** (F): Click the **Full Screen** icon to show the video on the full monitor screen; press **Esc** or click the **Full Screen** icon again to exit full-screen mode
- **Sync button**: Click **Sync** to move to the **WatchGuard Video Player** for synchronized events with **1-Up**

  If there is no synchronizing (sync) data available for an event, the **Sync** button is inactive (gray).

---

*Note: Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.*

---

For information about synchronized playback with **1-Up**, see *Synchronized event playback with 1-Up* on page 175. For information about synchronized playback with **2-Up**, see *Synchronized event playback with 2-Up* on page 178.
Synchronized event playback with 1-Up

Synchronized event playback with **1-Up** allows you to simultaneously play back video and audio from exported events that were recorded at the same time using different devices. You access synchronized event playback through single event playback, if the exported event you are playing back contains sync data.

**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.

Using the **1-Up** player, you can play back video from one device and audio from another device at the same time (page 180). The **1-Up** player always shows one video screen.

The **WatchGuard Video Player** for synchronized event playback with **1-Up** includes the following elements:

- **File menu**: Click File to navigate to another export package and play back its video
- **Event category**: Shows the event category assigned by the officer when the event that is playing back was recorded
- **Event start date and time**: Shows the date and time that the recorded event started
- **Vehicle/Device ID**: Shows the name of the 4RE DVR or VISTA Body Camera that recorded the event
- **Officer name**: Shows the name of the officer who recorded the event
- **Device type**: Indicates the type of device used to record the event, either 4RE or VISTA

---

**File menu**:
- **File**: Navigate to another export package and play back its video
- **Event category**: Show the event category assigned by the officer when the event that is playing back was recorded
- **Event start date and time**: Show the date and time that the recorded event started
- **Vehicle/Device ID**: Show the name of the 4RE DVR or VISTA Body Camera that recorded the event
- **Officer name**: Show the name of the officer who recorded the event
- **Device type**: Indicate the type of device used to record the event, either 4RE or VISTA
Chapter 5. Exporting Evidence

- **Audit Log button**: Click Audit Log to open the Audit Log for the event that is playing back
  If no audit log was included in the export package, the Audit Log button is inactive.
  For information about the Audit Log, see viewing the event audit log on page 97.
- **Event Details button**: Click Event Details to open the Event Details popup for the event that is playing back
- **Toggle Thumbnails ( ):** Click the Toggle Thumbnails control to hide or show the Camera Views Panel
- **Camera Views Panel**: Shows all the camera views that you included with the recorded events that were exported together; each event has its own section on the panel
  - **Thumbnail images**: Click a thumbnail image to start playing back the associated camera view
    The camera view that is currently playing back is outlined and shaded in yellow.
  - **Camera views metadata**: Shows information about each event and camera view listed in the Camera Views Panel
    Each event shows the category, device type, start data and time, officer name, and device ID. Each camera view shows the view name (for example, Camera 1) and the video duration.
  - **Audio track buttons**: Click an audio track button from any camera view to play back that audio track with the video
    Available audio tracks for a camera view show as buttons on the thumbnail image. The button for the audio track that is currently playing back is yellow.

  **Note**: Each camera view includes at least one audio track; however, the availability of an audio track does not necessarily mean that audio was recorded on that track for the camera view. For example, if no microphone was on, no audio was recorded. The audio track is still present but with no audio recorded.

- **Go to Start ( ):** Click the Go to Start icon to restart the video from the beginning
- **Play/Pause**: Click the Play/Pause icon to start or stop playback of the video
- **Playback Speed ( ):** Click the Playback Speed icon to increase the playback speed to two times normal speed (2x)
  Click the 2x icon to increase to four times normal speed (4x). Click the 4x icon to increase to eight times normal (8x). Click the 8x icon to return to normal speed.
- **Playback Progress bar**: Indicates how much of the video has been played back and how much is remaining
  The Playback Progress bar changes to orange as a video plays back. Click anywhere on the progress bar (orange or black part) to start the video playback from that point.
- **Time Elapsed/Duration**: Shows how much of the current video has been played back and how long the video is
- **Volume ( ):** Click and drag the Volume control to adjust the volume of the audio playback
Synchronized event playback with 1-Up

- **Captions**: Click the Captions icon to turn on or off the on-screen text.
  The Captions icon is inactive if no subtitles were included in the export, or the subtitles were embedded in the video during export processing.
  For information about the on-screen text included in an exported event, see Including on-screen text on page 142.

- **Snapshot**: Click the Snapshot icon to take a still image of the current video frame that you can save as a separate image file.
  When you click the Snapshot icon, the still image appears in a dialog box separate from the video player. Click Save to navigate to the location where you want to save the image file.

- **Full Screen**: Click the Full Screen icon to show the video on the full monitor screen; press Esc or click the Full Screen icon again to exit full-screen mode.

- **1-Up button**: When yellow, shows that the 1-Up player is active; when gray, shows that the 1-Up player is inactive.
  Click 1-Up when the button is gray to move to synchronized event playback with 1-Up.

- **2-Up button**: When gray, shows the 2-Up player is inactive; when yellow, shows that the 2-Up player is active.

- **Sync button**: Click Sync to move back to the Recorded Event Playback for single event playback.
  For information about single event playback, see Single event playback on page 172.
Synchronized event playback with 2-Up

Synchronized event playback with 2-Up allows you to simultaneously play back video and/or audio from exported events that were recorded at the same time using different devices. You access synchronized event playback through single event playback, if the exported event you are playing back contains sync data.

**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.

Using the 2-Up player, you can play back video from two devices and audio from another device at the same time (page 182). The 2-Up player always shows two video screens.

The WatchGuard Video Player for synchronized event playback with 2-Up includes the following elements:

- **File menu**: Click File to navigate to another export package and play back its video
- **Event category**: Shows the event category assigned by the officer when the event that is playing back was recorded
- **Event start date and time**: Shows the date and time that the recorded event started
- **Vehicle/Device ID**: Shows the name of the 4RE DVR or VISTA Body Camera that recorded the event
- **Officer name**: Shows the name of the officer who recorded the event
- **Device type**: Indicates the type of device used to record the event, either 4RE or VISTA
Synchronized event playback with 2-Up

- **Audit Log button**: Click Audit Log to open the Audit Log for the event that is playing back. If no audit log was included in the export package, the Audit Log button is inactive. For information about the Audit Log, see Viewing the event audit log on page 97.

- **Event Details button**: Click Event Details to open the Event Details popup for the event that is playing back.

- **Toggle Thumbnails ( ):** Click the Toggle Thumbnails control to hide or show the Camera Views Panel.

- **Camera Views Panel**: Shows all the camera views that you included with the recorded events that were exported together; each event has its own section on the panel.
  - **Thumbnail images**: Click a thumbnail image to start playing back the associated camera view; you play back two camera views at a time on the 2-Up player. The camera views that are currently playing back are outlined and shaded in yellow. When you click a thumbnail image to begin playback of the associated video, you must select which screen you want the video to play back in.

  ![Thumbnail Image](image)

  Click **Left** or **Right** to play back the video you selected in the corresponding screen.

  - **Camera views metadata**: Shows information about each event and camera view listed in the Camera Views Panel.
    Each event shows the category, device type, start data and time, officer name, and device ID. Each camera view shows the view name (for example, **Camera 1**) and the video duration.

  - **Audio track buttons**: Click an audio track button from any camera view to play back that audio track with the camera views' video. Available audio tracks for a camera view show as buttons on the thumbnail image. The button for the audio track that is currently playing back is yellow.

  ![Audio Track Button](image)

  **Note**: Each camera view includes at least one audio track; however, the availability of an audio track does not necessarily mean that audio was recorded on that track for the camera view. For example, if no microphone was on, no audio was recorded. The audio track is still present but with no audio recorded.

- **Go to Start ( ):** Click the Go to Start icon to restart the video from the beginning.

- **Play/Pause**: Click the Play/Pause icon to start or stop playback of the video.

- **Playback Speed ( ):** Click the Playback Speed icon to increase the playback speed to two times normal speed (2X).
Chapter 5. Exporting Evidence

Click the \(2\times\) icon to increase to four times normal speed (\(4x\)). Click the \(4\times\) icon to increase to eight times normal (\(8x\)). Click the \(8\times\) icon to return to normal speed.

- **Playback Progress bar**: Indicates how much of the video has been played back and how much is remaining
  The Playback Progress bar changes to orange as a video plays back. Click anywhere on the progress bar (orange or black part) to start the video playback from that point.
- **Time Elapsed/Duration**: Shows how much of the current video has been played back and how long the video is
- **Volume**: Click and drag the Volume control to adjust the volume of the audio playback
- **Captions**: Click the Captions icon to turn on or off the on-screen text
  The Captions icon is inactive if no subtitles were included in the export, or the subtitles were embedded in the video during export processing.
  For information about the on-screen text included in an exported event, see *Including on-screen text* on page 142.
- **1-Up button**: When gray, shows that the 1-Up player is inactive; when yellow, shows that the 1-Up player is active
- **2-Up button**: When yellow, shows that the 2-Up player is active; when gray, shows the 2-Up player is inactive
  Click 2-Up when the button is gray to move to synchronized event playback with 2-Up.
- **Sync button**: Click Sync to move back to the Recorded Event Playback for single event playback
  For information about single event playback, see *Single event playback* on page 172.

*Playing back a camera view with an audio track from a different device*

Using the **WatchGuard Video Player** for synchronized event playback with 1-Up (page 175), you can play back video from one device with audio from another device (for example, 4RE DVR video with VISTA WiFi audio) if the events occurred in the same time frame and both have synchronization (sync) data.

**Note**: Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.

The events must be exported together (in the same export package) so they show on the synchronized event playback player together.
Playing back a camera view with an audio track from a different device

To play back video from one device with audio from another device:

1. Access the **WatchGuard Video player** for the exported video that you want to play back.
   For instructions how to access exported video using the WatchGuard Video Player, see *Accessing exported video using the WatchGuard Video Player* on page 169.

2. Click **Sync**.
   The single event player changes to the **1-Up** synchronized event player.

3. On the **Camera Views Panel**, locate the event whose video you want to play back, then click the appropriate camera view.
Chapter 5. Exporting Evidence

4. On the **Camera Views Panel**, locate the event whose audio you want to play back with the video, then click the appropriate audio track button.

5. Use the playback controls as needed.

**Playing back two camera views and an audio track from different devices**

Using the **WatchGuard Video Player** for synchronized event playback with **2-Up** (page 178), you can play back video from two devices with audio from a third device (for example, video from a 4RE DVR and a VISTA WiFi with audio from a second VISTA WiFi) if the events occurred in the same time frame and both have synchronization (sync) data.

**Note:** Sync data is present with events recorded by the 4RE DVR, version 4.0 and higher, and VISTA WiFi, version 2.0 and higher.

The events must be exported together (in the same export package) so they show on the synchronized event playback player together.
To play back video from two devices with audio from a third device:

1. Access the **WatchGuard Video player** for the exported video that you want to play back.
   
   For instructions how to access exported video using the WatchGuard Video Player, see *Accessing exported video using the WatchGuard Video Player* on page 169.

2. Click **Sync**.

   The single event player changes to the **1-Up** synchronized event player.
Chapter 5. Exporting Evidence

3. Click **2-Up**.

The **1-Up** synchronized event player changes to the **2-Up** synchronized event player.

![Synchronized event player](image)

4. On the **Camera Views Panel**, locate the events whose video you want to play back, then click the appropriate camera views.

5. On the **Camera Views Panel**, locate the event whose audio you want to play back with the video, then click the appropriate audio track button.

![Camera views panel](image)

6. Use the playback controls as needed.
Chapter 6. Checking Out VISTA Cameras

In this chapter...

- Checking out a USB-connected VISTA using the USB Dashboard (page 187)
- Checking out VISTA from the VISTA Dashboard (page 193)
- Checking out VISTA using Rapid Checkout (page 197)
- Printing a Checkout Report (page 199)
- Checking out VISTA using Kiosk Mode (page 201)
- Setting up Kiosk Mode (page 204)
- VISTA SmartConnect Preferences: Using VISTA with SmartConnect (page 208)
- Using the VISTA Dashboard (page 210)
Chapter 6. Checking Out VISTA Cameras

Overview

In Evidence Library 4 Web (EL4 Web), the process of checking out a VISTA® Body Camera assigns a configuration to the camera and the camera to an officer.

Note: A configuration assigns agency-defined settings to the VISTA camera. VISTA configurations are set up by your agency in Evidence Library Administrator (EL Administrator) Device Management. For information on setting up VISTA configurations, see Configuring the VISTA Camera on page 307.

Depending on your agency and system setup, each officer can check out his own camera or a clerk or quartermaster can check out multiple cameras to be assigned to other officers. In most cases, when checking out VISTA, individual officers can also set up their own SmartConnect (page 208), Device, LED, and notification preferences.

In EL4 Web, there are four ways you can check out VISTA Body Cameras:

- From the USB Dashboard
- From the VISTA Dashboard, individually
- From the VISTA Dashboard using Rapid Checkout mode
- Using Kiosk Mode

How your agency sets up its system determines which way you check out VISTA Body Cameras:

- If your agency connects VISTA to EL4 Web using individual USB Bases, you use the USB Dashboard to check out VISTA Body Cameras (page 187)
- If your agency connects VISTA to EL4 Web using VISTA Transfer Stations, you use the VISTA Dashboard to check out VISTA Body Cameras (page 192)
  - From the VISTA Dashboard, you can check out VISTAs individually or using Rapid Checkout.
- If your agency connects VISTA to EL4 Web using VISTA Transfer Stations AND you want officers to be able to check out cameras themselves from a pool of cameras, you use Kiosk Mode to check out VISTA Body Cameras (page 200)
Checking Out VISTA Cameras from the USB Dashboard

If your agency connects VISTA to Evidence Library 4 Web (EL4 Web) using individual USB Bases, you use the USB Dashboard to checkout VISTA Body Cameras. For instructions how to access and other information about the USB Dashboard, see Using the USB Dashboard on page 40.

To check out a VISTA Body Camera from the USB Dashboard:

1. On the USB Dashboard, identify the VISTA Body Camera you want to check out.

2. Click the Actions menu icon for the VISTA Body Camera you want to check out, then select Checkout Device.

The Checkout Device dialog box opens showing the selected camera.
Chapter 6. Checking Out VISTA Cameras

**Note:** The fields on the **Checkout Device** dialog box show the current assigned officer and setting (configuration) for the camera.

3. If you want to change the name of the officer who is checking out the VISTA Body Camera, click the **Select an Officer** field and select the new officer name.

**Note:** If your agency enters badge numbers in EL4 Web, the badge number appears beside the officer name in the list:

4. If you want to change the configuration assigned to the VISTA Body Camera, click the **Camera Setting** field and select the new configuration name.

**Important!** Before you change your VISTA Body Camera’s configuration, verify your configuration selection with your supervisor or system administrator.

5. If you want to change the **SmartConnect**, **Officer**, or **Device Preferences** for the VISTA Body Camera, click **Change Preferences**.
The Preferences section opens.

6. If you want to set or change your VISTA SmartConnect Preferences:
   a. Check the Use with VISTA SmartConnect checkbox.
      The VISTA SmartConnect Preferences section opens.

For information about setting your VISTA SmartConnect Preferences, see VISTA SmartConnect Preferences: Using VISTA with SmartConnect on page 208.
b. Enter or change the **Password** you want to use with your **SSID** to connect your smartphone (with the VISTA SmartConnect application installed) to the VISTA WiFi or VISTA XLT™ checked out to you.

**Note:** The **Password** must be between 8 and 63 characters and cannot contain spaces.

**Tip:** Make a note of your assigned **SSID** and the **Password** that you choose for use with the smartphone app. If you forget the password you set up, it cannot be reset unless you bring the VISTA camera back to the agency and check it out again.

7. If you want to set or change your **Officer Preferences**:

   a. Click the LED or alert fields that you want to change and select the new settings.

   **Note:** Any changes that you make to the **Officer Preferences** fields are associated with your officer name at checkout. The next time that you check out a VISTA Body Camera, your preferences are automatically applied to the camera.

   b. Click the **Preferred VISTA Type** field and select the type of VISTA camera you prefer to use, if that type is available for checkout.

   **Note:** The system applies the VISTA-type preference for you during the **Rapid Checkout** or **Kiosk** checkout process, if the preferred VISTA type is available.
8. If you want to change the device identifier of the VISTA Body Camera, click the **Device ID** field and edit the identifier as needed.

   ![Device Preferences](image)

   **Important!** WatchGuard recommends that you set a unique, user-friendly name for the VISTA Body Camera, for example, VSBike01, the first time you check it out from EL4 Web, then do not change it.

   Changing the identifier in the **Device ID** field does NOT change the device serial number.

9. Click **Checkout Device**.

   EL4 Web loads all of your settings on the VISTA Body Camera, shows that it has been checked out, then ejects it from the computer.

   ![VISTA is checked out](image)

   When VISTA is ejected, it disappears from the **USB Dashboard**.

   **Important!** The configuration containing the new settings is NOT applied to VISTA until you undock it.
Chapter 6. Checking Out VISTA Cameras

Checkout Using the VISTA Dashboard

If your agency connects VISTA to EL4 Web using VISTA Transfer Stations, you use the VISTA Dashboard to check out VISTA Body Cameras. For information about the VISTA Dashboard, see Using the VISTA Dashboard on page 210.

From the VISTA Dashboard, you can:

- **Check out specific VISTAs individually** *(page 193)*
  
  In this case, you select the camera from the VISTA Dashboard that you want to check out for yourself or assign to another officer. The system allows you to select all the checkout options, then closes the Check Out Device dialog box when you are finished checking out the camera.

- **Use Rapid Checkout** to check out multiple VISTAs one right after the other *(page 197)*
  
  With Rapid Checkout, the system selects the camera that is in the best condition (battery and storage) and assigns it to the officer you select. The system allows you to assign multiple cameras without closing the Check Out Device dialog box. You close the dialog box when you are finished checking out VISTA Body Cameras.

  **Note:** You cannot select officer preferences when you use Rapid Checkout. Any existing officer preference associations are applied during the Rapid Checkout process; if individual officer preferences do not exist for a selected officer, the default officer preferences are applied.

- **Generate and print a Checkout Report** for up to the last 24 hours of checkouts *(page 199)*
  
  The report only shows the latest checkout for each VISTA Body Camera.
Checking out individual VISTA cameras from the VISTA Dashboard

To check out a VISTA Body Camera individually from the VISTA Dashboard:

1. On the VISTA Dashboard, identify the VISTA Body Camera you want to check out.

2. Click the Actions menu icon for the VISTA Body Camera you want to check out, then select Check Out Device.

The Check Out Device dialog box opens showing the selected camera.

Note: The fields on the Check Out Device dialog box show the current assigned officer and setting (configuration) for the camera.
Chapter 6. Checking Out VISTA Cameras

3. If you want to change the name of the officer who is checking out the VISTA Body Camera, click the **Select an Officer** field and select the new officer name.

   **Note:** If your agency enters badge numbers in EL4 Web, the badge number appears beside the officer name in the list:

   ![Select an Officer Field](image)

4. If you want to change the configuration assigned to the VISTA Body Camera, click the **Camera Setting** field and select the new configuration name.

   ![Camera Setting Field](image)

   **Important!** Before you change your VISTA Body Camera’s configuration, verify your configuration selection with your supervisor or system administrator.

5. If you want to change the **SmartConnect**, **Officer**, or **Device Preferences** for the VISTA Body Camera, click **Change Preferences**.
Checking out individual VISTA cameras from the VISTA Dashboard

The **Preferences** section opens.

![VISTA Dashboard with Preferences section highlighted]

6. If you want to set or change your **VISTA SmartConnect Preferences**:
   a. Check the **Use with VISTA SmartConnect** checkbox.
      
      The **VISTA SmartConnect Preferences** section opens.

      ![VISTA SmartConnect Preferences]

      For information about setting your **VISTA SmartConnect Preferences**, see **VISTA SmartConnect Preferences: Using VISTA with SmartConnect** on page 208.

   b. Enter or change the **Password** you want to use with your **SSID** to connect your smartphone (with the VISTA SmartConnect application installed) to the VISTA WiFi or VISTA XLT checked out to you.

      **Note:** The **Password** must be between 8 and 63 characters and cannot contain spaces.

      **Tip:** Make a note of your assigned **SSID** and the **Password** that you choose for use with the smartphone app. If you forget the password you set up, it cannot be reset unless you bring the VISTA WiFi back to the agency and check it out again.
Chapter 6. Checking Out VISTA Cameras

7. If you want to set or change your **Officer Preferences**:  
   a. Click the LED or alert preferences fields that you want to change and select the new settings.

   ![Officer Preferences](image1)

   **Note:** Any changes that you make to the **Officer Preferences** fields are associated with your officer name at checkout. The next time that you check out a VISTA Body Camera, your preferences are automatically applied to the camera.

   b. Click the **Preferred VISTA Type** field and select the type of VISTA camera you prefer to use, if that type is available for checkout.

   **Note:** The system applies the VISTA-type preference for you during the **Rapid Checkout** or **Kiosk** checkout process, **IF** the preferred VISTA type is available.

8. If you want to change the device identifier of the VISTA Body Camera, click the **Device ID** field and edit the identifier as needed.

   ![Device Preferences](image2)

   **Important!** WatchGuard recommends that you set a unique, user-friendly name for the VISTA Body Camera, for example, VSBike01, the first time you check it out from EL4 Web, then do not change it.

   **Changing the identifier in the Device ID field does NOT change the device serial number.**

9. Click **Check Out Device**.
Checking out using Rapid Checkout

EL4 Web loads all of your settings on the VISTA Body Camera and shows that it has been checked out.

![Image](image.png)

When VISTA is checked out, it disappears from the **VISTA Dashboard**. In the applicable VISTA Transfer Station, the checked-out camera begins beeping and scrolling the assigned officer name on the display to indicate that it was checked out.

---

**Important!** If the checked-out camera is not removed from the VISTA Transfer Station within five minutes, it stops indicating its checked-out status and reappears on the **VISTA Dashboard**.

---

### Checking out using Rapid Checkout

To check out multiple VISTA Body Cameras, one right after another, using **Rapid Checkout**:

1. On the **VISTA Dashboard**, click **Rapid Checkout**.

   ![Image](image.png)

   The **Check Out Device** dialog box for **Rapid Checkout** opens.

   ![Image](image.png)

2. Click the **Location** field and select the location of the VISTA Transfer Station that you want to check cameras out from.

3. Click the **Officer Name** field and select the officer you want to assign the VISTA Body Camera to.
Chapter 6. Checking Out VISTA Cameras

**Note:** You cannot select officer preferences when you use Rapid Checkout. Any existing officer preference associations are applied during the Rapid Checkout process; if individual officer preferences do not exist for a selected officer, the default officer preferences are applied.

**Note:** If your agency enters badge numbers in EL4 Web, the badge number appears beside the officer name in the list.

4. Click the **Officer Configuration** field and select the configuration you want to assign to the VISTA Body Camera.

5. Click **Assign Device**.

6. Repeat steps 2 through 5 as needed to rapidly check out the number of VISTA Body Cameras you need to assign for a shift.

   As you assign each camera, EL4 Web shows the checkout details on the bottom of the Check Out Device dialog box and loads the selected configuration on the VISTA Body Camera.

   ![Check Out Device dialog box](image)

   As each VISTA is assigned, it disappears from the **VISTA Dashboard**.

   In the applicable VISTA Transfer Stations, each assigned camera begins beeping and scrolling the assigned officer name on the display to indicate that it was checked out.

7. If needed, click **Print Checkout Report** to print a report listing all the checkouts you just performed. The printed checkout report can help you pull the VISTA Body Cameras you just assigned. For more information about the checkout report, see *Printing a Checkout Report* below.

   ![Print Checkout Report](image)

   **Important!** If each checked-out camera is not removed from the VISTA Transfer Station within five minutes, it stops indicating its checked-out status and reappears on the **VISTA Dashboard**.

8. Click **Close** to close the Check Out Device dialog box.
Printing a Checkout Report

You can generate and print a checkout report from the **VISTA Dashboard** itself or from the **Rapid Checkout** dialog box. For more information about rapidly checking out VISTA Body Cameras from the **VISTA Dashboard**, see *Checking out using Rapid Checkout* on page 197.

![Checkout Report]

**From the VISTA Dashboard**

When you generate a checkout report from the **VISTA Dashboard**, you select a timeframe for the checkouts you want to include. The timeframe options include the last 6, 8, 10, 12, and 24 hours.

To print a checkout report from the **VISTA Dashboard**:

- Near the top right of the **VISTA Dashboard**, click **Checkout Report**, then select the timeframe you want to cover in the report.

The report opens in the **Print** dialog box. It shows the latest checkout for each VISTA during the selected timeframe.

**Important!** If the checkout report preview does not open, change your browser settings to allow popups.

**From the Rapid Checkout dialog box**

When you generate a checkout report from the **Rapid Checkout** dialog box, the printout contains the checkout information listed at the bottom of the **Check Out Device** dialog box.

To print a checkout report for **Rapid Checkout**:

- On the **Check Out Device** dialog box for **Rapid Checkout**, click **Print Checkout Report**.

The report opens in the **Print** dialog box.

**Important!** If the checkout report preview does not open, change your browser settings to allow popups.
Chapter 6. Checking Out VISTA Cameras

Checkout Using Kiosk Mode

If your agency connects VISTA to Evidence Library 4 Web (EL4 Web) using VISTA Transfer Stations AND you want officers to check out cameras themselves from a pool of cameras, you use Kiosk Mode for officers to check out VISTA Body Cameras.

From the Kiosk, officers can check out VISTA Body Cameras for their own use, changing their preferences or assigned configuration in the process, as needed. When an officer checks out a VISTA Body Camera using the Kiosk, the system selects the camera that is in the best condition (battery and storage) and assigns it to the officer.

For instructions how to check out VISTA from the Kiosk, see Checking out VISTA cameras from the Kiosk on page 201.

Note: An administrator must set up each Kiosk according to its location. For instructions and information about setting up a Kiosk for a specific location, see Setting up Kiosk Mode on page 204.
Checking out VISTA cameras from the Kiosk

To check out a VISTA Body Camera from a Kiosk:

1. On the Kiosk screen, click the **Enter An Officer Name** field and begin entering your name.

   ![Select an Officer Screen]

   **Note:** You can also click the drop-down arrow in the **Enter An Officer Name** field and select your name from the officer list.

2. When your name appears on the list, select it.

   **Note:** If your agency enters badge numbers in EL4 Web, your badge number appears beside your name in the list:

   ![Select an Officer Screen with Badge Number]

3. If you want to change the configuration assigned to your VISTA Body Camera, the **SmartConnect Preferences**, or other **Officer Preferences**, click **Change Officer Preferences/Device Settings**.
Chapter 6. Checking Out VISTA Cameras

The **Preferences** section opens.

4. If you want to change the configuration assigned to the VISTA that you are checking out, click the **Select a Configuration** field and select the new configuration name.

   **Important!** Before you change your VISTA’s configuration, verify the change with your supervisor or system administrator.

5. If you want to set or change your **VISTA SmartConnect Preferences**:
   a. Check the **Use with VISTA SmartConnect** checkbox.

   The **VISTA SmartConnect Preferences** section opens.

   For information about setting your **VISTA SmartConnect Preferences**, see VISTA SmartConnect Preferences: Using VISTA with SmartConnect on page 208.
b. Enter or change the **Password** you want to use with your **SSID** to connect your smartphone (with the VISTA SmartConnect application installed) to the VISTA WiFi or VISTA XLT checked out to you.

---

**Note:** The **Password** must be between 8 and 63 characters and cannot contain spaces.

---

**Tip:** Note the assigned **SSID** and the **Password** you choose for the smartphone app. If you forget the password, it cannot be reset unless you bring the VISTA WiFi back to the agency and check it out again.

---

6. If you want to set or change your **Officer Preferences**:
   
a. Click the preferences fields that you want to change and select the new settings.

---

**Note:** Any changes you make to the **Officer Preferences** fields are associated with your name at checkout. The next time you check out a VISTA Body Camera, your preferences are automatically applied to the camera.

---

b. Click the **Preferred VISTA Type** field and select the type of VISTA camera you prefer to use, if that type is available for checkout.

---

**Note:** The system applies the VISTA-type preference for you during the **Kiosk** checkout process, if the preferred VISTA type is available.

---

7. Click **VISTA Checkout**.

   The VISTA Body Camera is checked out from EL4 Web. Your assigned camera is shown, with its location, on the Kiosk screen below the **VISTA Checkout** button.
Chapter 6. Checking Out VISTA Cameras

**Tip:** The location of your assigned camera includes the name and the slot number of the Transfer Station where VISTA is docked. In the example above, the checked out VISTA Body Camera **VISTA04** is located in the Transfer Station named **Left VISTA Station**, in slot number **5**. If a checked out camera location reads, for example, **VSBike01, B/4**, the camera **VSBike01** is located in Transfer Station **B**, slot number **4**.

8. Note the location, then retrieve the specified VISTA Body Camera from the appropriate VISTA Transfer Station slot. The camera will be beeping and scrolling your name across its display.

**Important!** If the camera you checked out is not removed from the VISTA Transfer Station within five minutes, it stops beeping and the Display Backlight turns off. The camera is still checked out to you, but can be harder to identify.

Setting up Kiosk Mode

For officers to use Evidence Library 4 Web (EL4 Web) **Kiosk Mode** to check out VISTA Body Cameras, you must set up each Kiosk to point to a specific VISTA Transfer Station location.

**Note:** You can have multiple VISTA Transfer Stations in one Kiosk location.

You set up the Kiosk using your EL4 Web administrator account. Once you have the Kiosk set up, you log back into it using an account you created especially for the Kiosk. Logging in with this Kiosk account disables the Kiosk administrative function and prevents the Kiosk screen from automatically timing out.

To set up a Kiosk for a VISTA Transfer Station location:

1. Create a user account for logging in to the Kiosk.

**Tip:** You set up a Kiosk account in Evidence Library Administrator (EL Administrator) Security Management with help from your network administrator. For information about using EL Administrator Security Management to set up user groups and accounts, see Chapter 9. Managing Security on page 351.

2. Log in to EL4 Web using your administrator account.
3. Move your mouse over the **Manage** tab and select **Kiosk Mode**.
Setting up Kiosk Mode

A generic Kiosk window opens, in administrator mode, showing the **Actions** menu icon on the bottom left.

4. Click the **Actions** menu icon.

The **Kiosk Options** dialog box opens.

5. Click the **Kiosk Service Location** field and select the VISTA Transfer Station location specific to this Kiosk.

6. Click **Save Location**.

The location you selected is assigned to this Kiosk.
Chapter 6. Checking Out VISTA Cameras

7. From the browser window address bar, copy the Kiosk URL that includes the location.

8. Click the **Logout** icon to log out of the Kiosk, then close the browser window.

9. On the desktop of the Kiosk computer, create a shortcut to the Kiosk URL you copied.

   ![Image of Kiosk shortcut]

   **Note:** The form of the shortcut icon is determined by your default browser. See Microsoft help for instructions to create a shortcut.

10. Double-click the Kiosk shortcut icon you created.

    The EL4 Web **Secure Sign In** screen opens for the Kiosk location you set up.

    ![Image of Secure Sign In screen]

11. Log in to EL4 Web using the Kiosk account credentials you created in step 1.
A Kiosk window opens for the location you selected. Because you logged in using the Kiosk account, no Actions menu icon appears on the bottom left.

**Important!** Once you have logged in using the Kiosk account, the Kiosk window does not automatically time out. If someone logs the Kiosk out or closes the browser window, you must double-click the shortcut and log in again using the Kiosk account.

12. Click Fullscreen on the bottom left to expand the Kiosk screen to the full size of the monitor.

**Important!** Full screen mode hides the browser window address bar.

This Kiosk location is ready for officers to check out VISTA Body Cameras for their own use. For instructions how to check out VISTA Body Cameras from this Kiosk, see Checking out VISTA cameras from the Kiosk on page 201.
Chapter 6. Checking Out VISTA Cameras

VISTA SmartConnect Preferences: Using VISTA with SmartConnect

**Note:** Only the Wi-Fi® versions of VISTA (VISTA WiFi and VISTA XLT) can connect to the VISTA SmartConnect smartphone application. For information about VISTA WiFi, VISTA XLT, and Smartconnect, see the VISTA HD Wearable Camera User Guide.

If configured to do so, VISTA WiFi or VISTA XLT can serve as a hotspot for the VISTA SmartConnect smartphone application. SmartConnect allows you to categorize events, live stream, or play back video from VISTA WiFi or VISTA XLT as well as control some of the camera's functionality.

If your agency configures its VISTA cameras to work with the VISTA SmartConnect smartphone application, you set up the camera-to-smartphone Wi-Fi connection permissions when you check out your VISTA WiFi or VISTA XLT camera.

The **VISTA SmartConnect Preferences** fields in the **Preferences** section on the **Check Out Device** dialog boxes:

- Show your assigned **SSID** (unique Wi-Fi network name)
- Allow you to set a corresponding **Password**

**Note:** The **Password** must be between 8 and 63 characters and cannot contain spaces.

To access the **VISTA SmartConnect Preferences** fields:

- Check the **Use with VISTA SmartConnect** checkbox in the expanded **Preferences** section.

The **SSID** and the **Password** that you set up in **VISTA SmartConnect Preferences** allow you to connect your smartphone (with SmartConnect installed) to the Wi-Fi hotspot from the VISTA WiFi or VISTA XLT checked out to you.

The unique SSID and password combination is associated with your name (the **Officer Name** assigned to the VISTA WiFi). When you check out any VISTA WiFi or VISTA XLT camera, your unique SSID/password combination is automatically associated with that camera.
Tip: Make a note of your assigned SSID and the Password that you choose for use with your smartphone. If you forget the password you set up, it cannot be reset unless you bring the VISTA camera back to the agency and check it out again.

You enter the SSID and Password in the Wi-Fi settings on your smartphone the first time you want to connect the SmartConnect app with VISTA. This adds the VISTA WiFi hotspot network to the list of Wi-Fi networks on your phone so it can be accessed again in the future. Unless you change your password, you only need to enter your SSID and password once, the first time you connect. After the first time, your smartphone automatically recognizes the VISTA WiFi hotspot network when the hotspot is active.
Chapter 6. Checking Out VISTA Cameras

Using the VISTA Dashboard

If your agency connects VISTA to Evidence Library 4 Web (EL4 Web) using VISTA Transfer Stations or VISTA WiFi Bases, you use the VISTA Dashboard to monitor the VISTA Body Cameras while they are docked.

You can check out VISTAs from Transfer Stations using the VISTA Dashboard. You can check out VISTA from a WiFi Base using the VISTA Dashboard ONLY if the WiFi Base is on the same network as EL4 Web (that is, NOT in a vehicle).

For information about checking out VISTAs using the VISTA Dashboard, see Checkout Using the VISTA Dashboard on page 192.

**Note:** If your agency wants each officer to check out his own VISTA Body Camera from the VISTA Transfer Station, your agency can also use **Kiosk Mode** for checkout. For information about using Kiosk Mode for checkout, see Checkout Using Kiosk Mode on page 200.

To access the VISTA Dashboard:

- Move your mouse over the Manage tab, then select VISTA Dashboard.
When you dock a VISTA Body Camera into a VISTA Transfer Station, the camera appears as a row on the **VISTA Dashboard**. On the **VISTA Dashboard**, you can identify and monitor the following information for each docked VISTA:

- **Battery**: Shows an icon representing the battery status of the VISTA Body Camera; as the battery charges, the icon updates to show the new available battery status.
  
  The available battery levels associated with the battery icons are:
  
  - ![Battery Icon](image)
  - : From 0 to 25 percent available
  - ![Battery Icon](image)
  - : From 26 to 50 percent available
  - ![Battery Icon](image)
  - : From 51 to 75 percent available
  - ![Battery Icon](image)
  - : From 76 to 100 percent available

  When you move your mouse over the icon, a tooltip shows you a specific value for the available battery percentage.

- **Storage**: Shows an icon representing the storage space status of the VISTA Body Camera; as events are imported, the icon updates to show the new available storage space status.
  
  The available storage space levels associated with the storage space icons are:
  
  - ![Storage Icon](image)
  - : From 0 to 25 percent available
  - ![Storage Icon](image)
  - : From 26 to 50 percent available
  - ![Storage Icon](image)
  - : From 51 to 75 percent available
  - ![Storage Icon](image)
  - : From 76 to 100 percent available

  When you move your mouse over the icon, a tooltip shows you a specific value for the available storage space percentage.

- **Status**: Shows the import status of the events on the VISTA Body Camera.

- **Device**: Shows the agency-assigned device ID or the serial number for the VISTA Body Camera.

- **Location**: Shows the physical location of the VISTA Transfer Station where the VISTA Body Camera is docked.

**Note**: The location and station names of each VISTA Transfer Station are configured by your system administrator.

- **Station/Slot**: Shows the name and slot number of the VISTA Transfer Station where the VISTA Body Camera is docked.

- **Last Checkout**: Shows the date and time that the VISTA Body Camera was last checked out.

- **Officer**: Shows the name of the officer currently assigned to the VISTA Body Camera.

- **Event**: Shows the number of events remaining to be imported from the VISTA Body Camera; as events are imported from the camera, the number decreases.
Chapter 6. Checking Out VISTA Cameras

- **Size**: Shows the total storage size of events remaining to be imported from the VISTA Body Camera; as the events are imported from the camera, the size diminishes by the size of the event just imported
- **Firmware**: Shows the current version of firmware on the VISTA Body Camera

From the **VISTA Dashboard**, you can:

- Check out specific VISTA Body Cameras individually (page 193)
- Check out VISTA Body Cameras using **Rapid Checkout** (page 197)
- Print a **Checkout Report** (page 199)
- Sort the VISTA Body Camera records
  - Click the column heading for the element you want to sort by.
- Filter the VISTA Body Camera records by **Status** or **Location**
  - Click the **Filter** icon in the column you want to filter by, then enter the values you want to use for the filter.
Chapter 7. Managing Evidence Storage

In this chapter...

- Evidence storage and retention setup workflow (page 216)
- Online video storage locations and tier setup (page 222)
- Video Processing storage setup (page 246)
- Import storage setup (page 250)
- Export storage setup (page 251)
- Offline archive storage location setup (page 252)
- Case storage setup (page 253)
- Storage status notification setup (page 255)
- Evidence retention rule setup (page 259)
- Evidence cleanup scheduling (page 263)
Overview

In Evidence Library 4 Web (EL4 Web), you use the Evidence Management module, accessed through the EL4 Web client, to manage your evidence storage.

**Important!** WatchGuard recommends that you have your IT administrator set up your agency’s evidence management. The instructions in this chapter assume the user has administrator credentials as well as an understanding of IT concepts.

The major functions in Evidence Management are:

- Setting up the storage tiers and locations where EL4 Web stages, processes, and stores your agency’s video evidence (page 217)
- Setting up notifications to indicate changes in the status of the storage locations (page 255)
- Setting up rules for evidence retention and cleanup (page 259)
- Scheduling automatic evidence cleanup (page 263)

**Note:** To use Evidence Management, you must be assigned the correct permissions by your system administrator in EL Administrator Security Management.
Accessing Evidence Management

Note: These instructions correspond to step 3 in the Evidence Management workflow (page 216).

In EL4 Web, you access Evidence Management through the EL4 Web client.

- Move your cursor over the Manage tab and select Evidence Management.

The Evidence Management page opens showing the initial tier for Online Video storage.
Chapter 7. Managing Evidence Storage

Setting up evidence storage and retention workflow

The following steps make up a possible workflow for initially setting up EL4 Web Evidence Management:

**Important!** WatchGuard recommends that you have your IT administrator set up your agency’s evidence management. The instructions in this chapter assume the user has administrator credentials as well as an understanding of IT concepts.

1. If not already done, set up disk storage configuration according to WatchGuard best practices.
   For WatchGuard disk drive configuration best practice, see the Evidence Library 4 Web Installation Guide.
2. If not already done, set up the following storage drives/volumes as shared folders (page 219):
   - Online Video (page 222)
   - Video Processing (page 245)
   - Import (page 250)
   - Export (page 251)
   - Offline Archive (optional) (page 252)
   - Case (optional) (page 253)

   **Important!** WatchGuard recommends that you set up security credentials for all of your storage locations.

   If you do not set up security credentials for your storage locations, you must grant permissions on the Import storage location for any individual computers where the Evidence Library Transfer Agent is installed. For more information or help, contact WatchGuard Customer Service.

When you designate your agency’s storage locations in Evidence Management, you point EL4 Web to these locations.

**Warning!** Do not nest storage locations inside of other storage locations. Nesting storage locations can corrupt all involved locations. For more information on setting up storage locations correctly, see Shared folders on page 219.

3. Access Evidence Management. (page 215)
4. Set up tier 1 for Online Video storage. (page 223)
5. Add tiers and locations to Online Video storage as needed. (page 228)
6. Set up the Video Processing storage locations. (page 246)
7. Set up an Import storage location. (page 250)
Managing Storage Locations

After you have installed Evidence Library 4 Web (EL4 Web), you must set up storage locations before EL4 Web can function properly.

**Note:** Work with your WatchGuard representative to determine how much storage space your agency needs and how that space should best be configured to meet your agency's evidence storage needs. For information on storage drive configuration best practices, see the Evidence Library 4 Web Installation Guide.

To view and/or set up your agency's storage:

- Click the tab in the left column of the **Evidence Management** page for the storage type you want to view or set up.

![Storage Locations Screenshot](image-url)
Chapter 7. Managing Evidence Storage

**Important!** WatchGuard recommends that you have your IT administrator set up your agency’s evidence management. The instructions in this chapter assume the user has administrator credentials as well as an understanding of IT concepts.

EL4 Web uses six types of storage location:

- **Online Video**: Long-term storage, made up of tiers (containing locations), used as primary evidence storage (page 222)

  Online Video storage is required. The first tier in Online Video storage must be on-premise, but additional tiers can be on-premise or in the cloud. The first tier is used in conjunction with the Video Processing storage locations to process newly imported video before it is made available online.

- **Video Processing**: Temporary storage, used as the main processing area for newly imported evidence before it is moved back into Online Video storage (page 245)

  Video Processing storage is required. Video Processing can have multiple locations, but they must all be on-premise and local to their corresponding Job Queue Worker Services.

**Important!** Every instance of Job Queue Worker Service in the system must have a local Video Processing storage location.

- **Import**: Temporary storage, used as the staging area for newly imported evidence before it is moved into Online Video storage (page 250)

  Import storage is required. Import storage can have multiple locations, but they must all be on-premise.

- **Export**: Short-term storage, used as the holding area for export packages that are ready to be downloaded; the export packages age out of the Export storage area after a configurable amount of time (page 251)

  Export storage is required. Export storage can have multiple locations, but they must all be on-premise.

- **Offline Archive**: Long-term storage, used as permanent storage for evidence marked by the system to be archived (page 252)

  Offline Archive storage is required to use EL4 Web's archive functionality. Offline Archive storage can have multiple locations; they can be either on-premise or in the cloud.

- **Case**: Long-term storage, used as evidence storage for any file added to a case, except recorded event evidence from the 4RE DVR or VISTA Body Camera (which stays in Online Video storage) (page 253)

  Case storage is required to use the EL4 Web Case Management module. Case storage can have multiple locations; they can be either on-premise or in the cloud.

You can set up Notifications that write information to various system event logs when there are changes in the status of these storage locations. (page 255)
Shared folders

When you set up your agency's storage drives/volumes, you must set each of them up as a shared folder (also called a share).

Each shared folder/storage location must be unique and separate from the others. One storage location cannot contain another location (also called nested).

For example, a shared folder/storage location that you created for Online Video storage should not contain a shared folder/storage location for any other type of storage (Import, Export, Offline Archive, Case, or another Online Video location).

**Warning!** Do not nest storage locations inside of other storage locations. Nesting storage locations can corrupt all involved locations.

User and group account permissions

When you set up a shared folder, you add user or group accounts to two properties:

- **Sharing**
- **Security (NTFS)**

You assign permissions to each account when you add the account to the property.

You add the same users or user groups for both the **Sharing** and **Security (NTFS)** properties.

You assign permissions to each user or group account as you add them for each property.

<table>
<thead>
<tr>
<th>User or group account</th>
<th>Sharing permission needed</th>
<th>Security (NTFS) permission needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everyone</td>
<td>Not needed or Read only</td>
<td>Not needed</td>
</tr>
<tr>
<td>AD machine account</td>
<td>Full control</td>
<td>Full control</td>
</tr>
<tr>
<td>Designated domain user</td>
<td>Full control</td>
<td>Full control</td>
</tr>
<tr>
<td>Local SYSTEM</td>
<td>Full control</td>
<td>Full control</td>
</tr>
</tbody>
</table>

Setting up a shared folder

To set up a shared folder:

1. Create a folder on one of your agency's storage drives, for example, **Import**, in the appropriate location.

   **Tip:** As part of your Evidence Library 4 Web (EL4 Web) installation planning, you should have determined the location for each storage drive. For more information, see the Disk drive configuration best practice section in the Evidence Library 4 Web Installation Guide.

2. Right-click the new folder, then select **Properties**.
Chapter 7. Managing Evidence Storage

3. On the **Properties** dialog box, click the **Sharing** tab.

4. Click **Advanced Sharing**.

5. On the **Advanced Sharing** dialog box, check the **Share this folder** checkbox.

6. Enter the new folder name in the **Share name** field, then add a $ to the end of the share name to make it hidden, for example, **Import$**.

7. Click **Permissions**.
8. On the **Share Permissions** dialog box, add each of the users or groups listed in the *User and group account permissions table* (page 219).

9. Assign each account the corresponding **Sharing** permission (from the table).

10. Click **OK**.

11. On the **Properties** dialog box, click the **Security** tab, then click **Edit**.
12. On the Security Permissions dialog box, add each of the users or groups listed in the User and group account permissions table (page 219).

13. Assign each account the corresponding Security permission (from the table).

14. Click OK then Close to save the changed properties on the new folder.

15. Repeat steps 1 through 14 for all your agency's storage locations.

***Note:*** NAS and SAN devices have different interfaces through which to create shares. See your device's manufacturer's documentation for instructions how to create shares and apply permissions on the particular device.

When you set up your on-premise storage locations in EL4 Web, you add the security credentials you assigned while setting up the shared folders.

**Setting up Online Video storage**

**Online Video** storage functions as your agency's primary evidence storage. It serves as long-term storage for events recorded by the 4RE DVR and the VISTA Body Camera. You can fully access and work with events stored in **Online Video** storage (search for, play back, export, etc). **Online Video** storage is required.

**Important!** You must set up **Online Video, Import, and Video Processing** storage before Evidence Library 4 Web (EL4 Web) can import any events.

Typically, when you set up **Online Video** storage, you set up:

1. First tier on premise, for event processing in conjunction with the **Video Processing** location (page 223)
2. Additional tiers, either on premise (page 228) or in the cloud (page 234)
3. Storage locations in each additional on-premise tier (page 230) or cloud tier (page 236)

**For more information about...**

Online Video storage, see About Online Video storage on page 240.
Setting up the first tier

Note: These instructions correspond to step 4 in the Evidence Management workflow (page 216).

When you first access Evidence Management in EL4 Web, the first tier already exists. The system uses the first tier for event processing (in conjunction with the Video Processing location), so it is automatically set up as an on-premise tier.

To set up the first tier:

1. Access Evidence Management. (page 215)
   The Manage Storage Locations pane of the Evidence Management module opens showing the default first tier, Local Tier, under Online Video Storage.

   ![Manage Storage Locations pane](image)

   Important! If you have upgraded from a version of EL4 Web prior to version 4.1, the Local Tier shows all of your existing storage locations. Contact your WatchGuard representative for help reconfiguring your existing storage locations.

2. Click the Edit icon (📝) for the Local Tier to edit the first tier name and attributes.
   The Edit Tier dialog box opens.

   ![Edit Tier dialog box](image)
Chapter 7. Managing Evidence Storage

**Note:** The first tier must be on premise, so the cloud is not available as an option for the first tier.

3. Enter the **Name** for the first tier.

**Note:** Use a name that is meaningful for your agency.

4. Select whether you want the first tier to use **Rollover** or **Round Robin** to store events in the first tier locations.

   For more information about the supported storage usage types, see *Rollover versus round-robin usage* on page 242.

5. Click **Update**.

   The name and attributes you assigned to the first tier show under **Online Video Storage**.

   **Note:** If you are upgrading, you do not need to set up additional storage locations for the first tier. You can use the locations that you have.
6. Click the first tier + sign to add a storage location to the first tier. The **Add Storage Location** dialog box opens.

7. Enter the **Name** for the storage location on the first tier, then click **Browse**.

   **Note:** Use a name that is meaningful for your agency. The special characters \, i, ?, ¿, ", /, : are not supported.

   The **Browse** panel slides down.
8. Enter the UNC path to the storage location you set up as part of your disk storage configuration process.

**Warning!** Only enter a UNC path to a storage location that is not already in use. Adding an existing location as a new location can corrupt both locations.

**Note:** The disc storage configuration process corresponds to steps 1 and 2 of the Evidence Management workflow ([page 216](#)).

9. Click the + sign next to the location, then check the **Use Security Credential** checkbox. The security credentials fields open below the checkbox.
10. Enter the **Account Name** and **Password** you set up when you set up your storage drives as shared folders (page 219).

   **Note:** Typically, WatchGuard recommends that you set up security credentials for all of your storage locations. However, if the storage location you select does not require security credentials, you do not need to check the **Use Security Credential** checkbox. Contact WatchGuard Customer Service for more information.

11. Click **OK**.
   
The storage location you selected is noted on the dialog box, and the **Allocation** fields for the location appear below it.

12. Enter the amount of space on the selected drive location that should be allocated to this storage location.

   **Warning!** Allowing the storage location to fill completely (100 percent) can cause the location to become unusable.
Chapter 7. Managing Evidence Storage

13. Click **Add**.

The storage location is added to the first tier.

14. Repeat steps 6 through 13 to add further locations to the first tier, if desired.

*Adding an on-premise video storage tier*

**Note:** These instructions correspond to step 5 in the Evidence Management workflow (page 216).

For more information about tiers, see **Tiers** on page 240.

To add an on-premise tier to **Online Video Storage**:

1. Click **Add Tier**.

The **Add Tier** dialog box opens.
2. Enter the **Name** for the new tier.

   ![Note: Use a name that is meaningful for your agency.]

3. Select whether you want to use **Rollover** or **Round Robin** for any locations in this tier. For more information about the supported storage usage types, see *Rollover versus round-robin usage* on page 242.

4. Select **On Premise** as the **Storage Type**. For more information about supported storage tier locations, see *On-premise versus cloud storage* on page 242.

5. Enter the amount of time (**Days** or **Years**) you want the system to keep events in the previous tier before moving them to this new tier. For more information about moving events from tier to tier, see *Moving events to the next tier automatically* on page 243.

6. Click **Add**.

   The new tier is added to **Online Video Storage**.

7. Add one or more storage locations to the tier.

   For instructions how to add storage locations to an on-premise tier, see *Adding a storage location to an on-premise tier* on page 230.
Chapter 7. Managing Evidence Storage

Adding a storage location to an on-premise tier

*Note:* These instructions correspond to step 5 in the Evidence Management workflow (page 216).

For more information about storage locations, see *Storage locations* on page 241.

To add a storage location to an on-premise tier:

1. Click the + sign for the on-premise tier where you want to add the location.

The *Add Storage Location* dialog box opens.

2. Enter the **Name** for the storage location on the on-premise tier, then click **Browse**.

*Note:* Use a name that is meaningful for your agency. The special characters \, i, ?, ¿, ", /, : are not supported.
Adding a storage location to an on-premise tier

The **Browse** panel slides down.

3. Enter the UNC path to the storage location you set up as part of your disk storage configuration process.

   **Warning!** Only enter a UNC path to a storage location that is not already in use. Adding an existing location as a new location can corrupt both locations.

   **Note:** The disc storage configuration process corresponds to steps 1 and 2 of the Evidence Management workflow (page 216).

4. Click the + sign next to the location to select it, then check the **Use Security Credential** checkbox.

   **Tip:** After you enter the computer name (\<ComputerName>\) for the path to the storage location, you can click **Update List** and navigate to the location you set up.
Chapter 7. Managing Evidence Storage

The security credentials fields open below the checkbox.

5. Enter the **Account Name** and **Password** you set up when you set up your storage drives as shared folders (page 219).

**Note:** Typically, WatchGuard recommends that you set up security credentials for all of your storage locations. However, if the storage location you select does not require security credentials, you do not need to check the **Use Security Credential** checkbox. Contact WatchGuard Customer Service for more information.

6. Click **OK**.

The storage location you selected is noted on the dialog box, and the **Allocation** fields for the location appear below it.

7. Enter the amount of space on the selected drive location that should be allocated to this storage location, then click **Add**.
Adding a storage location to an on-premise tier

**Warning!** Allowing the storage location to fill completely (100 percent) can cause the location to become unusable.

The location is added to the on-premise tier.

8. Repeat steps 1 through 7 to add further locations to the on-premise tier, as needed.

**Tip:** If you want to change the priority of a storage location within a tier, click and hold the Handle icon ( HANDLE ), then drag the storage location up or down in the list.
Chapter 7. Managing Evidence Storage

Adding a cloud video storage tier

**Note:** These instructions correspond to step 5 in the Evidence Management workflow (page 216).

For more information about tiers, see Tiers on page 240.

To add a cloud tier to Online Video Storage:

1. Click Add Tier.

   ![Add Tier dialog box](image)

   The Add Tier dialog box opens.

2. Enter the Name for the new tier.

   **Note:** Use a name that is meaningful for your agency.

3. Select whether you want to use **Rollover** or **Round Robin** for any locations in this tier.

   For more information about the supported storage usage types, see Rollover versus round-robin usage on page 242.

4. Select **Microsoft Azure Cloud** as the Storage Type.

   For more information about supported storage tier locations, see On-premise versus cloud storage on page 242.
5. Enter the amount of time (Days or Years) you want the system to keep events in the previous tier before moving them to this new tier.

For more information about moving events from tier to tier, see Moving events to the next tier automatically on page 243.

6. Click Add.

The new tier is added to Online Video Storage.

7. Add one or more storage locations to the tier.

For instructions how to add storage locations to a cloud tier, see Adding a storage location to a cloud tier below.
Chapter 7. Managing Evidence Storage

Adding a storage location to a cloud tier

**Note:** These instructions correspond to step 5 in the Evidence Management workflow (page 216).

For more information about storage locations, see *Storage locations* on page 241.

To add a storage location to a cloud tier:

1. Click the + sign for the cloud tier where you want to add the location.

The **Add Storage Location** dialog box opens.

2. Enter the **Name** for the storage location on the cloud tier.

   **Note:** Use a name that is meaningful for your agency. The special characters \, i, ?, ä, " , /, : are not supported.

3. Enter your agency's Microsoft® Azure Government cloud account information in the remaining fields.
4. Click **Test** to verify the connection to your agency's cloud storage location.

   **Note:** If the connection comes back as invalid, verify your agency's Microsoft Azure Government cloud account information was entered correctly then try again.

5. Once the connection is verified, click **Add**.
   The location is added to the cloud tier.

6. Repeat steps 1 through 5 to add further locations to the cloud tier, as needed.

---

**Editing a video storage tier**

For more information about tiers, see **Tiers** on page 240.

To edit the name or attributes for a tier:

1. Click the **Edit** icon (edit) next to the **Name** of the tier you want to edit.
   The **Edit Tier** dialog box opens.

2. Edit the tier attributes as needed, then click **Update**.
Chapter 7. Managing Evidence Storage

Editing a storage location for an on-premise tier

For more information about storage locations, see Storage locations on page 241.

To edit a storage location for an on-premise tier:

1. Click the Edit icon ( ) for the storage location whose name or attributes you want to edit. The Edit Storage Location dialog box opens.

2. Edit the storage location attributes as needed, then click Update.

Important! If the storage location you are editing requires credentials, make sure the Use Security Credential checkbox is checked, and verify the Account Name and Password for the storage location.

Note: You cannot edit the path to the storage location once you have saved it. If you need to change the path to a storage location, contact WatchGuard customer service for help.
Editing a storage location for a cloud tier

For more information about storage locations, see Storage locations on page 241.

To edit a storage location for a cloud tier:

1. Click the Edit icon for the storage location whose name or attributes you want to edit. The Edit Storage Location dialog box opens.

2. Edit the storage location attributes as needed, then click Update.

Note: You cannot edit the Storage Account Name or Endpoint Suffix for the cloud location. The system combines these values to create the web address (URL) to your agency’s cloud storage, that is, the path to the location. You cannot edit the path to a storage location once it is saved.

If you need to change your agency’s Microsoft Azure Government cloud settings for a storage location, contact WatchGuard customer service for help.
Chapter 7. Managing Evidence Storage

About Online Video storage

Online Video storage is unique among the types of EL4 Web storage: it consists of storage tiers (below), each containing one or more storage locations (page 241). You set up each tier individually to take advantage of the different types of storage you have available to your agency, for example, SSD (solid-state drive), HDD (hard disk drive), and cloud (Microsoft® Azure government).

Online Video storage functions as your agency’s primary evidence storage. It serves as long-term storage for events recorded by the 4RE DVR and the VISTA Body Camera. You can fully access and work with events stored in Online Video storage (search for, play back, export, etc). Online Video storage is required.

Important! You must set up Online Video, Import, and Video Processing storage before EL4 Web can import any events.

You set up your storage drive types and configuration as part of your planning and preparation to install or upgrade to EL4 Web.

Note: For information on storage drive configuration best practices, see the Evidence Library 4 Web Installation Guide.

You set up some of the individual tier features using EL4 Web Evidence Management:

- Tier location, either on-premise or in the cloud (page 242)
- Storage location usage, either rollover or round robin (page 242)
- Amount of time before events are moved to the next tier (page 243)

Important! Work with your WatchGuard representative to determine how much storage space your agency needs and how that space should best be configured to meet your agency’s evidence storage needs.

For an example of a common Online Video storage configuration, see Online Video storage examples on page 244.

Tiers

Tiers allow you to set up your agency's primary evidence storage (Online Video) using multiple drives of varying quality and performance. Tiers also give you the option of using the cloud for some of your agency’s long-term online evidence storage.

When you first access Evidence Management, the first tier already exists. The system uses the first tier for event processing, in conjunction with the Video Processing storage locations, so the first tier is automatically set up as an on-premise tier. You edit the first tier to finish setting it up. For instructions how to set up the first tier, see Setting up the first tier on page 223.
Important! When you upgrade from an Evidence Library version prior to EL4 Web version 4.1, existing Video storage locations automatically become part of the first tier. Contact your WatchGuard representative for help reconfiguring the first tier storage locations.

You can set up additional tiers either on premise or in the cloud. Events automatically move from the first tier to the next tier after they are processed. When applicable, events move on to additional tiers as they age.

For example, you can set up Online Video storage with three tiers:

- First tier, HDD, on premise, RAID 5 or RAID 10
  In this example, the first tier functions partially as a processing tier, in conjunction with the Video Processing storage locations. (The Video Processing locations would be set up on SSD drives. For more information, see Video Processing storage on page 245.) The events move onto another drive for storage as soon as processing is finished.
- Second tier, HDD, on premise, RAID 5, RAID 6, or RAID 10
  Continuing the example, events move to the second tier as soon as they have finished processing. They remain in the second tier storage for a configurable amount of time.
- Third tier, cloud
  Events move to the cloud after a configurable amount of time. In Online Video storage in the cloud, events remain online and fully accessible.

For more information about...

Adding an on-premise tier, see page 228.
Adding a cloud tier, see page 234.

Storage locations
You must add at least one storage location to each tier. When you add a storage location, you set up the path to the storage drive and indicate how much of the location can be used for evidence storage (Allocation).

Note: Each storage location takes on attributes of the tier, for example, on premise (page 242), round robin (page 242).

A storage location can be open or secure. When you set up a path to a secure network location, you also enter the network admin credentials. The system uses these credentials any time it adds events to the secure location. You only have to enter the credentials one time when you initially add the storage location.

Note: Once you save the path to a location, you can no longer edit that path.
Chapter 7. Managing Evidence Storage

You can allocate how much of each location to use for storage as an amount of space (for example, 500 GB, 2 TB) or a percentage of the whole location. You should always allocate something less than 100 percent of a storage location.

**Warning!** Allowing a storage location to fill completely (100 percent) can cause the location to become unusable.

If you add multiple locations to a tier, you can change the priority of the locations:

- Click and drag the **Handle** icon (▲) to move the storage location up or down in the list.

![Handle icon](image)

*For more information about…*

Adding a storage location to an on-premise tier, see page 230.

Adding a storage location to a cloud tier, see page 236.

**On-premise versus cloud storage**

Evidence Management in EL4 Web supports on-premise and cloud storage. For on-premise storage, EL4 Web supports most common types of disk storage. For cloud storage, EL4 Web supports the Microsoft Azure government cloud. For recommendations for storage types and configurations, see the planning sections of the *Evidence Library 4 Web Installation Guide*.

You assign the **On Premise** or **Cloud** storage attribute at the tier level. Any tier except the first tier can be either on premise or in the cloud. The first tier (participates in event processing) must be on premise. An on-premise tier only has on-premise storage locations. A cloud tier only has storage locations in the cloud.

**Rollover versus round-robin usage**

Evidence Management supports both the rollover and round-robin methods of storage usage.

With rollover, the system uses one storage location at a time. When the first storage location reaches the allocated limit, EL4 Web begins using the second storage location within the tier. The system rolls over from one storage location to the next in the order that the locations are listed within the tier.

With round robin, the system spreads its usage across all the storage locations within the tier, one event at a time stored in each location. The system moves from one storage location to the next, event by event, in the order that the locations are listed within the tier.

You assign the **Rollover** or **Round Robin** attribute at the tier level. Any tier can be assigned either method. All the locations within the tier participate in that method.
Moving events to the next tier automatically

**Note:** You can edit the method of storage usage from *Rollover* to *Round Robin* (or vice versa) at any time.

You can change the usage order of the locations within the tier:

- Click and drag the *Handle* icon for the location you want to move up or down in the list order.

![Image showing the order of storage locations](image)

**Moving events to the next tier automatically**

When you add a tier to *Online Video* storage, you tell the system when events should move to this new tier using the *Move here from previous tier after* fields.

You can enter any number of days or years up to a limit of 99 years.

![Image showing the add tier dialog](image)

**Tip:** Set the *Move here from previous tier after* value to 0 days when you add your second tier. The system uses the first tier for processing (with the *Video Processing* locations), so moving events off the first tier as soon as possible can help performance. Setting this value to 0 days for the second tier moves events off the first tier immediately after they are processed.
Chapter 7. Managing Evidence Storage

**Online Video storage examples**

An example using three tiers:

- **First tier**: HDD, RAID 5 or RAID 10, **On Premise**

  ![First tier diagram](image)

  The first tier has one storage location, used in event processing. Events move off this tier onto the second tier as soon as they have finished processing.

- **Second tier**: HDD, RAID 10, **On Premise**

  ![Second tier diagram](image)

  The second tier has two locations. The system moves events from the first tier to this tier as soon as it has finished processing them. The events are stored in the locations on this tier using the **Round Robin** method. Events move off this tier onto the third tier after 90 days, unless they are archived or purged before 90 days. For more information on archiving, purging, and retention rules, see *Managing Evidence Retention and Cleanup* on page 257.
Third tier: Cloud (Microsoft Azure Government)

The third tier consists of your agency’s cloud storage in the Microsoft Azure Government cloud. The system moves events from the second tier to this tier after 90 days. Events moved onto this tier (cloud storage) remain on this tier until they are archived or purged.

Other common Online Video storage configurations:

- **Two tiers**: First tier, HDD, **On Premise, Round Robin**; second tier, Microsoft Azure Government cloud
  
  For this example, the first tier (used in event processing) has multiple storage locations. The system uses the locations in a **Round Robin** fashion. Events move to the second tier (cloud storage) immediately after processing. They stay in the cloud until they are archived or purged.

- **One tier**: HDD, **On Premise, Round Robin**
  
  For this example, the tier has multiple storage locations. EL4 Web uses these locations, in a **Round Robin** fashion, in event processing and for storage. Events are processed (in conjunction with a Video Processing location) and stored in the same storage location. They stay in this location until they are archived or purged.

**Video Processing storage**

In Evidence Library 4 Web (EL4 Web), version 4.4, Video Processing storage serves as a temporary storage location for events recorded by the 4RE DVR and the VISTA Body Camera. The Video Processing location functions as the main processing area for newly imported video evidence before the evidence is moved back into Online Video storage for final processing. Video Processing storage is required.

**Important!** You must set up Video Processing, Online Video, and Import storage before EL4 Web can import any events.

Video Processing can have multiple locations, but each must be on-premise and local to its corresponding Job Queue Worker Service.
Chapter 7. Managing Evidence Storage

**Important!** Every instance of Job Queue Worker Service in the system must have a local Video Processing storage location.

Video Processing storage functions only as a processing location, in conjunction with the first tier of Online Video storage (page 240).

WatchGuard recommends that you set up any Video Processing storage locations using the highest performing storage drive available to your agency, for example, SSD. This setup allows EL4 Web to do its most intensive event processing (transcoding) on high-speed, high-performance drives. (The Online Video first tier can be set up on an HDD drive.)

**Note:** Video Processing storage processes two events at a time by default.

In this setup, the system moves the events onto a lower-performing drive (for example, HDD) for storage after event processing is finished.

Setting up a Video Processing storage location

**Note:** These instructions correspond to step 6 in the Evidence Management workflow (page 217).

To add a storage location to Video Processing storage:

1. Click the + sign under Video Processing.

   The Add Storage Location dialog box opens.
2. Click the **Name** field then select the name of the computer where you set up the storage location for **Video Processing** as part of your disk storage configuration process.

**Note:** The disc storage configuration process corresponds to steps 1 and 2 of the Evidence Management workflow (page 216).

3. Click **Browse**.

   The **Browse** panel slides down.
Chapter 7. Managing Evidence Storage

4. Enter the UNC path to the storage location on the computer you selected in the Name field list.

**Warning!** Only enter a UNC path to a storage location that is not already in use. Adding an existing location as a new location can corrupt both locations.

5. Click the + sign next to the location to select it, then check the Use Security Credential checkbox.

   The security credentials fields open below the checkbox.

6. Enter the Account Name and Password you set up when you set up your storage drives as shared folders (page 219).
Setting up a Video Processing storage location

**Note:** Typically, WatchGuard recommends that you set up security credentials for all of your storage locations. However, if the storage location you select does not require security credentials, you do not need to check the Use Security Credential checkbox. Contact WatchGuard Customer Service for more information.

7. Click **OK**.

   The storage location you selected is noted on the dialog box, and the **Allocation** fields for the location appear below it.

8. Enter the amount of space on the selected drive location that should be allocated to this storage location, then click **Add**.

   **Warning!** Allowing the storage location to fill completely (100 percent) can cause the location to become unusable.

The **Video Processing** storage location is added.

9. Repeat this procedure until all your system’s Job Queue Workers have corresponding **Video Processing** storage locations.

   For more information about...

   **Online Video** storage, see page 222.

   **Export** storage, see page 251.
Chapter 7. Managing Evidence Storage

**Offline Archive** storage, see page 252.

**Case** storage, see page 253.

Exporting evidence, see page 119.

### Import storage

In Evidence Library 4 Web (EL4 Web), **Import** storage serves as temporary storage for events recorded by the 4RE DVR and the VISTA Body Camera. It functions as the staging area for newly imported video evidence before the evidence is moved into **Online Video** storage. **Import** storage is required. For information on importing recorded events, see *Chapter 2. Importing Evidence* on page 29.

---

**Important!** You must set up **Import**, **Online Video**, and **Video Processing** storage before EL4 Web can import any events.

---

Because the system uses **Import** storage for event staging, it is automatically set up **On Premise**. You must add at least one storage location to **Import** storage.

---

**Setting up an Import storage location**

---

**Note:** These instructions correspond to step 7 in the Evidence Management workflow (page 217).

---

To add a storage location to **Import** storage:

1. Click the + sign under **Import**.

2. Follow the instructions (steps 2 through 7) for adding a storage location to an on-premise tier (page 230).

**For more information about...**

- **Online Video** storage, see page 222.
- **Video Processing** storage, see page 245.
- **Offline Archive** storage, see page 252.
- **Case** storage, see page 253.
Export storage

In Evidence Library 4 Web (EL4 Web), Export storage is short-term storage.

**Note:** For faster exports, WatchGuard recommends that you use SSD for your Export storage.

It functions as the holding area for export packages that are ready to be downloaded. The export packages remain available for download in the Export storage area until they age out, after a configurable amount of time (2-14 days). Export storage is required. For information on downloading export packages, see Using the My Exports tab on page 156.

**Important!** You cannot export evidence from EL4 Web until you have set up an Export storage location.

Because the system uses Export storage for holding export packages, it is automatically set up On Premise. You must add at least one storage location to Export storage.

Setting up an Export storage location

**Note:** These instructions correspond to step 8 in the Evidence Management workflow (page 216).

To add a storage location to Export storage:

1. Click the + sign under Export.

2. In the Retention Policy field, select how long you want export packages to remain available for download from the Export storage location.

3. Follow the instructions (steps 2 through 7) for adding a storage location to an on-premise tier (page 230).

**Note:** The system also uses the Export storage area as an on-premise work space when uploading case attachments to Case storage.
For more information about...

- **Online Video** storage, see page 222.
- **Video Processing** storage, see page 245.
- **Import** storage, see page 250.
- **Case** storage, see page 253.
- Exporting evidence, see page 119.

### Offline Archive storage

In Evidence Library 4 Web (EL4 Web), **Offline Archive** storage serves as long-term storage for events recorded by the 4RE DVR and the VISTA Body Camera. It functions as a permanent storage location for video evidence marked by the system to be archived. **Offline Archive** storage is required if your agency chooses to use EL4 Web's archive functionality.

When an event is archived, its video and data files are moved to the **Offline Archive** storage location. A record of the archived event remains in the database. You cannot play back an archived event, but the record of the event shows in **Search** results. Events can be archived manually or automatically.

**Offline Archive** storage can be **On Premise** or in the **Cloud**. You must add at least one storage location to **Offline Archive** storage.

For information about manually archiving events, see *Manually Archiving Events* on page 98.
For information about automatically archiving events using retention rules, see *Evidence retention rules* on page 259.
Setting up an Offline Archive storage location

Note: These instructions correspond to step 9 in the Evidence Management workflow (page 217).

To add a storage location to Offline Archive storage:

1. Click the + sign under Offline Archive.

2. If you want to set up an Offline Archive location On Premise, follow the instructions (steps 2 through 7) for adding a storage location to an on-premise tier (page 230).

   If you want to set up an Offline Archive location in the Cloud, follow the instructions (steps 2 through 5) for adding a storage location to a cloud tier (page 236).

For more information about...

Online Video storage, see page 222.
Video Processing storage, see page 245.
Import storage, see page 250.
Export storage, see page 251.

Case storage

In Evidence Library 4 Web (EL4 Web), Case storage is long-term storage. It functions as the evidence storage location for any file attached to a case in EL4 Web Case Management, except events recorded by the 4RE DVR or VISTA Body Camera. Recorded events that are made part of a case remain in Online Video storage. Case storage is required if your agency chooses to use the EL4 Web Case Management module. For information about Case Management in EL4 Web, see Chapter 4. Working with Cases on page 101.

Case storage can be On Premise or in the Cloud. You must add at least one storage location to Case storage.

Note: The system uses the Export storage area as an on-premise work space when you upload case attachments to Case storage. For more information about Export storage, see Export storage on page 251.
Chapter 7. Managing Evidence Storage

**Setting up a Case storage location**

*Note: These instructions correspond to step 10 in the Evidence Management workflow (page 217).*

To add a storage location to **Case** storage:

1. Click the + sign under **Case Storage**.

2. If you want to set up a **Case** storage location **On Premise**, follow the instructions (steps 2 through 7) for adding a storage location to an on-premise tier (page 230).

   If you want to set up a **Case** storage location in the **Cloud**, follow the instructions (steps 2 through 5) for adding a storage location to a cloud tier (page 236).

*For more information about…*

- **Online Video** storage, see page 222.
- **Video Processing** storage, see page 245.
- **Import** storage, see page 250.
- **Export** storage, see page 251.
- **Offline Archive** storage, see page 252.
Storage status notifications

**Note:** Setting up storage **Notifications** corresponds to step 11 in the Evidence Management workflow (page 216).

In Evidence Library 4 Web (EL4 Web), you can set up notifications that write information to system event logs when there are changes in the status of your agency’s storage locations.

**Tip:** WatchGuard Technical Services can help you set up your local system to notify you when a storage status notification is written to the event logs. Contact your WatchGuard representative for information.

To view and set up storage status notifications:

- Click **Notifications** in the left column of the **Evidence Management** page.

![Notifications](image)

**Note:** Any changes you make to **Notifications** are automatically saved.

You set up four different notifications and a threshold:

- **Storage Low**: When enabled, notifies you when the overall storage level across a storage tier or type has reached the **Threshold** you set up

**Note:** The **Storage Low** and **Storage Full** notifications apply only across an individual tier in **Online Video** storage. They apply across all combined locations for each of the other storage types.

The **Storage Low** notification is enabled by default. This notification is written to the web server’s event log.

For example, you have four locations set up in the second tier of **Online Video** storage. You have your **Threshold** set to 60 percent. When the combined locations in the second tier
storage reach 60 percent full overall, a notification is written to the event log. The system continues to write **Storage Low** notifications to the event log until the storage level of the combined second tier storage locations goes below the 60 percent threshold.

- **Storage Full**: When enabled, notifies you when not enough storage space exists across a storage tier or type for an event that is being imported

  The **Storage Full** notification is enabled by default. This notification is written to the web server's event log.

  **Warning!** Allowing a storage location to fill completely (100 percent) can cause the location to become unusable.

- **Storage Offline**: When enabled, notifies you when an individual storage location of any storage type has become unavailable

  The **Storage Offline** notification is enabled by default. This notification is written to the web server's event log.

- **Remote Upload**: When enabled, notifies you when the storage level of an individual wireless upload server has reached the **Threshold** you set up

  **Note**: An EL4 Web system may have multiple wireless upload servers. These servers were set up (including their storage locations) during the EL4 Web installation or upgrade process.

  The **Remote Upload** notification is enabled by default. This notification is written to the individual wireless upload server's event log.

- **Threshold**: Click and drag the **Threshold** meter control to set the **Storage Low** and **Remote Upload** notification levels; when a storage tier or type exceeds this threshold, the system writes the notification to the corresponding event log

  The system uses the **Threshold** percentage for the **Storage Low** notification and the **Remote Upload** notification.

  **Note**: The **Threshold** percentage is on top of the **Allocation** percentage you set for every storage location you added.

  For example, you add a location and allocate 80 percent of that location for storage. You set the notification **Threshold** percentage to 60 percent. This means that a **Storage Low** notification is written to the event log when the storage level exceeds 60 percent of the 80 percent allocation of the storage location.
Managing Evidence Retention and Cleanup

Evidence Library 4 Web (EL4 Web) cleans up the event data in your agency’s evidence storage locations according to **Retention Rules** (page 259) that you set up. You can schedule data cleanup to run automatically (page 262), or you can run it manually (page 264), as needed.

The **Retention Rules** determine when EL4 Web archives or purges event data. These rules correspond to the categories set up for the **EventCategory** event tag in Device Management. For information about the **EventCategory** event tag, see *Setting up the EventCategory event tag* on page 334.

The **Cleanup Scheduling** determines whether EL4 Web runs its data cleanup operation automatically on a schedule or manually per user request.

**Note:** WatchGuard recommends that you schedule data cleanup to run automatically.

---

### Retention Rules

<table>
<thead>
<tr>
<th>Category</th>
<th>Keep Online</th>
<th>Keep Archived</th>
<th>Time</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>X</td>
<td>X</td>
<td>火炬1</td>
<td>永远保留</td>
</tr>
<tr>
<td>Traffic Warning</td>
<td></td>
<td></td>
<td>火炬1</td>
<td>永远保留</td>
</tr>
<tr>
<td>Traffic Classics</td>
<td></td>
<td></td>
<td>火炬1</td>
<td>永远保留</td>
</tr>
<tr>
<td>Incident</td>
<td></td>
<td></td>
<td>火炬1</td>
<td>永远保留</td>
</tr>
<tr>
<td>BUI</td>
<td></td>
<td></td>
<td>火炬1</td>
<td>永远保留</td>
</tr>
<tr>
<td>Drug</td>
<td></td>
<td></td>
<td>火炬1</td>
<td>永远保留</td>
</tr>
<tr>
<td>Emergency</td>
<td></td>
<td></td>
<td>火炬1</td>
<td>永远保留</td>
</tr>
<tr>
<td>Fire</td>
<td></td>
<td></td>
<td>火炬1</td>
<td>永远保留</td>
</tr>
</tbody>
</table>

### Cleanup Scheduling

The **Cleanup Scheduling** panel allows you to schedule the data cleanup operation.

**Note:** WatchGuard recommends that you schedule data cleanup to run automatically.
Chapter 7. Managing Evidence Storage

**Note:** You can also manually archive or purge an individual event from the **Events** tab. For information on manually archiving an individual event, see Manually Archiving Events on page 98. For information on manually purging an individual event, see Manually Purging Events on page 100.

Setting up evidence retention rules

**Note:** These instructions correspond to step 12 in the Evidence Management workflow (page 216).

To set up evidence retention rules:

1. Click **Retention Rules** in the left column of the **Evidence Management** page. The list of **Retention Rules** opens.

2. Set the **Default** retention rule:
   a. Set how long events should remain online, in the **Default Keep Online** column.
   b. Set how long events should remain archived, in the **Default Keep Archived** column.

For more information about the **Default** retention rule, see **Default rule** on page 260.
3. Set rules for any event categories that should be treated as exceptions to the **Default** retention rule. For a category that you want to set as an exception:
   a. Check the **Override Default** checkbox in the **Keep Online** column.
   b. Set how long events tagged with this category should remain online, in the **Keep Online** column.
   c. Check the **Override Default** checkbox in the **Keep Archived** column.
   d. Set how long events tagged with this category should remain archived, in the **Keep Archived** column.
   e. Repeat steps a through d for any other categories that you want to set as exceptions.

For more information about setting exceptions to the **Default** rule, see **Exceptions to the Default rule** on page 261.

**Evidence retention rules**

The **Retention Rules** determine when EL4 Web cleans up (archives or purges) event data. These rules correspond to the categories set up for the **EventCategory** event tag in Device Management.

The rules tell EL4 Web:

- How long to keep an event available online
- Whether an event should be archived and how long it should remain archived
- Whether an event should be purged and when it should be purged

Once you set up the **Retention Rules**, the **EventCategory** tag that an officer applies to a recorded event controls which rule the system applies to the event. Depending on what you set up, some categories are stored longer than others, and some are automatically archived or purged at the end of their retention period.
Chapter 7. Managing Evidence Storage

**Note:** A recorded event that has been attached to a case in EL4 Web Case Management is exempt from any archive and purge rules while it is attached to the case. Once the event is no longer part of a case, it is again subject to the retention rules. For information on Case Management, see Chapter 4. Working with Cases on page 101.

When you set up your agency's evidence retention rules (page 258), you set up:

- The **Default** rule (below)
- Exceptions to the **Default** rule (page 261)

**Note:** Any changes you make to the **Retention Rules** are automatically saved.

**Default rule**

The **Default** rule sets how long, by default, events should remain available in **Online Video** storage (page 222), and how long, by default, they should remain archived in **Offline Archive** storage (page 252).

<table>
<thead>
<tr>
<th>Keep Online</th>
<th>Keep Archived</th>
<th>Total Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Duration</td>
<td>Years</td>
</tr>
<tr>
<td>Categories</td>
<td>Override Default</td>
<td>Override Default</td>
</tr>
</tbody>
</table>

If you set a limit on how long events should remain archived, once an event reaches that time limit, the event is purged.

The values you set for the **Default** rule are automatically set for each of the individual event categories in the **Retention Rules** list.
Exceptions to the Default rule

You set up any exceptions to the Default Retention Rule on a category basis. If you want all events to be archived and purged on the same schedule, regardless of category, you only need to set the Default rule.

If you want certain categories of events to be treated differently, you set up each of those categories separately as exceptions that Override Default. For example, you may want all events categorized as Traffic Warning to be purged after 60 days online and all events categorized as Assault to remain online indefinitely. All the rest you want to follow the Default rule.

![Retention Rules Table]

You can set exceptions for either the Keep Online value, the Keep Archived value, or both values.
Chapter 7. Managing Evidence Storage

Scheduling automatic evidence cleanup

**Note:** These instructions correspond to step 13 in the Evidence Management workflow (page 216).

To schedule automatic event data cleanup:

1. Click **Cleanup Scheduling** in the left column of the **Evidence Management** page.
   
   The **Cleanup Scheduling** pane opens.

2. Check the **Enabled** checkbox to indicate that you want to set up an automatic data cleanup schedule.
3. Select a **Schedule** option: **Daily**, **Weekly**, or **Monthly**, then select or enter the appropriate values.

![Screenshot of the Cleanup Scheduling form]

The values you set are saved automatically to the database.

**Evidence cleanup**

Evidence cleanup applies the evidence retention rules that you set up to the events in Evidence Library 4 Web (EL4 Web) evidence storage. When EL4 Web runs its event data cleanup, it goes through all applicable storage locations, keeping, archiving, or purging events according to the retention rules that apply.

The values you enter for **Cleanup Scheduling** determine whether EL4 Web runs its event data cleanup:

- Automatically on a schedule (page 264)
- Manually per user request (page 264)

---

**Note:** WatchGuard recommends that you schedule data cleanup to run automatically.
Chapter 7. Managing Evidence Storage

**Automatic**

You can schedule EL4 Web's event data cleanup ([page 262](#)) to run **Daily, Weekly, or Monthly**:

- **Daily**: Runs event data cleanup once per day at the time you set

  ![Daily Schedule](image)

  For example, you can set cleanup to run every day at 3 AM.

- **Weekly**: Runs event data cleanup one or more times per week on the days and at the time you set

  ![Weekly Schedule](image)

  For example, you can set cleanup to run twice per week, on Monday and Thursday, at 3 AM.

- **Monthly**: Runs event data cleanup once per month on the date and at the time you set

  ![Monthly Schedule](image)

  For example, you can set cleanup to run once per month, on the 20th, at 3 AM.

---

**Note:** You can manually run event data cleanup at any time, even if you have set up data cleanup to run automatically on a schedule.

---

**Manual**

You can manually run event data cleanup, as needed, instead of or in addition to the scheduled automatic cleanup. To run cleanup manually:

- Click **Run Manually**.

When you manually run the event data cleanup, the system uses the same retention rules it does for the scheduled automatic cleanup.
Chapter 8. Managing Devices

In this chapter...

- Configuring 4RE DVRs (page 270)
- Configuring VISTA Body Cameras (page 307)
- Setting up event tags (page 331)
Overview

For Evidence Library 4 Web (EL4 Web), Evidence Library Administrator (EL Administrator) Device Management helps you manage both your fleet of 4RE® DVRs and your set of VISTA® Body Cameras. You use Device Management to set up configurations for both devices. A configuration assigns settings to each device in a way that is specific to its user’s needs. The **4RE Management** feature in Device Management also lets you deploy a 4RE configuration to your 4RE DVRs.

**Note**: You assign a VISTA configuration to a VISTA Body Camera using the **Checkout** feature in EL4 Web. For information on checking out VISTA from EL4 Web, see Chapter 6. Checking Out VISTA Cameras on page 185.

The major features in Device Management are:

- 4RE DVR management ([page 270](#))
- VISTA Body Camera management ([page 307](#))
- Event tag management ([page 331](#))

**Important!** To use EL Administrator Device Management, you must be assigned the correct permissions by your system administrator in EL Administrator Security Management. If you cannot access EL Administrator or, once you access it, you do not see the **Device Management** tab, you do not have system permission to work with Device Management. If you need system permission to use Device Management, contact your system administrator.
Accessing Device Management

You access Device Management through the administrative module for Evidence Library 4 Web (EL4 Web), Evidence Library Administrator (EL Administrator).

1. On the desktop of the computer where EL Administrator is installed, double-click the Evidence Library Administrator icon.

   The **Evidence Library Administrator Sign In** dialog box opens.

![Evidence Library Administrator Sign In dialog box]

2. Enter your **Username** and **Password**, then click **Sign-In**.

   The WatchGuard Evidence Library Administrator opens with the **Device Management** tab active.

![WatchGuard Evidence Library Administrator window]
Using Device Management

The Evidence Library 4 Web (EL4 Web) Device Management module helps you manage your fleet of 4RE DVRs and set of VISTA Body Cameras. You use Device Management to set up configurations then deploy or assign them to your devices. A configuration assigns the settings on a device in a way that is specific to its user’s needs.

Using Device Management, you can set up one or more configurations for each device type depending on the needs of your agency. How do you determine whether your agency needs a single configuration or multiple configurations for each type of device?

Agencies with a smaller number of officers may only need a single configuration for each type of device; larger agencies with many officers filling different roles may need multiple configurations. Consult with your WatchGuard representative when determining which options are best for your agency.

Single configurations for smaller agencies

Generally, a smaller agency can implement a single configuration for its entire fleet of 4REs or set of VISTAs. Specifically, a single configuration for each device type is appropriate under the following conditions:

- Officers operate any of the devices at any given time; in other words, all officers rotate through the 4RE-equipped vehicles or the VISTA cameras
- All devices of each type in the agency have the same values set up for officer permissions, recording properties, device behavior, and equipment, as applicable

Multiple configurations for larger agencies

If an agency has many possible scenarios for its devices (for example, multiple unique officer roles, in-car equipment setups, or recording property values), the agency needs multiple configurations for each type of device. Each configuration is set up to handle a different scenario. EL4 Web Device Management can handle as many configurations as needed.

An agency could conceivably create a unique configuration for each device the agency uses. In this case, the agency has complete flexibility to configure each device according to its unique set of officer preferences, recording property values, etc. Each configuration is set up and then managed separately.

For the most common multiple-configuration arrangement, an agency sets up unique configurations for a few groups of users/devices, for example, patrol, K9, traffic, drug interdiction. In this case, those devices used for drug interdiction (or patrol, K9, or traffic) would all have the same configuration loaded on their 4REs or VISTAs.
Setting Up System Settings

Note: These instructions correspond to step 2 on both the 4RE recommended workflow (page 271) and the VISTA recommended workflow (page 308).

The System Settings is the first screen that opens when you access Evidence Library Administrator (EL Administrator). You use the System Settings to customize EL Administrator for your agency. Using the System Settings you set up:

- Your agency name
- Which WatchGuard devices (4RE DVR and VISTA Body Camera) your agency uses and needs to configure
- If you use both devices, whether you want the system to automatically link together applicable events recorded by both devices

To set up the System Settings:

1. Access EL Administrator.

2. Enter the name of your agency in the Department Name field.

Tip: The amount of space available for your agency name on the 4RE DVR display screen is limited. If you enter a name the 4RE considers too long, the system truncates it starting from the right (the end of the name). When you set the name of your agency or department, consider using abbreviations when possible; for example, for Highwater Police Department, enter **HPD** or **Highwater PD**.
Chapter 8. Managing Devices

3. If your agency does not use the 4RE DVR, clear the **Enable 4RE Management** checkbox.

   **Note:** 4RE Management is enabled by default.

4. If your agency does not use the VISTA Body Camera, clear the **Enable VISTA Management** checkbox.

   **Note:** VISTA Management is enabled by default.

5. If your agency does not want related 4RE and VISTA recorded events to be automatically linked at import, clear the **Turn on Automatic Event Linking** checkbox.

   **Note:** Automatic Event Linking is enabled by default.

Configuring the 4RE DVR

The **4RE Management** feature in Evidence Library Administrator (EL Administrator) helps you manage your fleet of 4RE DVRs. You use 4RE Management to set up 4RE configurations then deploy them to your 4RE DVRs.

The major sections of the 4RE Management feature are:

- Setting up the list of 4RE DVRs (page 274)
- Creating and setting up a 4RE configuration (page 278)
- Deploying a 4RE configuration (page 297)

WatchGuard follows a basic workflow when setting up an agency's fleet of 4RE DVRs. This WatchGuard workflow is one possible way of configuring the 4RE DVR and does not necessarily cover all possible 4RE Management situations. To see the steps in the WatchGuard workflow, see *Recommended workflow for configuring a 4RE DVR* on page 271.

**Accessing 4RE Management**

To access the 4RE Management feature:

- On the **System Settings** screen, click **Click to manage in-car video**.
  
  For information on **System Settings**, see Setting Up System Settings on page 269.
The **4RE Management Operations** dialog box opens.

---

**Recommended workflow for configuring a 4RE DVR**

**Note:** The workflow in this section is basic; it does not necessarily cover all possible **4RE Management** situations. In addition, many aspects of the workflow are determined by your agency protocols, so they cannot be completely addressed in the user guide.

This workflow gives an example of how and when it seems most logical to perform a task in **4RE Management**. It is intended to serve as a guide only.

The following steps make up a recommended workflow for initially configuring your fleet of 4RE DVRs:

2. If not already done, set up your agency name and other system settings. (page 269)
3. Access **4RE Management**. (page 270)
4. Assign your agency 4RE administrator password. (page 272)
5. Create initial default configurations. (page 279)
6. Add 4RE DVRs to the agency vehicle list. (page 275)
7. Verify each vehicle on the list is assigned to a configuration; if it is not, assign it to a configuration. (page 281)
8. Assign enrollments (user groups) to each configuration. (page 282)
9. If not already done, set up system event tags. (page 331)
10. Set the recording properties for each configuration. (page 284)
11. Set up the DVR behavior for each configuration. (page 291)
12. Set the import settings for each configuration. (page 295)
13. Confirm the configuration settings, save each configuration, then close **4RE Management**.
14. Reaccess **4RE Management**.
15. Manually deploy each configuration to the corresponding 4RE DVRs. (page 298)
Chapter 8. Managing Devices

Setting up agency 4RE settings

**Note:** These instructions correspond to step 4 on the 4RE recommended workflow (page 271).

Generally, you set your agency’s 4RE information once in Evidence Library Administrator (EL Administrator), then do not need to change it.

To set the agency settings for the first time:

1. Access **4RE Management**.
   
   For instructions how to access **4RE Management**, see Accessing 4RE Management on page 270.

2. On the **4RE Management Operations** dialog box, click **Edit configuration**.

   ![4RE Management Editor dialog box](image)

   The **4RE Management Editor** dialog box opens showing your current 4RE agency settings.

3. If you want to make video files on the 4RE removable USB thumb drive unusable by anything except Evidence Library 4 Web (EL4 Web), double-click **Enable USB Security** to change the value to **Yes**.

4. If you want to make video files on the 4RE removable USB thumb drive viewable in the Evidence Library Express (ELX) Viewer, double-click **Enable USB for ELX Viewer** to change the value to **Yes**.
5. If you want to change the default units that display on-screen with the 4RE temperature, from Fahrenheit to Celsius, double-click **Temperature Display Units**.

The **Edit Property** dialog box opens.

6. Select **Celsius**, then click **Save**.

7. If you want to change the default units that display on-screen with radar or GPS speed, from Mph to Kph, double-click **Speed Display Units**.

The **Edit Property** dialog box opens.

8. Select **Kph**, then click **Save**.

9. If you want to change the default 4RE administrative password, double-click **Admin In-Car Password**.

---

**Important!** The in-car administrative password is common to all your fleet 4RE DVRs. Changing the password in this section affects the 4RE password for all of your fleet.
Chapter 8. Managing Devices

Note: The default administrative password is set by the manufacturer to ABCDE1.

The DVR In-Car Administrative Password dialog box opens.

10. Enter the new 4RE administrative password twice, then click Save.
11. On the 4RE Management Editor dialog box, click Apply.

All Vehicles list

With Evidence Library 4 Web (EL4 Web), you add your agency's 4RE DVRs to a central list, All Vehicles. The All Vehicles list contains settings identifying each 4RE that records video evidence for your agency.

When you enter the 4RE's information on the All Vehicles list, you can assign it to a 4RE configuration.

When you deploy a 4RE configuration, you select which 4REs should have that configuration applied to them. The system generates a configuration file specific to each 4RE DVR using the configuration assignment you made for the 4RE when you added it to the All Vehicles list. For more information on deploying 4RE configurations, see Deployment on page 297.

To access the All Vehicles list:

- Click All Vehicles in the left pane of the 4RE Management Editor dialog box.

On the All Vehicles list you can:

- Add new 4RE DVRs (page 275)
- Edit existing 4RE DVRs (page 277)
Adding a new 4RE DVR to the All Vehicles list

Note: These instructions correspond to step 6 on the 4RE recommended workflow (page 271).

To add a new 4RE DVR to the All Vehicles list:

1. Click All Vehicles in the left pane of the 4RE Management Editor dialog box.
   The All Vehicles list appears.

2. Click New.
   The Create New Vehicle dialog box opens.

3. Enter the unique ID for the new 4RE DVR in the Vehicle ID field and select the radar type, if applicable.

   Note: Each Vehicle ID should be unique.
Chapter 8. Managing Devices

4. Select the 4RE's **Network Connection Type**, then enter the **Device IP Address** for the device you selected, if applicable.

   **Note:** If you do not know the IP address for the wireless radio you selected in the **Network Connection Type** field, contact WatchGuard Customer Service for help.

5. If this 4RE's video will be live-streamed to Watch Commander, enter the IP address or machine name of the Watch Commander server and the **Control Port** number if different than the default.

   **Important!** The default port number **25820** will be the control port in most cases. Do not change the port number without consulting your WatchGuard representative.

6. Choose whether the 4RE should alert that its video is being live-streamed, with an icon on the display screen or a beep.

7. Select the configuration this 4RE will be assigned to, then choose whether the configuration should automatically deploy to that 4RE DVR the next time it connects to the agency network.

   For information about setting up configurations for the 4RE DVR, see **4RE configurations** on page 278.

   For information about deploying 4RE configurations automatically or manually, see **Deployment** on page 297.

8. If this 4RE will receive its IP address from a WatchGuard Smart Power Switch in the vehicle, check **Enable DHCP client**.

9. Click **Create**.

   The new 4RE DVR is added to the **All Vehicles** list with the settings you provided.

10. Click **Apply** on the bottom of the **4RE Management Editor** dialog box.
Editing properties for an existing 4RE DVR

To edit the properties of an existing 4RE DVR on the All Vehicles list:

1. Click **All Vehicles** in the left pane of the **4RE Management Editor** dialog box.
   The **All Vehicles** list appears.

2. Select the 4RE whose properties you want to edit, click **Edit**, then **Edit selected vehicle**.
   The **Edit Vehicle** dialog box opens.

3. Edit, update, or add information to the settings for this 4RE, then click **Save**.
   The settings for the selected 4RE DVR are updated on the **All Vehicles** list.

4. Click **Apply** on the bottom of the **4RE Management Editor** dialog box.
4RE configurations

To use your WatchGuard 4RE DVR with Evidence Library 4 Web (EL4 Web), you must configure it using the Evidence Library Administrator (EL Administrator) 4RE configuration feature.

In EL4 Web, a 4RE configuration is a group of settings that you apply to a 4RE DVR. When deployed to a DVR, the configuration automatically sets up the DVR so it meets the specific needs of its users. You can create multiple configurations, each corresponding to a use of 4RE in your agency; for example, you can set up different configurations for patrol, K9, drug intervention vehicles, or interview rooms.

4RE configurations are listed on the 4RE Management Editor dialog box.

- Click Configurations in the left pane of the 4RE Management Editor dialog box to open the list of existing 4RE configurations.

From the list of 4RE configurations, you can add new configurations or edit existing configurations.

You can add a new 4RE configuration two ways:

- Create a new configuration that uses system default settings (page 279)
- Copy an existing configuration and give it a new name (page 280)

Once you add a 4RE configuration, you need to set it up. There are five main 4RE configuration areas to set up:

- Assigned Vehicles (page 281)
- Assigned Enrollments (page 282)
- Recording Properties (page 284)
- DVR Behavior (page 291)
- Import Settings (page 295)

To access these configuration areas:

- Click the plus sign (+) next to the configuration name in the left pane of the 4RE Management Editor dialog box.
Creating a new 4RE configuration

**Note:** These instructions correspond to step 5 on the 4RE recommended workflow (page 271).

To create a new configuration with system default settings:

1. Click **Configurations** in the left pane of the 4RE Management Editor dialog box.
   The list of 4RE configurations appears.

2. Click **New**.
   The Create New Configuration dialog box opens.

3. Enter a name for the new configuration in the **Name** field, then click **Create**.
   The new configuration with system default settings is added to the list of your agency configurations.
Chapter 8. Managing Devices

Copying an existing 4RE configuration

To create a new configuration from a copy of an existing configuration:

1. Click **Configurations** in the left pane of the 4RE Management Editor dialog box.
   The list of 4RE configurations appears.

2. Select the configuration you want to copy, click **Edit**, then select **Create a copy of selected configuration**.
   The Create New Configuration from Copy dialog box opens.

3. Enter a name for the copy of the configuration in the **Name** field, then click **Create**.
   The new configuration copied from an existing configuration is added to the list of your agency 4RE configurations.
Assigning a 4RE DVR to a configuration

Note: These instructions correspond to step 7 on the 4RE recommended workflow (page 271).

The Assigned Vehicles list shows the 4RE DVRs assigned to a 4RE configuration. Using the Assigned Vehicles list, you can assign additional 4REs from the All Vehicles list to the selected 4RE configuration, or unassign 4REs from the configuration, making them available to assign to another configuration.

A 4RE DVR can have only one 4RE configuration, but a 4RE configuration can have more than one 4RE DVR assigned to it.

To assign a 4RE DVR to a 4RE configuration:

1. On the 4RE Management Editor dialog box, select the 4RE configuration you want to assign a 4RE DVR to, then click the plus sign (+) next to the configuration name.
   The configuration expands to show its five parts.

2. Click Assigned Vehicles.
   The Assigned Vehicles list appears.

3. In the Available Vehicles section, select the 4RE you want to assign to the configuration, then click Assign.
Chapter 8. Managing Devices

The 4RE is assigned to its new configuration: the name of the 4RE DVR moves from the Available Vehicles section to the Vehicles Assigned To <Configuration> section on the Assigned Vehicles list.

4. Click Apply on the bottom of the 4RE Management Editor dialog box.

Tip: You can also assign a 4RE DVR to a 4RE configuration when you add the 4RE to the All Vehicles list. On the Create New Vehicle dialog box, in the Assign to Configuration field, select the configuration you want to assign the new 4RE DVR to. For more information, see Adding a new 4RE DVR to the All Vehicles list on page 275.

Assigning a user group to a 4RE configuration

Note: These instructions correspond to step 8 on the 4RE recommended workflow (page 271).

In Evidence Library 4 Web (EL4 Web), users are assigned to a 4RE configuration through user groups. User groups are set up by your system administrator according to your agency’s network security policies in conjunction with the features in Evidence Library Administrator (EL Administrator) Security Management.

Note: For information on EL Administrator Security Management, see Chapter 9. Managing Security on page 351. For information about your agency’s user groups, contact your system administrator.

The Assigned Enrollments list shows the user groups assigned to a 4RE configuration. Using the Assigned Enrollments list, you can assign additional user groups to the selected 4RE configuration, or unassign user groups from the configuration.

Tip: Click the plus sign (+) next to an assigned user group to see the list of individuals in the user group. The individual names under each of the user groups assigned to a 4RE configuration together make up the list of names an officer sees on the corresponding 4RE DVR.
A user group can be assigned to more than one 4RE configuration. To assign a user group to a 4RE configuration:

1. On the **4RE Management Editor** dialog box, select the 4RE configuration you want to assign a user group to, then click the plus sign (+) next to the configuration name. The configuration expands to show its five parts.

2. Click **Assigned Enrollments**. The **Assigned Enrollments** list appears.

3. In the unassigned section, select the user group you want to assign to the configuration, then click **Assign**. The user group is assigned to its new 4RE configuration: the user group name moves from the unassigned section to the assigned section on the **Assigned Enrollments** list.

4. Click **Apply** on the bottom of the **4RE Management Editor** dialog box.
Chapter 8. Managing Devices

Setting the 4RE Recording Properties

**Note:** These instructions correspond to step 10 on the 4RE recommended workflow (page 271).

In Evidence Library Administrator (EL Administrator), the 4RE **Recording Properties** allow you to set:

- Video quality for front, secondary, and panoramic cameras
  
  For information on the video quality options for cameras connected to the 4RE, see 4RE video quality settings on page 287.

- Auto-start record settings and record-start delay

- Auto-stop settings and maximum event time

- Whether 4RE participates as a recording group member for event starts and stops

- Additional record time
  
  When Pre- or Post-Event Time is enabled, 4RE continuously records then saves video from a period of time before a recorded-event start or after an event stop. Pre-event video is added before the start of the recorded event, post-event video after the stop of the event (page 290).

- Maximum event size

- Configuration event tags
  
  For information about setting up system event tags, see Setting Up Event Tags on page 331.

To set up the **Recording Properties** for a 4RE configuration:

1. On the 4RE Management Editor dialog box, select the 4RE configuration whose **Recording Properties** you want to set, then click the plus sign (+) next to the configuration name.

The configuration expands to show its five parts.
2. Click **Recording Properties**.

The **Recording Properties** settings appear.

3. Set the **Front Camera Settings**.
   a. Set whether an officer has permissions to select or change the front camera's state on the 4RE DVR.
      
      For information on user permissions, see *4RE user permissions settings* on page 290.
   b. Verify that you want to use critical rules on the 4RE to determine which video quality is saved for a recorded event.
   c. If you are using critical rules on the 4RE, select the **Critical** and **Routine Video Quality** and **Frame Rate** for the front camera.
      
      For information on front camera video quality settings, see *Front camera* on page 287.

4. Set the **Secondary Camera Settings**.
   a. Set whether an officer has permissions to select or change a secondary camera's state on the 4RE DVR.
      
      For information on user permissions, see *4RE user permissions settings* on page 290.
   b. Select the **Video Quality** and **Frame Rate** for the secondary cameras.
      
      For information on secondary camera video quality settings, see *Secondary camera* on page 288.
5. Set the **Panoramic Camera Settings**.
   a. Set whether an officer has permissions to select or change a panoramic camera's state on the 4RE DVR.
      For information on user permissions, see *4RE user permissions settings* on page 290.
   b. Select the **Video Quality** and **Frame Rate** for the panoramic camera.
      For information on panoramic camera video quality settings, see *Panoramic camera* on page 289.

6. Set up the **Auto Start Record** settings.
   a. Mark which settings you want to use to automatically start a recorded event.
   b. Mark the settings where you want to set a record-start delay, as applicable.
   c. If you choose to use a delay, set the amount of time the 4RE should delay before starting a recorded event.

   **Note:** The amount of time you set for a record-start delay applies to all the settings that use a delay. You cannot set one amount of time for one record-start setting and another amount of time for another setting.

   d. If you want the 4RE to start a recorded event when it is informed by another group member (VISTA camera) that the other group member has started an event, check the **Group member start** checkbox.

7. Select how much **Pre-Event** and **Post-Event Time** you want to add to a recorded event using the **Additional Record Time** section.

8. Set up the **Auto-Stop Record** settings.
   a. Select how long the 4RE should wait after all record-start settings are inactive before it prompts an officer to stop an event.
   b. If you want the 4RE to stop its recorded event when informed by another group member (VISTA camera) that the other group member has stopped an event, check the **Group member stop** checkbox.

9. If you want to enable the 4RE DVR to periodically remind the officer (with a beep) that it is still capturing a recorded event, in the **Recording Reminder Alerts** section, select the **Alert every** option, then enter the interval between reminders.

10. If you want to split large events on the 4RE DVR, in the **Maximum Recorded Event Size** section, select the maximum size a recorded event should be.

11. If you use the USB thumb drive to transfer events from the 4RE to EL4 Web, and if you transfer events less often than one time per day (for example, once per week), enter the number of hours you want 4RE to wait before it rewrites events on the USB thumb drive (for example, **168 Hours**, for 7 days), in the **USB Events** section.

12. If you want to enable the 4RE DVR to automatically stop a recorded event when it reaches a specified duration, in the **Maximum Recorded Event Time** section, select the **Stop after** option, then enter the maximum event length.

13. Verify that you want an officer to have permissions to override the default video resolution setting for a recorded event on the 4RE using the **Event Override Controls** section.
14. Assign event tags to the 4RE configuration using the **Assigned Event Tags** section.

**Important!** You MUST check the checkbox for each event tag that you want to assign to the 4RE configuration. If you do not check the checkbox to include the event tag in the configuration, the event tag will NOT show on the 4RE display screen, even if you make it a required event tag.

For information on setting up event tags, see *Setting Up Event Tags* on page 331.

15. Click **Apply**.

### 4RE video quality settings

The 4RE **Recording Properties** allow you to set the quality of video the 4RE DVR saves from its connected cameras: front, secondary, or panoramic.

**Note:** For information on the VISTA Body Camera video quality settings, see VISTA video quality settings on page 318.

**Front camera**

The quality of the video that the 4RE DVR saves from the front camera depends on whether the recorded event is tagged as critical or routine. What is considered critical or routine is determined by your agency. Usually critical recorded events are saved using the highest quality video and others are saved at a lower quality.

**Note:** You can designate a category of recorded event as critical using the **Critical** checkbox when you set up the event tags that an officer responds to at the end of an event. For more information on setting up event tags, see *Setting Up Event Tags* on page 331.
The higher the video quality you select, the better the quality of the resulting video and the larger the needed storage space. The following table lists the front camera’s supported video quality options with each one’s resolution and storage space needs:

<table>
<thead>
<tr>
<th>Video quality</th>
<th>Video resolution</th>
<th>Frames per second</th>
<th>Storage space (GB per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD high resolution</td>
<td>1280 x 720</td>
<td>30</td>
<td>2.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>1.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.55</td>
</tr>
<tr>
<td>HD medium resolution</td>
<td>1280 x 720</td>
<td>30</td>
<td>1.76</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.44</td>
</tr>
<tr>
<td>HD low resolution</td>
<td>1280 x 720</td>
<td>30</td>
<td>1.32</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.33</td>
</tr>
<tr>
<td>SD high resolution</td>
<td>864 x 480</td>
<td>30</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.22</td>
</tr>
<tr>
<td>SD medium resolution</td>
<td>864 x 480</td>
<td>30</td>
<td>0.66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.16</td>
</tr>
<tr>
<td>SD low resolution</td>
<td>864 x 480</td>
<td>30</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.11</td>
</tr>
</tbody>
</table>

**Secondary camera**

The front-facing camera is considered the primary camera. All other cameras, except the panoramic camera, are considered secondary cameras. For more information about the panoramic camera, see Panoramic camera below.
The higher the video quality you select, the better the quality of the resulting video and the larger the storage space need. The following table lists a secondary camera's supported video quality options with each one's resolution and storage space needs:

<table>
<thead>
<tr>
<th>Video quality</th>
<th>Video resolution</th>
<th>Frames per second</th>
<th>Storage space (GB per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SD high resolution</strong></td>
<td>720 x 480</td>
<td>30</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.22</td>
</tr>
<tr>
<td><strong>SD medium resolution</strong></td>
<td>720 x 480</td>
<td>30</td>
<td>0.66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.16</td>
</tr>
<tr>
<td><strong>SD low resolution</strong></td>
<td>720 x 480</td>
<td>30</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.11</td>
</tr>
</tbody>
</table>

**Panoramic camera**

The panoramic camera is part of WatchGuard's HD Panoramic Camera. The HD Panoramic Camera contains two cameras: a rotatable HD (high definition) camera that functions as the front camera in the vehicle, and a fixed panoramic camera that has a very wide field of view. For information about Front Camera Settings, see Front camera on page 287.

The higher the video quality you select, the better the quality of the resulting video and the larger the storage space need. The following table lists the panoramic camera's supported video quality options with each one's resolution and storage space needs:

<table>
<thead>
<tr>
<th>Video quality</th>
<th>Video resolution</th>
<th>Frames per second</th>
<th>Storage space (GB per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High resolution</strong></td>
<td>1280 x 240</td>
<td>30</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.22</td>
</tr>
<tr>
<td><strong>Medium resolution</strong></td>
<td>1280 x 240</td>
<td>30</td>
<td>0.66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.16</td>
</tr>
<tr>
<td><strong>Low resolution</strong></td>
<td>1280 x 240</td>
<td>30</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7.5</td>
<td>0.11</td>
</tr>
</tbody>
</table>
Chapter 8. Managing Devices

4RE user permissions settings

The 4RE Recording Properties allow you to set permissions for an officer to select or change a camera's state from the 4RE DVR. The available options are:

- Camera on, off, or background
- Camera on or background
- Force camera on
- Camera on or off

Selecting an option that includes the Camera off permission allows the officer to turn the applicable camera off from the 4RE; NO video is recorded from the camera that is off.

Selecting an option that includes the Camera background permission allows the officer to treat the video from the applicable camera as background. This means that video from the camera is recorded, but the officer has the option, on the 4RE, to include (or exclude, by default) that camera's video from the recorded event. Background video is always included in a Record-After-the-Fact® (RATF) event.

4RE pre-event

The pre-event feature enables a device to continuously record then save video for a period of time before a recorded-event start. The pre-event video is added before the start of the recorded event.

For example, you start a recorded event, manually or automatically, at 2:15 pm. You stop the event, manually or automatically, at 2:35 pm. After adding in a configured pre-event video time of 1 minute, the recorded event includes video recorded from 2:14 pm to 2:35 pm.

4RE pre-event video time can be None up to 10 minutes.
Setting the 4RE DVR Behavior properties

**Note:** These instructions correspond to step 11 on the 4RE recommended workflow (page 271).

In Evidence Library Administrator (EL Administrator), the 4RE **DVR Behavior** settings allow you to set:

- Time zone and locale where your agency is located
- IP address where the 4RE DVR connects to Evidence Library 4 Web (EL4 Web) to upload video wirelessly, if applicable
- Whether a non-supervisor officer has permission to change some of the settings or review video that is not his own on the 4RE
- Radar speed values to be displayed on the 4RE screen and included in the recorded event, if applicable
- Format for GPS coordinates appearing on the 4RE screen and whether the GPS speed should be displayed if no radar is connected to the system
- Whether speed values should be saved as part of the metadata associated with the recorded event
- When and how the 4RE is automatically powered on and off, if it is in a vehicle
- How much delay should occur before the 4RE is automatically shut down once the ignition is turned off
- What information to display as text on the 4RE screen
- Rules for the activation of wireless, cabin, and auxiliary microphones connected to a 4RE
- Whether the 4RE DVR Display Screen should go blank when the vehicle begins to move

To set up the **DVR Behavior** for a 4RE configuration:

1. On the **4RE Management Editor** dialog box, select the 4RE configuration whose **DVR Behavior** you want to set, then click the plus sign (+) next to the configuration name.

   The configuration expands to show its five parts.
Chapter 8. Managing Devices

2. Click **DVR Behavior**.

The **DVR Behavior** settings appear.

3. Set the time zone for your agency.
   a. Double-click the **Time zone** property.
   b. On the **Edit Property** dialog box, select the time zone where your agency operates, then click **Save**.

4. Set the **Locale** for your agency.
   a. Double-click the **Locale** property.
   b. On the **Edit Property** dialog box, select the language and location applicable to your agency, then click **Save**.

   **Note:** The **Locale** value defaults to the language and location value set for your EL4 Web server.
5. If your agency uses a wireless network to upload video to EL4 Web, set the Wireless Service IP address.
   a. Double-click the **Server IP address** property.
   b. On the **Server Settings** dialog box, set the **Server IP Address** for the EL4 Web Wireless Service, then click **Save**.

6. Set whether an officer has permission to change certain 4RE settings without a supervisor password.
   Double-click a property to change its value.

7. Set what level of video review an officer can perform on the 4RE without a supervisor password.
   a. Double-click the **Officer video review level** property.
   b. On the **Edit Property** dialog box, select the video review level, then click **Save**.

8. If a radar is connected to the system, set which radar values should be displayed on the 4RE screen.
   Double-click a property to change its value.

9. Set the GPS-coordinate format to display on-screen.
   a. Double-click the **GPS output format** property.
   b. On the **Edit Property** dialog box, select the GPS format, then click **Save**.

10. Set whether the speed calculated by the GPS should be displayed if no radar is connected to the system.
    Double-click the property to change its value.

11. Set whether the speed data should be stored with the metadata in the EL4 Web database.
    Double-click the property to change its value.

12. If the 4RE DVR is in a vehicle, set the rules regarding whether it should automatically power on or off with the vehicle ignition.
    Double-click a property to change its value.

13. If set to automatically power off with the vehicle ignition, set how much delay should occur before the 4RE automatically shuts down after the ignition is turned off.
    a. Double-click the **Ignition shutdown time** property.
    b. On the **Edit Property** dialog box, select how long the 4RE should wait before automatically shutting down after the ignition is turned off, then click **Save**.
    c. If your agency uploads video wirelessly from the 4RE DVR, double-click the **Wireless transfer shutdown timer** property.
    d. On the **Edit Property** dialog box, select how long the 4RE should wait before fully shutting down if it is still transferring video when the ignition shutdown timer expires, then click **Save**.

   For more information about the shutdown timers, see below.

14. Set what information should be displayed as text or graphics on the 4RE screen.
    Double-click a property to change its value.
Chapter 8. Managing Devices

15. Set the rules for the activation of wireless, cabin, and auxiliary microphones connected to a 4RE.
   Double-click a property to change its value.
16. Set whether the 4RE Display Screen should go blank when the vehicle begins to move.
   Double-click the property to change its value.
17. Click **Apply**.

**Shutdown timers**

If you use the 4RE DVR in a vehicle, and set it to automatically power off when the ignition turns off, you can use the 4RE shutdown timer features. The shutdown timers allow you to set how long the 4RE DVR should wait before automatically shutting down once the vehicle ignition is turned off. There are two shutdown timers:

- **Ignition shutdown timer**: Automatically starts counting down when the ignition is turned off
- **Wireless transfer shutdown timer**: Automatically starts counting down when the *Ignition shutdown timer* reaches 0 AND recorded events still remain to be uploaded to Evidence Library 4 Web (EL4 Web)

**Ignition shutdown timer**

The *Ignition shutdown timer* allows you to set how long the 4RE should wait before it automatically starts shutting down once the ignition is turned off. **0 through 60 minutes** are the available options, **5 minutes** is the default option.

With the *Ignition shutdown timer*, you can set the 4RE to start shutting down immediately when you turn off the vehicle's ignition (**0 minutes**) or you can set it to start shutting down after a delay. For example, if you set a delay value of **10 minutes** for the *Ignition shutdown timer*, as soon as you turn off the vehicle's ignition, the 4RE starts counting down from 10 minutes. The 4RE is still on and fully functional during the countdown time. When the countdown reaches 0, the 4RE starts shutting down.

**Note:** If your agency uses a wireless network to transfer video to EL4 Web and the 4RE contains recorded events that need to be uploaded, when the *Ignition shutdown timer* reaches 0, the *Wireless transfer shutdown timer* starts counting down.

If you turn the ignition back on during that 10 minute delay period, the countdown is stopped and the 4RE goes on functioning normally. There is no wait for the 4RE to power back on.

**Wireless transfer shutdown timer**

The *Wireless transfer shutdown timer* allows you to set how long the 4RE should wait before it fully shuts down if it is still wirelessly transferring video when the *Ignition shutdown timer* reaches 0. **0 through 60 minutes** are the available options, **30 minutes** is the default option.
If a vehicle is in range of your agency's wireless network and its 4RE contains recorded events that need to be uploaded to EL4 Web, the Wireless transfer shutdown timer starts when the Ignition shutdown timer has finished counting down.

While the Wireless transfer shutdown timer is counting down, the 4RE display screen is black and the cameras are off. No video is being captured. During this mode, some lights on the display control panel blink so you know the 4RE is still uploading video. Every part of the system is sleeping, except video upload. Because all resources are dedicated to uploading video, the upload is faster than it was prior to the Wireless transfer shutdown timer startup.

Wireless upload of recorded events takes as much time as needed, up to the value set for this shutdown timer. If the shutdown timer is set to 30 minutes, and the 4RE only needs 22 minutes to upload its video, the 4RE completely shuts down after it finishes uploading at 22 minutes. If the 4RE needs 48 minutes to upload all its pending recorded events, and the property is set to 30 minutes, the 4RE completely shuts down after 30 minutes when the timer has finished counting down. Any pending events still on the 4RE will be uploaded the next time the Ignition shutdown timer reaches 0 and the vehicle is in range of the agency’s wireless network.

If you restart the 4RE system while the Wireless transfer shutdown timer is counting down (by turning the ignition on or pressing the Power Up button), because the system is not fully shut down, it does not take as long to be fully functional as it would if the system were completely shut down.

Setting the 4RE Import Properties

Note: These instructions correspond to step 12 on the 4RE recommended workflow (page 271).

In Evidence Library Administrator (EL Administrator), the 4RE Import Settings allow you to indicate whether Evidence Library 4 Web (EL4 Web) should import recorded events from a 4RE USB thumb drive automatically or manually.

Note: The 4RE Import Settings only apply to recorded events imported from a 4RE DVR USB thumb drive. The 4RE Import Settings do NOT apply if your agency imports recorded events wirelessly from its fleet of 4RE DVRs.

If you choose to import automatically, when a 4RE USB thumb drive containing recorded events is connected to EL4 Web, EL4 Web automatically imports those events. The import
Chapter 8. Managing Devices

takes place in the background so you can work in other areas of EL4 Web while recorded events are importing.

---

**Important!** Automatic import requires that you have designated a storage location. For information on setting up storage locations, see Chapter 7. Managing Evidence Storage on page 213.

---

If you choose to import manually, you can set up how your agency should handle event categorization and officer assignment during import.

To set up the **Import Settings** for a 4RE configuration:

1. On the 4RE **Management Editor** dialog box, select the 4RE configuration whose USB thumb drive **Import Settings** you want to set, then click the plus sign (+) next to the configuration name.

   The configuration expands to show its five parts.

   ![Image of 4RE Management Editor]

2. Click **Import Settings**.

   The **Import Settings** appear.

   ![Image of Import Settings]

3. Select whether you want to import recorded events from a 4RE USB thumb drive automatically or manually.
4. If you want your agency to import events manually:
   a. Verify that you want to allow officers to categorize recorded events during the manual import process.
   b. If you want to require officers to categorize recorded events before they are imported, check the **Require all events to be categorized** checkbox.
      Checking this checkbox automatically checks the **Allow editing of the event category prior to import** checkbox.
      
      **Important!** When this option is selected, EL4 Web does not allow the import process to continue until the officer categorizes any uncategorized recorded events to be imported.

   c. Verify that you want to allow officers to assign or edit an officer name during the manual import process.
   d. If you want officers to have the option to delete a recorded event prior to import, check the **Allow events to be deleted prior to import by officer/user** checkbox.
      
      **Important!** An officer must also have the delete permission assigned to his user group in EL Administrator Security Management to delete events before import. For information on adding roles to user groups, see Chapter 9, Managing Security on page 351.

   e. If you want any unassigned recorded events to automatically be assigned to the officer logged into EL4 Web at import, check the **Automatically assign all unassigned events to the logged in user** checkbox.
      
      **Note:** EL4 Web only automatically assigns unassigned events to the logged-in officer when the officer has the correct permissions assigned in EL Administrator Security Management.

For information and instructions for manual recorded event import, see Manually Importing from USB-Connected Devices on page 34.

5. Click **Apply** on the bottom of the 4RE Management Editor, if applicable.

---

**Deployment**

Once you have set up or updated a 4RE configuration in Evidence Library Administrator (EL Administrator), you deploy it to a 4RE DVR. When 4RE software updates become available, you need to deploy those as well.

There are two ways to deploy a 4RE configuration (page 298) or software update (page 303):

- Manually using a USB thumb drive
- Automatically through your agency’s wireless network, if applicable

You can use the 4RE Management Operations dialog box to access the settings and dialog boxes you need to deploy a configuration or software update automatically or manually.
Chapter 8. Managing Devices

- On the System Settings screen, click Click to manage in-car video.
  For information on System Settings, see Setting Up System Settings on page 269.

The 4RE Management Operations dialog box opens.

![4RE Management Operations dialog box](image)

**Deploying a configuration**

You can deploy a 4RE configuration manually or automatically. You always deploy manually in the following two situations:

- First time a configuration is loaded on a 4RE DVR
- Your agency does NOT use a wireless network to connect to its fleet of 4RE DVRs

In all other situations, you deploy a 4RE configuration automatically through your agency's wireless network.

For instructions how to deploy a 4RE configuration manually, see Deploying a Configuration Manually below. For instructions how to deploy a 4RE configuration automatically, see Deploying a configuration automatically on page 302.

**Deploying a configuration manually**

*Note: These instructions correspond to step 15 on the 4RE recommended workflow (page 271).*

The first time you deploy a configuration to the 4RE DVR, you must deploy manually with a USB thumb drive. Even if your agency uses a wireless network, you must deploy the first 4RE configuration manually. Until you set up the 4RE DVR manually with the first configuration, no connection can be made between the 4RE and the Evidence Library 4 Web (EL4 Web) server.

If your agency does not use a wireless network to connect to its fleet of 4RE DVRs, you must manually deploy a 4RE configuration, whether it is the 4RE DVR's initial configuration or an update.

When you manually deploy a 4RE configuration, you use an empty thumb drive (minimum 512 MB), or a thumb drive that has been used only for deploying 4RE configuration files.
Important! If your agency uses thumb drives to transfer video to EL4 Web, you should use one thumb drive for importing recorded events from a 4RE and another thumb drive for configuring the 4RE. These two functions should not be done with the same thumb drive.

To deploy a 4RE configuration manually:

1. On the 4RE Management Operations dialog box, click Deploy configurations manually.

The USB Deployment Operations dialog box opens listing all the 4RE DVRs on the All Vehicles list.

2. Check the checkboxes next to the IDs of the 4RE DVRs (Vehicle) you want to deploy a 4RE configuration to, then click Deploy Configuration.

The Select Folder dialog box opens.
3. If you have not already done so, insert the USB thumb drive into the computer, navigate to and select the thumb drive, then click **Select Folder**.

![Select Folder](image)

**Important!** Make sure you select the thumb drive at the top level.

The **Configuration Deploy Completed** message box opens confirming that the 4RE configurations were successfully saved to the thumb drive.

![Configuration Deploy Completed](image)

4. Click **OK**.

5. Eject the thumb drive correctly for the operating system on the EL Administrator computer.

**Warning!** You must eject the thumb drive correctly for the operating system you have installed. Removing the USB thumb drive incorrectly can result in corruption of data or other unexpected results.

See Microsoft Windows help for instructions to safely remove a thumb drive for your operating system.

6. Load the 4RE configuration on the 4RE DVR using the thumb drive.

For instructions how to load the 4RE configuration on the 4RE DVR, see **Deploying a configuration to a 4RE DVR** on page 301.
Deploying a configuration to a 4RE DVR

The first time you deploy a configuration to a 4RE DVR, you must deploy manually with a USB thumb drive. Even if your agency uses a wireless network, until the first configuration is manually deployed, no connection can be made between the 4RE and the Evidence Library 4 Web (EL4 Web) server.

If your agency does not use a wireless network, you always deploy a configuration manually using a USB thumb drive.

After you have loaded an 4RE configuration on a USB thumb drive, you deploy it to the 4RE DVR.

To deploy a 4RE configuration to a 4RE DVR:

1. If needed, remove the USB thumb drive containing stored recorded events from the DVR. For instructions how to safely remove a USB thumb drive from a 4RE DVR, see Removing a USB thumb drive safely from a 4RE DVR on page 41.

   **Warning!** It is critical that you only remove a USB thumb drive from a 4RE DVR when it is safe to do so. Removing the USB thumb drive too early can result in loss of evidence or other unexpected results when data is imported from the USB thumb drive.

   **Note:** If your agency uses USB thumb drives to transfer video to EL4 Web from your 4RE DVRs, you should use one USB thumb drive for importing recorded events from a 4RE and another USB thumb drive for configuring the 4RE. These two functions should not be done with the same USB thumb drive.

2. Plug the USB thumb drive containing the 4RE configuration into the 4RE DVR.

   The **Select Configuration** screen appears on the 4RE display screen.

   ![Select Configuration Screen](image)

3. Select the configuration you want to deploy, then touch **Load**.

   **Tip:** Each configuration listed on the **Select Configuration** screen corresponds to a specific 4RE DVR. Select the configuration appropriate to the 4RE you are working on.
Chapter 8. Managing Devices

The **Supervisor Login** screen appears.

4. Enter your supervisor password, then touch **Login**.

The **It is now safe...** message box appears.

5. Touch **OK** and remove the USB thumb drive containing the 4RE configuration from the 4RE DVR.

**Note:** If a message appears on the 4RE display screen instructing you to reboot the 4RE, touch **OK**. Remove the configuration USB thumb drive, power the 4RE DVR off, wait 10 seconds, then power it back on.

6. If needed, replace the USB thumb drive containing recorded events in the 4RE DVR.

**Deploying a configuration automatically**

After the initial 4RE configuration has been manually deployed to the 4RE DVR, if your agency uses a wireless network to connect to its 4REs, you can set Evidence Library 4 Web (EL4 Web) to automatically deploy any changes made to a 4RE configuration. You set up automatic 4RE configuration deployment using the **Automatic Configuration Deployment Switch**.

The **Fleet Management Deployment Settings** dialog box allows you to enable the automatic deployment of 4RE configurations to 4RE DVRs using your agency’s wireless network. **Automatic Configuration Deployment** is disabled by default.
To enable automatic 4RE configuration deployment:

1. On the 4RE Management Operations dialog box, click **Edit**.

   The **Fleet Management Deployment Settings** dialog box opens.

   ![Dialog Box Image]

   2. Select the **Enable** option, then click **OK**.

   When the **Automatic Configuration Deployment** switch is enabled, if an updated configuration is available for a 4RE DVR, when the 4RE enters an agency wireless hotspot (or otherwise connects to the agency network), the updated configuration is deployed to the 4RE automatically. You do not have to do anything else to deploy the configuration.

   **Note:** You can enable or disable an individual 4RE DVR's ability to receive automatic configuration deployments when you add it to the **All Vehicles** list.

   For more information on adding a vehicle to the **All Vehicles** list, see Adding a new 4RE DVR to the All Vehicles list on page 275.

**Deploying a 4RE DVR software update**

You can deploy a 4RE DVR software update:

- Manually using a USB thumb drive on each individual 4RE DVR in your fleet
- Automatically using your wireless network

You deploy a 4RE software update using the same method that you normally use to deploy a 4RE configuration. If your agency does not have a wireless network, you deploy manually. If you do have a wireless network, you deploy the software update automatically.

**Deploying a 4RE DVR software update manually**

When you receive a 4RE DVR software update from WatchGuard, you can load it directly from the USB thumb drive to each individual 4RE in your fleet. If your agency does not use a wireless network to connect with its 4RE DVRs, this is the only way you can update them.

To manually update a 4RE DVR:

- Remove the USB thumb drive containing stored recorded events from the 4RE, plug the USB thumb drive containing the 4RE DVR software update into the 4RE, then follow the prompts on the display screen.
Chapter 8. Managing Devices

For instructions how to safely remove a USB thumb drive from a 4RE DVR, see Removing a USB thumb drive safely from a 4RE DVR on page 41.

**Warning!** It is critical that you only remove a USB thumb drive from a 4RE DVR when it is safe to do so. Removing the USB thumb drive too early can result in loss of evidence or other unexpected results when data is imported from the USB thumb drive.

Deploying a 4RE DVR software update automatically

If your agency uses a wireless network to connect to its 4RE DVRs, you can upload a 4RE DVR software update once to Evidence Library Administrator (EL Administrator) 4RE Management and let it deploy the software upgrade for you automatically.

**Important!** Before you upgrade the software on your 4RE DVRs, verify the current software version for each 4RE DVR. If the version you are upgrading from is more than one major release behind the upgrade version for any 4RE DVR (for example, current version 1.x to upgrade version 3.6.x), there may be other preparation steps you need to make before upgrading that 4RE DVR. You can find the current version of each of your 4RE DVRs in the 4RE Software Version column on the All Vehicles list (page 274).

WatchGuard recommends that you read the release notes for any major versions in between the current and upgrade versions to confirm whether any additional preparation is needed before upgrading. If you have questions about upgrading your 4RE DVRs, please contact WatchGuard Customer Service.

To upload the 4RE DVR software update to EL Administrator:

1. On the 4RE Management Operations dialog box, click Update 4RE software.
Deploying a 4RE DVR software update automatically

The **Import Device Software Upgrade Package** dialog box opens.

2. Click **Import**.

The **Select WatchGuard Upgrade Package** dialog box opens.

3. Navigate to the WatchGuard 4RE DVR software update package ZIP files, select the ZIP file that has the version number in the filename, then click **Open**.

The **Success** message box opens indicating that the 4RE software update package has been successfully uploaded to EL Administrator.

4. Click **OK**.
5. Open the **All Vehicles** list.

After a few minutes, the **Repository 4RE Software Version** field on the **All Vehicles** list updates to the version you uploaded. Once that happens, the 4RE DVR software update is ready to be automatically deployed to your fleet of 4RE DVRs. As your 4REs connect to your agency’s network (wirelessly or wired), and after any video is uploaded from the 4RE to EL4 Web, EL Administrator automatically pushes out the software update to the 4RE DVR.

### Setting your In-Car Supervisor Password

**Important!** You must have supervisor permissions assigned to you to set up or change an **In-Car Supervisor Password** in Evidence Library Administrator (EL Administrator).

The **In-Car Supervisor Password** is the password that each 4RE DVR Supervisor uses on the 4RE DVR. Each 4RE DVR Supervisor has his or her own password.

**Note:** For information about user roles and other security issues, see Security Management (page 351) or your system administrator.

To set up or change your **In-Car Supervisor Password**:

1. From the **Tools** menu in Evidence Library Administrator (EL Administrator), select **My Account**, then Change In-Car Supervisor password.

   ![In-Car Supervisor Password dialog box](image)

   The **In-Car Supervisor Password** dialog box opens.

2. Enter your **New Password** twice, then click **Save**.
Configuring the VISTA Camera

The **VISTA Management** feature in Evidence Library Administrator (EL Administrator) helps you manage your set of VISTA Body Cameras. You use **VISTA Management** to set up VISTA configurations. VISTA configurations are then assigned to the VISTA cameras when they are checked out from Evidence Library 4 Web (EL4 Web). For more information about checking out VISTA Body Cameras, see *Chapter 6. Checking Out VISTA Cameras* on page 185.

The major sections of the **VISTA Management** feature are:

- Setting default officer preferences (*page 308*)
- Creating and setting up a VISTA configuration (*page 310*)
- Upgrading VISTA firmware (*page 325*)

WatchGuard follows a basic workflow when setting up an agency's set of VISTA cameras. This WatchGuard workflow is one possible way of configuring the VISTA Body Camera and does not necessarily cover all possible **VISTA Management** situations. To see the steps in the WatchGuard workflow, see *Recommended workflow for configuring a VISTA camera* on page 308.

**Accessing VISTA Management**

To access the **VISTA Management** feature:

- On the **System Settings** screen, click **Click to manage wearable camera**.
  
  For information on **System Settings**, see *Setting Up System Settings* on page 269.

The **VISTA Management Editor** dialog box opens showing the **New Officer Preferences** and **Other Options**.

![VISTA Management Editor](image-url)
Recommended workflow for configuring a VISTA camera

**Note:** The workflow in this section is basic; it does not cover all possible VISTA Management situations. This workflow gives an example of how and when it seems most logical to perform a task in VISTA Management. It is intended to serve as a guide only.

The following steps make up a recommended workflow for configuring your set of VISTA Body Cameras:

1. Access Evidence Library Administrator. ([page 25](#))
2. If not already done, set up your agency name and other system settings. ([page 269](#))
3. Access VISTA Management. ([page 307](#))
4. Set up the VISTA default officer preferences. (below)
5. Create initial default configurations. ([page 311](#))
6. Assign enrollments (user groups) to each configuration. ([page 312](#))
7. If not already done, set up system event tags. ([page 331](#))
8. Set the recording properties for each configuration. ([page 314](#))
9. Set the device properties for each configuration. ([page 319](#))
10. Set the import settings for each configuration. ([page 321](#))
11. Set the network settings for each configuration. ([page 323](#))
12. Confirm the configuration settings, save each configuration, then close VISTA Management.

The VISTA configurations are ready to be assigned to the VISTA cameras when they are checked out from Evidence Library 4 Web (EL4 Web). For information about checking out VISTA Body Cameras, see Chapter 6. Checking Out VISTA Cameras on page 185.

### Setting the VISTA New Officer Preferences

**Note:** These instructions correspond to step 4 on the VISTA recommended workflow (above).

With Evidence Library Administrator (EL Administrator), you can set the default behavior for the alerts and notifications on your VISTA Body Cameras in New Officer Preferences. The defaults you set in New Officer Preferences are pushed to each new VISTA when it is first checked out from Evidence Library 4 Web (EL4 Web).

**Note:** Officers can individually set these preferences when they check out VISTA cameras. Once officers set their preferences, their preferences override the default preferences at checkout. For more information, see Chapter 6. Checking Out VISTA Cameras on page 185.
The default officer preferences allow you to set:

- Brightness level of the VISTA LEDs
- Type of alert notification (audio, vibration, or both)
- Audio level of alerts, if applicable

To set the default **New Officer Preferences**:

1. Access **VISTA Management**.
   
   For instructions how to access **VISTA Management**, see *Accessing VISTA Management* on page 307.

   The **VISTA Management Editor** dialog box opens showing the **New Officer Preferences**.

2. Set whether VISTA should light its LEDs, and if so, how bright they should be.
3. Verify that you want VISTA to automatically dim its LEDs between 8 PM and 8 AM.
4. Set whether VISTA should alert the officer as needed, and if so, what form those alerts should take.
5. Set whether VISTA should sound a tone to alert the officer as needed, and if so, at what volume the tone should sound.
6. Click **Save**.

**Enabling VISTA Other Options**

Below the default officer preferences, you can enable two **Other Options** for your set of VISTA cameras:

- **Enable VISTA Camera For ELX Viewer**: When enabled, allows video from a VISTA camera to be viewable on the Evidence Library Express (ELX) Viewer
  
  The **Enable VISTA Camera For ELX Viewer** checkbox is clear by default.

- **Enable Automatic Configuration Deployment**: When enabled, allows a new VISTA configuration to be applied to cameras automatically when they are docked
  
  The **Enable Automatic Configuration Deployment** checkbox is checked by default.
Chapter 8. Managing Devices

VISTA configurations

To use your WatchGuard VISTA Body Camera with Evidence Library 4 Web (EL4 Web), you must create a configuration for it using the Evidence Library Administrator (EL Administrator) VISTA configuration feature.

In EL4 Web, a VISTA configuration is a group of settings that you apply to a VISTA Body Camera. When assigned to a VISTA camera, the VISTA configuration automatically sets up the camera so it meets the specific needs of its user. You can create multiple configurations, each corresponding to a use of VISTA in your agency; for example, you can set up different configurations for patrol, bike patrol, or drug intervention officers depending on their needs.

VISTA configurations are listed on the VISTA Management Editor dialog box.

- Click Configurations in the left pane of the VISTA Management Editor dialog box to open the list of existing VISTA configurations.

From the list of VISTA configurations, you can add new configurations or edit existing configurations.

You can add a new VISTA configuration two ways:

- Create a new configuration that uses system default settings (page 311)
- Copy an existing configuration and give it a new name (page 312)

Once you add a VISTA configuration, you need to set it up. There are five main VISTA configuration areas to set up:

- Assigned Enrollments (page 312)
- Recording Properties (page 314)
- Device Properties (page 319)
- Import Settings (page 321)
- Network Settings (page 323)

To access these configuration areas:

- Click the plus sign (+) next to the configuration name in the left pane of the VISTA Management Editor dialog box.
Creating a new VISTA configuration

**Note:** These instructions correspond to step 5 on the VISTA recommended workflow (page 308).

To create a new VISTA configuration with system default settings:

1. Click **Configurations** in the left pane of the **VISTA Management Editor** dialog box. The list of VISTA configurations appears.

2. Click **New**.

   The **Create New Configuration** dialog box opens.

3. Enter a name for the new configuration in the **Name** field, then click **Create**.

   The new VISTA configuration with system default settings is added to the list of your agency VISTA configurations.
Chapter 8. Managing Devices

Copying an existing VISTA configuration

To create a new configuration from a copy of an existing configuration:

1. Click Configurations in the left pane of the VISTA Management Editor dialog box.
   The list of VISTA configurations appears.

2. Select the configuration you want to copy, click Edit, then select Create a copy of.
   The Create New Configuration from Copy dialog box opens.

3. Enter a name for the copy of the configuration in the Name field, then click Create.
   The new configuration copied from an existing configuration is added to the list of your agency VISTA configurations.

Assigning a user group to a VISTA configuration

Note: These instructions correspond to step 6 on the VISTA recommended workflow (page 308).

In Evidence Library 4 Web (EL4 Web), users are assigned to a VISTA configuration through user groups. User groups are set up by your system administrator according to your agency’s network security policies in conjunction with the features in Evidence Library Administrator (EL Administrator) Security Management.
Assigning a user group to a VISTA configuration

For information on EL Administrator Security Management, see Chapter 9. Managing Security on page 351. For information about your agency's user groups, contact your system administrator.

The Assigned Enrollments list shows the user groups assigned to a VISTA configuration. Using the Assigned Enrollments list, you can assign additional user groups to the selected VISTA configuration, or unassign user groups from the configuration.

Tip: Click the plus sign (+) next to an assigned user group to see the list of individuals in the user group. The individual names under each of the user groups assigned to a VISTA configuration together make up the list of names an officer sees on EL4 Web when he checks out a VISTA camera.

A user group can be assigned to more than one VISTA configuration. To assign a user group to a VISTA configuration:

1. On the VISTA Management Editor dialog box, click the plus sign (+) next to the name of the VISTA configuration you want to assign a user group to.

   The configuration expands to show its five parts.

2. Click Assigned Enrollments.

   The Assigned Enrollments list appears.

3. In the unassigned section, select the user group you want to assign to the configuration, then click Assign.

   The user group is assigned to its new VISTA configuration: the user group name moves from the unassigned section to the assigned section on the Assigned Enrollments list.

4. Click Save on the bottom of the VISTA Management Editor dialog box.
Chapter 8. Managing Devices

Setting the VISTA Recording Properties

**Note:** These instructions correspond to step 8 on the VISTA recommended workflow (page 308).

In Evidence Library Administrator (EL Administrator), the **Recording Properties** for the VISTA Body Camera allow you to set:

- Video quality
  
  For information on the VISTA video quality options, see *VISTA video quality settings* on page 318.

- Additional record time (**Pre-Event Time**)
  
  When **Pre-Event Time** is enabled, VISTA continuously records then saves video from a period of time before a recorded-event start. Pre-event video is added before the start of the recorded event (page 319).

- Whether VISTA continuously captures video for the Record-After-the-Fact® (RATF) feature

- Whether VISTA WiFi can stop its own event during a group event

  **Note:** Only VISTA WiFi or VISTA XLT can participate in group events.

- Whether you must press the VISTA **Record Start/Stop** button twice to stop a recorded event

- Whether audio is recorded all the time instead of only during events

- Whether you can mute VISTA audio

- Whether audio is completely disabled for all VISTA recording

- Periodic recording reminder

- Auto-start record settings and record-start delay

- Whether VISTA WiFi or VISTA XLT participates as a recording group member for event starts and stops

  **Note:** Only VISTA WiFi or VISTA XLT can be a member of a recording group.

- Maximum event size and time

- Configuration event tags
  
  For information about setting up system event tags, see *Setting Up Event Tags* on page 331.
To set up the **Recording Properties** for a VISTA configuration:

1. On the **VISTA Management Editor** dialog box, click the plus sign (+) next to the name of the VISTA configuration whose **Recording Properties** you want to set.

   The configuration expands to show its five parts.

2. Click **Recording Properties**.

   The **Recording Properties** settings appear.

3. Set the **Recording Settings**.

   a. Select the **Video Quality** and **Frame Rate** for the VISTA camera.

   For information about VISTA video quality settings, see **VISTA video quality settings** on page 318.

   **Important!** For the best experience, WatchGuard recommends that you keep the default frame rate of 30 frames/second.
b. Select the amount of pre-event video you want automatically saved as part of the event.

c. If you want VISTA to continuously capture and save video that can be used to create RATF events, check the **Enable Record-After-the-Fact** checkbox.

d. If you want VISTA to be able to stop its own event during a group event, check the **Allow manual stop** checkbox.

e. If you want to require a second button press (**Record Start/Stop** button) to confirm an event stop on VISTA, check the **Stop recording confirmation** checkbox.

f. If you want VISTA to record audio whenever the camera is capturing video, check the **Force microphone on all the time** checkbox.

g. If you want to be able to mute VISTA audio, check the **Allow muting** checkbox.

h. If you want to disable audio for all VISTA recording, check the **Disable audio** checkbox.

---

**Note:** Checking the **Disable audio** checkbox deactivates the **Force microphone on** and **Allow muting** checkboxes. When **Disable audio** is selected, these audio checkboxes no longer apply.

---

4. If you want to enable the VISTA camera to periodically remind the officer that it is still capturing a recorded event, in the **Recording Reminder Alerts** section, select the **Alert every** option, then enter the interval between reminders.

5. If you are using the VISTA Vehicle Kit, set up the **Auto-Start Record** settings:

---

**Important!** The **Auto-Start Record** settings only apply when the associated inputs are connected to the Smart Power Switch. For more information, see the VISTA Vehicle Kit Installation and User Guide.

---

a. Mark the input settings you want to use to automatically start a recorded event on VISTA WiFi or VISTA XLT.

b. Mark the settings where you want to set a record-start delay.

---

**Warning!** Typically, VISTA WiFi and VISTA XLT do not record video or audio during the delay period. For more information, see the VISTA Vehicle Kit Installation and User Guide.

---

c. If you choose to use a delay, set the amount of time the camera should delay before starting a recorded event.

---

**Note:** The amount of time you set for a record-start delay applies to all the settings that use a delay. You cannot set one amount of time for one record-start setting and another amount of time for another setting.
6. Set up the **Recording Groups** section:

   **Note:** The **Recording Groups** section only applies to VISTA WiFi and VISTA XLT.

   a. If you want VISTA WiFi or VISTA XLT to start a recorded event when it is informed by another group member (VISTA or 4RE) that the other group member has started an event, check the **Group member start** checkbox.

   b. If you want VISTA WiFi or VISTA XLT to stop a recorded event when it is informed by another group member (4RE) that the other group member has stopped an event, check the **Group member stop** checkbox.

   **Note:** The **Group member stop** setting only applies when there is a 4RE and at least one VISTA WiFi or VISTA XLT in the recording group.

7. If you want to split large events on the VISTA camera, in the **Maximum Recorded Event Size** section, select the maximum size a recorded event should be.

8. If you want to enable VISTA to automatically stop a recorded event when it reaches a specified duration, in the **Maximum Recorded Event Time** section, select the **Stop after** option, then enter the maximum event length.

9. Assign event tags to the VISTA configuration using the **Assigned Event Tags** section.

   **Important!** You must check the checkbox for each event tag that you want to include in the VISTA configuration.

   **!** Only the **EventCategory** tag appears on the VISTA camera display, if it is assigned to the configuration; other assigned event tags can be answered at import or in the event details after import.

   For information about setting up event tags, see Setting Up Event Tags on page 331.

10. Click **Save** on the bottom of the **VISTA Management Editor** dialog box.
Chapter 8. Managing Devices

**VISTA video quality settings**

The quality of the video that VISTA saves depends on the video quality and frame rate you select in the VISTA Recording Properties. The higher the video quality you select, the better the quality of the resulting video and the larger the storage space need.

*Note: For information on the 4RE DVR video quality settings, see 4RE video quality settings on page 287.*

The following table lists VISTA's supported video quality options with each one's resolution and storage space needs:

<table>
<thead>
<tr>
<th>Video quality</th>
<th>Video resolution</th>
<th>Frames per second</th>
<th>Storage space (GB per hour)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HD high resolution</td>
<td>1280 x 720</td>
<td>30</td>
<td>2.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>1.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>0.73</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>0.37</td>
</tr>
<tr>
<td>HD medium resolution</td>
<td>1280 x 720</td>
<td>30</td>
<td>1.76</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>0.59</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>0.29</td>
</tr>
<tr>
<td>HD low resolution</td>
<td>1280 x 720</td>
<td>30</td>
<td>1.32</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>0.46</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>0.22</td>
</tr>
<tr>
<td>SD high resolution</td>
<td>864 x 480</td>
<td>30</td>
<td>0.88</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>0.29</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>0.15</td>
</tr>
<tr>
<td>SD medium resolution</td>
<td>864 x 480</td>
<td>30</td>
<td>0.66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>0.22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>0.11</td>
</tr>
<tr>
<td>SD low resolution</td>
<td>864 x 480</td>
<td>30</td>
<td>0.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>0.22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>0.15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>0.07</td>
</tr>
</tbody>
</table>
**VISTA pre-event**

The pre-event feature enables a device to continuously record then save video for a period of time before a recorded-event start. The pre-event video is added before the start of the recorded event.

For example, you start a recorded event, manually or automatically, at 2:15 pm. You stop the event, manually or automatically, at 2:35 pm. After adding in a configured pre-event video time of 1 minute, the recorded event includes video recorded from 2:14 pm to 2:35 pm.

VISTA pre-event video time can be **None** up to **2 minutes**.

**Setting the VISTA Device Properties**

*Note: These instructions correspond to step 9 on the VISTA recommended workflow (page 308).*

In Evidence Library Administrator (EL Administrator), the VISTA **Device Properties** allow you to set:

- Time zone and locale where your agency is located
- VISTA power-saving settings
  - Sleep
  - Automatic power off
- Timers to limit VISTA upload and charge time in the vehicle

*Note: These timers are only applicable if you use a VISTA WiFi base with your VISTA Body Cameras in the vehicle.*

- GPS enabled or disabled

*Note: GPS is only available on VISTA WiFi or VISTA XLT cameras.*
To set up the **Device Properties** for a VISTA configuration:

1. On the **VISTA Management Editor** dialog box, click the plus sign (+) next to the name of the VISTA configuration whose **Device Properties** you want to set.
   
   The configuration expands to show its five parts.

2. Click **Device Properties**.
   
   The **Device Properties** settings appear.

3. Select the **Time Zone** where the VISTA cameras using this configuration operate.

4. Select the **Locale** (language and location) applicable to your agency.

   **Note:** The **Locale** value defaults to the language and location value set for your EL4 Web server.
5. Set the **Sleep Mode** settings.
   a. Verify that you want your VISTA cameras to sleep ONLY after a period of time with no camera motion.
   b. Enter the amount of time that must elapse with no camera motion before VISTA sleeps.

6. Set the **Automatic Off** settings.
   a. Verify that you want your VISTA cameras to automatically turn off ONLY after a period of time with no camera motion.
   b. Enter the amount of time that must elapse with no camera motion before VISTA automatically turns off.

7. Set the **Power Behavior Settings**.
   a. Enter the number of minutes that VISTA is allowed to upload video wirelessly from the vehicle after the ignition is turned off in the Wireless shutdown timer.
   b. Enter the number of minutes that VISTA is allowed to charge its battery in the vehicle after the ignition is turned off in the Maximum battery charge timer.
   c. If you want GPS enabled on your VISTA WiFi or VISTA XLT cameras, check the **Enable GPS** checkbox.

8. Click **Save** on the bottom of the **VISTA Management Editor** dialog box.

---

**Setting the VISTA Import Settings**

**Note:** These instructions correspond to step 10 on the VISTA recommended workflow (page 308).

In Evidence Library Administrator (EL Administrator), the **VISTA Import Settings** allow you to indicate whether Evidence Library 4 Web (EL4 Web) should import recorded events from a USB-connected VISTA Body Camera automatically or manually.

**Note:** The **VISTA Import Settings** only apply to recorded events imported from a USB-connected VISTA camera. The **VISTA Import Settings** do NOT apply if your agency imports recorded events from its set of VISTA cameras using the WatchGuard VISTA Transfer Station.

If you choose to import automatically, when a USB-connected VISTA camera containing recorded events is connected to EL4 Web, EL4 Web automatically imports those events. The import takes place in the background so you can work in other areas of EL4 Web while recorded events are importing.

**Important!** Automatic import requires that you have designated a storage location. For more information about setting up storage locations in EL4 Web, see Chapter 7. Managing Evidence Storage on page 213.

If you choose to import manually, you can set up how your agency should handle event categorization and officer assignment during import.
Chapter 8. Managing Devices

To set up the **Import Settings** for a VISTA configuration:

1. On the **VISTA Management Editor** dialog box, click the plus sign (+) next to the name of the VISTA configuration whose **Import Settings** you want to set.

   The configuration expands to show its four parts.

   ![VISTA Management Editor](image)

2. Click **Import Settings**.

   The **Import Settings** appear.

   ![Import Settings](image)

3. Select whether you want to import recorded events from a USB-connected VISTA camera automatically or manually.

4. If you want your agency to import events manually:
   a. Verify that you want to allow officers to categorize recorded events during the manual import process.
   b. If you want to require officers to categorize recorded events before they are imported, check the **Require all events to be categorized** checkbox.

      Checking this checkbox automatically checks the **Allow editing of the event category prior to import** checkbox.

      **Important!** When this option is selected, **EL4 Web does not allow the import process to continue until the officer categorizes any uncategorized recorded events to be imported.**

   c. Verify that you want to allow officers to assign or edit an officer name during the manual import process.
   d. If you want officers to have the option to delete a recorded event prior to import, check the **Allow events to be deleted prior to import by officer/user** checkbox.
Important! An officer must also have the delete permission assigned to his user group in EL Administrator Security Management to delete events before import. For more information about security management in EL Administrator, see Chapter 9. Managing Security on page 351.

e. If you want any unassigned recorded events to automatically be assigned to the officer logged into EL4 Web at import, check the **Automatically assign all unassigned events to the logged in user** checkbox.

**Note:** EL4 Web only automatically assigns unassigned events to the logged-in officer when the officer has the correct permissions assigned in EL Administrator Security Management.

For information and instructions for manual recorded event import, see *Manually Importing from USB-Connected Devices* on page 34.

5. Click **Save** on the bottom of the **VISTA Management Editor**, if applicable.

### Setting the VISTA Network Settings

**Note:** These instructions correspond to step 11 on the VISTA recommended workflow (page 308).

In Evidence Library Administrator (EL Administrator), the VISTA **Network Settings** allow you to set:

- Whether you want VISTA WiFi or VISTA XLT to function as a hotspot for the VISTA SmartConnect smartphone application, and if you do, whether snapshots are allowed on the smartphone

  For instructions how to use SmartConnect, see the *VISTA HD Wearable Camera User Guide*.

**Note:** Only VISTA WiFi and VISTA XLT can connect to the smartphone app.

**Warning!** When the **Allow Snapshots** option is enabled, you can save snapshots from the VISTA SmartConnect app to the smartphone's photo gallery. This potentially makes the phone part of the chain of evidence.

- Whether you want VISTA to wirelessly upload directly from the vehicle to Evidence Library 4 Web (EL4 Web), and if you do, the IP address of the EL4 Web wireless upload server
Chapter 8. Managing Devices

**Note:** VISTA wireless upload from the vehicle is only possible if you use a VISTA WiFi base with your VISTA Body Cameras in the vehicle.

To set up the **Network Settings** for a VISTA configuration:

1. On the **VISTA Management Editor** dialog box, click the plus sign (+) next to the name of the VISTA configuration whose **Network Settings** you want to set. The configuration expands to show its five parts.

2. Click **Network Settings**.

   The **Network Settings** appear.

3. Set the **Integration with VISTA SmartConnect** settings.
   a. If you want to allow VISTA WiFi or VISTA XLT to connect with the VISTA SmartConnect smartphone app, check the **VISTA SmartConnect Enabled** checkbox.
   b. If you want to allow users to capture snapshots of video from the VISTA SmartConnect app and save them to the smartphone’s generic photo gallery, check the **Allow Snapshots** checkbox.

   **Warning!** When the **Allow Snapshots** option is enabled, you can save snapshots from the VISTA SmartConnect app to the smartphone’s photo gallery. This potentially makes the phone part of the chain of evidence.
4. Set the **Mobile Network Settings**.
   a. If you want VISTA to wirelessly upload video from the WiFi base in the vehicle directly to EL4 Web, select **Evidence Library** from the **Event Transfer Destination** drop-down list.
   
   The **Server IP Address** field appears.

   ![Server IP Address field](image)

   b. Enter the **Server IP Address** for the EL4 Web wireless upload server.

5. Click **Save** on the bottom of the **VISTA Management Editor** dialog box.

### Deploying a VISTA firmware update

You can deploy a firmware update to your agency's VISTA Body Cameras:

- Automatically, to any camera as it connects to Evidence Library 4 Web (EL4 Web)
- Manually, to one USB-connected camera at a time, using the Evidence Library Transfer Agent

### Deploying a VISTA firmware upgrade automatically

You can deploy a firmware upgrade to your agency's VISTA Body Cameras automatically when they connect to Evidence Library 4 Web (EL4 Web).

---

**Note:** EL4 Web only automatically upgrades VISTA firmware; it does NOT automatically downgrade. If you need to downgrade VISTA's firmware version, you must manually apply the earlier firmware version to the camera. For instructions how to manually update VISTA's firmware, see Deploying a VISTA firmware update manually on page 326.

---

For the system to deploy an upgrade automatically, you must first upload the VISTA firmware upgrade to Evidence Library Administrator (EL Administrator) VISTA Management. Then EL4 Web can deploy the firmware upgrade for you automatically as each camera connects to it.

To upload the VISTA firmware upgrade to EL Administrator:

1. Click **Update Device Firmware** on the **VISTA Management Editor**.
Chapter 8. Managing Devices

The **Import Device Software Upgrade Package** dialog box opens.

![Import Device Software Upgrade Package Dialog Box]

2. Click **Import**.

   The **Select WatchGuard Upgrade Package** dialog box opens.

3. Navigate to the WatchGuard VISTA firmware update package TAR files, select the TAR file that has the correct version number in the filename, then click **Open**.

![Select WatchGuard Upgrade Package Dialog Box]

   The **Success** message box opens indicating that the VISTA firmware update package has been successfully uploaded to EL Administrator.

![Success Message Box]

4. Click **OK**.

   The VISTA firmware update you uploaded to EL Administrator will deploy automatically to each VISTA Body Camera, if needed, when the camera next connects to EL4 Web.

**Deploying a VISTA firmware update manually**

If you need to manually deploy a firmware update to one VISTA camera, you can use the Evidence Library Transfer Agent to upload the new firmware package to a USB-connected VISTA camera.

The Evidence Library Transfer Agent is the piece of Evidence Library 4 Web (EL4 Web) that runs on your local computer. You can access it from the Windows notification area (system tray). For more information about the Transfer Agent, see *Evidence Library Transfer Agent* on page 26.
To manually deploy a VISTA firmware update:

1. Right-click the **Evidence Library Transfer Agent** icon in the system tray, then select **Show Window**.

   ![Show Window](image)

   The Evidence Library Transfer Agent opens.

2. Select **VISTA Actions** from the **File** menu.

   ![VISTA Actions](image)

   The **VISTA Actions** dialog box opens.

3. Make sure the **Update Firmware** option is selected in the **Choose Action** field, then select the VISTA camera you want to upload firmware to from the **Choose Device** field.

4. Click **Browse**.
Chapter 8. Managing Devices

5. Navigate to the location of the VISTA firmware update files.

![Image showing the location of VISTA firmware update files]

6. Select the TAR file that has the applicable version number in the file name, then click **Open**.

   The location of the TAR file is filled in the **Browse Folder Location** field on the **VISTA Actions** dialog box.

7. Click **Update**.

   The firmware uploads to the VISTA camera, and the camera is ejected from EL4 Web.

   The **next time** you dock the camera, the firmware is updated on the camera.

---

**Warning!** **DO NOT REMOVE VISTA from the dock while its firmware is updating.**

Removing VISTA from the dock during the firmware update can cause the camera to completely stop functioning.
Requesting a VISTA state capture

If you need to capture the state of a VISTA camera for troubleshooting purposes, you can use the Evidence Library Transfer Agent to take the state capture from a USB-connected VISTA camera.

The Evidence Library Transfer Agent is the piece of Evidence Library 4 Web (EL4 Web) that runs on your local computer. You can access it from the Windows notification area (system tray). For more information about the Transfer Agent, see Evidence Library Transfer Agent on page 26.

To take a VISTA state capture:

1. Right-click the Evidence Library Transfer Agent icon in the system tray, then select Show Window.

The Evidence Library Transfer Agent opens.

2. Select VISTA Actions from the File menu.

The VISTA Actions dialog box opens.
Chapter 8. Managing Devices

3. Click the **Choose Action** field and select **Request State Capture**.

![Choose Action Field](image)

4. If you have multiple USB-connected VISTA Body Cameras, click **Choose Device** and select the device whose state you want to capture.

5. Click **Request**.

   The state capture request is sent to the VISTA camera, the camera is ejected from EL4 Web, and the **State Capture Requested** dialog box opens.

![State Capture Requested Dialog](image)

6. Click **Close**.

   The **next time** you dock the camera, the state capture is uploaded to the EL4 Web data folder.
Setting Up Event Tags

Note: These instructions correspond to step 9 on the 4RE recommended workflow (page 271) and step 7 on the VISTA recommended workflow (page 308).

Event tags are questions or statements that the system prompts officers to answer after they stop a recorded event.

- **On the 4RE**: Officers are prompted to give a response for each event tag when they press the 4RE's Stop button
- **On VISTA**: Officers are prompted to give a response to the EventCategory event tag after they press the Record Start/Stop button to stop a recorded event

Only the EventCategory tag appears on the VISTA camera, but you can assign secondary tags to VISTA to be answered at or after import.

Note: Event tag answers can be added or edited from two locations in EL4 Web: the import preview dialog box at manual import and the event details page after an event is imported. For information about editing event tag answers at import, see Using the Import Events dialog box on page 36. For information about editing event tag answers on the event details page, see Viewing and Editing Event Details on page 91.

In Evidence Library 4 Web (EL4 Web), you set up all your event tags, for both 4RE and VISTA, in the same Evidence Library Administrator (EL Administrator) location, the Event Tags Editor.

![Event Tags Editor](image)

You can set up as many tags as your agency needs, but you can only assign a maximum of six event tags to a configuration. You assign event tags to a configuration in Recording Properties for both 4RE and VISTA.

The system provides the EventCategory event tag (page 334). The event category is used to classify a recorded event, for example, as a citation or a drug event. The category tag is a drop-down list tag type. Its list of answers consists of event categories.
Secondary event tags (page 337) can identify anything else (other than the category) that your agency determines needs to be documented about a recorded event, for example, the gender or description of the suspect. Secondary tags can be either a drop-down list tag type or a short text answer tag type.

When you set up event tags, you also identify:

- Event categories that are considered critical (below)
- Event tags that require an answer (page 333)
- Event tag answers that can be retired (page 333)

Creating secondary event tags

In EL Administrator, you can set up secondary event tags (page 337) in two forms:

- Drop-down selection list
- Short text answer

For either form, you can use a predefined event tag template or create a custom event tag.

When you select an event tag from the list of predefined event tag templates, the event tag and its attributes are added to your agency list of event tags, fully defined. You can edit the predefined event tag if you want to, but you do not have to edit it for the event tag to function normally in the system.

For a custom event tag, you define the event tag prompt and any applicable answers from scratch.

Marking an answer Critical

When you set up a drop-down list event tag, you can designate any of the answers on the selection list as Critical. Typically, agencies only apply the critical designation to certain answers (categories) for the EventCategory event tag.

To mark an event tag answer as Critical:

- Check the Critical checkbox next to the 4RE and VISTA answers you want to designate as Critical.

**Important!** The Critical checkbox applies to both the 4RE and VISTA answers in the row. You cannot make an answer critical on one device only. It always applies to both devices.

On the 4RE

The front camera connected to the 4RE can be configured for two camera streams, each set up with a different video quality.

When an officer selects a category designated critical for a recorded event, the event is saved using the Critical Video Quality. Typically events tagged with a critical category are saved to the database with higher video quality.

Events tagged with a critical category upload first during import.
For more information about setting up different video qualities for the 4RE DVR camera streams, see Setting the 4RE Recording Properties on page 284.

**On VISTA**

Events tagged with a critical category upload first during import.

**Marking an answer Retired**

If you do not want to include an answer in the drop-down selection list for a device, you can designate the answer as Retired. A retired answer does not display as a selection option on the device when an officer stops a recorded event.

**Note:** You retire an answer rather than delete it because the answer may have been previously used to tag a recorded event.

To mark an event tag answer as Retired:

- Check the Retired checkbox for the appropriate device next to the display answer you want to retire, on the drop-down list Event Tag Editor.

**Making an event tag required**

When you make an event tag required, the event tag prompt remains on the device display until the officer enters an answer.

A non-required tag prompt remains on the device display for an amount of time you specify, then it disappears. The officer does not need to enter an answer before the prompt disappears.

To make an event tag required:

- Select the Require event tag answer option in the Display Settings section of the Event Tag Editor.

**Note:** The event tag prompt is overridden if the officer starts another recorded event.

**On the 4RE**

You can make any event tags required. The 4RE will show each tag on the display, one at a time, waiting on an answer for any required tags before moving to the next one.

**On VISTA**

You can only make the EventCategory tag required. (EventCategory is the only tag that can appear on the VISTA display.) By default, the Event Category tag is not required.
Setting up the EventCategory event tag

The system-provided EventCategory event tag is used to classify a recorded event. This event tag prompts officers to categorize events using a list of agency-determined categories, for example, warning, citation, injury, drugs.

The event category is user for:

- Searching for evidence on the Events tab (page 52)
- Applying retention rules to events stored in the database (page 259)

Typically, some EventCategory classifications are kept longer than others.

---

**Important!** A recorded event could be improperly purged or archived if an officer sets an event category value incorrectly. If you have the correct permissions, you can change the value of a recorded event’s EventCategory tag on the event details page (page 92).

---

- Determining whether the 4RE event video is saved at the critical video quality (page 332)

To set up the EventCategory event tag:

1. At the top of either the 4RE Management Editor or VISTA Management Editor dialog box, click All Event Tags.

   The Global Event Tag Definitions dialog box opens.

2. Verify that the EventCategory event tag is selected, then click Edit Tag.
The **Editing Event Tag** dialog box opens showing the attributes for the **EventCategory** event tag.

![Editing Event Tag Dialog Box](image)

3. If needed, edit existing categories on the answer lists.
   a. Highlight the **Display Answer** you want to edit, then enter your changes.
   b. Press **Enter**.

4. If needed, add new categories to the answer lists.
   a. Click **Add**.
      The **Create Dropdown Answer for Tag** dialog box opens.
   b. Enter the **Display Answer** for both **4RE** and **VISTA**.

   ![Create Dropdown Answer for Tag](image)

   **Note:** The two display answers do not have to be identical. **VISTA** and **VISTA WiFi** only have 8 characters available in their display. If a category has more than 8 characters, the category scrolls across the display.

   c. If you want the new category to be designated as critical, check the **Classify answer as critical** checkbox then click **OK**.
Chapter 8. Managing Devices

The new category is added to the bottom of the lists of Display Answers.

d. If you do not want to display the new category on one of the devices, check the Retired checkbox for the appropriate device.

5. If needed, adjust the Display Order of the categories for each device.
   a. In the appropriate Display Order section, select the category whose place in the order you want to change.
   b. Use the up and down arrows next to the Display Order section to move the selected category up or down in the list.

6. Verify that you want to require an officer to categorize recorded events on 4RE.

7. Verify that you want to require an officer to categorize recorded events on VISTA.

   Tip: If you do not want to require categorization, select the Dismiss event tag prompt after option and enter the number of seconds that the EventCategory tag should remain on the VISTA display before it disappears automatically.

8. Click OK.
Setting up secondary event tags

If your agency wants to document more than an event category about each recorded event, you set up secondary event tags to document these other attributes.

Secondary event tags can be set up in two forms:

- Drop-down selection list
- Short text answer

The form you select depends on the kind of information you want to document about the recorded event.

Important! Only the EventCategory tag appears on the VISTA camera, but you can assign secondary tags to VISTA to be answered at import or from event details after import. For information about editing secondary tags at import, see Secondary event tags on page 39. For information about editing secondary tags on the event details page, see Basic event details section on page 92.

Drop-down selection list form

A drop-down selection list event tag prompts the officer to select an answer from a list of options. When you set up a drop-down list event tag, you enter the question (prompt) and all the answers that you want to appear on the list for the officer. Gender or Jurisdiction are examples of drop-down selection list event tags.

You can add a secondary drop-down list event tag in two ways:

- Using a predefined event tag template (below)
- Creating a custom event tag (page 341)

You can also edit a drop-down list event tag (page 344) after you create it.

Short text answer form

A short text answer event tag prompts officers to enter an alphanumeric or numeric value in a field. When you set up a text answer event tag, you enter the question (prompt) and select whether the text answer is restricted to alphanumeric or numeric values. SuspectDescription or GangAffiliation are examples of short text answer event tags.

You can add a secondary text answer event tag in two ways:

- Using a predefined event tag template (page 345)
- Creating a custom event tag (page 347)

You can also edit a short text answer event tag (page 349) after you create it.
Chapter 8. Managing Devices

**Adding a drop-down list event tag using a template**

To set up a new drop-down selection list event tag from a predefined template:

1. At the top of either the 4RE Management Editor or VISTA Management Editor dialog box, click **All Event Tags**.

   The **Global Event Tag Definitions** dialog box opens.

2. Just above the list of event tags, click **Add Tag**.

   The **Create New Event Tag** dialog box opens.

3. Click the **Pre-defined event tag templates** link.

   The **Add New Event Tags from Templates** dialog box opens.
4. Check the **Select the suspect's gender** checkbox, then click **OK**.

**Note:** On the list of predefined event tags, only one is a drop-down list event tag: **Gender**.

The **Gender** event tag is added to the list of event tags on the **Global Event Tag Definitions** dialog box.

5. Verify that the **Gender** event tag is selected, then click **Edit Tag**.

The **Editing Event Tag Gender** dialog box opens.

6. If needed, edit existing answers on the **Display Answers** lists.
   a. Highlight the **Display Answer** you want to edit, then enter your changes.
   b. Press **Enter**.

7. If needed, add new answers to the **Display Answers** lists.
   a. Click **Add**.

   The **Create Dropdown Answer for Tag** dialog box opens.
b. Enter the **Display Answer** for both 4RE and VISTA, then click **OK**.

![Create Dropdown Answer for Tag](image)

**Note:** You must enter a **Display Answer** for both 4RE and VISTA; however, the VISTA event tag only displays at import and on event details after import. For information about editing secondary tags at import, see Secondary event tags on page 39. For information about editing secondary tags on the event details page, see Basic event details section on page 92.

The new event tag answer is added to the bottom of the lists of **Display Answers**.

![Editing Event Tag Gender](image)

c. If you do not want to display the new answer for one of the devices, check the **Retired** checkbox for the appropriate device.

8. If needed, adjust the **Display Order** of the event tag answers for each device.

   a. In the appropriate **Display Order** section, select the category whose place in the order you want to change.

   b. Use the up and down arrows next to the **Display Order** section to move the selected event tag answer up or down in the list.
9. Select whether you want to require an officer to answer this event tag on 4RE.

If you want to require an answer on the 4RE, select the **Require event tag answer** option.
If you do NOT want to require an answer on the 4RE, select the **Dismiss event tag prompt after** option and enter the number of seconds that the event tag should remain on the 4RE display screen before it disappears automatically.

**Note:** Only the **EventCategory** tag shows on the VISTA display.

10. Click **OK** on the **Editing Event Tag** dialog box.
11. Click **OK** on the **Global Event Tag Definitions** dialog box.

**Adding a custom drop-down list event tag**

To set up a new custom drop-down selection event tag:

1. At the top of either the **4RE Management Editor** or **VISTA Management Editor** dialog box, click **All Event Tags**.

The **Global Event Tag Definitions** dialog box opens.

2. Just above the list of event tags, click **Add Tag**.

The **Create New Event Tag** dialog box opens.
Chapter 8. Managing Devices

3. Click the Selectable answers in a dropdown list link.

A blank Add New Tag dialog box opens for a drop-down selection list event tag.

4. Enter the name of the new custom event tag in the Add New Tag field.

   ![Add New Tag dialog box]

   **Note:** The custom event tag name must be alphabetic (upper or lower case) with no spaces, and no longer than 31 characters.

5. Click Add.

   The Create Dropdown Answer for Tag dialog box opens.

6. Enter a Display Answer for both 4RE and VISTA, then click OK.

   ![Create Dropdown Answer for Tag dialog box]
Adding a custom drop-down list event tag

**Note:** You must enter a Display Answer for both 4RE and VISTA, but the VISTA tag only displays at import and on event details after import. For information about secondary tags at import, see Secondary event tags on page 39. For information about secondary tags on the event details page, see Basic event details section on page 92.

7. Repeat steps 5 and 6 as many times as needed for the drop-down list tag.

The event tag answers are added to the lists of Display Answers.

8. If you do not want to display one of the answers for one of the devices, check the Retired checkbox for the device.

9. If needed, adjust the Display Order of the event tag answers for each device.
   a. In the appropriate Display Order section, select the category whose place in the order you want to change.
   b. Use the up and down arrows next to the Display Order section to move the selected event tag answer up or down in the list.

10. Enter the custom event tag Prompt that will appear on the 4RE for the officer to respond to.

11. Select whether you want to require an officer to answer this event tag on 4RE.

   If you want to require an answer on the 4RE, select the Require event tag answer option.

   If you do not want to require an answer on the 4RE, select the Dismiss event tag prompt after option and enter the number of seconds that the tag should remain on the 4RE before it disappears.

   **Note:** Only the EventCategory tag shows on the VISTA display.

12. Click OK on the Add Event Tag dialog box.

13. Click OK on the Global Event Tag Definitions dialog box.
Chapter 8. Managing Devices

**Editing a drop-down list event tag**

To edit a drop-down selection list event tag:

1. At the top of either the 4RE Management Editor or VISTA Management Editor dialog box, click All Event Tags.

The Global Event Tag Definitions dialog box opens.

2. Select the drop-down list event tag you want to edit, then, just above the list of event tags, click Edit Tag.

The Editing Event Tag dialog box opens for the drop-down list event tag you selected.

3. Edit the fields as needed.

---

**Important!** Only the EventCategory tag appears on the VISTA camera, so any edits you make to the VISTA fields only appear with the secondary event tags on import and on event details. For information about editing secondary tags at import, see Secondary event tags on page 39. For information about editing secondary tags on the event details page, see Basic event details section on page 92.
4. Click OK on the **Editing Event Tag** dialog box.
5. Click OK on the **Global Event Tag Definitions** dialog box.

**Adding a text answer event tag using a template**

To set up a new short text answer event tag from a predefined template:

1. At the top of either the **4RE Management Editor** or **VISTA Management Editor** dialog box, click **All Event Tags**.

   The **Global Event Tag Definitions** dialog box opens.

2. Just above the list of event tags, click **Add Tag**.

   The **Create New Event Tag** dialog box opens.
3. Click the **Pre-defined event tag templates** link.

The **Add New Event Tags from Templates** dialog box opens.

4. Check the checkbox for the short text answer event tag template you want to add, for example, **SuspectDescription**, then click **OK**.

The event tag you selected is added to the list of event tags on the **Global Event Tag Definitions** dialog box.

5. Verify that the event tag that you added is selected, then, just above the list of event tags, click **Edit Tag**.

The **Editing Event Tag** dialog box opens for the new text answer event tag you just added.
Adding a custom text answer event tag

6. Select whether you want to require an officer to answer this event tag on the 4RE.
   If you want to require an answer on the 4RE, select the **Require event tag answer** option.
   If you do NOT want to require an answer on the 4RE, select the **Dismiss event tag prompt after** option and enter the number of seconds that the event tag should remain on the 4RE display screen before it disappears automatically.

7. Select whether the short text answer the officer enters on the 4RE should be **Alphanumeric only** or **Numeric only**.

8. Click **OK** on the **Editing Event Tag** dialog box.

9. Click **OK** on the **Global Event Tag Definitions** dialog box.

---

**Adding a custom text answer event tag**

To set up a new custom short text answer event tag:

1. At the top of either the **4RE Management Editor** or **VISTA Management Editor** dialog box, click **All Event Tags**.
   The **Global Event Tag Definitions** dialog box opens.

   ![Global Event Tag Definitions](image1)

   2. Just above the list of event tags, click **Add Tag**.
   The **Create New Event Tag** dialog box opens.

   ![Create New Event Tag](image2)

---
3. Click the **Text field answer** link.

A blank **Add New Tag** dialog box opens for a short text answer event tag.

![Add New Tag dialog box](image)

4. Enter the name of the new custom event tag and the **Prompt** that will appear on the 4RE for the officer to respond to.

![Add Event Tag dialog box](image)

**Note:** The custom event tag name must be alphabetic (upper and/or lowercase) with no spaces, and no longer than 31 characters.

5. Select whether you want to require an officer to answer this event tag on the 4RE.

If you want to require an answer on the 4RE, select the **Require event tag answer** option.

If you do NOT want to require an answer on the 4RE, select the **Dismiss event tag prompt after** option and enter the number of seconds that the event tag should remain on the 4RE display screen before it disappears automatically.

6. Select whether the short text answer the officer enters on the 4RE should be **Alphanumeric only** or **Numeric only**.

7. Click **OK** on the **Add Event Tag** dialog box.

8. Click **OK** on the **Global Event Tag Definitions** dialog box.
Editing a text answer event tag

To edit a short text answer event tag:

1. At the top of either the 4RE Management Editor or VISTA Management Editor dialog box, click All Event Tags.

   The **Global Event Tag Definitions** dialog box opens.

   ![Global Event Tag Definitions](image1)

2. Select the text answer event tag you want to edit, then, just above the list of event tags, click **Edit Tag**.

   The **Editing Event Tag** dialog box opens for the text answer event tag you selected.

   ![Editing Event Tag](image2)

3. Edit the fields as needed.

4. Click **OK** on the **Editing Event Tag** dialog box.

5. Click **OK** on the **Global Event Tag Definitions** dialog box.
Chapter 8. Managing Devices

This page intentionally left blank.
Chapter 9. Managing Security

In this chapter...

- EL4 Web security roles (page 354)
- Managing Evidence Library 4 Web (EL4 Web) security in an Active Directory® (AD) environment (page 358)
- Managing EL4 Web security in an Active Directory Lightweight Directory Services (LDS) environment (page 361)
Overview

Evidence Library 4 Web (EL4 Web) controls user permissions for its server and for associated devices (4RE DVR and VISTA Body Camera) using security groups. Each security group is made up of individual users. You set up EL4 Web security groups using one of the following options:

- Your existing agency Active Directory® (AD) environment (page 358)
  For this option, you set up your security groups in AD, then import them into the Evidence Library Administrator (EL Administrator) Security Management module.

- A stand-alone AD Lightweight Directory Services (LDS) environment (page 361)
  For this option, you set up your security groups directly in EL Administrator Security Management.

Once you set up the security groups, you assign EL4 Web roles to each group to give its users the appropriate permissions. For information about the individual roles in Security Management, see Security Management Roles on page 354.

Accessing Security Management

You access Security Management through the administrative module for Evidence Library 4 Web (EL4 Web), Evidence Library Administrator (EL Administrator).

1. On the desktop of the computer where EL Administrator is installed, double-click the Evidence Library Administrator icon.
   The Evidence Library Administrator Sign In dialog box opens.

2. Enter your Username and Password, then click Sign-In.
Accessing Security Management

The WatchGuard Evidence Library Administrator opens with the **Device Management** tab active.

3. Click the **Security Management** tab then the **Security Management** button.

The **Security Management** dialog box opens.

---

**Note:** The Security Management dialog box changes depending on whether you use EL4 Web in an Active Directory® (AD) environment or an AD Lightweight Directory Services (LDS) environment.
Security Management Roles

Roles in Evidence Library 4 Web (EL4 Web) Security Management represent the permissions that can be assigned to a user group. Security roles are generally narrow in their scope, so multiple roles need to be assigned to a user group to give them all the permissions they need to do their job.

For example, for a user group that needs to work extensively with evidence in EL4 Web, you can assign:

- **User**: Needed to log into EL4 Web

  **Important!** Groups must be assigned the User role to log in to EL4 Web.

- **Enhanced Search and Review**: Needed to search for, play back, and review details of events recorded by any officer
- **Edit Recorded Event Properties**: Needed to edit recorded event details
- **Review Detailed Audit**: Needed to view the detailed history of recorded events in EL4 Web
- **Case Management**: Needed to create new cases and work with any case in the Case Management module
- **Evidence Management**: Needed to set up and manage evidence storage locations as well as manually purge recorded events
- **Archive Restore**: Needed to archive and/or restore recorded events from archive

The following table lists the EL4 Web security roles with their descriptions:

<table>
<thead>
<tr>
<th>EL4 Web Role</th>
<th>Description</th>
<th>Automatically includes</th>
<th>Does NOT include</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Inherits all security roles and permissions except Officer and Supervisor</td>
<td>All roles except Officer and Supervisor</td>
<td>• Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Supervisor</td>
</tr>
<tr>
<td>Archive Restore</td>
<td>Allows users to move recorded events from the main video storage to the archive storage location and restore them from archive back to main video storage</td>
<td></td>
<td>• User</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Enhanced Search and Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Evidence Management</td>
</tr>
<tr>
<td>Case Management</td>
<td>Allows users to create and work with any cases and their attachments in the Case Management module</td>
<td>Case Worker</td>
<td>• User</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Export</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Enhanced Search and Review</td>
</tr>
</tbody>
</table>
## Security Management Roles

<table>
<thead>
<tr>
<th>EL4 Web Role</th>
<th>Description</th>
<th>Automatically includes</th>
<th>Does NOT include</th>
</tr>
</thead>
</table>
| Case Viewer                | Allows users to view any cases and their attachments in the Case Management module                    |                                                                                         | • User  
• Case Worker  
• Export  
• Enhanced Search and Review |
| Case Worker                | Allows users to create cases and work with any cases they create or are assigned to in the Case Management module |                                                                                         | • User  
• Export  
• Enhanced Search and Review |
| Delete Before Import       | Allows users to mark an event for deletion before manual import                                        |                                                                                         | • User  
• Officer |
| Device Management          | Allows users to work in the Device Management module to create, manage, deploy device configurations as well as deploy device software upgrades | Device Provisioner                                                                      | • User  
• Evidence Management  
• User Security Management |
| Device Provisioner         | Allows users to check out a VISTA Body Camera to any officer on the list of VISTA configuration users  |                                                                                         | • User  
• Device Management  
• Kiosk       |
| Edit Recorded Event Properties | Allows users to edit recorded event details                                                            |                                                                                         | • User  
• Enhanced Search and Review |
| Edit Recorded Event Tags   | Allows users to edit the event category and secondary event tags                                       |                                                                                         | • User  
• Enhanced Search and Review  
• Edit Recorded Event Properties |
| Enhanced Search            | Allows users to search for and display on the Events tab events recorded by any officer                |                                                                                         | • User  
• Officer  
• Enhanced Search and Review  
• Search and Review Restricted Events |
## Chapter 9. Managing Security

<table>
<thead>
<tr>
<th>EL4 Web Role</th>
<th>Description</th>
<th>Automatically includes</th>
<th>Does NOT include</th>
</tr>
</thead>
</table>
| Enhanced Search and Review        | Allows users to search for, play back, and review details of events recorded by any officer | Enhanced Search                         | • User  
• Officer  
• Search and Review  
• Restricted Events  
• Edit Recorded Event Properties |
| Evidence Management                | Allows users to work in the Evidence Management module to set up evidence storage locations, retention rules, and cleanup schedules; allows users to manually purge recorded events, from the Events tab; allows users to access the CLOUD-SHARE configuration page to set up the CLOUD-SHARE Export Worksheet tab | • User  
• Device Management  
• User Security Management  
• Enhanced Search and Review  
• Archive Restore  
• Share |
| Export                            | Allows users to export evidence to a disc or a local/network computer location; allows users to trim video from a recorded event | Review Detailed Audit                   | • User  
• Enhanced Search and Review  
• Enhanced Case Worker  
• Case Management  
• Share |
| Import                            | Future use                                                                  |                                         |                                                        |
| Kiosk                             | Allows users to log into a Kiosk that has its administrative function (setting or changing Kiosk location) disabled | • User                                  |                                                        |
| Live Streaming Video              | Allows users to access the Watch Commander application                      | • User  
• Officer                                |                                                        |
| Officer                           | Allows users to be assigned to device configurations in the Device Management module | • User                                  |                                                        |
| RATF                              | Allows users to request Record-After-the-Fact® (RATF) events from VISTA Body Cameras | • User  
• Supervisor  
• Enhanced Search and Review   |                                                        |
<table>
<thead>
<tr>
<th>EL4 Web Role</th>
<th>Description</th>
<th>Automatically includes</th>
<th>Does NOT include</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Detailed Audit</td>
<td>Allows users to view detailed audit information about a recorded event as part of event details</td>
<td></td>
<td>• User&lt;br&gt;• Enhanced Search and Review</td>
</tr>
<tr>
<td>Search and Review Restricted Events</td>
<td>Allows users to search for, play back, and review details of recorded events flagged as restricted</td>
<td></td>
<td>• User&lt;br&gt;• Enhanced Search and Review&lt;br&gt;• Enable Restricted Access&lt;br&gt;• Edit Recorded Event Properties</td>
</tr>
<tr>
<td>Share</td>
<td>Allows users to export evidence to EvidenceLibrary.com for sharing with other agencies or organizations</td>
<td></td>
<td>• User&lt;br&gt;• Enhanced Search and Review&lt;br&gt;• Enhanced Case Worker&lt;br&gt;• Case Management&lt;br&gt;• Evidence Management&lt;br&gt;• Export</td>
</tr>
<tr>
<td>Supervisor</td>
<td>Allows users to be assigned to a 4RE configuration as an in-car supervisor</td>
<td>Officer</td>
<td>• User</td>
</tr>
<tr>
<td>Unassigned</td>
<td>Allows users to assign any unassigned events at import, and search for and play back unassigned events after import</td>
<td></td>
<td>• User&lt;br&gt;• Officer&lt;br&gt;• Enhanced Search and Review&lt;br&gt;• Edit Recorded Event Properties</td>
</tr>
<tr>
<td>User</td>
<td>Allows users to log in to EL4 Web, then, search for, play back, and edit details of events that they recorded, if applicable</td>
<td>Officer</td>
<td></td>
</tr>
<tr>
<td>User Security Management</td>
<td>Allows users to work in the Security Management module to manage users, user groups, and security roles</td>
<td></td>
<td>• User&lt;br&gt;• Device Management&lt;br&gt;• Evidence Management</td>
</tr>
</tbody>
</table>
Chapter 9. Managing Security

Setting Up Security in an AD Environment

If your agency uses Active Directory® (AD), you set up your user groups in AD, then import them into Evidence Library Administrator (EL Administrator) Security Management.

The process of setting up security groups in EL Administrator has two parts:

- Adding the user groups to EL Administrator that you set up in AD (page 359)
- Assigning Evidence Library 4 Web (EL4 Web) roles to the user groups (page 360)
  
You assign roles to a group according to the function of the group. For a list of EL4 Web roles with their descriptions, see Security Management Roles on page 354.

Best practices for working with AD

Your agency’s EL4 Web server must be on your domain and integrated with your AD environment. This means that your EL4 Web server is joined to your local domain and that AD is used to authenticate any EL4 Web users.

Before installing EL4 Web

In AD, before you install EL4 Web or its supporting software:

- Create a domain account with local administrator rights on the EL4 Web server

  Warning! Use this account to log in to the EL4 Web server you are setting up, then use the same account when the software asks for a username and password during the EL4 Web installation. Using a different username and password will cause the installation to fail.

- Create AD security groups (user groups) and add users to each group (see below)
  
After EL4 Web is installed, you assign roles to these groups in EL Administrator Security Management. For instructions how to assign roles to user groups, see Assigning roles to AD user groups on page 360.

Creating EL4 Web user groups in AD

In EL4 Web, roles are assigned to groups of users rather than individual users. You set up these groups of users in AD using individual network user names.

When you set up the EL4 Web user groups in AD:

- Name the EL4 Web groups according to a convention, using meaningful names, for example, wg_officers, wg_supervisors
- Set the EL4 Web groups up as AD security groups, NOT distribution groups

Once EL4 Web has been installed, you use the Security Management module to query for all your AD groups. After you add the groups to EL Administrator, you assign them EL4 Web roles.
Adding AD user groups

To add AD user groups to Security Management, in EL Administrator:

   
   For instructions how to access Security Management, see Accessing Security Management on page 352.

2. On the **Group Enrollments** tab of the **Security Management** dialog box, click **Find All**.

   ![Security Management dialog box](image)

   All of your agency’s AD groups populate the list in the **All Active Directory Groups** section.

3. Select each AD group that you created to use in EL4 Web, then click **Enroll**.

   **Note:** You can select multiple groups at once using either **Shift + click** or **Ctrl + click**.

   ![Security Management dialog box](image)
Chapter 9. Managing Security

Assigning roles to AD user groups

After you have added the Active Directory® (AD) groups to Evidence Library Administrator (EL Administrator), assign them EL4 Web roles:

1. In EL Administrator, access Security Management.
   
   For instructions how to access Security Management, see Accessing Security Management on page 352.

2. Click the Group Roles tab then select the group you want to assign roles to.

3. Select each Role you want to assign to the selected group, then click Add Role.

![Security Management](image1)

The Role is added to the selected group.

![Security Management](image2)
Setting Up Security in an AD LDS Environment

If your agency does not have an Active Directory (AD) server, you administer users and user groups using AD Lightweight Directory Services (LDS), through the Evidence Library Administrator (EL Administrator) Security Management module.

Users, user groups, and roles

In this security environment, you do not assign roles to users directly. You create user groups and assign one or more security roles to those groups. When you create users, you can assign them to one or more user groups. By managing users and user groups in this way, you can easily grant a new set of permissions to many users at once, rather than assigning those new permissions to users one by one.

Setup process

The process of setting up users and groups has four parts, all of which are done inside the EL Administrator tool:

1. Create and set up an administrator account. (page 362)
2. Add user groups and assign roles to those groups. (page 367)
   You assign EL4 Web roles to a user group according to the role that group has at your agency.
   For a list of EL4 Web roles with their descriptions, see Security Management Roles on page 354.
3. Add user accounts. (page 369)
4. Assign users to user groups. (page 370)
Chapter 9. Managing Security

Creating and setting up an LDS administrator account

To create a Lightweight Directory Services (LDS) administrator account in Evidence Library Administrator (EL Administrator) Security Management:

1. In EL Administrator, access Security Management.
   For instructions to access Security Management, see Accessing Security Management on page 352.

2. On the **User Groups** tab of the Security Management dialog box, click **Create Group**.

   ![Create Group dialog box](image1)

   The **Create New User Group** dialog box appears.

3. In the **Group Properties** section, name the group **Administrators** and add a brief description of the group, such as **EL4 Web administrators**.

   ![Create New User Group dialog box](image2)
4. In the **Group Roles** section, select the **Administrator** check box, then click the **Create** button.

5. Click the **Users** tab to view the list of users.

6. Click **Create User**.

The **Create New User** dialog box appears.
7. In the **Person's Identity** section, enter your name and any other information your agency requires.

8. Your **Username** is automatically generated when you enter your information. You can change it now, if you wish. Enter and re-enter your **Password**, then click the **Create** button.
9. Click the **User Groups** tab.

![User Groups tab](image)

10. Click **Administrators** to highlight it, then click **Edit Group**.

![Administrators Group](image)

11. Click your name in the **Non Members** box in the lower right.

![Non Members box](image)
Chapter 9. Managing Security

12. Click the left arrow button to move your name from the **Non Members** box to the **Members** box.

13. Click the **Save** button.

14. Log out of EL Administrator and log back in using this new administrator account.
Adding LDS user groups and assigning roles

To add Lightweight Directory Services (LDS) user groups to Evidence Library Administrator (EL Administrator) Security Management:

1. In EL Administrator, access Security Management.
   For instructions to access Security Management, see Accessing Security Management on page 352.


3. In the Group Properties section, enter the name of the group and a brief description.

4. In the Group Roles section, select one or more check boxes to assign the corresponding security roles to this group.

The Create New User Group dialog box appears.
You assign EL4 Web roles to a user group according to the role that group has at your agency. For a list of EL4 Web roles with their descriptions, see Security Management Roles on page 354.

**Note:** Anyone in a group that includes the Administrator or Security role can make changes to the LDS setup.

5. Click the **Create** button.
Adding LDS user accounts

To create a Lightweight Directory Services (LDS) user account in Evidence Library Administrator (EL Administrator) Security Management:

1. In EL Administrator, access Security Management.
   
   For instructions to access Security Management, see Accessing Security Management on page 352.

2. On the Users tab, click **Create User**.

   ![Create New User dialog box](image)

   The **Create New User** dialog box appears.

3. In the **Person's Identity** section, enter their name and any other information your agency requires.

   ![Create New User dialog box](image)
4. The **Username** is automatically generated when you enter their information. You can change it now, if you wish. Enter and re-enter their **Password**, then click the **Create** button.

![Create New User dialog box](image)

**Assigning LDS users to user groups**

After you have added Lightweight Directory Services (LDS) users and groups to Evidence Library Administrator (EL Administrator), there are two ways to assign users to user groups:

- **Editing user groups**: Use this method to add several users at a time to one user group (page 371)
- **Editing users**: Use this method to assign a single user to multiple groups (page 373)
Assigning users to groups on the Edit User Group dialog box

1. In EL Administrator, access Security Management.
   For instructions to access Security Management, see Accessing Security Management on page 352.

2. In the User Groups tab, click a name to highlight it, then click Edit Group.

3. Click a name in the Non Members box in the lower right. Select multiple names at once using either Shift + click or Ctrl + click.
Chapter 9. Managing Security

4. Click the left arrow button to move your name from the **Non Members** box to the **Members** box.

5. Click the **Save** button.
Assigning users to groups on the Edit User dialog box

1. In EL Administrator, access Security Management.
   For instructions to access Security Management, see Accessing Security Management on page 352.

2. In the Users tab, click a group to highlight it, then click Edit User.

   ![Edit User dialog box]

   The Edit User dialog box appears.

3. Click Roles/User Groups.

   ![User Roles dialog box]

   The User Roles dialog box appears.
Chapter 9. Managing Security

4. Click **Add to Group** to access the drop-down menu.

![Add to Group](image1)

5. On the drop-down menu click a user group.

![User Group](image2)

6. Repeat this process to add more roles, if needed. Then click the **Save** button.
Index

exported player, 162
Audit Log button, export player, 172
Auto-Start Record Settings
  4RE DVR, 286
  VISTA, 316
auto-stop event
  4RE DVR, 286
  VISTA camera, 317
Auto-Stop Record Settings, 286
Auto Update checkbox, 51
automatic
  event linking, 269
  evidence cleanup, 262-264
  firmware update, VISTA, 325
import
  ethernet-connected devices, 31
  from Transfer Station, 31
  from USB, 295
  from WiFi Base, 31
  USB-connected devices, 32
power off, VISTA, 321
VISTA configuration deployment, 309
Automatic Configuration Deployment switch, 302

B
background recording, 290
battery charge timer, VISTA, 321
battery status, VISTA Dashboard, 211
blank screen on movement, 294
browsers, supported, 22-23
bulk adding files to cases, 109
bulk deleting files from cases, 110
Burn to Disc export destination, 144

C
camera state, 290
camera views
  events, 54
  exporting, 140
Camera Views Panel, export player, 173
captions
  including for export, 142
  metadata, 82
  on export playback, 173, 180
  on exported player, 160
  on playback, 65, 69, 76, 177
Case Management overview, 102
case storage, 253-254
case workers
  adding, 115
  permissions, 117
Case Workers tab, 117
cases
  adding
    files, 109
    links, 111
  creating, 103
  deleting, 105
  files, 110
  links, 112
event details, 96
export, 134
purge and archive rules, 103
removing recorded events, 108
search, 113
viewing attachments, 114
category event tag, 334
retention rules, 259
checkout
  kiosk mode, 200-201
  kiosk setup, 204
  overview, 186
  rapid, 192, 197
  report, 199
  USB Dashboard, 187
  VISTA Dashboard, 192-193
Chrome, 22
cleaning up evidence storage, 257, 259, 262
cleanup
daily, 264
manual, 264
monthly, 264
weekly, 264
Cleanup Scheduling, 257
CLOUD-SHARE
  configuring, 150
  export, 148
  forwarding, 150
  playback, 150
  recipients, 148
security types
  access code, 149
  secured, 149
unsecured, 149
cloud storage, 242
  adding locations, 236
  adding tiers, 234
  editing locations, 239
  URL, 237, 239
configurations
  assigning
    enrollments, 4RE DVR, 282
    enrollments, VISTA, 312
    vehicles, 281
  copying, 280
  creating, 279, 311-312
  deploying to 4RE DVR, 298, 302
  deploying to VISTA automatically, 309
  loading, 301
configuring
  4RE DVR, 270-271
  CLOUD-SHARE, 150
  overview, 278, 310
  VISTA, 307-308, 310
creating cases, 103
credentials, storage location, 226, 232, 241
critical event tags, 332
critical rules, 285
D
daily evidence cleanup, 264
dashboard
  USB, 40
  VISTA, 210
data cleanup, 257, 259, 263
default retention rule, 260
deleting
cases, 105
files from cases, 110
links from cases, 112
Department Name field, 269
deploying
  configuration, 4RE, 298, 302
  configuration, VISTA, automatic, 309
  firmware update, VISTA, 325
  overview, 297
  software update, 4RE DVR, 303-304
destinations for export, 143
  DVD robot, 145
  local computer folder, 143
  media burner, 144
  secure cloud, 148
Device Management
  4RE DVR, 270
  accessing, 267
  larger agencies, 268
  overview, 266
  permissions, 266
  smaller agencies, 268
  using, 268
  VISTA camera, 307
devices
  configuring, 278, 307
  properties, 319
disable audio, VISTA, 316
Display Units, 273
display, blanking on movement, 294
drag-and-drop locations, 242
DVD Robot export destination, 145
DVR Behavior, 291
E
ELX Viewer, 309
embedding text for export, 142
Enable DHCP client, 276
enabling
  4RE DVR management, 269
  GPS on VISTA, 321
  integration with SmartConnect, 324
  Record-After-the-Fact, VISTA, 316
  VISTA camera management, 269
  wireless upload for VISTA, 325
Endpoint Suffix, cloud, 237, 239
enrollments
  assigning to 4RE DVR configurations, 282
  assigning to VISTA configurations, 312
Event Details button, export player, 172
event details, editing, 91
event tags, 331
  assigning, 287, 317
  category, 334
  critical, 332
  required, 333
  retired, 333
  secondary, 94, 332, 337
    drop-down list, 337, 341
    editing, 344, 349
    templates, 338, 345
text answer, 337, 347
Index

**events**
- archiving, 93, 98
- export playback
  - 1-Up, 175
  - 2-Up, 178
  - single, 172
- export player, 164
- exporting, 121, 124
- import properties, 94
- importing, 30, 34
- linking
  - automatic, 269
  - manual, 60
- list view, 56
- managing, 48
- metadata, 82
- playback, 62
  - 1-Up, 66
  - 2-Up, 73
  - single, 63
- preview, 39
- purging manually, 100
- restoring from archive, 99
- searching for, 49-50, 52
- staging, 250
- storing, 217
- sync export, 127
- unlinking, 61

**evidence**
- retention, 257
- storage cleanup, 257, 262-263
  - daily, 264
  - manual, 264
  - monthly, 264
  - weekly, 264
- Evidence Management
  - accessing, 215
  - workflow, 216
- expiration, CLOUD-SHARE, 148

**export**
- destinations, 143
  - CLOUD-SHARE, 148
  - DVD robot, 145
  - local computer folder, 143
  - media burner, 144
  - preferences, 146
- formats, 140-141
- queue, 156
- storage, 251
- sync export, 62, 70
- export playback
  - 1-Up, 175, 180
  - 2-Up, 178, 182
- export player
  - accessing, 169
  - installing, 164-165
  - overview, 164
- Export Summary, 155
- Export Worksheet, 136
- exporting events, 138
  - camera views, 140
  - cases, 140
  - linked, 139
  - multiple, 124
  - overview, 120
  - single, 121
  - summary, 155
- sync export, 62, 70, 127, 139
- trimmed video, 139

**F**
- files
  - adding to cases, 109
  - deleting from cases, 110
- firmware update
  - 4RE DVR, 303
    - automatic, 304
    - manual, 303
  - VISTA, 325
    - automatic, 325
    - manual, 326
- first tier, 223-224, 240
- folders, shared, 219
- forcing microphone on
  - 4RE, 294
  - VISTA, 316
- formats, export, 140
- forwarding shares, 150
- Front Camera Settings, 285
  - video quality, 287
- Full Access permission, 118

**G**
- GPS
  - coordinate format, 293
  - enabling on VISTA, 321
- Group Actions menu, 57, 59
Index

group event
  4RE start, 286
  VISTA start, 317
  VISTA stop, 317

group member start
  4RE, 286
  VISTA, 317

group member stop, VISTA, 317

H
holding area, export, 251

I
IE, 22
ignition auto on/off, 293
Ignition Shutdown Timer, 4RE DVR, 294
import
  properties, 94
    4RE DVR, 295
    VISTA, 321
storage, 250
Import Events dialog box, 36
importing
  4RE DVR, 31
  automatic, 31-32
  editing secondary tags, 39
  manual, 34, 36
  overview, 30
  previewing events, 39
Transfer Station, 31
VISTA camera, 31
WiFi Base, 31
wireless, 31
Importing banner, 55
Include Subtitles checkbox, 142
installing export player, 164-165
integration with SmartConnect, 324
Internet Explorer, 22
IP assignment, 276
item selection for export, 138

J
Job Queue Worker Service, 245

K
kiosk mode, 200-201
  setup, 204

L
LDS
  administrator account, 362
  assigning roles, 367
environment, 361
  groups, 361
    adding, 367
    setup, 361
user accounts
  adding, 369
  assigning to user groups, 370
Lightweight Directory Services
  administrator account, 362
  assigning roles, 367
  environment, 361
  groups, 361
    adding, 367
    setup, 361
user accounts
  adding, 369
  assigning to user groups, 370
linking events, 55
  automatically, 269
  event details, 95
  manual, 60
links
  adding to cases, 111
  deleting from cases, 112
loading configuration on 4RE, 301
Local Computer export destination, 143
locations, storage, 241
  adding credentials, 226, 232
  case, 253-254
  cloud, 236, 239
  export, 251
  import, 250
  on premise, 230, 238
  shared folders, 219
  video processing, 245-246

M
management functions, 24-25
manual
  evidence cleanup, 263-264
  import properties
    4RE DVR, 295
    VISTA, 321
  importing, 34, 36
  linking, 60
Mark Event for Delete button, 38
Maximum Recorded Event Size
  4RE DVR, 286
  VISTA, 317

EL4 Web User Guide
WGD00133 Revision L

379
Index

Maximum Recorded Event Time
   4RE DVR, 286
   VISTA, 317
media
   export, 140
   export destinations, 143
type, 144
metadata, 82
captions, 82
graph, 83
   trimming video, 86
Metadata button, 66
monthly evidence cleanup, 264
moving events from previous tier, 243
multiple event export, 124
muting VISTA, 316
My Exports, 138, 156
N
Network Connection Type field, 276
network credentials, storage, 241
network settings, VISTA, 323
new officer preferences, 308
notifications, storage status, 218, 255
   Remote Upload, 256
   Storage Full, 256
   Storage Low, 255
   Storage Offline, 256
threshold, 256
O
officer
   permissions, 293
   preferences, 190, 308
Offline Archive storage, 252-253
on-premise storage, 242
   adding locations, 230
   adding tiers, 228
   editing locations, 238
on-screen text, 293
Online Video storage, 222, 240
   adding tiers, 228, 234
   examples, 244
override video resolution, 286
P
Panoramic Camera Settings, 286
   video quality, 289
Partial banner, 55
password
   4RE DVR
      administrator, 273
      supervisor, 306
   VISTA checkout, 208
Permanently Embed... Text checkbox, 142
permissions
   Case Management, 102
   case workers, 117
   Device Management, 266
   Evidence Management, 354
   export, 120
   roles, 354
   trimming video, 86
playback
   1-Up, 66, 77
   2-Up, 73, 79
export
   1-Up, 175, 180
   2-Up, 178, 182
   single, 172
metadata, 83
   overview, 62
   shares, 150
   single, 63
timeline, 69, 76
playing back exported video, 169
pre-event time
   4RE DVR, 286
   VISTA, 316
preferences
   checkout
      Kiosk, 202
      USB Dashboard, 189
      VISTA Dashboard, 195
   export destination, 146
   new officer, 308
Prevent Archive switch, 93
Prevent Purge switch, 94
previewing events, 39
purge and archive rules, cases, 103
purging
   automatic, 257
   data cleanup, 257, 259
   manual, 100
   preventing, 94
R
radar values, 293
rapid checkout, 192, 197
RATF, VISTA, 44, 316
Read-Only permission, 118
Recipients field, 148
Record-After-the-Fact, VISTA, 44, 316
record start settings
  4RE DVR, 286
delay, 286
  VISTA, 316
record stop confirmation, 316
recorded events
  adding to case, 103, 106
  exporting, 120-121, 124
  importing, 30-32, 34
  managing, 48
  playing back, 62
  playing back after export, 164
  removing from cases, 108
  storing, 217
  sync export, 127
recording group
  4RE start, 286
  VISTA start, 317
  VISTA stop, 317
recording properties
  4RE DVR, 284
  VISTA, 314
Recording Reminder Alerts
  4RE DVR, 286
  VISTA, 316
Remote Upload notification, 256
required event tags, 333
resolution
  4RE DVR video, 287
  video override, 286
  VISTA video, 318
Restrict Access switch, 93
results, search
  rows, 53
  sort, 57
Retention Policy, export storage, 251
Retention Rules, 257, 259
  default rule, 260
  event categories, 259
  exceptions, 261
  setting, 258
retired event tags, 333
robot, DVD burner, 145
roles
  assigning
    AD, 360
    LDS, 361
  security, 354
rollover, storage, 242
round robin, storage, 242
rules, evidence retention
  default, 260
  exceptions, 261
  setting, 258
S
  scheduling evidence cleanup, 262-264
screen, blanking on movement, 294
searching
  for cases, 113
  for events, 49-50
  results, 52
    rows, 53
    sort, 57
    views, 56
Secondary Camera Settings, 285
  video quality, 288
secondary event tags, 332, 337
  drop-down list, 337, 341
  editing, 94, 344, 349
  editing at import, 39
  searching with, 50
  templates, 338, 345
  text answer, 337, 347
Secured security type, 149
security
  Accessing, 352
  overview, 352
  selecting items for export, 138
  Share Connection String, 151
  Share Expiration field, 148
Index

Share Security field, 149
shared folder setup, 219
shutdown timers, 293
  4RE DVR, 294
  VISTA, 321
single event
  export, 121
  playback, 63
sleep mode, VISTA, 321
Smart Power Switch, assigning IP, 276
SmartConnect Preferences, setting, 208
  Kiosk, 202
  USB Dashboard, 189
  VISTA Dashboard, 195
SmartConnect, enabling integration, 324
snapshot
  export playback, 173, 177
  exported player, 159
  from SmartConnect, 324
  playback, 65, 69
software update
  4RE DVR, 303-304
  VISTA, 325-326
splitting events, 54
  4RE DVR, 286
  VISTA, 317
SSID, 208
  Kiosk, 202
  VISTA Dashboard, 189, 195
staging events, 250
status, VISTA, 211
storage
  allocation, 242
  cleanup, 262-263
  cloud, 242
  on premise, 242
  rollover, 242
  round robin, 242
  setup examples, 241, 244
  usage, 242
Storage Account Name, cloud, 237, 239
Storage Full notification, 256
storage locations
  adding cloud, 236
  adding credentials, 226, 232
  adding on premise, 230
  archive, 252-253
  case, 253-254
  cleanup, 257
  editing cloud, 239
  editing on premise, 238
  export, 251
  import, 250
  shared folders, 219
  video processing, 245-246
Storage Low notification, 255
Storage Offline notification, 256
storage status
  notifications, 218, 255
  Remote Upload, 256
  Storage Full, 256
  Storage Low, 255
  Storage Offline, 256
  threshold, 256
VISTA Dashboard, 211
storage tiers, 240
  adding cloud, 234
  adding on premise, 228
  editing, 237
storage types
  Offline Archive, 252
  Online Video, 222, 240
  summary, 218
subtitles, 82
  export, 142
supervisor password, 4RE DVR, 306
supported browsers, 22
Sync button
  export player, 174
  playback, 66
sync export, 62, 70, 127
synced event export playback
  1-Up, 175, 177, 180
  2-Up, 178, 180, 182
  overview, 164
synced event playback
  1-Up, 66, 70, 77
  2-Up, 73, 76, 79
timeline, 69, 76
System Settings, 269
  table view, event list, 56
tagging events, 331
  assigning, 287
category, 334
critical, 332
required, 333
retired, 333
secondary, 332, 337
drop-down list, 337, 341
editing, 344, 349
templates, 338, 345
text answer, 337, 347
text on-screen, 293
threshold, storage status, 256
thumbnail size, 56
tiers, storage, 240
  adding cloud, 234
  adding on premise, 228
editing, 237
  first, 223-224
time zone, 292, 320
timeline
  1-Up playback, 69
  2-Up playback, 76						timers
  4RE, 293
  VISTA, 321
tool, trim, 84
Transfer Agent, 26
Transfer Station
  import, 31
  VISTA status, 210-211
triggers
  delay, 286
  record
    4RE DVR, 286
    VISTA, 316
trimming video, 84-86
  export, 131

U
unlinking events, 61
Unsecured security type, 149
upgrading
  4RE DVR software, 303-304
  VISTA firmware, 325-326
usage, storage, 242
USB-connected devices, 40
  importing from, 32, 34
USB Dashboard, 40
  accessing, 40
  checkout, 187
USB Settings, 4RE DVR, 272

USB thumb drive, removing from 4RE DVR, 41
user accounts
  LDS
    adding, 369
    assigning to user groups, 370
  Lightweight Directory Services
    adding, 369
    assigning to user groups, 370
user groups
  Active Directory, 358
  AD, 358
  adding
    Active Directory, 359
    AD, 359
    LDS, 367
    Lightweight Directory Services, 367
  assigning roles, 360
  assigning to configurations, 282, 312
  LDS, 361
  setup, 361
  Lightweight Directory Services, 361
  setup, 361
user permissions, 4RE, 290

V
Vehicle Dynamics search, 50
Vehicle ID, 275
vehicles
  adding, 275
  assigning to configurations, 276, 281
  editing, 277
  ignition power on/off, 293
  list, 4RE, 274
video
  formats for export, 141
  quality
    4RE DVR, 285-287, 289
    front camera, 287
    panoramic camera, 289
    secondary camera, 288
    VISTA, 315, 318
  resolution override, 286
  trimming, 84-86
  for export, 131
viewer, ELX, 309

Usage and Privacy Notice
Index

VISTA checkout
  kiosk mode, 200-201
  kiosk setup, 204
  overview, 186
  rapid, 192, 197
  USB Dashboard, 187
  VISTA Dashboard, 192-193
configuring, 307
disabling audio, 316
enabling
  GPS, 321
  wireless upload, 325
force microphone on, 316
group event
  start, 317
  stop, 317
integration with SmartConnect, 324
management, 269, 307
  accessing, 307
muting, 316
Record-After-the-Fact (RATF), 44
status, 211
Transfer Station import, 31
WiFi Base import, 31
VISTA Dashboard, 210
  accessing, 210
  checkout from, 192-193
W
Watch Commander, 276
web
  browsers, 22-23
  client, 22-23
weekly evidence cleanup, 264
WiFi Base
  importing, 31
  VISTA status, 210-211
wireless
  import, 31
  service IP address, 293
  VISTA upload, 31, 325
Wireless Shutdown Timer, VISTA, 321
Wireless Transfer Shutdown Timer, 4RE DVR, 294
workflows
  configuring 4RE DVR, 271
  configuring VISTA, 308
  evidence storage and retention, 216