



CSAS User Guide

CSAS v3.16



The name 'CSAS' and the pylon logo are registered Trademarks of Forensic Analytics Ltd. Forensic Analytics has and will continue to take all reasonable efforts to ensure that the information contained in this material is accurate and up to date. Forensic Analytics Ltd's responsibility for inaccurate or out of date information contained in this material is limited to the correction of such errors, Forensic Analytics Ltd will not be responsible for any losses (actual or consequential) that may result from such errors.

Copyright Notice: The content of this document is copyrighted and all rights are reserved by Forensic Analytics Ltd. Apart from fair dealing for the purposes of research or private study, as permitted under the Copyright, Designs and Patents Act 1988, the contents of this document may only be reproduced or transmitted in any form or by any means with the prior permission in writing of Forensic Analytics Ltd.

Contents

1	User Guide Overview	1
2	CSAS Product Description	2
2.1	CSAS Product Range	3
2.1.1	CSAS.....	3
2.1.2	CSAS RF Survey	3
2.1.3	CellView.....	3
2.1.4	CSAS Server.....	3
2.1.5	CDAN Nexus.....	4
2.1.6	CSAS Product Integration.....	4
2.2	Accessibility.....	4
3	Installing CSAS.....	5
3.1	Downloading CSAS Installer	5
3.2	Host PC Requirements.....	5
3.3	Initial Install.....	6
3.3.1	Installing CSAS.....	6
3.3.2	CSAS Local Startup Wizard	12
3.3.3	Licence Wizard.....	13
3.3.4	CSASv3 Upgrade.....	15
3.3.5	Uninstall CSAS	17
3.3.6	Adding Additional Licences.....	18
4	Opening CSAS and Logging In	19
5	General Operation	21
5.1	Modes.....	21
5.1.1	Standalone Mode	21
5.1.2	Server Mode.....	22
5.1.3	Hybrid working	22
5.2	Licence Options.....	23
5.2.1	Dedicated Licences	23
5.2.2	Floating Licence.....	24

5.3	Teams & Security Levels.....	27
5.3.1	Teams.....	27
5.3.2	Security Levels.....	27
5.3.3	Standalone Mode Settings	28
5.4	CSAS Layout	29
5.4.1	Tabbed Browsing.....	29
5.5	Top Row Buttons and Controls.....	30
5.5.1	File Menu	30
5.5.2	Admin Menu	30
5.5.3	Configuration.....	33
5.5.4	Utilities	34
5.5.5	Help Menu	35
5.5.6	Search Across Cases	38
5.5.7	CSAS Server Connection Status	39
5.5.8	Intel Mode	39
5.5.9	Profile Menu	40
5.6	Grid Filtering and Controls	43
5.6.1	Column Control Menu	43
5.7	Case Management.....	45
5.7.1	Copy Case.....	45
5.7.2	Export Case.....	46
5.7.3	Delete Case.....	46
5.7.4	Change Team.....	48
5.7.5	Change Owner	49
5.7.6	Rename	49
5.7.7	Edit Case Prefilters.....	50
5.7.8	Edit Time Zone	50
5.8	User Management	52
5.8.1	Standalone Mode	52
5.8.2	Server Mode.....	52
5.8.3	Assigning a Team.....	52
5.8.4	Assigning a Security Level	52
5.9	Case Workflow.....	53
5.10	Regulatory & Accreditation Support.....	54

5.10.1	Case Review.....	54
5.10.2	Case Status & Case Notes.....	54
5.10.3	Intel-only Users	55
6	CSAS Home Screen	57
6.1	Using the CSAS Home Navigation Pane.....	58
6.1.1	New Case	58
6.1.2	Manage Cases	58
6.1.3	Recent Cases and All Cases	58
6.2	Using the Search Pane	60
7	Case Home Navigation Panel	61
7.1	Changing the Default Landing Page	61
8	Setting Up a New Case	62
9	Importing and Exporting Cases	65
9.1	Importing a Case.....	65
9.2	Exporting a Case.....	67
10	Importing Files	69
10.1	Supported Data Types	69
10.2	Layout.....	70
10.3	Grid and Controls	70
10.3.1	Import Files Grid	70
10.3.2	Generic Grid Controls.....	73
10.3.3	Right-click Controls and Actions Menu.....	73
10.4	Importing Files	73
10.4.1	Updating File Details.....	78
10.4.2	Continuity Details.....	78
10.4.3	File Import Wizard	78
10.4.4	Importing USA Device Ping Data	82
10.4.5	Reloading Failed Files	84
10.4.6	Post-update file warnings.....	85
10.4.7	Parsing Updates	85
10.5	Visual Parser	86
10.5.1	How to view the visual parser	86
10.5.2	General Operation	86

10.5.3	Colour Coding	87
10.5.4	Common Processed Information Tabs.....	88
10.5.5	File-type Specific Tabs	89
10.6	Deleting Files	91
10.7	Settings Sidebar	92
10.7.1	Opening the Settings Sidebar	92
10.7.2	Changing Parsing Rules	92
10.7.3	Parsing Date/Time Overrides.....	96
10.8	Exporting / Printing	97
11	Using Attributions	99
11.1	Layout.....	99
11.2	Attribution Functions	100
11.3	Splitting Attributions.....	102
11.4	Grid and Controls	104
11.4.1	Generic Grid Controls.....	104
11.4.2	Attribution Data Grid	104
11.4.3	Right-click Menus	106
11.4.4	Edit Attributions popup	106
11.4.5	New Identifier	110
11.4.6	Importing Attributions.....	111
11.4.7	Auto Attribution.....	115
11.4.8	Edit Style	115
11.4.9	Decode SMS Platform Identifiers.....	116
11.4.10	Print	117
11.4.11	Export.....	118
11.4.12	Clearing Attributions	118
11.4.13	Attribution Library.....	118
11.5	Attribution Report.....	121
12	Using the Right Sidebar	122
12.1	Selecting the Filters Tab.....	122
12.1.1	Case-wide Filter (Off/On) Function.....	123
12.1.2	Source Data	123
12.1.3	Saving and Opening a Case Snapshot	123
12.1.4	Cell Logic	126

12.1.5	Date & Time	127
12.1.6	Locations.....	129
12.1.7	Event Types	130
12.1.8	Quick Filters.....	131
12.2	Selecting the Settings Tab.....	132
12.2.1	Case Wide Settings.....	132
12.2.2	Case Hub Settings.....	132
12.2.3	Data Display	135
12.2.4	Matching	136
12.2.5	Redaction.....	139
12.3	Selecting the Export Tab.....	140
12.3.1	File Export.....	141
12.3.2	Printing	141
13	Using Case Dashboards	142
13.1	Dashboard Controls	142
13.1.1	Widget Controls.....	142
13.1.2	Grid Controls.....	143
13.1.3	Data Selection and Filtering	143
13.2	General Investigation Dashboard	144
13.2.1	Exporting / Printing.....	145
14	Using Case Hub	147
14.1	Layout.....	147
14.2	General Operation.....	148
14.3	Using the Grid	148
14.3.1	Viewing Data	148
14.3.2	Grid Controls and Filtering	148
14.3.3	Changing Views and Column Layouts	149
14.3.4	Grid Right-click Menus	149
14.3.5	Changing Between Multi row and Single row Views.....	158
14.4	Using Lookup in NMPR	160
14.4.1	Overview.....	160
14.4.2	Setting Up the NMPR Feature	161
14.4.3	Launching an NMPR Lookup.....	162
14.4.4	Exporting NMPR Lookup Results	164

14.4.5	NMPR Data Exports in Case Outputs.....	165
14.5	Using Lookup in CSAS Cases	168
14.6	Using Mapping	168
14.6.1	Map Controls.....	168
14.6.2	Map Settings.....	169
14.6.3	Viewing Data	178
14.6.4	Right-click Menus	178
14.6.5	Cell Visualisations.....	183
14.6.6	Map Labels	187
14.6.7	Map Label Templates	191
14.6.8	Icon Styles.....	193
14.6.9	Map Styles.....	198
14.6.10	Location Search	199
14.6.11	Marquee Select.....	201
14.6.12	Layers, Locations and Events	202
14.6.13	Animation	212
14.6.14	Location Export & Import.....	215
14.6.15	Using Live GPS Import	217
14.6.16	Device Location Visualisation	224
14.6.17	Centroids	228
14.6.18	Heatmap Mode	230
14.7	Using the Details Panel	231
14.7.1	Locations.....	231
14.7.2	Top Cells.....	231
14.7.3	Nominals.....	232
14.7.4	CellView.....	234
14.7.5	RF Survey.....	236
14.7.6	Show/Hide Tabs.....	237
14.8	Using Case Snapshots.....	238
14.9	Using Map Exports	240
14.9.1	Export As an image	240
14.9.2	Export To Powerpoint.....	240
14.9.3	Export To KML/KMZ	240
14.10	Using New Map	242

14.11	Using CellView	244
14.11.1	How is the Data Gathered	244
14.11.2	Output Examples	244
14.11.3	Caveats and Limitations.....	245
14.11.4	Preparation	247
14.11.5	Using CellView	247
14.11.6	Using CellView Lookup Process.....	249
14.11.7	Understanding Coverage Visualisation	250
14.11.8	Getting the Best Results.....	251
14.12	Time Offset, Merging and Adjustment.....	253
14.13	Using Cell Confidence	256
14.14	Printing / Exporting	258
15	Using Case Outputs.....	260
15.1	Layout.....	260
15.2	Creating a New Output File	261
15.3	Grids and Controls	261
15.3.1	Grid and Column Controls	262
15.3.2	Grid Right-click and Actions Menu	263
15.3.3	Template Panel Right-click Menus.....	264
15.3.4	Options Tab.....	264
15.3.5	Sidebars	264
15.4	Output Formats	265
15.4.1	Selecting Templates	265
15.4.2	Selecting Fast Time Reports.....	267
15.4.3	Selecting User Templates.....	270
15.5	Deleting a Case Output.....	271
15.6	Template Builder	272
15.6.1	CSAS Templates	272
15.6.2	Template Builder Layout & Controls.....	273
15.6.3	Template Formatting.....	275
15.6.4	Headers & Footers	276
15.6.5	Repeat Column Header Row	276
15.6.6	Sheet Types.....	277
15.6.7	Template Description.....	278

15.6.8	Field Lists.....	279
15.6.9	Excel Formula Field Tags	280
15.6.10	Add Formulas Panel	281
15.7	Exporting / Printing	285
16	Using Case Cells	286
16.1	Hierarchical View of Cell Records	286
16.2	Layout.....	287
16.3	Viewing and Updating Cell Records.....	288
16.4	Grids and Controls	288
16.4.1	Grid and Column Controls	288
16.4.2	Grid	288
16.4.3	Right-click and Actions menus	289
16.4.4	Case Cells Detail panel.....	289
16.4.5	Choosing Different Views	290
16.4.6	Sidebars	290
16.5	Editing Case Cell Records	290
16.6	Manual Override Records	291
16.7	Defining O2 3G SAC Cells	292
16.8	Printing and Exporting	294
17	Using Analytics	295
17.1	Layout.....	297
17.2	Grids and Controls	298
17.2.1	Grid Columns and Layout Controls.....	298
17.2.2	Controls.....	298
17.2.3	Sidebar Tabs	298
17.2.4	Using Drilldowns	299
17.2.5	Report Grid Right-click Menus	299
17.2.6	Selecting and resizing panes.....	301
17.3	Using the Activity Hotspot query	302
17.3.1	Supported Data Types	302
17.3.2	Layout.....	302
17.3.3	Filters & Controls	303
17.3.4	Understanding the results.....	304

17.4	Using the Average Event Distribution query	306
17.4.1	Supported Data Types	306
17.4.2	Layout.....	306
17.4.3	Filters & Controls	306
17.4.4	Understanding the results	308
17.5	Using the Cell Usage query	309
17.5.1	Supported Data Types	309
17.5.2	Layout.....	309
17.5.3	Filters & Controls	312
17.5.4	Understanding the results	314
17.6	Using the Concurrent Calls query	317
17.6.1	Supported Data Types	317
17.6.2	Layout.....	317
17.6.3	Filters & Controls	318
17.6.4	Understanding the results	319
17.7	Using the Contact Summary query	321
17.7.1	Supported Data Types	321
17.7.2	Layout.....	321
17.7.3	Filters & Controls	323
17.7.4	Understanding the results	323
17.8	Using the Contact Summary by Date Range query 325	
17.8.1	Supported Data Types	325
17.8.2	Layout.....	325
17.8.3	Filters & Controls	327
17.8.4	Understanding the Results	329
17.9	Using the Contacts Between query	332
17.9.1	Supported Data Types	332
17.9.2	Layout.....	332
17.9.3	Filters & Controls	334
17.9.4	Understanding the results	335
17.10	Using the Correlation query	338
17.10.1	Supported Data Types	338
17.10.2	Layout.....	338

17.10.3	Filters & Controls	341
17.10.4	Understanding the results	341
17.11	Using the Drug Line Analysis query	341
17.11.1	Supported Data Types	343
17.11.2	Layout.....	343
17.11.3	Filters & Controls	344
17.11.4	Understanding the results	346
17.12	Using the First Cell Last Cell query	349
17.12.1	Supported Data Types	349
17.12.2	Layout.....	349
17.12.3	Filters & Controls	351
17.12.4	Understanding the results	352
17.13	Using the IMEI Summary query	355
17.13.1	Supported Data Types	355
17.13.2	Layout.....	355
17.13.3	Filters & Controls	356
17.13.4	Understanding the Results	357
17.14	Using the Inactivity Chart query	360
17.14.1	Supported Data Types	360
17.14.2	Layout.....	360
17.14.3	Filters & Controls	361
17.14.4	Understand the results	361
17.15	Using the Pivot Builder query	363
17.15.1	Supported Data Types	366
17.15.2	Layout.....	366
17.15.3	Filters & Controls	368
17.15.4	Understanding the results	371
17.16	Using the Potential Colocation query.....	372
17.16.1	Potential Colocation.....	373
17.16.2	Use Cases	376
17.16.3	Supported Data Types	379
17.16.4	Layout.....	379
17.16.5	Filters & Controls	380
17.16.6	Comparing using End Cells / Locations	383

17.16.7	Colouring.....	385
17.16.8	Selecting Different Modes	386
17.16.9	Selecting Data and Group Options	387
17.16.10	Running a Prebuilt Query.....	387
17.16.11	Customising the Grid Layout	387
17.16.12	Generating Co-location Data.....	388
17.16.13	Understanding the results.....	388
18	Case Reports.....	394
18.1	Disclosure Report	394
18.1.1	Setting Disclosure Status	394
18.1.2	Reviewing Disclosure Data.....	395
18.1.3	Creating a Disclosure Report.....	395
18.2	Phone/Attribution/File Summary.....	396
18.3	Continuity Log	397
19	Case Audit	398
19.1	Layout.....	398
19.2	Filters & Controls	399
20	RF Survey	400
20.1	RF Survey Module.....	400
20.1.1	Opening the RF Survey module.....	401
20.1.2	Importing RF Survey Data	402
20.1.3	Exporting Data to View in Case Hub	403
20.1.4	Viewing RF Survey coverage data in Case Hub	404
20.2	RF Survey Tab.....	405
21	Logging Out and Closing CSAS	406
22	Hybrid Mode	408
22.1	Switching Modes	408
22.2	Online Mode.....	409
22.2.1	CSAS Login.....	410
22.2.2	Open Cases.....	410
22.2.3	Case Search.....	410
22.2.4	Creating a New Case	410
22.2.5	Opening an Existing Case	410
22.2.6	Checking Out a case.....	411

22.2.7	Managing Cases	411
22.2.8	Checking out a Floating Licence	412
22.2.9	Checking server connection & case status	412
22.3	Offline Mode	413
22.3.1	Switching back to online mode	413
22.4	CSAS Server Administration.....	414
22.4.1	Logging in to CSAS Server.....	415
23	Training & Support	420
23.1	Training.....	420
23.1.1	Recommended Technical Pre-requisite courses	420
23.1.2	Training Pathway for New CSAS users.....	420
23.1.3	Training Pathways for Existing CSAS users	421
23.2	Support.....	421
24	Troubleshooting	422
24.1	Help & Support.....	422
24.1.1	Where to Get Help	422
24.1.2	How To...Contact CSAS Support.....	422
24.1.3	Accessing the Secure Support website.....	422
24.2	Common Issues	423
24.2.1	Updating the CSAS Application	423
24.2.2	CSAS Version Numbers	423
24.3	Licensing Issues	424
24.3.1	Checking Licence Details	424
24.3.2	Expired Licence.....	424
24.3.3	Online Activation – Licence does not Exist	424
24.3.4	Floating Licence Unavailable	424
24.3.5	Floating Licence Server Unavailable	425
24.3.6	Check out a Floating Licence	425
24.3.7	No access to expected features	425
24.4	User & Team Management Issues	426
24.4.1	User can't view expected case(s)	426
24.4.2	Expected results not appearing in case search	426
24.4.3	Moved to a new Team, can't see old cases	426
24.5	Starting CSAS	427

24.5.1	Unable to open CSAS	427
24.5.2	Forgotten username or password	427
24.6	Case Creation & Management Issues	428
24.6.1	In Standalone mode, can't see other users' cases.....	428
24.6.2	CSAS won't allow a new case to be created	428
24.6.3	Existing case name clashes with a new case	429
24.6.4	Cases no longer needed	429
24.6.5	Change prefilter dates after a case has been created	429
24.7	Import Files Issues	430
24.7.1	'Unrecognised' Files	430
24.7.2	'Not Imported' Files	431
24.7.3	'Not Parsed' Files.....	431
24.7.4	How To...Use the Support Rescue Formats.....	432
24.7.5	How To...Check Imported File Details	434
24.7.6	How To...Update File Details	434
24.7.7	How to...add a missing subject for a handset download	435
24.7.8	How to...vary the processing rules for a file	435
24.7.9	'Missing' events	436
24.7.10	Unable to View Imported Files	437
24.7.11	Deleting & Re-importing Files	437
24.7.12	Special Handling for .csv Files	437
24.7.13	Sending Unrecognised/Unloaded Files to CSAS Support	438
24.7.14	Anonymising Files before sending them to Support	438
24.7.15	Recognising Handset Download files.....	438
24.8	Attributions Issues.....	443
24.8.1	Clear an incorrect attribution	443
24.8.2	Import attributions from a non-standard Excel file	443
24.9	Dashboard Issues	443
24.9.1	No data appearing in the Dashboard	443
24.10	Case Hub Issues	444
24.10.1	No data appearing in Case Hub	444
24.10.2	Cell Address Details Not Being Displayed	444

24.10.3	Invalid Date Formats	445
24.10.4	Incorrect Data Appearing in Columns	445
24.10.5	'Missing' Text Messages	446
24.10.6	'Incorrect' Timestamps	447
24.10.7	Timing Advance 'point locations' not appearing	447
24.11	Case Outputs Issues.....	447
24.11.1	No data appearing in Case Outputs template	447
24.11.2	Template Files Corrupted	448
24.12	Analytics Issues.....	448
24.12.1	No data appearing in the selected Analytics query.....	448
24.13	CellView Issues	449
24.13.1	CellView tab not visible	449
24.13.2	No CellView results returned for a cell	449
24.13.3	No CellView results returned for any cells	449
24.14	RF Survey Issues	449
24.14.1	RF Survey tab not visible	449
24.14.2	No RF Survey results returned for a cell	449
24.15	Case Cells Issues	450
24.15.1	Understanding Cell ID Formats	450
24.15.2	Converting Between Decimal & Hexadecimal.....	450
24.15.3	Special handling for Hexadecimal Cell IDs	451
24.16	Miscellaneous.....	451
24.16.1	Moving to a new PC	451
24.16.2	I've moved to a new PC, but can't find my CSAS cases	452
25	Glossary.....	453

1 User Guide Overview

This User Guide is organised in a standardised way, with sections that contain different types of information, identified using different icons:



WHY is the task necessary?



WHEN should the task be done?



WHO should do the task?

Sections start with a description about **WHAT** the function of a task is, and an overview of **WHAT** it does. No icon has been used for **WHAT**.

The 'WHO' entry indicates whether a CSAS user, administrator or support person would usually perform the function. The hierarchy of users employed in this guide is as follows:

- CSAS Support/Operations – related to installing CSAS and CSAS Server.
- Local IT Support – related to installing CSAS and CSAS Server.
- Local CSAS Administrator – related to licensing and updates.
- CSAS User – for all other functions.

Where appropriate, a section may also include details of:

- the Stepped Procedure necessary to accomplish a task.
- any Troubleshooting steps that can be taken if problems are experienced with a task.
- a link to an explanatory video clip – help videos are hosted in the CSAS online training portal, clips will only be available if the portal is accessible from your location.
- links to other relevant sections of the user guide.

2 CSAS Product Description

CSAS is a software tool that has been designed to streamline cell site analysis and general digital forensics work by automating many of the basic data handling processes.

The tool allows you to perform:

- » Source data handling and processing.
- » Mapping of processed data.
- » Analysis of processed data.
- » Creating reports and court exhibits from imported data.

The main task performed by CSAS is to automate the task of processing ('parsing' or 'cleansing' as it is sometimes known) call detail records (CDRs) and other forms of digital evidence into a common, usable format.

In many jurisdictions, cellular service providers (CSPs) are obliged to provide CDR information to relevant authorities on request. In the UK, this process is managed under IPA (Investigatory Powers Act) legislation. Other forms of digital evidence are provided under separate legislation, such as the Data Protection Act (DPA).

Different CSPs employ different CDR record formats, meaning that investigations that encompass data from more than one CSP are required to deal with sets of data that may be presented in a number of different and incompatible formats.

The process of 'parsing' these data records into a common and usable format using manual techniques can be laborious and time consuming. The use of manual processes also introduces the possibility of data processing mistakes or omissions due to understandable human error. Some organisations have developed their own macros or data processing applications, but these require on-going maintenance and upgrades to accommodate new source data formats.

CSAS imports source data records presented in a variety of formats - all current and most historical UK CDR formats are currently supported, as are many non-UK CDR formats, many formats of ANPR/ALPR data can be handled, as can the most commonly used handset download output formats and a variety of other source data types. CSAS automatically 'parses' or processes source data files into a common format, stores the data in a database and makes it available for viewing and analysis by analysts, investigators and other digital forensics professionals.

Once you have created the required basic or filtered datasets they can be mapped and analysed within CSAS or can be exported or output to Microsoft Excel or other formats for further external analysis. CSAS supports a number of prebuilt output templates and new or bespoke format templates can be easily created and added to the system.

CSAS also supports the creation of 'Exhibit' format workbooks, which can be used to create 'printer- friendly' and 'court-ready' call schedules that have headers/footers, page numbers and other details pre-formatted. The Exhibit format set also includes examples of the 'single line' presentation format favoured by some analysts and police forces as well as the 'multi row' formats preferred by some independent expert witnesses.

assigning specific colours to significant subject (or 'target') phone numbers and other

identifiers (IMEIs, IMSIs, vehicle registrations, etc) and also allows you to add attribution details (the names of the alleged users of each significant phone or other identifier) which can be included in Exhibit format output reports.

2.1 CSAS Product Range

CSAS forms part of a wider, integrated product range. More details can be found at www.forensicanalytics.co.uk/solutions/.

2.1.1 CSAS

CSAS is a mature and proven technology trusted by analysts and investigators to automate the processing and analysis of time-critical comms data.

CSAS recognises and imports over 400 CDR, handset download, ANPR, telematics, tracker and other formats, typically at a rate of over 1000 events per second.

Other time-consuming aspects of data analysis are also automated, including creating maps, running analytical queries and creating call schedules for both intelligence and court use.

2.1.2 CSAS RF Survey

CSAS RF Survey is an extra licensable module in CSAS that deals with the measurement logs captured during forensic radio surveys. RF surveys capture details of the set of cells that provide coverage at a surveyed location or can be used to map to coverage footprint of individual cells. These details can then be used in conjunction with evidence provided by call records to give an accurate real-world view of where cells used by suspects' phones provide coverage. Forensic RF surveys are useful in that they can provide empirical evidence to show where a suspect could have been located when they were connected to a cellular network.

2.1.3 CellView

CellView is an extra licensable feature within CSAS that makes use of crowd-sourced cell coverage data to provide an 'intel only' view of the areas covered by particular cells. Although it cannot be viewed as being as evidentially robust as RF Survey data, CellView has the benefit of being available immediately, without having to wait for the results of an RF survey to be provided, meaning that CSAS users can get an instant idea of the approximate coverage area of a cell used by a suspect's phone.

2.1.4 CSAS Server

CSAS Server enables seamless case sharing and collaboration between CSAS users within an organisation.

Standalone CSAS instances create their own local database and store their users' cases and case data locally. CSAS Server hosts a central case database for an organisation in which all cases, imported source data and analytical results are stored.

Users are able to log in to their CSAS Server account from any CSAS client within their organisation and can therefore work on their cases and data from any suitably equipped machine within their network.

2.1.5 CDAN Nexus

Most LEAs (Law Enforcement Agencies) have historical stores of digital forensics data that may never have been centrally processed and analysed in a methodical way.

CDAN Nexus shares the same data processing functions as CSAS and can import and can be set to automatically work through new and historical data files and normalise them into usable data. Imported data is indexed to make it instantly searchable – bringing details of much of an organisation's store of digital forensics data to users' fingertips.

The process creates an indexed database of historical data organised on a case-by-case basis. Once the Index is available, CDAN Nexus allows users to search for identifiers and highlights the coincidence of phone numbers, IMEIs and IMSIs across different cases, allowing investigators to see links and patterns that may not previously have been visible.

2.1.6 CSAS Product Integration

The elements of the CSAS product range integrate to provide a full end-to-end solution:

- » CSAS can be deployed to as many workstations as required within an organisation.
- » smaller organisations are able to deploy CSAS in standalone mode, but larger organisations will generally enhance CSAS with the collaborative capabilities of CSAS Server.
- » CDAN Nexus is also able to be deployed as a standalone system – either to provide accessed to 'cleansed' data and standard reports or to process data to be ingested by another vendor's analytical system – or as part of a wider CSAS environment.
- » CDAN Nexus and CSAS complement each other within an organisation, with CDAN Nexus providing centralised index and search functions and CSAS supporting analysts and investigators who are working on complex cases.

2.2 Accessibility

Forensic Analytics has conducted an independent assessment of the CSAS V3 application against the Web Content Accessibility Guidelines (WCAG) 2.2.

The assessment identified several accessibility issues. Notably, given the complexity of the analytics and mapping, much of the user interface cannot be operated using only a keyboard. In addition, users may find that significant portions of content are announced unexpectedly when navigating with a screen reader.

The development team are in the process of reviewing the results and prioritising time and resources to address the specific issues identified. It is expected that accessibility issues will be rectified during future release cycles along with prioritised functional enhancements."

3 Installing CSAS

This section is intended to show you how CSAS is typically installed, using various installation wizards.

You will use the following phases to install and configure CSAS:

- » CSAS v3 Setup - allows you to select where the CSAS installation files and the case folder will be saved, you will also configure the mode CSAS will operate in – standalone (where each individual copy of CSAS operates separately), server (where copies of CSAS within the same organisation are linked via a CSAS Server) or a mix of both.
- » CSAS Local Startup Wizard - allows you to select the country in which CSAS will be operating and other basic operating parameters.
- » Licence Wizard - allows you to get CSAS activated using a licence code.

3.1 Downloading CSAS Installer

If you manage your own software installs, the CSAS installer file can be downloaded from the Forensic Analytics secure Customer Portal at secure.forensicanalytics.co.uk (username and password can be obtained from CSAS Support).

Once logged in, click on Downloads in the left sidebar, then set the 'All Types' dropdown to 'Software Package' and the 'All Products' dropdown to 'CSAS v3' and the latest version of CSAS will be listed and available for download.

The CSAS installer file should be saved to the host PC before installing – installer files will be named using the format 'CSAS_V3_Installer_Version....msi' – double-click on the file to begin the installation. Details of the process to follow are provided below.

NOTE – you must have Administrator permissions on your PC to install CSAS – this may be a task that is performed by your organisation's IT team instead.

3.2 Host PC Requirements

CSAS operates on a Windows PC platform only – it has been tested on all Windows releases from Windows 10 upwards.

The host PC upon which the CSAS application is deployed must have the following minimum specifications:

- Windows 10 or higher.
- Intel i5 processor or higher.
- 8GB RAM or higher.
- At least 1GB of available space on the hard disk.
- Microsoft .NET Framework v8.

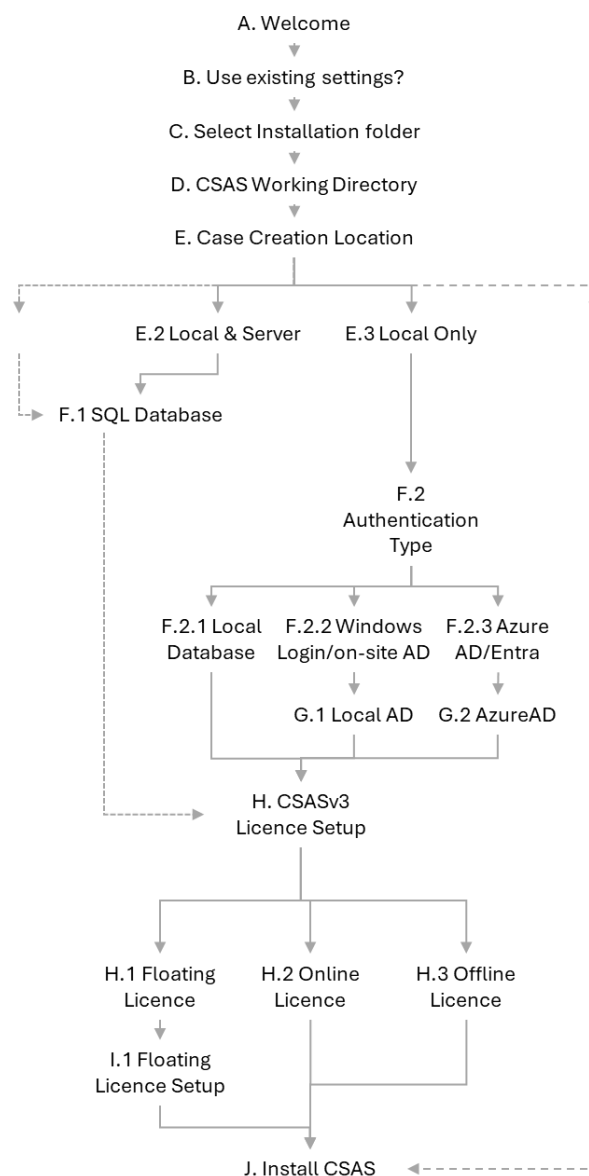
CSAS users require access to the folder in which the CSAS database and case folders are stored – this defaults to the user's AppData\Roaming folder but can be defined elsewhere during installation. Network share or cloud-based folder locations for the CSAS database are not recommended for host PCs that are likely to occasionally lose network connectivity (e.g. laptops).

More details can be found in the document *0388-TECH CSAS v3 Technical Description* which is available from the CSAS Support website.

3.3 Initial Install

3.3.1 Installing CSAS

A standard initial installation progresses is described below; details of upgrades and reinstallations will be covered later.

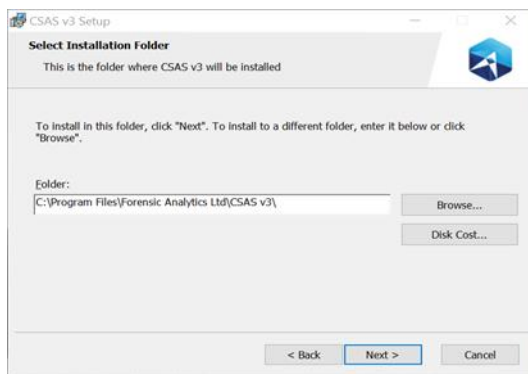




A - Welcome. Double-click on the installer file and the install wizard will open.

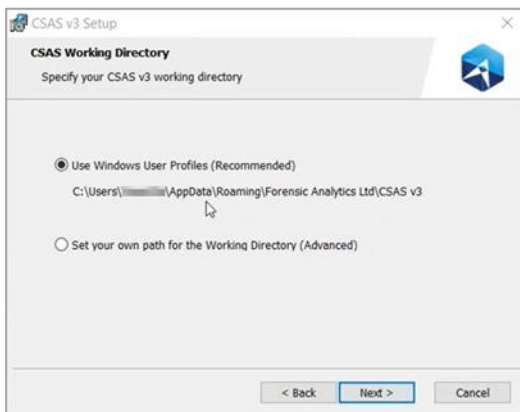
In each screen, click 'Next' to continue, 'Back' to return to the previous screen and 'Cancel' to close the installer with abandon the install.

You will be asked to make several choices during the install, the answers to which will be provided by your IT team or CSAS Support.



C - Installation Folder. You'll be asked to confirm the location for the CSAS programme files – the default location for this is the C:\Program Files\CSAS v3\ folder.

The default location is recommended unless there is a compelling technical reason to install the program elsewhere.



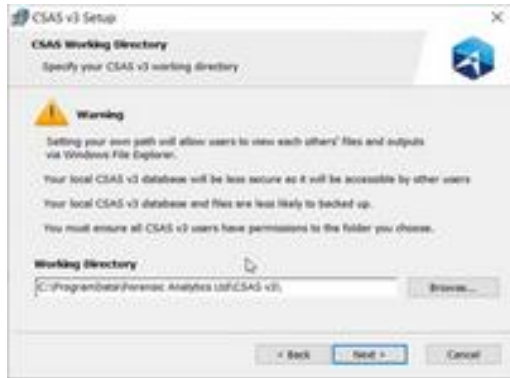
D - CSAS Working Directory. CSAS creates a folder in which to store its local database and copies of the source input files and created output reports and maps.

The default location for this is

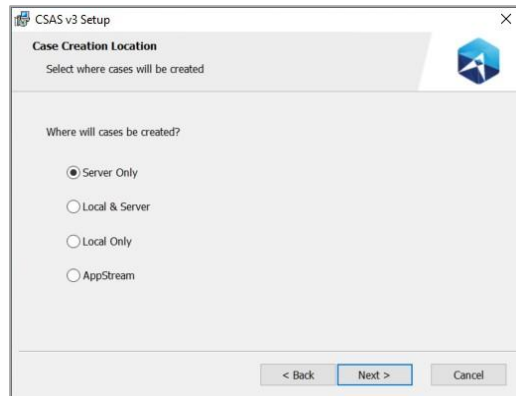
C:\Users\< user > \AppData\Roaming

It is possible to specify a folder location elsewhere on the host PC, if required.

The storage folder location must be set during installation and cannot be changed later without uninstalling and reinstalling CSAS again. Although this means that it is possible to select a network share location (or a cloud backup application, such as Dropbox or Box) in which to store the CSAS database this is not recommended as network lag and conflicts with other applications attempting to access that folder could severely impact CSAS performance.

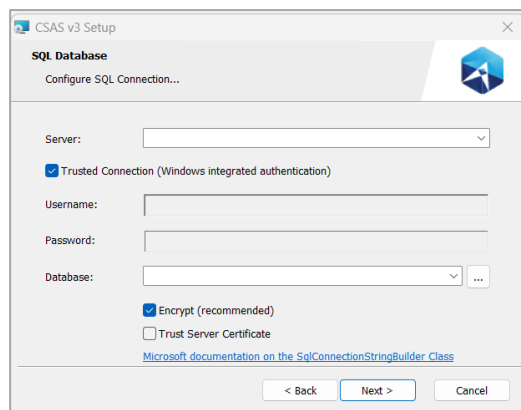


If you choose a custom location for the CSAS case folder, be aware that for standalone deployments on shared PCs (where multiple users might have their own separate CSAS installations), any case folder location other than the default might lead to users being able to access each other's case folders using Windows Explorer.



E – Create Case Locations. This option specifies where CSAS case data will be stored – cases can be saved to the local CSAS database (on the host PC), they can be saved to a CSAS Server database (within your organisation's network) or they can be saved to the cloud (if your organisation uses a cloud deployment).

Your IT team will tell you which mode your organisation uses



F.1 server only option

If selected, all case data will be stored on CSAS Server and cases cannot be downloaded to be worked on offline.

For this option you will need to enter:

Server address

User's log in credentials

Database name

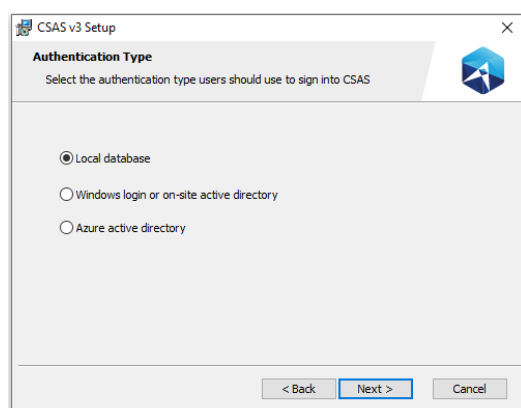
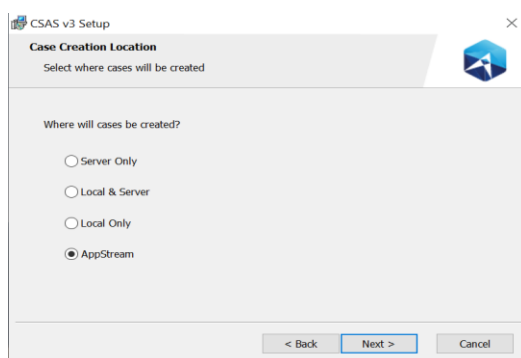
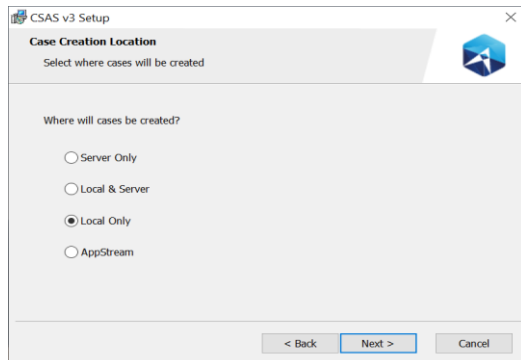
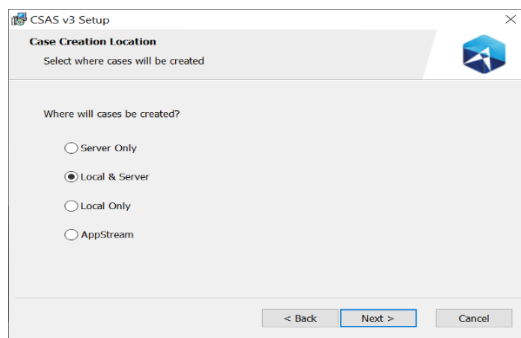
The server address will generally be an IP address optionally followed by a port number – e.g. 10.10.10.10,1234.

If the Trusted Connection option is ticked, the server log in details will be added automatically – if you have specific database username/password details, untick this option and enter the details manually.

If the database name (usually 'CSASIdentity') doesn't populate automatically, click on the three dots next to the database name dropdown and select the database from the list – it might take several seconds to populate list as the installer logs on to the server and retrieves the details.

It is highly recommended that you leave the 'Encrypted' option ticked, to protect the connect to the database. If your CSAS Server is operating without a security certificate or is using a locally configured certificate, check the 'Trust Server

Certificate' option.



E.2 - local & server option

If selected, cases can be saved to either the local database or CSAS Server.

You'll be asked to provide server details, as in F.1 above, and local database details, as below.

E.3 - local only option

In this mode, you'll only be able to work in Standalone mode, with cases saved to the local database - there will be no option to use CSAS Server.

If either local mode option is selected, you'll be asked to create a username and password to use for local database authentication in a later step.

E.4 - Cloud option

The AppStream option relates to a cloud-based deployment option, which will generally be set up by CSAS Operations.

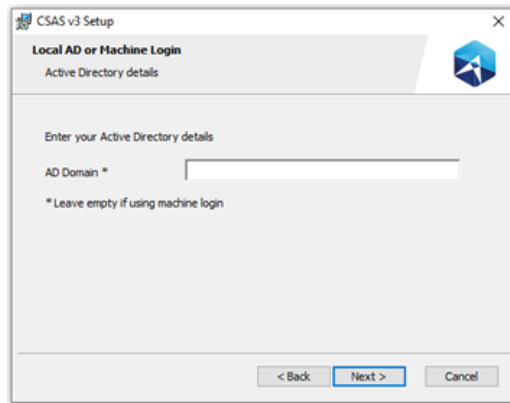
F.2 - Authentication Type. This screen sets the authentication to be used for a local database, with options of:

Local database, where you'll set your own local username and password

Windows login or on-site active directory, where you'll re-use your local Windows login details

AzureAD (or Microsoft Entra), where you'll re-use your organisation's log in details

If you select Local Database, you'll be asked to set up your username and password in the Local Startup Wizard, that runs once the installer has finished.



CSAS v3 Setup
Local AD or Machine Login
Active Directory details

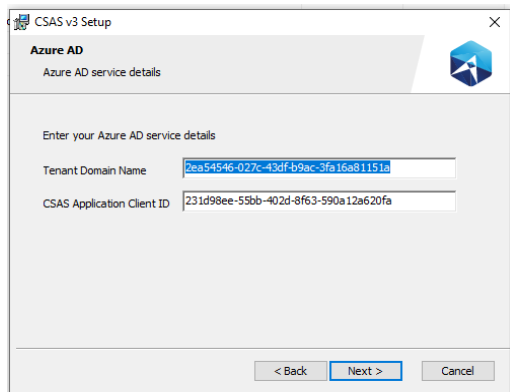
Enter your Active Directory details

AD Domain *

* Leave empty if using machine login

< Back Next > Cancel

G.1 – Local AD or Machine Login. If you selected Windows Login or on-site Active Directory as the Authentication Type in screen F.2, this screen will ask you for your local AD Domain details – your IT team can help you with these details if you don't have them.



CSAS v3 Setup
Azure AD
Azure AD service details

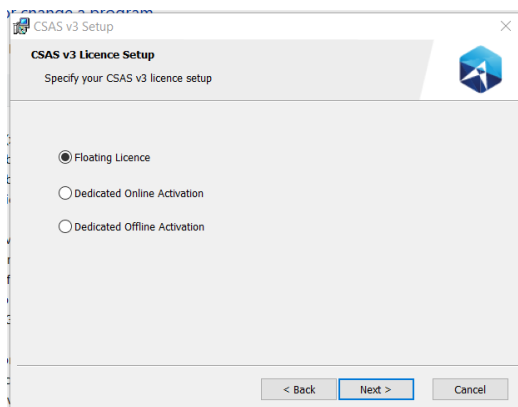
Enter your Azure AD service details

Tenant Domain Name

CSAS Application Client ID

< Back Next > Cancel

G.2 – Azure AD. If you selected 'Azure AD' as the Authentication Type in screen F.2, this screen asks you for your Azure AD (now called Microsoft Entra) details - your IT team can help you with these details if you don't have them.



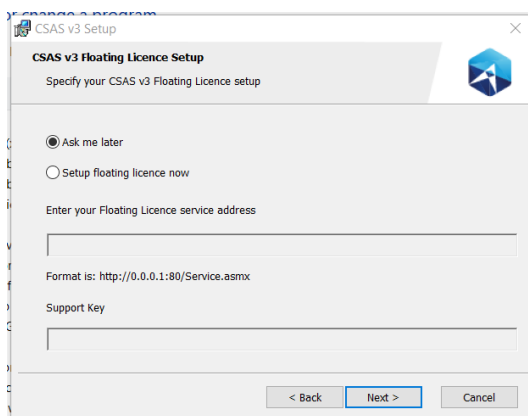
CSAS v3 Setup
CSAS v3 Licence Setup
Specify your CSAS v3 licence setup

☒ Floating Licence
☐ Dedicated Online Activation
☐ Dedicated Offline Activation

< Back Next > Cancel

H – Licence Setup. CSAS requires an activation licence to operate.

If you're using a floating licence, the details will be added in the next screen, if you are using the other options, the licence details will be entered in a later step, but CSAS needs to know at this stage which type of licence you will be using – please select one of the presented options.



CSAS v3 Floating Licence Setup
Specify your CSAS v3 Floating Licence setup

☒ Ask me later
☐ Setup floating licence now

Enter your Floating Licence service address

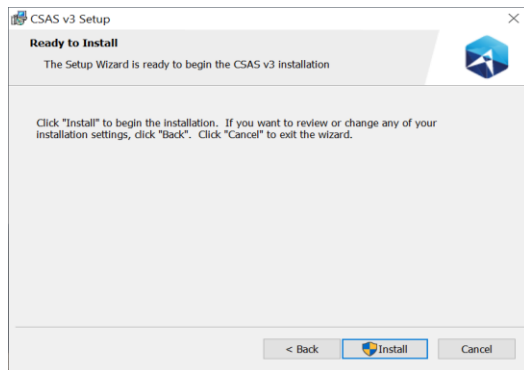
Format is: `http://0.0.0.1:80/Service.asmx`

Support Key

< Back Next > Cancel

I1 – Floating Licence Setup. If you selected the floating licence option in screen H, you can enter the details now or leave it until later.

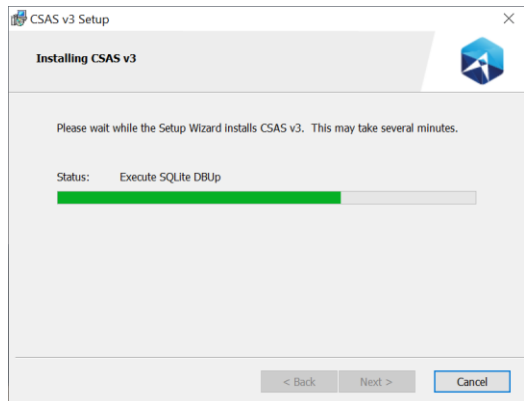
Your IT team or CSAS Support will provide you with the address of the server (in the format `https://0.0.0.1:80/service.asmx`) and also a support key, which validates the server address.



J - Install CSAS. Once all options have been correctly selected, click 'Install' to begin the installation.

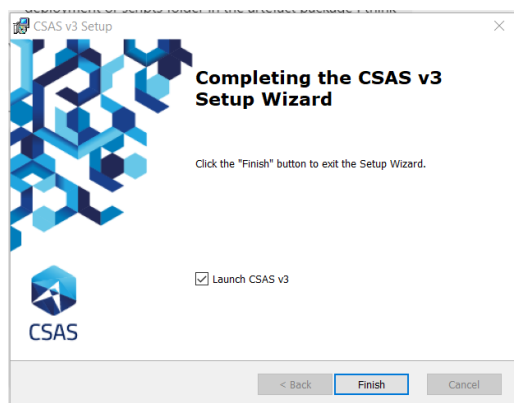
You may be required to confirm that you're happy to proceed with the installation and might have to provide administrator credentials before the process starts.

The screen will provide feedback on the progress of the install.



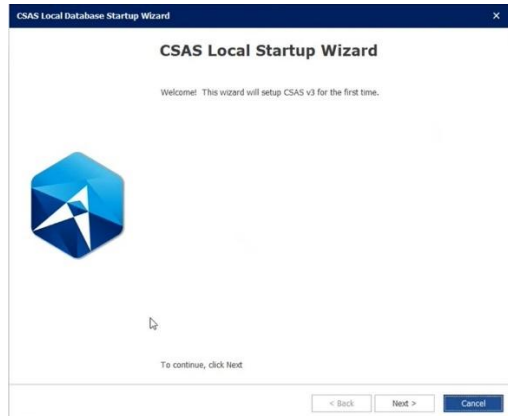
Once the install is complete, click 'Finish'.

The installer will close and the next stage of process will begin.



3.3.2 CSAS Local Startup Wizard

The Local Startup Wizard runs for a new installation; it is not required for an upgrade or reinstall. It captures details of the country CSAS will be operating in and, for Standalone deployments, allows you to create your CSAS login and password.



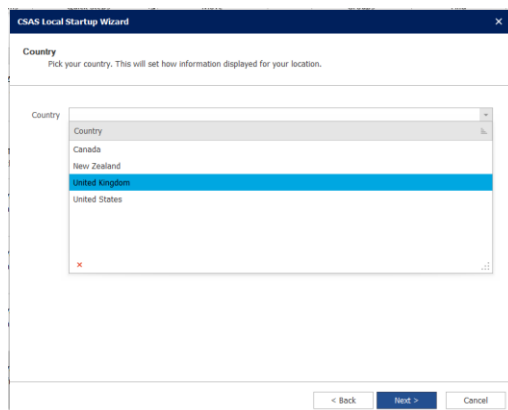
CSAS Local Startup Wizard

Welcome! This wizard will setup CSAS v3 for the first time.

To continue, click Next

< Back Next > Cancel

When the process starts, click 'Next' to continue.



CSAS Local Startup Wizard

Country

Pick your country. This will set how information displayed for your location.

Country

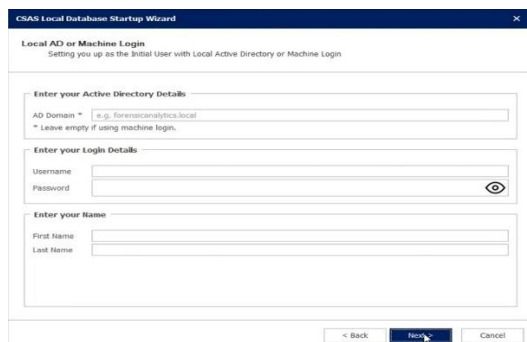
Canada
New Zealand
United Kingdom
United States

< Back Next > Cancel

Please select the country CSAS will be operating in.

This is used to set parameters such as 'home country' dialling prefix, time zone and date format.

If you selected the 'server only' option in the main installer, CSAS database details will have already been entered and the wizard will close at this point.



CSAS Local Startup Wizard

Local AD or Machine Login

Setting you up as the Initial User with Local Active Directory or Machine Login

Enter your Active Directory Details

AD Domain * [e.g. forensicanalytics.local]
* Leave empty if using machine login.

Enter your Login Details

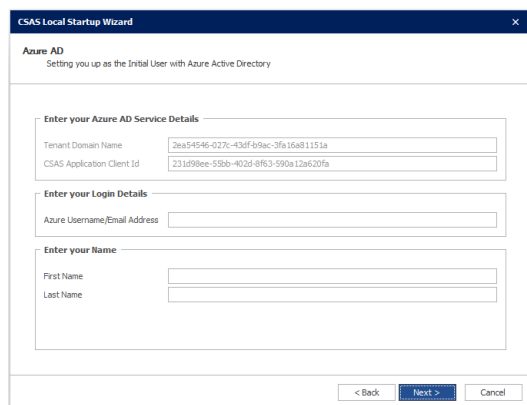
Username
Password

Enter your Name

First Name
Last Name

< Back Next > Cancel

If you selected 'Windows Login or Onsite Active Directory' please provide the required user details. Your local AD domain details will have been entered via the installer.



CSAS Local Startup Wizard

Azure AD

Setting you up as the Initial User with Azure Active Directory

Enter your Azure AD Service Details

Tenant Domain Name
CSAS Application Client Id

Enter your Login Details

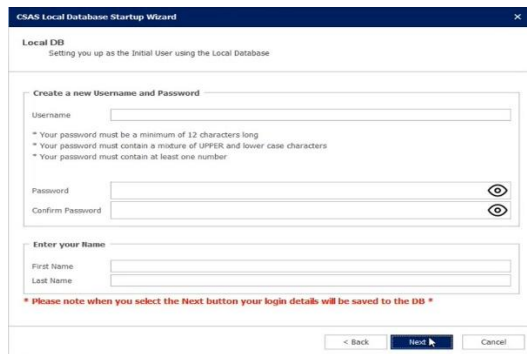
Azure Username/Email Address

Enter your Name

First Name
Last Name

< Back Next > Cancel

If you selected 'Azure Active Directory' (which is also known as Microsoft Entra ID), please enter the required user details. Your AAD domain and application ID will have been entered via the installer.



CSAS Local Database Startup Wizard

Local DB
Setting you up as the Initial User using the Local Database

Create a new Username and Password

Username:

Password: 

Confirm Password: 

Enter your Name

First Name:

Last Name:

* Please note when you select the Next button your login details will be saved to the DB *

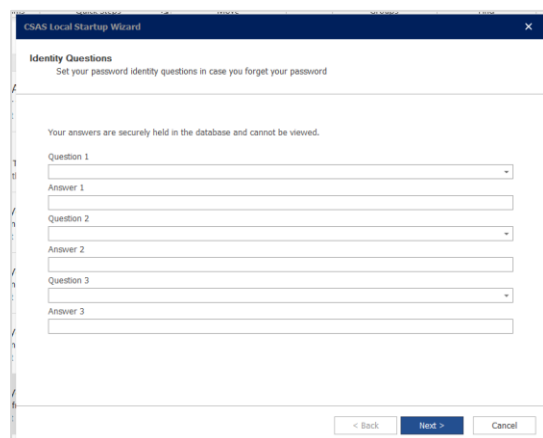
< Back Next > Cancel

If you selected 'local database' as the authentication type during the installation – which would be used for a basic Standalone deployment – please enter a username and password.

If these details haven't been provided to you, you could create your own – please make a note of the username and password you select, without them you won't be able to access CSAS

For the 'local database' option, you'll be asked to select three questions and provide answers – these will be used in the event that you forget your local CSAS password.

If you use the other authentication options (Active Directory or AzureAD) you'll need to contact your IT Team in the event that you forget the password you use to access CSAS.



CSAS Local Startup Wizard

Identity Questions
Set your password identity questions in case you forget your password

Your answers are securely held in the database and cannot be viewed.

Question 1:

Answer 1:

Question 2:

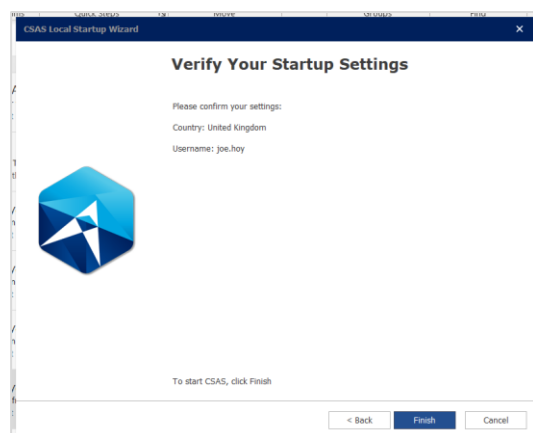
Answer 2:

Question 3:

Answer 3:

< Back Next > Cancel

The local setup is now complete, click 'Finish' to close the wizard and move on to the last step.



CSAS Local Startup Wizard

Verify Your Startup Settings

Please confirm your settings:

Country: United Kingdom

Username: joe.hoy



To start CSAS, click Finish

< Back Finish Cancel

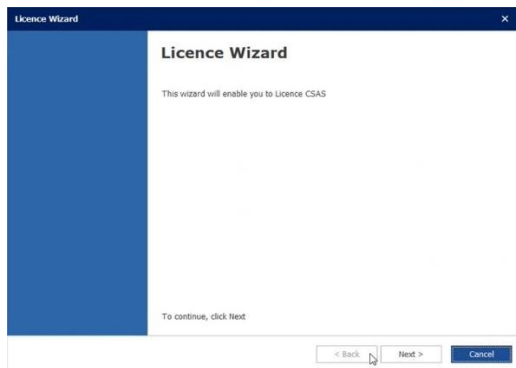
The default time zone and date format for your instance of CSAS is set during initial installation – CSAS reuses the current Windows time zone and 'culture' settings, which determine things like date format (dd/mm/yyyy, mm/dd/yyyy, etc). The time zone can be set to alternative values on a case-by-case basis via the [Manage Cases](#) menu. Date format can be changed by updating your Windows culture settings.

3.3.3 Licence Wizard

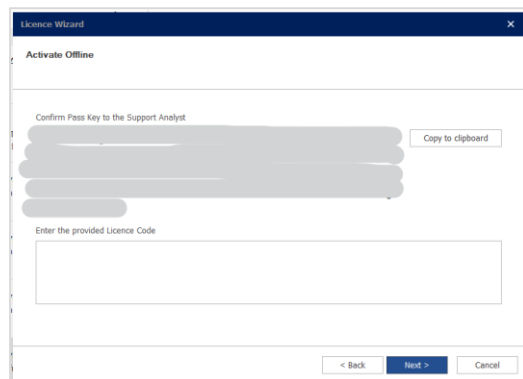
The Licence Wizard opens automatically after the Local Setup Wizard closes if no existing valid licence details can be found – it guides you through the process of adding an activation licence for your CSAS deployment.

Note: You only need to complete the Licence Wizard if you selected 'Use Online' or 'Use

Offline' licensing options from the CSAS v3 Licence Setup window in the installer.



Once the Licence Wizard opens, click 'Next' to continue.



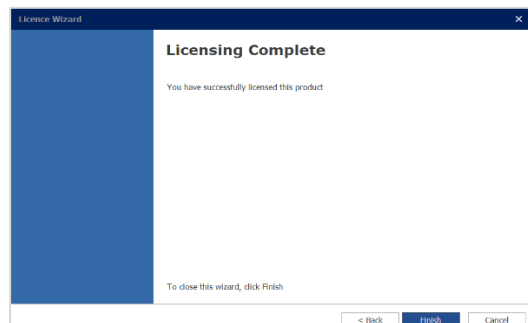
If you selected 'Dedicated Online Activation' in the installer, you will be asked to provide an online licence key.

This will be provided by your IT team or by CSAS Support.

Paste the provided key into the text box.

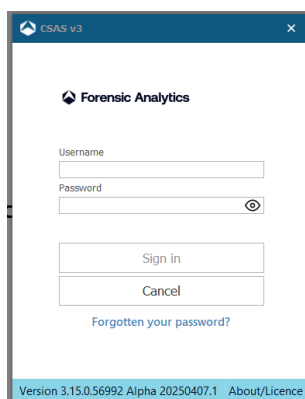
If you selected 'dedicated online activation' in the installer, you'll be presented with an almost identical screen – please paste the online activation key in the text box.

If you paste the activation key into the popup window, please check to make that no additional leading or trailing characters also get copied – such as trailing spaces or new line feeds – these could confuse the activation process.



If the keys were valid and were entered correctly, licensing will complete and CSAS will be available for use.

If the key activation fails, please rerun the key entry and make sure that no additional characters or spaces were entered.



Click the 'Finish' button.

The CSAS login window opens.

Enter your login credentials.

CSAS opens.

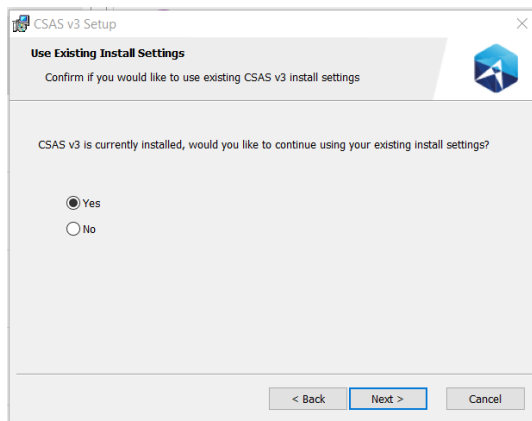
3.3.4 CSASv3 Upgrade

If CSAS has already been installed and you wish to install an updated version, the process is a truncated version of the one outlined above.

If none of the details of the installation have changed, if the authentication method remains the same, if the operating country and time zone are the same and if the licence is still valid, most of the steps performed during a fresh install can be skipped.



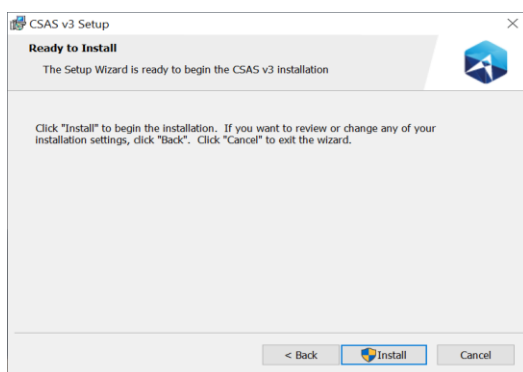
Double-click on the installer file to begin the upgrade process.



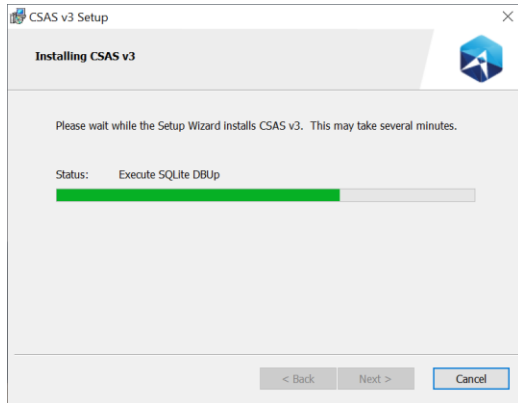
If the installer detects an existing version of CSAS, it asks whether you wish to install using the same settings.

If 'yes' the installer will go straight to the install phase.

If 'no' it will trigger the full installer process as outlined above.



You may be required to confirm that you're happy to proceed with the installation and might have to provide administrator credentials before the process starts.



The screen will provide feedback on the progress of the install.



Once the install is complete, click 'Finish'.

The installer will close and the next stage of process will begin.

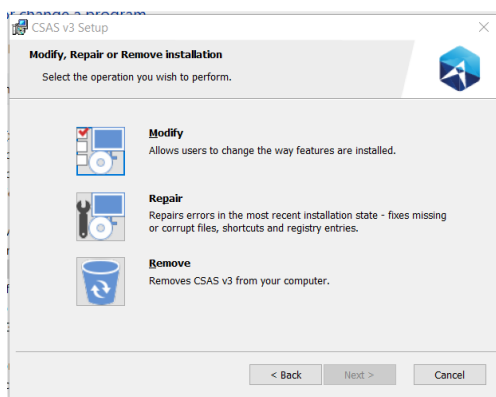
If the licence key and local setup details have not changed, you will be taken straight to the CSAS login screen.

3.3.5 Uninstall CSAS

CSAS can be uninstalled via the Windows Control Panel > Programs & Features option.



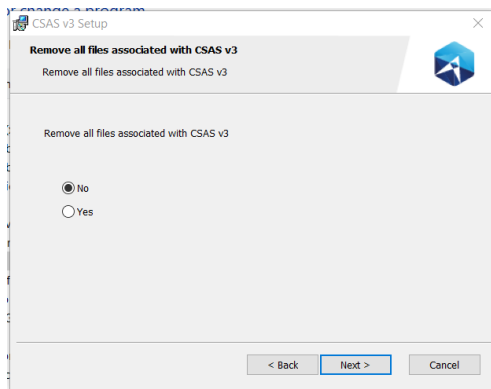
Once selected, the installer runs and you are offered three options:



Modify – lets you change key installation settings, such as authentication method

Repair – reruns the install to replace missing or corrupt files

Remove – uninstalls CSAS



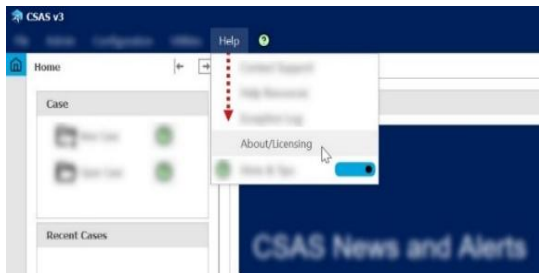
If the 'remove' option is selected, you'll be asked if you want to remove all files associated with CSAS – if you select 'yes', **this will remove all user folders, including the case folder and the local database and you will lose all locally saved CSAS cases.**

Please be careful when using this option.

3.3.6 Adding Additional Licences

The install process adds a CSAS activation licence, allowing the main CSAS application to operate. There are two optional features in CSAS that require additional licences – CellView and RF Survey.

Once you get logged into CSAS, if necessary, you can add a CellView and/or an RF Survey licence via the 'About/Licensing' option in the 'Help' menu (see *Top Row Buttons and Controls*):



When you click the 'About/Licensing' option, the 'About CSAS' pop-up window opens. To add a licence, see the *About/Licensing* section.

Why, When, Who

	This function is necessary to install and setup CSAS in the way that best suits the user and / or their organisation.
	This function is undertaken whenever you install a new or updated version of CSAS.
	This function is typically carried out by the following users:
	>> CSAS Operations >> IT Support >> CSAS administrator >> CSAS User (for small organisations with no IT team)

Stepped Procedure

The various procedures were outlined in the preceding sections.

Troubleshooting

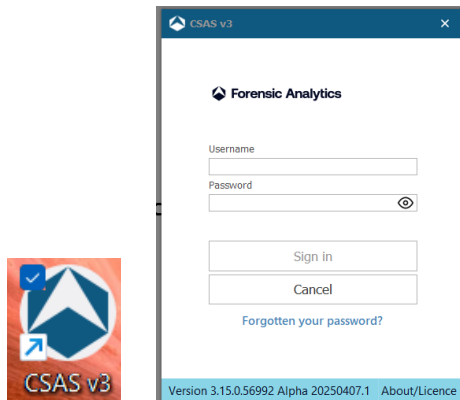
Most issues associated with installing or uninstalling CSAS relate to the lack of administration permissions or lack of required database credentials. Please ensure you have full details of the required configuration before starting the installer process.

See also

- >> Any CSAS configuration or setup details provided by your organisation.
- >> Any deployment installation notes provided by Forensic Analytics.

4 Opening CSAS and Logging In

This function allows you to start CSAS and enter your username and password to log in.



When the installation and setup wizards have finished, a CSAS shortcut icon will appear on your desktop.

Double-clicking on the icon opens the CSAS log in screen.

Enter your CSAS username and password.

If CSAS has just been installed, or if it has recently been updated, there may be some other pop-up messages that appear before the login screen opens, these messages relate to updates and checks that are being performed on the local CSAS database and are nothing to be concerned about.

Standalone Mode

In standalone mode, your username and password will have been setup during installation, along with a set of account recovery questions to be answered for a 'lost' password. If your password is lost and cannot be recovered, you won't be able to access CSAS and **all case data will be lost**, so it's important that you don't forget your password, or the answers to the recovery questions. If you forget your login password and CSAS is configured to operate in local only or local & server mode, the click on the 'forgotten your password' link to launch the password recovery questions.

Server Mode

In Server mode, your username and password are managed by your organisation's IT team and will be provided to you when your account is set up. If you forget your CSAS password in Server mode, you'll need to contact your IT team for help, CSAS Support have no access to your organisation's authentication system and will not be able to help.

Why, When, Who

	This function is necessary to validate that you're an authorised user of CSAS, to prevent unauthorised use of the system and to allow you access to the permitted functions CSAS.
	This function is undertaken whenever you log into CSAS
	This function is typically carried out by the following users:  CSAS User.

Stepped Procedure

1. In the name field, enter your CSAS username.
2. In the Password field, enter your CSAS password.
3. Click on the  button. The log in screen closes and the CSAS Home screen opens.

The exact log in behaviour is dependent upon how authentication has been configured for your system.

Troubleshooting

If the user Login attempt is unsuccessful this may be down to several possible reasons:

- » Incorrect Username or Password: Re-try the login procedure ensuring that the password was entered correctly (including any upper/lower case letters). Click on the 'eye' icon next to the password to check the entered text.
- » If you are sure that correct username and password were entered, please contact your local CSAS administrator for support.
- » If you are unsure of the correct password, select the 'Forgotten your password?' link if available and follow the on-screen instructions to re-set the password.
- » If CSAS is operating in Server mode and an online 'forgot password' function isn't available for your organisation, then you will need to contact your local CSAS administrator or IT Team to trigger a password reset.

Note: CSAS Support generally can't help with local password issues.

For information on common troubleshooting issues refer to *Troubleshooting*.

5 General Operation

CSAS activities are arranged around the concept of the 'Case':

- » Each case is created as a separate logical entity in the CSAS database and acts as a container for the data related to an investigation.
- » Each case can have one 'owner' at any one time, who has read and write permissions and is able to add or remove data from the case. In Server mode, each case can have any number of 'viewers', who have read-only access to the case and can't add or remove data. The case owner can be changed, allowing a different user to gain editing rights to the case if required.
- » Cases are created and linked to a Team – which could be a general team within an organisation or could be a team created for a specific purpose or investigation.
- » Individual CSAS users can be members of one or more Teams. All members of a Team can access and view the cases that belong to that Team (but only one Team member will be the 'owner' of each case at any one time).
- » Individual users, Teams and cases are all assigned a Security Level. Team members will only be able to view cases within their Team that are at or below their Security Level.

Note: The creation of Teams and Security Levels is only applicable to Server-mode deployments connected to a local CSAS Server. If the instance of CSAS you are using is not connected to CSAS Server, even if it is connected to your network, it is classed as being in Standalone mode.

The Teams and Security Levels structure is designed to allow organisations to manage access to cases of different levels of sensitivity.

5.1 Modes

CSAS can operate in two modes:

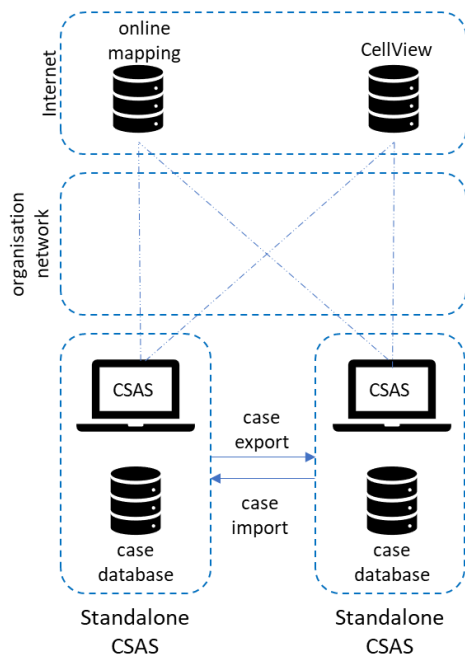
- » Standalone – where each copy of CSAS works independently on its host computer and keeps all case data stored in a local database.
- » Server-based – where a group of copies of CSAS within the same organisation connect to a CSAS Server. Users have the option to save cases in the server database and work on them there, or they can 'check out' a case to their local database and work on it locally.

Some features are only available in 'server mode'.

When in server mode, individual cases can be checked out/checked in using the CSAS Server connection control in the CSAS top row controls.

5.1.1 Standalone Mode

The term 'standalone' mode relates to the way in which a copy of CSAS configured to work in that mode operates in respect of case sharing and interworking with other copies of CSAS in the users organisation.

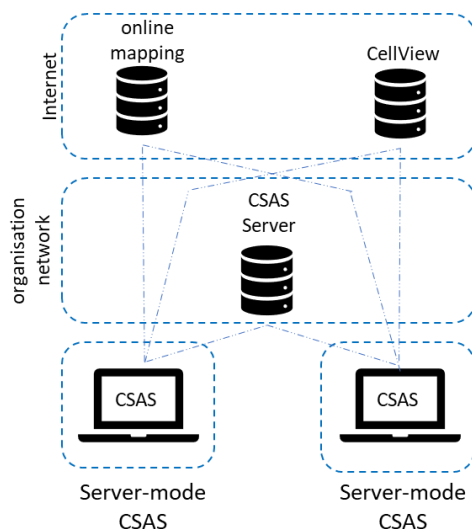


The host PC might be connected to the network and the Internet, the instance of CSAS running on that PC may be able to connect to Internet resources like online mapping and CellView, but it won't be connected to CSAS Server or to other instances of CSAS.

In that sense, in Standalone mode, each copy of CSAS 'stands alone', manages its own local case database and only interacts with other instances of CSAS at one remove, via functions such as Case Export/Case Import.

5.1.2 Server Mode

In 'server mode', each copy of CSAS is configured to connect to their organisation's CSAS Server (or to a particular CSAS Server, if the organisation has more than one).

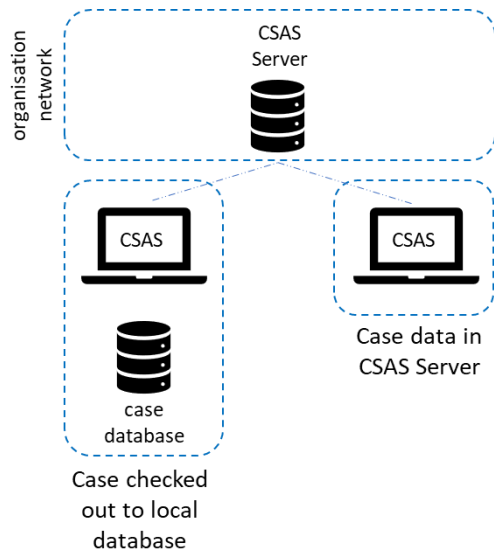


The host PC connects to the organisation's network and has access to Internet resources like online mapping and CellView. It also connects to CSAS Server.

Case sharing and collaborative work are managed via CSAS Server, with multiple users able to access the same cases concurrently.

5.1.3 Hybrid working

It is also possible, depending on configuration, to work in a hybrid way in Server mode, with the option to check out or download a case to the local CSAS case database so it can be worked on while disconnected from the organisation's network.



If your CSAS Server is configured to allow cases to be checked out, you can check a case out using the CSAS Server connection control in the top row whilst the required case is open in CSAS.

You must be the case owner to make changes to a checked-out case.

If you've checked the case out so you can work on it when not connected to your organisation's network, you may also need to check out a floating licence to keep your copy of CSAS active whilst disconnected.

Other users who share a case will not be able to access it whilst it is checked out, so it is important to remember to check the case back in again when you've finished with it.

5.2 Licence Options

CSAS supports two main types of licence:

- » Dedicated licences – which are dedicated to a particular instance of CSAS on a specific host PC – the licence ties that copy of CSAS to the PC.
- » Floating licences – which can be assigned to an instance of CSAS temporarily and shared between a larger population of CSAS users.

The licence type to be used is selected during the initial installation of CSAS – if you change the licence type being used (if, for example, you initially install CSAS using a dedicated licence but at some point later, switch to using floating licences), CSAS will need to be reinstalled and the new licence type selected.

5.2.1 Dedicated Licences

Dedicated licences are created individually by CSAS Support and are used to activate a copy of CSAS which is tied to a specific PC. Dedicated licences are distributed using 'activation codes', which are validated by Forensic Analytics and can only be used once.

Dedicated licences are set to last for a fixed amount of time, usually a year, and allow CSAS to activate and control the set of permitted features within CSAS that users have access to.

If you need to move your copy of CSAS to a different PC during the lifetime of a dedicated licence, you'll need to arrange to get the old licence cancelled and a new licence created.

The validation and activation of dedicated licences can work in two different ways – online activation and offline activation.

Online Activation

With this option, licences and activation codes can be created by CSAS Support in advance and the individual activation codes can be distributed via email to individual users to be copied into their dedicated copies of CSAS.

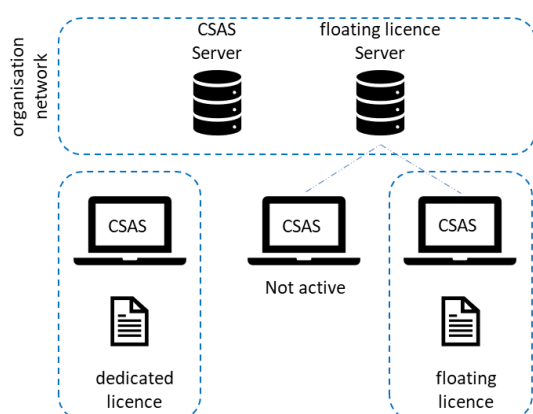
Online activation codes need to be checked and verified by the Forensic Analytics licence server, so the host PC needs to have Internet access available when CSAS is being installed.

Offline Activation

Offline activation can be used if the host PC does not have Internet access, or if it has limited access to applications like email but can't access the Forensic Analytics licence server.

Offline activation requires some interaction between the user (or their IT support team) and CSAS Support. When the instance of CSAS is ready to be licensed, a licence 'pass key' can be generated (via the [Help > About/Licensing > Licence](#) screen), which needs to be sent to CSAS Support. This key is very long, so it is simpler if it can be emailed to us rather than read out over the phone.

CSAS Support then generate an activation key and send it back (again, it is very long, so email would be preferable to having to read the key out) to be pasted into the licence screen. If the codes were copied correctly, CSAS will be activated.



5.2.2 Floating Licence

There is a one-to-one relationship between a dedicated licence and an activated copy of CSAS, so an organisation would need to purchase as many dedicated licences as they have copies of CSAS. In larger organisations, this could be unnecessary, as not all potential CSAS users are likely to want to use their copy of CSAS at the same time.

Floating licenses can offer a more efficient way to licence larger CSAS deployments.

An organisation employing floating licences is provided with a floating licence server. CSAS Support create a floating licence with a specific number of activations – each activation allows one active user to share the floating licence concurrently.

For example, a floating licence with 10 activations, deployed to an organisation that has 20 CSAS users, would allow 10 of the 20 users to be active concurrently. Once all activations were in use, any further users would have to wait for a licence to become free before they could activate their copy of CSAS.

If the organisation found that their activations were never all in use, they could reduce the number of activations they pay for; if, on the other hand, they find that all activations are in use all the time and users are spending too much time waiting to access CSAS,

they could purchase additional activations.

An individual floating licence server can have more than one licence, each with its own 'pool' of activations, deployed to it, so it could serve multiple different groups of CSAS users. Users simply need to be given the details for the correct licence pool to use when connecting to CSAS.

Different licence pools can also be used to allow different groups of users within an organisation to access different sets of CSAS features. For example, if an organisation has 100 CSAS users, but they only want 20 of those users to be able to access the CSAS RF Survey capability, they could create one licence pool, with a licence that enables RF Survey and a separate licence pool with a licence that doesn't enable that feature. The 20 RF users would be provided with details of one pool. The remaining 80 users would share the other pool.

Floating Licence Expiry

Floating licences can be highly sought-after in busy organisations. An activation is granted for a set period of time, often 24-hours but sometimes as little as 2-hours. At the end of the allocation period, you'll need to reapply for a floating licence activation.

The expiry time of your current floating licence activation is shown in the bottom right corner of the CSAS screen.



This information is updated in real time. You'll receive warnings before the activation expires.

Floating Licence Checkout

A copy of CSAS that is configured to use a floating licence must be connected to the organisation's network and contact the floating licence server in order to acquire an activation. Also, once a copy of CSAS has its floating licence activated, it must check in with the server every five minutes to have the activation refreshed – if CSAS misses a check in, the floating licence deactivates – so each copy of CSAS must stay connected to the organisation's network while CSAS is in use.

If the user needs to disconnect from their network but still needs access to CSAS (if, for example, they need to go to court and need CSAS as part of their presentation), they'll either need to connect to their network using a VPN or, if the floating licence server is configured to allow it, they could 'check out' a floating licence.

Floating licence checkout is managed from the Help > About/Licensing > Licence screen. If the option is permitted, once a floating licence has been activated, the Licence screen will show a 'Check Out' button to trigger the process.

Licence Type: Floating		Expiry Date: 26/06/2024		Checked out until: Not Checked Out	
	Remove Licence	Check Out	Deallocate	Licence Activation Url https://test.fa-licensing.com:81/service...	
				Update	

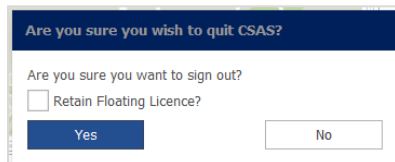
Once checked out, the 'Checked out until' box will show the date and time the check-out ends. You'll need to reconnect to your organisation's network and check the floating

licence back in again before the expiry time – CSAS will lock and will not be able to be used if the check-out expires.

Releasing a Floating Licence early

If you find that you've finished your CSAS work earlier than expected, you can release the floating licence activation back into the pool for someone else to use.

To release a floating licence early, either close CSAS and do not tick the 'retain floating licence' option



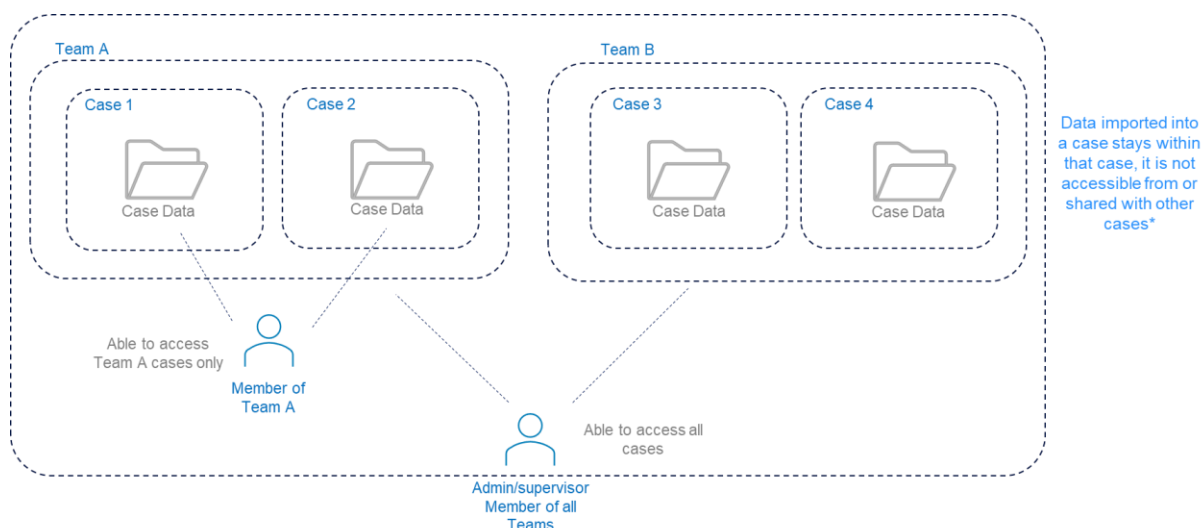
Or visit the Help > About/Licensing > Licence tab and select 'deallocate', the licence will be released and CSAS will close.



5.3 Teams & Security Levels

In Server mode, CSAS is designed to support collaboration between users, allowing users to work on the same shared cases and search for identifiers in cases created by colleagues. Uncontrolled case and information sharing could be detrimental to the requirements of operational and information security, however, so although collaboration is possible, it is tightly controlled.

User access to cases and their data is managed via a 'two dimensional' security model based on Teams and Security Levels.



5.3.1 Teams

All users are members of at least one Team within their organisation; individual users can be members of multiple Teams if required.

Cases belong to Teams; when a case is created, it is linked to a Team of which the case owner is a member.

All members of a Team have access to the cases that are linked to that Team, although only one Team member can be the 'case owner' at any one time, all members of the Team can have 'read only' access to the Team's cases.

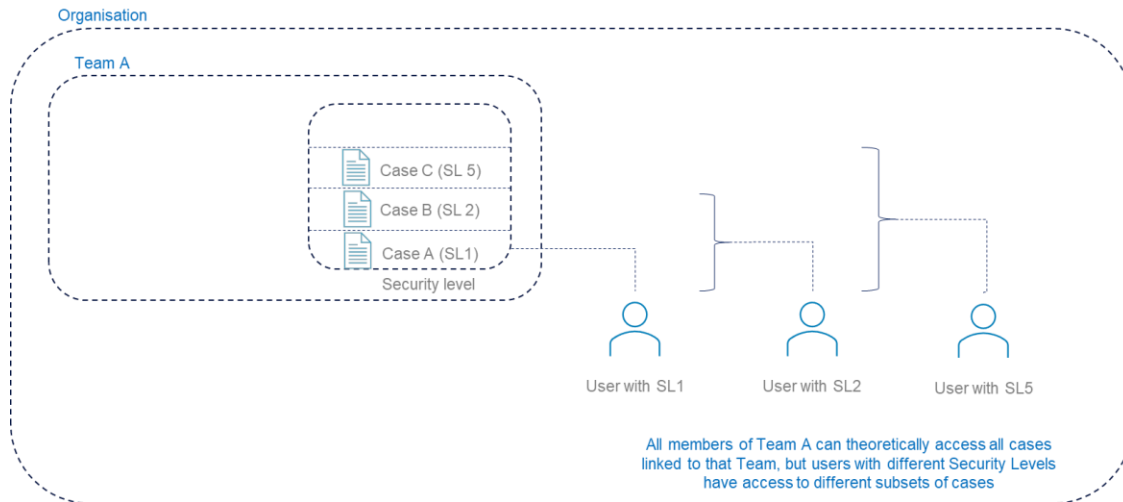
If you're not a member of the linked Team, you cannot gain access to any of the cases linked to that Team.

New Teams can be created by your CSAS administrator via CSAS Server, where they can also manage the users associated with each Team.

5.3.2 Security Levels

Within each Team, users and cases are assigned a Security Level; users only have access to cases that are at or below their security level.

There are five Security Levels (SL1 is lowest, SL5 is highest). Each Team's minimum security level is set when the Team is created – for example, if a Team has a minimum security level of SL3, only users of SL3 and upwards would be allowed to join that Team and only cases with SL3 and upwards would be linked to that Team.



Imagine a Team has a minimum security level of SL1. The Team has a mix of users with various security levels from SL1 upwards. A new case is created with a security level of SL1 – all users linked to that Team potential have access to that case. A second case is created with SL5 – only Team members who have SL5 would be able to access that case.

Team and User security levels are managed via CSAS Server and can be changed by your CSAS administrator.

5.3.3 Standalone Mode Settings

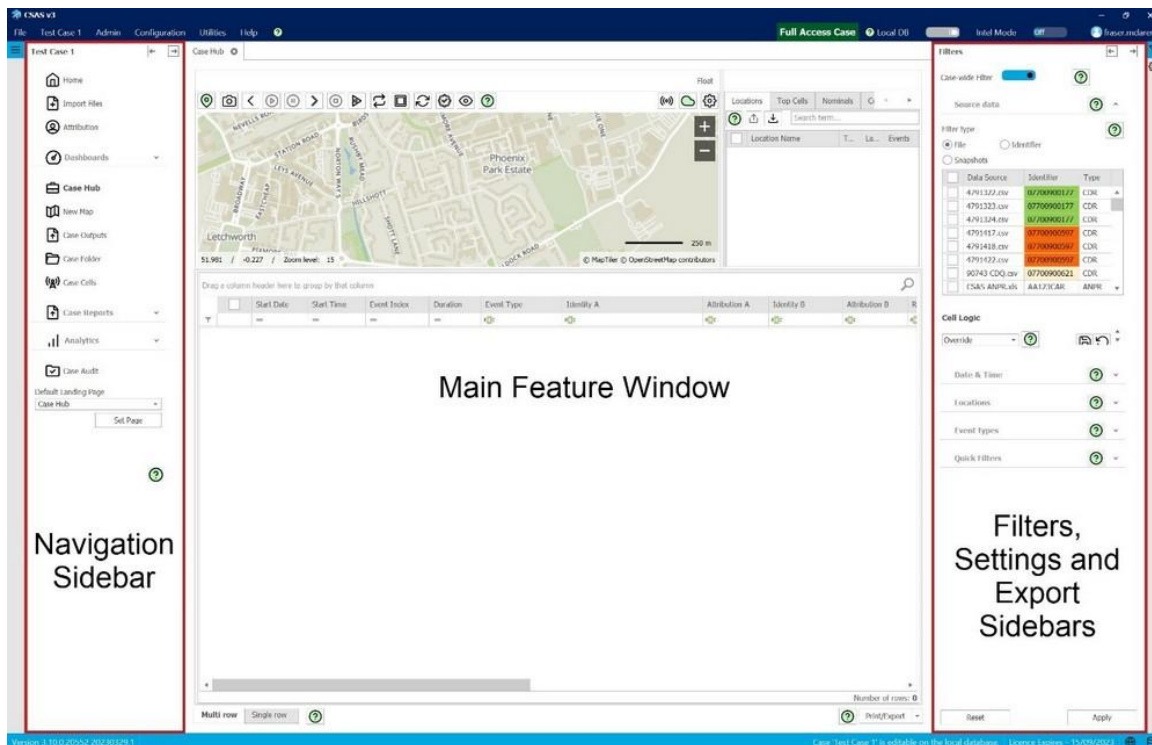
A CSAS deployment in Standalone mode is designed to support one user on one copy of CSAS; case sharing is only possible via the Case Export/Case Import features. In such a limited environment, there is no need for complex case sharing controls, so a Standalone deployment has one Team (Default Team) and has no options for creating additional Teams.

A standalone user is created with the highest security level, SL5.

When standalone cases are created, the case defaults to SL5 but there is the opportunity to set the case SL to a lower value. This would usually be done if there was a possibility of the case being shared at some later point (via case export/import) with a user who had a lower security level.

5.4 CSAS Layout

CSAS is laid out with a set of basic panels that are consistent throughout each screen and feature:



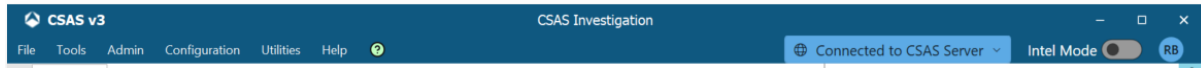
- » The Top Row menu buttons and controls provide access to 'global' functions that either apply to the operation of CSAS in general or relate to the fundamental operation of the current case.
- » When you open a case, the name of the open case is displayed on the left side of the toolbar.
- » When you click on the open case name, a drop-down menu opens from which you can quickly select the CSAS feature you want to use for the case.
- » The Navigation sidebar (or left sidebar) offers the ability to move between screens and features in the current case.
- » The Sidebars on the right of the screen (right sidebar) provide access to a consistent set of filtering, settings and export options within the current case.
- » The main feature window is where the data and functions of each feature are displayed.

5.4.1 Tabbed Browsing

Once a case is opened, CSAS presents different analytical and data processing feature on individual tabs, as the work on a case develops, multiple tabs may be opened, each hosting a different feature. To move between features within a case, simple click between the appropriate onscreen tabs.

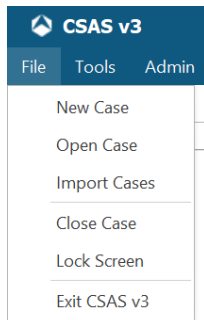
5.5 Top Row Buttons and Controls

The top row buttons and controls provide access to a set of frequently used buttons and are arranged along the top menu bar. When a case is open, the case name is displayed centrally in the top row:



5.5.1 File Menu

The 'File' drop-down menu provides access to the following options:



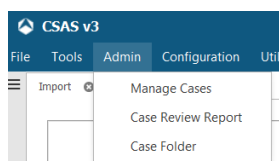
- » New Case – a shortcut to open a new case. See *New Case*.
- » Open Case – a shortcut to the open case control to open an existing case. See *Open Case*.
- » Import Cases – opens the case import screen. See *Importing and Exporting Cases*.
- » Close Case – closes the current case and returns to CSAS Home. See *Close Case*.

- » Lock Screen - displays the login window over a greyed-out screen. See *Opening CSAS and Logging In*.
- » Exit CSAS v3 – closes the application, all case data will be saved when this happens. See *Logging Out and Closing CSAS*.

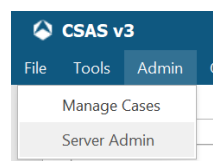
Closing a Case

If you close the currently open case, CSAS will save the imported data and created reports ready for you to access them again next time they are required. There are no additional 'save data' steps required when closing a case and no data should be lost when a case is closed.

5.5.2 Admin Menu



Standalone Mode



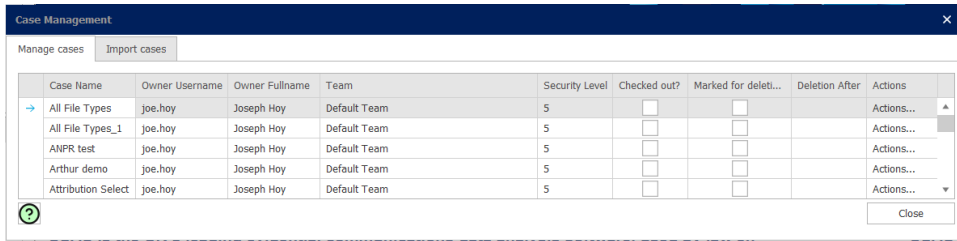
Server Mode

The 'Admin' drop-down menu provides access to the following options:

- » Manage Cases (in both modes)
- » Case Review Report (in Standalone mode only)
- » Case Folder (in Standalone mode only)
- » Server Admin (in Server mode only)

Manage Cases

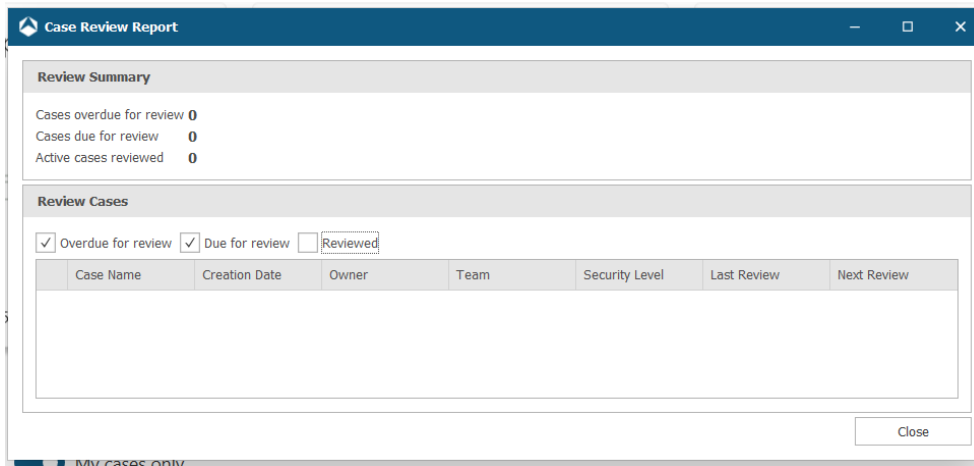
This option opens the 'Case Management' screen:



This menu option opens a pop-up window, from which you can manage your existing cases, including changing the case time zone, and import a new case. See *Case Management*.

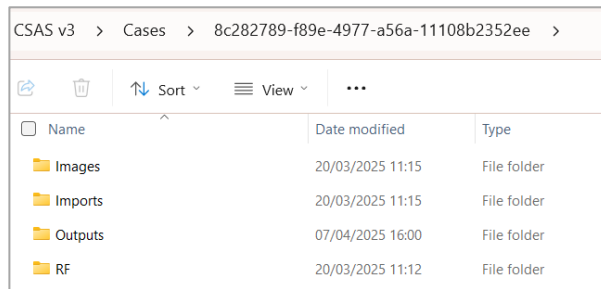
Case Review Report

The Case Review feature is designed to help users who operate within a regulated or accredited forensics process keep track of the age and state of their cases and will provide an indication of when cases are due for a review. See *Case Review*.



Case Folder

This menu option opens the local case folder in Windows Explorer, allowing the current set of Input and Output files for the case to be viewed:



It may also provide access to other case resources, such as saved reports and images.

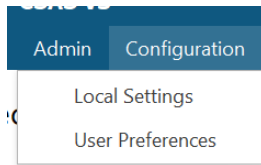
Each CSAS case is assigned a unique case ID, which is a long alphanumeric string known as a GUID, as shown in the screengrab above.

This is used as the folder name within the CSAS case folder – case names can be changed, using the Case Management > Rename feature, but the case ID remains constant throughout the lifetime of the case. Cases cannot be easily found by searching via Windows Explorer, however, due to the complex case ID and the recommended way of gaining access to the case folder is via the Case Folder option.

Server Admin

This option opens a connection to the configured CSAS Server to allow access to user and case admin features. Only registered CSAS Server admins will be able to log in to CSAS Server. Please contact your local IT team or CSAS administrator to gain access to this feature.

5.5.3 Configuration



The 'Configuration' drop-down menu provides access to the following options:

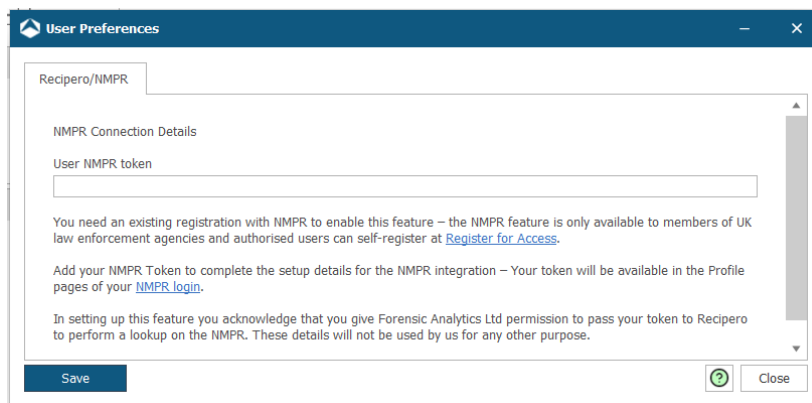
- » Local Settings.
- » User Preferences.

Local Settings

Local Settings provides access to a set of global CSAS settings (which control fundamental aspects of CSAS activity) and should only be accessed under direction from FA Support.

User Preferences

Selecting this menu option opens the 'User Preferences' pop-up window:

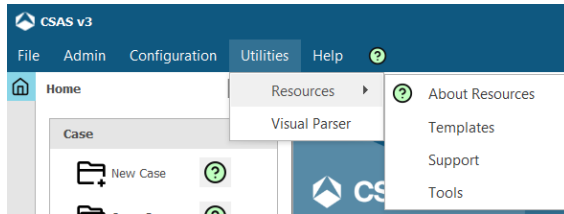


Currently, the only option available in this menu is to set NMPR Configuration details.

The NMPR Lookup feature is included in Case Hub and allows users in specific countries (currently UK and Australia) to look up details of identifiers such as IMEIs on a central database operated by Recipero. To use the CSAS NMPR Lookup you must first register with Recipero and obtain a user token, which can be pasted into CSAS in the User preferences screen. More details can be found at thenmpr.com. Please see [Using Lookup in NMPR](#) for more details.

5.5.4 Utilities

The 'Utilities' drop-down menu provides access to the following options:



Resources:

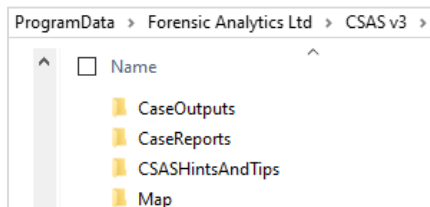
Templates
Support
Tools

Resources

The Resources option provides access to a set of folders which offer a range of help and support resources:

Templates

When you click 'Templates', Windows Explorer opens a folder from which you can access the various templates used by CSAS:



- » CaseOutputs – hosts the report and Fast Time templates used by Case Outputs.
- » CaseReports – hosts the templates used by the Disclosure Reports.
- » CSASHintsAndTips – hosts the template used to populate the 'help' popups.
- » Map – hosts the label templates used by CSAS Mapping.
- » The folder also currently houses the set of map label templates used by CSAS RF module maps; these will be moved to a more suitable location in a later release

Support

When you click 'Support', Windows Explorer opens a folder which contains a set of generic 'rescue templates', which are used to help import unrecognised or unstructured data into CSAS, plus a number of help and guidance documents.

Tools

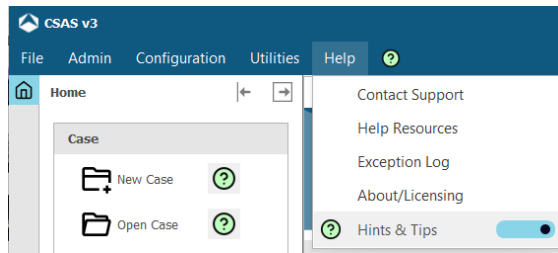
The Tools folder contains a set of macros and other tools that can be used to pre-process some types of data before importing them into CSAS.

Visual Parser

This option opens the Visual Parser, which provides an opportunity to view the way in which individual source files were processed by CSAS. See [Visual Parser](#) for more details.

5.5.5 Help Menu

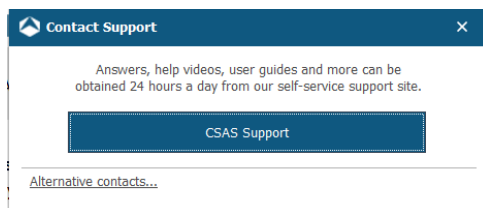
The 'Help' menu provides access to a number of help and information resources:



- >> Contact Support
- >> Help Resources
- >> Exception Log
- >> About/Licensing
- >> Hints & Tips.

Contact Support

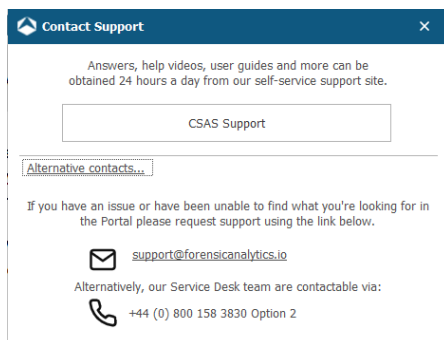
Selecting 'Contact Support' opens a pop-up window giving access to contact details for the CSAS Support team:



The preferred method for contacting CSAS Support is to use the online ticketing system embedded in the CSAS Support site.

To raise a new support ticket:

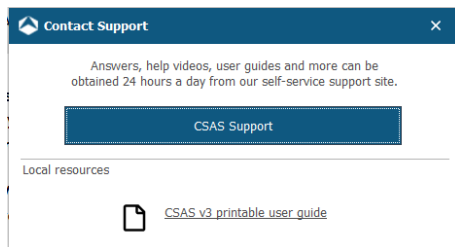
- Click on the **CSAS Support** button
- Log in to the CSAS Support site (use the email contact option mentioned below to request a Support site account if you don't already have one)
- Once in the Support site, select 'Tickets' from the navigation sidebar section and click on 'Create Ticket'
- Fill out the required details, adding as much detail as you can about the issue you've experienced, including, if possible, the set of steps required to replicate the problem. Details of existing open tickets will also be shown in the support site.



Clicking 'Alternative contacts...' expands the pop-up window and provides some additional contact methods.

Note: These additional methods can be slower than using the online ticketing system and are generally not preferred.

Help Resources

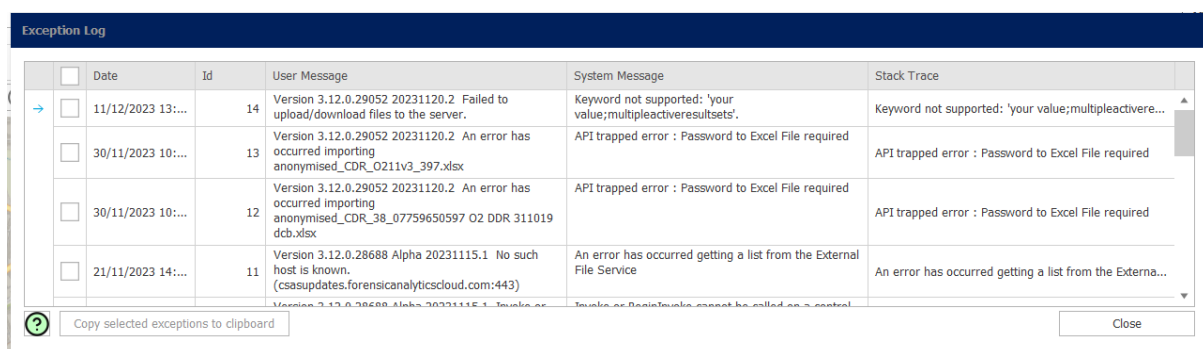


The 'help resources' tab provides access to a range of 'self-help' resources, including a copy of this CSAS user guide and a link to the CSAS Support website.

Additional resources, including links to 'how to' videos and online training courses will be added in a future release.

Exception Log

The exception log captures details of 'exceptions' or errors that could cause CSAS to stop working and shut down:



This feature provides more details about bugs or issues experienced by CSAS and would generally only be accessed under the direction of Forensic Analytics Support.

Exceptions listed in the 'Exception Log' pop-up can be selected using the checkboxes and copied to your clipboard by clicking on the **Copy selected exceptions to clipboard** button and pasting into a format of your choice, such as an email.

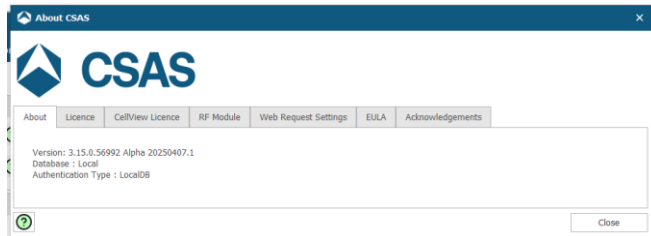
Alternatively, you can choose to hide an exception(s) by clicking on the **Hide selected exceptions** button.

You can then close the pop-up window by clicking on the **Close** button.

About/Licensing

Selecting 'About/Licensing' opens the 'About CSAS' pop-up window:

From this window, you can select one of the following tabs:



- >> About
- >> Licence
- >> CellView Licence
- >> RF Module
- >> Authentication
- >> Web Request Settings
- >> EULA
- >> Acknowledgements

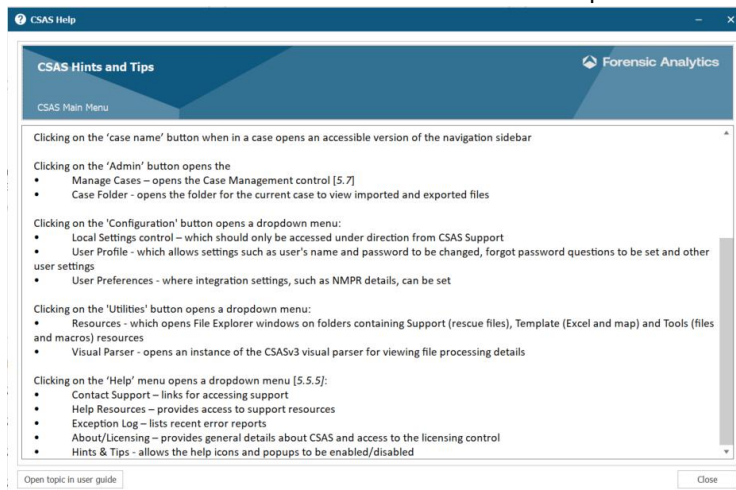
- >> The '**About**' tab - provides details of the CSAS version number, the configuration of the database (local and/or server) and the selected user authentication method.
- >> The '**Licence**' tab - provides details of the main CSAS activation licence deployed to your copy of CSAS, along with the Support Key (which may be required if you contact CSAS Support). It also details the Organisation you are registered as belonging to, the contact details CSAS Support has registered for you and your licence expiry date and licence type.
- >> The '**CellView Licence**' tab - shows details of the optional CellView licence your organisation may have purchased for you. If you have been provided with a CellView licence, you can activate it using this tab. If you don't have a licence, but would like to use the CellView feature, please contact your organisation's CSAS administrator or your Forensic Analytics account manager.
- >> The '**RF Module**' tab - shows your RF Module Licence Type, Expiry Date and Organisation etc. If you have been provided with a RF Survey licence, you can activate it using this tab. If you don't have a licence, but would like to use the RF Survey feature, please contact your organisation's CSAS administrator or your Forensic Analytics account manager.
- >> The '**Authentication**' tab - shows your current authentication settings. The authentication method in use can be changed via this tab, but we strongly recommend that you don't make any changes before you have discussed it with your local IT support team or with CSAS Support.
- >> The '**Web Request Settings**' - CSAS employs a set of basic network and Internet communications settings, including setting the maximum time the application waits for a response to messages and the encryption method it employs. Some networks require specific settings to be used and this tab provides the opportunity to change those settings in the event that CSAS is unable to communicate with network or Internet resources. We strongly recommend that these settings are not changed without discussing it with your local IT team or with CSAS Support.
- >> The '**EULA**' tab - provides access to a copy of the End Licence User Agreement, which users accept when they log in to CSAS.
- >> The '**Acknowledgements**' tab - lists details of open source and other third-party

software libraries and packages that are used within CSAS. All third-party add-ins are regularly tested by an independent external provider as part of the CSAS software verification process.

Hints & Tips

Clicking the  slider allows you to toggle CSAS Help '?' icons on / off.

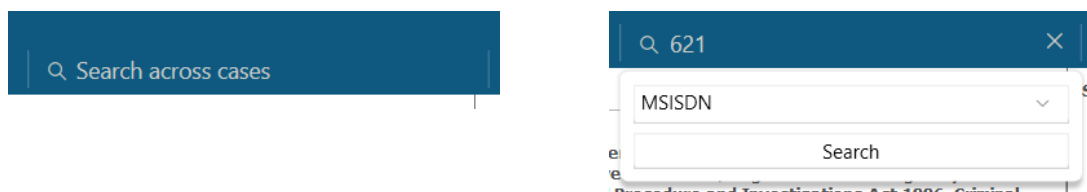
You'll see the '?' icons at various places around the home screen and in other CSAS features. When you click on any '?' icon, a CSAS Help pop-up window opens giving you hints about the function / feature, for example:



The '?' icon also gives you a link to the relevant section in the user guide and also, where applicable, provides a link to relevant online help video clips.

5.5.6 Search Across Cases

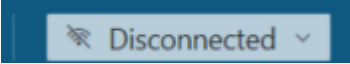
The search field allows users to search for identifiers and other data across all cases they have access to and is available either whilst actively viewing a case or when the CSAS home screen is displayed.



Enter a full or partial identifier, select the identifier type (MSISDN, IMSI, IMEI, etc) and click Search. In Standalone mode, only the local CSAS database will be searched, but if you are connected to CSAS Server, then all cases that you have permission to view will be searched. A popup window displays a list of CSAS cases in which the specified identifier was found; clicking on a case will open it (if it is currently accessible). See [Cross Case Search](#).

5.5.7 CSAS Server Connection Status

This drop-down control is only available in Hybrid mode installations. The control allows users to view their current connection status as well as select cases to move between the central, shared CSAS Server database and their local 'per user' CSAS database.

» When the status shows 'Disconnected'  CSAS is only connected to the local database, allowing you to work on cases when not connected to your organisation's CSAS Server. Checked out (e.g. downloaded) cases will still be available in read-only mode on CSAS Server for other users to view.

» When the status shows 'Connected to CSAS Server'

 CSAS is working connected to your organisation's central CSAS Server database. Any changes that you make to a case in Server Mode will be immediately available to view by other users accessing the same case from the server in read-only mode.

As well as improved performance, the case check-out option (along with the ability to check-out a floating licence) allows users who normally work on CSAS whilst connected to their organisation's server to download a case, and work on it offline.

Note: To use this feature, you must anticipate that a server case (e.g. a case that is currently stored on the CSAS Server database) will need to be accessed when your PC is no longer connected to the server and the case must be downloaded to the local database before server connectivity is lost. For example, if you know you are going to be in court and will need access to CSAS from there but also know that you will have no access to your organisation's network from that location, you'll need to check the CSAS case out and download it to your local CSAS database to continue to have access to it whilst in court. It is not possible to download a case from your organisation's CSAS Server once you have disconnected from your organisation's network.

5.5.8 Intel Mode

This is an 'On/Off' select button which allows you to enable or disable Intel Mode.

Intel Mode provides the option to view events captured in some types of source data (currently it is only captured from some types of CDR) that, although they are included in the source data files, do not relate directly to activities undertaken by the 'subject' of the source file. This type of event can be classed as a 'non-subject' event.

All CDRs provide details of the activities undertaken by the subject phone – calls and texts made and received, mobile Internet connections established – but some CDR types also provide details about the activities of the 'other' (or 'non-subject') phone engaged in those calls and texts. Usually, information related to non-subject phones isn't regarded as usable evidence but can be regarded as useful intel. For example, a CDR produced by one network will show details of a subject phone receiving a text message but might also show details of the non-subject phone sending that message. Authorisation to analyse the activities of the subject phone will have been provided in the warrant or other permissions that was granted to allow the CDRs to be requested; but warrants rarely give

permission to analyse the activities of any non-subject phones whose data appears in those CDRs. This means that subject phone records can be regarded as legitimate evidence, non-subject phones generally can't.

With the Intel Mode switch 'off', CSAS displays only events that are regarded as being 'evidential', but with the Intel Mode switch 'on' any additional events that were included in source files but which relate to non-subject phones will also be displayed.

When enabling Intel Mode, you'll notice the top rows of the CSAS user interface change colour (from blue in 'evidential' mode to red in 'intel' mode), which is intended to alert you to the change in mode and also to remind you that some events now displayed should not necessarily be regarded as evidence. Each 'intel' event is also clearly marked in the Case Hub grid, by filling in the row index number and the event type in red, so that 'evidential' and 'intel' events can be clearly distinguished.

☐	Start Date	Start Time	Event Index	Duration	Event Type	Identity A
	=	=	=	=		
+ ☐	08/01/2017	15:37:09	1	00:00:00	Outgoing Text	07700908010
+ ☐	23/01/2017	16:24:19	2	00:00:10	Outgoing Voice	07700908010
+ ☐	23/01/2017	16:24:54	3	00:00:00	Outgoing Text	07700908010
+ ☐	23/01/2017	16:25:08	4	00:00:00	Outgoing Text	07700908010
+ ☐	25/01/2017	16:43:20	5	00:00:00	Outgoing Text	88857700903126

Intel Mode really only has an impact on Case Hub and Case Outputs. In Case Hub, the additional 'intel' events will be displayed in the grid but will be clearly differentiated from 'evidential' events. In Case Outputs, the list of available export templates is reduced to only those that contain a specific 'Intel Mode' column, so that 'intel' events can be clearly distinguished.

As 'intel' events generally contain no phone location data, they will not appear in CSAS maps and they are ignored by Analytics and Dashboard queries.

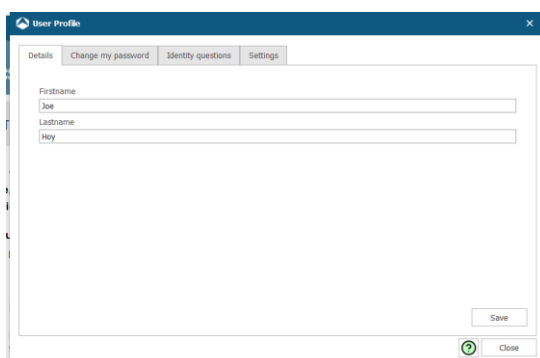
5.5.9 Profile Menu

On the far right of the top row, the  Profile button, featuring the user's initials, provides the following options:

- >> *My Profile*
- >> *Sign Out*

My Profile

Selecting 'My Profile' opens the 'My Profile' pop-up window.

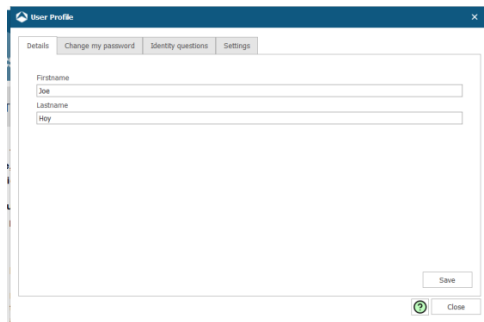


From this pop-up window, you can view and update your profile (the options presented are dependent upon what authentication method was chosen when CSAS was installed, and the methods used by the organisation).

In Server mode, using both the 'active directory' and 'CSAS Server authentication' options, usernames and passwords can only be changed by the organisation's administrators (or IT department), so the password management options will not be displayed.

'Change my password' only works when the 'local database' authentication option is selected, which is used for fully 'standalone' or non-server deployments of CSAS.

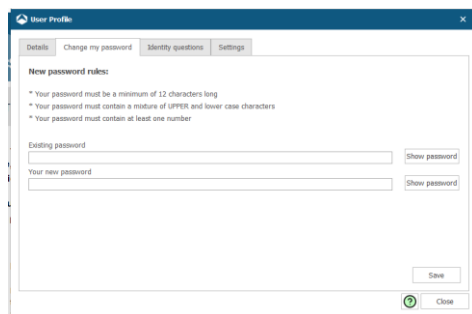
Details



The 'Details' tab in the 'User Profile' window shows fields for 'Firstname' (Joe) and 'Lastname' (May). There is a 'Save' button at the bottom right and a 'Close' button with a green checkmark icon at the bottom left.

View your details (first and last name). These details are added to identify the 'author' of any output documents you create in a case. If you need to edit any information you can enter it directly into the text fields. Save changes by clicking on the **Save** button.

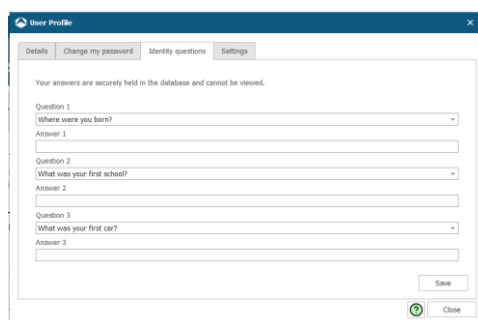
Change My Password



The 'Change my password' tab displays 'New password rules' with three bullet points: 'Your password must be a minimum of 12 characters long', 'Your password must contain a mixture of UPPER and lower case characters', and 'Your password must contain at least one number'. It includes fields for 'Existing password' and 'Your new password', each with a 'Show password' button. A 'Save' button is at the bottom right, and a 'Close' button with a green checkmark icon is at the bottom left.

In standalone mode, with local database authentication, you can change your CSAS password using this tab. The new password can be entered directly into the text fields – please make note of the password strength rules shown at the top of the tab. Save changes by clicking on the **Save** button.

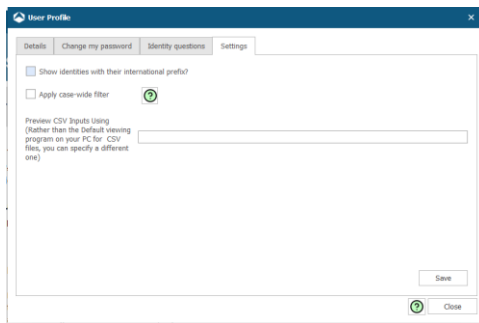
Identity Questions



The 'Identity questions' tab shows a note: 'Your answers are securely held in the database and cannot be viewed.' It contains three questions with dropdown menus and text input fields: 'Question 1: Where were you born?', 'Question 2: What was your first school?', and 'Question 3: What was your first car?'. A 'Save' button is at the bottom right, and a 'Close' button with a green checkmark icon is at the bottom left.

In standalone mode, with local database authentication, you will have been asked to enter a set of identity questions when CSAS was first installed – these are used as part of the 'forgotten password' process. If you wish to view or update your identity questions, you can do so via this tab. Save your changes by clicking on the **Save** button.

Settings



The Settings tab offers the option to:

Select whether phone numbers are shown with their full international prefix (e.g. 447700900123) or with a domestic prefix (e.g. 07700900123).

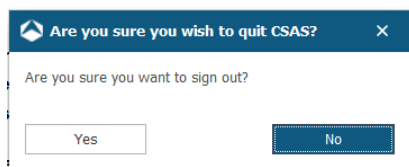
Globally enable or disable Case Wide filters - if the Case Wide Filters box is ticked, that mode of filtering will be enabled by default in all cases. If it is unticked, cases will be opened with that mode disabled.

Select a specific application to use to view CSV files - CSAS usually opens CSV files in whichever application is set as the default in Windows (see Windows Settings > Apps > Default Apps > choose default applications by file type > .csv). If you want CSAS to open CSV files in a different application, without changing the Windows default for other applications, paste a link to the required application here. For example, if you wanted CSAS to open CSV files in Notepad++, you'd paste a link like this - *C:\Program Files\Notepad++\notepad++.exe*. This option should generally only be changed after consulting you IT team or CSAS Support.

You can close the 'My Profile' pop-up window by clicking on the Close button.

Sign Out

Selecting Sign Out simply signs you out of CSAS using the following pop-up window:



Note: If a floating licence is in use, there will be a checkbox in the window to release the current floating licence. You'll need to tick this checkbox. Dedicated licences will not be released or removed via this option. The floating licence time remaining is given at the bottom right-hand corner of the CSAS screen if floating licences are in use.

See [Logging Out and Closing CSAS](#) for more details.

Why, When, Who

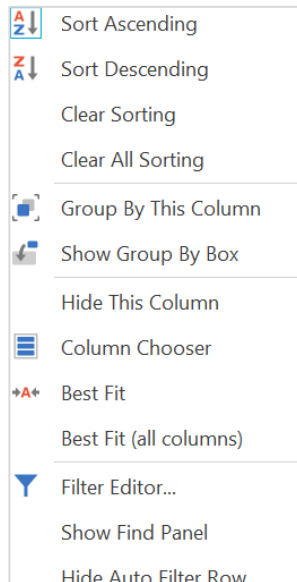
	This function is necessary to allow you to view and change CSAS configuration options and to access help and support resources.
	This function is undertaken whenever you need to administer CSAS settings or get help and support
	This function is typically carried out by the following users: >> CSAS User (and above).

5.6 Grid Filtering and Controls

Most CSAS screens contain a data grid or table of some kind. All of these grids are constructed in the same way and offer the same basic set of control features.

5.6.1 Column Control Menu

Within the Data Grid, you can access the grid control menu by right-clicking in any column header.



- » 'Sort Ascending'/'Sort Descending' - resorts the grid by the selected column. Clear All Sorting returns the grid to its default order (sorted by identifier).
- » 'Group By This Column' - if activated, shows the Group By bar, which allows the grid contents to be grouped into 'bands' by dragging the required column header into the Group By box - for example, if 'identifier type' is dragged to the box, the grid will resort into bands, one band for each identifier type.
- » 'Hide This Column' - hides the selected column from view, so you can customise the grid view.
- » Column Chooser presents a list of currently hidden columns that can be added back into the grid.

- » 'Best Fit/Best Fit (all columns)' - resizes the width of the selected columns to display the data in full.
- » 'Filter Editor...' - displays a 'narrative filter builder' panel.
- » 'Show/Hide Find Panel' - opens a powerful 'whole grid' search bar.
- » 'Show/Hide Auto Filter Row' - opens a filter bar in row 1, where you can type in items to filter the data to within that column.

The set of columns on display in most grids can be customised as required. You can:

- » Customise the column layout - drag a column to a different position in the grid by left clicking and holding a column header then dragging it to the required position.
- » Add extra columns to a grid by right-clicking on a column header to activate the control menu and select 'column chooser'. Select the required column name from the chooser list and drag it to the required position.
- » Remove columns from the grid, use the 'Hide this Column' option in the column control menu to remove the column from the current layout.
- » Custom column layouts can be saved to be used again later – see [Grid](#) for more details.

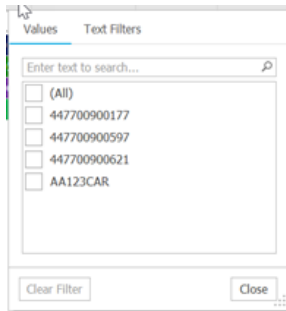
Column Header Sorting Options

You can sort and resort the grid based on the content of any column – simply left-click in the column header of the column you wish sort by. Click once to resort in ascending order or click again to sort in descending order.

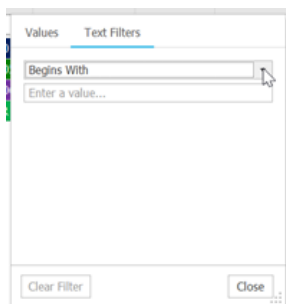
Column Header Filter Option Menus

The contents of each column can be filtered based on multiple values found in the column data.

Clicking on the 'filter'  icon in the column header activates a drop-down menu which lists the unique contents of the column. This allows you to choose one or some of the values to filter the column to show.

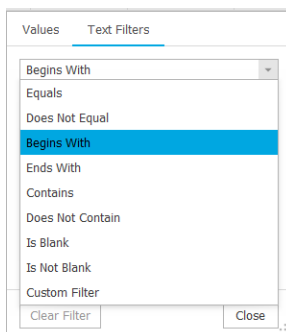


Note: The construction of the filter menu differs depending on the type of data displayed in each column, with simple lists of unique values in columns that contain numbers or text through to date pickers for columns that contain dates/times



The menu also contains an option to build a narrative or 'text' query using pre-set query descriptions.

To use this feature, first select the query type from the dropdown menu.



It also offers a 'custom filter' option which allows two conditions to be set that are linked as either an 'AND' or an 'OR' query.

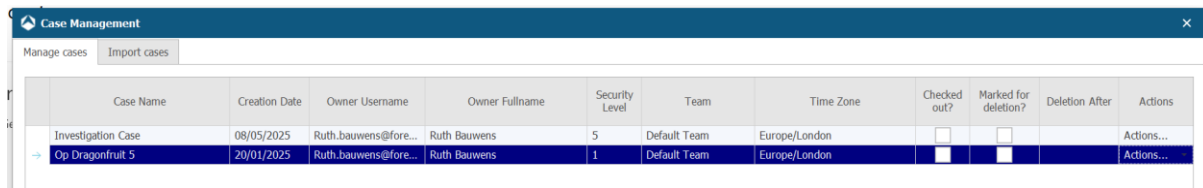
Then you can select the value or values the query will operate on.

If matching data is found in the selected column, the grid will filter to show just those rows

The same basic functionality is applied to all grids and tables in the application.

5.7 Case Management

This function allows you to manage the cases you have access to. Selecting 'Case Management' opens the following pop-up window:



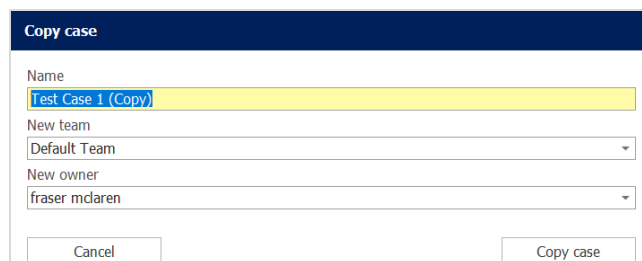
Case Name	Creation Date	Owner Username	Owner Fullname	Security Level	Team	Time Zone	Checked out?	Marked for deletion?	Deletion After	Actions
Investigation Case	08/05/2025	Ruth.bauwens@fore...	Ruth Bauwens	5	Default Team	Europe/London	☐	☐		Actions...
Op Dragonfruit 5	20/01/2025	Ruth.bauwens@fore...	Ruth Bauwens	1	Default Team	Europe/London	☒	☒		Actions...

From the 'Case Management' pop-up window, right clicking on any case (or clicking on the 'Actions' column) will give you the following options:

- » Copy Case
- » Export Case
- » Delete Case
- » Change Team
- » Change Owner
- » Rename
- » Edit Case Prefilters (you may need to scroll the list to view this option)
- » Edit Time Zone

5.7.1 Copy Case

Selecting 'Copy Case' allows you to create an exact copy of an existing case but assign it a new Name, New team and/or new owner using the drop-down menus. When selecting 'Copy Case' the following pop-up window is displayed:



Copy case

Name
Test Case 1 (Copy)

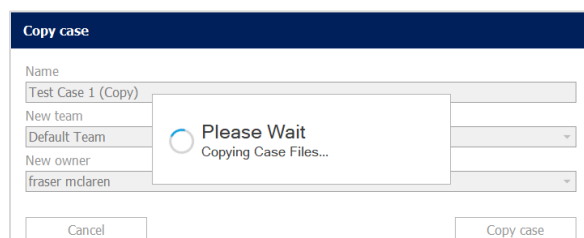
New team
Default Team

New owner
fraser mclaren

Cancel Copy case

Stepped Procedure

- From the 'Copy Case' pop-up window, update the case name if the default name is not suitable. You can then select the 'New team' and 'New owner' from the drop-down menus if required and click on the **Copy case** button. A message is displayed:



Copy case

Name
Test Case 1 (Copy)

New team
Default Team

New owner
fraser mclaren

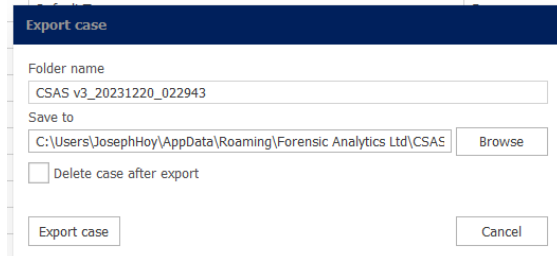
Cancel Copy case

Please Wait
Copying Case Files...

- You'll then see the copied case in the list of cases in the Open Case menu. If it's been shared with a new Team or a new User, they will also see the case in their own case lists.

5.7.2 Export Case

In Server mode, cases can be shared with selected other CSAS users via CSAS Server. This option is not available in Standalone mode, so CSAS also supports the option to export a case to a zip folder so it can be shared with another CSAS user.



Stepped Procedure

1. In the Manage Cases popup, select the case to be exported by ticking the box for the appropriate row.
2. Select 'Export Case' from the Actions menu.
3. The Export Case popup provides a suggested name for the export zip folder – if you wish to change this, simply delete the suggested name and replace it with your preferred name.
4. By default, CSAS will save the exported case zip file to the CSAS case folder. If you wish to save it somewhere else, simply click 'Browse' and choose a location.
5. If you want the case to be deleted from the local database after it has been exported, tick the box. Case deletion is irrevocable.
6. When you're ready, click 'export case'. Depending on the size of the case, this process could take several minutes to complete, CSAS will confirm when the export is complete. If you are sharing the exported case with another CSAS user, you can send the zip file to them using your preferred method.
7. An exported case can be imported into CSAS using the Import Cases option outlined below.

5.7.3 Delete Case

CSAS supports options to delete old or unwanted cases from the case database. Only a 'case owner' can delete a case from a CSAS Server database.

When a case is deleted, all imported data for the case is removed from the case database, all copies of imported files, all outputs (maps, analytics reports, case outputs reports, etc), all case snap shots are deleted. A deleted case cannot be recovered.

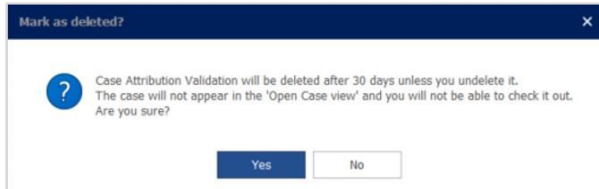
The delete case function has three options:

Mark as Deleted

This function allows you to initiate the deletion of a case from CSAS. As case deletion is irrevocable, CSAS provides a 'cooling off' period of 30 days after a case has been marked for deletion – in this time the case can be undeleted again or, if the 30 days elapses, the case will be deleted.

Stepped Procedure

1. To begin the deletion process, select the case to be deleted in the Manage Cases list and select the 'Mark for Deletion' option in the right-click or Actions menus. The following pop-up message appears:



2. If you wish to proceed with the deletion process, click 'yes', if you wish to cancel the deletion process, click 'no'.
3. The case will be marked to be deleted in 30 days.

Security Level	Checked out?	Marked for deleti...	Deletion After	Actions
5	☐	☐		Actions...
5	☐	☐		Actions...
5	☐	☒	01/04/2022	Actions...
5	☐	☐		Actions...

Delete Immediately

This function allows you to override the 30-day cooling off period and delete a case from CSAS immediately.

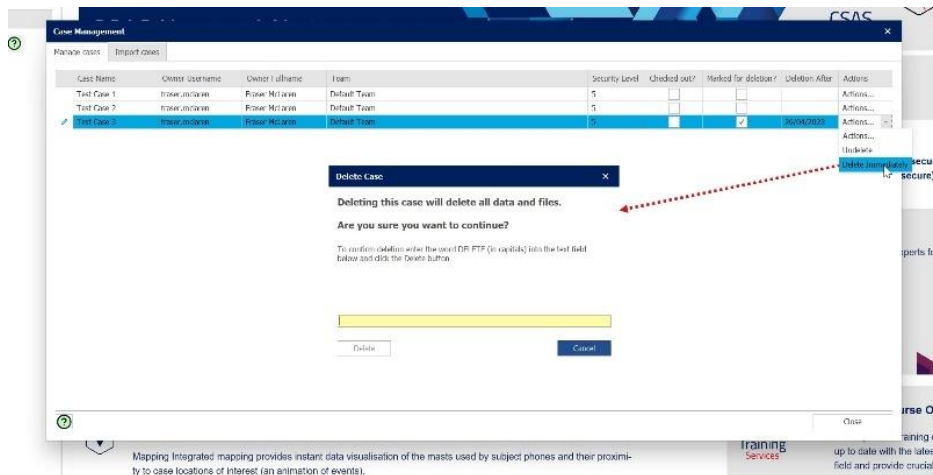
Note: To do this, you must first mark the case for deletion (see *Mark as Deleted*), then, from the 'Case Management' pop-up window, select the case you want to delete from the 'Manage cases' list.

Stepped Procedure

1. From the 'Case Management' pop-up window, select the case you want to Delete Immediately ('Test Case 3' is selected for example). The case row is highlighted:



2. To delete the required case, right-click on the selected row (or select from the 'Actions...' drop-down menu at the end of the row) and choose 'Delete Immediately'. The 'Delete Case' pop-up window is displayed:
3. To confirm you want to delete the case, in the text field enter, in caps, the word 'DELETE'; this acts as a method of making sure the case is not accidentally deleted: the delete process is permanent.



4. At this point you can:
- » Choose not to delete the case by clicking **Cancel** and close the pop-up window.
 - » Choose to delete the case and all files and data by entering the word 'DELETE' and clicking the **Delete** button. A 'Please Wait, deleting' message is displayed then the 'Delete Case' pop-up window closes: the case is now deleted from CSAS. CSAS deletion is irrevocable.

Undelete Case

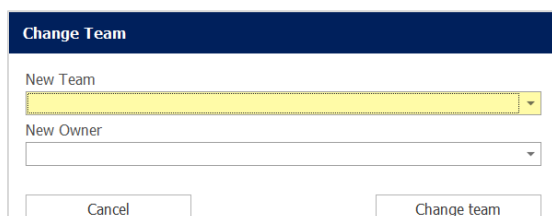
The scheduled deletion can be cancelled at any time during the 30-day cooling off period by selecting the case, right-clicking and selecting 'undelete'. The scheduled delete is cancelled and the case goes back to being generally available.

5.7.4 Change Team

Selecting 'Change Team' from the drop-down menu under 'Actions...' allows you to select, for an existing case, a new team and new case owner.

This option only works in Server mode (as there is no option to create additional teams in standalone mode). Only teams that have already been created via CSAS Server will be available to select. Only teams that you are a member of will be displayed. If the team you wish to transfer a case to is not listed, please select a team that you do have access to or contact your local CSAS Administrator to request access to the required Team.

When selecting 'Change Team' the following pop-up window is displayed:



Stepped Procedure

1. From the 'Change Team' pop-up window, select the 'New Team' and 'New Owner' from the drop-down menus and click on the **Change team** button.
2. The 'Change Team' pop-up window closes and the 'Case Management' pop-up window is displayed; you will see the new team and new owner of the case has

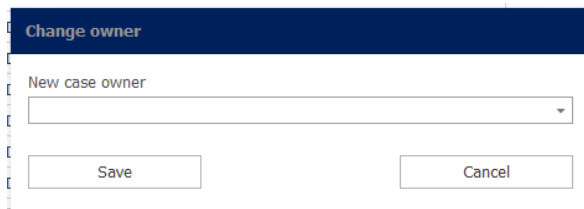
changed.

5.7.5 Change Owner

Selecting 'Change Owner' allows you to select, for an existing case, a new case owner using the dropdown menu. Although each case is shared with all members of the Team to which it is linked, only one member of the Team (the case owner) can edit a case at any one time, all other Team members have read-only access to the case, so a change of ownership is required if a different Team member needs access to edit or add data to a case.

This option only works in Server mode (as there is no option to create additional users in standalone mode). Only other users that are members of the team the case belongs to will be displayed. If the user you wish to transfer ownership of a case to is not listed, please select a user who does have access or contact your local CSAS Administrator to request that the required user be added to the Team.

When selecting 'Change owner' the following pop-up window is displayed:

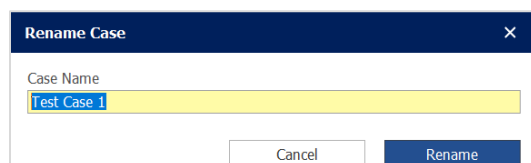


Stepped Procedure

1. From the 'Change owner' pop-up window, under 'New case owner', select from the dropdown menu a member of the linked Team and click on the **Save** button.
2. The 'Change owner' pop-up window closes and the 'Case Management' pop-up window is displayed; the owner of the case is changed.

5.7.6 Rename

Selecting 'Rename' allows you to rename an existing case by typing a new name in the text box. When selecting 'Rename' the following pop-up window is displayed:



Although the case name will be changed, the case ID (as used for the naming of the case folder in the CSAS 'cases' folder) will not change.

Stepped Procedure

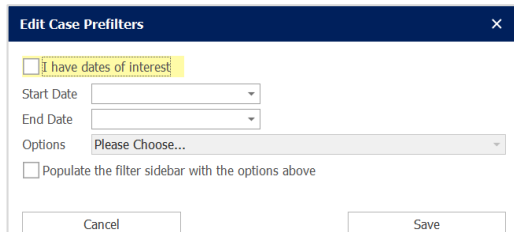
1. From the 'Rename Case' pop-up window, enter in the text box the new name of the case and click on the **Rename** button.
2. The 'Rename Case' pop-up window closes and the 'Case Management' pop-up window is displayed; the name of the case is changed.

5.7.7 Edit Case Prefilters

Case Prefilters set a limited date/time span for case data – only records that fall within the set period will be imported. Case prefilters can optionally be set when a case is first created, but they can be viewed or edited using this option.

Stepped Procedure

1. When selecting 'Edit Case Prefilters' the following pop-up window is displayed:

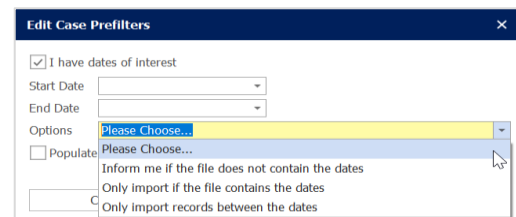


The 'Edit Case Prefilters' window contains the following elements:

- ☐ I have dates of interest
- Start Date: [dropdown]
- End Date: [dropdown]
- Options: Please Choose... [dropdown]
- ☐ Populate the filter sidebar with the options above
- Buttons: Cancel, Save

2. Ticking the 'I have dates of interest' checkbox makes the window 'live'. You can then add a 'Start Date' and 'End Date' as required.

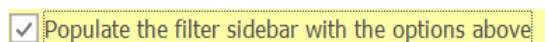
3. From the Options drop-down menu, you can choose one of the following options:



The 'Options' dropdown menu is open, showing the following options:

- Please Choose...
- Inform me if the file does not contain the dates
- Only import if the file contains the dates
- Only import records between the dates

4. You can also choose to populate the filter sidebar with your chosen Start and End Dates by ticking the checkbox:



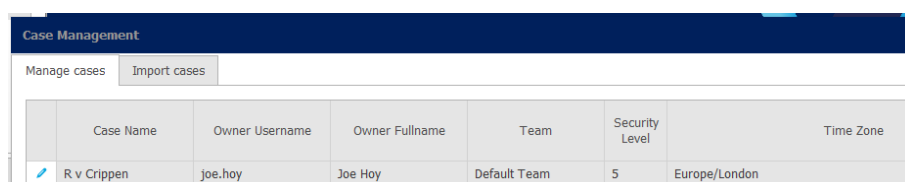
☒ Populate the filter sidebar with the options above

5.7.8 Edit Time Zone

By default, each case's time zone is set to match the time zone setting of the host PC. It is possible to change the time zone for a case when it is being created – see [New Case](#) – and also once a case has been created, via this menu.

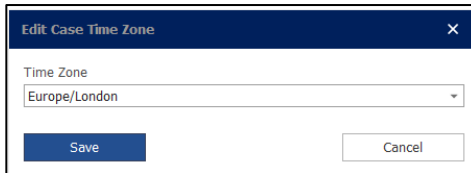
Stepped Procedure

1. The change of time zone affects how dates and times are presented within CSAS. On importing a new file, CSAS attempts to determine the UTC/GMT time for each event and also the offset from UTC/GMT to be employed for that case. Dates/times are then presented with the required offset applied. Times without explicit UTC offsets indicated are assumed to be in the default time zone for the case. If dates within a case are being displayed with the wrong UTC offset applied, it might be that changing the case time zone will solve the issue.
2. The current time zone for a case is displayed in the Manage Cases menu:



Case Management						
Manage cases		Import cases				
	Case Name	Owner Username	Owner Fullname	Team	Security Level	Time Zone
	R v Crippen	joe.hoy	Joe Hoy	Default Team	5	Europe/London

3. When you select 'Edit Time Zone' the following popup is displayed:



The dialog box titled "Edit Case Time Zone" has a close button (X) in the top right corner. It contains a "Time Zone" label above a dropdown menu currently showing "Europe/London". At the bottom, there are two buttons: "Save" and "Cancel".

4. Select a different time zone for the case from the dropdown menu:



The dialog box is shown with the dropdown menu open, displaying a list of time zones. The list includes: Europe/London, Europe/Oslo - (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna, Europe/Paris - (UTC+01:00) Brussels, Copenhagen, Madrid, Paris, Europe/Podgorica - (UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague, Europe/Prague - (UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague, Europe/Riga - (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius, Europe/Rome - (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna, and Europe/Samara - (UTC+04:00) Izhevsk, Samara. The "Europe/Riga" option is highlighted in blue.

You can select from the dropdown list or start typing a time zone in the box to filter the list and get to the required time zone more quickly

5. The updated case time zone will be displayed in the Manage Cases menu:



The "Case Management" interface shows a table with the following data:

Case Name	Owner Username	Owner Fullname	Team	Security Level	Time Zone
R v Crippen	joe.hoy	Joe Hoy	Default Team	5	Europe/Riga

Why, When, Who



The Case Management functions are necessary to provide opportunities to manage the set of cases you have access to.



This function is undertaken whenever cases need to be managed.



This function is typically carried out by the following users:

- >> CSAS Administrator
- >> CSAS User

5.8 User Management

CSAS supports operation in standalone mode (where each instance of CSAS works independently, and does not connect to a local CSAS Server), and also in Server mode.

All users, whether using standalone mode or server mode, must belong to a Team and need to be assigned an appropriate security level.

5.8.1 Standalone Mode

In standalone mode, with no connection to CSAS Server, once the CSAS software has been installed on the user's PC they'll be asked to set up a local user.

CSAS in standalone mode only allows one user account to be set up per deployment, so there are no controls or options to allow additional users to be created or that allow the current user to be changed.

If a new user needs to be set up for a standalone deployment, CSAS and its data will need to be deleted and a fresh install initiated to set up a new user.

5.8.2 Server Mode

The expected typical installation of CSAS is within a networked deployment, where a distributed population of CSAS copies connect to a central CSAS Server within an organisation. In this use case, a local CSAS administrator will set up all user accounts centrally via CSAS Server. Depending on the authentication method used, the CSAS Administrator will either provide each registered user with a username and password or will arrange for their accounts to be linked to the local Active Directory service.

5.8.3 Assigning a Team

Users belong to Teams; in Server mode a CSAS Admin can add multiple users to a single Team and individual users can belong to more than one Team. Teams are part of an Organisation, a CSAS Admin can create multiple Teams within a single Organisation.

5.8.4 Assigning a Security Level

Each new user will need to be assigned the appropriate security level for the Team the new user wants to join – their security level must be equal to or higher than the minimum-security level of the Team they are being assigned to. The minimum user security level for each Team is stipulated when a Team is created.

5.9 Case Workflow

The basic stages of a CSAS-enabled digital forensics analysis case are as follows:

	New Case	Create a new case Set date prefiltering limits Import source data files	New Case
	Import Files	Add file continuity details Update file details with any missing information	Importing Files
	Attributions	Add identifying colours and attribution names to identifiers Set attribution validity dates Import existing attributions	Attributions
	Dashboard	View a summary of important case information View imported data in a grid View imported data in a map	Dashboards
	Case Hub	Filter data and create case snapshots Export map content to Powerpoint	Case Hub
	Case Outputs	Create intel reports and court exhibits from the imported data	Case Outputs
	Analytics	Create Fast Time reports Analyse imported data with a range of powerful queries	Analytics
	Case Lifecycle	Add/remove source data files Add/edit attributions Create/edit snap shots Create maps & analytical reports	

Each stage of this process is described in detail in this guide.

5.10 Regulatory & Accreditation Support

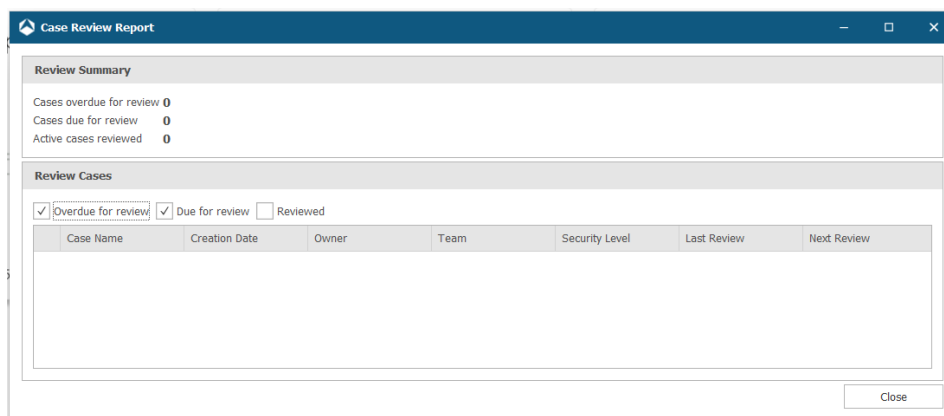
Most, if not all, instances of CSAS will be deployed in organisations that are subject to some form of regulatory oversight (such as the UK Forensic Science Regulator's Code of Practice) and will generally have to obtain and maintain some form of procedural or quality accreditation (such as ISO17025). CSAS offers a number of features to help organisations and individual users meet the requirements of such regulatory environments.

5.10.1 Case Review

CSAS includes a simple Case Review function, which provides an indication to users when created cases, whether they're actively being worked on or not, may need to be reviewed.

For instances of CSAS operating in Standalone Mode, when not connected to an organisations' CSAS Server, the Admin menu offers a Case Review Report option. The report lists all cases 'owned' by the user that are approaching or have passed a review date.

In the initial version of Case Review, the review period is fixed at one year from the date the case was created; future iterations of the feature may provide more flexibility to set a different review period if required.



The report lists cases in three review states:

- » Cases overdue for review (more than one year since last review)
- » Case due for review (approaching one year since last review)
- » Active cases reviewed (recently reviewed)

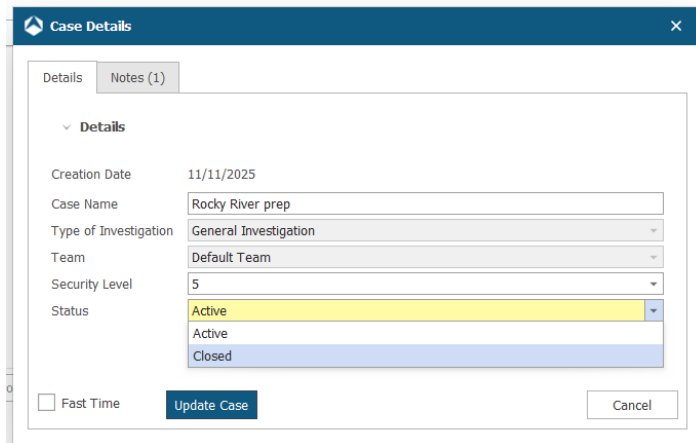
Opening a case (e.g. from the All-cases list on the CSAS Home page), constitutes a review, there are no specific actions required to indicate that a review has taken place. Case Reviews are only indicated for cases in the 'Active' state – see the next section for details of the Case Status feature.

5.10.2 Case Status & Case Notes

Many regulated processes require practitioners to capture 'contemporaneous notes' detailing the actions they perform whilst working on a case. Even in less rigorously defined processes it is often useful to have the option to make notes in a case to act as an aide memoire.

When a CSAS is open, the 'tools' menu offers access to the Case Details feature.

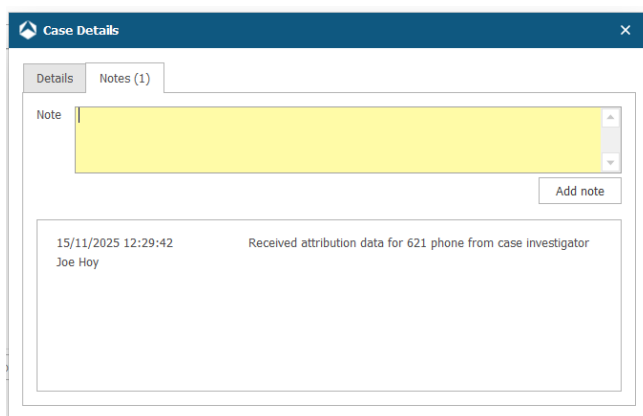
The first tab provides access to the basic case setup details that were entered when the case was first created – case name, type of investigation, Team, security level and time zone. It also provides access to an additional 'status' field.



Case Status defaults to 'Active', indicating that the case is actively being worked on and is therefore eligible for the Case Review process. If a case is no longer being actively worked on, but hasn't been deleted or archived, it can be set to the 'Closed' status, which removes it from the Case Review process.

Of course, if further work is required for a 'closed' case, it can be reverted to the 'active' state again at any time.

A second tab in the Case Details popup provides access to the Case Notes feature.



Simple, text-based notes can be added to a case at any time. Each new note is listed alongside the timestamp and the details of the user who added it.

Details of new notes are captured in the case audit log and notes cannot be altered or deleted after being added.

Click 'Update Case' on the Details tab to save any changes made to the case details or case notes.

5.10.3 Intel-only Users

In regulated organisations, there are likely to be rules in place that dictate the level of training a staff member must have before being able to access certain types of data or application. For example, the procedures may indicate that only staff members who have completed an accredited series of training courses in the use of CSAS are permitted to produce evidential outputs from that application.

To support users who are required to adhere to such restrictions, in server-based CSAS deployments, it is possible to create user types with different levels of access and capability.

Full users, who would be expected to have completed full training in CSAS and its use, are able to access all functions and have unrestricted ability to output analytical and

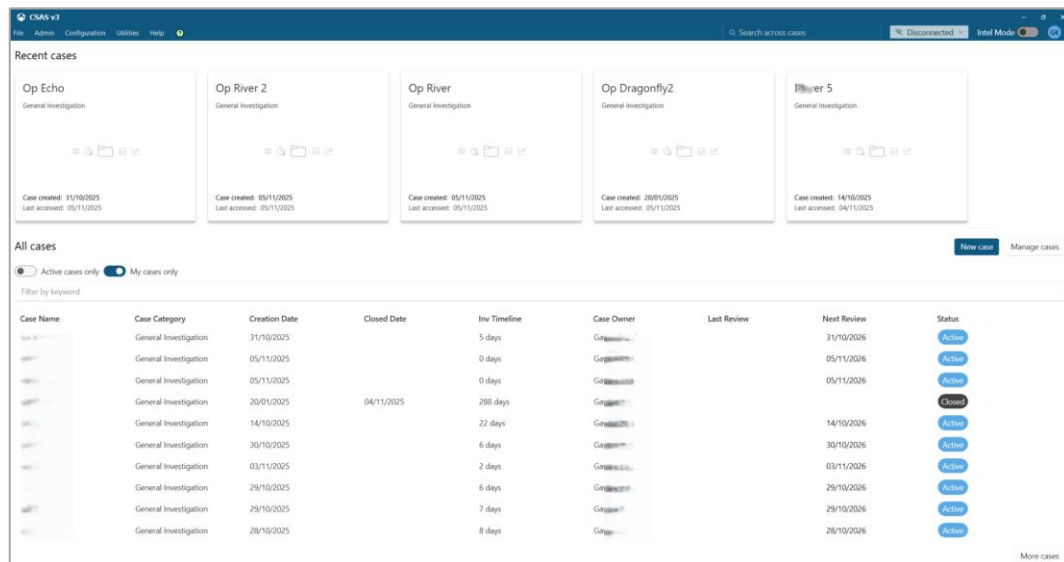
evidential product from their cases.

Intel-only users can also be created. Although they have the same set of CSAS features, any output they create from a case will be watermarked with 'Intel-only' indications, showing that the product they create should not be permitted to be used as evidence, unless it is first reviewed and approved by a fully trained colleague.

The user type is set in the CSAS Server admin portal by the local CSAS administrator. Users can be converted to 'full' status once they meet their requirements of their particular organisation.

6 CSAS Home Screen

The CSAS home screen is the main landing page for CSAS and is displayed after you log in – it provides access to new and existing cases. Scrolling down the home page, users can find links to other Forensic Analytics products and services as well as contact details should you require support:



The home page displays up to the five most recently accessed cases across the top of the screen for easy access. Clicking on one of these recent case icons will open that case. Below recent cases, users can find links to create a new case and manage all their cases.

The 'All cases' section of the home page displays more detailed information about the ten most recently accessed cases. Below that, the 'More cases' button allows users to access the full list of cases that they can open.

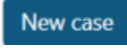
Use the scroll bar on the right to access Product and Services information and links to CSAS Support at the bottom of the screen.

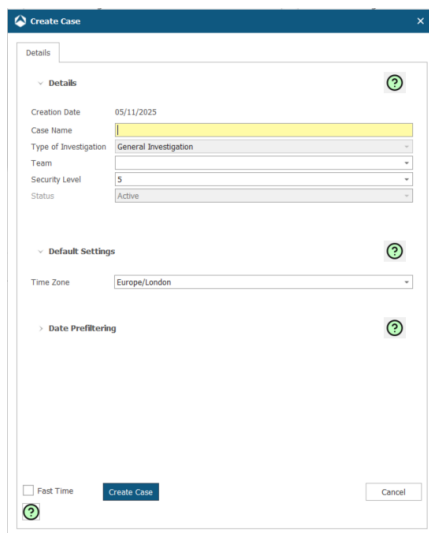
6.1 Using the CSAS Home Navigation Pane

The following functionality can be accessed directly from the CSAS home page or from the File drop down menu available from the top bar as discussed in section 5.5.1.

- » New Case
- » Manage Cases
- » All Cases
- » Case Search
- » Cross Case Search

6.1.1 New Case

Selecting the New Case icon  opens the 'Create Case' pop-up window:



From this pop-up window you can create a new case by populating the 'Case Name' text field and selecting from the drop-down menus then clicking on the  button.

See Also

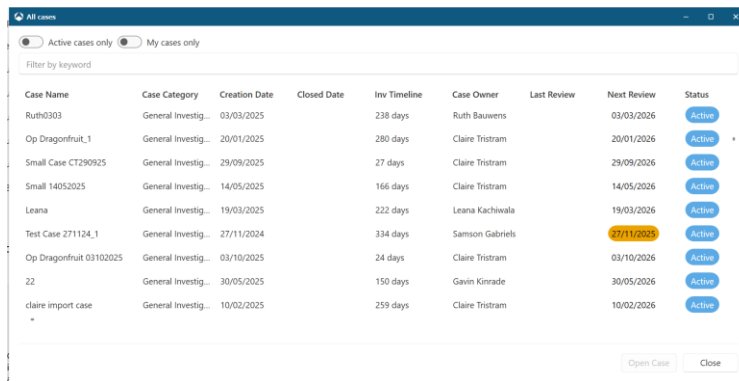
Setting up a New Case

6.1.2 Manage Cases

This button provides access to the same Manage Cases feature as is accessible via the Admin top line menu. See [Manage Cases](#).

6.1.3 Recent Cases and All Cases

To open a case in the Recent Cases section, click on it once. In the All-Cases section, double-click on a row to open the associated case. Clicking the More Cases icon, at the bottom of the All Cases table, opens a new window.



Case Name	Case Category	Creation Date	Closed Date	Inv Timeline	Case Owner	Last Review	Next Review	Status
Ruth0303	General Investig...	03/03/2025		238 days	Ruth Bauwens		03/03/2026	Active
Op Dragonfruit_1	General Investig...	20/01/2025		280 days	Claire Tristram		20/01/2026	Active
Small Case CT290925	General Investig...	29/09/2025		27 days	Claire Tristram		29/09/2026	Active
Small 14052025	General Investig...	14/05/2025		166 days	Claire Tristram		14/05/2026	Active
Leana	General Investig...	19/03/2025		222 days	Leana Kachiwala		19/03/2026	Active
Test Case 271124_1	General Investig...	27/11/2024		334 days	Samson Gabriels		27/11/2025	Active
Op Dragonfruit 03102025	General Investig...	03/10/2025		24 days	Claire Tristram		03/10/2026	Active
22	General Investig...	30/05/2025		150 days	Gavin Kinrade		30/05/2026	Active
claire import case	General Investig...	10/02/2025		259 days	Claire Tristram		10/02/2026	Active

This window lists all cases that you have access to in the current database. Users should check the status of the CSAS Server connection button to ensure they are configured for the correct database.

The 'Case Owner' field identifies the current case owner, who has permission to update and edit the case. Other users, who are members of the same team, will have read-only access to the case unless a change of owner is initiated in the Case Management menu.

If a case is available to you, double clicking on the case in the list will open it for viewing and, if you are the owner, editing.

The filter bar at the top of the grid allows you to search within the case list to find the case you want to open.

Stepped Procedure

1. From the Case Home page, you can open an existing case by clicking on the relevant case.
2. After a few seconds, the selected case opens and will default to the Import data screen.

Note: If files have already been imported, the selected case opens via 'Case Hub', if no files have been imported, the selected case will open via the 'Import Files' screen (unless you've selected a different landing page for your new and existing cases).

See also

- >> *Using Case Hub*
- >> *Case Management*

6.2 Using the Search Pane

The 'Search across cases' pane allows you to quickly search, within all Cases that you have access to, for cases that contain different types of Identifiers as follows:

- » MSISDN – phone numbers
- » IMSI – subscriber identifiers
- » IMEI – mobile device identifiers
- » VRM – vehicle registration marks, number plates, license plates
- » Attribution Name – the 'user's name' attributed to a phone number or other identifier
- » MAC Address – WiFi device identifier.
- » IP Address – Internet address assigned to a device
- » Site Name – cell site/tower name
- » Cell ID – identifier for a cell on a cell site

For a more focused search, you can search for just a particular identifier type and search for a partial or full identifier (for example a telephone number).

Just select the identifier type and then enter a partial or full identifier into the search box.

For partial searches, omit the initial '0' or international prefix from the number.

Clicking the  icon will open the 'Search Results' pop-up window:

Search

MSISDN

07700900

🔍

MSISDN 7700907268												
For best results, remove the initial '0' or country code from the MSISDN												
Drag a column header here to group by that column												
Matching Results	Tar...	Attribution	Attribution Start	Attribution End	Case Owner	CaseName	Activity In Case Start	Activity In Case End	Team Name	Location	Status	Acti...
→ 07700907268	No	Unknown 7			Ruth Bauw...	Op Dragonfruit	11/12/2025	19/01/2026	Default Team	Local	Available	Acti...
07700907268	Yes	Unknown 7			Ruth Bauw...	Op Dragonfruit	11/12/2025	19/01/2026	Default Team	Local	Available	Acti...
07700907268	No	Unknown 4			Ruth Bauw...	Ruth2808	28/08/2025	24/09/2025	CSAS Team	Server	Locked By: Ruth B...	Acti...
07700907268	No	Unknown 3			Ruth Bauw...	offline audit 2	20/11/2025	20/11/2025	Default Team	Server	Locked By: Ruth B...	Acti...
07700907268	No				Ruth Bauw...	Export/Import 3.14.0	10/02/2025	05/06/2025	Default Team	Server	Available	Acti...

196 matching results found

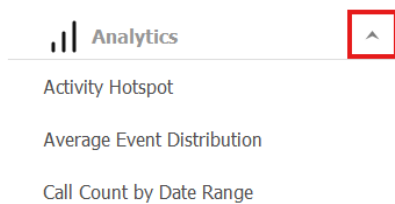
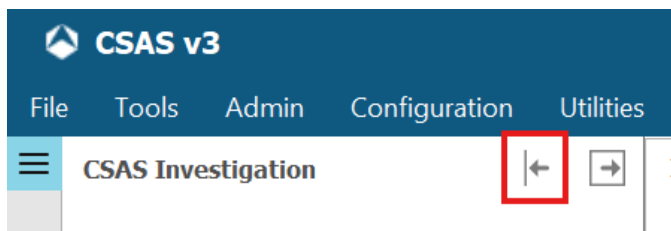
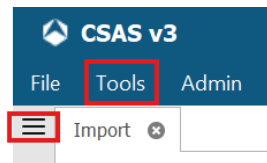
The search results provide a list of local and server cases, that you have permission to access, within which the searched for identifier was found, including details of the case location (local/server) and availability.

From the 'Search Results' pop-up window, you can select and open the case related to a matching result by clicking on the  button. The 'Case Hub' screen (or selected default case landing screen) is displayed when the case is opened.

7 Case Home Navigation Panel

The Case Home navigation panel is displayed once a case is opened. It occupies the left side of the screen and provides access to the features available in your current open case.

The same set of links are also provided from the 'Tools' dropdown menu included in the top row menus once a case is opened.



The navigation panel can be opened by clicking on the 'hamburger' menu icon located at the top left of the main CSAS window

The navigation panel confirms the name of the current open case and can be dismissed by clicking on the 'close' icon at the top right of the panel

Most features open when the associated navigation panel icon is clicked.

Some features have multiple screens, however, so the icon acts as dropdown menu. Click on the down arrow to view all options, then click on a specific menu item to launch the associated feature.

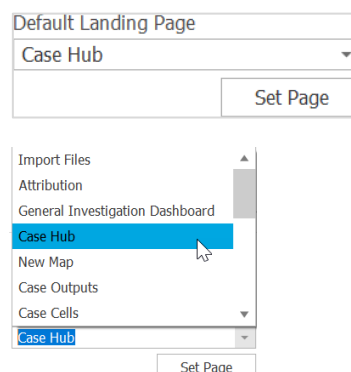
Each of the features is described in more detail in their own dedicated sections.

7.1 Changing the Default Landing Page

Unless otherwise configured, brand new CSAS cases open in Import.

The 'default landing page' function allows you to choose an alternative CSAS screen to open existing cases in.

All screens are selectable from the drop-down menu. Just select the screen from the drop-down menu, then to set that screen as your default case landing page, click the **Set Page** button.



The next time you login to an existing case, this will be your case landing page.

8 Setting Up a New Case

This function allows you to set up a new CSAS case.

When a new case is created, the person who created the case is the initial case owner. The owner of a case is shown in the 'Case Management' window (see *Case Management*). In server mode, where cases can be shared with other members of the same Team, you can change the owner of a case by selecting 'Change Owner' from the 'Actions' drop-down menu in Case Management (see *Case Management* > *Change Owner*).

If you aren't the case owner but are in the same team as the case (and have a suitable security level) will have read-only access to the case, which means you can view, filter and analyse data in the case, if it is saved to CSAS Server, but are not able to add, change or delete data.

Other users are not able to access a case, even if they have permission to do so if the case has been checked out and downloaded to the case owner's local CSAS database.

Selecting 'New Case' from the home page or admin menu opens the 'Create Case' pop-up window:

Details for the new case are entered into CSAS using the 'Create Case' pop-up window. Setting up a new case involves entering a unique name for the 'Case Name'.

It is necessary to populate the 'Case Name' field with a unique case name. (CSAS will warn if the suggested name is not unique) to create a new case. Users may be required to select a team if multiple options are available. The other fields will be set to use default options but can be changed based on the needs of the case.

The following information describes the various fields and drop-down menus in the 'Create Case' pop-up window:

- » Case Name - this field allows you to enter the required Case Name.
- » Type of Investigation – Currently only 'General Investigation' is available although additional case types will be supported in future releases.
- » Team – in Server mode, this selects the Team the case will be linked to (in Standalone mode there is only one 'Default Team' created). Only Teams that you are a member of will be listed here. By default, cases are shared with all members of the linked Team, who will all have read-only permissions for the case. If a case is sensitive and shouldn't be widely shared, it may be sensible

to create (or ask the CSAS Administrator to create) a new Team with more limited membership to link the case to.

- » Security Level – each user within a Team (and indeed, each Team itself) is assigned a Security Level (from 1, lowest security to 5, highest security). Team members will only be able to view and access cases that are linked to their Team and are at or below their Security Level. An alternative method of ensuring that sensitive cases are not shared unnecessarily with all members of a Team is to set some Team members at low Security Levels and ensure that sensitive cases are assigned high security levels.

Note: For security reasons the security level field defaults to the highest security level to which you have access.

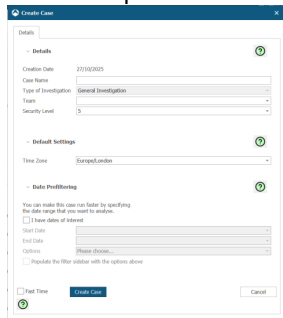
- » Time Zone – this defaults to the time zone the host PC (or virtual machine) is set to, but can be changed if, for example, a specific case contains data for a different country or a different time zone within your country. Changing this value affects how event timestamps are presented in CSAS. If it becomes necessary to change the time zone associated with a case, this can be achieved in the Manage Cases menu.
- » Date Prefiltering – this offers a means of reducing the amount of data imported into a case, which in turn can have an effect on CSAS's performance when working on or uploading/downloading that case. Date prefiltering ensures that the Import Files function only imports events that are between the selected 'start' and 'end' dates will be imported into the case, but there are three options:
 - Inform me if the file does not contain events between the selected dates – during the Import Files phase, if files are selected for import that do not contain events for the selected period, you will be informed but the file will not be skipped.
 - Only import if the file contains events between the selected dates - during the Import Files phase, if files are selected for import that do not contain events for the selected period, the file will be skipped.
 - Only import records between the selected dates – during the Import Files phase, if files are selected for import that contain events that span across the selected dates, only those events within the dates will be imported, events outside the dates will be skipped.
 - The 'Populate the filter sidebar with the options above' checkbox feature ensures that the 'Date/Time' filter in the 'Filter' sidebar is pre-populated with the selected dates as the earliest and latest dates for the case that can be filtered to.
- » Fast Time – ticking this option automatically enables the Auto-attribute function in Import Files and activates a 'suggested next step' button at the foot of each screen.

Why, When, Who

	This function is necessary to allow you to create a unique new case to import data into.
	This function is undertaken when a new case or investigation starts.
	This function is typically carried out by the following users:  CSAS User (and above)

Stepped Procedure

1. From the CSAS Home screen click the New case button. The 'Create Case' pop-up window opens:

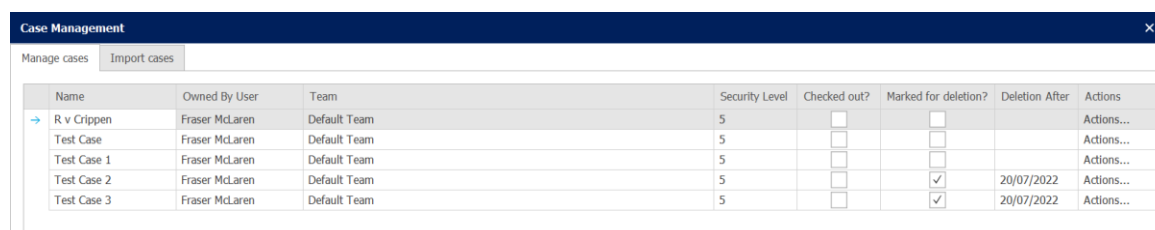


2. In the 'Details' pane, enter in the text field the name of the new Case (for example Test Case 1) - if the case name you enter is not unique a warning will be displayed, and you'll have to edit the case name before you can continue.
3. Then optionally, if you don't want to use the default values, using the drop-down menus to choose the Team (for example Default Team) and Security Level (for example '5').
4. If you wish to change the time zone associated with the case, you can select a different time zone from the dropdown menu.
5. Optionally, if you want to add pre-filtering dates, using the calendar drop-down menus, select the required 'Start Date' and 'End Date'. **Note:** Only events that are between the selected 'start' and 'end' dates will be imported into the case.
6. From the 'Options' field, using the drop-down menu select one of the options.
7. If required, tick the 'Populate the filter sidebar with the options above' checkbox.
8. To create the new case, click on the **Create** button. The 'Create Case' pop-up window closes and the 'Import Files' screen opens:

9 Importing and Exporting Cases

This function allows you to import existing v2 and v3 cases into CSAS v3 and export CSASv3 cases.

This function is selectable from the 'Case Management' window. From the top ribbon, select *Admin > Manage Cases* - the 'Case Management' pop-up window opens:



Name	Owned By User	Team	Security Level	Checked out?	Marked for deletion?	Deletion After	Actions
R v Crippen	Fraser McLaren	Default Team	5	☐	☐		Actions...
Test Case	Fraser McLaren	Default Team	5	☐	☐		Actions...
Test Case 1	Fraser McLaren	Default Team	5	☐	☐		Actions...
Test Case 2	Fraser McLaren	Default Team	5	☐	☒	20/07/2022	Actions...
Test Case 3	Fraser McLaren	Default Team	5	☐	☒	20/07/2022	Actions...

To export a case you need to select the 'Manage cases' tab. To import a case you need to select the 'Import cases' tab.

9.1 Importing a Case

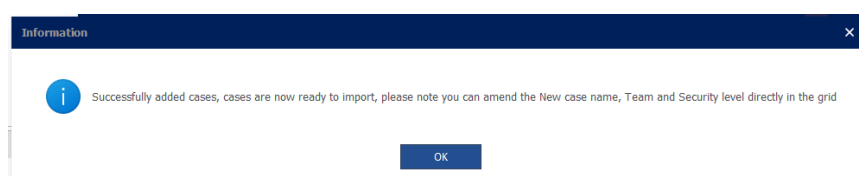
This function allows you to:

- » Import a CSAS v2 zip file so you can migrate CSAS v2 cases to CSAS v3.
- » Import a CSAS v3 zip file.

CSAS v3 processes source data files in generally the same way that CSAS v2 did, but there are some instances where CSAS v3 can extract more data from a source file than CSAS v2 could. For this reason, when migrating cases from CSAS v2 to CSAS v3 the source data files will be reprocessed in CSAS v3, rather than simply importing the data that was held in the original CSAS v2 case. CSAS v2 attributions are imported without amendment.

Stepped Procedure

1. The required cases must have been exported from CSASv2 or CSASv3 prior to commencing this process and the exported zip file must be available for import.
2. From the 'Case Management' window, click the 'Import cases' tab, then at the bottom of the window, click 'Browse' and select the location of a CSAS zip file you want to import to your latest version of CSAS:
3. Select the required zip file and click 'Open'
4. If a valid case is found in the selected zip folder, you'll see a popup confirming that the selected case is now ready for import.



5. The case you select to import is shown in the Import Cases grid:

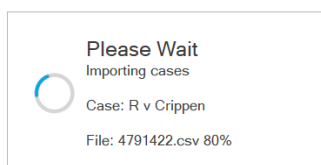


	Case name	New case name	Team	Security level	CSAS version	Open after Import
☒	R v Crippen	R v Crippen_1	Default Team	5	Version 3	☐

6. If necessary, in the Import Cases grid you can:

- » Change the 'New case name' - this is the name the case will be known by in CSAS v3, so if the original case name is not unique or if you want to change or amend it for any other reason, there is an opportunity to do that before the import is triggered. If the case name already exists in your local database, CSAS will add an index number to the end of the case name - e.g. R v Crippen_1
- » Change the 'Team' the case will be linked to in CSAS v3 - the Import Cases grid will show the default team, but you can choose a different one if you have access to other teams.
- » Change the 'Security level' that will be applied to the case in CSAS v3 - the Import Cases grid will select the highest security level associated with the selected team, but you can choose a different level if required.
- » The menu will confirm the CSAS version (v2 or v3) that was used to create the case.
- » You have the option of automatically opening the case as soon as it is imported by ticking the 'Open after Import' checkbox.

7. When you click on the **Import** button, your case will start importing and a progress message is displayed:



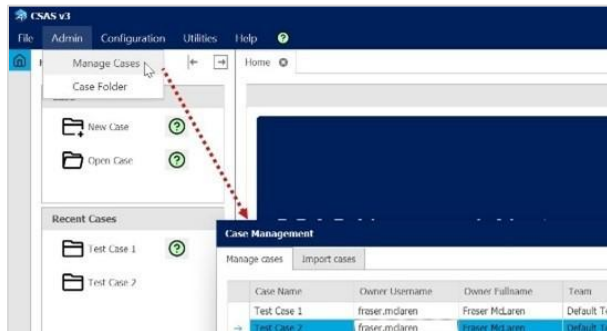
8. Once the import process has successfully completed, the import case will be available to access via the Open Case menu.

Troubleshooting

The most common issue associated with importing a CSAS case is that the selected zip file is not one that contains an exported CSAS case. Please make sure you select the correct zip file to import.

9.2 Exporting a Case

Cases can be exported from CSASv3, to be archived or to share a case with another Standalone user, using the *Admin > Manage Cases* tab:



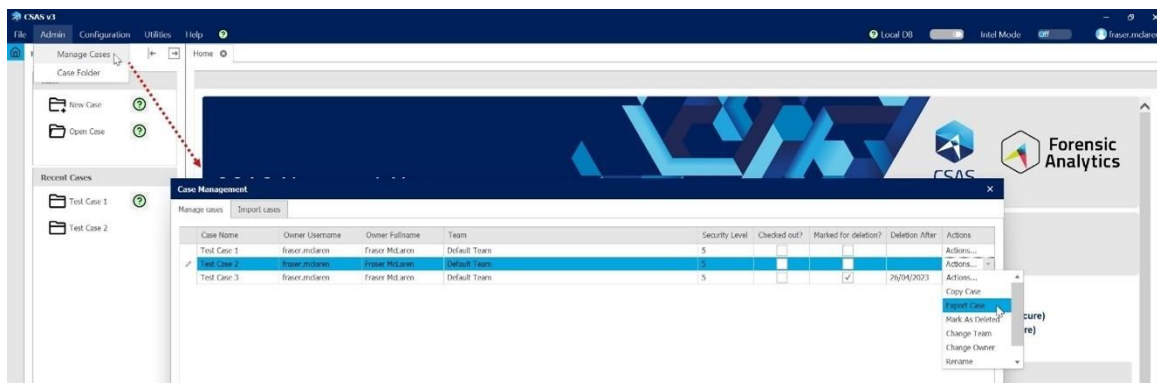
Note: Cases can only be exported in the CSASv3 format, it is not possible to export a case in the CSASv2 format, so exporting v3 cases to be imported into v2 is not supported.

The exported zip file contains a small database containing only the data from the selected case, copies of all imported case data files, copies of all created case output files, all case attributions. This should allow a full working copy of the case to be created when it is imported into another copy of CSAS.

It is also possible to set CSAS to delete the original version of the case once the export has successfully completed – this allows the case export function to also act as a basic 'case archive' function. Cases that no longer need to be retained in a 'live' CSAS database, but that might one day need to be reviewed, can be exported and deleted, with the exported zip file being used as an archived copy of the case.

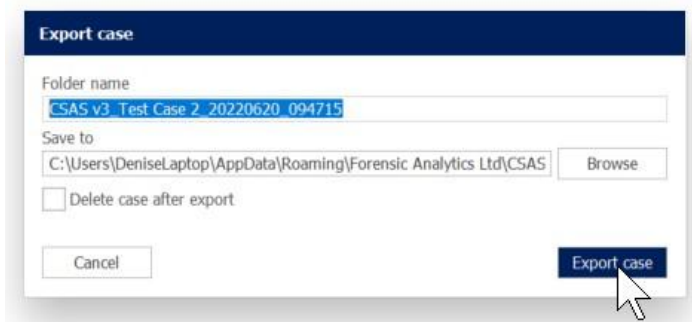
Stepped Procedure

1. From the 'Manage cases' tab, select the case you want to export by clicking on the 'Actions...' drop-down menu and selecting 'Export Case':

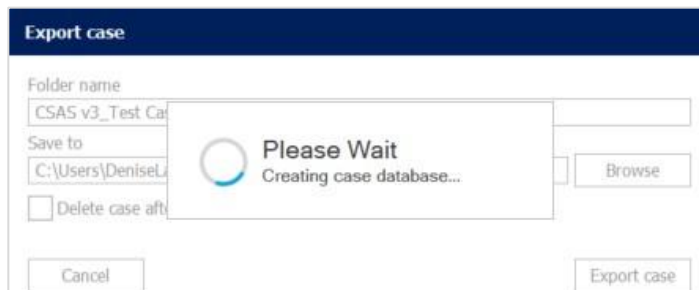


Note: You can also access the same drop-down menu by right-clicking on the selected grid row.

- The 'Export case' pop-up window opens:



- CSAS suggests a folder name and 'save to' location for the zip file, however, you can change both – CSAS will remember the last used 'save to' folder destination and adds that automatically the next time. You can also decide whether you want to automatically delete the case once it has exported.
- Clicking the Export case button starts the export process:



- Once the case has successfully exported, you can provide the zip file to a colleague to import into their CSAS instance.

Why, When, Who

	This function is necessary to allow you to export and import CSAS cases so they can be shared by users if CSAS Server isn't available.
	This function is undertaken at any time you want to import or export a case between copies of CSAS.
	This function is typically carried out by the following users: » CSAS User

10 Importing Files

This function allows you to import source data files for analysis by CSAS.

Source data files belong to a case. All source data files are imported using the 'Import Files' screen, with the exception of Attribution files, which can also be imported using the 'Attribution' screen. Any mix of supported file types can be imported together and the files are recognised and imported in one operation – which is different to how the equivalent feature in CSAS v2 worked, meaning the CSAS v3 process is simpler and more streamlined: there is also a File Import Wizard to help you import files which have failed parsing.

After setting up a new case, CSAS opens the 'Import Files' screen automatically.

When accessing an existing case, you can access Import Files by navigating to the Home Navigation pane and clicking on the Import Files button .

10.1 Supported Data Types

This section lists the different source data file formats which can be imported into CSAS for comms data analysis. These are:

- » .xls files.
- » .xlsx files
- » .csv files
- » .xml files (currently for some handset download and drone log files only)
- » .zip files (currently for Encrochat/Venetic files and some social media data types)
- » .txt files (currently only for specific US CDR formats)
- » .ivo files (containing Berla vehicle download data)

Note: The vast majority of source data files will be in .csv and .xls/xlsx formats.

The data types contained in the files that CSAS currently recognises include:

- » Communications Data – CDRs, DDRs, cell/tower dumps, cell address files for selected mobile, landline and VoIP (voice over IP) networks
- » Device location – ping and timing advance data from selected networks
- » ANPR/ALPR data – many different formats of number plate recognition data
- » Handset downloads
 - MSAB XRY and XAMN outputs in xlsx and xml formats
 - Cellebrite UFED outputs in xlsx format
 - Blue Lights Digital Odyssey outputs in xlsx format
 - Radio Tactics Aceso outputs in xml format
- » Selected vehicle telematics and GPS tracker data
- » Selected social media/Internet communication logs.

- » Selected vehicle download/extract formats – e.g. Berla.
- » Broadband router DHCP/usage log files

Note: Almost any additional types of data can be imported using the File Import Wizard or the set of CSAS rescue templates.

If CSAS is unable to import a source file type, or if it fails to recognise a file that should be recognised, please use the *File Import Wizard* first, if the source file type still cannot be imported, then contact CSAS Support. See [Import Files Issues](#) for more details about how to deal with unrecognised files.

Once a new case has been set up in CSAS, the source data files can be imported ready for analysis and mapping. All source data files are imported using the Import Files screen.

Why, When, Who

	This function is necessary to allow the import of source data files.
	This function is undertaken at any time.
	This function is typically carried out by the following users:
	» CSAS User

10.2 Layout

The Import screen is laid out in two sections:

- » File Import List - the top section lists the files that have been selected for import
- » Imported Files Grid - the bottom section lists the files that have been imported.

Each section has its own set of controls and features.

10.3 Grid and Controls

10.3.1 Import Files Grid

The 'Import Files' grid currently has four modes – 'Basic', 'Advanced', 'Disclosure' and 'Date Range'.

Basic

In 'Basic' mode the Import Files grid displays basic information about each imported file:

- » Import Status
- » Filename
- » Parser Version
- » Subject Identifier
- » File Type
- » Details

Basic Advanced Disclosure Date Range ?

	Status	Filename	Parser Version	Subject Identifier	File Type	Details	Actions
→	Imported	2421 Home Address GN06 POL.xlsx	2.3.0.130		POI Layer	Information: The data file is in a Rescue format rather than an original source file and has been manually	...
	Imported	2421 0213.xlsx	2.3.0.130	07700902421	CDR	Information: Instance of CDR Record not loaded - StartTime or Both PhoneA/PhoneB are not populated	...
	Imported	2421 cellebrite.xlsx	2.3.0.130	35201770090268	Handset	Information: Invalid Cells not loaded or Blank lines encountered	...
	Imported	3852 Home Address GN06 POL.xlsx	2.3.0.130		POI Layer	Information: The data file is in a Rescue format rather than an original source file and has been manually	...
	Imported	3852 0213.xlsx	2.3.0.130	07700903852	CDR	Information: Invalid Cells not loaded or Blank lines encountered	...
	Imported	ANPR data - BS79PTS only v1.xls	2.3.0.130	BS79PTA	ANPR		...
	Imported	ANPR data - multiple VRMs v1.xls	2.3.0.130		ANPR		...
	Parser Failed	EE Timing Advance.bt			Unknown	User Action Required: Requested phone number unknown. Open 'Update file details' via the actions menu	...
	Imported	GN06 - events & locations.xlsx	2.3.0.130		POI Layer	Information: The data file is in a Rescue format rather than an original source file and has been manually	...
	Imported	Telematics BS79PTA.xlsx	2.3.0.130	BS79PTA	Telematics		...

Requires Attention Some files require attention, click on Advanced for more information.

Case Contains a total of 51487 records.

? Print or Export Attributions >

Advanced

In 'Advanced' mode a more detailed grid is displayed:

Basic **Advanced** Disclosure Date Range ?

	Status	Filename	Attribution	Subject Identifier	File Type	Details	Actions
→	Imported	2421 Home Address GN06 POL.xlsx			POI Layer	Information: The data file is in a Rescue format rather than an original source file and has been manually	...
+	Imported	2421 0213.xlsx	Multiple	07700902421	CDR	Information: Instance of CDR Record not loaded - StartTime or Both PhoneA/PhoneB are not populated	...
+	Imported	2421 cellebrite.xlsx	Unknown 3	35201770090268	Handset	Information: Invalid Cells not loaded or Blank lines encountered	...
+	Imported	3852 Home Address GN06 POL.xlsx			POI Layer	Information: The data file is in a Rescue format rather than an original source file and has been manually	...
+	Imported	3852 0213.xlsx	Unknown 5	07700903852	CDR	Information: Invalid Cells not loaded or Blank lines encountered	...
+	Imported	ANPR data - BS79PTS only v1.xls	Unknown 1	BS79PTA	ANPR		...
+	Imported	ANPR data - multiple VRMs v1.xls			ANPR		...
+	Parser Failed	EE Timing Advance.bt			Unknown	User Action Required: Requested phone number unknown. Open 'Update file details' via the actions menu	...
+	Imported	GN06 - events & locations.xlsx			POI Layer	Information: The data file is in a Rescue format rather than an original source file and has been manually	...
+	Imported	Telematics BS79PTA.xlsx	Unknown 1	BS79PTA	Telematics		...

Requires Attention Some files require attention, click on Advanced for more information.

Case Contains a total of 51487 records.

? Print or Export Attributions >

This mode additionally shows:

- » Attribution name for each file
- » CSAS file format ID
- » Call/Event count
- » Cell/Location count
- » The imported date
- » The file creation date
- » An indication of whether Intel mode event processing was enabled when the file was imported
- » An indication of whether the file contains any Intel mode events.
- » Details of the CSAS version and Parser version that were used to import each file

Disclosure

In 'Disclosure' mode the grid displays columns which can be used to create disclosure reports:

Basic

Advanced

Disclosure

Date Range

	Call/Event count	Cell/Location count	Format ID	Provider	Data from	Data to	File Status	Sensitivity	Comments/notes	Parser Version	Actions
▼	=	=	📄	📄	= ▼	= ▼	= ▼	= ▼	📄	📄	
→	no responsibility for the accuracy of this data file.	0	1	CDR48-UK4...	UK_Generic	01/01/0001	31/12/9999	Used	Non-Sensit...	2.3.0.130	...
		488	98	CDR71-UK5...	UK_O2	11/03/2024	21/03/2024	Used	Non-Sensit...	2.3.0.130	...
		515	13	HSD88-UK7...	Cellebrite	12/03/2024	21/03/2024	Used	Non-Sensit...	2.3.0.130	...
	no responsibility for the accuracy of this data file.	0	1	CDR48-UK4...	UK_Generic	01/01/0001	31/12/9999	Used	Non-Sensit...	2.3.0.130	...
		1338	248	CDR71-UK5...	UK_O2	12/03/2024	30/03/2024	Used	Non-Sensit...	2.3.0.130	...
		11	11	ANPR02-UK...	UK_Met	19/03/2024	19/03/2024	Used	Non-Sensit...	2.3.0.130	...
		128	11	ANPR02-UK...	UK_Met	19/03/2024	19/03/2024	Used	Non-Sensit...	2.3.0.130	...
	identity.	0	0			01/01/0001	31/12/9999	Used	Non-Sensit...		...
	no responsibility for the accuracy of this data file.	6	6	CDR48-UK4...	UK_Generic	18/03/2024	18/03/2024	Used	Non-Sensit...	2.3.0.130	...
		59	57	ANPR01-UK...	UK Tracker	19/03/2024	19/03/2024	Used	Non-Sensit...	2.3.0.130	...

Requires Attention

Some files require attention, click on Advanced for more information.

Case Contains a total of 51487 records.

Print or Export

Attributions >

The disclosure status of each file – including whether data from the file was used in the investigation and whether the data is considered to be sensitive or not – is displayed in the grid.

The disclosure status information, plus any comments you may wish to add, can be set in the Update File Details popup.

Note: For information about creating disclosure reports, see *Using the Case Reports Button*.

Date Range

In 'Date Range' mode, at the far-right side of the grid, you'll see a coloured 'coverage' bar chart indicating the date range covered by each file, allowing the overlap between all files imported into a case (and also any gaps in date coverage) to be quickly determined:

Drag and drop files here

Browse to files...

☐ Auto attribute

Import files

Remove selected

Remove All

?

☐ Basic
 ☐ Advanced
 ☐ Disclosure
 ☒ Date Range

?

Subject Identifier	Attribution	File Type	Details	Format ID	Provider	Data from	Data to	File Status	Sensitivity	Comments/notes	8/2012	9/2012	Actions
07700900177		CDR		CDR23-UK3...	UK_T-Mobile	29/08/2012	05/09/2012	Used	Non-Sen...				...
07700900177		CDR		CDR23-UK3...	UK_T-Mobile	29/08/2012	05/09/2012	Used	Non-Sen...				...
07700900177		CDR		CDR24-UK4...	UK_T-Mobile	29/08/2012	05/09/2012	Used	Non-Sen...				...
07700900597		CDR		CDR23-UK3...	UK_T-Mobile	14/08/2012	02/09/2012	Used	Non-Sen...				...
07700900597		CDR		CDR23-UK3...	UK_T-Mobile	14/08/2012	02/09/2012	Used	Non-Sen...				...
07700900597		CDR		CDR24-UK4...	UK_T-Mobile	14/08/2012	02/09/2012	Used	Non-Sen...				...
07700900621		CDR	File Problem: Instanc...	CDR01-UK01...	UK_O2	14/08/2012	11/09/2012	Used	Non-Sen...				...

4

Parsing and Syncing

All files have been imported, proceed to Attribution.

Case Contains a total of 4139 records.

?

Print or Export

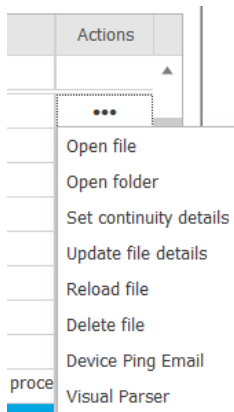
Attributions >

10.3.2 Generic Grid Controls

The 'Import Files' grid shares a common set of filtering and layout controls with the other grids in CSAS. Details of how to apply filters, customise the column layout and other grid control options are provided in *Grid Filtering and Controls*.

10.3.3 Right-click Controls and Actions Menu

Once the source data files have been imported, you can choose different actions by left or right-clicking in any row or in the 'Actions' column:



» Open File – opens the selected file in the appropriate file viewer - xls/xlsx files get opened in Excel (or an open office equivalent if installed), csv files get opened in notepad.

» Open folder – opens the CSAS case folder that the imported source file has been copied to.

» Set continuity details – provides an opportunity to add details about where each file came from and how it was acquired (you multi-select rows and add the same details to multiple files if required).

» Update file details – provides an opportunity to manually add missing file details, such as the subject identifier for the file and the date range.

» Reload File – deletes and reimports the file

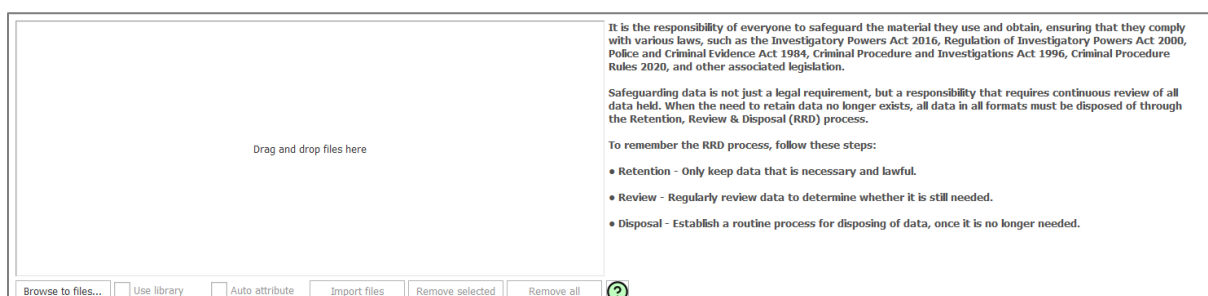
» Delete file – deletes the selected file from the case (you can multi-select files and delete them en masse if required).

» File Import Wizard/Device Ping Email – either option is shown depending on circumstances and open the general File Import Wizard or the specific Device Ping pop-up window.

» Visual Parser – launches the selected file in the Visual Parser so that the parsing rules and actions employed to process that file can be viewed.

10.4 Importing Files

Once the 'Import' screen opens, you can select new files to be imported and view files that have already been imported. Before doing this, you should read the warning message at the top of the import window (only appears for UK users):



You can 'drag and drop' source data files from a Windows file explorer pop-up into the

import window or browse for files using the **Browse to files...** button. If you drag an entire folder into the import window, CSAS will import all files found in the folder and in any sub-folders – in this sense it replicates the 'import all files in path' feature found in CSASv2.

Multiple files can be added to the same import operation by using the **Browse to files...** button or dragging & dropping multiple times to select files from different locations.

If incorrect files are accidentally added to the import list, they can be removed from the list before being imported, by highlighting the file in the list and clicking the **Remove selected** button; if all files need to be removed from the list prior to importing them, click on the **Remove All** button.

The 'auto-attribute' feature can be used as a time-saving option, by automatically assigning attribution colours and a generic attribution name ('Unknown N') to each subject identifier as the files are imported. Tick the checkbox to activate this feature as necessary.

The 'use library' feature is a facet of the Attribution Library and instructs CSAS to check for unassigned attributions in the Library when importing new files.

You begin the import process by clicking the 'Import Files' button. Once an import has started, the 'Import Files' button changes into a 'Cancel' button, allowing you to cancel the import process if you need to.



The horizontal bar at the bottom left-hand corner of the window shows you the overall parsing (processing) progress, and the bar alongside each file name shows you the progress for each individual source data file.

☒ Basic
 ☐ Advanced
 ☐ Disclosure
 ☐ Date Range
 

	Status	Filename	Subject Identifier	File
☐	Imported	anonymised_174_VF GPRS.csv		
☐	Imported	anonymised_173_02 voice.csv		
☐	Imported	anonymised_172_02 GPRS.csv		
☐	Imported	anonymised_171_H3 voice.csv		
☐	Imported	anonymised_170_H3 IPLOCNS.csv		
☐	Imported	anonymised_169_EE.csv		
☐	Imported	anonymised_DDR.xlsx		
☐	Imported	Anonymised NAS ANPR.csv		
☐	Syncing	367700902758418.zip		
☐	Syncing	2421 anonymised.xls		

Parsing and Syncing
 Parsing and Syncing, Please Wait.

The states that can be shown for imported files are:

- » No fill colour – pending, queued for import but not started yet
- » Yellow – parsing and syncing (writing to the database) in progress
- » Green – successfully imported.
- » Orange – issues encountered or file has no data within prefiltering date range
- » Red – file unrecognised, not parsed, empty or failed in some other way.

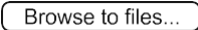
Note: Additional information related to files in the orange or red states may be shown in

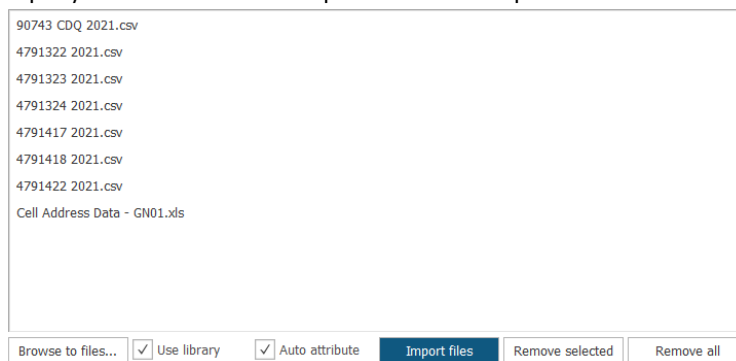
the 'details' column in the grid.

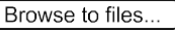
The overall progress bar may stay yellow for some seconds after all of the imported files have moved to the green 'Imported' state. During this time, CSAS is calculating any required 'override cell' records and syncing the data to the database – in server mode, this process may be delayed if the network connection to CSAS Server is slow.

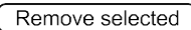
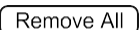
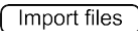
Note: If a source data file does not contain the prefilter date range selected in 'Setting Up a New Case' then the file will not be imported and may be coloured orange. If a source data file fails parsing and is coloured red, you can right-click on the necessary failed file(s) and select from the drop-down menu 'File import wizard'. Using the wizard, you can select column data types, data formats and select the row event type etc. By doing this you are effectively setting up manual parsing instructions for the failed file(s).

Stepped Procedure

1. Create a new case or open an existing case to import the files into. A new case will open directly into the Import Files screen; in an existing case it may be necessary to select  Import Files from the case navigation panel.
2. The files to be imported can be drag/dropped into the window at top left (where it says 'drag and drop files here') or you can click on the  button, a new file explorer window opens where you can browse and select the source data files you want to import.
3. In your Windows file explorer window, highlight the source data file(s) you want to import then click on the  button. The source data files selected will be displayed in the browser pane of the Import screen:



Multiple files can be added to the same import operation and the  button can be used multiple times to select files from different locations.

4. If incorrect files are accidentally added to the import list, they can be removed from the list before being imported, by highlighting the file in the list and clicking the  button; if all files need to be removed from the list prior to importing them, click on the  button.
5. The 'auto-attribute' feature can be used as a time-saving option, by automatically assigning attribution colours and a generic attribution name ('Unknown N') to each subject identifier as the files are imported. Tick the checkbox as necessary.
6. Once the required set of source files has been selected, click on the  button. CSAS will begin Parsing the files. The horizontal bar at the bottom left-hand corner of the window will show the overall parsing progress and the bar alongside

each file name will show the progress for each individual source data file.

	Status	Filename	Subject Identifier	File Type	Details	Actions
☐	Imported	90743 CDQ.csv	07700900621	CDR		...
☐	Imported	4791324.csv	07700900177	CDR		...
☐	Imported	4791418.csv	07700900597	CDR		...
☐	Imported	4791417.csv	07700900597	CDR		...
☐	Imported	4791322.csv	07700900177	CDR		...
☐	Imported	4791422.csv	07700900597	CDR		...
☐	Imported	Cell Address Data - GN01.xls		Cell data		...
☐	Imported	4791323.csv	07700900177	CDR		...
☐	Pending	colocation test end cells prep.xlsx				...

Parsing and Syncing Parsing and Syncing, Please Wait.

Case Contains a total of 4881 records imported in 1.17 seconds

Print or Export Attributions >

- If you wish to stop the import process after it has started – for example, if you selected a large number of files to import but then realised you'd selected the wrong ones – the 'Import Files' button changes into a 'Cancel' button once the process has started. Click 'Cancel' to end the process after the file that is currently being worked on has completed. Files imported up to that point will have been added to the case database, but any remaining ones will be skipped.

anonymised_182_ANPR.xlsx
anonymised_185_cellexts_with_eufi.xlsx

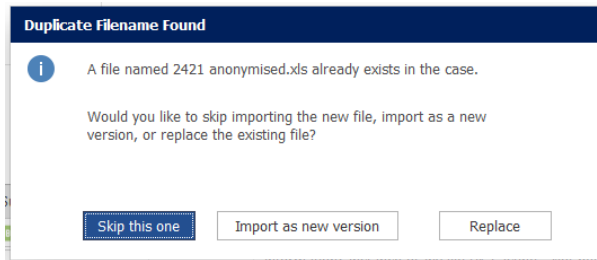
Browse to files... ☒ Auto attribute 

- Once all files have been imported, a popup may appear indicating that cell overrides are being calculated. Once the entire process has completed, the progress bar will provide an indication of the number of records that were imported and the total import time.
- Files that have imported correctly will have a green indicator bar and their contents can be viewed in Case Hub. Files that require additional attention will have a red or orange indicator and may need to be manually imported using the File Import Wizard – more information may be shown in the 'Details' column for these files, indicating what the issue might be.

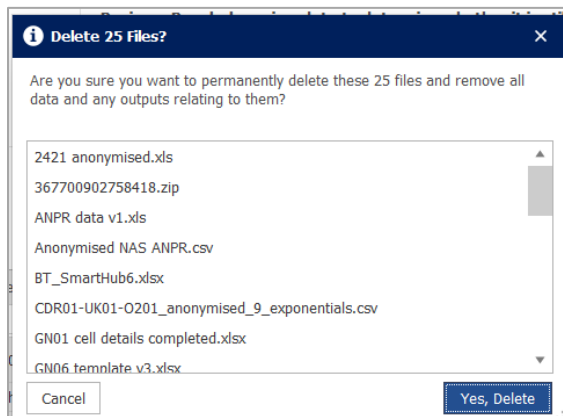
Details

Information: Instance of CDR Record not loaded - StartTime or Both PhoneA/PhoneB are not populated
Information: Invalid Cells not loaded or Blank lines encountered
Information: Instance of IMEI missing significant digits - Exponent/Truncation?
Information: Instance of Phone number missing significant digits - Exponent/Truncation?
Information: Invalid Cells not loaded or Blank lines encountered
Information: Instance of Invalid UK Easting - Not between 0 and 800000.
Information: Instance of Invalid UK Northing - Not between 0 and 1400000.
Information: Invalid Cells not loaded or Blank lines encountered
Information: Invalid Cells not loaded or Blank lines encountered
Information: Invalid Cells not loaded or Blank lines encountered

- Files may not be imported if CSAS cannot determine the associated subject identifier. For example, CSAS may not be able to determine the subject phone number for a CDR file. If this happens, the missing information can be added via the [Update File Details](#) option.
- If you attempt to import a file that already exists in the case (based on filename), CSAS will ask you what you which action to take, with options of skip the file (don't import it), import as new version (add an index number to the file name), replace (delete the existing with and replace it with the new one).



12. If you want to delete a file which has not been correctly imported, then from the 'Actions' column at the far right of the grid, click on the dropdown menu and select 'Delete file'. The 'Delete File?' pop-up window opens and confirms the file or set of files that have been selected for deletion:



13. From the 'Delete File?' pop-up window, check that the file name(s) to be deleted are correct then click on the **Yes** button.
14. Once you have successfully imported the source data files, you have several options; you can:
 - » 'Print or Export' the contents of the Import Files grid
 - » Go to the 'Attributions' screen
 - » Go to any other function within the case
 - » 'Close' the case

10.4.1 Updating File Details

Files may not be imported if CSAS cannot determine the associated subject identifier. For example, CSAS may not be able to determine the subject phone number for a CDR file. If this happens, the missing information can be added via the Update File Details option.

You can update source data file details from the 'Update file details' pop-up window:

This pop-up window can be launched:

- » From the grid by right-clicking in a row
- » By clicking in the 'Actions' drop-down menu and selecting the option

The pop-up window gives you an opportunity to add missing file details, or to correct details that have been picked up incorrectly.

You can save your updates by clicking on the **Save** button.

Typically, this would be used to add a missing 'subject number' in the event that the normal parsing process failed to detect, which in turn meant that CSAS couldn't import the file correctly. The Update File Details popup can also be used to add a 'missing' subject number for a handset download file – handset downloads (as opposed to SIM downloads) often don't include details of the phone number(s) used with a handset, meaning that those details need to be added manually.

The Update File Details popup can also be used to set or edit details of a file's disclosure status, which will then be displayed in the Case reports > Disclosure Report.

Note: The file will be automatically deleted and reimported using the updated details.

10.4.2 Continuity Details

The 'Set Continuity Details' pop-up window gives you an opportunity to add file continuity (chain of custody) data to the data exhibits in a case:

These details can show the source of the file and how and when it was received.

Multiple rows in the Import Files can be selected together if the same continuity details apply to all of those files.

Note: If the same continuity details are valid for multiple files, then you can use the checkboxes in

the 'Import Files' grid to select the appropriate rows before the pop-up window is triggered: the same continuity details will be applied to all selected files.

10.4.3 File Import Wizard

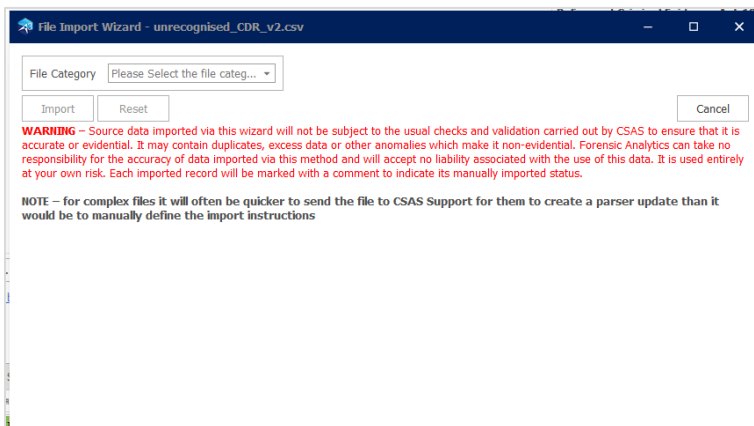
The File Import Wizard allows you to manually process source data files which fail to be

parsed automatically.

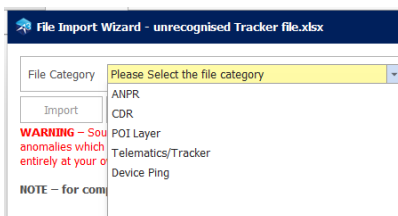
The wizard attempts to detect file type, column data types, column data formats and CSAS event types. You can manually confirm the type of file, the start row, column headers and data types and the content imported from the source data file. CSAS then tries to guess what data type and format is in each column and sets the 'column data type' and 'data format' fields as appropriate.

If a source data file fails parsing, right-click on the necessary failed file(s) and select from the drop-down menu 'File import wizard'.

Before the 'File Import Wizard' pop-up window opens, a warning window opens. You must read the warning then select the necessary 'File Category' from the drop-down menu:



Selecting a 'File Category', for example 'CDR', displays a grid and controls in the same window:

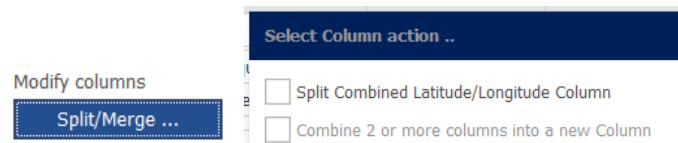


Note: Using the wizard to manually parse source data files adds a comment to each imported file stating that the record has been imported manually and has not had any processing rules applied to it, therefore CSAS cannot guarantee that the data is reliable. These files will have their event index number and event type coloured orange.

From the window, you can select from the drop-down menu and checkboxes to manually parse the file:

- » Using the 'File Category' drop-down menu: select the type of file or what you think the file type is. The file type primes the column data type options so if you select 'CDR' the column choices reflect the types of data you would expect to see in a CDR file.
- » Using the 'Subject Identifier' field, type the subject or target identifier (e.g. phone number, IMEI, VRM/license plate, etc) for the file, for example '447700900763'.

- » Using the 'Subject Identifier Type' drop-down menu, select the identifier type for example MSISDN, IMEI, IMSI etc.
- » Usually, the grid column headers will be on row '1' in the source file, however, if the file contains metadata you'll need to indicate where the column header row should be – for example, if there are 15 rows of metadata, the column headers will be on row 16. To do this, using the 'Column Headers are on row' up / down arrows, select which row you want the wizard to capture the column headers from and then click the **Pre-Process** button to reload the data into the grid from the correct start row.
- » The Modify Columns control allows you to manage the splitting and merging of columns:



- If the source file has merged latitude/longitude data in one column (e.g. 51.12345,-0.23456), the control can be used to split that combined data into separate columns.
 - If the source file contains separate columns that should be combined (e.g. several columns that contain 'comments' type descriptive or narrative data), the control can be used to combine them together into one column for import.
- » From the header rows, for each column, select the correct (or closest) column data type and data format:

	Skip	Index	CSAS Event Type	Date and Time of Call
▼	☐	=		
	☐			Start Date & Time 
	☐			dd/mm/yyyy hh:... 
	☐	1	Unknown 	2020-04-01 13:11:11

Note: The wizard is configured to expect a minimum set of columns in order for the imported data to be usable within CSAS – if the minimum set of required columns hasn't yet been defined, the wizard will display a red X in row 1 of the Index column. Hovering over the X will launch a popup that lists the remaining required, but missing, columns.

	Skip	Index	CSAS Event Type	Date and Time of Call	Calling CC
▼	☐	=			
→	☐			Not Required 	Not Required
	☐				

 Please select either Duration, End Date and End Time or End Date & Time

If the file to be imported is a CDR and if that file contains cell IDs that don't already include MCC (country code) and MNC (network code) details – for example, if the cell ID data simply lists the cell ID itself (12345) and isn't in the full CGI format (234-30-12345-12345) – then it would be helpful to manually add those details. This will enable CSAS to compile

globally unique cell references for each cell, which in turn will allow the imported data to link up with the CellView and RF Survey features:

- » In the 'MCC' text field, enter the cell's Mobile Country Code (e.g. 234 for the UK).
- » In the 'MNC' text field, enter the cell's Mobile Network Code (e.g. 30 for EE UK).

Other columns also have specific requirements, a selection of which are listed below:

- » From the 'CSAS Event Type' column, the drop-down menu in each row shows a list of acceptable event types that CSAS recognises. Select one CSAS event type that most closely matches the original event type, for example, if the original event type is 'MS Originating SMS' (what Vodafone call an outgoing SMS) then you could select 'Outgoing SMS'. As long as the Original Event Type column has been identified, the wizard looks at all the other rows in the grid that have the same original event type and sets them to the same value, however, you can manually change this by selecting a different value from the drop-down menu as necessary.
- » Using the 'Skip' checkboxes, you can select which rows in the grid you don't want to import, effectively manually setting up the parsing instructions for the file(s). Depending on your choices and to speed thing up, you can click the or buttons.

At the bottom of the window are more buttons which allow you to:

- » Import the file by clicking the button.
- » Cancel the wizard by clicking the button.
- » Reset the grid back to its starting state before you made any selections by clicking the button.

To import the selected row(s), click the button.

The data is processed into a rescue format by the wizard, which is saved using the filename 'ImportWizard_< original file name >'. This is passed to the parser for processing and the data is imported into the case.

The original, unrecognised source data file is left in the imported files grid and you may wish to delete it after the Import Wizard has successfully completed.

When the import is complete a pop-up message is displayed:



10.4.4 Importing USA Device Ping Data

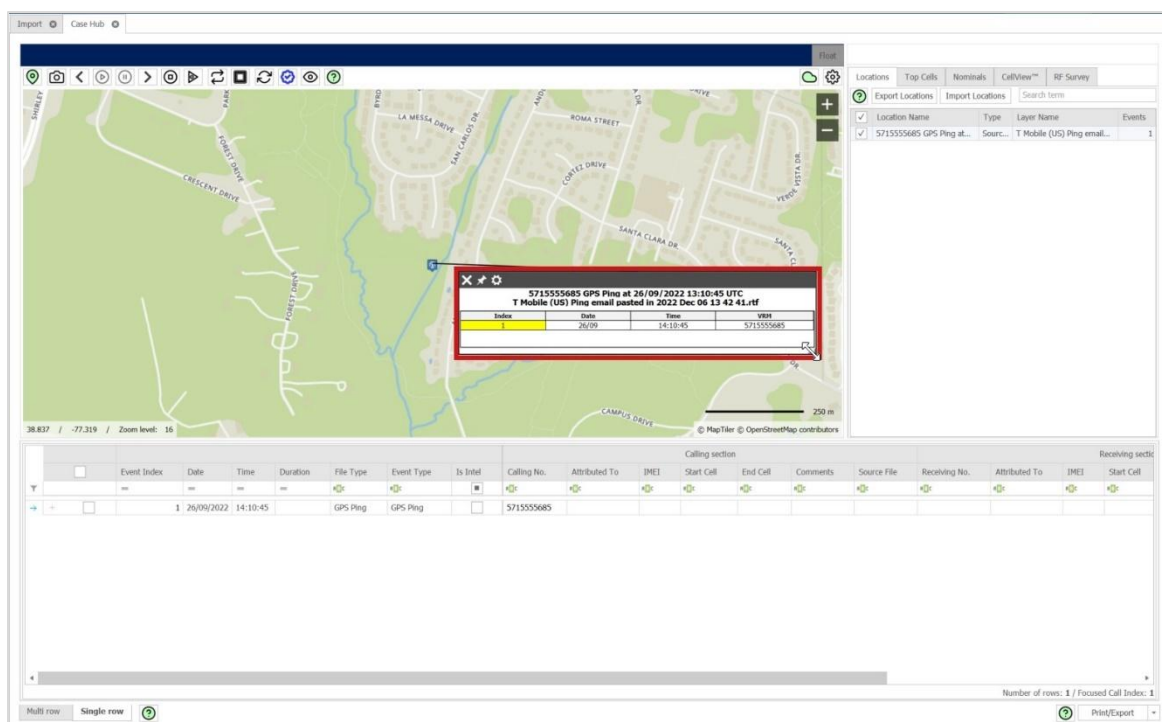
Law enforcement agencies in the US are able to request real-time device location or 'ping' data from network providers, which gives the device's current location within a tolerance.

US LEAs can request historical location details (e.g. 'where *was* this phone during this time period?'), which are usually delivered in CSV or Excel files similar to CDRs. These files can be imported in the normal way via the Import Files function.

It is also possible to request 'immediate' location pings (e.g. 'where *is* this phone now?'), responses to which are usually delivered via email, or they can request a recurring 'ping', which typically returns a response email every 10 or 15 minutes for a set period of time.

Ping email responses can be imported and parsed using the 'File import Wizard - Device Ping' window, which can be opened by a right-click drop-down menu on the Imported Files Grid on the 'Import' screen.

If you need to import a ping response email, you can import the ping data by copying / pasting the details from the email into the 'File import Wizard - Device Ping' window. When you import the ping data into CSAS, it can be displayed on a map:



The screenshot displays the CSAS interface with a map view. A location pin is placed on the map, and a pop-up window shows the following details:

Index	Date	Time	IMEI
1	26/09	14:10:45	5715555685

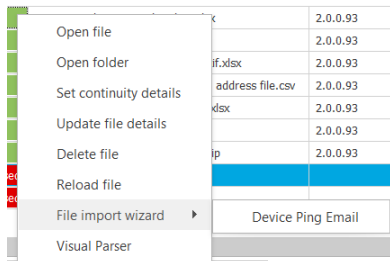
Below the map, a table lists the imported data:

Event Index	Date	Time	Duration	File Type	Event Type	Is Intel	Calling No.	Attributed To	IMEI	Start Cell	End Cell	Comments	Source File	Receiving No.	Attributed To	IMEI	Start Cell
1	26/09/2022	14:10:45		GPS Ping	GPS Ping		5715555685										

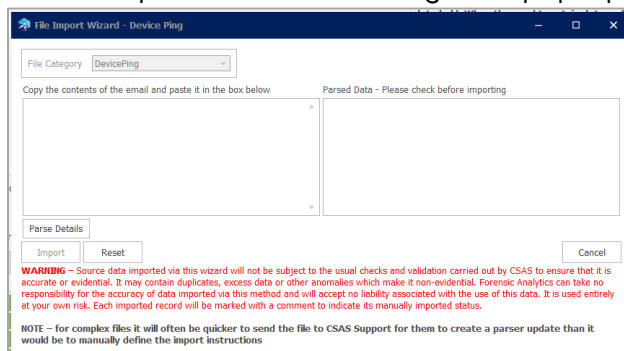
The interface also includes a sidebar with tabs for Locations, Top Cells, Nominals, CellView, and RF Survey. The bottom status bar shows 'Number of rows: 1 / Focused Call Index: 1' and 'Print/Export' options.

Stepped Procedure

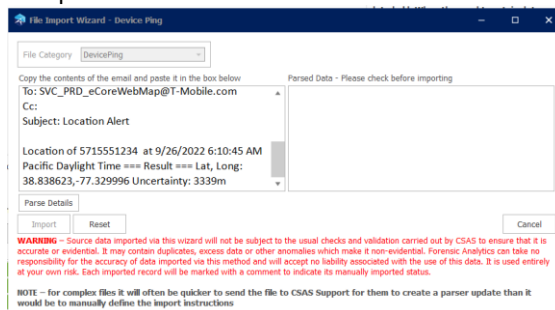
1. To import ping email content into a CSAS case: from the Import Files screen, hover over any of the parsed files, right-click and select *File import wizard* > *Device Ping* from the drop-down menu:



2. The 'File Import Wizard - GPS Ping Data' pop-up window opens:



3. From this pop-up window you can copy / paste the content from the email into the first pane:

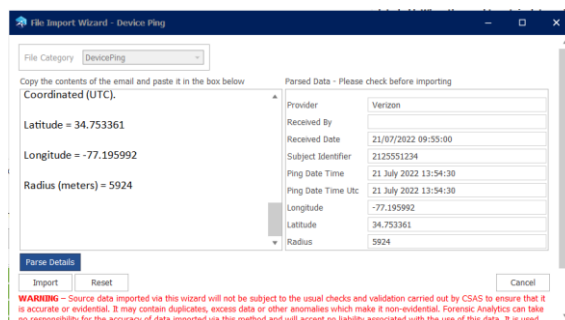


Open the email

highlight all text and copy

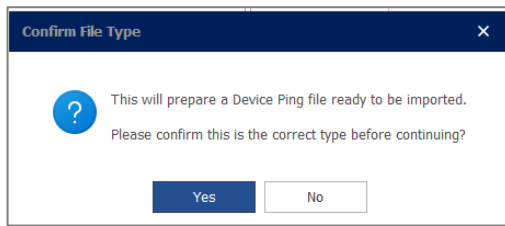
hover over the left panel in the Import Wizard, right click and paste the email content into the window

4. Click the **Parse Details** button. If the email format is recognised, the 'Parsed Data' pane populates:



5. Check that the details in the pane match those in the source email: Provider, Received By, Received Date, Subject Identifier, Ping Date Time, Ping Date Time UTC, Longitude, Latitude and Radius.

6. If the parsed details are correct, click the **Import** button to import the data into the CSAS case. A confirmation popup opens:



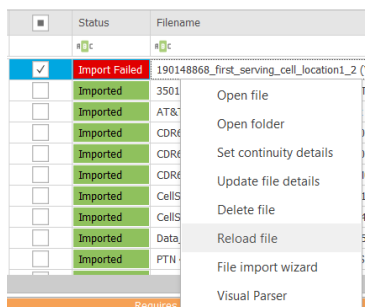
7. Confirm by clicking the **Yes** button.
8. If the data is imported correctly, a further confirmation popup opens. Click 'OK' to dismiss it
9. The imported ping data will now be listed in the Import Files grid and will be available to be viewed in case Hub.

Troubleshooting

For information on common troubleshooting issues refer to *Troubleshooting*.

10.4.5 Reloading Failed Files

CSAS sometimes fails to import data from specific files or file types; often, these issues are fixed in a later version, so after an application update it is possible to retry the import of failed files.



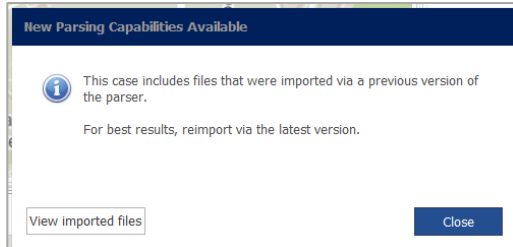
After a CSAS update, a failed file can be reimported by right-clicking on the file in the Import Files grid and selecting 'Reload File'.

The existing version will be deleted from the case and represented for import.

This process doesn't only have to be used for failed files; any imported file can be reloaded at any time.

10.4.6 Post-update file warnings

Updates of the CSAS application often include improvements to parsing rules and processes, which can sometimes amend the set of events extracted from source data files to provide a more accurate representation of the source data.



When you open an existing case after an update has been applied, CSAS will warn you if the case contains files for which the parsing rules have changed – clicking on the 'View Imported files' button in the information popup opens the Import Files screen.

Affected files are highlighted in the Import Files grid – the 'Parser Version' column shows the older version that was used to import the file and is highlighted in red – and you'll be offered the opportunity to delete and reimport the affected files using the updated parsing rules.

Status	Filename	Parser Version	Subject Identifier
Imported	ReportNelos_2284852 (AT04 DevLoc).bt	1.9.1.77	14845488273
Imported	T_Mobile_Tower_List_GSM_2019-06_Philadelp...	1.9.1.77	
Imported	email-5671055-2019-030500-6639572 (SP06 D...	1.9.1.77	14845542301

Improvements for Format CDR71-UK54-0210

No specific improvements for this structure

The Visual Parser offers the opportunity to examine the parsing rules applied to imported files. Please note that any Analytics reports or call schedules that were previously output using the affected files may need to be reviewed and, if necessary, re-exported after applying the parsing update.

If you hover over a list entry that has the parser update warning showing (parser version highlighted in red) a popup label appears and provides details of any changes that have been made to the parsing of that specific format.

10.4.7 Parsing Updates

New data formats and changes to existing data formats are released by providers from time to time. Parsing patch files, known as CSFS files, containing details of simple format recognition changes are used to update the instructions CSAS uses for recognising and processing source file formats.

In normal circumstances, CSFS patch files are distributed automatically – each instance of CSAS, that has access to the Internet, checks for updates each time the user logs in. For automated updates to work, your network must allow access to <https://csasupdates.forensicanalyticscloud.com>.

In exceptional circumstances, CSAS Support may send CSFS update files to individual users – if you are sent a CSFS file you need to save it to the following location to be imported into CSAS:

C:\Users\< username >\AppData\Roaming\Forensic Analytics Ltd\CSAS v3

10.5 Visual Parser

CSAS is designed to be both an intelligence tool and an evidential tool, meaning that the output of CSAS should be able to be used in court. Users must therefore have confidence that the output of CSAS is accurate and also be able to prove the continuity of the evidence provided.

To enable CSAS to be regarded as being an evidential tool it includes a function that provides details of the decisions made by CSAS when processing and transforming source data files. This feature is known as the Visual Parser.

The Visual Parser processes individual source data files and provides details of the CSAS 'parsing rules' that were followed when processing that file.

10.5.1 How to view the visual parser

The Visual Parser is launched for a file from the Import Files screen – highlight the required file and right-click and select 'Visual Parser' from the dropdown menu.

The Visual Parser will open and will automatically process the selected file, which will be processed using the same rules base as would be used to process the file in the main CSAS application.

The Visual Parser screen is divided into two main areas:

- » Left side – Source Data grid – shows the original raw data from the selected file, organised into tabs, if the source file had tabs
- » Right side - Processed Data grid – shows the processed data and associated information in a series of tabs, including:
 - Results – an overview of the stats for the processed file
 - Rule Summary – provides a list of the rules employed to process the file
 - Comms Meta Data – provides an overview of the file metadata
 - Processed data – a set of file type-specific tabs that display the processed/parsed data from the file for Calls, Cells, IMEIs, IMSIs

10.5.2 General Operation

Once a source file has been processed, the raw data will appear in the left-side window. The processed data and related information will appear in the tabs in the right-side window.

To view the corresponding processed data for a given source data row, double-click on the required source row (in the left side window) and it and the corresponding processed row in the right-side window will be shown side by side in the top row of each window, as shown in the diagram.



Idx	Column2	Column3	Column4	Column5	Column6
12	14/08/2021	11:30:27	Voice Calls Originating	447700900621	447700900621
13	14/08/2021	11:38:40	Voice Calls Terminating	447700900344	447700900621
14	14/08/2021	11:41:19	Voice Calls Terminating	447700900374	447700900621
15	14/08/2021	11:41:25	Calls Forwarded	447700900374	447700900621
16	14/08/2021	11:41:37	Calls Forwarded	447700900374	447700900621

Source Line	Status	Call Type	Start Time	End Time	Start Time UTC	End Time UTC
12	Valid	OutgoingVoice	14/08/2021 11:30:27	14/08/2021 11:38:40	14/08/2021 10:30:27	14/08/2021 10:38:40
13	Valid	IncomingVoice	14/08/2021 11:38:40	14/08/2021 11:41:19	14/08/2021 10:38:40	14/08/2021 10:41:19
14	Valid	IncomingVoice	14/08/2021 11:41:19	14/08/2021 11:41:25	14/08/2021 10:41:19	14/08/2021 10:41:25
15	DeletedAPP	OutgoingFor...	14/08/2021 11:41:25	14/08/2021 11:41:37	14/08/2021 10:41:25	14/08/2021 10:41:37

If a source row was processed using a parsing rule, the details of the rule (and other related information about the record) are shown in a dropdown menu in the processed data grid – if additional data is available, a '+' symbol will appear in column 1 of the

processed data grid, click on the plus symbol to launch the child menu.

+	14	Valid	IncomingDiver	14/08/2021 11:...	14/08/2021 11:...	14/08/2021 10:...	14/08/20
-	15	DeletedAtPP	OutgoingFor...	14/08/2021 11:...	14/08/2021 11:...	14/08/2021 10:...	14/08/20
Phones Rule Results							
	Code	Other Record ID	Rule Description	Detail			
→	02-2b		Save Merged Incoming Record as Cell Divert				

The child menu will show the rule employed for the record in the Rule Results tab. If any phone numbers were parsed from the record, they will be summarised in the Phones tab and if any cell locations were found in the record, they will appear in the Cells tab.

10.5.3 Colour Coding

The Visual Parser uses colours to indicate the operation performed on each row of data, with the same set of colours used in the Source Data and Processed Data grids.

- » Red – removed without using any of the data
- » Dark Green – processed and used with no changes (no parsing rules applied)
- » Light Green – processed with some changes (at least one parsing rule applied), including being merged with another record
- » Yellow – merged with another record and removed
- » Orange – rule applied/calculation made but then removed at a later stage

+	DeletedAtPP	Unknown	24/01/2017 18:25:00	24/01/2017 18:25:00	24/01/2017 18:25:0
+	Valid	OutgoingSMS	25/01/2017 16:43:20	25/01/2017 16:43:20	25/01/2017 16:43:2
-	Delete	Unknown	25/01/2017 16:43:20	25/01/2017 16:43:20	25/01/2017 16:43:2
-	Delete	Unknown	25/01/2017 16:43:20	25/01/2017 16:43:20	25/01/2017 16:43:2
	Valid	NetworkIn	25/01/2017 16:43:23	25/01/2017 16:43:23	25/01/2017 16:43:2

Some rows may also have one or more fields coloured light green, this indicates that the contents of that field have been calculated or extrapolated from other information in the record. For example, if a call record contains a 'start time' and a 'duration', CSAS will calculate the 'end time' by adding those values together – the resulting 'end time' files will be coloured light green to indicate that it is a calculated value.

Processed data rows are also given a 'status' to further indicate the processes that were performed on them:

- » Valid – means the data in the row was used
 - Valid + green infill means 'used with no changes'
 - Valid + light green means 'used with some changes or merging'
- » Delete – means the row was not used – deletion can take place at different stages of the process
 - Delete + red infill – deleted immediately, no data captured
 - Delete + light green – deleted after merging some data with another row
 - DeleteAtParsing – usually means that an empty row or separator row has been removed
 - DeleteAtPP – means the row was removed during 'post processing' after comparing it to other rows – e.g. it was a duplicate row

10.5.4 Common Processed Information Tabs

Visual Parser layouts for all source file types include a common set of information tabs:

Results	Rule Summary	Comms Meta Data
---------	--------------	-----------------

Results – this lists the source file details (file name, CSAS format ID, type of file, detected time zone); it provides a statistics table showing the count of various types of information found in the file (calls, cells, IMEIs, IMSIs, etc); and also lists any file processing warnings.

Results

Rule Summary

Comms Meta Data

Calls

Cells

IMEIs

IMSIs

PhoneNumbers

Result

Loaded

Structure

CDR01-UK01-0201

Message

Type of Data

CDRBilling

File Time Zone

GMT Standard Time

Counts (Double click on Row to Navigate to records)

Record	Total	Deleted	Valid
Calls	1609	79	1530
Cells	131	0	131
IMEIs	1	0	1
IMSIs	1	0	1
PhoneNumbers	96	0	96

Trace / File Warnings

(6)Instance of Phone Number being non numeric
(320)Instance of Cell not loaded -
LAC/SAC/TAC/CI are all blank

Rule Summary – lists the full set of rules that were applied to the source file, with a count of the number of times that each rule was used.

Results	Rule Summary	Comms Meta Data	Calls	Cells	IMEIs	IMSIs	PhoneNumbers	
Rule	Count	Description						
GEN1	1	Period From Date derived from Start Time						
GEN2	1	Period To Date derived from End Time						
GEN4	1	Requested Phone derived from Most frequent occurring ...						
O2-1b	58	Merge Preceding Outgoing(CF) Duration/EndTime						
O2-1c	58	Save Merged Outgoing Record						
O2-2a	21	Merge Preceding Incoming(CF) Duration/EndTime						
O2-2b	21	Save Merged Incoming Record as Cell Divert						
O2-3a	503	Swap Cell Details for Incoming Call						
O2-3c	32	Changed incoming to Cell Divert						
				Source Line	Status	Cell Type	Start Time	
				+	7	DeletedAtPP	OutgoingForw...	14/08/2021 11:...
				+	32	DeletedAtPP	OutgoingForw...	14/08/2021 13:...
				+	39	DeletedAtPP	OutgoingForw...	14/08/2021 13:...
				+	54	DeletedAtPP	OutgoingForw...	14/08/2021 15:...
				+	70	DeletedAtPP	OutgoingForw...	14/08/2021 18:...
				+	72	DeletedAtPP	OutgoingForw...	14/08/2021 18:...
				+	91	DeletedAtPP	OutgoingForw...	14/08/2021 21:...
				+	104	DeletedAtPP	OutgoingForw...	15/08/2021 12:...
				+	153	DeletedAtPP	OutgoingForw...	15/08/2021 21:...
				+	174	DeletedAtPP	OutgoingForw...	16/08/2021 13:...
				+	191	DeletedAtPP	OutgoingForw...	16/08/2021 15:...

Clicking on a rule summary row launches a list of the records for which that rule was used, plus a summary of the processed data captured for each row by the rule.

Comms Meta Data – this tab provides a summary of the source file meta data, including the file type and direction, the date period and the target/subject identifier.

Results	Rule Summary	Comms Meta Data	Calls	Cells
Field	Value			
Direction	Unknown			
TargetType	TargetPhone			
Period From	14/08/2021 10:08:20			
Period To	11/09/2021 16:35:11			
Target Phone	447700900621			
Period Derived	True			
Target Derived	True			

The date coverage period can either be 'derived' – which means that it was calculated by searching for the first and last events in the file – or not derived – which means that the date range was explicitly indicated in the file metadata.

Similarly, if the file's 'target' or 'subject' identifier is not explicitly indicated in the metadata, it will be derived by processing the first few records and determining the target identifier for file from those records, which would be classed as a 'derived' target.

10.5.5 File-type Specific Tabs

Each specific file type will have Processed Data tabs that are applicable to the data found in those files. The table below summarises the addition tab types that are available and the file types they relate to, there then follows a brief explanation of each tab type.

File Type	CDR	Cell addresses	Handset download	ANPR/ALPR telematics, GPS tracker	Locations & events	Social media takeout	Router/IP logs	Encrochat
Calls	X							X
Cells	X	X						X
IMEIs	X		X					X
IMSIIs	X		X					X
Phone number	X							X
Events			X	X	X			X
MACs			X					
Contacts			X					X
Cameras				X				
Vehicles				X				
General locations						X		
Extraction details							X	
Device details			X					
User IDs			X				X	
Network Readings			X				X	
Groups			X				X	
Device Locations			X					X

- » Calls – lists the processed call records found in a source file which will be displayed in a time-ordered list within Case Hub
- » Cells – lists the individual cell locations found in the source file
- » IMEIs – lists the individual IMEIs found in the source file
- » Device details – for a handset download file, will show associated details such as IMEI or IMSIs – lists the individual IMSIs found in the source data
- » Phone Numbers – provides a list of the unique phone numbers found in the source data
- » Events – offers a time-ordered list of the events found in the source data,

- combined from all source tabs, which will be displayed within Case Hub
- » MACs – a list of the individual MAC addresses found in the source file
 - » Contacts – lists all contact names found in the source whether in a specific phone book or in line with the event data, which can be made available to CSAS attribution search
 - » Cameras – lists the unique ANPR/ALPR camera locations found in the source file. For telematics and tracker files, this tab lists the individual reported device locations.
 - » Vehicles – lists the individual vehicle identifiers (number/licence plates) found in an ANPR/ALPR file
 - » General Locations – list the individual device locations (based on lat/long) found in a takeout file
 - » Extraction Details – provides details of when the source data was downloaded from a broadband router
 - » Device Details – provides details about the host router for a router download file
 - » User IDs – lists all identifiers, beyond phone numbers, found in SMS, chat and other content in the source file
 - » Network Readings – lists WIFI hotspots and Bluetooth beacons listed as having been connected to or detected in a handset download file, along with the date/time associated with those records
 - » Groups – lists any 'group messaging' groups defined within the messaging data in a handset download
 - » Device Location – lists any locations (usually based on lat/long) found within the source data, which can be displayed on CSAS maps

There is no option to save or export information from the Visual Parser.

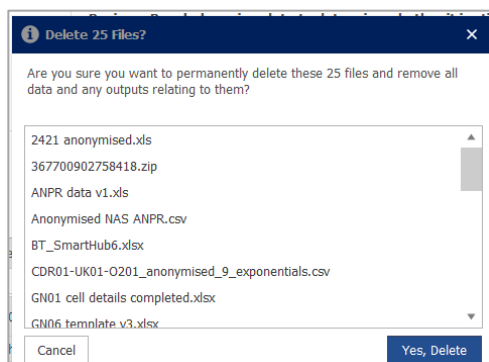
10.6 Deleting Files

You can delete source data files from a case using the 'Import Files' screen.

Note: The deletion of a case file cannot be reversed and the data cannot be recovered. When a file is deleted, all records from it are removed from the CSAS case database and will no longer appear in any grids, charts maps or reports created within the case. However, if a file is deleted accidentally, it can simply be reimported back into the case again.

Stepped Procedure

1. If you want to delete a file which is listed in the 'File Import' window at the top of the screen, and it has not yet been processed, then select the file and click the **Remove selected** button.
2. If you want to delete a file after it has been processed and it is shown in the 'Import Files' grid, then select the file(s) to be deleted by ticking the checkbox for the row in the Import Files grid, then from the 'Actions' column at the far right of the grid, click on the drop-down menu and select 'Delete file'.
3. The 'Delete X Files?' pop-up window opens:



4. From the 'Delete File?' pop-up window, check that the file name(s) to be deleted are correct and then click on the **Yes** button.

10.7 Settings Sidebar

The 'Import Files' screen includes a sidebar on the right-hand side of the screen, which is used to host different filters, options and settings.

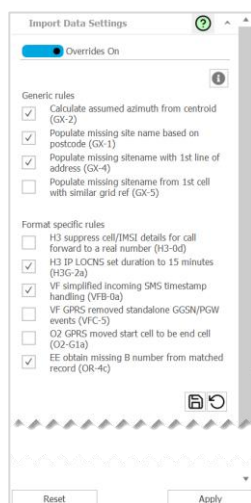
10.7.1 Opening the Settings Sidebar

The Import Files sidebar has a  'settings' icon at the top in the right-side frame. If the sidebar is open and you want to close it, just click on the 'close' icon:



The sidebar moves to the right and closes.

10.7.2 Changing Parsing Rules



The CSAS parser uses a set of rules that govern how each type of file and how each type of record within each file gets processed.

There are some circumstances in which some of these rules can be viewed as optional and CSAS provides an opportunity to enable or disable certain rules as required. You can see the list of rules in the Settings sidebar, which is split into 'Generic rules' and 'Format specific rules'.

Each of the rules is described below:

Rule Type	Rule	What Does it Do	Description
Generic UK	GX-2	Allows a missing azimuth to be calculated from the centroid for Eastings and Northings values (Vodafone UK Only).	This rule is ENABLED by default. Vodafone UK records are used to provide a centroid and no azimuth. In these cases, CSAS calculates an 'assumed azimuth' by measuring the bearing between the site Ordnance Survey Grid Reference (OSGR), the Cell Site Easting & Northing coordinates and the OSGR, and the Centroid Easting & Northing coordinates. Disabling this rule stops the calculation and leaves the azimuth field blank.
Generic UK	GX-1	Allows missing site names to be populated by using the non-blank site names from another site that shares the same non-blank postcode.	This rule is ENABLED by default. By default, CSAS populates the missing site names in records if a suitable site name has been found in other records within the same case, but only if the record has a postcode - it does this based on postcode and works on the assumption that only one cell site per Telecommunications Operator (TO) will be found within the same full postcode. For example: If a record has no site name but does

Rule Type	Rule	What Does it Do	Description
			have a postcode (for example, 'SW1A 1AA'), CSAS checks if any other records in the case data for the same operator have the same postcode; if they do CSAS inserts the site name from that record into the missing record.
Generic UK	GX-4	Populates the missing site name from the 1st line of the address.	This rule is ENABLED by default. Cells having a blank or invalid site name will use the first line of address if provided (dependant cells etc.) - Three / Vodafone / EE. If the imported file extension is .CSV and the address line contains a comma separated address, the first 20 characters of the address are used.
Generic	GX-5	Populates the missing site name from the 1st cell with a similar grid reference.	This rule is DISABLED by default. Uses the non-blank site name from another site that shares the same grid reference to populate the blank site name.
Generic UK	GX-6	For EE (UK) only - converts unmatched non-subject records into 'implicit' subject events	The rule is DISABLED by default. EE usually has matched subject and non-subject records for each event (e.g. matched inbound and outbound records for the same connection). Occasionally, the subject record is lost, meaning that the event is only described by a non-subject record. When enabled, this rule creates an 'implicit' subject for that event. When disabled, only an intel record is created.
Format specific	H3 UK	Suppresses cell / IMSI details for call forward to a real number (H3-0d) (for UK - Three / H3 formats (H301, H302).	This rule is DISABLED by default. Enabling this rule captures details of a non-subject phone and Case Hub, Analytics and Case Outputs will include those details in the grids and statistics. H3 records related to call forwarding events sometimes show details (IMEI, IMSI) of the 'forwarded to' phone rather than the file's subject phone (if the forwarded to phone is also an H3 phone). These details are ignored by default, but this rule commands CSAS to keep those details in the output record.

Rule Type	Rule	What Does it Do	Description
Format specific	H3 UK IP LOCNS	Sets duration to 15 minutes (H3G-2a).	This rule is ENABLED by default. Disabling this rule sets durations to zero. H3 IP Location records list the Cell IDs seen to be connected to within 15-minute observation periods. The records list the start time of the 15-minute period in which the Cell ID was seen, but provide no information as to when within that 15- minute period the cell was actually connected to or for how long; therefore, no true Duration is known however opinions vary as to whether this should be listed as having no duration (00:00:00), or a duration of 15 minute (00:15:00) to represent the observation window time period. This is further explained as follows: The H3 IP Locations output is displayed the data in 15-minute blocks with the “Start Time” listed being the start time of that 15-minute time period. The data displays Cells seen in network traffic used for data services within that 15-minute period. Therefore, a record with a Start Time of 10:00 would show cells used at some point between 10:00 and 10:15 but with no greater granularity as to when within the 15-minute period. Listing the duration as 00:15:00 is incorrect as it gives the false impression that the connection through that cell ran from 10:00 to 10:15. Similarly, however listing the duration as 00:00 appears to indicate an exact time (i.e., the connection to the cell took place at 10:00). Since we need to put some kind of value in the Duration field, this rule gives the user the choice as to whether they display the duration as 00:00:00 or 00:15:00.
Format specific	VF UK	VF simplifies the incoming SMS timestamp handling (VFB-0a).	This rule is ENABLED by default. The delivery timestamp for incoming SMS events is shown in column HY (Timestamp SMS Delivered) in the source data. Historically this timestamp was presented in UTC (Universal time or GMT) but is occasionally presented in BST. CSAS adds an hour to the column HY timestamp to bring it into line with BST when required. Disabling this rule commands CSAS to assume BST is used for column HY timestamp, stopping CSAS from adding an extra hour to SMS delivery timestamps, and may cause the wrong time to be shown if the source data was actually presented in UTC rather than BST.

Rule Type	Rule	What Does it Do	Description
	VF UK	VF GPRS 'sub-session' records (VFC-0a)	This rule is DISABLED by default. When enabled, this rule detects PGW 'sub-session' records in VF data session CDRs and uses the Start Time for the event. When disabled, CSAS instead captures the Change Time for the record, which offers a more realistic view of when the subject device used the associated cell ID.
	VF UK	VF GPRS 5G SA records (VFC-0b)	This rule is ENABLED by default. When enabled, this rule detects 'from 5G Core' records in VF data session CDRs and uses the Change Time for the event, which offers a more realistic view of when the subject device used the associated cell ID.. When disabled, CSAS instead captures the Open Time for the record.
Format specific	VF GPRS	VF GPRS removes all PGW / GGSN events whether they can be matched with SGW / SGSN events or not (for Vodafone UK Only) and may result in details of some data sessions that are only described in PGW / GGSN events being captured.	This rule is DISABLED by default. Enabling this rule can be useful if you believe the device is roaming abroad, as in this case only GGSN / PGW events would be generated by Vodafone. SGW / SGSN - Serving GPRS support node (2g / 3g PS core network node). PGW / GGSN - Gateway GPRS support node.
Format specific	O2 GPRS	O2 GPRS moves start cell to be end cell (O2-G1a) (O2 only).	This rule is DISABLED by default. O2 MDE records will list the cell used at or before the time the record was closed (the End time). This is different to all other networks who generally list the cell used at or before the Start Time of the record; however, up until late 2020, O2 listed the Cell misleadingly in the Start Cell field. This rule corrects this mistake by moving the Cells listed on the MDE records from the Start Cell fields to the End Cell fields.
Format specific	EE	EE gets the missing B number from a matched record (OR-4c) (EE only).	This rule is ENABLED by default. On occasions, Incoming EE Records (the Mobile Terminating Call (MTC)) can be provided within a BLANK calling number. When enabled, this rule attempts to identify a paired Mobile Originating Call (MOC) record for the same call and then extracts the calling number from the MOC record and uses it as the calling number for the MTC record.

- » Clicking the  button launches a pop-up window that provides more details about each rule
- » Clicking the  button sets the current state of the variable rules as the default for all cases
- » Clicking the  button restores all variable rules to their default state.

Who, When, Why

	This function is necessary to select different filters, options and settings, control overrides and parsing rules.
	This function is undertaken at any time you are importing files to a case.
	This function is typically carried out by the following users: » CSAS User

10.7.3 Parsing Date/Time Overrides

These options allow users to override the case/default time zone for a set of imported files and also allow the date/time format to be specifically set for those files.

Generally, the timestamps used for events in a case are synchronised to a particular time zone, that way the events displayed in Case Hub can be shown in relation to each other – for example, Suspect A in London (UTC +0) and sends a text message to Suspect B in Hong Kong (UTC +8). Suspect A's CDR shows a timestamp for sending the text at 12:00:00 UTC, but Suspect B's CDR shows their phone receiving the SMS 10 seconds later at 20:00:10 UTC +8. In most cases, it would be more useful to adjust Suspect B's timestamps to show their actions in UTC to match Suspect A's data. Applying an offset of -8 hours to Suspect B's data would allow those events to be shown in relation to each other.

The Parsing Date/Time Override control is in the right sidebar in the Import Files screen.

Parsing Date/Time Overrides

☐ Override Timezone for new files

☐ Override Short Date Format for new files

If a file or set of files to be imported into a case relate to a different timezone from the other files in the case, the timezone can be overridden (e.g. the events can be shown in the equivalent time in the case timezone) for those files – tick the 'Override timezone for new files' checkbox and select the required timezone for this files, then import them.

For example:

- Your case is set to your default timezone of EST (US Eastern, UTC -5).
- The majority of your case files are also in EST.
- One of your case files is in Pacific timezone (UTC -8).
- Import the Pacific timezone file separately from the others – import the EST files first using the default timezone.
- Then set the Date/Time override to Pacific (UTC -8) and import the Pacific timezone file.

- The events from the Pacific timezone file will be shown in the equivalent EST times and will be shown in the correct relationship to the events from the other files.

Don't forget to uncheck the option to return to the case default timezone after the specific files have been imported.

Much the same can be achieved for the format in which event date/timestamps are displayed – if you find that the date format is being displayed in Case Hub incorrectly for a file, delete it from the case, then set the 'Override short date format...' option, import the files and reset the option back to its default value again.

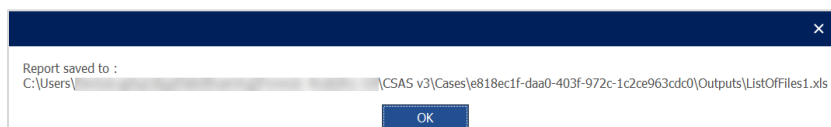
10.8 Exporting / Printing

Clicking on the Print or Export button a drop-down menu is displayed with the following options:

- » Export All
- » Export Selected
- » Print All
- » Print Selected.

Export All

This option exports the entire contents of the Import Files grid and auto generates an Excel report which is saved to the case folder. The following message pop-up window is displayed:



Clicking on the OK button closes the window and opens the report.

Export Selected

This option exports only selected rows from the Import Files grid and auto generates an Excel report which is saved to the case folder. You can select individual source data files via the checkboxes. The report opens in the same manner as for 'Export All'.

Print All

This option prints all entries in the Import Files grid. The following pop-up window is displayed:

Selection	Status	Filename	Subject Identifier	File Type	Details	Actions
☐	Imported	90743 CDR.csv	07700000127	CDR		...
☐	Imported	4791324.csv	07700000127	CDR		...
☐	Imported	4791418.csv	07700000127	CDR		...
☐	Imported	4791417.csv	07700000127	CDR		...
☐	Imported	4791322.csv	07700000127	CDR		...
☐	Imported	4791422.csv	07700000127	CDR		...
☐	Imported	Call Address Data - GMSI.xls	07700000127	Call data		...
☐	Imported	4791323.csv	07700000127	CDR		...

Clicking on 'File', 'View' and 'Background' gives you various options for page setup, tool bar, status bar, colour and watermark options. You can edit the print file by choosing buttons from the tool bar at the top of the pop-up window.

To print click on the  button.

Print Selected

This option prints selected rows from the Import Files grid. You can select individual source data files via the checkboxes. The report opens in the same manner as for 'Print All'.

11 Using Attributions

This function allows you to assign colours to significant subject (or 'target') identifiers, such as phone numbers, registration/licence plate numbers, IMEIs, IMSIs, MAC addresses and other identifiers and to also add attribution 'nominals' (the names of the alleged users of each significant phone or other identifier) which can be displayed in Case Hub or in Analytics reports and can also be included in output call schedules.

Once a Case has been created or at any time during the working life of a Case, you may want to add, edit or delete the attributions for significant identifiers.

This function can also be used to 'colour' or 're-colour' significant identifiers during the lifetime of a Case if required.

The set of significant identifiers defined for a Case – both 'real' subject identifiers with data files imported and 'person of interest' identifiers that have been in contact with a case subject - will be listed in the 'Attribution' tab.

Each significant identifier can have the following attribution details defined:

- » Identifier Attributed To – this is the attributed name (e.g. John Smith) or another label (e.g. Dirty Phone) associated with the identifier. This field can be left blank, although the 'auto-attribution' feature will add a generic nominal (such as 'Unknown 1') if a real name isn't specified
- » Text Colour/Background (fill) Colour and Recent Colours – allows you to select the colours to be used to highlight the identifier in grids, charts and tables within CSAS (see below for a more detailed explanation). The 'Recent Colours' dropdown allows you to choose a colour combination that you've selected before.
- » Attribution validity period – shows the date and time period during which the current attribution will be applied to the selected identifier – this allows the same identifier (e.g. a phone number) to be attributed to different individuals over time. CSAS doesn't currently support overlapping attribution validity periods.
- » Details of any source data files that have been loaded for the target identifier will be listed in the 'Imported Subject Files' box and identifiers that have attributions linked to handset download files will be highlighted.

Subject identifiers detected during source data file import will be added to the identifier list automatically, colouration and attribution details can then be added if required.

11.1 Layout

The 'Attribution' feature has a main screen that lists the selected set of case identifiers and shows the nominals, colours and validity periods assigned to them. There is also a Details popup that contains the controls that allow names, colours and validity periods to be set.

There are also a number of function buttons along the top and bottom of the Attributions window that perform various tasks.

Identifier Type	Identifier	Attributed Nominal	Attribution Start	Attribution End	Actions
MSISDN	07700900122	Unknown 6			
MSISDN	07700900177	Unknown 5			
MSISDN	07700900212	Unknown 7			
MSISDN	07700900597	Unknown 3			
MSISDN	07700900621	Unknown 13			
MSISDN	07700900818	Unknown 2			
MSISDN	07700901111	Unknown 1			
MSISDN	07700902222	Unknown 4			
MSISDN	07700903852	Unknown 9			
MSISDN	07700905617	Unknown 14			
IMSI	234267700907675	Unknown 11			
IMEI	35201770090268	Unknown 8			
MSISDN	447700902421	Unknown 10			
VRM	BS79PTA	Unknown 12			

Attribution functions are available by clicking on the button from the navigation sidebar or by selecting 'Attributions' in the navigation dropdown menu.

11.2 Attribution Functions

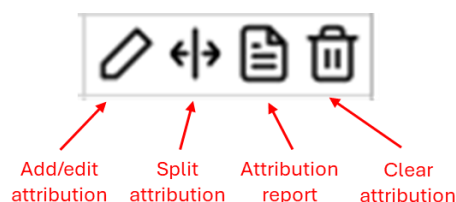
The 'Attribution' screen allows you to:

- » See a Data Grid of source data file identifiers and their attributions, so new ones can be set as required.

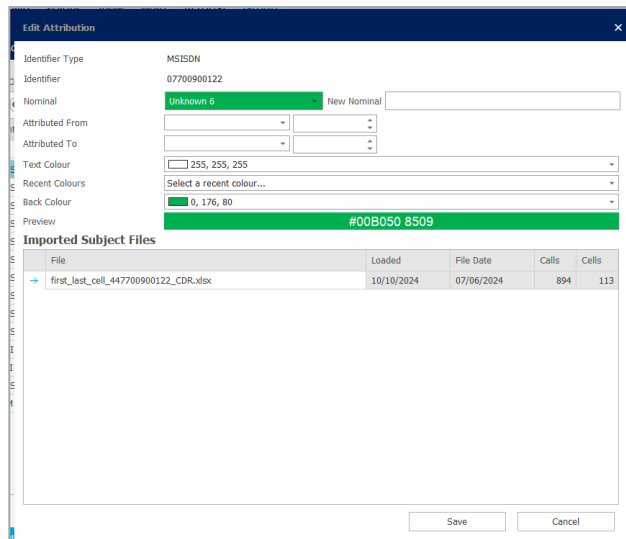
Identifier Type	Identifier	Attributed Nomi...	Attribution Start	Attribution End	Actions
MSISDN	07700900122	Unknown 6			
MSISDN	07700900177	Unknown 5			
MSISDN	07700900212	Unknown 7			

- » The functions that allow attributions to be manually added, edited, viewed and deleted are available icons on the right-hand side of each row of the Attribution grid.

The features are:



- » Clicking on the 'add/edit' button or simply double-clicking on a row in the grid opens the Edit Attribution popup, which supports a number of features:



» Select an existing nominal name from the drop-down list in the Attribution Details popup or enter a new nominal against an existing record.

» Optionally, if an identifier is linked to a nominal for only a specific date period, an attribution validity period can be set for the selected identifier using the 'Attributed From'/'To' dates and times boxes.

Clicking the **Save** button in the Edit Attributions popup saves your selected Attribution colours.

Other actions that can be performed in the Attributions screen are managed via the function buttons and include:

- » New – allows users to manually add a new Attribution. If the identifier isn't found in current case data, the attribution is saved to the Manage Nominals list and will be applied to an identifier later if data related to it is imported into the case. See *New Identifier*.
- » Import Attributions - for information, see *Importing Attributions*.
- » Automatically select attribution colours for any unattributed identifiers shown in the data grid by clicking on the **Auto attribute** button - for information, see *Auto Attribution*.
- » Edit Style – allows the colours for an identifier to be quickly edited without having to launch the full Edit Attribution popup. See *Edit Style*.
- » Auto-attribute and decode SMS platform identifiers. See *Decode SMS*.
- » Print or Export the contents of the Attributions grid.
- » Clear selected attributions' - for information, see *Clearing Attributions*.

Stepped Procedure

To manually add a simple attribution:

1. From the list in the Attributions grid, select the identifier you want to attribute. If the identifier isn't visible, for example because it is a non-subject identifier, you may have to use the filter toggles at the top of the grid to get the identifier in view.
2. Double-click on the required row or click the edit (pencil) icon at the right-hand end of that row, this opens the Edit Attributions popup.
3. If you want to assign the identifier to an existing attribution (e.g. to a name you've

already used in the case), then from the 'Nominal' drop-down menu, select the required nominal.

4. If you want to add a new nominal name, then enter it into the 'New Nominal' text box.
5. If you want to set a validity period for the new attribution, type or select the 'from' and 'to' dates for the attribution.
6. If you selected an existing nominal, the same colour scheme as was previously chosen for that nominal will be reused for the newly attributed identifier. If you want to select a different colour scheme for this nominal, select the required Text and Back colours from the drop-down menus or select from the Recent Colours list. The selected colour combination will be confirmed below the colour menus.
7. Check all details are correct.
8. To save the new attribution and close the Edit Attribution, click the button.
9. If you do not wish to save and apply the changes, click the Cancel button.

11.3 Splitting Attributions

This function allows you to add different attributions to an identifier over time. This would be used, for example, if a mobile device was passed from one suspect in a case to another. In that scenario, you would be able to apply one attribution to the first suspect for the period they were alleged to have been in control of that device and then change to a different attribution for the later period:

+	☐	202	16/08/2017	20:10:25	Outgoing Voice	07700902421	Dessi Khan	07700903632	
+	☐	203	16/08/2017	20:10:51	Outgoing Voice	07700902421	Dessi Khan	07700903632	
+	☐	204	17/08/2017	09:38:14	Outgoing Voice	07700902421	Jim Smith	07700903632	
+	☐	205	17/08/2017	10:03:25	Outgoing Voice	07700902421	Jim Smith	07700905186	
+	☐	206	17/08/2017	10:44:50	Incoming Text	0E888F838D87A83D8E23		07700902421	Jim Smith
+	☐	207	17/08/2017	12:06:12	Incoming Voice	07700905186		07700902421	Jim Smith

CSAS defaults to having just one attribution per identifier, but a split attribution can be added at any time.

If an identifier already has an attribution with a validity period assigned to it and a new split attribution is going to be added that covers some of the existing validity period, the existing attribution's validity period must be adjusted first before the new split attribution can be added – CSAS does not allow overlapping attributions.

If there are gaps in the overall attribution validity periods for an identifier – for example, if Attribution 1 covers January (with a blue fill colour) and Attribution 2 covers March (with a green fill colour), events associated with that identifier in January will have a blue attribution colour and those in March will have a green attribution colour, but any events in February will have no attribution colour – cells sites used by that identifier during that period will be shown on maps as white dots.

Stepped Procedure

Note: In this example, identifier '447700902421' has previously been attributed to 'Dessi Khan' with no validity period:

		Identifier Type	Identifier	Attributed Nominal	Attribution Start	Attribution End	Actions
	No...	=			=	=	
☐		MSISDN	07700903852	Unknown 2			
☐		IMSI	234267700907675	Unknown 4			
☐		IMEI	35201770090268	Unknown 1			
☒		MSISDN	447700902421	Dessi Khan			
☐		VRM	BS79PTA	Unknown 5			

- Before adding the additional attribution, you'll need to adjust the existing attribution for the identifier to add the validity period that relates to the original nominal. Highlight the row for the 2421 phone and click on the icon to open the Edit Attribution menu.

In this example, a validity period of '12/08-16/08' has been added:

Edit Attribution

Identifier Type

MSISDN

Identifier

447700902421

Nominal

Dessi Khan

Attributed From

12/03/2024 17:45:52

Attributed To

16/03/2024 23:59:59

The validity period is then visible in the main grid.

		Identifier Type	Identifier	Attributed Nominal	Attribution Start	Attribution End	Actions
	No...	=			=	=	
☐		MSISDN	07700903852	Unknown 2			
☐		IMSI	234267700907675	Unknown 4			
☐		IMEI	35201770090268	Unknown 1			
☒		MSISDN	447700902421	Dessi Khan	12/03/2024	16/03/2024	
☐		VRM	BS79PTA	Unknown 5			

- In the Attributions Grid, select the required identifier then click on the icon to add an additional attribution via the Edit Attribution menu.

Identifier Type

No...

Identifier

No...

Attributed Nominal

No...

Attribution Start

No...

Attribution End

No...

IMSI

234267700903645

Unknown 3

IMSI

234267700907675

Unknown 4

☒

MSISDN

447700902421

Dessi Khan

☐

MSISDN

447700903852

Unknown 2

Clear selected attribution

Add additional attribution

- The details panel activates and the 'new nominal' text box is highlighted to indicate that an additional nominal needs to be added – if an existing case nominal is to be used, it can be selected from the drop-down menu.
- In the Attributions Details panel, tick the 'valid for specific dates' checkbox, then using the drop-down menus, add the validity period for the additional attribution. This period cannot overlap with any existing validity periods for other nominals. If there are any gaps between the end of one validity period and the start of the next, and if there are any case events during that overlap, then those events will not have an attribution shown for them in CSAS. Ensure where possible that there are no gaps between validity periods, for example if period ends at midnight and the new validity period starts immediately, make sure that the end time for the first period is '23:59:59' and the start time of the next period is '00:00:00' on the next day.

© Forensic Analytics Ltd 2026

FA-487 v1.0

103

- In the Attributions Details panel, if necessary, select attribution colour(s) for the new attribution:

- To save the new attribution, click the **Save** button. The split attributions will be shown in the Attributions grid:

	MSISDN	447700902421	Jim Smith	17/03/2024	21/03/2024
	MSISDN	447700902421	Dessi Khan	12/03/2024	16/03/2024

- The change of attribution is clearly shown in screens like 'Case Hub', where the same identifier will be linked to different attributions at different points in time:

16/03/2024	20:10:25	447700902421	Dessi Khan
16/03/2024	20:10:51	447700902421	Dessi Khan
17/03/2024	09:38:14	447700902421	Jim Smith
17/03/2024	10:03:25	447700902421	Jim Smith

11.4 Grid and Controls

There are various filters and options which control what information is displayed in the Attributions Grid columns:

11.4.1 Generic Grid Controls

The Attributions grid shares a common set of filtering and layout controls with the other grids in CSAS. For details of how to apply filters, customise the column layout and other grid control options, see *Grid Filtering and Controls*.

11.4.2 Attribution Data Grid

The Attribution Data Grid consists of various columns:

	Identifier Type	Identifier	Attributed Nom...	Attribution St...	Attribution Enc	Actions
	MSISDN	447700902421	Jim Smith	17/03/2024	21/03/2024	
	VRM	8579PTA	Unknown 5			
	IMSI	234267700907675	Unknown 4			
	MSISDN	447700902421	Dessi Khan	12/03/2024	16/03/2024	
	MSISDN	07700903852	Unknown 2			
	IMEI	35201770090268	Unknown 1			
	MSISDN	07700907514				
	MSISDN	07700905186				
	MSISDN	07700908231				
	MSISDN	07700904306				
	MSISDN	07700905100				

Identifier Type Column

This column in the grid shows an icon that indicates the type of Identifier in each row:

» MSISDN

» IMEI

» VRM

» MAC Address

» IP Address

» IMSI

Identifier Column

This column in the grid displays the identifier for each row.

Attributed Nominal Column

This column displays the name of the individual to whom the identifier has been attributed.

Attribution Start Column

This column displays the start date and time of the 'validity period' during which the nominal was attributed to that specific Identifier. If a specific validity period hasn't been set, meaning that the nominal is linked to the identifier for the entire case period, then this field and the next will be blank.

Attribution End Column

This column displays the end date and time of the 'validity period' the nominal was attributed to that specific Identifier.

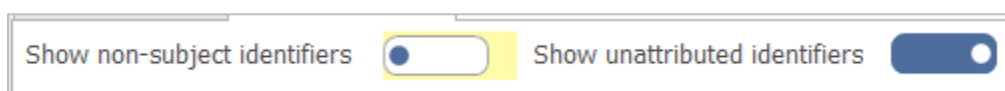
Actions Column

Includes buttons to launch the Edit Attributions popup, the Spilt attributions function, the Attribution Report, the Add Attribution and the Delete/Clear Attribution functions.

Grid Filter Toggles

The Attribution Grid can display details of all identifiers found in imported case data, whether they are /subject identifiers (that have imported source files linked to them) or are 'other' or non-subject identifiers (such as phone numbers that have been in Contact with a CDR file's subject phone).

The toggle switches along the top of the Attribution Grid allow you to filter the identifier list to ensure that only the required identifiers are currently in view.



The Attribution Grid checkboxes are:

Show Non-subject Identifiers (off)

With the toggle off, the grid only displays subject identifiers – those that are linked to an imported file

Show Non-Subject Identifiers (on)

With the toggle on, the grid will also include all other Identifiers found in the case files. Also known as 'non-target' identifiers, these are the identifiers that the subject identifiers have been in contact with.

Show unattributed identifiers (off)

With the toggle off, the grid will only include Identifiers which have attribution names assigned to them.

Show unattributed identifiers (on)

With the toggle on, the grid will also include Identifiers which do not have attribution

names assigned to them.

Further filtering options are provided by the 'auto-filter' bar in the top row of the grid and in the column header right-click menu.

11.4.3 Right-click Menus

There are no right-click options in the Attributions grid.

11.4.4 Edit Attributions popup

The Edit Attributions popup provides the opportunity to add/edit the Attribution name linked to an identifier and also to set/update the Attribution colours assigned to it. Each significant Identifier can have the following details defined:

- » Either select an existing nominal or enter a new nominal name – this is the attributed name (e.g. David SMITH) you associate with the Identifier. Attributed Nominal names are displayed in the 'Attributed Nominal' column in the Data Grid.
- » Attribute an Identifier with a From/To date/time validity period:
 - Attributed From – Validity periods are optional, but if set for an identifier this is the attributed date and time associated with the identifier. Date and time are shown in the 'Attribution Start' column.
 - Attributed To – this is the attributed date and time associated with the Identifier. Date and time are shown in the 'Attribution End' column.
- » Attribute an Identifier with text and background colours - Text Colour/Back Colour drop-down menus allow you to select colours to highlight the Identifier in the Data Grid.

Further information for these functions is given below:

Attributing an Identifier with an Existing or New Nominal Name

Identifier Type	MSISDN
Identifier	07700903852

The 'Identifier Type' and 'Identifier' stated at the top of the popup correspond with the selected row in the Data Grid.

You can attribute an Identifier in one of two ways:

Nominal	SMITH	⌵	⌵	New Nominal	JONES
Attributed From	Name				
Attributed To	SMITH				

- » Using the drop-down menu, you can Select an existing case Nominal name for a given Identifier or
- » Using the text field, specify a New Nominal name.

Note: You can select an existing nominal name if the identifier is going to be added to the set that have already been attributed to the same nominal – for example, if a suspect has more than one phone linked to them.

Linked Identifiers

Attribution data can be sourced from a variety of places, including handset download files – handsets generally have phonebooks that link names to phone numbers. If handset download files have been imported into a case and if those files include phonebook data, CSAS can extract that information to be used for attributions.

If an identifier with attribution data is found within an imported handset download file, CSAS will indicate this by displaying a 'linked' icon in the main Attributions grid and in the Edit Attributions popup.

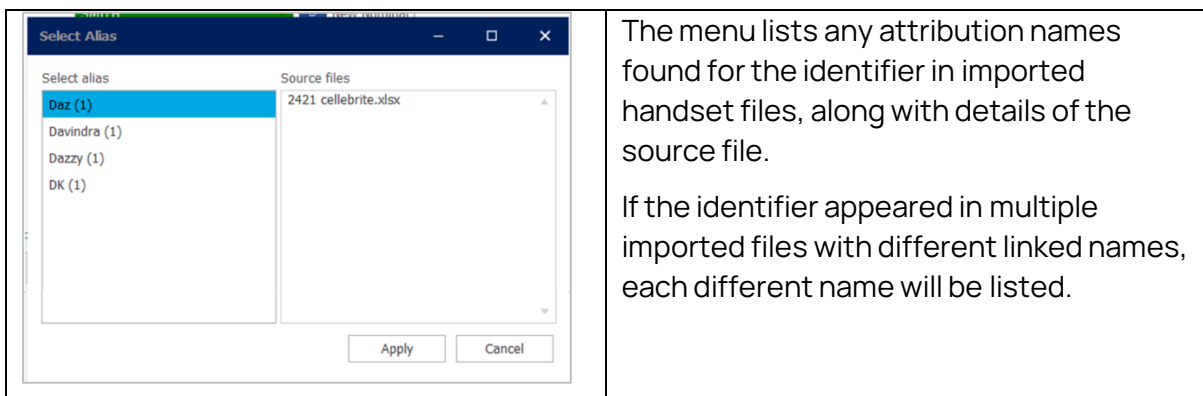


Clicking on the icon in the Edit Attributions popup launches the Select Alias function.

Select Alias

The Select Alias menu is available if the identifier is linked to any imported handset download files. The menu lists the attribution details of the identifier taken from the downloaded phone's address book.

To open the Select Alias list, click on the 'linked data' icon next to the nominal name box in Edit Attributions.



The menu lists any attribution names found for the identifier in imported handset files, along with details of the source file.

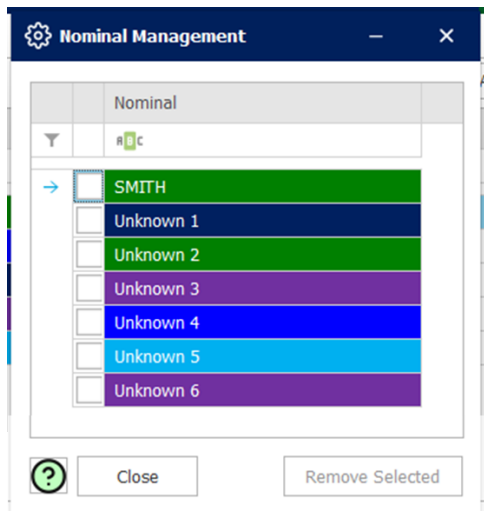
If the identifier appeared in multiple imported files with different linked names, each different name will be listed.

To use an attribution from a handset download file, select the required name and click Apply. The selected name will appear as the 'nominal' for that identifier and text/fill colours can then be added in the usual way.

To close the Select Alias menu without selecting a name, click Cancel.

Manage Nominals

The population of names/nominals added to a case over time can vary – new suspects may be added and old ones removed as a case progresses. Within CSAS, this can lead to unnecessary or unused attribution names being retained.

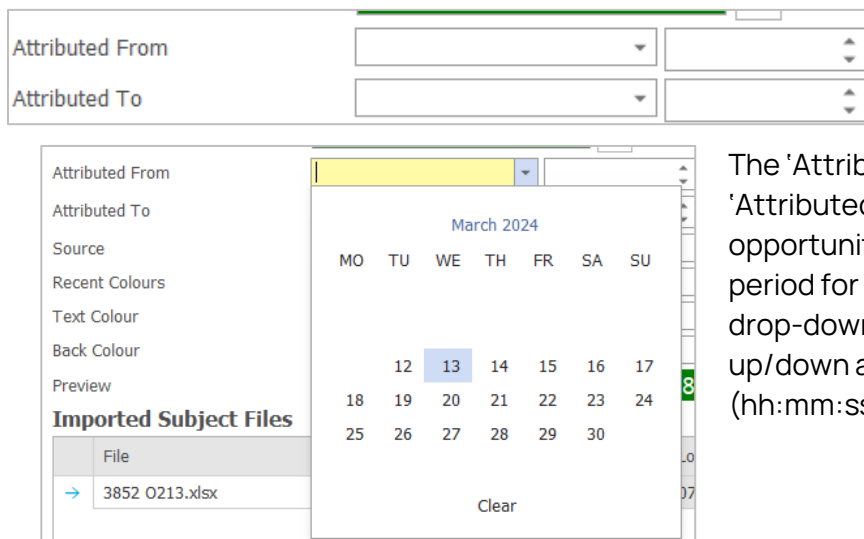


The 'Manage Nominals' button displays a list of all nominals that have been added to a case (and that are available to be selected from the 'Select Nominals' dropdown) and allows them to be deleted from the case if they are no longer required.

To remove a case nominal, select it from the list by ticking the checkbox, then click on Remove Selected.

Attributing an Identifier with a Date / Time Range

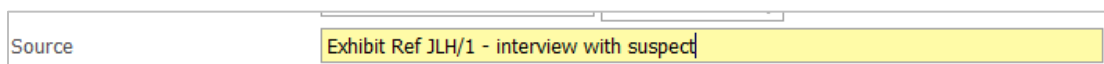
If the Attribution is only valid for a specific time period – for example, if intelligence suggests that Suspect A had use of a specific phone in January, but Suspet B had the phone in February, then 'validity dates' can be added to the attributions.



The 'Attributed From' and 'Attributed To' menus offer the opportunity to set a date/time period for the attribution using the drop-down calendars and up/down arrows for the time (hh:mm:ss).

Adding 'Source' details

The 'source' textbox offers the option of adding narrative details that indicate the source of the intelligence or evidence that supports the attribution.

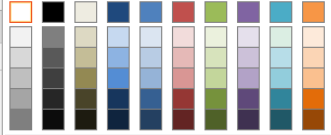


For example, the source could be an interview in which the suspect confirms their mobile phone number, or it could DMV/DVLA data that links an individual to a specific vehicle. Any text added to the Source box will be displayed in the Attribution Report for the selected identifier.

Attributing an Identifier with Colours

Recent Colours	Select a recent colour...
Text Colour	255, 255, 255
Back Colour	0, 128, 0
Preview	#008000 8509

Text Colour
Back Colour
Preview

☐ Automatic
Theme Colors

Standard Colors


Imported Subject Files

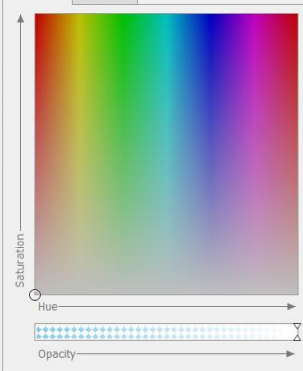
File	
→	3852 0213.xlsx

Clicking on the 'Text Colour'/'Back Colour' dropdowns opens a colour picker, which allows you to select identifying colours for each identifier or for a specific nominal from a set pallet.

Clicking on the 'more colours...' option opens a more complex selection popup.

Select Color

RGB Model
HSB Model



Red: 255
Green: 255
Blue: 255
Opacity: 255
FFFFFFFF

Sample:

This allows you to select a shade or hue from a colour chart or manually set a specific colour, by setting the RGB (red, green, blue) colour values or by entering the colour's 'hex code'.

Once the colour has been correctly defined or selected, click on OK to save the colour selection.

If you have a preferred set of colour combinations that you tend to reuse for all cases, CSAS remembers your most recent colour choices (from all cases) and presents them in a list under the Recent Colours dropdown, allowing you to quickly choose a combination to reuse.

Recent Colours	Select a recent colour...
Back Colour	
Preview	
Imported Subject Files	
File	
→	first_last_cell_44770090012

Name
#000000
#000000
#000000
#FFFFFF

The colours and names attributed to significant identifiers will be displayed in the Attributions Grid in Case Hub, in maps, in Analytics and in output Investigation and Exhibit workbooks. If validity periods have been added, only the valid name/colour combinations will be displayed in each period.

Imported Subject Files list

At the bottom of the details panel there is a grid which displays the Imported Subject

Files:

Imported Subject Files

File	Loaded	File Date	Calls	Cells
→ 4791323.csv	15/09/2021	30/04/2021	504	190
4791324.csv	15/09/2021	30/04/2021	343	180
4791322.csv	15/09/2021	30/04/2021	334	147

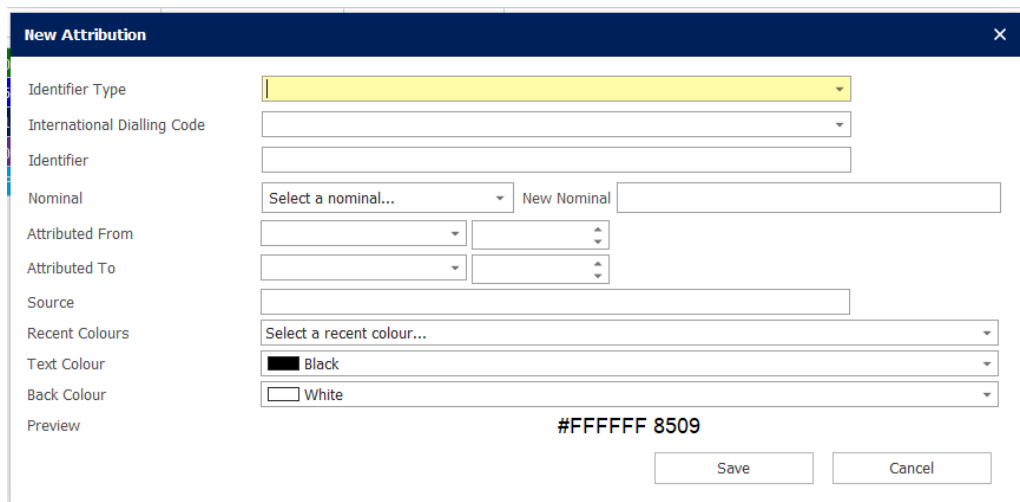
This lists the files that have been imported that relate to the selected identifier and offers a way of quickly linking an identifier to its relevant dataset.

You can save newly updated attribution values by clicking on the Save button.

11.4.5 New Identifier

The Attributions grid is populated using the subject and non-subject identifiers found in imported source files – attribution names and colours can be added to those identifiers to make them stand out in CSAS reports. Sometimes, a user may have a list of significant numbers in case, that they wish to add as attributions, but they have those numbers before they have any source data that refers to them – without the identifier appearing in an imported file, the identifier won't appear in the Attributions grid and therefore can't be attributed.

The New Identifier function is designed to help in these circumstances.



The 'New Attribution' dialog box contains the following fields and controls:

- Identifier Type:** A dropdown menu with a yellow highlight.
- International Dialling Code:** A dropdown menu.
- Identifier:** A text input field.
- Nominal:** A dropdown menu labeled 'Select a nominal...' and a 'New Nominal' text input field.
- Attributed From:** A dropdown menu and a numeric input field with up/down arrows.
- Attributed To:** A dropdown menu and a numeric input field with up/down arrows.
- Source:** A text input field.
- Recent Colours:** A dropdown menu labeled 'Select a recent colour...'.
- Text Colour:** A dropdown menu showing 'Black' with a color swatch.
- Back Colour:** A dropdown menu showing 'White' with a color swatch.
- Preview:** A label showing the hex code '#FFFFFF 8509'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

This function allows an identifier to be manually added to the case before it appears in imported data, in the expectation that when or if data including that identifier is loaded, the attribution details will be sitting there in the CSAS case waiting for it.

The New Identifier popup is largely similar to the Edit Attribution popup, with some additional steps required:

- » The user is asked to select the 'identifier type' – e.g. MSISDN, IMSI, IMSI, VRM, etc
- » If it is a phone number (MSISDN), the international dialling code is required
- » Beyond that, the fields are the same as for Edit Attributions.

The newly created identifier will be added to the Attributions grid, but won't be displayed in any grids, maps or charts within CSAS until linked source data is imported. If the 'nominal' field is left blank, CSAS will add a 'dummy' auto-attribution name.

11.4.6 Importing Attributions

Large cases may have large numbers of target identifiers and significant individuals (or 'nominals' as they're sometimes known). If CSAS is used from the start of a case, it may be that the list of attributed identifiers in the CSAS case grows organically as the case progresses, but in situations where CSAS begins to be used on a case that is already under way, it may be that there are already a large number of attributions that need to be loaded in. These are often stored and listed in an Excel spreadsheet.

Manually entering dozens or hundreds of attribution names/numbers is a time-consuming process, so CSAS supports the 'bulk' importation of these details from a spreadsheet.

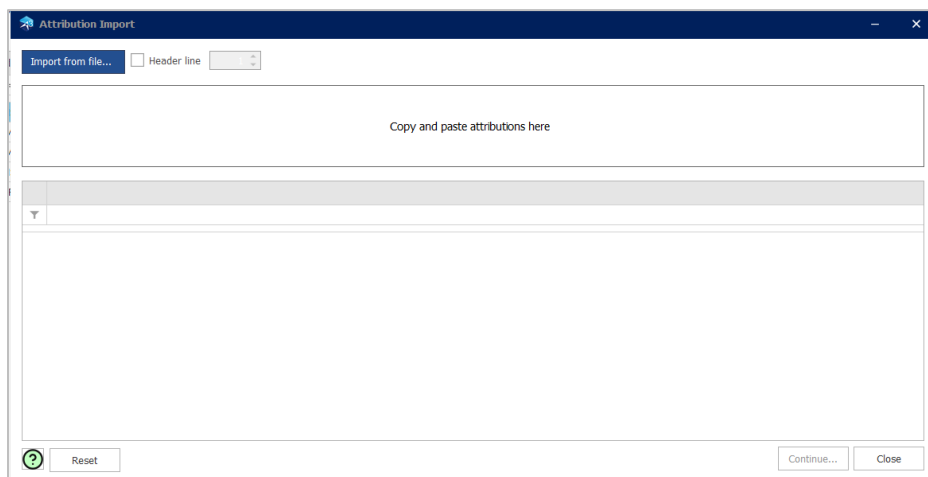
The import wizard is flexible enough to be able to import attributions from spreadsheets with a variety of column layouts. As a minimum, you need an 'Identifier' (or 'phone number') column, which has details of the identifier to be attributed, and an 'Attribution' column, which has details of the name to be assigned to the linked identifier. If additional columns containing other importable details are present, the import process will attempt to capture those too.

These include:

- » 'Valid From' – optional validity period start, showing the date/time from which the new attribution should start to be applied.
- » 'Valid to' – optional validity period end, showing the date/time the attribution should stop being applied.
- » Text colour name or Windows colour code
- » Fill colour name or Windows colour code

An example attributions template is available in the CSAS 'support' folder, which can be accessed using: Utilities > Resources > Support > GN07 Attributions import template.

If the source attributions sheet includes the required colours for each identifier, either by encoding the colour reference numbers in 'foreground' and 'background' columns or by directly colouring the identifier within the Excel cell, then CSAS will import those colours to use in the case.



The Import Attributions process can import data in two ways:

- » Clicking on the 'Import from file...' button opens a Windows file explorer popup to allow you to navigate to the required file (direct import)
- » If you have the source spreadsheet open in Excel, you can copy/paste the required columns into the Import Attributions screen (copy/paste import)

Direct import method

The direct import method requires the source file to be selected via Windows file explorer, with the data being imported via Excel. This method does not require Excel to be installed on the host machine and works with Excel alternatives such as OpenOffice.

When using the direct import method, the process currently only deals with single tab spreadsheets – if you attempt to load data from a multitab spreadsheet, it will take whatever data is in sheet 1.

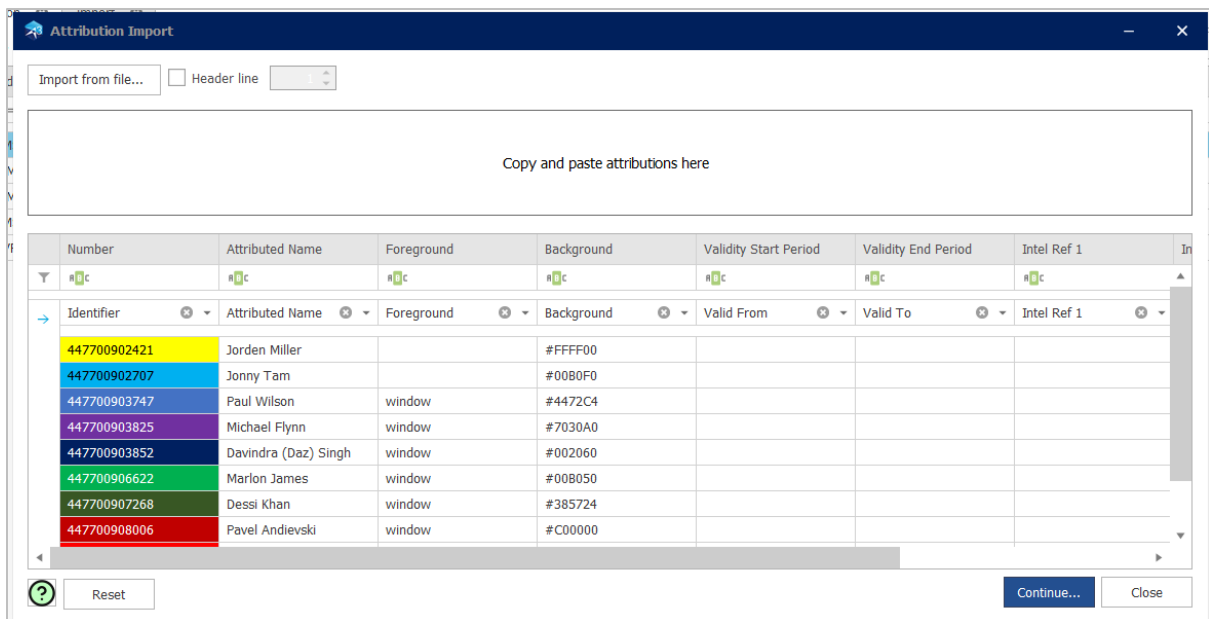
Copy/Paste Method

The copy/paste method requires Excel or an alternative such as OpenOffice to be installed on the host machine, as the spreadsheet needs to be open in order to copy the attribution data before pasting it into CSAS.

To import using this method, open the required spreadsheet, select the columns containing attribution details and copy, then click on the 'copy and paste attributions here' area in the Import Attributions popup and either hit 'ctrl+v' or right-click and select 'paste'.

Imported List

Using either method, if it is successful, the list of selected names/identifiers will be displayed in the Import Attributions popup:



The screenshot shows the 'Attribution Import' window. At the top, there is a button 'Import from file...' and a checkbox 'Header line'. Below this is a large text area labeled 'Copy and paste attributions here'. Below the text area is a table with the following columns: Number, Attributed Name, Foreground, Background, Validity Start Period, Validity End Period, Intel Ref 1, and In. The table contains several rows of data, including identifiers like 447700902421, 447700902707, 447700903747, 447700903825, 447700903852, 447700906622, 447700907268, and 447700908006. At the bottom of the window, there are buttons for 'Reset', 'Continue...', and 'Close'.

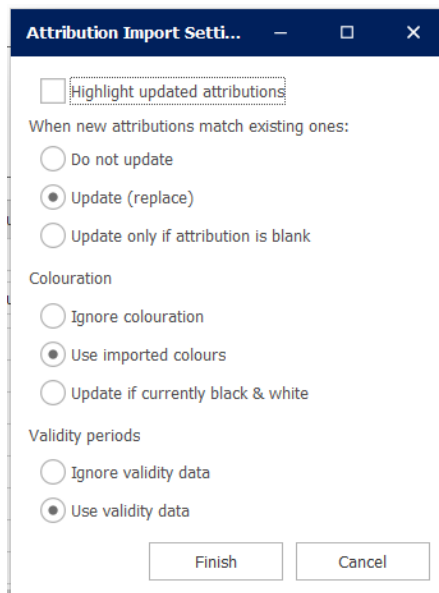
Number	Attributed Name	Foreground	Background	Validity Start Period	Validity End Period	Intel Ref 1	In
447700902421	Jorden Miller		#FFFF00				
447700902707	Jonny Tam		#0080F0				
447700903747	Paul Wilson	window	#4472C4				
447700903825	Michael Flynn	window	#7030A0				
447700903852	Davindra (Daz) Singh	window	#002060				
447700906622	Marlon James	window	#008050				
447700907268	Dessi Khan	window	#385724				
447700908006	Pavel Andievski	window	#C00000				

The header row from the source data should be shown along the top of the grid, with CSAS' best guess as to the content of each column shown in the dropdown menus on the next row.

If the source headers do not appear, it may be that they were not in row 1 in the source file. If that's the case, check the 'Header line' checkbox at the top of the form and set the spin box to show the actual header row and reimport the file.

If you are happy that the displayed list contains attributions that you wish to import, click 'Continue...' to proceed. If you wish to clear the grid and reimport the data, click 'Reset'. If you wish to abandon the import, click 'Close'.

Update Filters



The dialog box 'Attribution Import Settings' contains the following options:

- ☐ Highlight updated attributions
- When new attributions match existing ones:
 - ☐ Do not update
 - ☒ Update (replace)
 - ☐ Update only if attribution is blank
- Colouration
 - ☐ Ignore colouration
 - ☒ Use imported colours
 - ☐ Update if currently black & white
- Validity periods
 - ☐ Ignore validity data
 - ☒ Use validity data

Buttons: Finish, Cancel

If no attributions have previously been set in a case when attribution data is imported, there is no danger of the imported data contradicting any existing attributions. If attributions have already been set, either manually or during a previous Import Attributions activity, there is a possibility that the newly imported data may differ from the existing attributions. After clicking 'Continue...' the Attribution Import Settings popup appears to help to deal with this type of situation.

For reimports or updated attribution data, the options are:

- » 'Highlight updated attributions' option instructs CSAS to highlight the rows in the main Attribution grid that have been updated by this import – these will be shown with a grey infill.

☐		Identifier Type	Identifier	Attributed Nom...	Attribution Start	Attribution End	Actions
	No...	=	#BC	#BC	=	=	#BC
☒		MSISDN	07700900177	David WILLIAMS			...
☒		MSISDN	07700900597	Jorden JONES			...
☐		MSISDN	07700900621				...

- » Existing Attributions – controls what happens to updated attribution names:
 - Do not update – ignores the newly imported attribution name
 - **Update (replace)** – overwrite the existing attribution with the new one
 - Update only if attribution is blank
- » How to treat colouration – controls whether existing attribution colours are updated:
 - Ignore colouration – keep the existing attribution colours
 - **Use imported colours** – replace existing colouration
 - Update if currently black & white
- » Validity Periods – controls whether existing date ranges are updated

- Ignore validity data
- **Use validity data**

The default values are highlighted in bold, which means that the default action is to overwrite any existing attributions with the newly imported data.

CSA will post a warning message if you attempt to import more than 1000 rows of attribution data – the warning is for the possible impact on CSAS performance but can be dismissed if required.

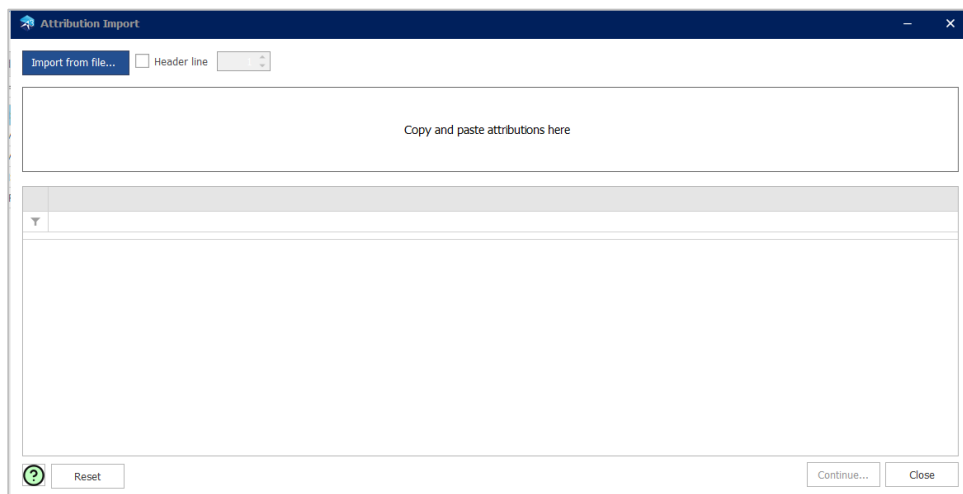
NOTE: The Import Attributions process currently only imports attributions for identifiers that appear in case data – it will ignore attributions in the imported list for identifiers that do not currently appear in the case data. The Import Attributions process may need to be rerun after each new set of files is imported into a case and, of course, the process will need to be rerun each time the case attributions list is updated, to ensure that CSAS is up to date. A future release of CSAS will include an Attribution Library function, that will store imported attributions that don't currently appear in case data and link them automatically if relevant data is imported.

Stepped Procedure – Bulk Import

1. To start the 'bulk' importation process, from the top of the Attributions Grid, click on the **Import Attributions** button:



2. This opens the Import Attributions popup:

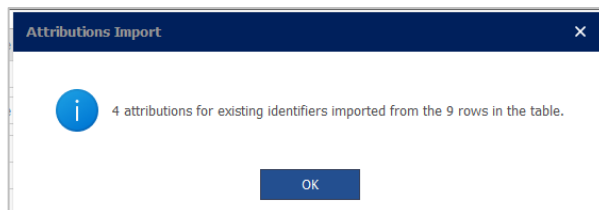


3. Clicking the 'Import from file...' button starts the direct import process – select the required Excel spreadsheet from which to import attribution data. Or open the spreadsheet that contains the required attribution data, copy it and paste it into the Import Attributions popup by right-clicking in the 'copy and paste here' zone or typing ctrl+v.
4. The grid in the popup will list the individual attributions found in the imported file and will also indicate the colour combinations and validity periods to be applied to them if those types of information were provided.

- If CSAS has not correctly identified the relevant columns, click on the column drop-down menus to indicate the 'identifier' and 'attributions' columns and any other significant columns you want to include. Columns that have data to be ignored should be set to 'unused'.

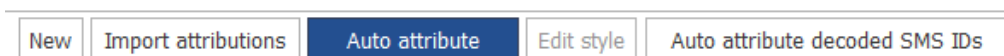
Number	Attributed Name	Background	Foreground
07700900209	Attributed Name		
07700900177	Background		#FFFFFF
07700900452	Foreground		
07700900270	Identifier		
07700900600	Not Used		
07700900201	Valid From		
07700900374	Valid To		

- Click on the 'Continue...' button to proceed
- If attribution data already exists in the case, in the filter popup, set the required 'update' options and decide whether you wish updated rows to be highlighted.
- Clicking the 'Finish' button imports the attributions into CSAS:
- When the import is complete, a popup will confirm whether the process was successful.



11.4.7 Auto Attribution

At the top of the Attributions Grid, the **Auto attribute** button mirrors the functionality of the similarly named feature on the 'Import Files' screen:



Clicking this button automatically assigns attribution colours and a dummy attribution name to each selected identifier. The colour combinations (for text and background/fill colours) are automatically selected to be contrasting – so light-coloured text will always be used with a dark colour background or vice versa.

This can be useful in cases that have a large number of identifiers when you just want to add a unique colour to them without having to go through and manually assign them.

Auto-attributed colours and nominals can be updated and overwritten later if a 'real' attribution is discovered.

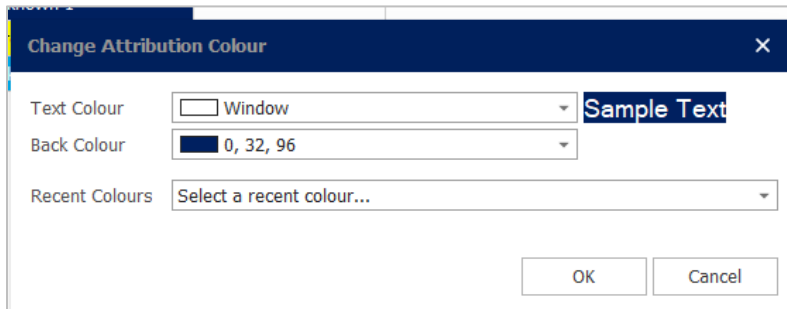
11.4.8 Edit Style

The Edit Style option provides quick access to the text/background colouration options

for an identifier. The Edit Style button only activates if a row in the Attribution grid is selected using the checkbox.



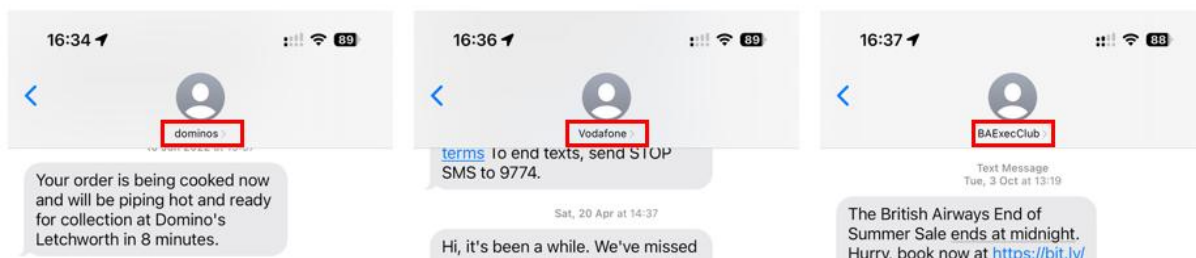
Once activated, the Edit Styles popup provides access to just the identifier colouration options – text/background colour and recent colours.



Make the required changes and click 'OK' to save them or 'Cancel' to reject them.

11.4.9 Decode SMS Platform Identifiers

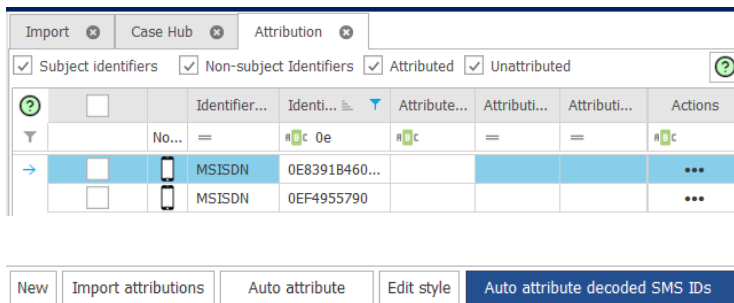
SMS text messages can be sent over a cellular network from two sources – most texts are sent from a mobile phone or device, in which case the 'from' or 'sending' party will be a mobile phone number or MSISDN. It is also possible for automated systems (or 'platforms') to send SMS messages as well – for example, if you order a pizza from Dominos you might get a text to tell you when it's ready for collection.



The 'from' party for platform-initiated messages is often an alphanumeric name (like 'dominos' or 'Vodafone') rather than a phone number. The network protocol that allows computer and web platforms to send text messages is called SMPP (Short Message Peer-to-Peer Protocol) and the sender's name is known as an SMPP Alias.

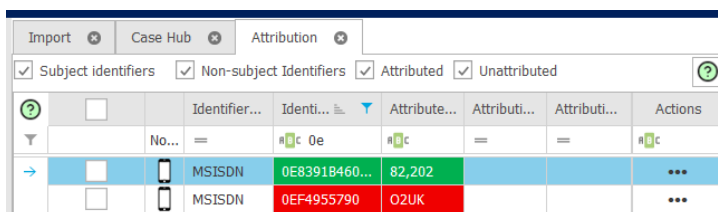
The SMPP Alias is carried through the network as a hexadecimal code but is usually decoded to show the Alias name by the receiving phone, as CDR data is captured while messages are travelling through the network, they often show the hexadecimal code rather than the Alias name. For example, administrative messages sent by the O2 network would be shown in a CDR using a sender address of 0EF4955790, but this would be decoded by the receiving phone to show a sender of 'O2UK'.

Some networks decode SMS platform addresses in their CDRs, but others show the raw hexadecimal code instead. If you import a CDR into CSAS that contains SMS platform numbers as hexadecimal codes, they can be automatically decoded to show the Alias name, which can then be used as the Attribution for that identifier.



The imported CDR file in the example contained messages from two SMS platforms, which were shown in the raw data using the hex version of the Alias.

To decode the Aliases to show them in plain text, highlight the identifiers in the grid that you wish to decode, then click on 'Auto attribute decoded SMS IDs'

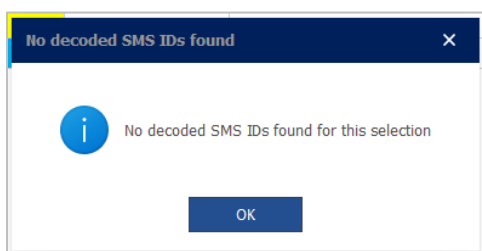


The plaintext version of the Alias will then be added as the Attribution for each selected identifier and Attribution colours could then be added as well.

Not all hex codes found in CDRs result in understandable Aliases – in the example above, one code decoded as 'O2UK', which is meaningful, but the other decoded as '82,202', which isn't. The O2 UK network has a well-known issue that corrupts the hex code shown in their CDRs, resulting in scrambled plaintext names; CSAS applies a fix to identifiers in some scenarios, which attempts to show the true Alias name rather than the scrambled version. The true hex version of the identifier, as presented in the source CDR, is displayed by CSAS without alteration in such circumstances.

Any attributions added in this can be removed (using the 'Clear selected attribution's feature) or updated at any time, just like Attributions that have been added using other methods.

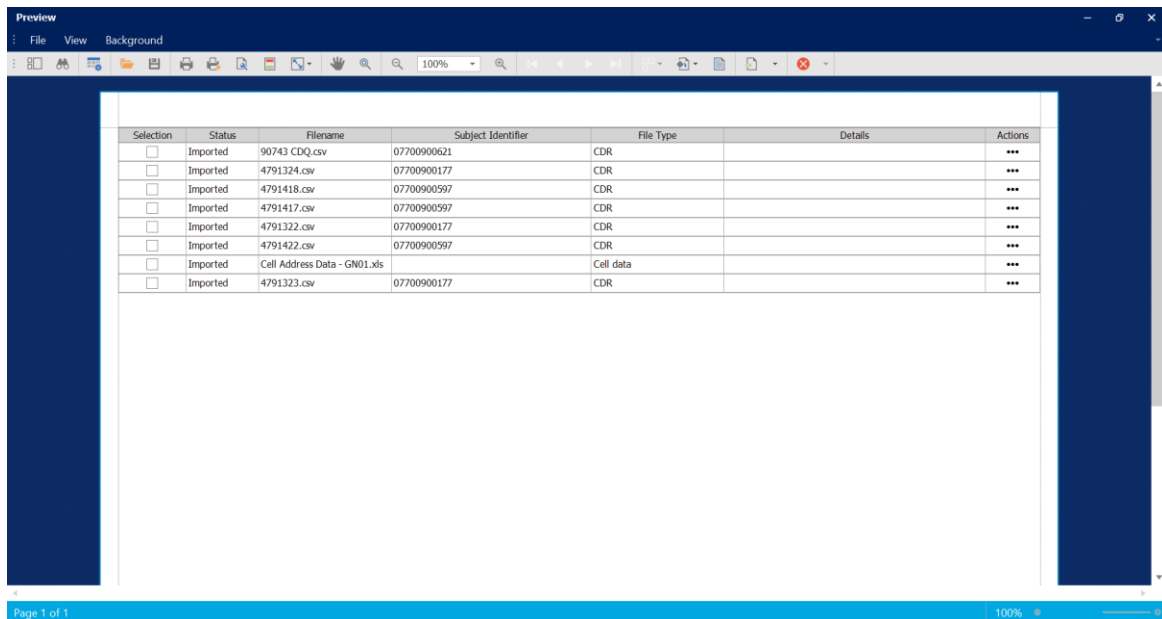
If no decodable SMS identifiers are found in the selected grid rows, the process will post a warning message:



11.4.10 Print

Clicking on the Print button outputs the current Attribution grid to the print preview screen.

If no Attribution grid rows are checked, the process outputs the entire grid, if a subset of rows are checked, the process outputs just those rows.

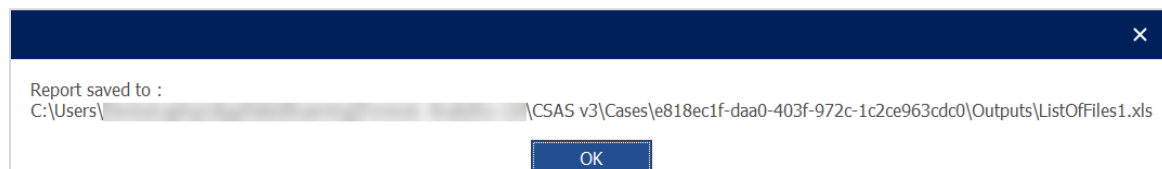


Clicking on 'File', 'View' and 'Background' gives you various options for page setup, tool bar, status bar, colour and watermark options. You can edit the print file by choosing buttons from the tool bar at the top of the pop-up window.

To print click on the  button.

11.4.11 Export

This option exports the entire contents of the Attributions grid and auto generates an Excel report which is saved to the case folder. The following message pop-up window is displayed:



Clicking on the **OK** button closes the window and opens the report.

11.4.12 Clearing Attributions

The attributions assigned to identifiers in CSAS are not permanent – they can be updated, if the evidence changes, and they can be deleted.

Deleting or clearing an attribution doesn't remove the identifier, it just removes the name and any colouration that has been applied to it.

An individual identifier's attribution data can be cleared by clicking on the 'trash' icon at the right-hand end of the grid row. Multiple attributions can be cleared by checking the checkbox for the required rows and clicking on the Clear button at the top of the grid.

11.4.13 Attribution Library

The attributions added or imported into CSAS must link to an identifier that is found in the imported case data – the data must be available in a case to have the name displayed alongside it.

In earlier releases of CSASv3 this meant that if Attribution data was attempted to be imported for identifiers that weren't found in the case, the attribution data for those identifiers was ignored and wasn't imported, which in turn meant that attribution lists sometimes had to be reimported multiple times, after additional CDRs were added to the case, to ensure that all known attributions were captured.

The Attribution Library provides a solution for that situation.

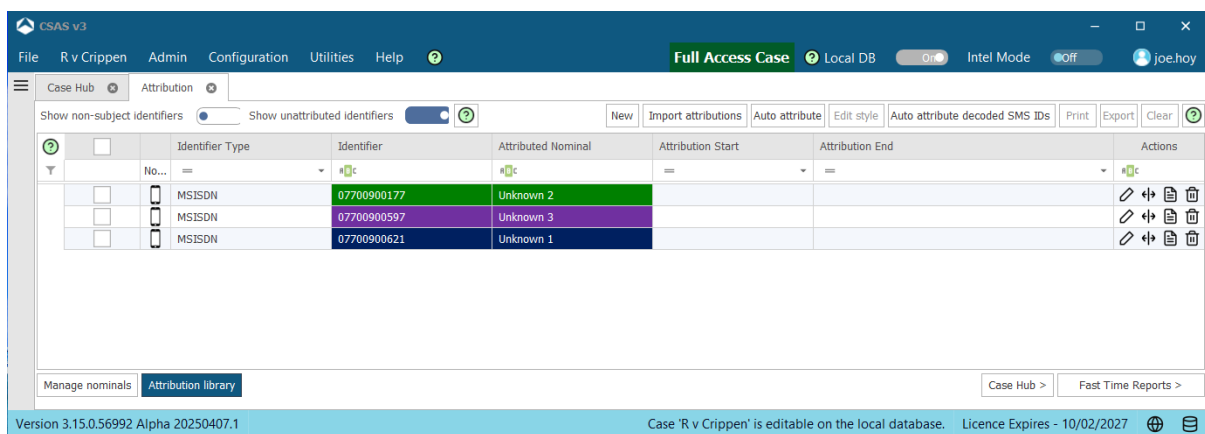
When an identifier and attribution are manually added to a case, or when a bulk import of attributions is made, details of identifiers that are found in the case data are added to the main attributions list, whilst a copy of all imported identifiers, whether they exist in the case data or not, get saved to the Attributions Library.

When additional files are imported into the case, CSAS checks to see if the 'use library' checkbox in the Import Files screen is ticked.



Browse to files... ☒ Use library ☒ Auto attribute Import files

If it is CSAS checks each new imported identifier against the saved details in the Library and moves the details into the main attributions list if a match is found – this means that attribution files only need to be imported into a case once, CSAS will use those attributions when an appropriate identifier is detected.



CSAS v3 Attribution

Full Access Case Local DB Intel Mode Off joe.hoy

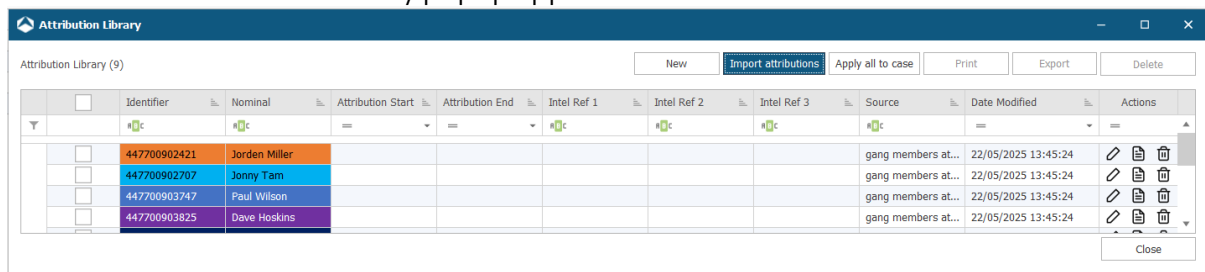
Show non-subject identifiers Show unattributed identifiers

Identifier Type	Identifier	Attributed Nominal	Attribution Start	Attribution End	Actions
MSISDN	07700900177	Unknown 2			
MSISDN	07700900597	Unknown 3			
MSISDN	07700900621	Unknown 1			

Manage nominals Attribution library

Version 3.15.0.56992 Alpha 20250407.1 Case 'R v Crippen' is editable on the local database. Licence Expires - 10/02/2027

Open the Attribution Library by clicking on the button in the bottom row of the Attribution screen. The Attribution Library popup appears.



Attribution Library (9)

New Import attributions Apply all to case Print Export Delete

Identifier	Nominal	Attribution Start	Attribution End	Intel Ref 1	Intel Ref 2	Intel Ref 3	Source	Date Modified	Actions
447700902421	Jordan Miller						gang members at...	22/05/2025 13:45:24	
447700902707	Jonny Tam						gang members at...	22/05/2025 13:45:24	
447700903747	Paul Wilson						gang members at...	22/05/2025 13:45:24	
447700903825	Dave Hoskins						gang members at...	22/05/2025 13:45:24	

Close

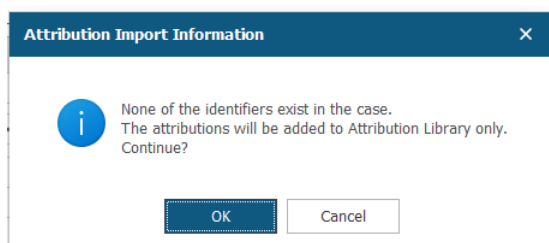
If no 'saved' attributions are loaded in the case, the popup grid is empty.

Entries in the Attribution Library grid can be edited, split and deleted using the buttons on the right-hand side of each row, in the same ways as in the main Attributions grid.

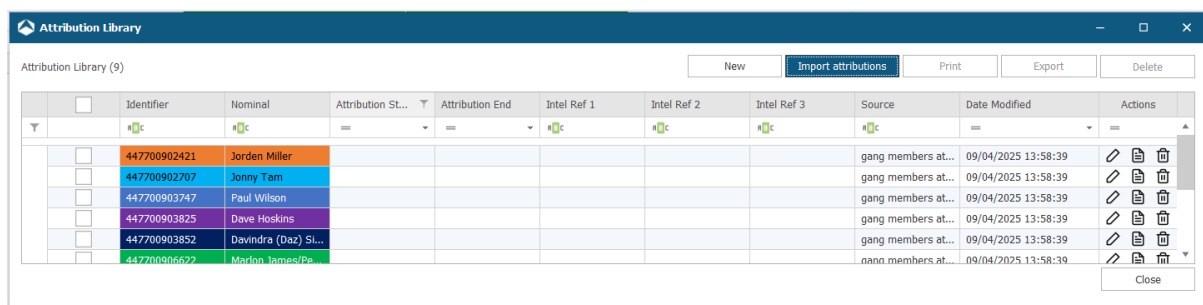
The popup has the following options:

- » **New** – manually add a new identifier to the Attributions Library, from where it can be added to the case attributions if required.
- » **Import attributions** – select an existing Excel spreadsheet containing attribution data and import or copy/paste the data into the case
- » **Apply all to case** – attribute unattributed identifiers in the case using the Attribution Library
- » **Print** – print the current Attribution Library grid or selected rows from the grid
- » **Export** – export the contents of the grid or selected rows to Excel
- » **Delete** – delete selected identifier(s) and attribution(s) from the Library

When new attributions are added or imported to a case, Attributions checks to see if any of them match existing case identifiers, if they do, the attribution is added or updated, if they don't then you will be warned:



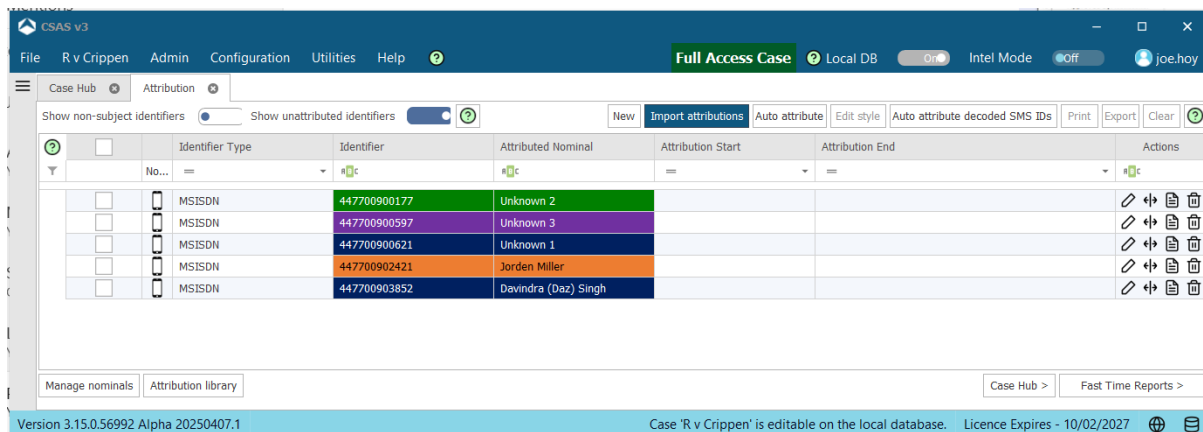
And the data will be added to the Attribution library



The "Attribution Library" window shows a table with the following data:

Identifier	Nominal	Attribution St...	Attribution End	Intel Ref 1	Intel Ref 2	Intel Ref 3	Source	Date Modified	Actions
447700902421	Jorden Miller						gang members at...	09/04/2025 13:58:39	[Edit] [Copy] [Delete]
447700902707	Jonny Tam						gang members at...	09/04/2025 13:58:39	[Edit] [Copy] [Delete]
447700903747	Paul Wilson						gang members at...	09/04/2025 13:58:39	[Edit] [Copy] [Delete]
447700903825	Dave Hoskins						gang members at...	09/04/2025 13:58:39	[Edit] [Copy] [Delete]
447700903852	Davindra (Daz) Si...						gang members at...	09/04/2025 13:58:39	[Edit] [Copy] [Delete]
447700906622	Markus James Pe...						gang members at...	09/04/2025 13:58:39	[Edit] [Copy] [Delete]

If at some later stage, a CDR or other file is loaded to the case that contains that identifier, CSAS will automatically move the details from the Library to the main Attributions list.



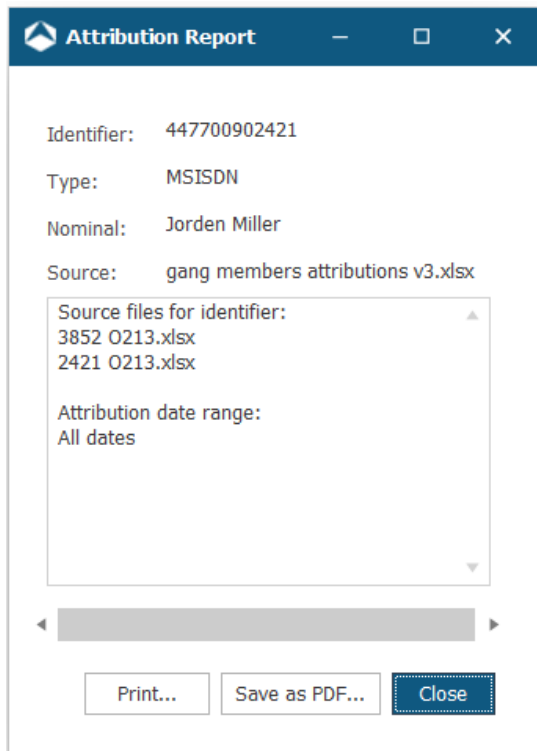
The main interface shows the "Attribution" tab with the following data in the attribution list:

Identifier Type	Identifier	Attributed Nominal	Attribution Start	Attribution End	Actions
MSISDN	447700900177	Unknown 2			[Edit] [Copy] [Delete]
MSISDN	447700900597	Unknown 3			[Edit] [Copy] [Delete]
MSISDN	447700900621	Unknown 1			[Edit] [Copy] [Delete]
MSISDN	447700902421	Jorden Miller			[Edit] [Copy] [Delete]
MSISDN	447700903852	Davindra (Daz) Singh			[Edit] [Copy] [Delete]

11.5 Attribution Report

The Attributions Report is available from the icons on the right-hand end of each row.

The report gathers together the basic information held in the CSAS case that indicates the identifier, the attribution name, the imported file(s) that are linked to the identifier and the source of any attributed names. The 'source' field is populated automatically with details of the source file the attribution was taken from (or indicates that it was added manually).



The 'Print' option opens the print preview window, from where the report can be sent to a printer.

The 'Save as PDF' option creates a PDF file of the report data, which can then be saved.

Once the report has been viewed or output, clicking 'Close' closes the popup.

Who, When, Why



This function is necessary to allow you to choose which Identifiers and attributed data is displayed in the Attribution Grid, to filter and customise the grid, add new and update existing attributions, clear attributions previously set but which are no longer needed and save your changes.



This function is undertaken anytime you need to add or make changes to attributions.



This function is typically carried out by the following users:

>> CSAS User

12 Using the Right Sidebar

CSAS utilises a consistent right sidebar that supports various tabs. Depending on which screen is open, you can select from the following sidebar tabs:

- » Filters
- » Settings
- » Export



The sidebars can be launched from the icons at the top of the right-hand side frame of the CSAS window.

Note: Not all sidebars are available in all screens.

Sidebar filters can be hidden at any time by clicking on the  button (shown when the panel is open) at the top right-hand side of the panel.

12.1 Selecting the Filters Tab

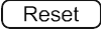
Selecting the 'Filters' tab  icon allows you to configure the way imported source data files are filtered and presented in the current screen.

The 'Filters' tab function allows you to select from the following filters:

- » Source data
- » Cell Logic
- » Date & Time
- » Locations
- » Event Types
- » Quick Filters.

These tabs allow you to select and filter the data loaded into the CSAS case tabs that are currently open. Filters can be applied at the same time as selecting the set of files to view and filters can also be applied and adjusted at any time after the data has been selected.

All filters are applied by clicking on the  button at the bottom right-hand corner of the window.

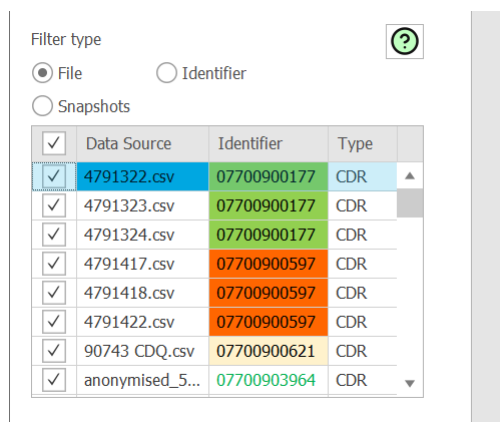
Note: From the 'Filters' window you can choose to reset the contents of the current dataset by clicking the  button. Clicking this button **clears** the grid and **resets** any filters to default values. In 'Case Hub' and 'Map Tabs', the  button also clears the current map.

12.1.1 Case-wide Filter (Off/On) Function

With 'case wide filtering' enabled, all open CSAS tabs will use the same set of selected and filtered case data – you only need to select the set of files to view and apply filters once and the same set of data will be analysed in all open tabs. This feature is useful if you want to view different aspects of the same dataset without having to re-enter the same set of filters repeatedly.

Deselecting the 'Case-wide filter' via the slider button allows you to 'decouple' individual screens/functions to show data for different identifiers or different time periods in each tab. For example, you may want to display a data set for one identifier in Case Hub and a data set for different Identifier in Analytics Call Summary. In that scenario, you would select the Case Wide Filters slider to the 'Off' position.

12.1.2 Source Data



	Data Source	Identifier	Type
☒	4791322.csv	07700900177	CDR
☒	4791323.csv	07700900177	CDR
☒	4791324.csv	07700900177	CDR
☒	4791417.csv	07700900597	CDR
☒	4791418.csv	07700900597	CDR
☒	4791422.csv	07700900597	CDR
☒	90743 CDQ.csv	07700900621	CDR
☒	anonymised_5...	07700903964	CDR

From the sidebar, in the Filters > Source data panel, using the 'Filter type' radio buttons, you can select which source data files or POI (point of interest) layers you want to display by selecting/deselecting in the checkboxes.

The 'Filter type' is selectable between 'File', attributed 'Identifier' and 'Case snapshot':

- » In 'File' mode you can select specific source data files.
- » In 'Identifier' mode, source files are aggregated based on the linked target/subject identifiers – selecting an identifier loads the data from all imported files linked to that identifier.
- » In 'Case snapshot' mode you can reload a previously saved case snapshot, there is also the option of saving a new 'snapshot' based on the data currently visible in the Case Hub grid.

The 'Source data' files list is edited based on the prefiltering selections that might have been made when the case was created, so the list of source files presented includes only those that match the current case prefiltering options.

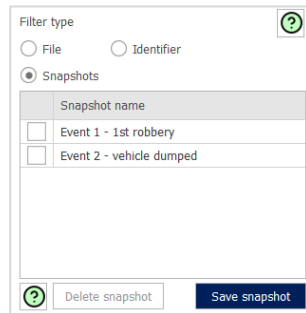
12.1.3 Saving and Opening a Case Snapshot

This setting allows you to save your current chosen filters and the loaded source data as a Case Snapshot. This allows you to revisit that specific dataset, with all of its filters applied, without having to reload and refilter the source data again. The Case Snapshot should also store details of the Case Hub map at the time the snapshot was saved, ensuring that when the snapshot is reopened, the map is displayed in exactly the same state as when it was saved.

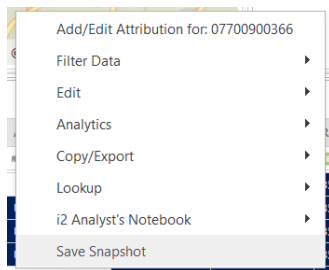
CSASv3 snapshots replace the 'case filter' and 'saved map' features found in CSASv2.

Saving a Case Snapshot

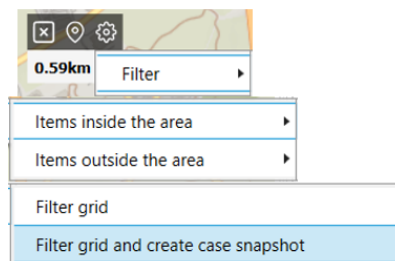
1. To save a case snapshot, first select the dataset and apply any filters necessary to isolate the required set of events.
2. A new Snapshot can be saved in four ways:



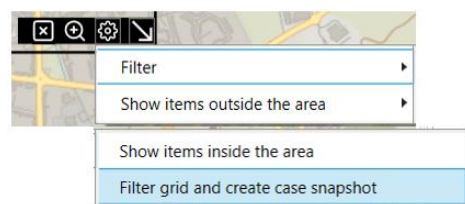
- A new Case Snapshot can be saved from any screen via the filter sidebar.
- Set the Filter type to 'Snapshots', then click on the 'Save snapshot' button.



- A new Case Snapshot can also be saved from Case Hub.
- Right click anywhere in the Case Hub grid and select 'Save Snapshot'.



- Case snapshots can be saved from the in map 'measure from here' tool.
- With a measurement radius label open, click on the gear icon, then select either of the 'filter' options (filter inside the radius or filter outside the radius) both options have a 'filter grid and create case snapshot' option.



- With a marquee select window open, click on the gear icon, then select either of the 'filter' options, both of which have a 'filter grid and create case snapshot' option.

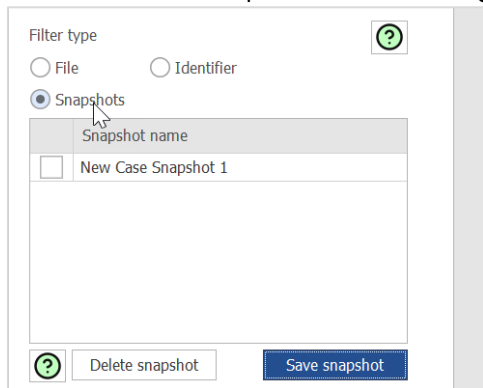
3. In either scenario, in the resulting popup, add a unique snapshot name and click 'Save'.



4. The selected dataset will be loaded ready to be analysed.

Opening a Case Snapshot

1. Under 'Filter type', select the 'Case snapshot' radio button then, from the panel, select a case 'Snapshot name' using the checkbox:



2. To launch a saved Case Snapshot in Case Hub, Case Outputs, Dashboard, Analytics and other CSAS screens, click the **Apply** button at the bottom of the panel.
3. The selected Case Snapshot opens and displays automatically.

Deleting a Case Snapshot

You can delete a 'Case Snapshot' by selecting a snapshot from the list and clicking on the **Delete snapshot** button.

12.1.4 Cell Logic

This setting allows you to select, via a drop-down menu, between 'Source' mode and 'Override' mode, which then determines the level and source of the cell address details added to the output file.



Data for cells is parsed from different source data files and collated into either Source or Override records.

A 'source' cell record contains only the cell location data found in the original source file. For example, if the source file format only includes, for each cell that is listed, the Cell ID and the site name (but does not include site postcode, cell azimuth, map coordinates, etc), the source cell records created for that file will only include the information provided and will be missing some important cell location details.

An 'override' record attempts to gather a complete set of cell location details for each cell ID, which can be used to fill in gaps in source records if required. For example, imagine a case dataset includes two types of CDR from the same operator – a 'voice & SMS' CDR format that includes full location details for all cells and a 'GPRS' CDR format that only includes a cell ID for each cell. Source cell records will be created for both files, but override records can also be compiled from the fuller set of data included in the 'voice & SMS' CDR.

When the contents of those files are listed in CSAS, if the cell logic is in 'source' mode, only the level of cell location provide in the source files is displayed – so records from the GPRS file will be missing details such as cell azimuth and map coordinates and the cells from that file will not be shown on any case maps. If the cell logic is in 'override' mode, however, any cell IDs that appear in both CDRs can have their location details enhanced – 'missing' details in the GPRS records can be 'filled in' from the additional data found in the voice & SMS records, allowing some of the GPRS cells to be displayed on the case map.

The use of cell overrides is particularly important for data from networks such as Vodafone and Three in the UK and most networks in the USA, where the source record only contains limited data, such as the cell ID, and an associated 'cell address' file or table provides the rest of the cell address information.

CSAS defaults to using 'Override' mode, but you can choose you own preferred default – if you change the settings you can click on the 'disk' icon to save the current settings as your preferred default for all cases, or you can click the 'reset' icon to return the setting to its system default.

12.1.5 Date & Time

Filtering via the 'Date & Time' panel allows you to trim the source data displayed in the current dataset based on:

- » Date/time range – based on 'From' and 'To' date/times
- » 'Time Slice'
- » 'Day of Week'.

Dates From/To

The 'From' date and 'To' date/times in the filter default to match the earliest and latest event which are applicable to the case, but you are able to select a narrower time period within those dates if required.

The Date & Time tickbox must be selected to activate the filter.

The 'From' and 'To' date/times can be chosen by:

- typing the required dates and times into the date boxes
- or by clicking into each date or time filed individually and using the up/down arrows to adjust them
- or they can be set via drop-down calendars, by clicking on the small down arrow on the right of the from/to text boxes.

For example, selecting a date 'From' 14/08/2023 10:45:00 'To' 30/08/2023 17:00:00 will alter the current dataset to show only data that falls within that date/time span.

This is useful if you are working on a large case or with files that cover long time periods, as it allows you to select a specific date and time period to view when loading any data into the current dataset.

Note: Using 'From' date and 'To' dates at the same time as selecting the source files to view may have performance benefits and enable Case Hub to load and run more quickly, as fewer events will need to be displayed in the grid or on the map.

To remove the Date/Time filter either:

- » Untick the Date & Time checkbox and hit Apply.
- » Click the  button below the 'To' box and hit Apply.
- » Click the Reset button.

Include Overlapping Events

☐ Include Overlapping Events

When a date/time filter is set that covers a period in the middle of a case, there is a possibility that some events start before the beginning of the filter period but end within the period, or conversely, there may be events that start during the filter period but end after it has finished. These are termed 'overlapping' events, as they cover times outside of the filter period.

By default, the date/time filter only displays events that occur fully within the filter period – e.g. they start after the 'from' date/time and end before the 'to' date/time. The 'include overlapping events' option expands the filter to include any event that was active during the filter period, even if it started before or ended after the selected date/time range.

With 'Include Overlapping Events' unticked, the filter will only include events starting on or after the filter 'from' time and starting on or before the filter 'to' time, so only includes events with a Start time within the filter period.

With 'Include Overlapping Events' ticked, the filter will include all events that were active during the filter period, even if they started before 'from' time or ended after 'to' time.

NOTE: you must click to send the updated filter to the grid if you make any changes to filter options, such as ticking the 'include overlapping' option.

Time Slice

☒ Time Slice

Between

☒ Include Overlapping Events

A Time Slice filter reduces a data set to only show events that occurred between specified times across the days that are analysed.

For example, with the date filter set From 29/08/2023 To 30/08/2023 and the Time Slice set between 10:45:00 and 17:00:00 the current dataset will only include events that took place on those dates between 10:45 and 17:00, it will exclude all events that took place outside of the Time Slice.

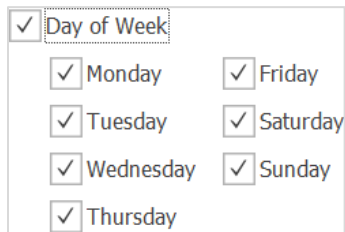
Check the Time Slice tickbox to activate the filter, then select the start and end times for the slice. Hit to activate the filter. This will filter events down to only those that occurred within this time period across all of the days in the date span.

The Time Slice filter also supports an 'overlapping events' option, allowing events that begin before or end after the time slice period but that are active during it to be included.

To remove the Time Slice filter either:

- » Untick the Time Slice checkbox and hit .
- » Click the button below the Time Slice time boxes and hit .
- » Click the button.

Day of Week



The image shows a 'Day of Week' filter panel. At the top is a checkbox labeled 'Day of Week' which is checked. Below it are seven checkboxes for the days of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. All seven checkboxes are checked.

The Day of Week filter reduces the current dataset to show only events that occurred on selected days - for example, if you are only interested in events that take place every Monday, you would untick all of the other days and only analyse events that occurred on Mondays.

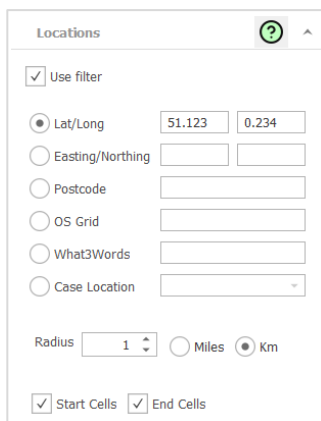
Check the Day of Week tickbox to activate the filter. All days are selected by default, so deselect any days that you do **not** wish to be included in the analysis. Hit **Apply** to activate the filter. This will filter events down to only those that occurred on the selected days in the date span.

To remove the Day of Week filter either:

- » Untick the Day of Week checkbox and hit **Apply**.
- » Reselect all unselected days and hit **Apply**.
- » Click the **Reset** button.

12.1.6 Locations

The 'Locations' panel allows you to filter the data in the current dataset to only show events that have coordinates that are within a set radius of a specific location.



The image shows the 'Locations' filter panel. It has a title bar with a question mark icon and an expand/collapse arrow. Inside, there is a 'Use filter' checkbox which is checked. Below this are several radio button options for location types: 'Lat/Long' (selected), 'Easting/Northing', 'Postcode', 'OS Grid', 'What3Words', and 'Case Location'. Each option has associated input fields. For 'Lat/Long', the fields contain '51.123' and '0.234'. Below these is a 'Radius' section with a numeric input set to '1' and two radio buttons for 'Miles' and 'Km' (selected). At the bottom are two checkboxes: 'Start Cells' and 'End Cells', both of which are checked.

The location to use as the centre point of the filter can be selected in a number of ways:

- » Latitude/longitude
- » Easting/Northing (UK-only coordinate system)
- » Postcode (or zip code) *
- » OS Grid (UK-only coordinate system)
- » what3words – identifies a 3m square
- » Case location – a POI defined within the case

* *The postcode/zip code option may be less accurate as the point location will be calculated as the centre of the post/zip code area, rather than as a specified point.*

You also have the opportunity to set the radius out from the point location and the measurement units (miles or kilometres).

Check the 'Use filter' tickbox in the Locations panel to activate the filter. Select a location type and enter coordinates if required, then set the radius. Hit **Apply** to activate the filter. Only events that took have coordinates associated with them that indicate that they took place within that radius will be listed in the grid and shown on the map – a pin icon will be shown on the map to indicate the point location and a radius circle will be

placed to indicate the filter area.

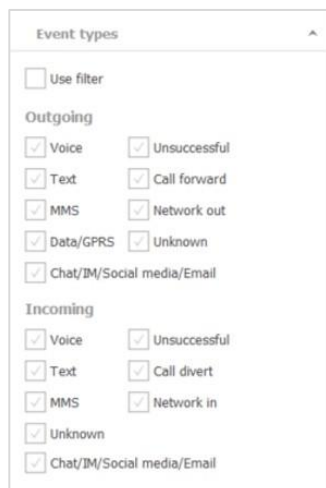
The Locations panel also includes two checkboxes that allow you to elect to include or exclude 'Start' Cells' and 'End Cells' from the analysis. This is only relevant to CDR data, where the 'Start Cell' refers to the cell a phone was connected to at the start of a call and the 'End Cell' refers to the cell reported to be in use at the end of a call. Some organisations have a blanket policy of not analysing end cell data, so this option allows end cell data to be excluded before data is loaded into the Grid and the associated Case Hub map.

To remove the Locations filter either:

- Untick the 'Use filter' checkbox and hit .
- Click the button.

12.1.7 Event Types

This setting allows you to select, using the checkboxes, the type of Outgoing and Incoming 'Events' you want to include in the current dataset. It mostly applies to data from CDR and handset download file types.



You can choose to exclude certain event types from the current dataset by unchecking the relevant event type.

For example, if you want to exclude GPRS/mobile data events from the current dataset, just tick the 'Use filter' checkbox option to enable the event filter and then untick the 'Data/GPRS' checkbox and hit .

All records for the selected event type(s) will be excluded from the current dataset.

To remove the Event Type filter either:

- Untick the 'Use filter' checkbox and hit .
- Retick any unselected event types and hit .
- Click the button.

The Event Type filer was designed to work with CDR/cell data and may cause unintended event filtering if used on other types of data.

12.1.8 Quick Filters

The Quick Filters are used to more easily apply filters that might otherwise be complex to configure. The filter currently only works with CDR data.

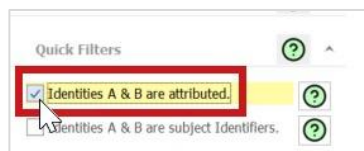
There are currently two quick filter types you can select:

- » Identities A & B are attributed (attributed identifiers only).
- » Identities A & B are subject identifiers (subject identifiers only).

Note: Only one filter can be selected at a time.

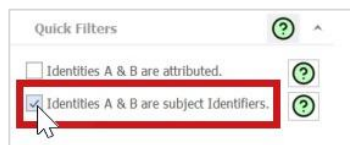
Identities A & B are attributed

Selecting this checkbox allows you to filter the current data set to only include records where the main identifiers have had attribution names assigned to them and can be summarised as 'calls/SMS between attributed phones only'.



For CDR data, this means that only records where both the A/Calling number and the B/Called number are attributed will be displayed.

Identities A & B are subject identifiers



Selecting this checkbox allows you to filter the current data set to only include records where both the main identifiers are subject identifiers and can be summarised as 'calls/SMS between subject phones only'.

The subject phones do not need to have been attributed to be included in this filter.

Quick Filters can be applied by selecting the require filter tickbox and hitting **Apply**.

To remove a Quick Filter either:

- » Untick the Quick Filter checkbox and hit **Apply**.
- » Click the **Reset** button.

Why, When, Who

	This right sidebar functions are necessary to target specific source data files and, optionally, provide more focused source data selection for analysis.
	This function is undertaken at any time.
	This function is typically carried out by the following users: » CSAS User

Stepped Procedure

Individual procedures were outlined in the specific sections above.

12.2 Selecting the Settings Tab

Selecting the 'Settings' tab  icon allows you to configure the way Case Hub and other screens present imported source data and influence what imported source data is shown in the grid. You can select the following options and filters:

- » Case Hub Settings
- » Data Display
- » Matching
- » Redaction

12.2.1 Case Wide Settings

With 'case wide settings' enabled, all open CSAS tabs will use the same settings – you only need to select and apply your preferred settings once and they will be applied to all open tabs. This feature is useful if you want to view different aspects of the same dataset without having to repeatedly change settings options.

Deselecting the 'Case-wide settings' via the slider button allows you to 'decouple' individual screens/functions to show data affected by different settings options in each tab. For example, you may want to display a data set for one identifier in Case Hub with Duplicate Matching enabled and the same set of data in another tab with that setting disabled. In that scenario, you would select the Case Wide Settings slider to the 'Off' position.

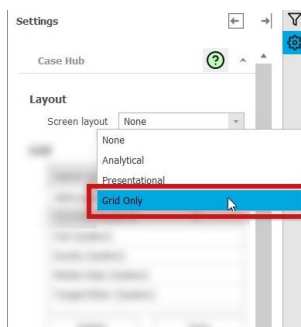
It is recommended that Case Wide Settings remain enabled at all times unless you have a specific reason to disable it.

12.2.2 Case Hub Settings

Note: This section is only available in 'Case Hub' and 'Map Tab' screens.

Layout

The menu, allows you to choose between different Case Hub layouts, which seek to maximise the amount of screen space made available to different aspects of Case Hub:



- » None – reverts to the current default option.
- » **Analytical** - used when you have a need to view both the data grid and a map but are more focused on viewing a reasonable amount of data.
- » **Presentational** - used when a user is more interested in viewing a map and is less focused on the content of the data grid, for example, when presenting case data.
- » **Grid Only** - used when you want to see just the data grid and no map tile.

These options provide a different default balance between the amount of the screen that is given to the grid (Analytical view) or to the map (Presentational view) or just the data grid (Grid Only).

You can also create a custom view by clicking and dragging the panel boundary frames so that you get your preferred proportion of map and grid panel sizes.

You can save a preferred layout by selecting your choice and hitting the  button at the foot of the Case Hub section or can revert to the system default using the  button.

Grid

This option provides a set of predefined and custom grid column layouts for you to choose from, including:

Layout name
Abbreviated (System)
Standard (System)
Full (System)
Events (System)
Mobile Data (System)

- » Abbreviated – shows a small subset of columns.
- » Standard – shows date/time, identifiers, basic cell details.
- » Full – shows all possible columns.
- » Events – features data most applicable to case events & locations.

- » Mobile data – features data most applicable to GPRS records.
- » Target/Other – lists identifiers by target/other rather than calling/called.
- » Any custom layouts you create will also be listed.

To use a specific layout from the list, simply click on the layout you want to use and click the button, the 'Case Hub' Data Grid reconfigures to use the selected layout.

Creating Custom Grid Layouts

The Case Hub grid is flexible both in terms of the set of columns it can include and the positioning of those columns. It is possible to customise the grid layout, by adding or removing columns or dragging the columns into a different order, so you can create your own preferred layout.

Once a personalised layout has created, add it to the list of layouts by clicking on the button.

Add saved grid layout

A pop-up window opens in which you can name and save your custom layout – the new custom layout must have a unique name within your user profile.

Layout name
Abbreviated (System)
Standard (System)
Full (System)
Events (System)
Mobile Data (System)
Target/Other (System)
New Grid Layout 1

Once a layout has been saved, it's added to the list shown under the 'Grid' section:

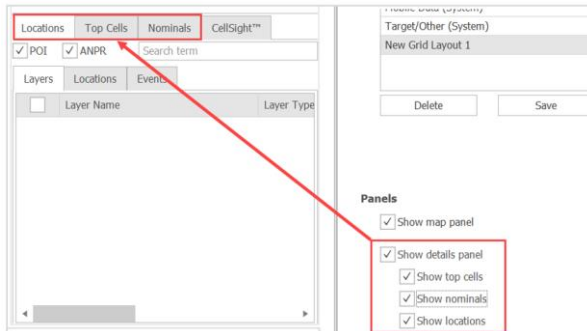
Target/Other (System)
Joe Layout 2

If a custom layout is no longer wanted, select it from the list and click .

Personalised grid layouts and the selected default grid layout, are saved in your CSAS user profile, providing access to them from wherever you access CSAS.

Panels

This setting allows you to select whether the map and details panels are visible by default and also which tabs to show in the Case Hub details panel.



The 'show map panel' option allows you to select whether to show or hide the map panel. The map panel shows the location of all cell sites/towers and event locations associated with the chosen Identifiers.

Note: It is possible to undock the map panel and move it to another screen, by clicking and holding the top row of the map frame and dragging it to another screen.

The 'show details pane;' option allows you to select whether to show or hide the details panel. If the details panel is visible, you can also select the tabs that are presented. When the 'Show details panel' checkbox is ticked, the panels selected by you are displayed on the right side of the Case Hub window:

Note: A maximum of 5 queries can be shown in the details panel at any one time.

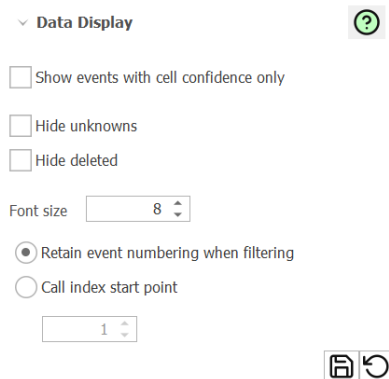
Large Dataset Warning

When working on very large cases, it may be sensible to hide the 'map' and 'details' panels and just work in the Case Hub grid. By hiding those panels, it means that CSAS does not have to keep them updated, which could improve performance for very large datasets. If you attempt to view more than a threshold number of records in Case Hub with the map and details panels visible, you'll be warned about possible poor performance and invited to hide those panels. The default threshold is 50,000 events, but you can change this to a higher or lower figure if you need to.

You can save a preferred grid column layout, panel visibility and large dataset warning threshold by selecting your choice and hitting the  button at the foot of the Case Hub section or can revert to the system default using the  button.

12.2.3 Data Display

The Data Display settings provide the opportunity to set global options for what data is included in the current dataset. The checkboxes allow you to control the way that data is visualised onscreen and also gives you some control over what data is visible:



» **'Show events with cell confidence only'**: hides events where cell confidence is false – this relates to CDR data only and generally relates to GPRS/mobile data events.

Cell confidence will be 'true' if CSAS has confidence that the subject device was using the cell shown for a record at the time of the timestamp for that record.

Cell confidence will be 'false' if it cannot be determined whether the device was using a cell 'at' that time or if it was using the cell sometime 'at or before' the timestamp time.

» **'Hide unknowns/deleted'**: when ticked, each of these checkboxes ensures that the corresponding classes of records are hidden in the current dataset.

- 'unknown' events are those where CSAS cannot determine a definite event type
- 'Deleted' events have been manually removed from the dataset using the Case Hub grid right-click Edit > Delete option, which marks selected records as logically deleted

» **'Font size'**: allows you to adjust the grid font size.

» **Event numbering options**. One of the following two options can be selected:

- **'Retain event numbering when filtering'**. When data is first loaded into the Case Hub grid, the events are numbered sequentially from 1. When filters are applied and rows that match the filter are hidden, this setting determines whether each row retains its original index number (meaning that there will be gaps in the numbering where rows are hidden) or whether all events will be renumbered from 1 again when the filter is applied.
- **'Call index start point'**: the Case Hub grid has an Event Index column that indicates the index (or order) of events. This field allows you to set the event number that the table starts with at the top. Events usually start with index '1', but you can change it to start at a different index number.

You can save your selections in order to create a default for future cases by clicking on the  button. You can restore the system default settings by clicking on the  button.

12.2.4 Matching

The 'Matching' tab function allows you to select from and choose options in the following panes:

- » Duplicate matching
- » Single row matching

Duplicate Matching

Imported data may, occasionally, contain duplicate events, for example, if you obtained the data for a subject phone in a CDR that covered January to March, but then also requested data for the same phone from February to May there would be an overlap period in which events were duplicated. CSAS can be set to ignore duplicates and not display them in Case Hub or Case Outputs or count them in Analytics or Dashboards.

The duplicate matching settings allow you to vary the criteria that are used for event matching, as there may be occasions where the default criteria are too specific to catch all duplicates.

This setting allows you to select, via checkboxes and drop-down menus, matching events from different files, to ensure that any duplicate records are found and only one of those records is displayed or counted. When the same event is recorded in multiple files there may be a slight difference to some of the values (e.g. the duration may be recorded as a second or two different). Sometimes the rules needed to identify these matching events need to be optimized for a particular file set you want to include in the grid.

The values included in the settings are:

☒ Duplicate Matching

☒ Start time
Tolerance (Seconds)

☒ Duration
Tolerance (Seconds)

☒ A/Calling number

☒ B/Called number

☒ Event type

☒ Start cell

☒ End Cell

☒ APN

☒ Combine concatenated SMS
Tolerance (Seconds)
Max msgs to combine

Start time

This function uses the start time of one of the matching parameters and allows you to select the number of seconds (Tolerance) that the start time can vary in other records and still be identified as the same event, so that the duplicates can be removed.

Duration

This function uses the duration of one of the matching parameters and allows you to select the number of seconds that the duration (Tolerance) can vary in other records and still be identified as the same event, so that the duplicates can be removed.

A/Calling number

Use the A/calling (the 'calling' phone) number when identifying a match. If there are versions of the same event record that either don't have an A number or that have a differently formatted A number, this option allows the matching process to ignore Calling numbers.

B/Called number

Use the B/called (the 'called' phone) number when identifying a match. If there are versions of the same event record that either don't have a B number or that have a differently formatted B number, this option allows the matching process to ignore Called numbers.

Event type

Use the event type when identifying matches (Outgoing/incoming voice, text, MMS, outgoing data etc.). If there are versions of the same event record that describe the event differently, this option allows the matching process to ignore the event type.

Start cell/End cell

Use the start cell (the cell which records the start of a record) and/or end cell (the cell that was in use at the end of a record) when identifying matches.

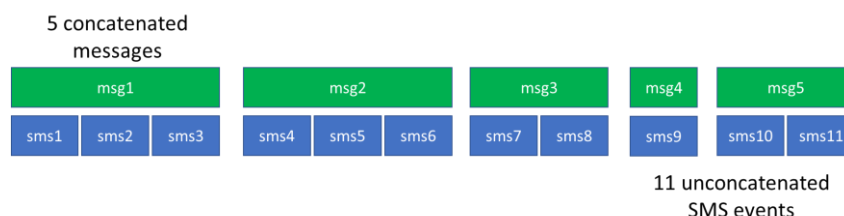
APN

The APN or Access Point Name is included in some network's GPRS/mobile data records – it indicates the data service the user was connecting to via the cellular network. As it is possible for a mobile device to have multiple concurrent connections to different APNs, it is sometimes the case that a CDR will contain multiple duplicate mobile data event records, one for each of those connections. Disabling this option should leave just one mobile data event each time instead of showing duplicates.

Note: Changing the matching settings away from the defaults can be useful when attempting to remove duplicates where the events are captured slightly differently in two or more records. There is also the potential, however, for a loosening of the matching rules to cause false positive matches to be made and legitimate records could be hidden from view.

Combine concatenated SMS

Text messages can carry a maximum of 160 characters, if a message contains more than the maximum number of characters it is split in two or more parts and sent in multiple text transmissions, each of which will be separately listed in the associated CDRs. The receiving phone puts back together (or 'concatenates') the individual text deliveries as a single message to be displayed to the receiving user.

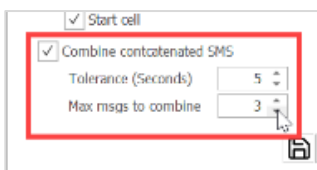


These records can be counted differently, depending on what's being analysed; if an accurate view of the number of substantive messages exchanged between individuals is required, then we should concatenate the delivery records and count just the messages exchanged; alternatively, if a view of the number of individual SMS events is required, then the records should remain unconcatenated and be counted individually.

CSASv3 applies SMS concatenation as a filter. All valid SMS records are passed through

to the case database from the parser and SMS Concatenation can be enabled or disabled by applying/removing the filter. CSAS applies SMS concatenation to CDRs from all networks, but Vodafone UK data has special handling as it provides additional information (the 'Concatenated Short Message Reference Number' field) that explicitly indicates individual records that belong to the same overall message. For all other networks, the process of SMS concatenation is something of a guess, based on finding sequences of records that have the same A/calling and B/called numbers and that were sent within a short time of each other which could be regarded as possibly belonging to the same overall message.

SMS Concatenation settings can be set/viewed/changed in the Settings sidebar, in the 'Duplicate Matching' drop-down panel. Tick the 'Combine concatenated SMS' checkbox to enable the filter or untick it to disable it.



You can set a tolerance for the maximum amount time (in seconds) between the first and last messages in a sequence, and set the maximum number of messages that can be combined

In this example, the Tolerance has been set to 5 seconds and the maximum number of messages to combine (concatenate) has been set to 3. The filter will look for SMS records that have the same A and B numbers, that all have timestamps within the same 5 second period and will combine a maximum of three records together to display details of just one SMS for that time period. If there were four matching records within a 5 second period, the filter would output two SMS records, one concatenating the first 3 records and one with the last record on its own.

When you make changes to the filter values, click the **Apply** button. The filter will find and merge matching SMS records and the Case Hub grid will refresh. The number of rows displayed in the grid may change depending on the parameters you set.

Note: This function can be used in both 'Multi row' and 'Single row' views.

Single-row Matching

This setting is used to manage the Singlerow grid view in Case Hub and the singlerow template options in Case Outputs. In a single row view, the paired incoming and outgoing records for calls or texts between subject phones are combined and displayed on the same row in the Case Hub grid or call schedule. This is sometimes regarded as offering a more accurate view of the overall number of substantive events contained in a dataset and is preferred by some investigators and courts. The settings in the 'Single-row matching' section allow you to select, via checkboxes and drop-down menus, how potentially matching events are identified and merged.

Different organisations have their own rules about what type of events should be combined in single row views (some allow SMS events to be combined, for example, while others prefer to display SMS events on separate rows) and in different scenarios the tolerances for matched events to be combined might need to be adjusted. The single row matching controls provide an opportunity to manage the settings used for combining records in this way. They allow you to choose whether voice, SMS and MMS events get combined at all, and if they are combined, to set the tolerances for triggering the

matching process.

For example, if SMS combination is allowed (if the outgoing and incoming records for an SMS are combined into a single row), the tolerance for the difference in the source records' start times can be set. If the tolerance is set to 10 seconds (the default value), matching records whose start times are less than 10 seconds apart will be combined, but those whose start times are more than 10 seconds apart will be shown on separate rows.

The full set of parameters for singlerow matching is as follows:

☒ Voice matching?	
Voice second limit	10
☒ Include Divert/Call Forwards?	
☒ SMS matching?	
SMS second limit	10
☒ MMS matching?	
MMS second limit	10
Use Start/End times from?	Outgoing

Voice matching?

This function turns on/off the matching of voice calls. If disabled, no voice call records will be matched. A tolerance value allows you to set the maximum permitted time difference between records that can be matched, which defaults to 10 seconds.

Include Divert/Call Forwards?

This function turns on/off the matching of voice calls with call divert and call forwarding events. When enabled, records for unanswered outgoing voice calls can be matched to the records of the resulting call forward or voicemail event.

SMS matching?

Turns on/off the matching of SMS events. If disabled, no SMS events will be matched. A tolerance value allows you to set the maximum permitted time difference between records that can be matched, which defaults to 10 seconds.

MMS matching?

Turns on/off the matching of MMS events. If disabled, no MMS records will be matched. A tolerance value allows you to set the maximum permitted time difference between records that can be matched, which defaults to 10 seconds.

Use Start/End times from?

This function allows you to choose where to take the timestamp for a combined pair of records from, with options to use the timestamp from the outgoing record, the incoming record or from whichever is earliest.

You can save your selections to create a default for future cases by clicking on the  button. You can restore the original system default settings by clicking on the  button.

12.2.5 Redaction

This setting allows you to select from and choose a set of methods for redacting or obscuring the identifiers viewed onscreen or sent to the output template. This is often done to reduce the 'collateral intrusion' associated with displaying the full details of contacted phone numbers and other identifiers in case data, it is sometime also used as way of protecting the identity of witnesses and informants. If enabled, redaction is applied to all qualifying identifiers displayed onscreen and also to those displayed in any output created from the case.

I	
Calling Number	
07700900189	
07700900621	
07700900621	
07700900621	Unredacted ('0' selected)
07700900366	
150	Redacted
0770***0597	

In these examples, the top rows contain unredacted identifiers, but the last row shows an identifier to which redaction has been applied.

The first and last N characters (N = 4 in this example) have been left unredacted and the characters in between have been replaced with a 'redaction character, which defaults to an asterisk.

The redaction settings include:

Leave first N unredacted	4
Leave last N unredacted	4
Redaction Character	*
What to redact	
☐ Identifier	☐ IMEI
☐ Name	☐ IMSI
Who to redact for	
☐ Subject identifiers	☐ Attributed
☒ Non-Subject identifiers	☐ Unattributed

- » 'Leave first N unredacted' - a checkbox which allows you to specify the number of leading digits of each identifier that will be left unredacted.
- » 'Leave last N unredacted' - a checkbox which allows you to specify the number of trailing digits in each identifier that get left unredacted.
- » 'Redaction character' - a text field which allows you to enter your chosen character which is displayed instead of the original unredacted character (this example shows an 'Asterisk' has been chosen):

- » 'What to redact' - using the checkboxes, you can choose to redact the following information in the output report:

- Identifier (phone number, IMEI, VRM, etc)
- Name (if an attribution name has been linked to an identifier)
- IMEI
- IMSI

- » 'Who to redact for' - using the checkboxes, you can choose to redact the following types of Identifiers in the output report:

- Subject identifiers (redacts subject/target identifiers)
- Non-Subject identifiers (redacts non-subject/non-target identifiers)
- Attributed (redacts identifiers that have been linked to attribution names)
- Unattributed (redacts identifiers that have not been linked to attributions).

You can save your selections in order to create a default for future cases by clicking on the  button. You can restore your original default settings by clicking on the  button.

12.3 Selecting the Export Tab

Selecting the 'Export' tab  icon allows you to export and print your selected data

output. The Export tab is only displayed for a limited number of screens.

12.3.1 File Export

Using the radio buttons, you can select which file format you want to export the selected data output to:

- ☒ Excel ☐ CSV ☐ Image
☐ PDF ☐ RTF ☐ HTML
☐ Word ☐ Text

You have two more export options selectable via the following checkboxes:

- ☒ Open document after export
☐ Export to multiple documents

The 'Open document after export' option instructs CSAS to launch the exported data in the appropriate viewer after the data has been exported and has been saved in the case folder – with this option deselected the exported file is simply saved to the case folder but not opened.

The 'Export to multiple documents' option allows you to choose to export all panes from the Dashboard to the same file (e.g. if Excel is the selected option, each pane is exported to a different tab in the same file), but with the option deselected, each pane is exported to a separate file.

When ready to export, click on the button. Once the file(s) have exported, a new screen will open from which you can further process the data output as necessary.

12.3.2 Printing

Once you have selected the data output you want to print, click on the button. A print 'Preview' screen will open from which you can select more options before finally printing the data output.

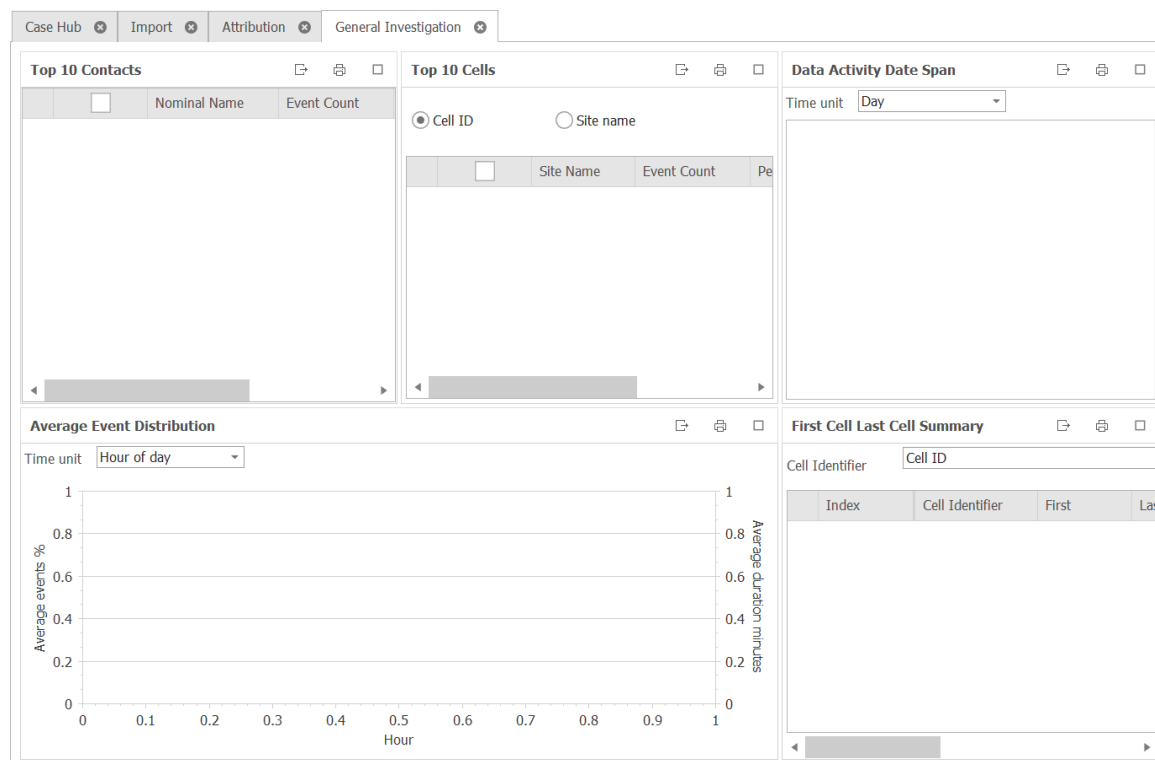
13 Using Case Dashboards

This function is designed to gather the facts and details from a case into one place to give you a quick 'heads up' on the most important data contained in that case.

All of the data available in a dashboard is also available in Analytics, it's just that the Dashboard gathers all of that data together in one easy to access view.

13.1 Dashboard Controls

The  button in the navigation panel includes a drop-down menu from which you can select the General Investigation Dashboard. This function allows you to review, at a glance, an overview of the important information for an open investigation:



The dashboard consists of a set of 'widgets', which each display the results of a different analytical query.

13.1.1 Widget Controls

Each widget includes a set of controls in its header row:



These allow you to:

- » Export the query results to Excel.
- » Print the query results.
- » Maximise the widget to fill up the whole screen.

13.1.2 Grid Controls

As with other CSAS grids, the widget grids offer a full set of filtering and column choice options. For details see *Grid Filtering and Controls*.

13.1.3 Data Selection and Filtering

The Dashboard displays data for the current dataset, which can be loaded and filtered as required from the Filter sidebar.

Who, When, Why

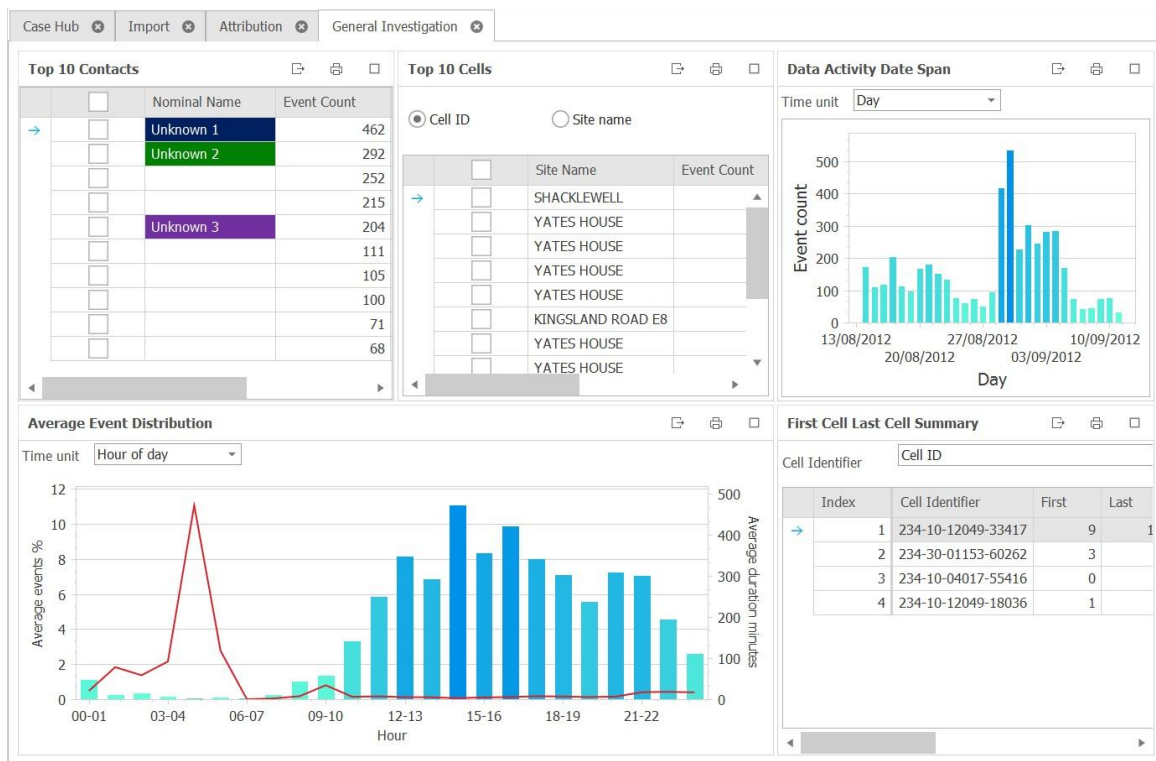
	This function is necessary to view at a glance the most relevant analytics information for a selected investigation and to print and/or export for review.
	This function is undertaken at any time Dashboard is used.
	This function is typically carried out by the following users: » CSAS User

Stepped Procedure

The operation of each individual widget is outlined below.

13.2 General Investigation Dashboard

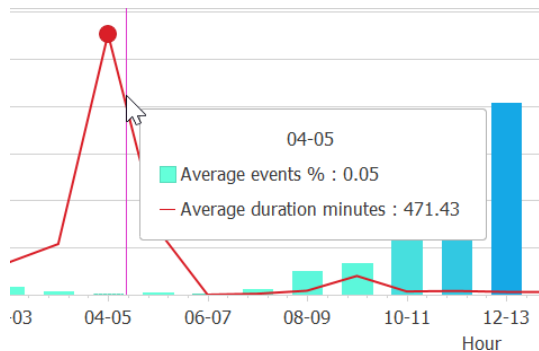
The General Investigation Dashboard is displayed as panes (or 'widgets') containing a mix of grids and graphs:



A typical Dashboard has 5 or 6 panes, which in the 'general investigation' Dashboard are:

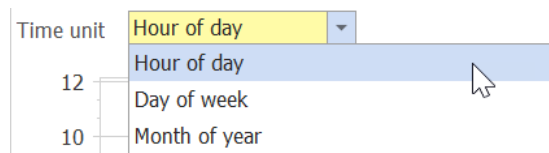
- » **'Top 10 Contacts'** - this pane displays a grid listing the top 10 contacts for the selected dataset by number of events.
- » **'Top 10 Cells'** - this pane displays a grid listing the top 10 cells or cell sites by number of events. The radio buttons toggle between a count of individual cell IDs and a count of cell sites.
- » **'Data Activity Date Span'** - this pane displays a graph showing the activity per day/week/month (selectable) covered by the dataset counted by number of events.
- » **'Average Event Distribution'** - this pane displays a graph showing the average number of events over an hour of day, day of week or month of year period (selectable).
- » **'First Cell Last Cell Summary'** - this pane displays a grid listing a summary of the first and last cell IDs/cell sites/cell postcodes (selectable) used during the selected time period.

Panes which contain a graph will display instant data by hovering the cursor over the graph:



As you scroll left to right the data adjusts accordingly.

You can manipulate the data that some graph panels display by selecting a different time unit from the 'Time unit' drop-down menu, for example:



Each time you select a different time unit the content of the graph automatically updates. Each pane can be:

- » Exported (refer to 'Exporting / Printing from any Dashboard Pane').
- » Printed (refer to 'Exporting / Printing from any Dashboard Pane').
- » Maximised to fill the whole screen.

13.2.1 Exporting / Printing

This function allows you to print / export from any Dashboard pane.

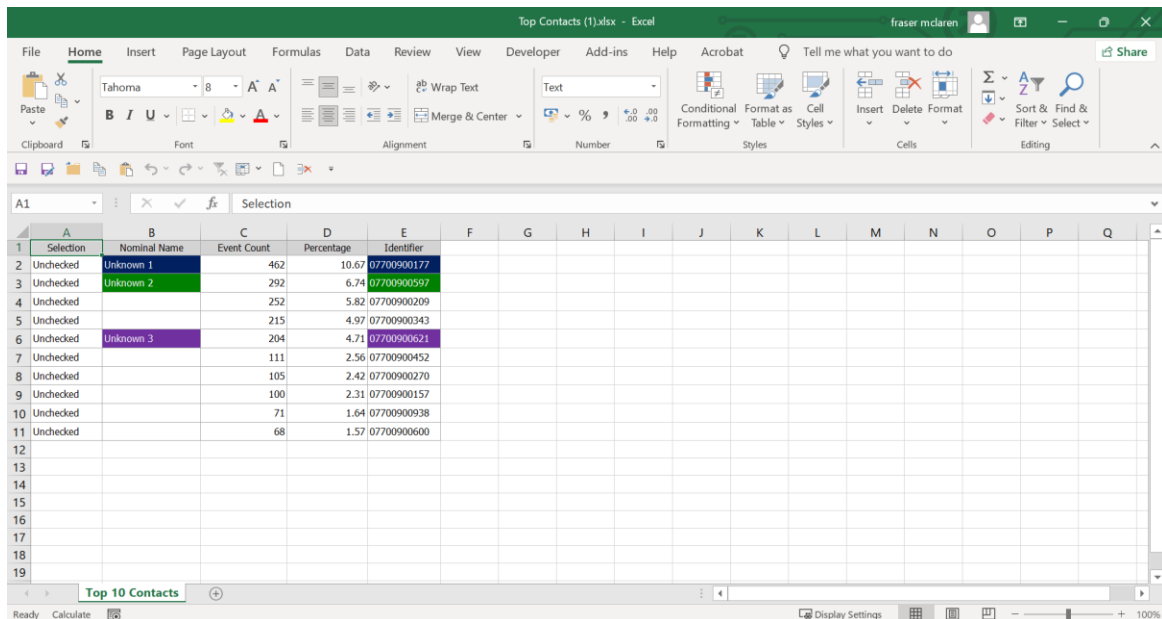
This function provides you with exporting and printing options via icons at the top right corner of each pane on the Dashboard:



Note: This exporting function differs to the 'Export' sidebar filter function as this function only exports to Excel.

Exporting

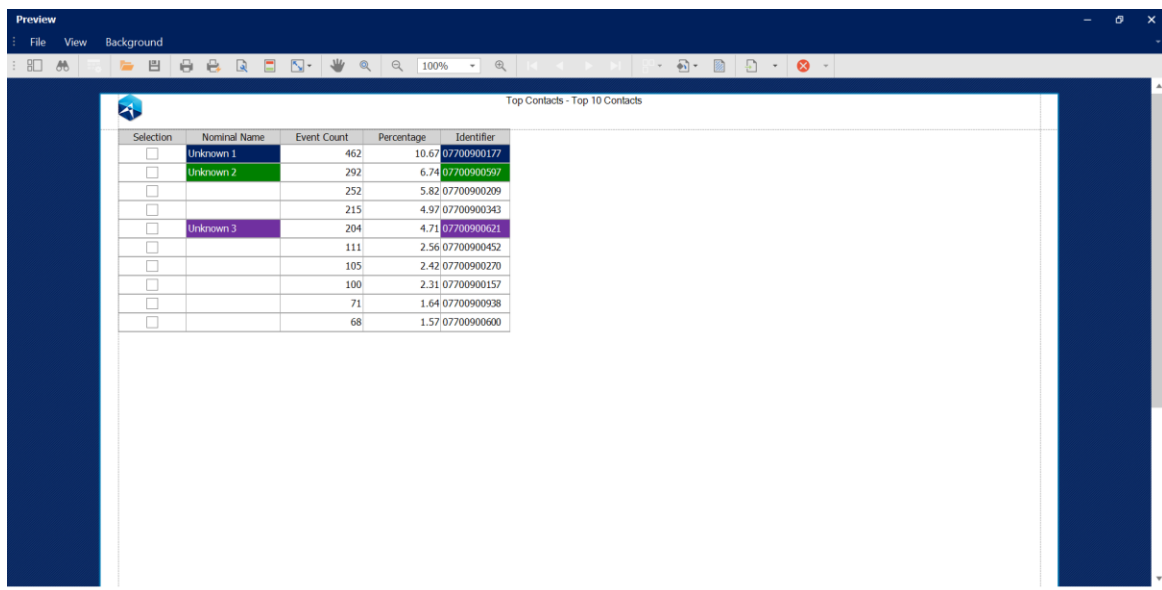
When you select to export a pane, for example 'Top 10 Contacts', an Excel file will open displaying the exported data. A copy of the file will also be automatically saved to the case 'Outputs' folder.



Selection	Nominal Name	Event Count	Percentage	Identifier
Unchecked	Unknown 1	462	10.67	07700900177
Unchecked	Unknown 2	292	6.74	07700900597
Unchecked		252	5.82	07700900209
Unchecked		215	4.97	07700900343
Unchecked	Unknown 3	204	4.71	07700900621
Unchecked		111	2.56	07700900452
Unchecked		105	2.42	07700900270
Unchecked		100	2.31	07700900157
Unchecked		71	1.64	07700900938
Unchecked		68	1.57	07700900600

Printing

When you select to print a pane, for example 'Top 10 Contacts', a 'Preview' pop-up window opens in front of the Dashboard:



Selection	Nominal Name	Event Count	Percentage	Identifier
☐	Unknown 1	462	10.67	07700900177
☐	Unknown 2	292	6.74	07700900597
☐		252	5.82	07700900209
☐		215	4.97	07700900343
☐	Unknown 3	204	4.71	07700900621
☐		111	2.56	07700900452
☐		105	2.42	07700900270
☐		100	2.31	07700900157
☐		71	1.64	07700900938
☐		68	1.57	07700900600

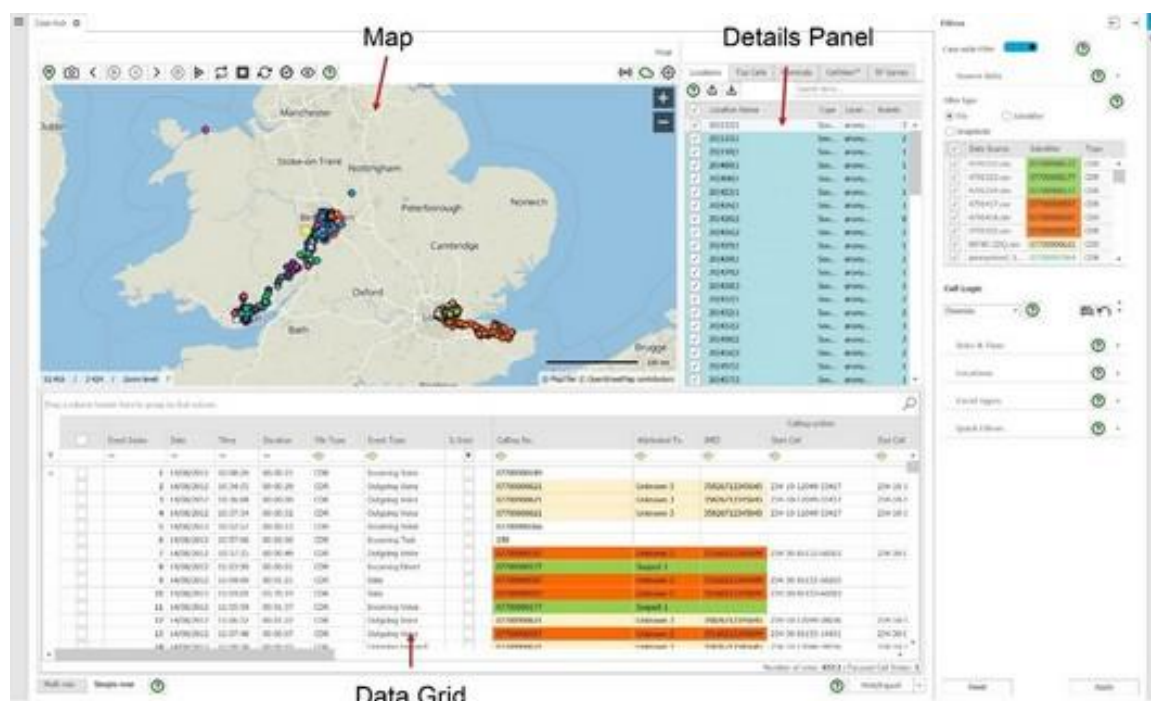
Clicking on 'File', 'View' and 'Background' gives you various options for page setup, tool bar, status bar, colour and watermark options. You can edit the print file by choosing buttons from the tool bar at the top of the pop-up window.

14 Using Case Hub

This function allows you to view case data, create detailed maps and access key analytic queries all in one screen. Case Hub provides you with phone data and phone download information (and also ANPR, event details and any other type of data that has been imported into the case), for selected source data files and to view that data all in one place.

14.1 Layout

The Case Hub screen is split up into windows or panels:



» Data Grid which can be switched between:

- 'Multi row' view
- 'Single row' view

» Map

» Details Panel:

- 'Locations'
- 'Top Cells'
- 'Nominals'
- 'CellView'
- 'RF Survey'.

14.2 General Operation

Case Hub functions are available by clicking on the  button from the 'Case Home' navigation panel (or by other screen prompts). The 'Case Hub' screen opens.

This function provides a grid which offers a central location within CSAS to view all case data. The grid is primarily designed to display imported call data (from source CDRs), but can also show handset download events, ANPR captures and any other imported event data that has a date/time component.

The 'Case Hub' grid can be filtered using a wide variety of filtering options (see *Using the Right Sidebar*) to ensure that you can view exactly the subset of events that you need to.

The 'Case Hub' grid is also used to drive the associated map and analytics panels, so by filtering the grid you are also filtering the data shown in the linked map and analytics queries.

To use the 'Case Hub' grid, select the source data files that you want to view (with a choice of CDRs, handset download, ANPR, case events files, etc), load them into the grid and view them.

'Case Hub' supports a 'Multi row' view, in which each call record is presented on a row of its own meaning that calls/texts between subject phones, where the data contains both the outgoing and incoming records for the event, is shown on two separate rows, and also a singlerow view, where the outgoing and incoming records for the same event are merged onto one row.

There are right-click menus in the grid header and inside the grid.

'Case Hub' has an integrated map that synchronises with the contents of the data grid, providing an immediate and responsive method for visualising case data.

14.3 Using the Grid

14.3.1 Viewing Data

You select the data to view in 'Case Hub' using the Filter sidebar, source data section. The 'Filter' sidebar filters can be used to tailor the dataset before sending it to the grid.

14.3.2 Grid Controls and Filtering

The 'Case Hub' grid shares a common set of filtering and layout controls with the other grids in CSAS.

For details of how to apply filters, customise the column layout and other grid control options, see *Grid Filtering and Controls*.

Using the Find Panel

All CSAS grids support an optional 'find' panel, which offers a powerful 'whole grid' search function that can be especially useful in case Hub. There are multiple ways to search for items within the Case Hub grid, but most of them are limited to searching within a particular column. The find panel is able to look in all columns and will highlight any instances of the search term and filter the grid to only display rows that include the search term.

Identity A	Attribution A	Identity B	Attribution B	Raw IMEI	IMSI	Start Cell (Raw)
07700908010		07700907086	Unknown 2			
07700908010		07700907086	Unknown 2			
07700908010		07700907086	Unknown 2			
07700908010		07700907086	Unknown 2			
07700908010		07700907086	Unknown 2	357777700902270	234157700909569	GBR-VF-933-6436

If the find panel isn't shown automatically, it can be enabled by right-clicking in the header row of any column and selecting 'Show Find Panel'.

Column Chooser

This is also a standard feature in all CSAS grids but, again, can be particularly useful in case Hub. The Column Chooser lists all available column types that aren't in view in the current grid layout. If you wish to create a bespoke grid layout, with your own selection and arrangement of columns, the Column Chooser (along with the Hide Column option) is a key tool to be used. Both Column Chooser and Hide Column are available from the main grid right-click menu.

14.3.3 Changing Views and Column Layouts

The 'Settings' sidebar, 'Case Hub' section hosts two controls that can influence the layout of the 'Case Hub' grid.

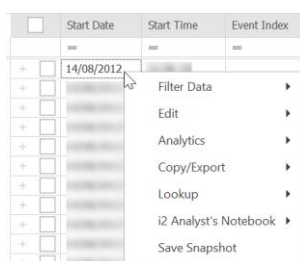
The 'Views' option can switch the overall layout of 'Case Hub' to make it more suitable for different usage scenarios – the 'Analytical' view prioritises the grid and makes the map panel smaller, whereas the 'Presentational' view prioritises the map and reduces the size of the grid. A third option of 'grid only' hides both the map and Details panels and displays only the grid – this is recommended for very large cases, where the updating of the map and Details panels could cause a dip in grid performance.

For details of these controls, see *Using the Right Sidebar*.

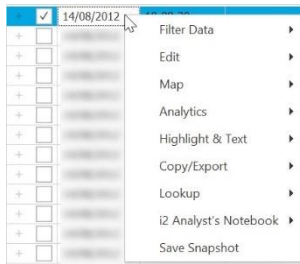
14.3.4 Grid Right-click Menus

In the grid, there are two slightly different right-click pop-up menus available, depending on whether you select to use 'Multi row' or 'Single row'.

When using 'Multi row', you have the following menu options:

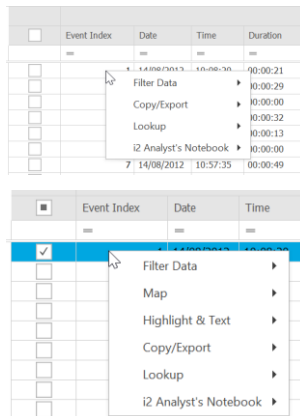


» Right-click anywhere on the grid, this version of the primary pop-up menu opens.



- » Select a checkbox for one of more rows in the grid and then right-click on them, an expanded version of the pop-up menu opens. The expanded version contains event-specific options that are only available once specific events have been selected.

When using 'Single row', you have the following abbreviated menu options:



- » Right-click anywhere on the grid, this version of the primary pop-up menu opens:
- » Select a checkbox for one of more rows in the grid and then right-click on them, an expanded pop-up menu opens.

Using the menus, you can select from a number of menu options to change the data presented in the grid.

Note: All menu options are described below and cover both 'Multi row' or 'Single row' grid options.

Filter Data

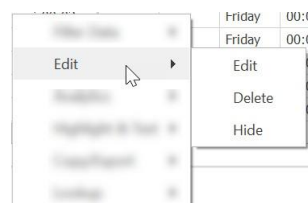
Offers options to filter the grid based on the rows that have been selected using the 'per row' checkboxes:

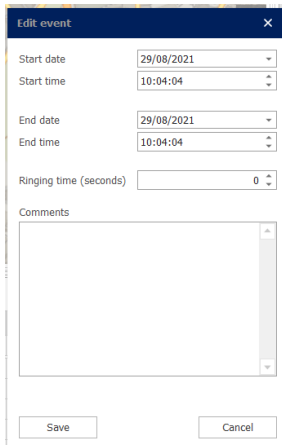
14/08/2012	10:57:06	00:00:00	CDR	Incoming Text	☐	150
14/08/2012						07700900597
14/08/2012						07700900177
14/08/2012						07700900597
14/08/2012						07700900597
14/08/2012						07700900177
14/08/2012						07700900621
14/08/2012	11:07:48	00:00:07	CDR	Outgoing Voice	☐	07700900597

Selecting 'Filter grid to selected rows' retains the highlighted rows and hides any others. The 'Filter grid to non-selected rows' does the opposite, hiding the highlighted rows and keeping the others.

Edit

Offers options to Edit, Delete or Hide a selected row in the grid:





The 'Edit event' dialog box contains the following fields:

- Start date: 29/08/2021
- Start time: 10:04:04
- End date: 29/08/2021
- End time: 10:04:04
- Ringing time (seconds): 0
- Comments: (text area)
- Buttons: Save, Cancel

The 'Edit' function allows a subset of the timestamp elements of the records for an event to be edited, these include:

- Start time
- Start date
- End time
- End date
- Ringing time

The 'Edit' function can also be used to add comments to an individual record – any comments added will be displayed in the Comments column in the Case Hub grid.

The 'Delete' function offers options to remove a record from the current dataset.

This process does not actually delete the record from the dataset, it merely marks it as logically deleted so it is ignored in all grids, charts, maps and outputs. This offers a non-destructive way of removing unwanted data from a case, e.g. in the event that duplicate events slipped through the parsing process. Details of any 'delete' action will be captured in the CSAS case audit.

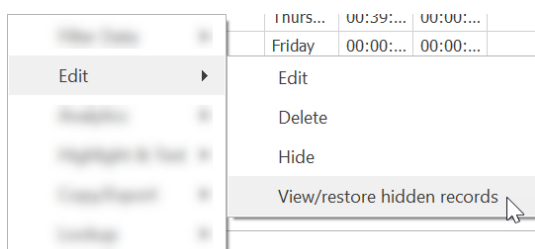
If the *Settings sidebar > Data Display > Hide Deleted* option is selected, any records marked as 'deleted' will be hidden in the Case Hub grid. If the *Hide Deleted* option is unselected, 'deleted' records will be displayed, but will be highlighted to indicate that they are being ignored.

You can Restore the deleted row(s) by right-clicking in the necessary row to open the filter menu and selecting 'Edit > Restore' (Note: you may need to unselect the *Hide Deleted* option to be able to view the deleted rows before you can restore them):

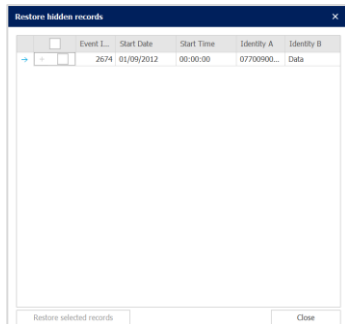
	Start Date	Start Time	Event Index	Timing Offset	Duration	Event Type	Identity A	Attribution A
	=	=	=	=	=			
+ ☒	29/08/2021	10:04:04	1		00:00:00	Emergency Ring	07700900393	
+ ☐	29/08/2021	10:54:37	2			Emergency Ring	07700900999	
+ ☐	29/08/2021	11:14:00	3			Emergency Ring	07700900021	
+ ☐	29/08/2021	11:26:22	4			Emergency Ring	07700900621	
+ ☐	29/08/2021	11:33:10	5			Emergency Ring	07700900621	

The row(s) colour changes back to a white background after the record has been restored.

When you select to Hide a row, a fourth option will be displayed in the sub-menu:



This feature is used for triaging data, allowing you to hide rows that are not currently important or relevant without removing them from the dataset.

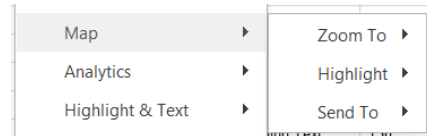


Clicking on the 'View/restore hidden records' option opens the 'Restore hidden records' pop-up window, which lists all currently hidden rows. You can select the row(s) you want to unhide then click on the **Restore selected records** button.

The selected row(s) are restored in the grid.

Map

offers further methods for allowing the grid and the map to interact:



Note: This option is only available when the grid rows have been ticked, not when they are merely highlighted.

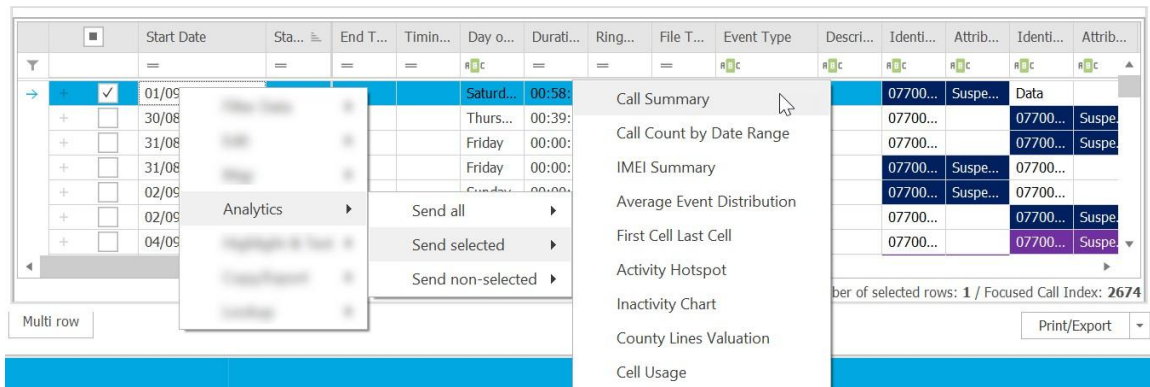
'Zoom To' instructs the map to zoom to the start site for the selected row. If multiple rows, covering multiple cells, are selected, the map zooms to an area that encompasses all selected cells, which may be less effective than zooming to just one site.

'Highlight' activates a pink highlight around the sites associated with the selected rows – with options of highlighting the start site, end site or start & end sites. There is also an option to remove any active highlights from the map.

'Send To' – sends the data associated with the selected row(s) to a new map, offering an additional method for creating a filtered dataset to analyse.

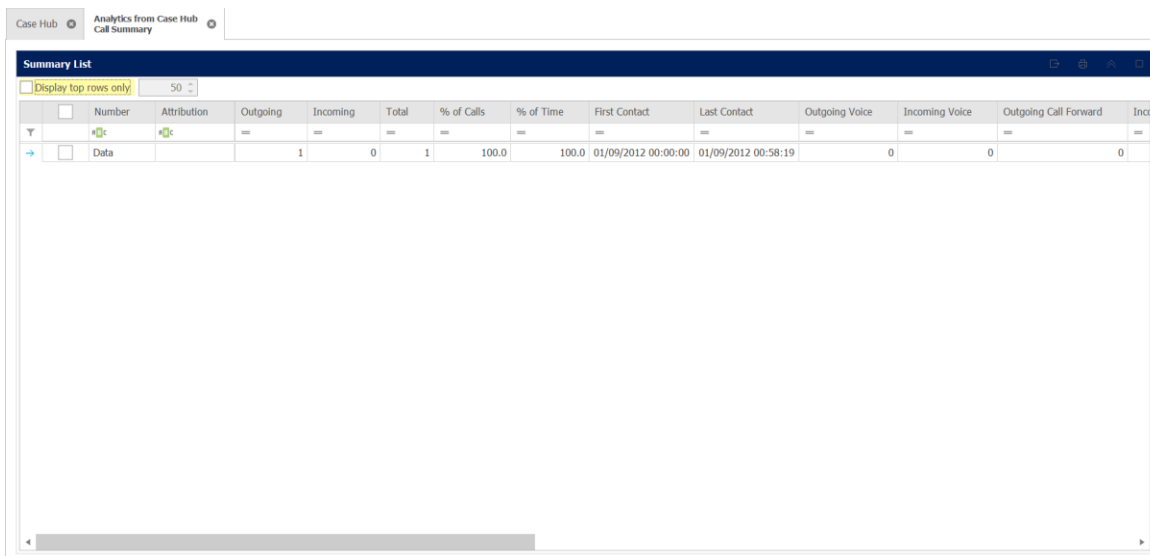
Analytics

sends selected, non-selected or all grid rows to a selected Analytics query:



Note: Only the 'Send All' option is available for unticked rows, all options are available for ticked Case Hub rows.

If you highlight a set of rows in the grid and then select to 'Send selected' to 'Call Summary', the Analytics 'Call Summary' screen opens with only the selected data displayed:

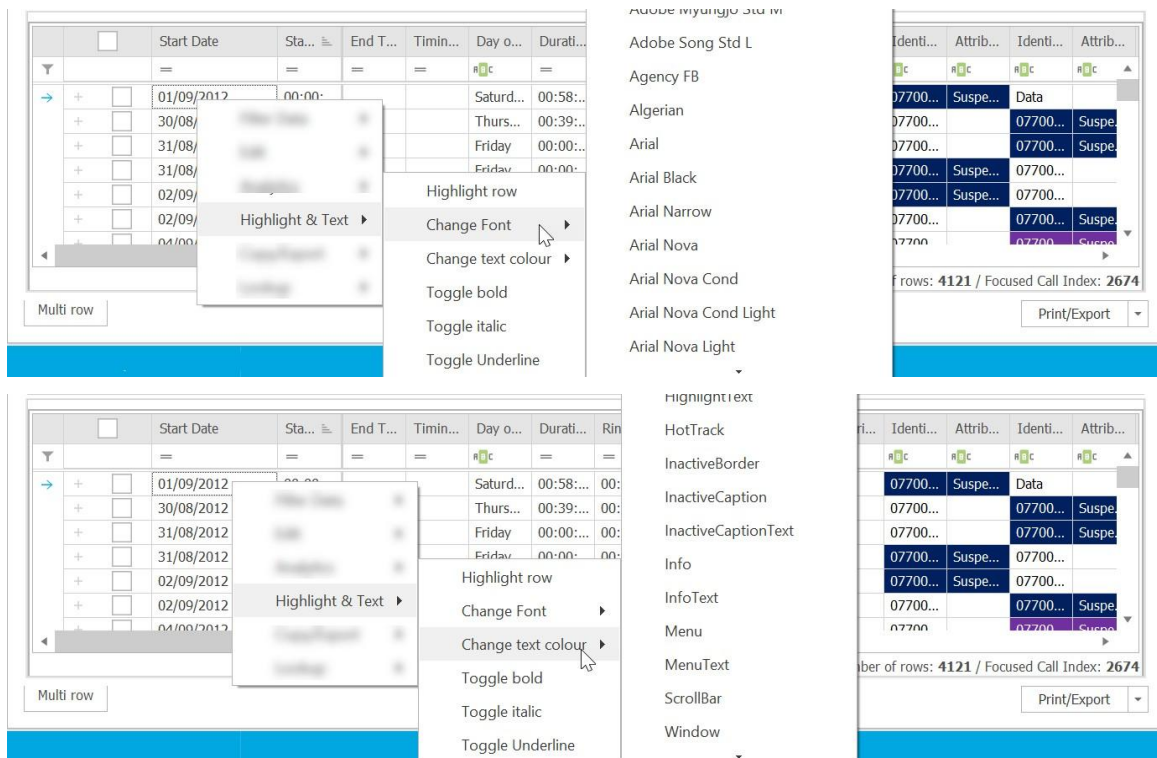


This feature gives a quick way of filtering data to be used in an Analytics query and allows queries to be run on-the-fly with a subset of case data.

Note: Sub-menus for 'Send all', 'Send selected' and 'Send non-selected' are the same.

Highlight & Text

changes the font style and fill colour for selected rows in the grid:

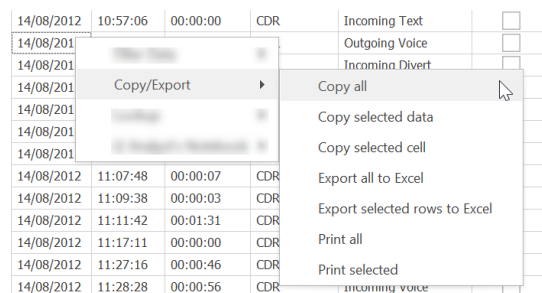


It is also possible to set text effects, such as bold, italic and underline for the data in the selected rows. Currently, any text effects applied using this function are not saved to the database and will be lost when Case Hub is closed.

Note: This option is only available when the grid rows have been ticked, not when they are merely highlighted.

Copy/Export

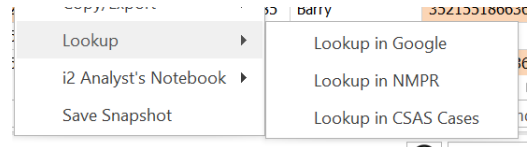
This feature offers options to copy or export selected or all data and cells to a clipboard, and print all or selected data for review:



'Copy All' copies the entire grid, 'Copy Selected' only copies ticked rows and 'Copy Cell' copies the contents of the cell the pointer is currently hovering over. The 'Export' and 'Print' options offer similar functions.

Lookup

This option opens a drop-down menu from which you can elect to send the selected to either a Google search page, use the NMPR Lookup feature or search for the selected identifiers in other CSAS cases.



Selecting 'Lookup in Google' sends the data in the grid cell under the pointer to a Google search page.

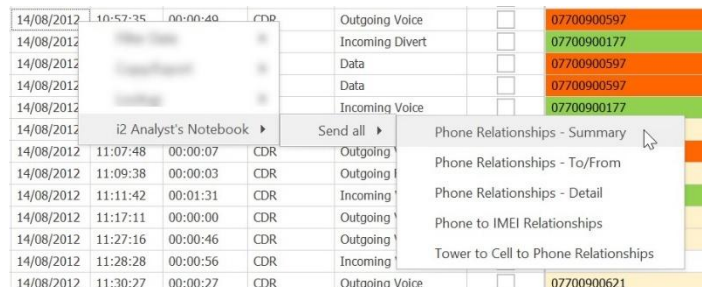
Lookup in NMPR and CSAS Cases are only available from Case Hub Multi row view layouts.

For information about selecting 'Lookup in NMPR', refer to *Using Lookup in NMPR*

For information about selecting 'Lookup in CSAS Cases', refer to [Cross Case Search](#).

i2 Analyst's Notebook

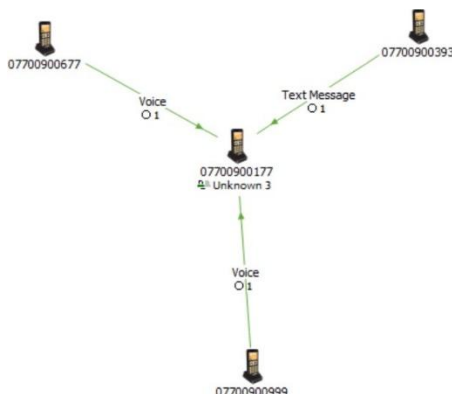
opens a drop-down menu from which you can select different options to send key analytical queries from CSAS v3 and into a local version of i2 Analyst Notebook.



Note: The following summaries assume you have an instance of i2 Analyst's Notebook installed on the same machine/virtual machine as CSAS. If your i2 Analyst's Notebook feature won't open i.e. is not available, you will see the following pop-up message:

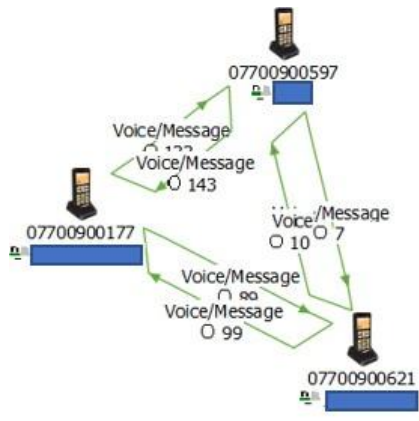


There are 5 pre-built queries you can choose from - these are summarised below:



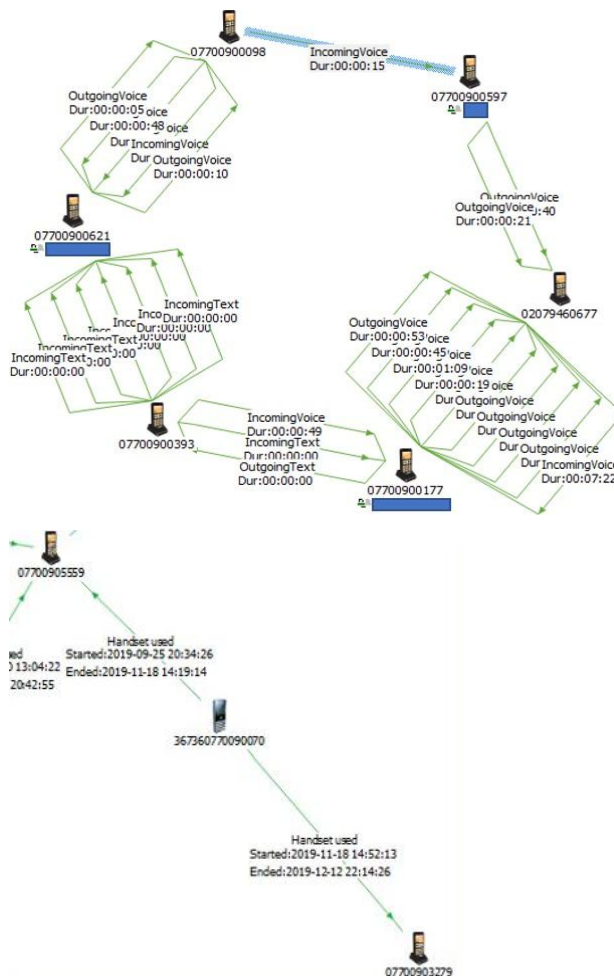
'Phone Relationships - Summary': allows you to launch i2 Analyst Notebook with your CSAS call data so that you can see the phone relationships summary for a particular phone.

Note: The arrows show the direction of the call / message which has taken place.



'Phone Relationships - To/From': allows you to see the direction of calls to a phone.

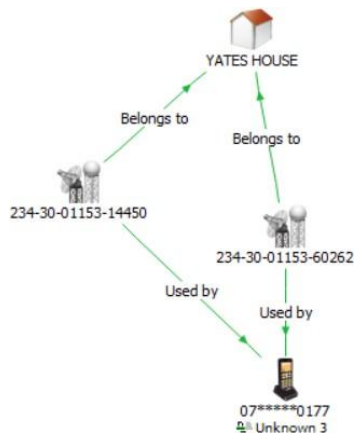
Note: The arrows show the links between the phones, summarising the direction and the number of calls.



'Phone Relationships - Detail': allows you to see details about a particular phone including call types, durations and attributions, and start times, for analysing.

Note: Every instance of a phone record is linked, and the links have attributes, call types, durations and start times.

'Phone to IMEI Relationships': allows you to see the interactions between handsets based on their IMEI.



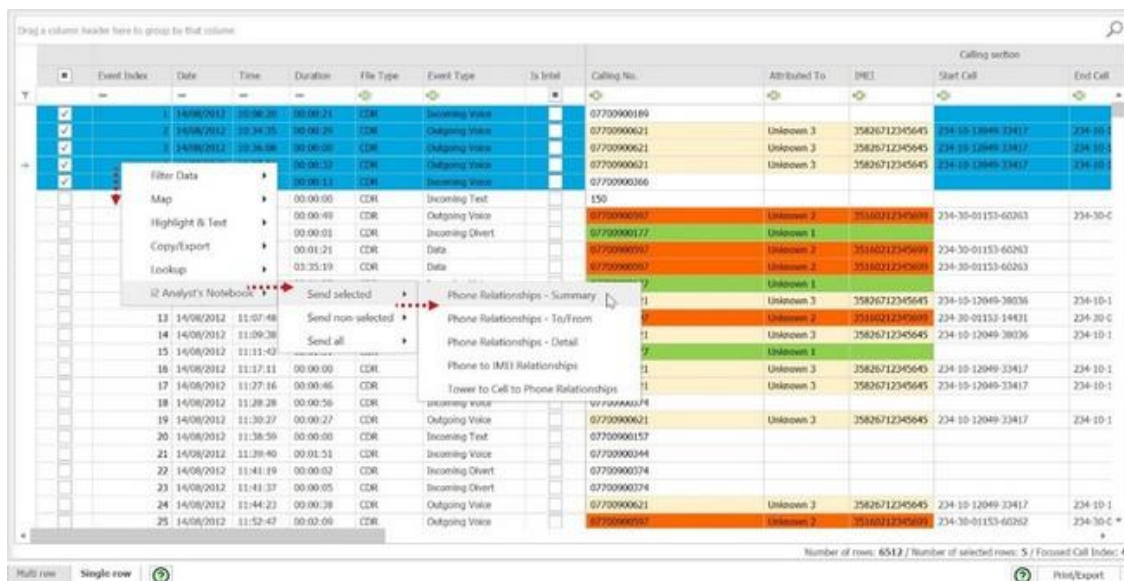
'Tower to Cell to Phone Relationships': allows you to visualise which cells belong to which towers the phone has been using from your CDR files.

Note: The arrows show the links between the phones, summarising the direction and the number of calls.

Stepped Procedure

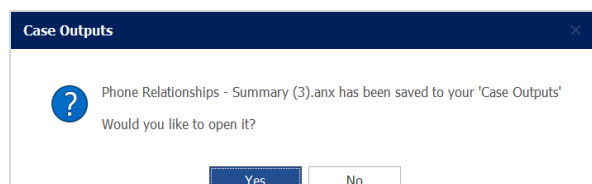
Selecting and sending data to i2 Analyst's Notepad:

- From the Case Hub grid:
 - Select the data you want to send to i2 Analyst's Notepad.
 - Right-click on your selected data and from the drop-down menu select, for example, 'Send to i2 Analyst's Notepad'.
 - Choose the query type, for example 'Phone Relationships - Summary':



Event Index	Date	Time	Duration	File Type	Event Type	Is Intel	Calling No.	Attributed To	IMEI	Start Call	End Call
1	14/08/2012	10:36:20	00:00:21	CDR	Incoming Voice		07700900189	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
2	14/08/2012	10:34:35	00:00:29	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
3	14/08/2012	10:36:06	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
4	14/08/2012	10:36:06	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
5	14/08/2012	10:36:06	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
6	14/08/2012	10:36:06	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
7	14/08/2012	10:36:06	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
8	14/08/2012	10:36:06	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
9	14/08/2012	10:36:06	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
10	14/08/2012	10:36:06	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
11	14/08/2012	10:36:06	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
12	14/08/2012	10:36:06	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
13	14/08/2012	11:07:48	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
14	14/08/2012	11:09:38	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
15	14/08/2012	11:11:40	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
16	14/08/2012	11:17:11	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
17	14/08/2012	11:27:16	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
18	14/08/2012	11:28:28	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
19	14/08/2012	11:30:27	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
20	14/08/2012	11:38:59	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
21	14/08/2012	11:39:40	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
22	14/08/2012	11:41:19	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
23	14/08/2012	11:41:37	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
24	14/08/2012	11:44:23	00:00:00	CDR	Outgoing Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1
25	14/08/2012	11:52:47	00:00:00	CDR	Incoming Voice		07700900021	Unknown 3	35826712345645	234-10-12049-33417	234-10-1

A pop-up message is displayed stating your 'Phone Relationships - Summary' has been saved to your Case Outputs:



- Click the **Yes** button. i2 Analyst's Notepad launches.

The use of the i2 Analyst's notebook feature is captured in the CSAS case audit and is listed as an 'i2 Integration Lookup' function.

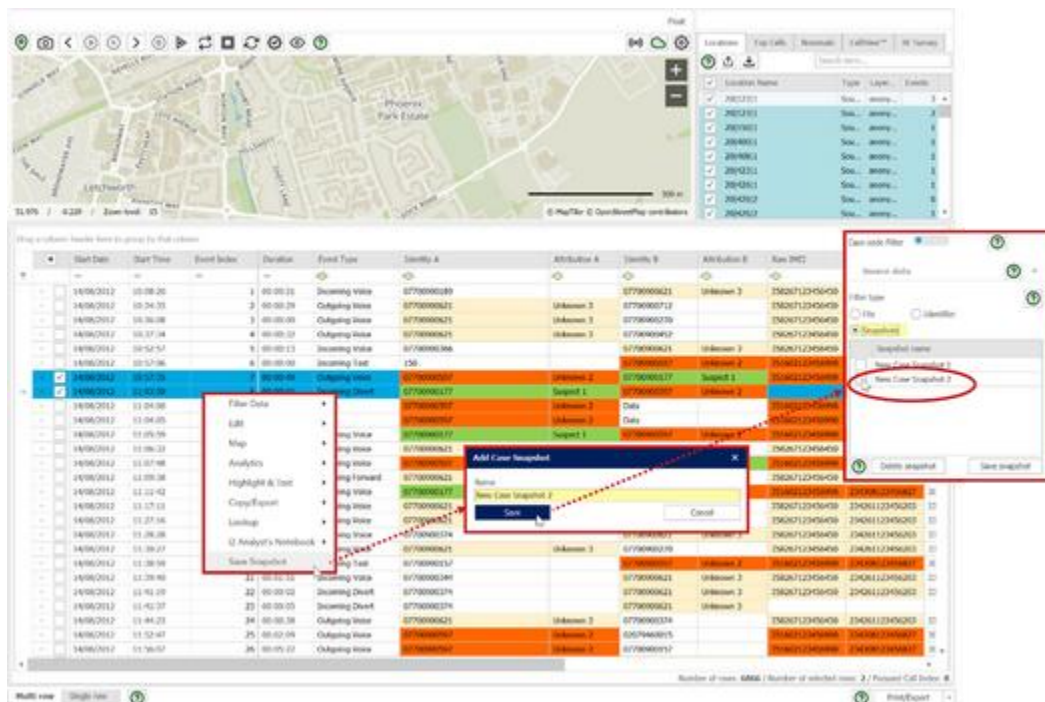
From the navigation sidebar, select 'Audit'. When the 'Audit' screen opens you will see audit details for each i2 Analysts Notebook instance:

Save Snapshot

This option allows you to save the selected rows in the grid as a new Case Snapshot.

Note: 'Save Snapshot' can be accessed from the 'Multi row' grid option only.

When selected, this function opens the 'Add Case Snapshot' pop-up window, from which you can enter a Name for the Snapshot and Save it:



Saved Snapshots are shown in the 'Source data' panel once you select the 'Snapshots' radio button.

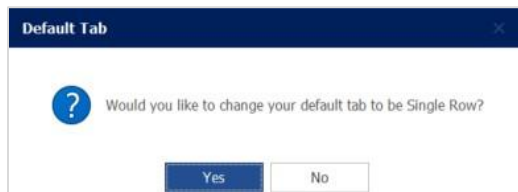
14.3.5 Changing Between Multi row and Single row Views

Call data can typically be presented within the Case Hub grid using two views:

- » Multi row – where each call record is presented on a separate row.
- » Single row – where each row in the grid has a 'calling' side and a 'called' side, allowing records for the same call/text between target phones (where there are two event records, one for the outgoing call and one for the incoming call) to be presented side by side on the same row.

The choice of Multi row or Single row view for a dataset has implications for things like call/event index numbering and the single row matching settings are therefore applied across a CSAS case, in Case Hub, Mapping and Case Outputs.

When you switch between Multi row and Single row views, a pop-up message box is displayed asking you to confirm your selection:



By confirming your selection you change the default grid view, so each time you open a case it will be displayed as Single row, and visa-versa depending upon your selection.

In **Multi row** view, each individual record is displayed on its own row in the grid or call schedule:

Event Index	Start Date	Start Time	Duration	Event Type	Identity A	Attribution A	Identity B	Attribution B	Raw IMEI	IMSI	Start Cell (Raw)	Start Site
1	29/08/2012	10:04:04	00:00:00	Incoming Text	07700900393		07700900177	Suspect 1	351602123456040	234308123456754	300481 e666	YATES HOR
2	29/08/2012	10:54:37	00:01:37	Incoming Voice	07700900999		07700900177	Suspect 1	351602123456040	234308123456754	300481 e666	YATES HOR
3	29/08/2012	11:14:00	00:09:38	Incoming Voice	07700900677		07700900177	Suspect 1	351602123456040	234308123456754	300481 3872	YATES HOR
4	29/08/2012	11:26:22	00:00:10	Incoming Voice	07700900621	Suspect 3	07700900177	Suspect 1	351602123456040	234308123456754	300481 3872	YATES HOR
5	29/08/2012	11:33:10	00:01:08	Incoming Voice	07700900621	Suspect 3	07700900177	Suspect 1	351602123456040	234308123456754	300481 3872	YATES HOR
6	29/08/2012	11:47:06	00:00:11	Outgoing Voice	07700900177	Suspect 1	07700900501		351602123456040	234308123456754	300481 3872	YATES HOR
7	29/08/2012	11:47:25	00:09:56	Outgoing Voice	07700900177	Suspect 1	07700900999		351602123456040	234308123456754	300481 3872	YATES HOR
8	29/08/2012	12:08:58	00:00:00	Incoming Text	249		07700900177	Suspect 1	351602123456040	234308123456754	300481 f0d9	LUPON HOR

This means that calls between subject phones, where both have outgoing and the incoming records, are displayed across two rows: one for the outgoing leg and one for the incoming leg. The same functionality is given when you send the selected grid data to a map, with the labels displaying as Multi row data.

In **Single row** view, each row presents the details of an entire connection, so both the outgoing and incoming records are shown together on the same row:

Event Index	Date	Time	Duration	File Type	Event Type	Is Intel	Calling No.	Attributed To	IMEI	Start Cell	End Cell	Comments
1	29/08/2012	10:04:04	00:00:00	CDR	Incoming Text		07700900393					
2	29/08/2012	10:54:37	00:01:37	CDR	Incoming Voice		07700900999					
3	29/08/2012	11:14:00	00:09:38	CDR	Incoming Voice		07700900677					
4	29/08/2012	11:26:22	00:00:10	CDR	Incoming Voice		07700900621	Suspect 3				
5	29/08/2012	11:33:10	00:01:08	CDR	Incoming Voice		07700900621	Suspect 3				
6	29/08/2012	11:47:06	00:00:11	CDR	Outgoing Voice		07700900177	Suspect 1	351602123456040	234-30-01153-14450	234-30-01153-14450	
7	29/08/2012	11:47:25	00:09:56	CDR	Outgoing Voice		07700900177	Suspect 1	351602123456040	234-30-01153-14450	234-30-02023-00968	
8	29/08/2012	12:08:58	00:00:00	CDR	Incoming Text		249					
9	29/08/2012	12:09:03	00:00:00	CDR	Incoming Text		249					

The rules used to combine qualifying records onto a single row are controlled by the *Settings sidebar > Singlerow Matching* filters. The settings options allow you to vary the methods used in Case Hub to detect events that should be paired and combined on the same row.

Note: Case Outputs also has both 'Multi row' and 'Single row' export templates available.

One possible consequence of switching between Multirow view and Singlerow view is that the event index numbers shown in the grid and in map labels might change.

For example, imagine a dataset contains 100 records; when displayed in Multirow view, those events will be numbered from 1 to 100. Further imagine that all calls/texts in the dataset are between subject phones, so the first two records, with index numbers 1 and 2, are a call between Subject phone 1 and Subject phone 2.

When Case Hub is switched to Singlerow view and if all of those records qualify for being merged onto a single row for each pair of records, the grid will only contain 50 rows. The first two records provide details of the same call, from phone 1 to phone 2, and so will be

merged into a single row with event index number 1. In the Case Hub map, the cell labels that detail that call, one for the outgoing phone and one for the incoming phone, will both show event index 1.

It is therefore not recommended to mix reports or maps created using both multirow view and singlerow view in the same case – to get consistent event numbering across all outputs in a case it is best to choose one view type and stick with it.

You can Print/Export from both grid views, see *Printing / Exporting*.

Who, When, Why

	This function is necessary to view some or all case data in a time ordered list, that can then be filtered and reviewed to display relevant case data.
	This function is undertaken whenever you have a need to view case data.
	This function is typically carried out by the following users: » CSAS User

14.4 Using Lookup in NMPR

14.4.1 Overview

NMPR (National Mobile Property Register) see www.thenmpr.com - is a service offered in selected countries by Recipero Ltd, who maintain a database for their customers of various items of property (mobile phones, bicycles, etc). If a registered item is stolen, the owner can report the loss to the NMPR database, along with any serial numbers or other identifying marks, which can then be used by the police to identify recovered stolen items. CSAS is currently only interested in NMPR records for mobile devices and performs lookups based on device IMEIs.

	Start Date	Start Time	Event Index	Timing Offset	Duration	Event Type
+	01/09/2021	15:05:52	2775	0	00:00:00	Outgoing Voice
+	01/09/2021	15:06:58			00:31	Outgoing Voice
+	01/09/2021	15:08:58			00:31	Incoming Voice
+	01/09/2021	15:09:41			00:21	Data
+	01/09/2021	15:09:58			14:53	Data
+	01/09/2021	15:22:54			10:30	Incoming Voice
+	01/09/2021	15:24:00			00:41	Outgoing Voice
+	01/09/2021	15:24:51			00:28	Data
+	01/09/2021	15:25:19			21:10	Data

Filter Data
 Edit
 Map
 Analytics
 Highlight & Text
 Copy/Export
 Lookup
 i2 Analyst's Notebook

Lookup in Google
 Lookup in NMPR

An NMPR lookup can be run directly from the Case Hub grid. In the Case Hub grid, select the required grid row or rows, right-click and from the drop-down menu select the 'Lookup in NMPR' option.

Note: By selecting 'Lookup in NMPR' you acknowledge that you and your organisation hold a valid licence and have permission to access NMPR data. The data provided by this NMPR Lookup function is supplied by Recipero Ltd under their terms & conditions and their acceptable use policy, which can be viewed at: <https://recipero.com/aup>. Forensic Analytics Ltd take no responsibility for the accuracy of the data returned by this lookup feature or for any consequences arising from the use or otherwise of that data.

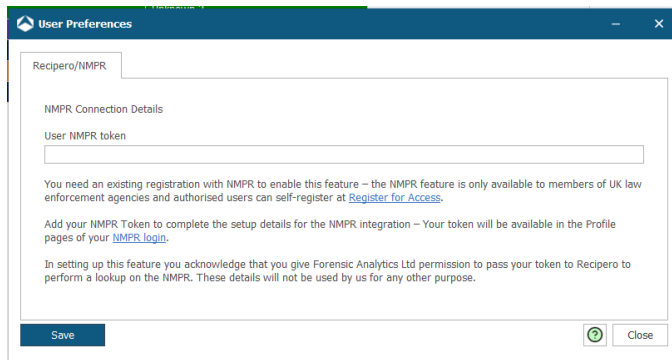
Note: By setting up this feature you acknowledge that you give Forensic Analytics Ltd permission to pass your token to Recipero Ltd to perform a lookup on the NMPR. These details will not be used by us for any other purpose.

Note: By setting up this feature you acknowledge that your organisation permits you to undertake NMPR Lookups and to make use of any data obtained from those lookups.

Selecting 'Lookup in NMPR' opens the 'NMPR Lookup' window from which you can see records where Identifiers are known to the database, however, you must first setup the NMPR feature.

14.4.2 Setting Up the NMPR Feature

If you select 'Lookup in NMPR' and you have not yet set up this feature in CSAS, the following pop-up window opens:



The 'User Preferences' window displays the 'Recipro/NMPR' tab. Under 'NMPR Connection Details', there is a text field for 'User NMPR token'. Below the field, a message states: 'You need an existing registration with NMPR to enable this feature -- the NMPR feature is only available to members of UK law enforcement agencies and authorised users can self-register at [Register for Access](#). Add your NMPR Token to complete the setup details for the NMPR integration -- Your token will be available in the Profile pages of your [NMPR login](#). In setting up this feature you acknowledge that you give Forensic Analytics Ltd permission to pass your token to Recipro to perform a lookup on the NMPR. These details will not be used by us for any other purpose.' At the bottom, there are 'Save' and 'Close' buttons.

Note: You must have your valid NMPR Token code available to set this feature up in CSAS. This is available in the Profile pages of your NMPR login.

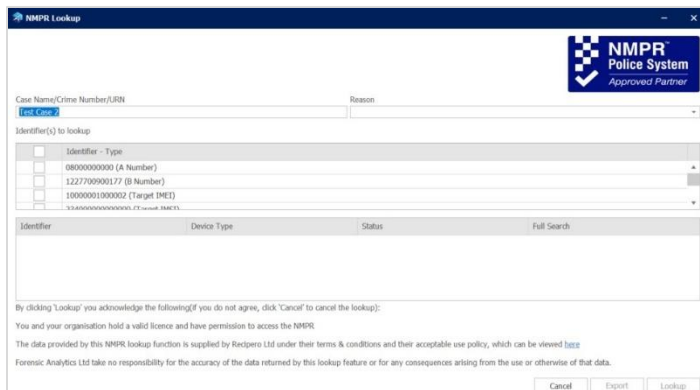
To complete the setup, enter or paste your NMPR Token code into the text field then click the **Save** button. A pop-up message opens stating your NMPR token has been saved:



Note: If the 'Lookup NMPR' feature is not successful, check that your NMPR registration is valid with NMPR support and if it is, contact CSAS Support. CSAS Support cannot help with expired or invalid NMPR tokens.

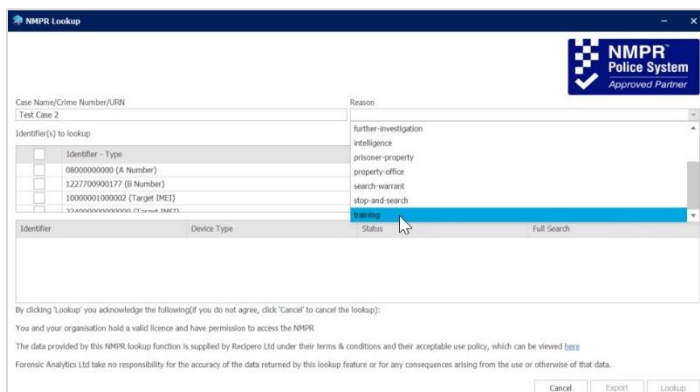
14.4.3 Launching an NMPR Lookup

If you select 'Lookup in NMPR', and you have correctly set up this feature in CSAS, the following pop-up window opens:



The NMPR Lookup window is displayed. It features a header with the NMPR Police System logo and 'Approved Partner' status. The main form includes fields for 'Case Name/Crime Number/URN' (containing 'Test Case 2') and 'Reason' (a dropdown menu). Below these is a section for 'Identifier(s) to lookup' with a table of checkboxes and identifier types: 'Identifier - Type', '08000000000 (A Number)', '122770000177 (B Number)', '10000001000002 (Target IMEI)', and '33440000000000000000 (Target IMSI)'. A table below this lists identifiers, device types, and statuses. At the bottom, there is a disclaimer and a 'Lookup' button.

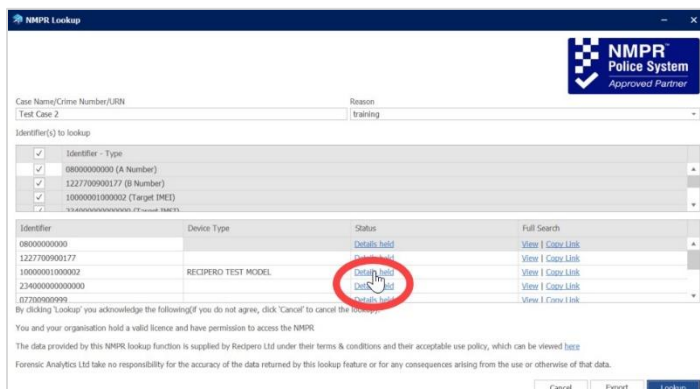
The pop-up window is automatically populated with the 'Case Name/Crime Number/URN', using the name of the current CSAS case, however, you must also enter a 'Reason' for conducting the lookup from the drop-down menu for doing the NMPR search:



The NMPR Lookup window is shown with the 'Reason' dropdown menu open. The menu lists several options: 'further investigation', 'intelligence', 'private property', 'property office', 'search warrant', 'stop-and-search', and 'training'. The 'training' option is highlighted. The 'Identifier(s) to lookup' section remains empty.

When you select a Reason, the 'Identifier(s) to lookup' grid automatically populates, based on the data contained in the selected rows in the Case Hub grid. Using the checkboxes you can select the Identifier you want to look up, for example, 'Target IMEI / IMSI', 'A Number' or 'B Number' etc. Lookups tend to be most successful for IMEIs.

Click the **Lookup** button and the results grid populates.

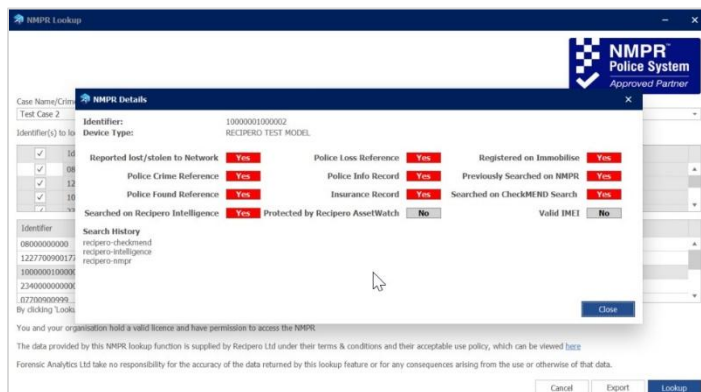


The NMPR Lookup window is shown with the 'Reason' set to 'training'. The 'Identifier(s) to lookup' section is now populated with a table of identifiers, device types, and statuses. The 'Status' column is circled in red. The 'Lookup' button is highlighted in blue.

Identifier	Device Type	Status	Full Search
08000000000		Details held	View Copy Link
122770000177		Details held	View Copy Link
10000001000002	RECIPERO TEST MODEL	Details held	View Copy Link
23460000000000		Details held	View Copy Link
07200000000		Details held	View Copy Link

If an IMEI was selected for the lookup, the Device Type field may contain details of the phone or device type, showing the manufacturer and model.

If other information is held for the selected Identifier(s), under the 'Status' column, a blue 'Details held' hyperlink is displayed. Click the hyperlink to open the 'NMPR Details' window:



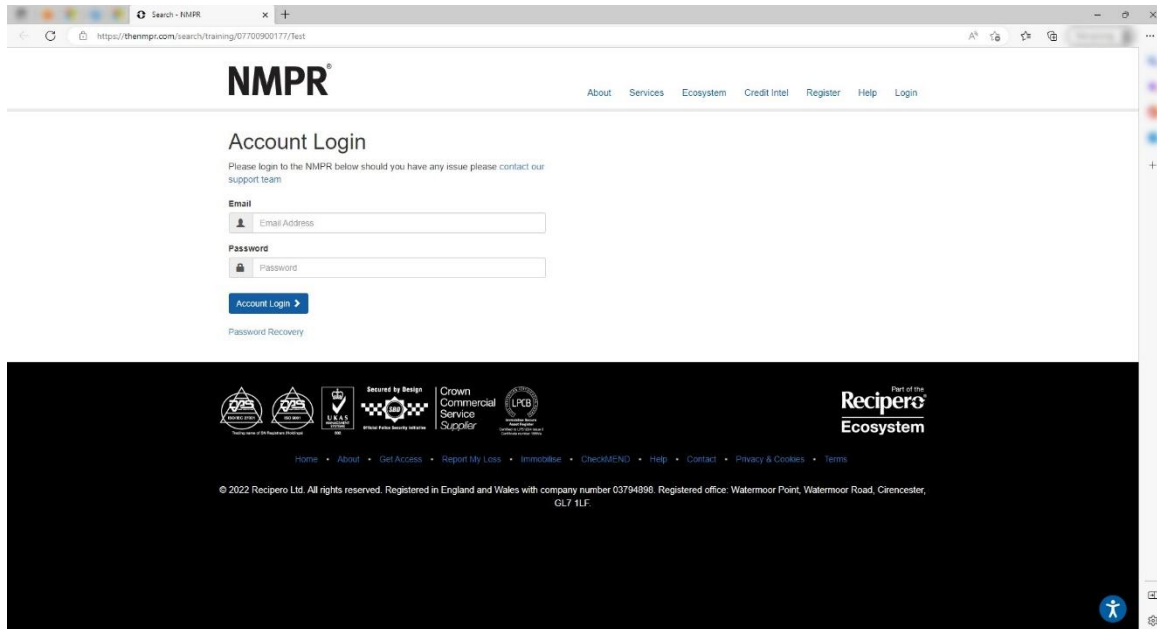
The NMPR Details popup mirrors the abbreviated details provided on the NMPR website and shows the status for the selected identifier for each of the fields maintained by NMPR, these include:

- » Reported lost/stolen to network – the handset has been reported as lost/stolen to the user's network operator
- » Police Crime Reference – a crime ref has been issued in relation to the loss/theft of the device, which may provide more details about it or its user
- » Police Found Reference – indicates that the device has been previously found by police and may be in police possession
- » Searched on Recipero Intelligence – the identifier has previously been searched for on another Recipero database
- » Police Loss Reference – device has previously been reported as lost to police
- » Police Info Record – details of the identifier have appeared in a police report, which may provide more details about it or its user
- » Insurance Record – a record of an insurance claim related to the device exists
- » Protected by Recipero AssetWatch – device has been registered with another Recipero service
- » Registered on Immobilise - device has been registered with another Recipero service
- » Previously searched on NMPR – identifier has been searched for previously on NMPR – details of previous searches may be shown at the bottom of the popup
- » Searched on CheckMEND search - identifier has been searched for previously on another Recipero service

» Valid IMEI – the lookup has returned a make/model for an IMEI search

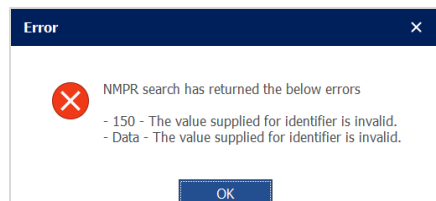
When a successful search is complete, you can also select the 'View' and 'Copy Link' hyperlinks under the 'Full Search' column in the grid:

» 'View' – opens the NMPR 'Account Login' page, you can login and review the full search data on the Recipero site.



» 'Copy Link' – copies a web link for the Recipero 'Account Login' page which you can paste into your web browser.

If the search fails, an 'Error' pop-up window is displayed:

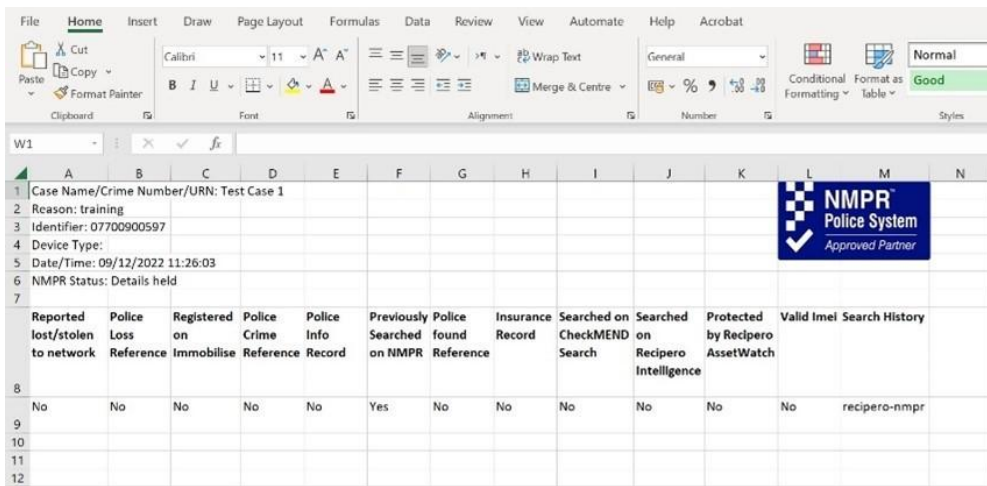


To cancel an NMPR lookup, click the **Cancel** button anytime.

14.4.4 Exporting NMPR Lookup Results

You can export the NMPR search results to Excel. Click on the **Export** button.

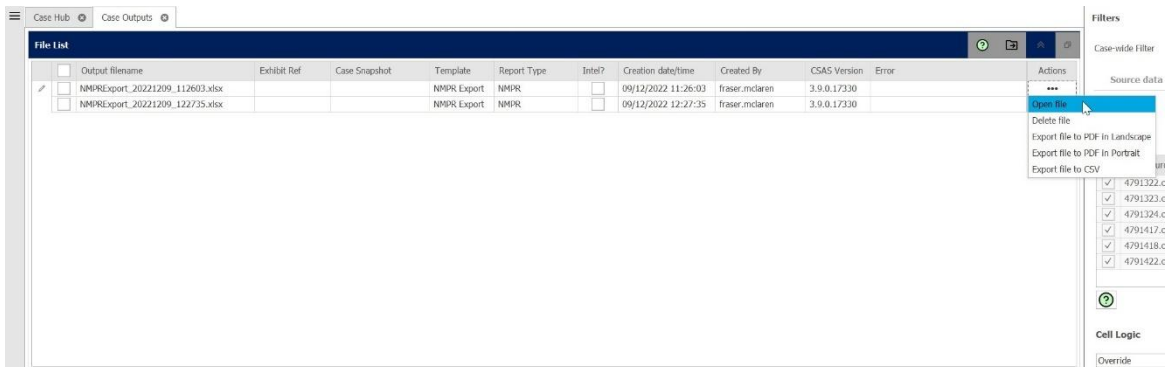
Your Excel report opens for further evaluation:



Reported lost/stolen to network	Police Loss Reference	Registered on Immobilise	Police Crime Reference	Police Info Record	Previously Searched on NMPR	Police found Reference	Insurance Record	Searched on CheckMEND Search	Searched on Recipero Intelligence	Protected by Recipero AssetWatch	Valid Imei	Search History
No	No	No	No	No	Yes	No	No	No	No	No	No	recipero-nmpr

14.4.5 NMPR Data Exports in Case Outputs

When you export the NMPR search results to Excel, the exported file is also displayed in 'Case Outputs', in the 'File List' grid:



Output filename	Exhibit Ref	Case Snapshot	Template	Report Type	Intel?	Creation date/time	Created By	CSAS Version	Error	Actions
NMPRExport_20221209_112603.xlsx			NMPR Export	NMPR		09/12/2022 11:26:03	fraser.mclaren	3.0.0.17130		...
NMPRExport_20221209_122735.xlsx			NMPR Export	NMPR		09/12/2022 12:27:35	fraser.mclaren	3.0.0.17130		...

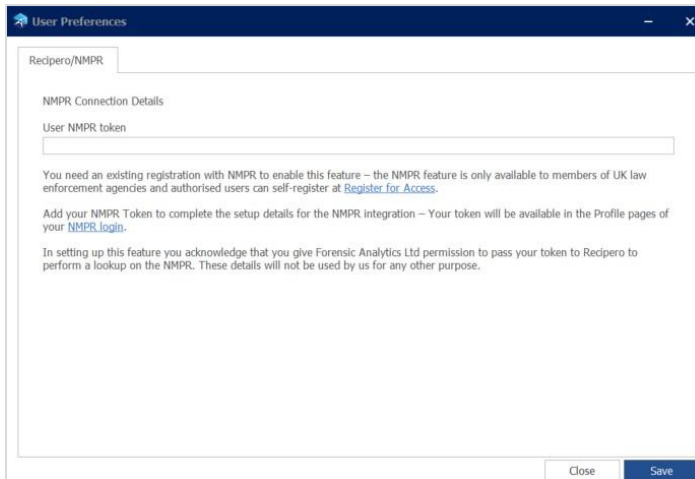
Clicking on 'Actions' opens a drop-down menu from which you can select the necessary action for the output.

Who, When, Why

	This function is necessary to configure CSAS and search NMPR data for records where phones are known to the database.
	This function is undertaken whenever you have a need to view details for an IMEI
	This function is typically carried out by the following users: >> CSAS User

Stepped Procedure

1. Setup the NMPR Lookup function. Go to 'Configuration' > 'User Preferences', the 'User Preferences' pop-up window opens:



User Preferences

Recipro/NMPR

NMPR Connection Details

User NMPR token

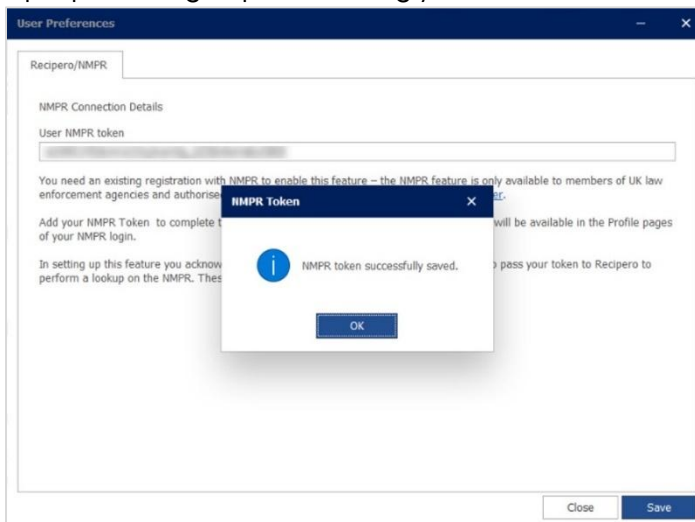
You need an existing registration with NMPR to enable this feature – the NMPR feature is only available to members of UK law enforcement agencies and authorised users can self-register at [Register for Access](#).

Add your NMPR Token to complete the setup details for the NMPR integration – Your token will be available in the Profile pages of your [NMPR login](#).

In setting up this feature you acknowledge that you give Forensic Analytics Ltd permission to pass your token to Recipro to perform a lookup on the NMPR. These details will not be used by us for any other purpose.

Close Save

2. Enter your NMPR Token code into the text field then click the **Save** button. A pop-up message opens stating your NMPR token has been saved:



User Preferences

Recipro/NMPR

NMPR Connection Details

User NMPR token

You need an existing registration with NMPR to enable this feature – the NMPR feature is only available to members of UK law enforcement agencies and authorised users can self-register at [Register for Access](#).

Add your NMPR Token to complete the setup details for the NMPR integration – Your token will be available in the Profile pages of your [NMPR login](#).

In setting up this feature you acknowledge that you give Forensic Analytics Ltd permission to pass your token to Recipro to perform a lookup on the NMPR. These details will not be used by us for any other purpose.

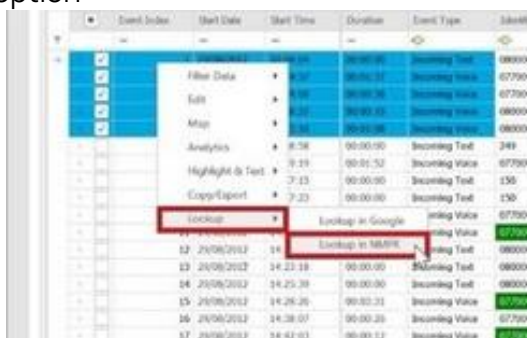
NMPR Token

NMPR token successfully saved.

OK

Close Save

3. Go to 'Case Hub' and load CDR files into the data grid. Select the necessary grid row then do a right-click and from the drop-down menu select the 'Lookup in NMPR' option:

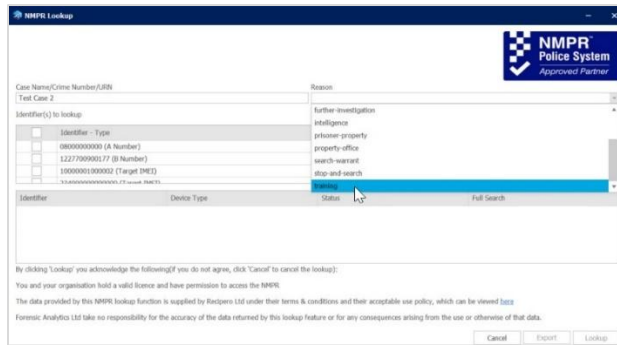


Event Index	Start Date	Start Time	Duration	Event Type	Identify
12	20/09/2012	14:22:18	00:00:00	Recording Value	0000000
13	20/09/2012	14:23:19	00:00:00	Recording Value	0000000
14	20/09/2012	14:25:39	00:00:00	Recording Value	0000000
15	20/09/2012	14:26:26	00:00:00	Recording Value	0000000
16	20/09/2012	14:28:07	00:00:00	Recording Value	0000000
17	20/09/2012	14:42:03	00:00:00	Recording Value	0000000

Context menu options: Filter Data, Edit, Map, Analytics, Highlight & Text, Copy/Export, **Lookup**, Lookup in Google, **Lookup in NMPR**.

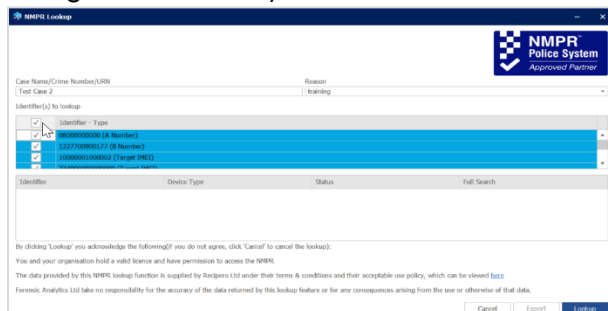
The 'NMPR Lookup' window opens and is automatically populated with the 'Case Name/Crime Number/URN'.

4. From the 'NMPR Lookup' window, in the 'Reason' field, select from the drop-down menu a Reason for doing the search:

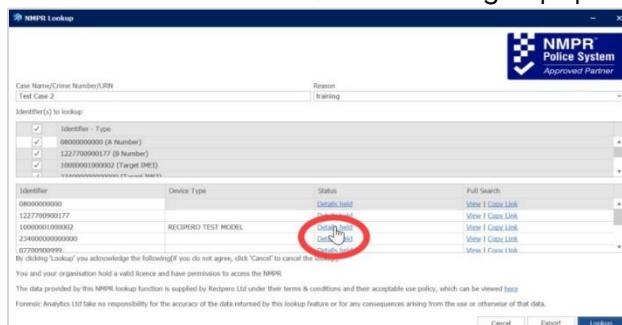


The 'Identifier(s) to lookup' grid automatically populates.

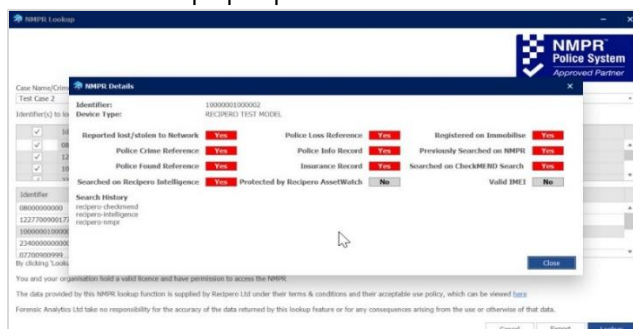
- From the 'Identifier(s) to lookup' grid, select the Identifier you want to look up by ticking the necessary checkboxes.



- Click the **Lookup** button, the results grid populates:



- If information is held for the selected Identifier, under the 'Status' column, a blue 'Details held' hyperlink is displayed. Click the necessary hyperlink to open the 'NMPR Details' pop-up window:



- Export the search results as necessary.
- Close the 'NMPR Lookup' window.

14.5 Using Lookup in CSAS Cases

Lookup in CSAS Cases is another way to access the [Cross Case Search](#) functionality available from the top header bar of the CSAS application.

To use Lookup in CSAS Cases from Case Hub in Multi row view, first select the rows with identifiers that you wish to search for.

Once a row is selected in Case Hub, right click and select Lookup -> Lookup in CSAS Cases. Users are then presented with a list of identifiers that can be searched for.

For example, when the following row is selected, it is possible to select up to four identifiers to search for across all cases to which the user has access.

Start Date	Start Time	Duration	Event Type	Identity A	Attribution A	Identity B	Attribution B	Raw IMEI	IMSI
04/08/2017	09:33:39	00:01:33	Incoming Voice	07700904219		07700907268	Unknown 7	356767700907310	234267700905592

Select identifiers to search

Identifier(s) to search

	Identifier Type	Nominal
☐	234267700905592 (Target IMSI)	
☐	356767700907310 (Target IMEI)	
☐	07700904219 (A Number)	
☐	07700907268 (B Number)	Unknown 7

4 search criteria rows

0 selected items

Search

Cancel

It is recommended to limit the number of identifiers used in each search, allowing more specific searches that can be executed more quickly.

Once one or more identifiers have been selected, use the Search button to execute the search. Results are returned as described in [Cross Case Search](#).

By selecting a case in the results grid, users can copy the attribution from that case into the current case by clicking "Copy attribution to this case". This process follows the process described in [Importing Attributions](#).

When attributions are imported into a case in this way, the source for the attribution is the name of the original case and will be shown as in the following example:

Source 

14.6 Using Mapping

The Case Hub mapping feature provides an opportunity to view the data in a case from a geographical perspective and the visualise the proximity or otherwise of key case events and locations to each other.

14.6.1 Map Controls

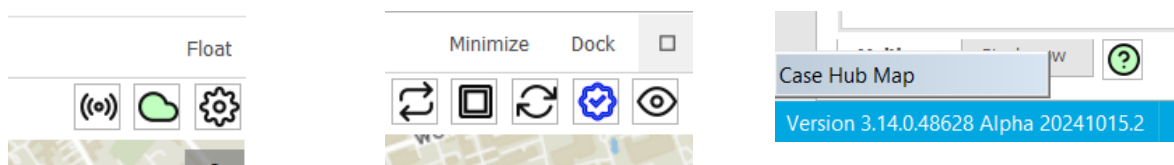
At the top of the map there is a ribbon hosting a set of map action buttons:



-  **Map source** – shows the current map source type (online or offline).
-  **Screengrab** – take a screengrab of the whole map panel and save it.
-  **Move back** – animation control that manually steps the sequence back by one event.
-  **Pause Animation** – animation control that pauses the event playback.
-  **Move Next** – animation control that manually steps forward by one event.
-  **Stop Animation** – animation control that stops event playback.
-  **Play and Record** – animation control that records the sequence as an mp4 file.
-  **Return to view** – returns the map to the frozen zoom level and framed areas previously set.
-  **Freeze View** – sets a frozen view to allow the map to be returned to exactly the same position later.
-  **Manual sync** – manually triggers the map to sync with the grid.
-  **Auto sync** – toggles the auto-syncing of the map and grid and grid on and off.
-  **Auto zoom and pan** – toggles the auto-zoom and pan feature on and off.
-  Displays mapping hints and tips.
-  **Open GPS Settings Window** – opens the 'GPS Receiver Settings' pop-up window. See *Using Live GPS Import*.
-  **Map type** – toggles between 'road' and 'aerial' map types.
-  **Settings** – opens the map settings pop-up window.

Floating & Docking Map Panel

Many CSAS have a two screen setup on their PC allowing – CSAS supports dual screen setups and allows the map panel to be floated away from Case Hub so it can be dragged to a second screen.



To float the map panel, click the 'float' button at the top right of the panel.

The map panel will pop out of the Case Hub screen and can be dragged to the second screen. If you need to minimise the floating map panel, click the 'minimize' button, The panel will be hidden, but can be maximised again by clicking on the 'Case Hub Map' button that appears at the bottom left of the main CSAS screen.

To reintegrate the map back into Case Hub, click 'dock'.

14.6.2 Map Settings

Clicking on the  button opens the 'Map Settings' pop-up window:

From the 'Settings' pop-up window you can select the following tabs:

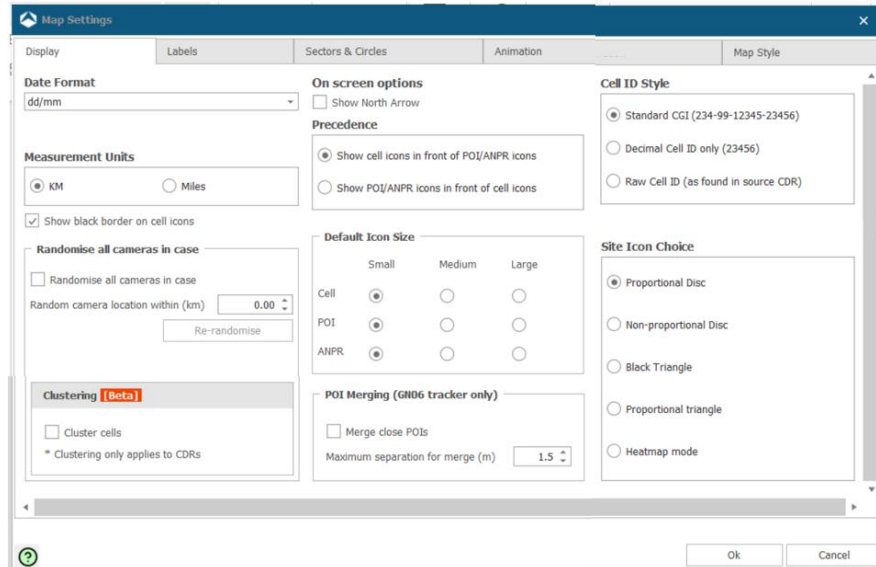
» Display

- » Labels
- » Sectors & Circles
- » Animation
- » Map Style

Any settings you elect to change get saved and become your new preference.

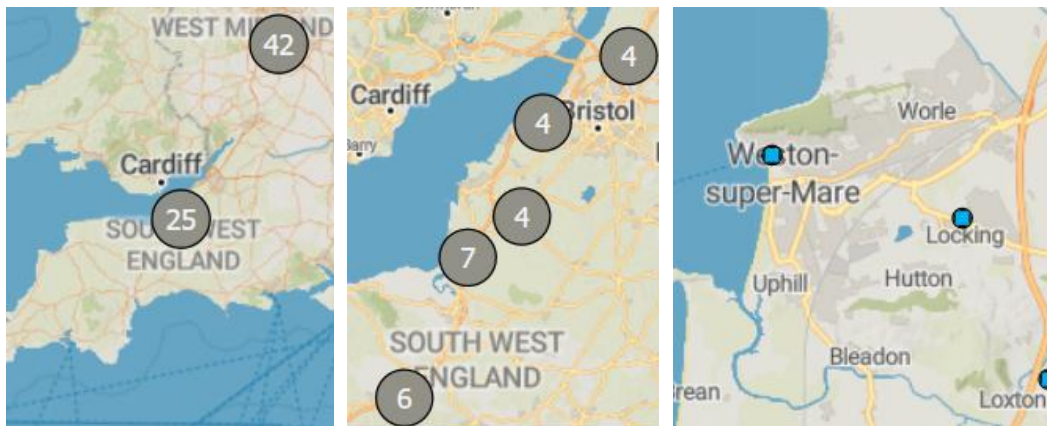
Display

Clicking on the 'Display' tab allows you to select from the following drop-down menus and checkboxes:



- » **Date Format** – changes the date format used in the popup map labels – the default is 'dd/mm' but other options are available.
- » **Measurement Units** – switches the map measurement units between miles and kilometres. The default is km.
- » **Show black border on cell icons** – ticking this checkbox forces a black outline to be drawn around each cell site icon, when disabled the icon is just filled in with the selected attribution colour with no outline. Enabled by default.
- » **Randomise all cameras in case** - controls the settings used for the randomisation of ANPR camera locations on the map. You can force all cameras to be shown in a randomised location and control the distance within which the randomisation takes place. For example, if it is set to 1km, each camera will be shown in a random location within 1km of its true location. Disabled by default.
- » **Clustering (beta)** – this option is in beta and is included for testing purposes only. When enabled, the feature clusters geographically close cell site icons and represents them with a count label. For example, if there were 25 cell sites in the same region shown on the map, with clustering enabled, when the map was zoomed out higher than zoom level 11, the sites would be clustered not one icon with a count of 25. When the map zooms in, the clusters are broken up into smaller units and below zoom level 11, the individual cell site icons are

displayed.



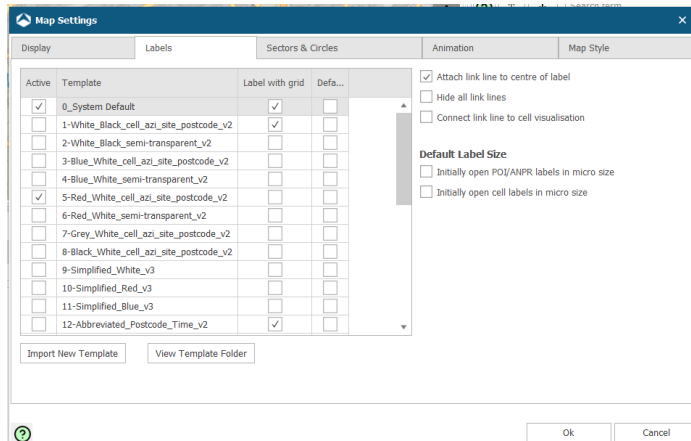
The intention is to make busy maps faster to load and more responsive to navigate. The beta version of the feature has been included to permit further testing and development and defaults to being disabled.

- » **Show North Arrow** – controls whether the north arrow icon is added to the map. Disabled by default.
- » **Precedence** – controls whether cell sites are shown in front of ANPR/POI icons (the default option) or vice versa.
- » **Default Icon Size** – sets the default size for each type of map icon. All default to small.
- » **POI Merging (GN06 tracker only)** – controls whether separate events (from a GN06 locations & events rescue template) linked to separate map coordinates that are very close to each other should be treated as being at the same location. The default tolerance for 'very close to each other' is 1.5m, but this can be altered.
- » **Cell ID Style** - allows you to select the format that cell IDs will be displayed in, with options of 'raw', 'decimal' and 'CGI'. CGI is the default.
- » **Site Icon Choice** – selects the default cell site icon style, with 'proportional disc' being the default.

You can confirm your selection by clicking on the button. The 'Map Settings' pop-up window closes and the map panel adjusts in accordance your selected settings.

Labels

Clicking on the 'Labels' tab allows you to select from the following checkboxes:



The main feature of this tab is the ability to choose the map label style to be used. The grid lists all loaded styles.

Select a map label template to use by clicking on the required checkbox in the Active column – when you then click OK the active label style will change.

If you want the selected label style to automatically open the event table part of the map label, tick the 'Label with grid' option for the required template.

If you wish to change the default map label style, tick the checkbox in the Default column for the required style.

The **Import New Template** button opens a Windows file dialogue that will help you find and import new map label templates that you have saved somewhere on your PC.

The **View Template Folder** opens the templates in Windows file explorer, so templates can be added, removed or edited.

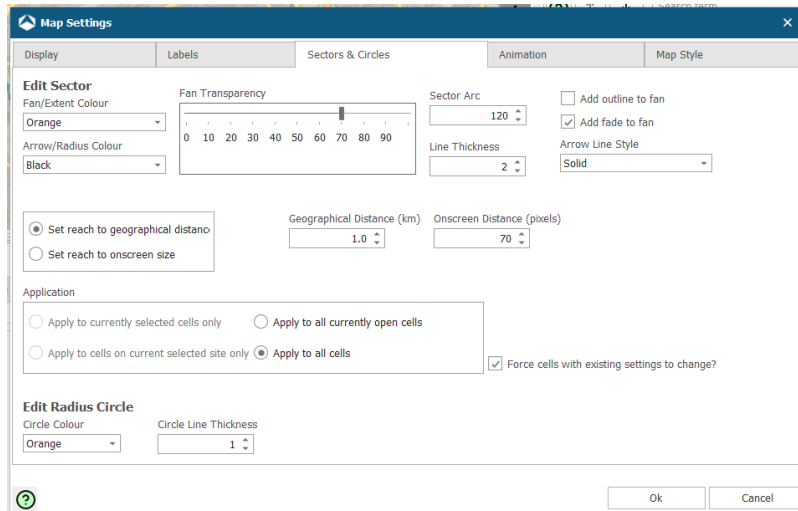
Other options on this tab are:

- » **Attach link line to centre of label** - when enabled the link line connects to the label at the top centre. When disabled it connects to the top left.
- » **Hide all link lines** – the link lines are forced into transparent mode and are effectively hidden on the map. Individual link lines can be toggled on or off using the control menu in the specific label.
- » **Connect link line to cell visualisation** – when enabled, the far end of the link line will connect to the centre of the cell coverage visualisation (fan, extent, arrow), when disabled the link line connects directly to the cell site icon.
- » **Default Label Size** – this controls the default size that cell and ANPR/POI labels are opened at – the options being 'micro' size (which have just one row of information in them) or regular sized labels.

You can confirm your selection by clicking on the **Ok** button. The 'Map Settings' pop-up window closes, and the map adjusts in accordance your selected settings.

Sectors & Circles

Clicking on the 'Sectors & Circles' tab allows you to select from the following drop-down menus and checkboxes:



- » **Fan/Extent colour** – changes the colour choice for the 'fan' and 'extent' cell visualisation options.
- » **Fan Transparency** – changes the transparency applied to the sector fan option.
- » **Sector arc** – sets the arc applied to the sector fan or extent options with a default value of 120°.
- » **Add outline to fan** – when ticked, adds a border outline to the fan.
- » **Add fade to fan** – when ticked, applies a fade to the fan image. This is a gradual fade to transparency, starting as opaque next to the cell site icon and fading to transparent at the edges of the fan. The effect is designed to indicate the gradual loss of power for a transmitted signal as it travels further from the cell site.
- » **Arrow/Radius colour** – changes the colour choice for the arrow or radius options.
- » **Line Thickness** – changes the line weight for the arrow/radius options.
- » **Line Style** – allows the line style for azimuth arrows to be solid or dashed.
- » **Visualisation size** – this option allows you to control the sizing of cell visualisations on screen. You can select either 'Set reach to geographical distance' or 'Set reach to onscreen size'. When selecting 'Set reach to geographical distance' the image is set to a particular size (defaults to 1km) and therefore expands or contracts on-screen as the map is zoomed in or out. When selecting 'Set reach to onscreen size' the image is set to a fixed onscreen size that stays the same when the map is zoomed in or out:
 - **Geographical Distance** – allows the geographical size of the image to be set (defaults to 1km).

- **Onscreen Distance'** – allows the fixed onscreen size to be set (defaults to 70 pixels, so the size may appear to vary on different resolution screens).

» **Application** – controls how the changed settings are applied with the following options:

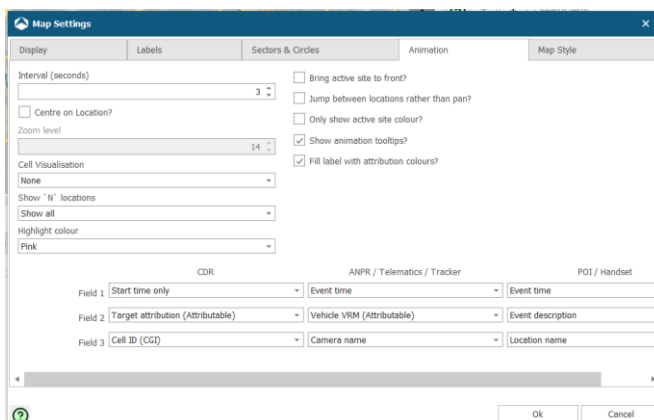
- 'Apply to currently selected cell only' – only applies the selected changes to the cell that was active when the settings control was accessed (this option only applies if you accessed the Settings control from the cell icon right click menu).
- 'Apply to cells on the currently selected site only' – applies the changes to all cells on the site that was active when the settings control was accessed (this option also only applies if you accessed the Settings control from the cell icon right click menu).
- 'Apply to all currently open cells' – applies the changes to all cells in the map that currently have a cell visualisation open.
- 'Apply to all cells' – applies the changes to all cells in the case, whether they are selected, open or otherwise
- You also have the option to force the new settings to apply to any cells in the case that currently have other settings. This is the way to change the default options for all cells.

» **Edit Radius Circle** – this allows the radius circles displayed for ping and point locations to be managed – the circle colour and the circle line thickness (in font points) can be selected and saved.

You can confirm your selection by clicking on the button. The 'Map Settings' pop-up window closes, and the map tile will adjust in accordance your selected settings.

Animation

Clicking on the 'Animation' tab allows you to set your map animation preferences:



» **Interval (seconds)** – sets the playback interval between events, with a minimum interval of 1 second, although the cell coverage and other animation features only work when the interval is 3 seconds or higher.

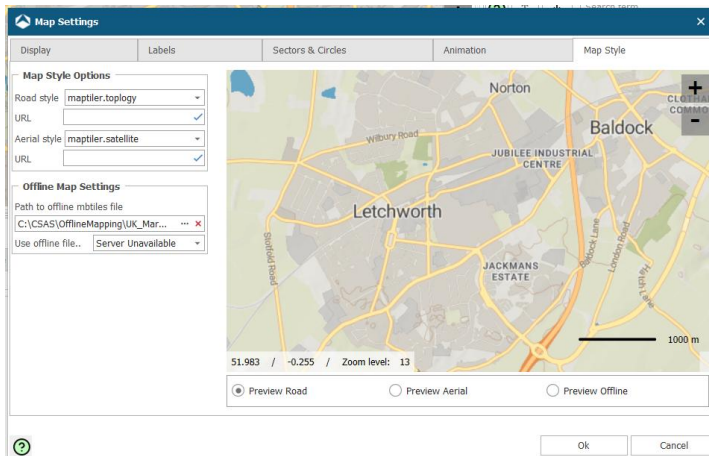
- » **Centre on Location?** – when enabled, the map moves to recentre on each new location. When disabled, the map stays static in its starting position, even if a location is off the edge of the map.
- » **Zoom level** – when enabled, this option zooms the map to the required zoom level at the start of the animation. This could allow you to start the animation with an overall view of the whole dataset and then zoom in to each individual location when the animation starts. This feature only works if the 'centre on location' option is enabled.
- » **Cell Visualisation** – when enabled, this option activates the selected cell coverage visualisation (fan, arms, arrow) for each cell as each event is shown.
- » **Show 'N' locations** – when enabled, this setting allows you to control the number of locations that are seen on screen at any one time. When 'Show All' is selected, all cell sites within the set to be animated will remain onscreen at all times, just being highlighted as a site is being used. If one of the numerical options in the drop-down menu is selected when configuring an animation, the system will hide all sites at the start of the animated sequence and will build them up as the animation progresses. The feature allows users to control the number of sites seen onscreen at once, using the values in the drop-down menu, only the current site and the last N sites will be shown together (where N = 1 to 10), meaning that as the animation builds up 'old' sites are hidden as each 'new' site appears – this can make for a more focused and less confusing animation.
- » **Highlight colour** – during the animation, CSAS will put an outline around the current active location (cell site, POI location, ANPR camera), this control sets the default colour for the highlight.
- » **Bring active site to front?** – when enabled, promotes the current active site to the 'front' of the stack of icons on the map, so that it is visible in the event that several icons are overlapping.
- » **Jump between locations rather than pan?** – when enabled, this setting causes the map to jump abruptly from one location to the next. When disabled, the map scrolls between the locations. This setting would be enabled in cases where the scrolling movement is causing map performance or rendering issues, such as might be experienced with a map containing large amounts of data.
- » **Only show active site colour?** – sites that have been used by several phones in the sequence can be partitioned to show the various phone's colours. During an animation, it can be difficult to quickly understand which phone was activate for a given call if the site is showing multiple colours. Enabling this option makes the map change the site icon momentarily to show just the currently active phone's colour.
- » **Show animation tooltips?** – this controls whether a tooltip label is shown alongside each location as it activates during the sequence.

- » **Fill label with attribution colours?** – if enabled, CSAS will fill the animation tooltip label with the appropriate attribution colours for fields such as 'calling number' and 'calling attribution'.
- » **Tooltip label field choices** – these settings allow you to choose the contents of the animation tooltip labels. There are three label styles (for CDRs, ANPR and POI events) and each label has up to three fields. You can choose the fields you want to view in each type of label.

You can confirm your selection by clicking on the button. The 'Map Settings' pop-up window closes, and the map tile will adjust in accordance your selected settings.

Map Styles

Clicking on the 'Map Style' tab allows you to select different map styles to use in mapping, with options to set the style to be used for maps, aerial views and offline mapping.



- » **Map Style Options** – this section selects the 'online' map styles to be used for both 'map' and 'aerial' types. The dropdowns for each type offer multiple map styles to choose from.
- » **Offline Map Settings** – this section offers the ability to select an offline map file (which can be downloaded from the CSAS Support site and must be saved locally on your PC). Offline maps allow mapping to continue to be used even if you're not online.

Map Style Options

CSAS mapping has three predefined online map style providers – Mapbox, Maptiler and Ordnance Survey. Mapbox and Maptiler styles offer global coverage, Ordnance Survey offers coverage of Great Britain (England, Wales and Scotland) only.

To change Road and/or Aerial map styles, simply select a new style from the dropdowns and click OK. The preview window displays the current selected type. The choice you make changes the current map and also changes your default choice for future maps.

If you don't want to use one of the preselected map styles and have an alternative map source or map server to connect to, it's possible to add a URL to connect to a custom map source instead – this can be added to the 'URL' box below the Road and Aerial style

dropdowns. Please contact CSAS Support for advice on the required format for the URL and the types of mapping server CSAS can interact with.

Offline Map Settings

CSAS supports the option of downloading one or more 'offline' map files, that can continue to provide map background details even if you are not connected to the Internet. Various offline map files are available from the CSAS Support type and custom files, covering specific countries or regions, can be created on request.

Once an offline map file has been downloaded, CSAS can be configured to use it by clicking on the three dots in the 'path to offline mbtiles file' box and then selecting the required file via Windows file explorer.

The control also captures your preference for when offline mapping should be used, with choices of:

- » **Server unavailable** – offline maps are only used if CSAS can't connect to the selected online source.
- » **If present** – CSAS prefers to use offline mapping if an offline map file has been selected.
- » **Always** – CSAS will always use offline mapping and will not attempt to use online maps.
- » **Never** – CSAS will never attempt to use offline mapping and will always use online maps.

You can confirm your selection by clicking on the button. The 'Map Settings' pop-up window closes, and the map tile will adjust in accordance your selected settings.

14.6.3 Viewing Data

The map panel is used to visualize the current dataset and can be synced to the Case Hub grid. Select the data you wish to view from the 'source files' list in the Filters sidebar and click 'Apply'.

If the 'auto-sync' button  (in the ribbon at the top of the map panel) is not activated, then the map will not automatically display the selected data, in which case you'll need to activate auto-sync or click on the 'manual sync' button  in the ribbon to force the map to update. The auto-sync feature is very useful but can lead to performance issues when used with very large maps.

Maps can be zoomed and panned to ensure that the required area is shown in the correct level of details.

Right-click menus within the map (connected to the map background and to the cell, POI and ANPR icons) provide a set of additional controls.

A 'marquee select' feature allows you 'click, hold and drag' anywhere on the map to instruct it to zoom in to the selected area.

Maps can be saved (as part of a Case Snapshot). The contents of a map can be captured as a screengrab and the map can be output to Powerpoint to use as part of an exhibit or presentation.

UK Mapping Disclaimer

The UK easting/northing coordinate system known as BNG (British National Grid), is based on a coordinate system called OSGB36. Most modern mapping products (CSAS Mapping, OpenStreetMap, Google, Bing, etc) are designed to work with GPS coordinates, which based on a coordinate system called WGS84. The OSGB36 and WGS84 models are slightly different shapes and sizes, which means that coordinates created for one system don't map exactly (without conversion) to the other.

If BNG (easting/northing) coordinates are converted directly to lat/long coordinates by an OSGB36-based system without correcting for the difference but are then displayed on a WGS84-based map (e.g. CSAS Mapping), a deviation of around 50-120m is introduced. OSGB lat/longs displayed on an OSGB-based map (e.g. ESRI ArcGIS) will not be affected by this deviation and will be placed correctly.

UK CSPs like Vodafone and Three include both BNG and lat/long coordinates in their disclosed cell location data. It is best to map this data by BNG (easting/northing) if using a WGS84-based mapping tool like CSAS to avoid cell sites being shown in the wrong location.

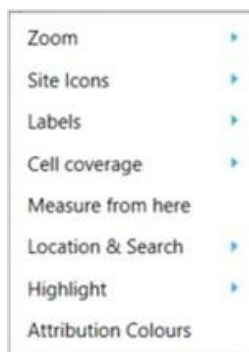
14.6.4 Right-click Menus

CSAS maps include a powerful set of right-click menus to provide further 'in map' controls and options, there are slightly different menus displayed when you right-click on the map background and on cell, POI and ANPR icons.

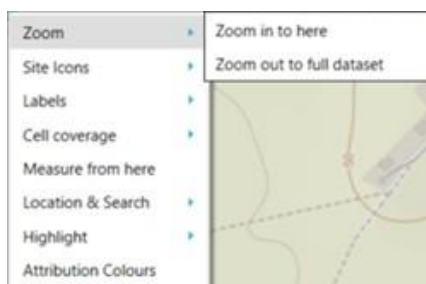
Cell Site Right-click

To open the 'Cell Site' drop-down menu, right-click on a cell site icon. The drop-down

gives you the following options:



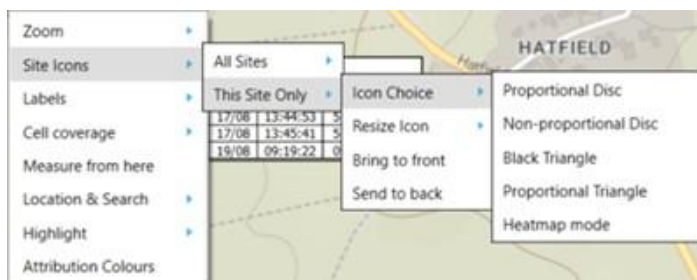
The details of each option are as follows:



'Zoom' – allows you to zoom in and out of the cell site on the map.

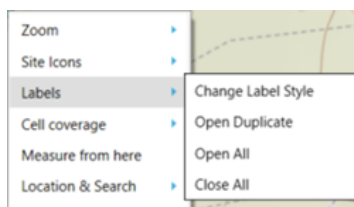
'Zoom in to here' zooms in to zoom level 16 to the point where the menu was triggered.

'Zoom out to full dataset' zooms out to appoint where all case locations in the map can be viewed in one go



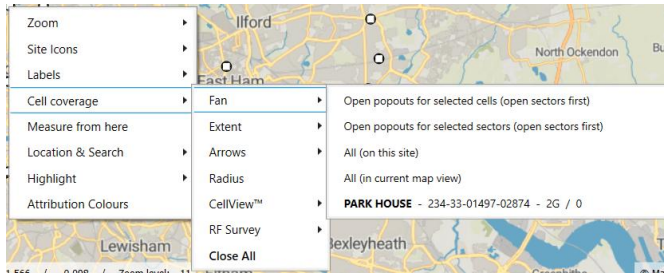
'Site icons' – gives you control over the style and size of the icon you clicked on. You can choose to change just the current icon or apply the change to all similar icons in the map.

Icon choice lets you choose between the various icon styles (see *Icon Styles*). The icon size can be changed, with options of small, medium or large – CSAS defaults to showing 'small' icons. In cases where there are several icons overlapping each other, the current icon can be brought to the front or sent to the back.



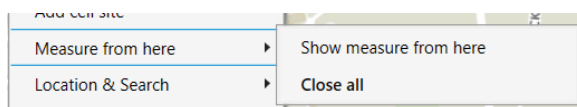
Left clicking on a cell site icon launches a cell labels, which identifies the cell site and lists the call events linked to that site. The 'Labels' menu option gives you the opportunity to change the label style (see *Map Labels*).

It also offers the chance to open a duplicate label for the current site, open labels for all sites that are currently visible on the map (up to a maximum of 30 sites to prevent an impact on map performance) and to close all open labels.



The 'cell coverage' option controls the opening of cell coverage visualisation options, including fans, extent arms, arrows, cell radius, CellView and RF Survey.

For each visualisation type, you can choose to view the coverage for any of the cells/sectors on each site. You also have the opportunity to open map label popouts for the selected sectors (either one for each sector or one combined label for all cells that share an azimuth). You can also elect to open the cell visualisation for all sectors on the selected site or for all sites currently in view (up to a maximum of 30 sites).



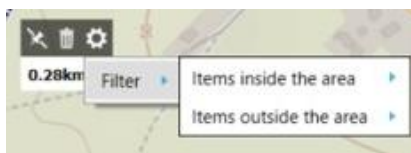
Measure from here opens a measurement radius on the map. There is also an option to close all open measurement radii.



The 'Show measure from here' option opens a measurement radius, from the point at which the menu was triggered.

The radius shows the distance from the source point (which defaults to kilometres but can be switched to miles).

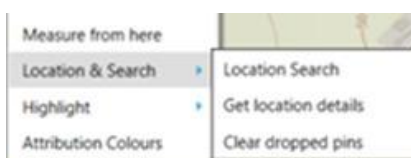
Multiple measurement radii can be open at a time.



The radius has a control menu which opens when you hover the mouse over the radius.

Using the control menu, the radius can be pinned open or dismissed.

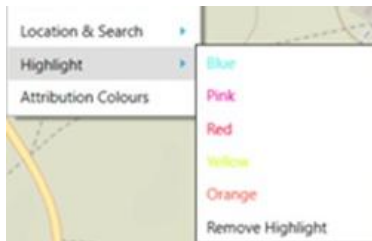
A filter menu also offers the opportunity to filter the map to hide all sites outside of the radius or all site inside the radius and to create snapshots from the filtered dataset.



The 'Location & Search' menu offers methods for finding locations.

'Location Search' – allows you to enter an address, postcode or map coordinates and have that location highlighted on the map (with a 'dropped' pin). 'Get location details' – opens a pop-up showing the address, postcode and map coordinates for the pointer location.

'Clear dropped pins' – clears any location pins that have been placed from previous searches.



'Highlight' allows you to add a coloured ring around the location to highlight it.

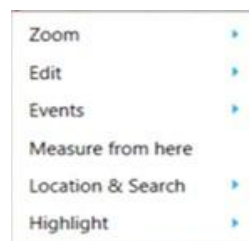
There are several colour options and an option to remove the highlight again.



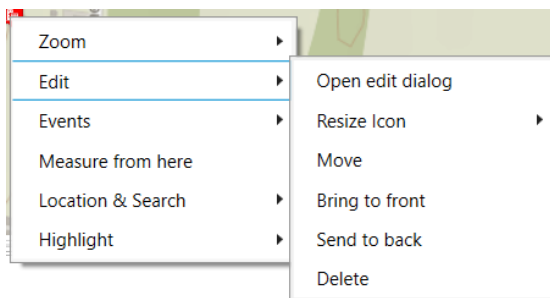
'Attribution Colours' gives you a shortcut to the Attributions screen so that identifier colours (and therefore cell site colours) can be quickly edited.

POI & ANPR Right-click

To open the 'POI & ANPR' drop-down menu, right-click on a POI or ANPR icon. The drop-down gives you the following options:

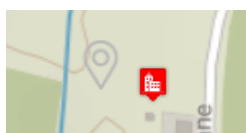


Details about menu options that aren't also found in the 'Cell Site' menu are as follows:



The Edit menu offers options to edit an existing POI or ANPR location (see [POI Location Icons](#) and [ANPR Icons](#) for more details of this menu option).

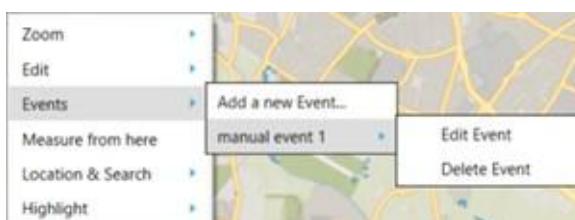
The icon can be resized – with options of small, medium and large.



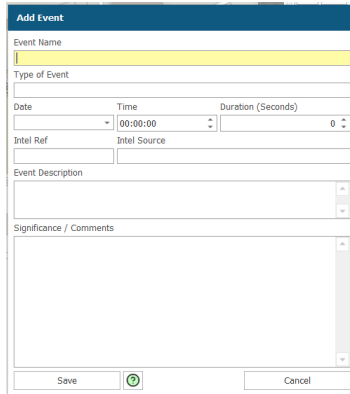
A POI icon can be moved if it has been placed incorrectly – when the 'move' option is triggered, a grey pin icon is placed in the original location for context and the POI icon moves with the mouse pointer, left-click to pin the icon to a new location.

POI & ANPR icons can be brought to the front (closer to the viewer) or sent to the back.

POI icons can be deleted if they are no longer required – this deletes the POI and any events associated with it from the case and cannot be recovered.



The 'Events' option allows events associated with a POI location to be managed – new events can be added or existing events can be deleted – deleted events cannot be recovered.



The 'Add Event' popup form contains the following fields:

- Event Name (text input)
- Type of Event (text input)
- Date (dropdown)
- Time (dropdown, showing 00:00:00)
- Duration (Seconds) (dropdown, showing 0)
- Intel Ref (text input)
- Intel Source (text input)
- Event Description (text area)
- Significance / Comments (text area)
- Buttons: Save, Cancel

The Add Event popup provides an opportunity to add a new event to a POI location - for example, if the POI location represents the location of a robbery in a case, the 'event' added to that location provides details of the time of the robbery.

Event Name is a free text field for whatever label you wish to apply to the event.

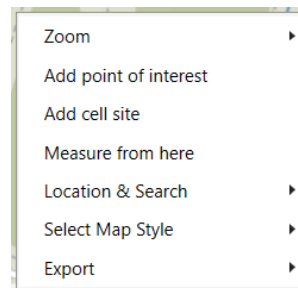
Type of Event is also free text and allows you to group events using bespoke categories.

Date and time relate to the start time for the event and a duration can optionally be added for events that last for a period of time. Intel Ref and Intel Source can be added to link the event to the statements or other evidence that detail it and Event Description and Significance/Comments are optional free text fields that allow you to add extra details.

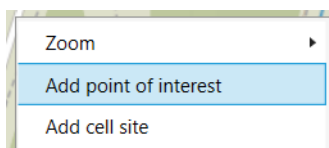
A subset of the data entered for the event will be shown in the Case Hub grid and in the map label for the POI location if the event is selected to be viewed.

Map Background Right-click

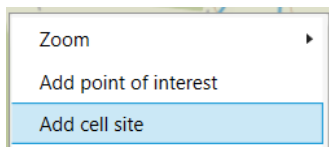
To open the 'Map Background' drop-down menu, right-click on the map background away from any icons. The drop-down gives you the following options:



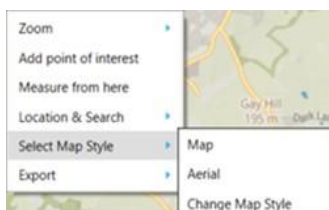
Details about menu options that aren't also found in the 'Cell Site' and 'POI & ANPR' menu are as follows:



This option allows you to manually add a POI (point of interest) icon to a map. The POI icon is placed under the pointer location. See [Manually Adding POIs](#) for more details.

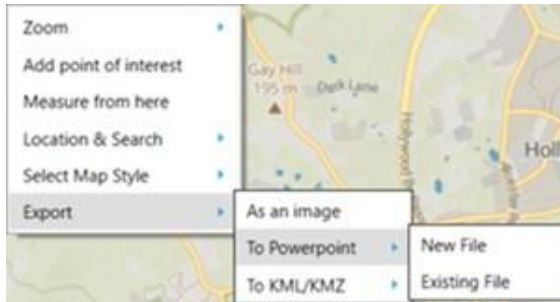


This option allows you to manually add a cell site icon to a map - for example, in a scenario where you are receiving verbal updates from a cellular operator in a live investigation. See [Manually Adding Cell Sites](#) for more details.



This option gives an alternative method for switching the map style between 'road' and 'aerial' (in addition to the button in the map panel ribbon).

There's also a shortcut to launch the 'Map Settings' > 'Map Style' pop-up menu.

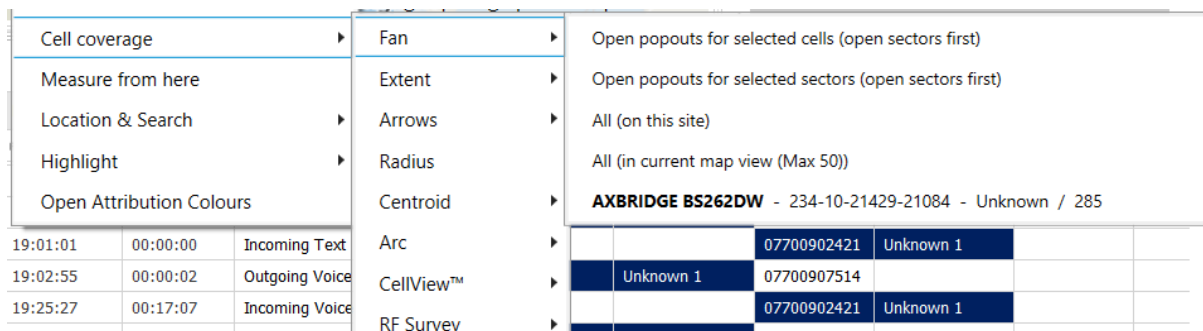


This option gives you access to various methods for exporting map content (see *Using Map Exports*).

Map content can be exported as an image to Powerpoint by copying it to a slide in a selected Powerpoint file. It can be exported as KML data, which can then be opened in other mapping products.

14.6.5 Cell Visualisations

The Cell Coverage options in the cell site right-click menu allow you to enable/disable sector fans, extent arms, azimuth arrows, coverage radius or, if you have licensed the features, CellView or RF Survey data, so you can view the area within which each cell is likely to be able to be used.



Each of the 'toggle' options shows a list of the cells/sectors that are known at the selected site and offers options to toggle on/off 'All' sectors (on the current site or in the current map view) or to toggle individual sectors.

The individual sectors are listed, along with their technology and azimuth, to enable the user to easily select the required sector to view.

The operation of this control is a simple toggle – e.g. it changes the state of each object to the opposite state. So, if a sector fan is currently enabled, toggling will disable it and vice versa.

The menu stays open after a cell/sector has been selected, allowing users to select multiple sectors to open at the same time if they wish. The menu only dismisses when the user clicks out of the menu on the map background, or if one of the 'open popouts for...' options is selected, which causes the selected sector coverage icons to open along with the required cell popout labels.

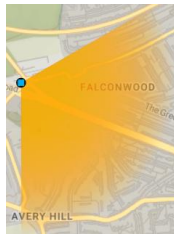
The 'All' functions work slightly differently – selecting the 'All (on this site)' or 'All (in current map view)' options switches on all cells that aren't currently on but doesn't toggle off those that are on. To close all cell visualisation, use the 'Close All' option in the main Cell Coverage menu.

All (in current map view) only works if there are fewer than 30 sites in view – this is to prevent an 'open all' command causing map performance issues by attempting to open hundreds of cells simultaneously.

The extent of each sector fan, extent arms or azimuth arrow can be altered by changing the Map Settings > Sectors > Geographical Reach (or Onscreen Distance) values – this can be changed for individual cells or set as a global default value.

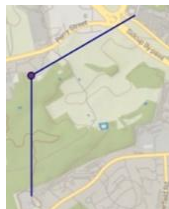
The colour of the visualisation of each cell/sector can also be changed in the Map Settings > Sectors popup. There are 10 colour choices available and the opacity (transparency) of each sector can also be varied from 10% (very see through) to 100% (opaque).

The cell visualisation options are:



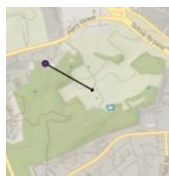
Sector Fan

This option displays a 'fan' (or 'wedge') shape to represent the approximate coverage area of a cell. It is orientated based on the cell's azimuth and defaults to showing a 120° coverage arc. The cell's onscreen 'reach' or radius is set to a default value and does not represent the actual cell coverage area.



Extent Arms

This option displays just the notional outer edges of the sector 'fan', with no infill, which is preferred in some jurisdictions as it does not intimate cell reach.



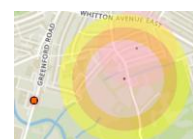
Azimuth Arrow

This option merely indicates the direction of the cell's stated azimuth and offers no visual clues as the cell's possible coverage area.



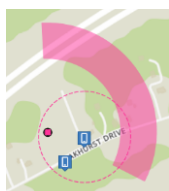
Coverage Radius

This option does not even indicate azimuth and simply displays an area around the cell site in which the cell might provide coverage.



Centroid

Vodafone UK provide additional cell coverage information in the form of a Centroid – more details are provided below.



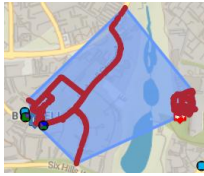
Arc/Radius Ring

Device location visualisation data provided in some countries, in the form of 'ping' and 'timing advance' data can also be displayed in CSAS maps.



CellView

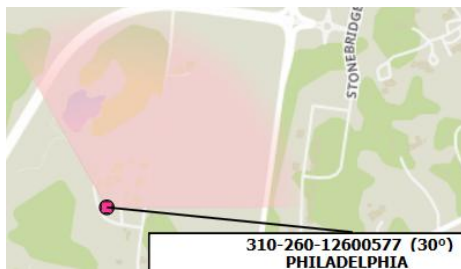
CellView depicts cell coverage as coloured polygon, showing the area within which the cell has been reported as providing coverage by the phone apps that provide the crowd-sourced raw data for the service.



RF Survey

This option is based on specific cell coverage evidence gathered in an RF Survey and depicts the actual cell coverage area as captured in the survey. It offers arguably the most accurate view of a cell's coverage area, depending on the completeness of the underlying survey data.

The various methods for displaying the coverage area of a cell involve accepting differing levels of assumption and approximation; for example, the coverage visualisation methods that are based on knowledge of the cells' azimuth (sector fan, extent arms, arrow) require several assumptions to be made, not the least of which is that the azimuth information provided by the network is correct.

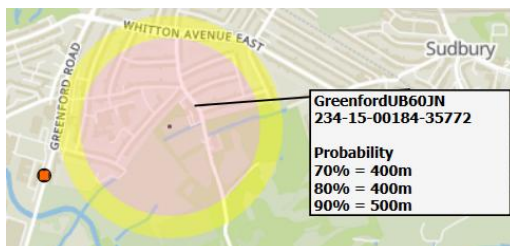


The azimuth displayed in this example is orientated at 30° from the cell site or tower, it is also shown with an arc of coverage of 120° and a 'reach' or coverage distance of 1km.

The azimuth data provided by the network is accepted as a fact, but the other values (arc and reach) are set using default values within CSAS.

A map such as this is therefore not necessarily showing a true representation of the cell's coverage area, it is instead providing a visual guide to the expect and approximate coverage area served by the cell. No evidence related to the actual coverage area or of the locations at which the cell can be expected to provide usable or 'serving' coverage can be taken from such a representation.

The 'centroid' data provided by some networks, including Vodafone UK, offers an indication of the possible location of a device that is using that cell. The data is offered as a set of 'probability' radius values.



In the example, Vodafone's data states that there is 90% probability that a device using cell 35772 is within 500m of a set of coordinates (indicated by the yellow ring on the map) and only an 80% or 70% probability of the device being in the smaller area within 400m of the stated point location.

Centroid data is offered, in part, to provide information to be used to determine the starting point for a search related to the user of a device, but the data provide is based on estimates and assumptions gathered from the network's radio planning system. Centroid maps do not offer an evidentially sound method of determining a cell's true coverage area.

Some networks offer device location data in the form of 'ping' or 'timing advance' data and these options are discussed in a later section.

The CellView feature offered as an additional extra in CSAS, uses crowd-sourced cell coverage data, provided by a partner to offer a real-world view of the reported coverage

of a cell. CellView is not affected by the assumptions inherent in azimuth-based coverage estimations and testing has shown a high degree of correlation between the coverage areas indicated by CellView and the actual coverage area of tested cells.



However, CellView data is affected by other assumptions, for example, in this image, CellView indicates that a cell has been reported as providing coverage in the area shaded in orange. As we have no information about which phones reported this coverage or where contributing were or were not located, we can't determine

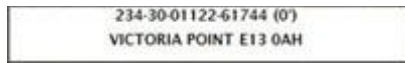
whether the coverage of the cell isn't shown extending further in the area bounded by the red dashed line because the cell really doesn't cover there or because no contributing phones sent coverage information from that area. The caveats and limitations associated with the use of CellView data are outlined more detail in a later section.

The only truly evidential way to determine a cell's coverage area is to undertake forensic RF surveys in the area. As long as the survey route was sufficiently comprehensive, a properly conducted RF survey should provide a robustly evidential view of the area served by the cells and the locations at which that cell would be used by a subject device.

The use of the less accurate cell coverage visualisation methods offered by CSAS in evidential maps submitted to court is perfectly acceptable, as long as the limitations of each method are understood and explained.

14.6.6 Map Labels

Clicking on a location icon opens a pop-up label giving details of the site and of the case events related to it:



The pop-up label is tethered to the parent location icon by a thin link line, ensuring you always know which site's details are being displayed. There is an option to hide the link line if required.

Map labels work in the same way for all location types, cell sites, POI locations and ANPR cameras. There are four types of map label to choose from:

- » Normal
- » Expanded (shown by default)
- » Simplified
- » Micro

The level of detail contained in the map label is controlled by the label type and the style template that is being used. A typical map label contains the following data:

Location details – shows the site or location name. For cell site labels, if the location that hosts the site also hosts other sites (e.g. if sites belonging to different networks share the same rooftop), then details of other sites at that location will populate the Sites drop-down.

Multiple Cells YATES HOUSE E2 6NU						
Date	Time	Duration	Calling	Called	Type	S/E
14/08	10:57:06	00:00:00	150	0597	T	(S)
14/08	10:57:35	00:00:49	0597	0177	V	(SE)
14/08	11:04:00	00:01:21	0597	Data	D	(S)
14/08	11:04:05	03:35:19	0597	Data	D	(S)
14/08	11:05:59	00:01:37	0177	0597	V	(SE)
14/08	11:07:48	00:00:07	0597	0177	V	(SE)
14/08	11:11:42	00:01:31	0177	0597	V	(SE)
14/08	11:38:59	00:00:00	0157	0597	T	(S)
14/08	11:52:47	00:02:09	0597	0015	V	(SE)
14/08	11:56:07	00:05:22	0597	0157	V	(SE)
14/08	12:07:40	00:00:28	0597	0570	V	(SE)
14/08	12:11:10	00:01:56	0597	0720	V	(SE)

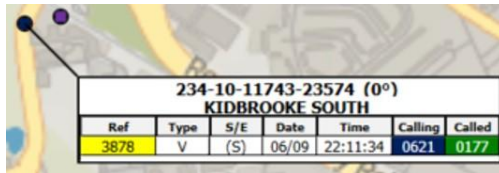
Cell details – for cell site labels, if more than one cell on a site was used, then multiple cells will be shown in the Cell drop-down – this defaults to showing details of 'all cells'.

Call or event details – a list of events (cellular events, POI events, ANPR captures) that match the current filters can be shown in the body of the expanded pop-out.

A map label can be configured using 'Map Settings' > 'Labels' to automatically open labels in 'expanded' mode, with the event table showing – this removes the need to open the event tables individual if they are always required to be in view. This is the default setting.

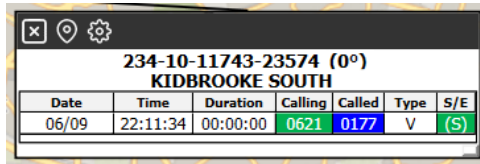
Label Controls

When initially clicked, pop-out map labels open on screen and then close if you open another map label elsewhere. You can choose one or more pop-out map labels to stay open by pinning them to the map. You can expand a map label to show call details and make map labels more visually attractive. To do this, map labels operate in several modes:



234-10-11743-23574 (0°)							
KIDBROOKE SOUTH							
Ref	Type	S/E	Date	Time	Calling	Called	
3878	V	(S)	06/09	22:11:34	0621	0177	

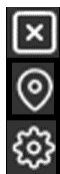
In 'mouseoff' mode – e.g., when the mouse pointer is not directly over the map label – the map label shows only the required site/call details.



234-10-11743-23574 (0°)							
KIDBROOKE SOUTH							
Date	Time	Duration	Calling	Called	Type	S/E	
06/09	22:11:34	00:00:00	0621	0177	V	(S)	

In 'mouseon' mode – e.g. when the mouse pointer is on the map label – a set of map label controls is displayed at the top left of the label.

The label controls are as follows:



Close the label.

Pin the label open. You can have multiple labels pinned open at the same time.

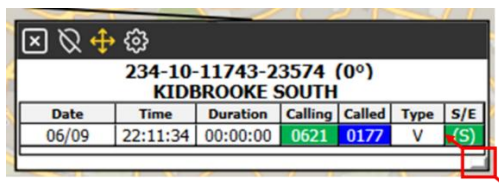
Open the options menu.

When a label has been pinned open, additional icons are displayed.



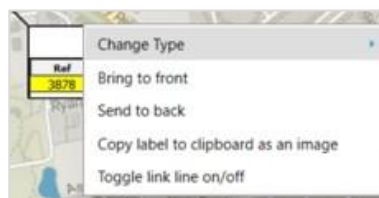
Unpin and close the label. You can close all labels in one go from the cell site right-click menu.

Move the label.



234-10-11743-23574 (0°)							
KIDBROOKE SOUTH							
Date	Time	Duration	Calling	Called	Type	S/E	
06/09	22:11:34	00:00:00	0621	0177	V	(S)	

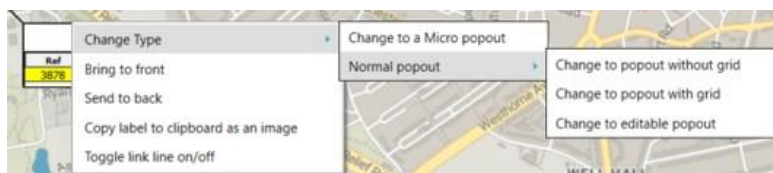
A 'resizing' box control also appears in the bottom right corner of the label. To drag the label to the required size, click and drag the control.



The label control menu allows you to change the label type, bring it to the front or send it to the back (in the event that labels are overlapping), copy the label to clipboard (so it can be passed into another application) and toggle the individual link line on/off.

Map Label Types

Several types of 'popout' map label are supported, each of which is further defined by a customisable template and a set of display options.



Micro popout label



Micro labels display only one line of text and are designed to take up as little space on the map as possible.

The data field displayed in the label is determined by the label template, different templates can be created that expose different data fields if required. Please contact

CSAS Support if you require a different map template to be created.

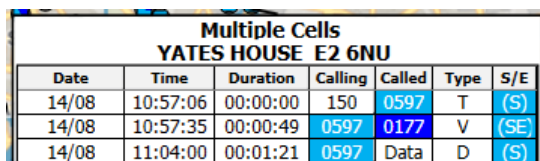
CSAS can be set to default to always showing micro labels by changing the setting in the Default Label Size options in the *Map Settings > Labels* menu.

Normal popout label

The normal popout label is the default option and selects labels that can display multiple sets of information. There are three configurations of normal label:

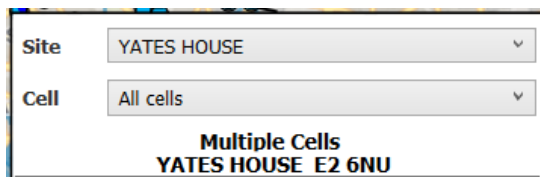


Popout without grid – the 'location' details are shown but the 'events' grid is hidden



Date	Time	Duration	Calling	Called	Type	S/E
14/08	10:57:06	00:00:00	150	0597	T	(S)
14/08	10:57:35	00:00:49	0597	0177	V	(SE)
14/08	11:04:00	00:01:21	0597	Data	D	(S)

Popout with grid - both the 'location' and 'events' sections are shown.



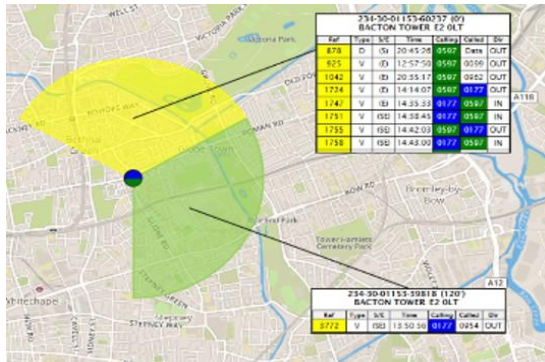
Selectable popout

In some scenarios, there may be multiple cell sites, possibly belonging to different networks, deployed at the same location – a shared tower or rooftop site, for example. The default option is for a label to display events for all cell sites (multiple sites) and cells (multiple cells) at a location, but if a cell site map label is switched to the 'selectable' type, the full control zone is expanded to reveal the Site and Cell dropdowns. This allows you to select a specific Site (if there is more than one cell site) and/or Cell (if more than one cell on the site was used by a phone) to display data for. If you want to display separate labels for different sites/cells, you can use the 'Open Duplicate' option in the cell site right-click > Labels menu to open additional popout labels, which can then each be customised to display data for the require site or cell.

The data field displayed in the label is determined by the label template, different templates can be created that expose different data fields if required. Please contact CSAS Support if you require a different map template to be created.

Duplicate Popout Labels for the Same Site

If necessary, it's possible to show multiple labels for the same cell site, in cell site labels, if required - you might want to do this to separately list the calls for each cell in different labels, each highlighting the particular cell's azimuth:



To activate multiple popouts for the same site, either right-click on the site icon and select *Popouts > Open Duplicate* then edit the separate labels to show the required combinations of site and cell or select the multiple cells that you want to view from the *cell/coverage > fan/arrow/extent* menu then click on one of the 'open popouts' options.

There are two additional options to the cell coverage menu, both allow popouts for the selected cells to be opened at the same time as opening the coverage icon:

Open popouts for selected cells (open sectors first)
Open popouts for selected sectors (open sectors first)
All (on this site)
All (in current map view)
BACTON TOWER - 234-30-00750-01282 - 2G / 240
BACTON TOWER - 234-30-00750-01284 - 2G / 0
BACTON TOWER - 234-30-01153-39813 - 2G / 240
BACTON TOWER - 234-30-01153-39815 - 2G / 0
BACTON TOWER - 234-30-01153-39818 - 2G / 120
BACTON TOWER - 234-30-01153-60235 - 2G / 120
BACTON TOWER - 234-30-01153-60236 - 2G / 240
BACTON TOWER - 234-30-01153-60237 - 2G / 0

- » 'Open popouts for selected cells' – if selected, this opens a separate popout label for each cells that was selected in the cells list. So if you've selected three cells in the cells list then three popout labels would also be opened.
- » 'Open popouts for selected sectors' – if selected, this opens one combined popout label for all cells that share the same sector/azimuth in the cells list. So if you've selected three cells that all share azimuth 0, only one combined label would be created.

To use either of these options, from the cells list first select the sectors that you want to see coverage icons for and then click the required 'Open popouts...' option.

Expanded Label/Event Lists

The 'expanded' version of the popout label includes an events list – each list is automatically filtered to show only events that match the currently selected set of identifiers and start/end dates. The expanded label also provides an additional set of control functions for the event lists:

M5 STH GLOUCESTER ANPR data v1.xls			
Index	Date	Time	VRM
29	19/08	09:41:33	WL48NEB
30	19/08	09:41:39	VA43WMP
31	19/08	09:41:42	QG37FME
32	19/08	09:41:43	KW29JNM
34	19/08	09:41:44	PB25EWA
33	19/08	09:41:44	KL98BLE
35	19/08	09:41:45	EE43NBI
36	19/08	09:41:48	HY80NWM
37	19/08	09:41:48	BS79PTA
39	19/08	09:41:49	TE25BPR
38	19/08	09:41:49	JH68HOY
40	19/08	09:41:52	AP28INV

The lists can be resorted by clicking on the necessary column header – click once to sort A-Z and twice to sort Z-A.

Locations that are linked to lots of events may have large numbers of events to display – the height of the call list can be varied, in 'mouseover' mode, by clicking and dragging the small 'resize' block on the bottom right of the popout box.

You can set popout labels to automatically open in 'expanded' mode, by selecting that option in the 'Map Settings' > 'Labels' tab.

14.6.7 Map Label Templates

A CSAS map loads with a 'system default' label style, but it's possible to replace this with a custom map label template which allows the map labels to look more like the individual label styles preferred by different customers.

The templates are editable, allowing new templates to be created to customise the design and layout of a label, but as they are written in programming format called 'json' they are not easily understandable by non-programmers. Please contact CSAS Support if you require a different map template to be created.

Bespoke map label templates created for CSASv2 cannot be used directly in CSASv3; if you have any bespoke CSASv2 labels that you would like to use in CSASv3, please contact CSAS Support to get them adapted.

Please see the [Map Settings > Labels](#) for details of how to select a specific map label.

Additional map label templates can be imported using the 'Map Settings' pop-up window. Map label templates are listed under the 'Labels' tab:

Stepped Procedure

You can import a new template by:

1. Clicking the 'Import New Template' button.
2. Navigate to where the template file (with a .json file extension) is stored and selecting the file you want to import. The files are copied to the templates folder ready to be used.
3. So you can see the set of files that are available, the 'View Template Folder' link opens the folder that the map labels templates are stored in. From this window, you can edit or delete your templates.
4. To select a different template to use within a map, from the 'Map Settings' pop-up window, select the 'Labels' tab (or click on the 'Change Label' style option in the cell site right-click menu) and select the required template from the drop-down list by ticking the Active column in the relevant row.
5. If you want the template to always open in expanded mode with the events table visible, tick the 'Label with grid' checkbox option:

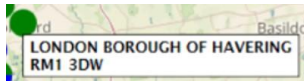
Active	Template	Label with grid	Defa...
☐	0_System Default	☒	☒
☐	1-White_Black_cell_azi_site_postcode_v2	☒	☐
☒	2-White_Black_semi-transparent_v2	☐	☐
☐	3-Blue_White_cell_azi_site_postcode_v2	☐	☐
☐	4-Blue_White_semi-transparent_v2	☐	☐

If you select the 'Default' checkbox option, the selected template will be your default for all maps.

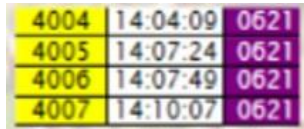
You can change map templates within a map as often as necessary, but all labels in the map will be changed and any pinned open labels may need to be closed and reopened to allow the style change to take effect.

Types of Map Label Template

There are several basic types of map label template styles:



Simplified labels - similar to the 'tooltip' labels that appear during animations and contain limited information. There are separate templates for simplified labels.



Movement labels - used on maps that show movement over a distance, often where there are lots of sites shown. Designed to take up as little room as possible. There are separate templates for 'movement' and other abbreviated formats.

20658 (01) CLOVE TOWN (32450 REPLACEMENT)						
Ref	Type	S/E	Time	Target	Other	Dir
4004	V	(SE)	14:04:09	0621	0229	OUT
4005	V	(SE)	14:07:24	0621	0177	OUT
4006	T	(S)	14:07:49	0621	0177	IN
4007	V	(SE)	14:10:07	0621	0229	OUT

Normal labels - designed to show site details and an optional call table.

Incident5 Incidents		
Date	Time	Name
19/08	09:06:55	Incident5

POI labels - provide details about point of interest locations and events

M5 STH BRISTOL AVONMOUTH ANPR data v1.xls		
Date	Time	VRM
19/08	10:35:55	CC45GGG
19/08	10:36:00	LK37NMT
19/08	10:36:01	SY14ATC
19/08	10:36:03	PPL29HMX

ANPR labels provide details about ANPR camera locations and vehicle captures

All 'normal' map label templates contain details of cell site, POI, ANPR and micro labels.

Cell ID Formats

You can configure the Cell ID format shown in popout labels and sidebar lists, using the *Map Settings > Display* menu. You can choose from the following options:



CGI Format Full - shows the full international cell ID format.



CGI Format - shows just the abbreviated cell ID portion of the international cell ID format.



Raw format - shows the cell ID format exactly as it appeared in the source data and not rearranged into the standard CGI format.

Bespoke Templates

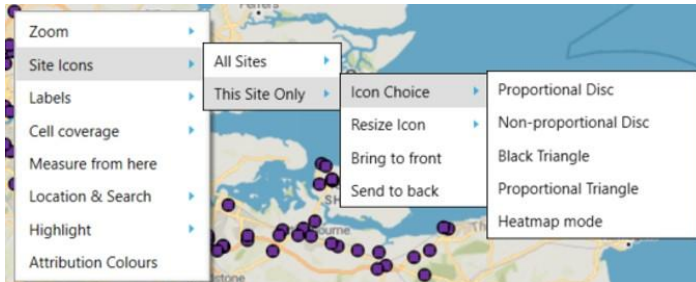
Bespoke label templates can be created on request - if none of the preloaded set of templates meet your requirements, please contact CSAS Support to discuss the options for getting a bespoke template created.

14.6.8 Icon Styles

This function allows you to choose different icon styles for use in maps, with different options available for cell site, POI and ANPR icons.

Cell Site Icons

Selecting the cell site right-click menu allows you to select the icon style using the 'Site Icons' option drill- down:



As well as being able to control the icon size, this menu also allows you to:

- » Change the style.
- » Send the label to back or bring it to the front.
- » Control the style of cell site pushpins that the map displays.

The available set of cell icon styles is as follows:



'Proportional Disc' – this icon choice shows the attribution colours of the phones that used the site and indicates the proportion of events made through that site for each phone.



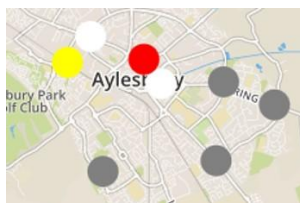
'Non-proportional Disc' – this icon choice divides the site icon equally determined by the number of phones that used it: halves for two phones, thirds for three, etc.



'Black Triangle' – this icon choice conforms to the UK Home Office 'evidential mapping' standard.



'Proportional Triangle' - this icon choice shows the colours of the phones that used the site



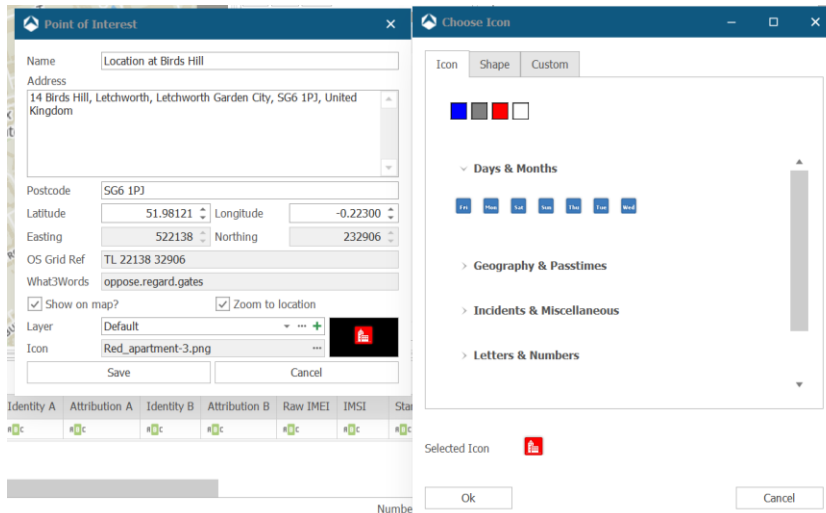
'Heatmap mode' – this icon choice shows how the colour of the cell site reflects the number of calls that were made through it – red for high usage, then orange, yellow, green, blue, white and grey. See [Heatmap Mode](#) for more details.

This icon choice is designed to make it simpler to understand the areas that a phone or group of phones were used in most commonly.

POI Location Icons

CSAS supports a large variety of icons for POI locations, all of which can be selected from the POI icon right-click 'Edit POI' menu.

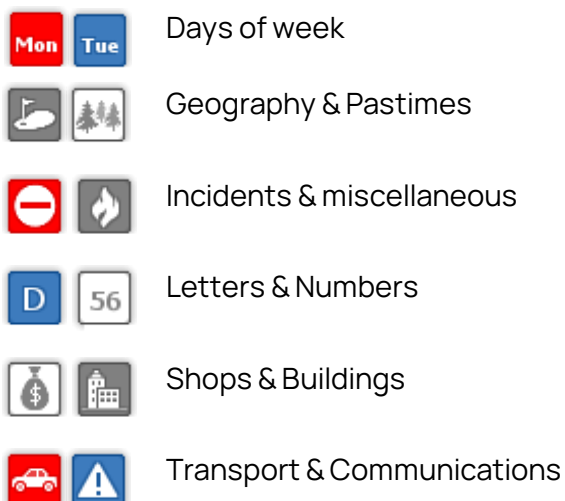
In the 'Edit POI' menu, to open the icon menu: at the end of the 'icon' section click on the ellipsis (three dots) to open the 'Choose Icon' pop-up window:



From the 'Choose Icon' pop-up window you can select an icon style (icon, shape or custom), then a colour and finally an icon group. Individual icons are available under the groups.

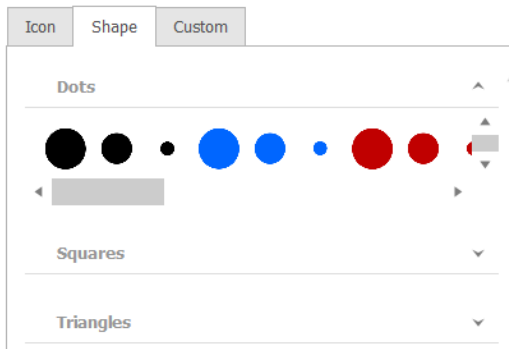
Icons

Icons are available in four colours (blue, grey, red and white) and are grouped into six categories:



The full set of preloaded icons can be viewed in the document 'CSAS Mapping – preloaded icons' which is available from the *Utilities > Resources > Support* folder.

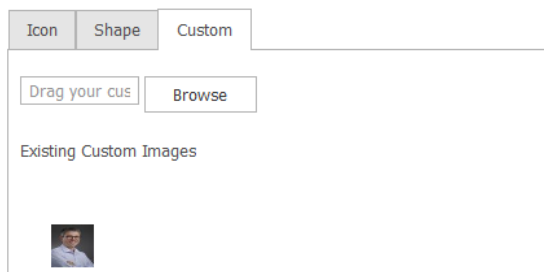
Shapes



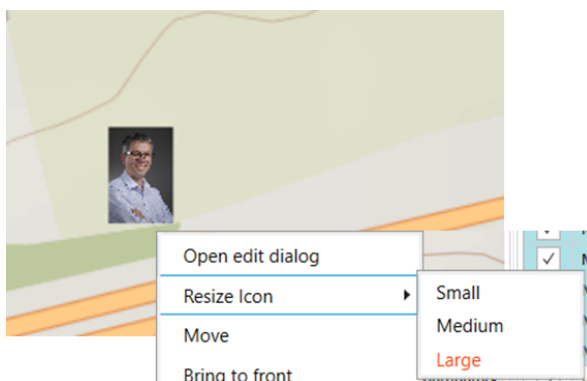
The icon set includes three types of shape – dots, squares and triangles – of various colours and in three sizes – small, medium and large

Custom Icons

You can import custom icons (in common graphic formats png or jpg), which can be used in place of a standard icon.

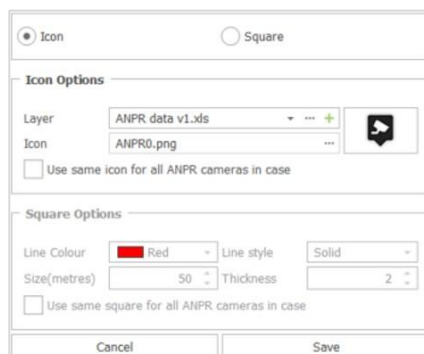


To import a custom image, from the 'Custom' tab, drag the image file to the dropbox or browse for the file via Windows file explorer.



Imported icons are reduced in size to fit in with the standard icon sizes within a CSAS map, but you use the Edit POI menu to set the image size to 'large' to make more visible

ANPR Icons



ANPR (or ALPR) locations use a 'camera' icon or a square shape that can be used to represent the general area within which the camera is located. Both can be edited in the ANPR right-click 'Edit' option.

Select between camera 'icon' or 'square' using the radio buttons in the Edit ANPR popup.

Icon

CSAS mapping defaults to using a red camera icon for ANP, but as with POI icons, you can change the selection by clicking on the ellipsis at the end of the 'icon' row and selecting a different icon – there are red, white, blue and grey camera icons available and it is also possible to use any other icon, shape or a custom image. For example, you could import the ANPR image of the subject vehicle to use as the icon for that camera.

If you choose a specific camera icon that you wish to use for all ANPR locations, tick the 'use the same icon for all ANPR cameras in case' option.

Square

Some organisations do not allow the exact location of ANPR/ALPR cameras to be disclosed and require any maps that detail ANPR activities to use a less definite method for indicating the camera's location. In many organisations, this is achieved by placing a square on the map that covers the general area in which the camera is located.



When the 'square' option is selected, you can choose the colour of the square outline, the style (solid, dotted) and thickness of the outline and the size of the square (in metres).

If you choose a specific camera icon that you wish to use for all ANPR locations, tick the 'use the same icon for all ANPR cameras in case' option.

Randomisation

An additional method for obscuring the exact location of each ANPR camera is to apply 'randomisation' to the placing of the icons. When applied, randomisation offsets the coordinates for all ANPR cameras in a within limits set in the *Map Settings > Display* menu.

Randomise all cameras in case

☒ Randomise all cameras in case

Random camera location within (km)

If the 'Randomise all cameras in case' box is ticked, camera positions are randomised within the distance set in the 'Random camera location within (km)' box.

Clicking 're-randomise' reapplies the process and moves the camera to new locations



This is an example of an ANPR icon shown at the camera's actual location.



This is the same camera after it has been randomised.

The randomisation process is applied to both icons and squares.

☒ Camera Randomised? (see settings)	☐ Moved?
☒ Show on map?	☐ Zoom to location

The 'Edit ANPR' popup indicates whether an individual camera location has been randomised or not.

The map coordinates shown in the Edit ANPR popup will be for the camera's displayed location – meaning that the coordinates will be adjusted to show the randomised location if randomisation is enabled.

14.6.9 Map Styles

CSAS maps are able to obtain mapping background 'tiles' from a variety of sources.

Internet Mapping

The default option is to obtain tiles from our Internet-based mapping suppliers, Maptiler, Mapbox and Ordnance Survey. This option requires that connectivity to the mapping providers is permitted by the host network and may involve the IT department having to open the network firewall or Internet proxy to whitelist the required URLs.

The URL stems to whitelist are:

- » api.maptiler.com
- » api.tiles.mapbox.com
- » osmaps.ordnancesurvey.co.uk

Custom Map Source

It's also possible to set a custom tile URL if, for example, a customer wished to use an existing or internal tile source with CSAS. This method won't work with all types of tile server and if you are contemplating using CSAS in conjunction with a third-party tile provider please discuss it with CSAS Support.

The custom URL text boxes in the Map Style Options tab in Map Settings, will expect the custom map source URL to be formatted in something the following way:

`http://26.11.11.217:90/styles/osm-bright/{zoom}/{x}/{y}.png`

Offline Mapping

An alternative is to deploy a database of map tiles on to the host PC itself; this therefore avoids any necessity to have the host PC connected to a network or to have to access the Internet.

The only downside to this option is that the tile and map content might not get updated as often as the Internet-based content would, but we are happy to arrange the distribution of updated mapping databases on a quarterly, half-yearly or annual basis.

Other limitations associated with offline tile file usage are that the 'aerial view' option is not supported and the address finder/get location details functions will not work fully when offline.

The files can also be very large – a file providing low level detail of even a fairly small country like the UK can be several tens of gigabytes, so we are also able to offer 'regional' files. These show the whole required country from a low-detail, high-level, but zoom in to show more detail for a particular region. For UK users, for example, we offer a range of regional offline tile files – these have more detailed views (down to zoom level 17) within the region but offer a lower resolution view of the rest of the country (at zoom level 14).

In addition to the standard file, that covers the whole UK at zoom level 14, regional tile files are available for:

- London & the southeast
- East
- Southwest
- Wales
- Midlands
- North
- Northeast
- Scotland
- Northern Ireland

Users can select the style of map background to use and also control their online/offline settings by selecting the 'change map style' option from the map right-click menu.

More information is available in document *0317-BRF CSAS Offline Tile Files*, which is available in the Support folder within CSAS and from the CSAS Support site.

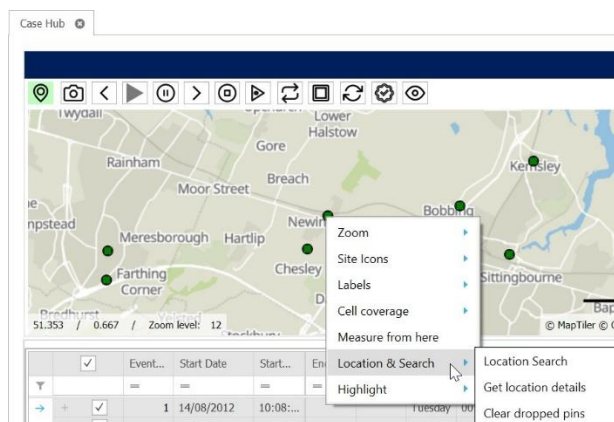
Bespoke offline map files can be created on request for any country or region in the world.

14.6.10 Location Search

The 'Location & Search' option in the map right-click menu allows you to find map coordinates and the nearest postal address details for the location under the pointer:

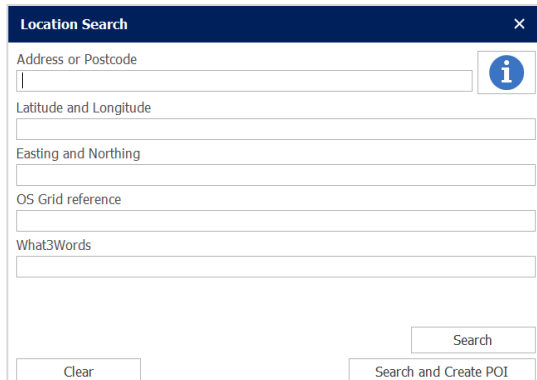
There are three options:

- » Location Search
- » Get Location details
- » Clear dropped pins



Location Search

Clicking on 'Location Search' opens a pop-up window that helps to search for an address, postal area or map coordinates:



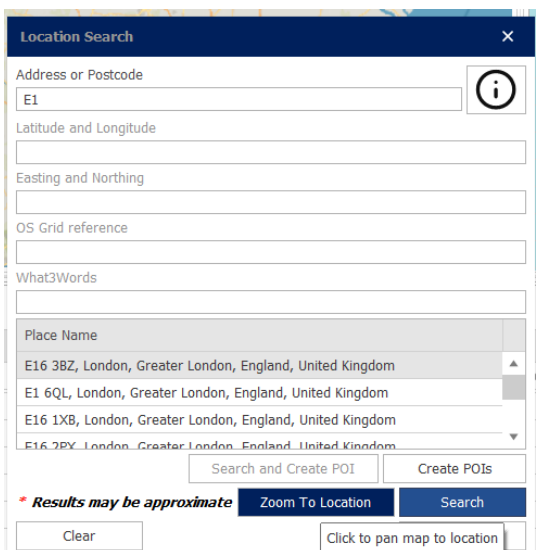
You can enter a full or partial address then: click on the 'Search' or 'Search and Create POIs' buttons, which will open a list of suggested matches for you to select from. Partial addresses may return a list of possible locations with varying degrees of accuracy, please make sure that addresses or locations found by the Location Search feature match your case requirements.

Note: You may need to drag the window up/down to see all Place Name results.

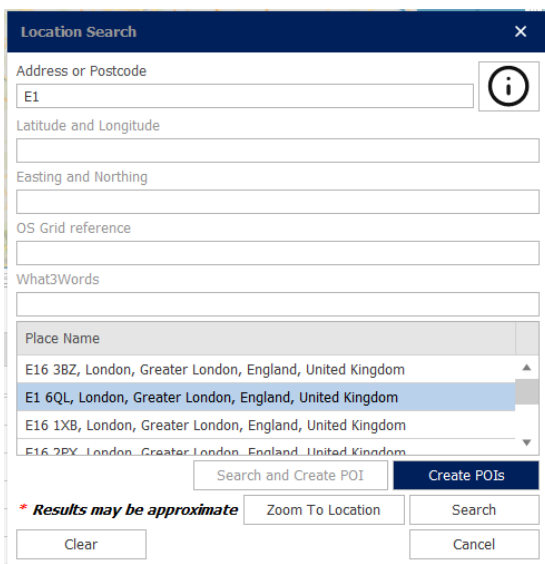
If you need to refine your search with more address details, add them and click 'Search' again or select the most appropriate suggested address and click 'Zoom to Location' to view it on the map.

This will drop a pushpin on the map.

If the location looks correct within the context of your case and you wish to create a POI at that location, right-click on the pushpin and select 'Add Point of Interest'.

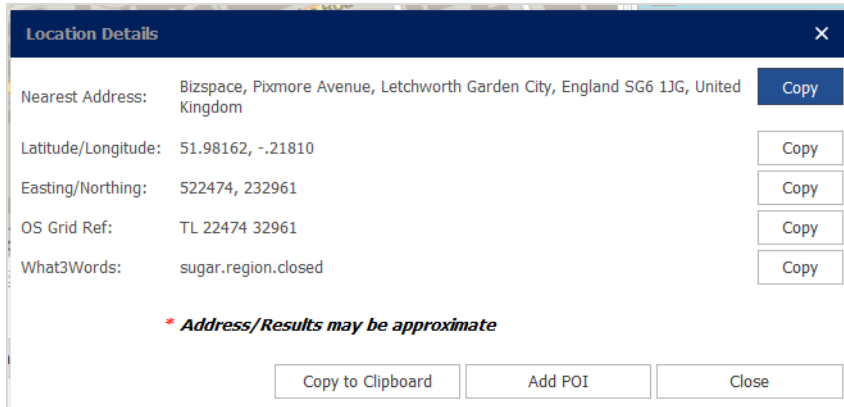


Alternatively, if one of the suggested addresses looks correct within the context of the case without needing to view it on the map, click 'Create POIs', which will open an 'Add Point of Interest' menu



Get Location Details

Selecting 'Get Location Details' opens the 'Location details' pop-up window which provides details of the map coordinates and the nearest postal address to the point under the pointer.



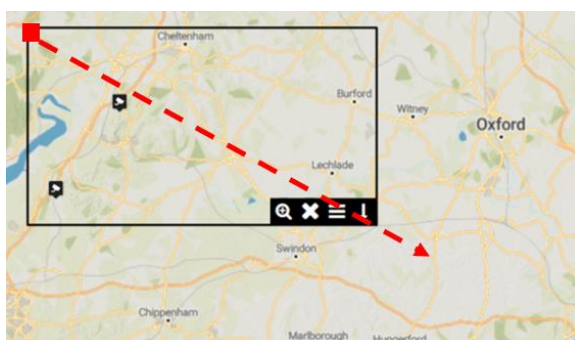
From which you can view and copy the address details, either row by row, using the appropriate 'copy' button or all details using the 'copy to clipboard' button. You can also create a POI at the clicked location.

Clear Dropped pins

The Location Search 'zoom to location' option drops a pin icon on the map at the selected point. Several successive search actions might result in several pins dropped across the map. If the dropped pins are no longer required, they can be cleared by selecting this option. If a pin is highlighting a location that is of interest in the case, right-click on the icon and select 'Add point of interest' to retain it in the case.

14.6.11 Marquee Select

The 'marquee select' or 'drag and hold' function gives you a more targeted way of zooming to the required area on a map:



To initiate a marquee select, right-click and hold (e.g. click but don't release the mouse button) at the top left of the area you wish to zoom to, then drag (without releasing the mouse button) to the bottom right of the zoom area, then release the mouse button.

The selected area will be bounded by a black outline and you'll see a menu at the bottom right of the selection shape which gives you the following controls:

-  Dismisses the selection shape without zooming.
-  Zooms the map to the selected area and dismisses the selection shape.
-  Opens the filter options menu.
-  Reactivates the selection window so the shape can be dragged further.

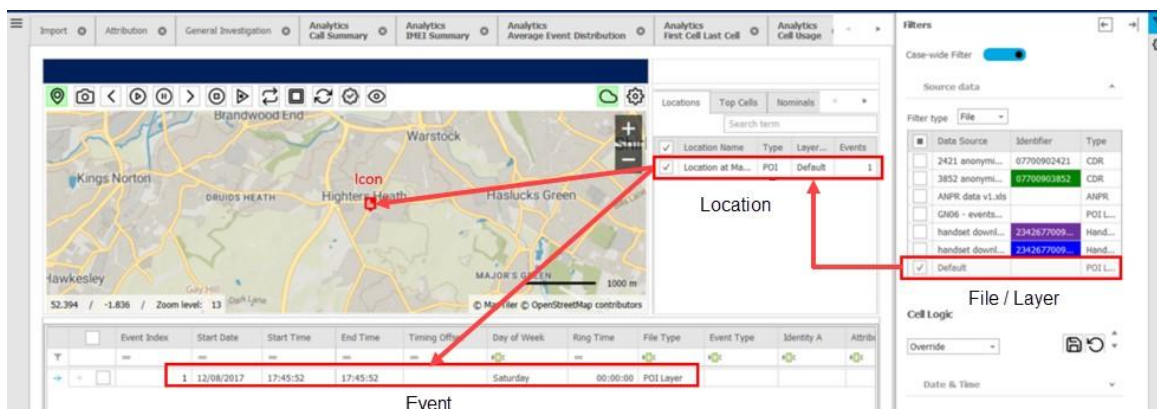
The marquee select area can be used as an alternative way of filtering the map and of creating Case Snapshots. Clicking on the filter options menu activates the following filter drill-down:



This allows you to filter and hide all locations inside the area or outside of it, and to filter and create a new 'Case Snapshot' based on the filtered data.

14.6.12 Layers, Locations and Events

Non-cellular data – ANPR, POI data, etc – is organised into a structure of files/layers, locations and events:



- » 'Files/layers' relate to the file the location data was imported from (e.g. an ANPR file imported into the case) or to a manually created layer for locations that are added directly to the map (e.g. by right-clicking on the map and adding a POI). Files/layers are listed in the Filter sidebar 'Source data' list and can be selected to be viewed in the same way that other source files are selected. If a file or layer is selected, then the locations and events related to it will be included in the current dataset and can be viewed in the map and the grid.
- » The 'Locations' detailed in each selected file/layer – e.g. an ANPR camera or a POI location – are listed in the 'Locations' tab. Locations can be viewed or hidden by ticking/unticking the checkbox associated with the location. Location icons will be shown on the map.

- » 'Events' related to a location – e.g. an ANPR capture or a POI event – are listed in main grid, along with cellular events, and will be listed in the map labels associated with the parent location. If a layer or a location are deselected, the events associated with them are removed from the grid. Non-cellular events will be included in map animations if selected.

Importing POIs

CSAS supports a standard 'rescue template' for importing POI data into a Case, known as the GN06 'locations & events' template.

Note: The rescue template is available from *Utilities > Resources > Support*.

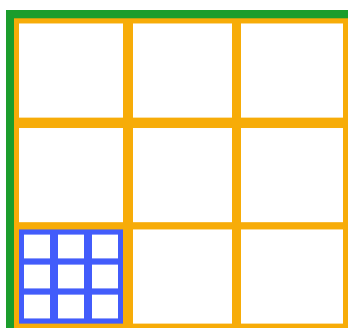
Latitude	Longitude	UTM Zone	Easting	Northing	w3w
----------	-----------	----------	---------	----------	-----

CSAS supports multiple map coordinate systems, including global standard systems such as latitude/longitude and country-specific systems such as the UK's easting/northing coordinates. An imported 'locations & events' dataset must contain at least one set of coordinates for each location.

The standard latitude/longitude coordinate system used by GPS and most other modern mapping applications, is based on a standard known as WGS84 and can, in theory, be accurate to the level of a centimetre or less. Each additional decimal place after the latitude or longitude value applies an order of magnitude more precision – for example, a lat/long coordinate value of 52,0 describes a square that is 111km on each side, whereas 51.1,0.1 describes an area that is 11.1km square, 51.12,0.12 resolves to an area that is 1.11km square and so on.

Many GPS applications return coordinates with 7, 8 or 9 decimal places, providing extreme precision for the associated locations. At the level of location awareness that CSAS requires, centimetre-level accuracy is not beneficial, so the additional storage space required to save very long lat/long coordinate numbers is a waste. CSAS therefore truncates any imported lat/long data to 5 decimal places – this provides an accuracy level of 1.11m, which should be more than enough for the maps the application creates.

The level of accuracy applied by CSAS to the most commonly imported coordinate systems are described as follows:



- » Easting/Northing - accurate to 1m² (blue box).
- » What3Words - accurate to 3m² (orange box).
- » Lat/Long - accurate to 10m² or better – this level of accuracy is considered to be accurate enough for placing an item or location in an area of interest.

Location and event data can be mapped into the template and can then be imported into a CSAS Case using 'Import Files', where the locations can be added to maps and the events can be added to the Case dataset.

Different countries and regions have their own map coordinate systems, such as the OSG (Ordnance Survey Grid) system used in the UK, many of which are based on fairly simple systems where a point location is measured to be a certain number of metres east and north of a common reference point, leading to coordinates that are expressed in 'eastings' and 'northings'. Globally, the various local easting/northing systems are coordinated within a system known as UTM (Universal Transverse Mercator) – UTM divides the world in multiple zones, within each zone there is a reference point and locations within the zone are expressed as eastings/northings in relation to that point. To be clear, OSG is not directly compatible with UTM.

CSAS accepts location data expressed in UTM coordinates – in the GN06 template there is an option to specify the UTM Zone and then show the easting and northing coordinates values within that zone. There are 60 UTM zones, which are divided into North and South sections – the UTM Zone covering most of the UK, for example, is 30N.

Populating a GN06 template with UTM data would look like this:

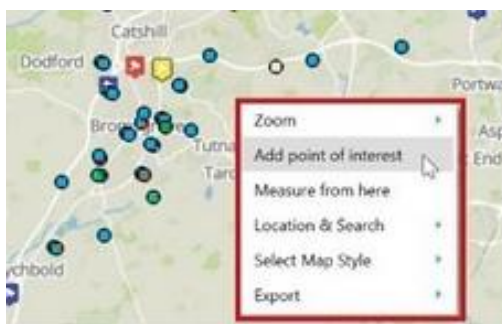
Latitude	Longitude	UTM Zone	Easting	Northing	w3w
		30N	123456	123456	

Which offers an alternative method for identifying map locations – the preference would always be to use standard latitude/longitude, however, as this introduces the least amount of uncertainty. More information about mapping coordinate systems can be found here <https://www.ordnancesurvey.co.uk/documents/resources/guide-coordinate-systems-great-britain.pdf>

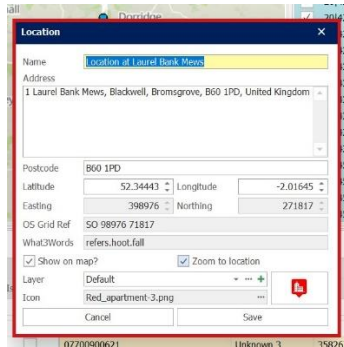
Note: Case events, often linked to POI locations, can also be added automatically via the GN06 template, or they can be added manually.

Manually Adding & Editing POIs

POIs can be manually added by right-clicking on the map background, over the required location, and selecting 'Add point of interest':

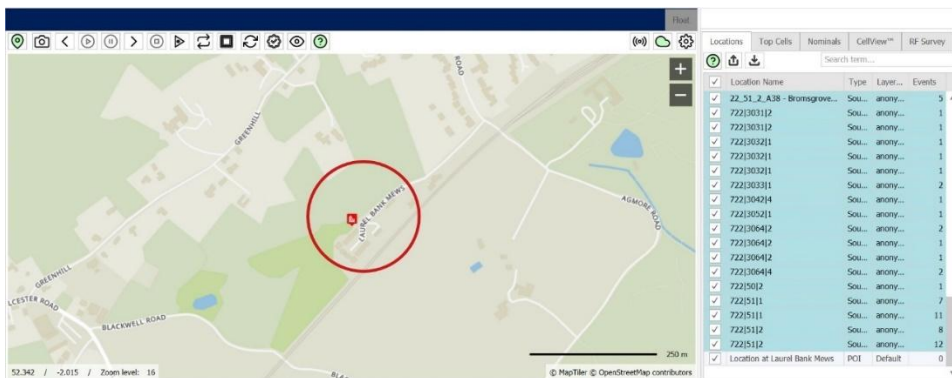


CSAS will automatically choose a location name and detect the address details of the location, including the approximate address and postcode, the map coordinates (lat/long, easting/northing, OS Grid and What3words). It will also assign the POI to the default 'layer' and assign a default icon to it.

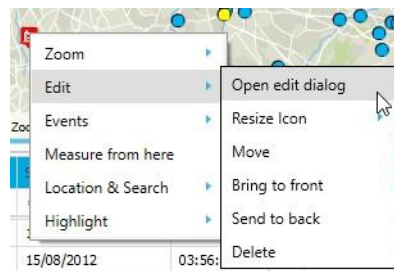


If you want to accept the default or automatically created details for the POI, all you have to do is click **Save**, but you can also change the name, address, layer and icon if you want to before saving it. Ticking the 'Zoom to location' checkbox will zoom the map to the new POI once it has been added:

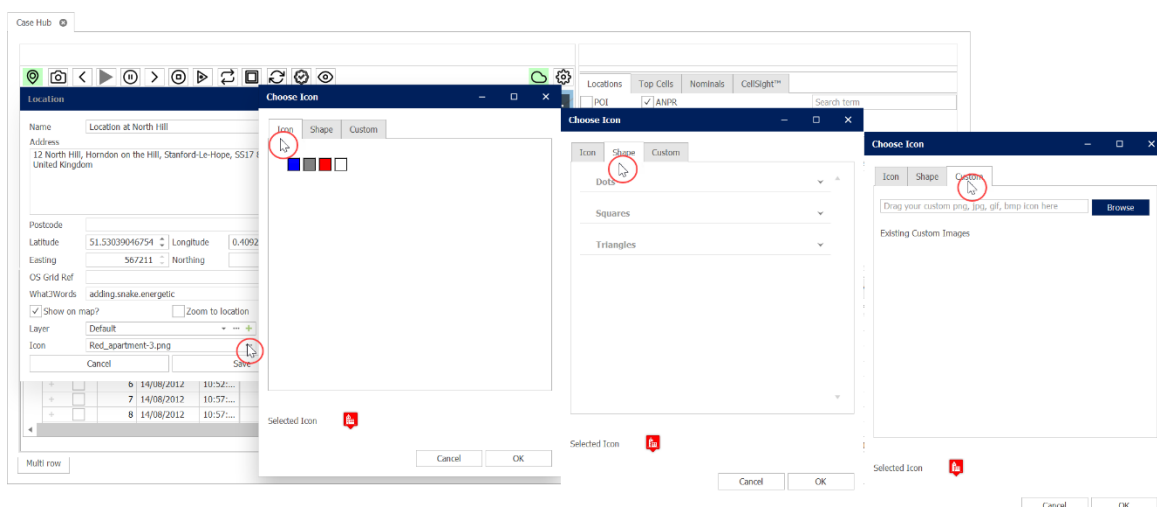
Click the **Save** button to create the new POI - it will be shown as an icon on the map and listed under the 'Locations' tab:



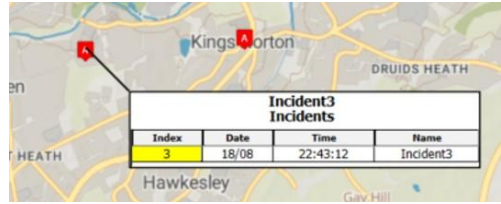
You can customise the type and colour of icon used by right-clicking on the icon created and selecting 'Edit' > 'Open edit dialog':



You can customise the icon colour, the shape or browse to select your own custom icon:



Double-clicking on the icon zooms-in closer and left-clicking on the icon displays a popout label similar to the type shown for cell sites.

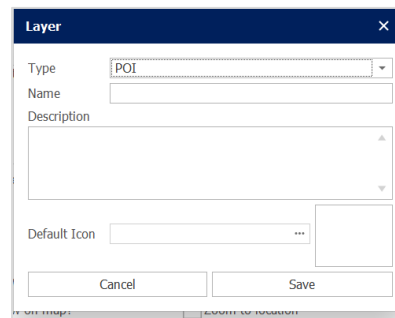


You can create multiple 'Layers' using the 'Location' pop-up window. To open the 'Location' pop-up window, right-click on the necessary location on the map.

To add a new 'Layer', next to the 'Layer' option, to the right of the 'Default' field click on the + icon:



The 'Layer' pop-up window opens over the 'Location' window:



Layer

Type:

Name:

Description:

Default Icon:

Cancel Save

You can enter a name for the new Layer, a description, browse/select/customise an icon and save the new Layer all from this pop-up window.

It's possible to add a POI location to a new map that doesn't contain any other data. Occasionally, the new POI icon might not appear on the map – if this happens do the following:

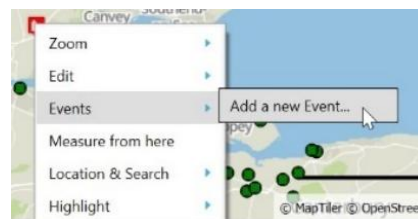
Stepped Procedure

1. Click on the button in the Filter sidebar.
2. From the source files list, select the layer the POI belongs.
3. Click the button, the POI should then appear as expected.

Manually Adding Events

Case events, often linked to POI locations, can be added automatically using the GN06 template or they can be added manually.

You can create 'Events' for the POI by right-clicking on the icon and selecting 'Add a new event...':

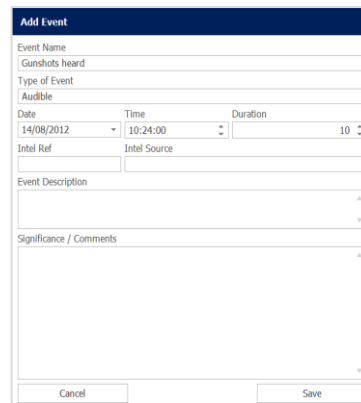


The 'Add Event' window opens, into which you can add the required 'Event' details:

Once you have added and saved the required 'Event' details, the information will be displayed in the CSAS grid, if the file or layer the event belongs to is selected in the 'Source files' list.

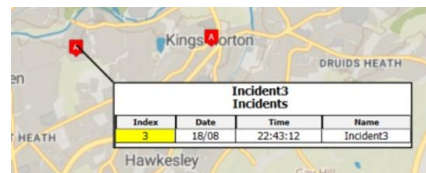
Note: You can add multiple Events for the same POI location.

Left clicking on any POI entry on the map will show the related Event(s):



The 'Add Event' window contains the following fields:

- Event Name: Gunshots heard
- Type of Event: Audible
- Date: 14/08/2012
- Time: 10:24:00
- Duration: 10
- Intel Ref:
- Intel Source:
- Event Description:
- Significance / Comments:
- Buttons: Cancel, Save

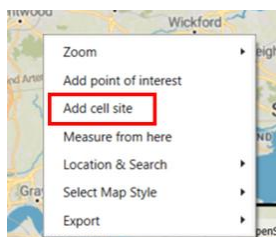


The POI Event(s) you create will be displayed in the Data Grid as a 'POI Layer' event:

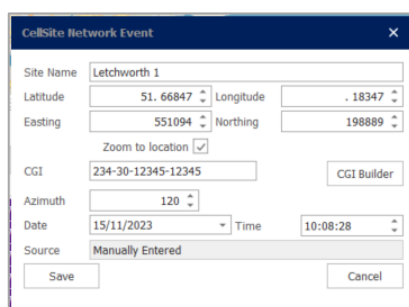
	Event Index	Start Date	Start Time	End Time	Timing Offset	Day of Week	Ring Time	File Type	Event Type	Identity A	Attrib
	1	12/08/2017	17:45:52	17:45:52		Saturday	00:00:00	POI Layer			

Manually Adding Cell Locations

Case Hub supports the option to manually add cell site locations and associated network events to a case map. Cells sites and events might be manually added to a CSAS map in circumstances such as a surveillance operation, where investigators are receiving verbal updates from a cellular provider as a suspect's device is used. In lieu of receiving the CDRs for those events, the investigator could add them to their case manually as the verbal updates are received.



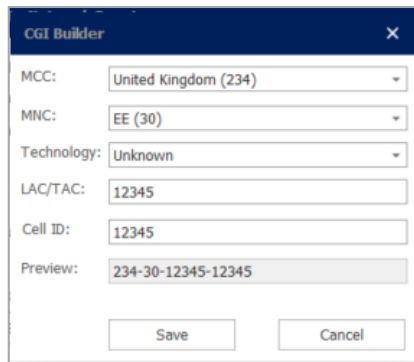
The feature is available from the map right-click menu – click anywhere on the map background that isn't covered by a cell, ANPR or POI icon and select 'Add cell site' to initiate a new manual cell site location.



The 'CellSite Network Event' window contains the following fields:

- Site Name: Letchworth 1
- Latitude: 51.66847
- Longitude: -1.18347
- Easting: 551094
- Northing: 198889
- Zoom to location: ☒
- CGI: 234-30-12345-12345
- CGI Builder:
- Azimuth: 120
- Date: 15/11/2023
- Time: 10:08:28
- Source: Manually Entered
- Buttons: Save, Cancel

The Cell Site Network Event popup provides the opportunity to add a cell site location, including cell ID and azimuth, and also to add details of an event that used the manually added cell.



CGI Builder

MCC: United Kingdom (234)

MNC: EE (30)

Technology: Unknown

LAC/TAC: 12345

Cell ID: 12345

Preview: 234-30-12345-12345

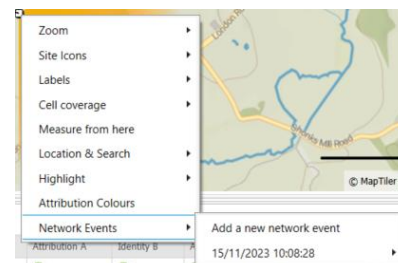
Save Cancel

The CGI builder helps the user navigate the creation of the globally unique CGI cell ID for the cell

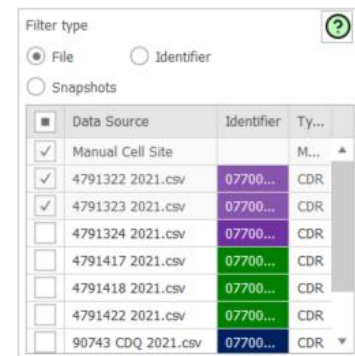
Once saved, the additional cell site and event details are available on the map and can be accessed and viewed in the same way as 'standard' cell site locations.



If additional events need to be added to an existing manual cell, right-click on the site icon and select 'Network Events' and then 'add a new network event'.



Manual cell sites and events are grouped under a reference of 'Manual Cell Site' in the file selection list in the right sidebar, allowing those manual cells to be shown or hidden as required.



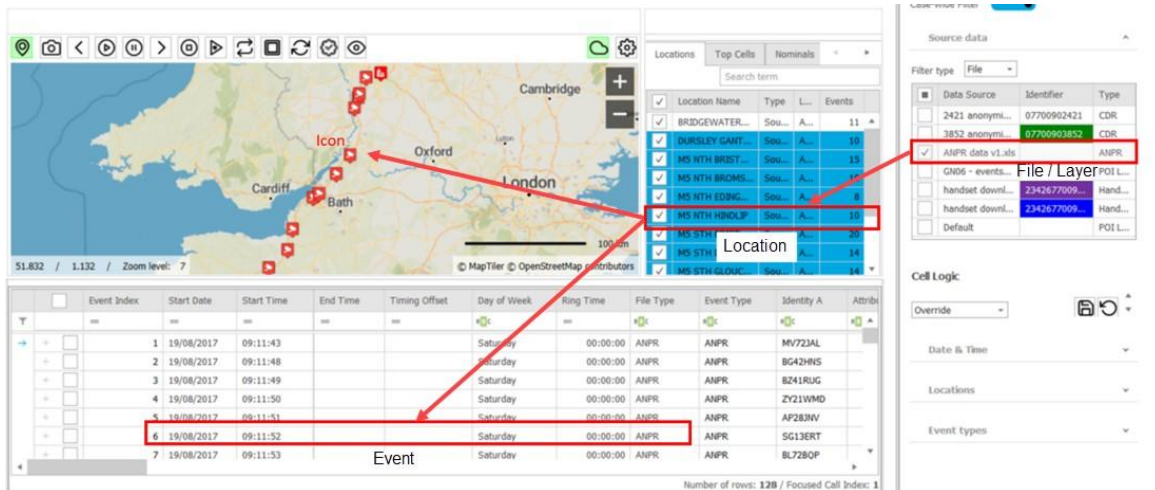
Editing ANPR Cameras and Captures

ANPR (Automatic Number Plate Recognition) is also known as ALPR (Automatic Licence Plate Recognition) and just LPR in some jurisdictions.

Optionally, if ANPR source files are available in a case, you can display ANPR camera locations on the map and ANPR capture events in the grid. Once you've imported and attributed the ANPR source files, they will be listed in the 'Source data' panel and will be available for analysis in the current dataset.

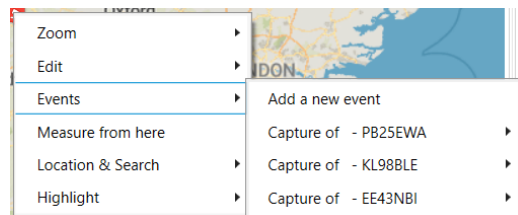
When an ANPR file is selected from the 'Source data' panel:

- » The cameras will be listed in the 'Locations' tab.
- » The camera icons will be shown in the map.
- » The ANPR captures will be shown in the grid along with POI events and call records:



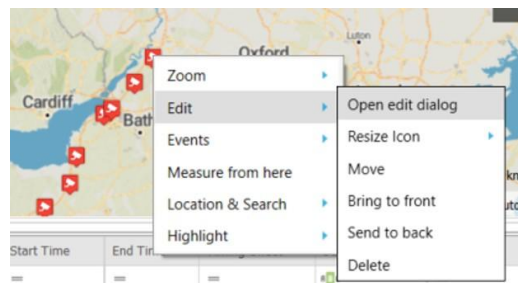
Events for a ANPR entry can be created in the same way as for a POI entry – by right-clicking on the ANPR camera icon and selecting 'Events'. Although ANPR events are usually imported from an ANPR file rather than added manually.

Event(s) for any ANPR camera location can be viewed via the right-click 'Events' menu, or by left clicking the camera icon and viewing the map label



M5 STH GLOUCESTER ANPR data v1.xls			
Index	Date	Time	VRM
29	19/08	09:41:33	WL48NEB
30	19/08	09:41:39	VA43WMP
31	19/08	09:41:42	QG37FME

You can edit ANPR camera locations using the right-click 'Edit' option:



The ANPR Edit control shows the name, address and map coordinates of the camera as well as the icon options.

ANPR camera locations can be displayed using either a standard 'camera' icon or as a square. It's also possible to randomise the camera location and show it somewhere within a specified radius of its true location; this feature allows CSAS to fit in with the restrictions that some organisations have about representing the true location of ANPR cameras on maps.

You can randomise the map location of one ANPR camera, by selecting 'Edit' from the menu and then the 'Camera Randomised?' checkbox.

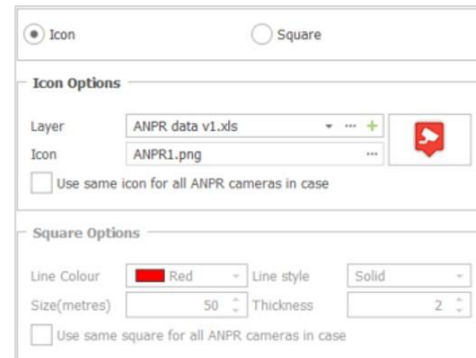


If you want to randomise all ANPR camera locations in a map, open the 'Map Settings' > 'Display tab' and tick the 'Randomise all cameras in case' checkbox:

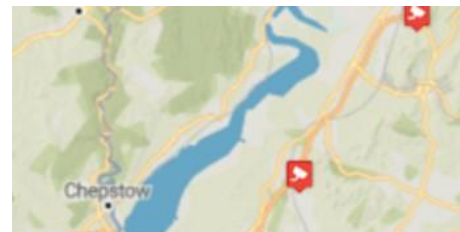


In the ANPR Edit popup, the type of icon used to represent an ANPR camera can also be selected from the edit menu.

Once you customise one camera in this way, it's possible to set all other ANPR cameras in the case to use the same settings if necessary.



If the option is set to 'Icon', the 'Icon Options' panel opens and the Layer and Icon style can be selected:



If the option is set to 'Square', the 'Square Options' panel opens. In square mode, the camera location isn't explicitly stated, instead an empty square is overlaid on the map – if 'randomisation' has also been enabled the square will be randomly offset from the camera's true location:



Note: The size, colour and line style of the ANPR square can be set. Once you customise one camera in this way, it's possible to set all other ANPR cameras in the case to use the same settings if necessary.

Events for a ANPR entry can be created in the same way as for a POI entry, although ANPR events are usually imported from an ANPR file. Event(s) for any ANPR entry can be viewed in the same way as for a POI entry.

Editing an entire Layer

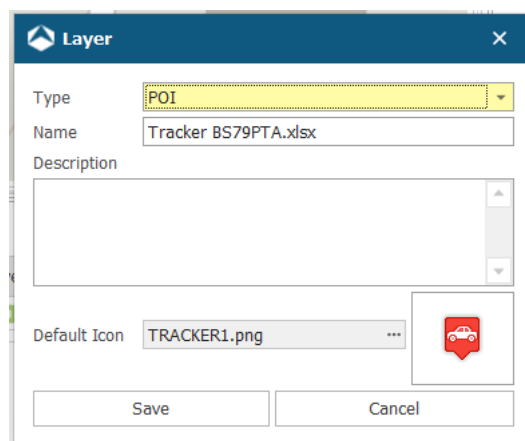
The 'edit' menus for POI and ANPR icons outlined above allow users to edit the details and change the icon of a single point at a time – it is also possible to change the icon and name for an entire layer (which means that the icon is changed for all members of that layer).

To edit an entire Layer:

- » With the required case open and Case Hub selected
- » Right-click on the required file or Layer in the right sidebar Filter type > File list

☐	Data Source	Identifier	Type	
☐	handset dow...	234267700...	Han...	▲
☒	Telomatics_R...	BS79PTA	Tele...	
☐	Tr...		Trac...	
☐	24		POI...	
☐	38		POI...	
☐	GN		POI...	

- » The 'Edit' option opens a pop that allows the layer name to be edited or changed and also allows a different icon to be selected for the layer.



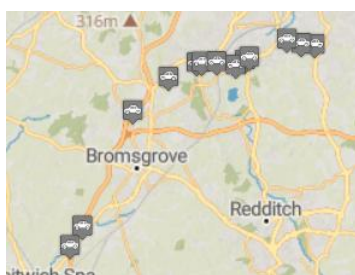
The 'Layer' dialog box shows the following fields:

- Type: POI (dropdown menu)
- Name: Tracker BS79PTA.xlsx (text box)
- Description: (empty text area)
- Default Icon: TRACKER1.png (text box with an ellipsis button and a car icon)
- Buttons: Save, Cancel

To change the name of a map Layer (this only works on layers, it is not possible to change the name of an imported file), set the amended layer name in the Name text box.

To change the Layer icon, click on the ellipsis (...) alongside the 'default icon' text box and select a new icon from the set that is presented.

- » The 'Set Icon' option offers a more abbreviated method for selecting a new icon and simply displays the folder that contains the preloaded icon set – select the new icon for the Layer or POI/ANPR file.
- » After making a change, the map will refresh and all icons for the selected layer or POI/ANPR file will be changed to the new selection.



Before



After

Using What3Words

What3words is a proprietary geocode system designed to identify any location anywhere in the world, with a resolution of about 3 metres (see www.what3words.com).

What3words encodes geographic coordinates into three dictionary words to give a location reference.

If you know the location reference for a location of interest, you can search for it using the 'Location Search' feature or you can filter a case to only show locations within a radius of that location using the Location filter.

To apply a Location filter enter it into the 'What3Word' field in the 'Locations' panel and click on the button to display it on the map.

Locations can also be imported into a case using a what3words description – the GN06 template includes a 'w3w' column for this purpose.

14.6.13 Animation

CSAS supports the option to animate map content, to make the progression of events and locations more easily understandable for a non-technical viewer.

This function allows you to:

- » Animate the progression of Cell icons on a map - you can see cell icons highlighted as animation progresses.
- » Animate the progression of ANPR icons on a map - you can see the ANPR camera icon highlighted as animation.
- » Animate the progression of POI icons on a map - you can see POI icons highlighted as the animation progresses.

The following examples use ANPR data to demonstrate map animation functions.

Triggering an animation

Before starting an animated sequence, you must first select the events to be included – you do this by ticking the checkbox in Case Hub grid column 1 for each event you wish to animate.

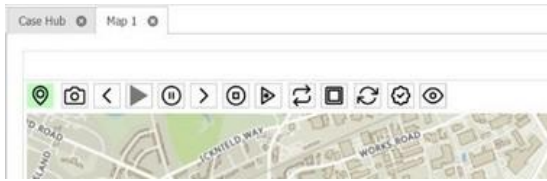
☐	Start Date	Start Time	Event Index	Timing Offset	Duration	Event Type	Identity A
	=	=	=	=	=		
+ ☒	19/08/2017	09:11:43	1	0		ANPR	MV72JAL
+ ☒	19/08/2017	09:11:48	2	0		ANPR	BG42HNS
+ ☐	19/08/2017	09:11:49	3	0		ANPR	BZ41RUG
+ ☐	19/08/2017	09:11:50	4	0		ANPR	ZY21WMD
+ ☒	19/08/2017	09:11:51	5	0		ANPR	AP28JNV
+ ☐	19/08/2017	09:11:52	6	0		ANPR	SG13ERT
+ ☒	19/08/2017	09:11:53	7	0		ANPR	BL72BQP

The selected events do not need to be contiguous, there can be gaps, and events will be 'played' in the order shown in the grid.

You must select at least two events in the grid for animation to commence.

Animation Controls

The animation controls reside in the ribbon at the top of the map panel:

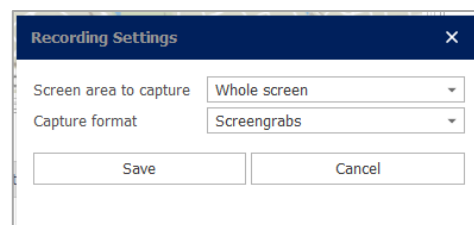
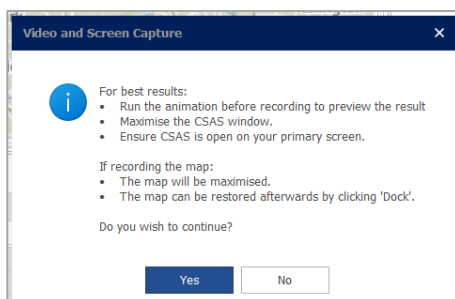


The full set of map control buttons are detailed in the [Map Controls](#) section, but the subset used to control animation includes:

-  This button moves the map animation backwards one event at a time.
-  This button plays the map animation automatically, using the options selected in [Map Settings > Animation](#)
-  This button pauses the map animation sequence.
-  This button moves the map animation forwards one event at a time.
-  This button stops the animated sequence.
-  This button records an animate sequence for later playback.

Recording an animated sequence

Clicking the  button opens a popup warning that the playback may take a long time if you select a large number of events and CSAS will also provide a popup listed the ways to ensure that the animation is recorded with the best quality.



CSAS will then show the 'Recording Settings' pop-up window.

From this window you can select the 'Screen area to capture', with options of:

- » Whole screen – including the Case Hub grid.
- » Map only – excluding the Case Hub grid.

You can also select the 'Capture format', with the following options:

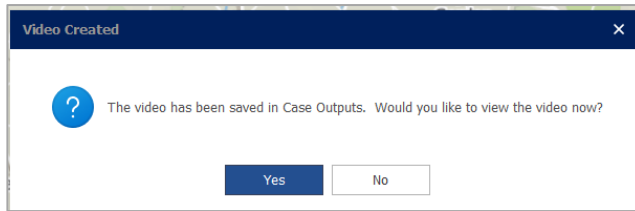
- » Screengrabs – each event in the sequence is captured as a screengrab, the whole set of screengrabs are saved to a selected folder.
- » Video – the whole sequence is captured as one moving animated video, in .mp4 format and saved to a selected location.
- » Screengrabs and video – both outputs are created.

Clicking the  button saves your selections and starts the recording process.

You can cancel the recording by clicking on the 'stop' button



At the end of the recording, the .mp4 file will be saved in the case's Case Outputs folder, which can be accessed via the Case Folder option in the navigation left sidebar.



If you wish to play the video immediately, click 'yes' on the Video Created popup.

Animation Settings

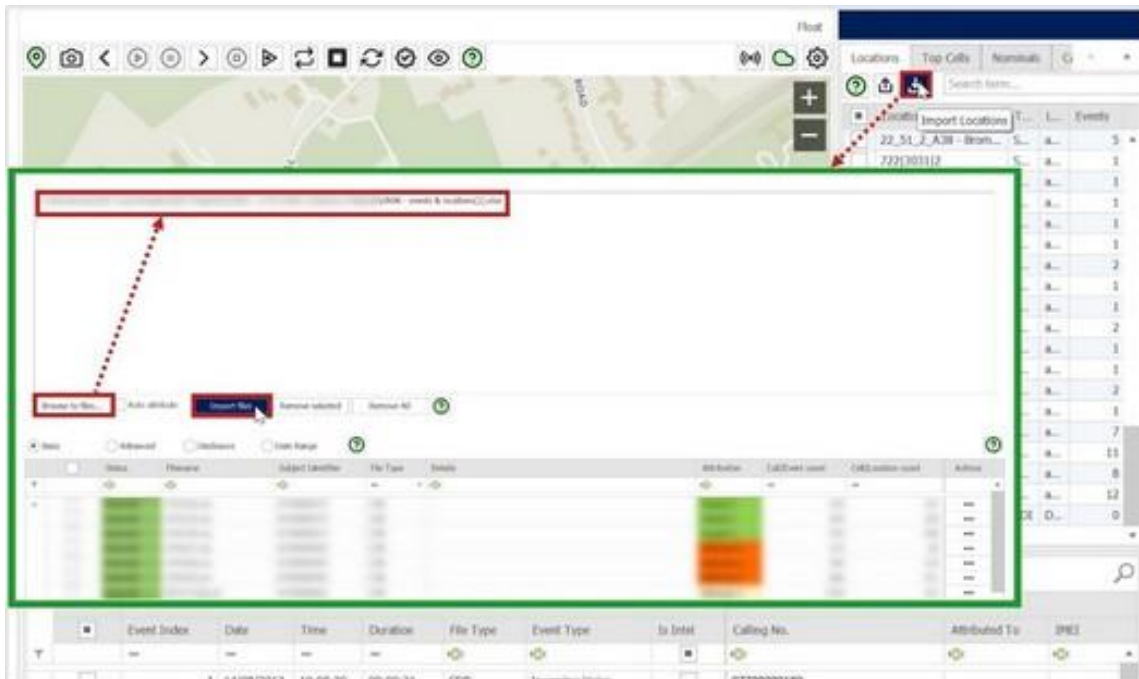
Clicking on the  button opens the 'Map Settings' pop-up window. Please see [Animation Settings](#) for more details.

Stepped Procedure

1. Using the 'Filters' sidebar, load the required dataset into 'Case Hub' making sure you that the correct set of cell sites, POI locations, ANPR cameras and other locations are shown in the map and that the associated events are listed in the grid.
2. From the grid, select the events you want to animate by ticking the required rows – only the ticked rows will be animated.
3. From the 'Map Settings' pop-up window, Select the required animation settings.
4. To confirm your settings, click on the  button. The 'Map Settings' pop-up window closes.
5. Make sure the map is adjusted to display the required area.
6. From the animation controls, click on the  button. The animation plays according to your settings. When the sequence starts, the current event will be highlighted in the map and also in the Case Hub grid, which will scroll to ensure that the current event is always in view. If you would rather record the animated sequence, click the  button. Records are saved in mp4 format.
7. The animation stops once all events have been played and the last location will remain highlighted until you click somewhere on the map. To play the animation again, you will need to select the events you want to animate and click on the  button.
8. If the map panel was maximised during the playback/recording, you may need to click on the 'Dock' button to redock it into the Case Hub window.

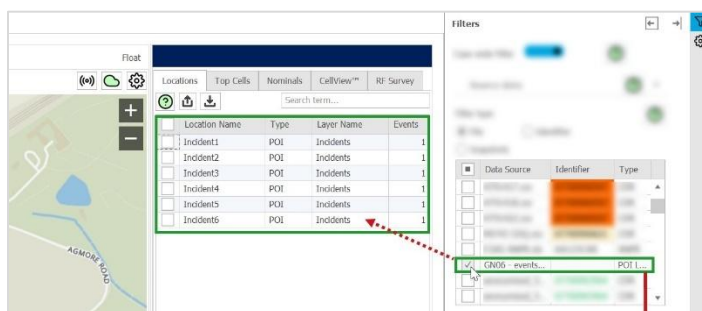
Importing Locations to the Map

To import a set of locations are a master map into a case you can either import the GN06 file via the Import Files screen, or you can click on the import  icon in the Locations tab, which really just opens the Import Files screen. Via the Import Files screen you can browse for and select the file you want to import, then click the button:



Note: Any GN06 file which has a set of locations can be imported into any case.

If the selected GN06 file imports correctly, it will be shown in the right sidebar Source Data list:



Select the data you want to see in the map using the checkboxes, then click the button again. The grid and the map refresh and show the selected data:

Note: Depending on your settings, you might need to refresh the map by clicking the  icon (see Using Mapping).

14.6.15 Using Live GPS Import

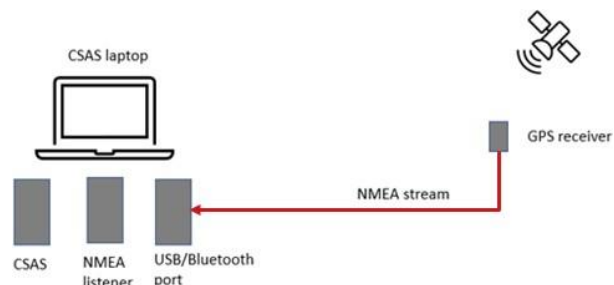
The live GPS import feature allows you to import NMEA messages directly into CSAS. It is accessible via the  button in the map control bar. Using a virtual serial port connected to CSAS, you can capture message data from a USB-connected GPS receiver and display the location data on a CSAS map.

This function is intended to help:

- » Collate data for missing persons and manhunt investigations, for example, auditing search teams and the locations searched, when compared to other datasets such as CDR, CellView, and ANPR.
- » Support investigations, for example, auditing investigation and enforcement team movements when compared with current datasets.

NMEA (National Marine Electronics Association) is the protocol used by GPS receivers.

Data in the messaging protocol is transmitted in 'strings' or 'sentences' from one 'talker' (e.g. a GPS receiver) to multiple 'listeners' (e.g. a PC). The GPS receiver would be local, generally attached to the CSAS user's vehicle, and be connected, via USB or Bluetooth, to a CSAS laptop:



All NMEA sentences start with the '\$' sign, and end with a carriage return and a line feed; each data field in the sentence is separated with a comma. For example, NMEA message "\$GPGGA,181908.00,3404.7041778,N,07044.3966270,W,4,13,1.00,495.144,M,29.200,M,0.10,0000*40" can be read as:

Part of NMEA Message	Description
GP	Defines a GPS position (GL would denote GLONASS)
181908.00	Timestamp (UTC in hours, minutes, and seconds)
3404.7041778	Latitude in DDMM.MMMMM format
N	Denotes North latitude (S denotes South of the equator)
07044.3966270	Longitude in DDDMM.MMMMM format
W	Denotes West longitude (E denotes East of the meridian)
4	Quality indicator (precision)
13	Number of satellites used to define the coordinate
1.00	Horizontal dilution of precision (HDOP)
495.144	Altitude of the GPS antenna
M	Unit of altitude (meters or feet)
29.200	Geoidal separation
M	Unit of the geoidal separation (meters or feet)
1.0	Age of the correction (if any)
0000	Shows the correction station ID (if any)
*40	A checksum

Setting up Live GPS Import

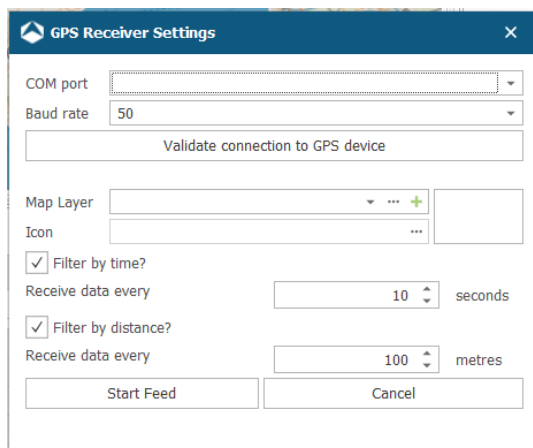
To setup live import of GPS tracker data directly into CSAS and see this data on a map, do the following:

Stepped Procedure

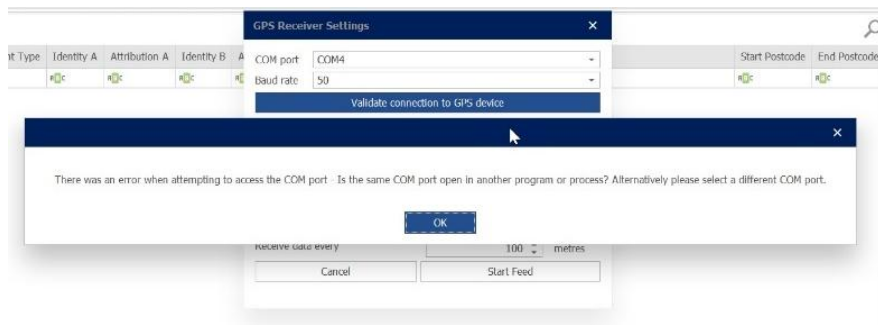
1. Connect a suitable GPS receiver to the USB port on your CSAS laptop. Alternatively, you can connect via Bluetooth. Any receiver that generates standard NMEA data should be compatible.
2. Login to CSAS.
3. Open the relevant CSAS case.
4. Open 'Case Hub'.
5. From 'Case Hub', go to the map. At the top of the map there is a ribbon with buttons:



6. Click the  icon on right side of the ribbon. The 'GPS Receiver Settings' window opens:

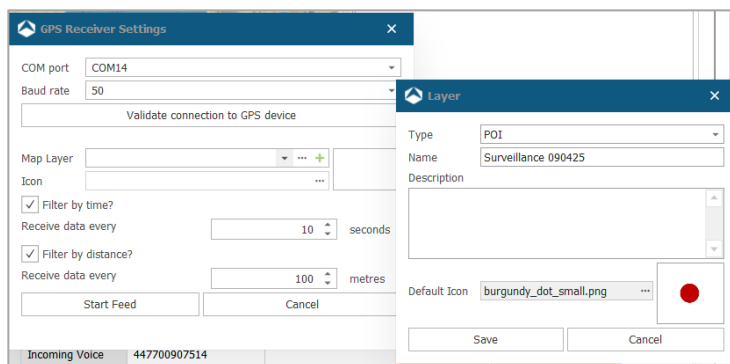


7. From the 'GPS Receiver Settings' window:
 - Select the necessary 'COM port'. For example 'COM3', 'COM4' etc.
 - Select the necessary 'Baud rate', this setting determines the speed of communication over the data channel i.e. the number of symbols per second. The GPS receiver's baud rate will be stated in the equipment's user manual, but a typical value for this would be 115200.
 - Click the 'Validate connection to GPS device' button. If the connection was not validated, for example an error accessing the chosen COM port, you will see the following pop-up message:



If necessary, select another COM port or contact CSAS Support for advice.

8. Select the necessary 'Map Layer'. If, for example, you select 'Default GPS layer', the 'Filter by time?' and 'Filter by distance?' checkboxes are automatically selected:



Note: If you want to create a new mapping layer, see Creating a New Mapping Layer.

9. If necessary, adjust the time filter by clicking the 'Filter by time?' checkbox and then using the up / down arrows. This reduces the amount of data generated by only capturing a GPS fix at the stated interval rather than once every second.
10. If necessary, adjust the distance filter by clicking the 'Filter by distance?' checkbox and then using the up / down arrows. This reduces the amount of data generated by only capturing a GPS if the receiver has moved more than a minimum distance since the last capture.

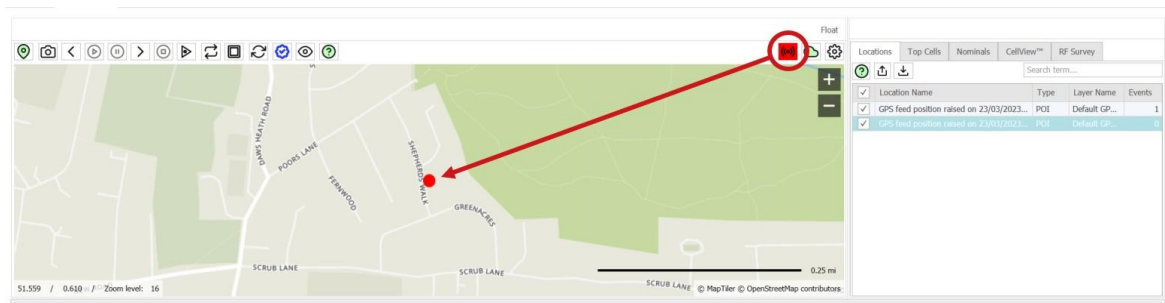
Starting Live GPS Import Feed

Start the live GPS import feature as follows:

Stepped Procedure

1. Click the **Start Feed** button. Recording starts. You will see a status update message:
 - 'Checking for data...'
 - 'Data being received...' or 'Data not being received – check connection or try another port...'
 - 'Data being fed back...'
2. When you start the live feed, the data being send back is **automatically recorded**, and the  icon flashes red. As the data is recorded it is shown on the

map and you will see the locations panel start to populate:



Depending on how your settings are configured, on the map, you can see:

The POI Location:

- » Latitude
- » Longitude.

The POI Event:

- » Date
- » Time
- » Type (GPS)
- » Event description (full NMEA string).

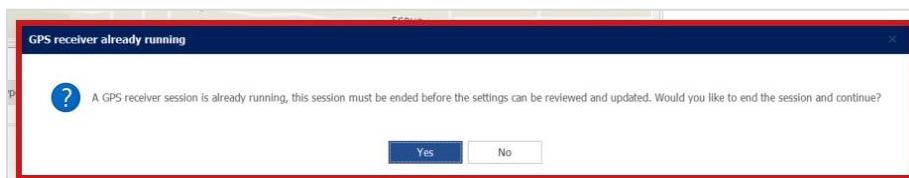
When you have captured the data required, you can stop the live GPS feed by clicking the  icon. The data is saved to Case Hub, based on your selected time and distance settings.

Recording more than One Live GPS Feed

Only one live GPS feed can be activated at a time - CSAS will NOT permit a second live feed as two feeds cannot run simultaneously. To start a second live feed, you have to cancel the first and then start another.

Losing the Live GPS Feed

If the feed is lost for 30 seconds or more, a live feed warning is displayed:



If the feed is lost, you elect to:

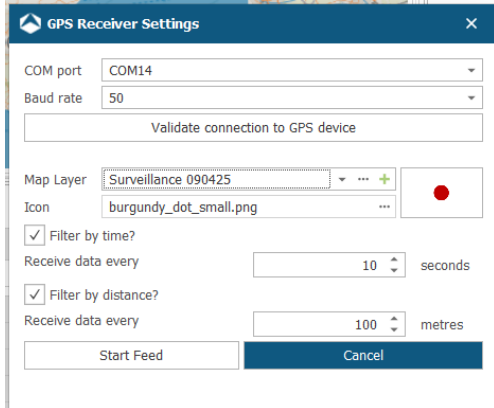
- » Close - the live feed is stopped and the data which have been captured is shown on the map.
- » Wait - another 30 seconds for the feed to reconnect, after which another Live Feed Warning pop-up is displayed.
- » Manage feed - you will be directed to the 'GPS Receiver Settings' pop-up window to review and amend the feed details.

Cancelling a Live GPS Feed Recording

You can cancel a live GPS feed recording as follows:

Stepped Procedure

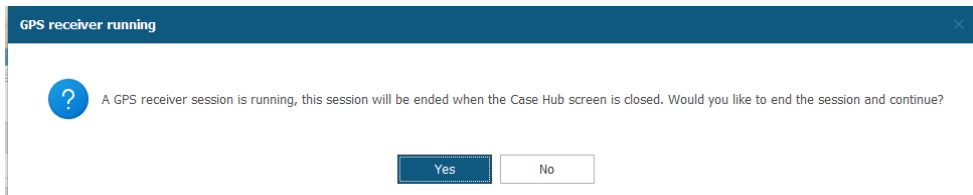
1. From the 'GPS Receiver Settings' window, click the **Cancel** button:



2. The recording stops.

Closing Case Hub During a Recording

If you are recording live GPS data and want to close Case Hub, the recording is stopped. If you decide to close Case Hub the following warning message is displayed:



Select 'No' to stay in Case Hub. Select 'yes' to stop the live GPS data recording and close Case Hub.

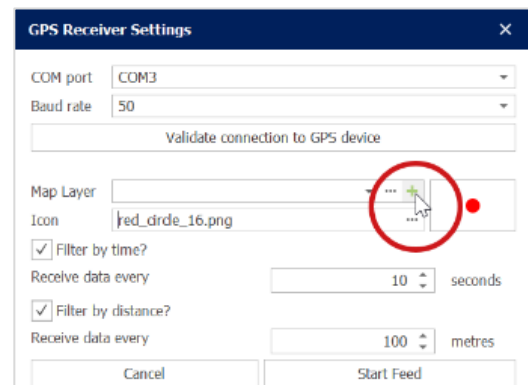
Creating a New Mapping Layer

If you wish to, you can create a new map layer with a new name for each individual GPS feed. Once the new map layer has been created, new data is added to it as it is received, and the map is updated.

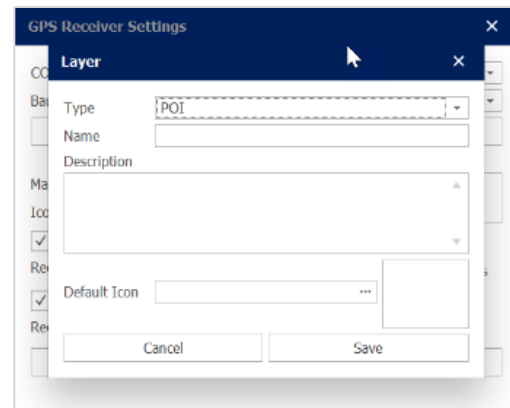
Create a new map layer as follows:

Stepped Procedure

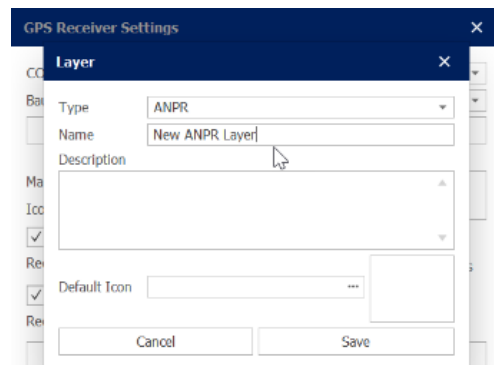
1. From the 'GPS Receiver Settings' window, click the '+' button:



2. The 'Layer' window opens:



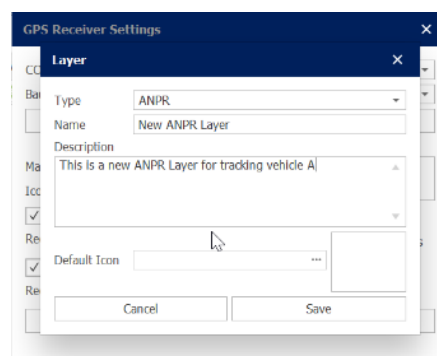
3. From the 'Layer' window:
 - Select the Type of Layer you want:
 - Enter a name for the new Layer:



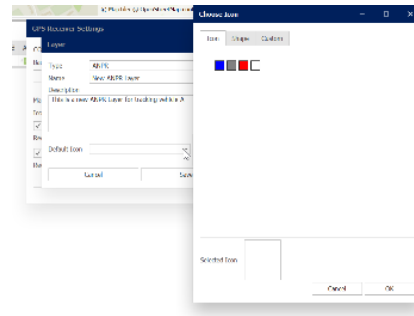
4. If you enter a name which has already been used, the following message is displayed.



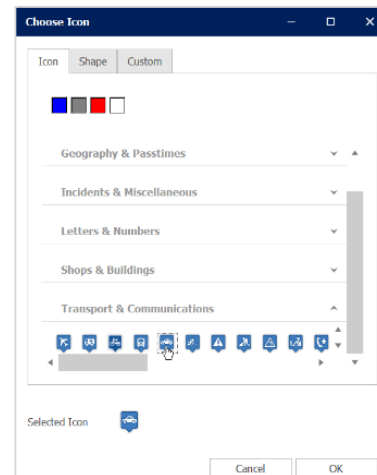
5. Enter a Description for the new Layer:



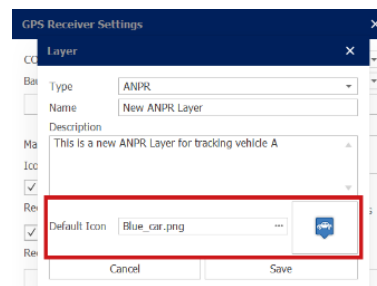
- Choose or create a Custom icon to display on the map:



- In this example, a blue car icon has been selected. Your selection is confirmed in the 'Layer' window:



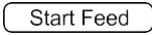
- The new layer is complete and has a layer name and an icon assigned to it.



Starting an Existing Live Feed

You can open an existing live feed and add new data to it.

Stepped Procedure

- Start the GPS tracker.
- Click the  icon on the right-hand side of the map ribbon. The 'GPS Receiver Settings' window opens.
- From the 'GPS Receiver Settings' window, select the existing live feed to start.
- From the 'GPS Receiver Settings' window, click the 'COM port' drop-down menu and select a different port.
- From the 'GPS Receiver Settings' window, click the 'Map Layer' drop-down menu and select a different map layer to add to the existing live feed.
- From the 'GPS Receiver Settings' window, click the  button. Recording starts.

Note: When you click button, the new data is shown with the existing data on the same map.

Overlaying GPS Data with an Existing Live Feed or Other Datasets

You can overlay new GPS receiver data with an existing map layer so you can see the GPS dot trail selected for the existing live feed overlaid against other data imported into the case, such as cell site locations. Simply select the other data types to be viewed in the map in the normal way before starting the GPS trail function.

Filters created within Case Hub

The GPS trail data captured by CSAS consists of a set of locations (the GPS coordinates of each capture) and events (the date & time of each capture), which means that the captured data is available to be filtered using the standard CSAS right sidebar filters.

Once you have captured the live GPS feed data required, then within Case Hub, you can select how much of that data you want to view on the map.

14.6.16 Device Location Visualisation

All cellular networks support a set of 'location-based services' (or LBS); these are enabled by a variety of technologies that are able to identify the current location of a specific mobile device with varying degrees of accuracy. The simplest forms of LBS can report details of the cell that a subject device is currently using and the accuracy of these methods vary widely depending on the type and size of cell. Other more complex methods use triangulation techniques to identify a device's location with an accuracy of less than 150m.

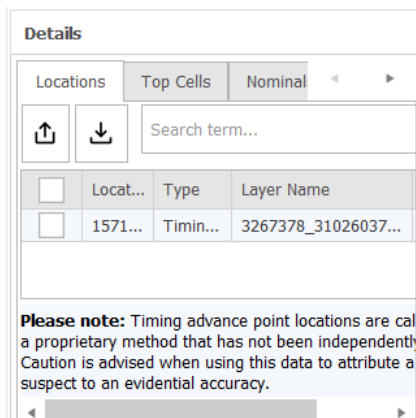
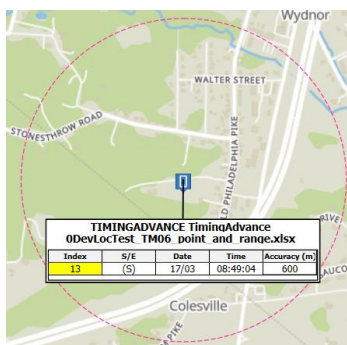
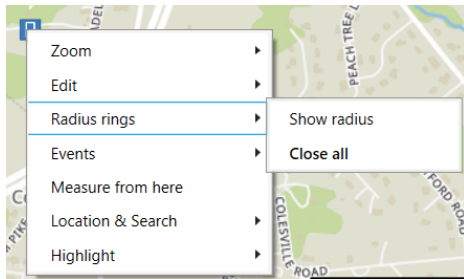
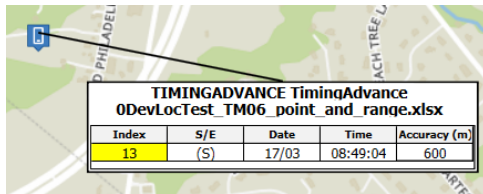
In some jurisdictions, notably the USA, law enforcement agencies are able to request location information for suspect devices and receive disclosures from cellular providers that are colloquially known as 'ping' data.

There are multiple techniques used by the networks to gather this data, but they can be generically grouped under the headings of 'ping' data (also sometimes known as SHIELD data), which identifies a point location for the searched for device, and 'timing advance' data, which indicates the approximate area where the device is located in relation to a cell site or tower. Ping data is generally only available as a 'forward facing' disclosure, in the sense that ping data isn't captured for a device until the agency submits a request, meaning that it isn't available historically. Timing advance data, although it is usually less exact than ping responses, is available historically and can be used to determine a device's approximate location at points in the past. Both ping and timing advance files are loaded into CSAS via the usual Import Files process.

US cellular carriers provide ping data in two formats – immediate, individual ping responses are often provided via email, with the ping coordinates contained within the text of the email; currently, users are required to copy/paste the content of the email to get it into CSAS using the [Import Files > File Import Wizard > Device Ping Email](#) feature. When multiple ping responses are requested, covering an extended period, carriers also disclose ping responses in a file format, which can be imported into CSAS via the normal Import Files process. Some file formats contain both ping and timing advance data for the same phone.

Ping Data

The device location data provided in 'ping' disclosures (also sometimes known as SHiLD or Specialised Historical Location data) provide point coordinates for the device's location along with an 'accuracy' radius; this type of location data isn't saying 'the phone was here' (referring to the point coordinates), it's saying 'the phone was somewhere in an area with this radius centred on this point'.



CSAS maps the point location for each ping result as a POI (Point of Interest) location.

Left clicking on a ping icon activates a POI label that shows the date and time of each location event plus the accuracy radius.

Right-clicking on a ping icon activates the POI context menu, which has an additional 'Radius rings' option.

Select 'Show radius' to view the accuracy radius rings and 'Close all' to close any open rings.

The fully activated visualisation provides an indication of the area the subject device was estimated to have been within at the stated time.

Ping, point location or SHiLD data is not generally regarded as necessarily being accurate. Some practitioners prefer not to use it in evidence, so in CSAS, for location data that is included in the same file as timing advance data (in T-Mobile and AT&T TA files, for example) this type of data is hidden by default and is only displayed if the corresponding checkbox in the Case Hub Details panel is checked.

Timing Advance Data

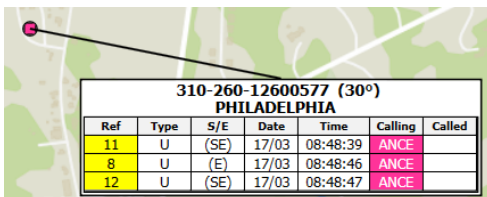
The timing advance process is used within cellular networks to allow the base station to continually measure the current delay experienced by messages travelling between it and each phone it's currently managing – the phone's distance from the tower can be inferred from the measured delay. Timing advance commands are then sent to each phone at regular intervals (up to several times per second) instructing it to adjust the time at which it transmits the bursts of data it sends to the base station; as a phone gets further away from the base station (delay increases) it is instructed to start transmitting bursts earlier (advancing them in time) to overcome the delay experienced by the data as it travels to the base station; as the phone gets closer to the base station it is instructed to retard its transmission time to reflect the reduced delay.

Timing advance measurements are being taken continuously when a phone is connected to a base station, in most networks however, these measurements are regarded as being 'ephemeral' data, they are calculated by the base station but are not usually captured or stored anywhere. In some jurisdictions, such as the USA, timing advance measurements taken by base stations are captured and are stored alongside the CDR data that is available for disclosure to law enforcement agencies.

Unlike ping data, which only becomes available after a lawful request has been made to start tracking a phone's location, timing advance data can be available historically and offers an enhanced method for determining a subject device's historical location.

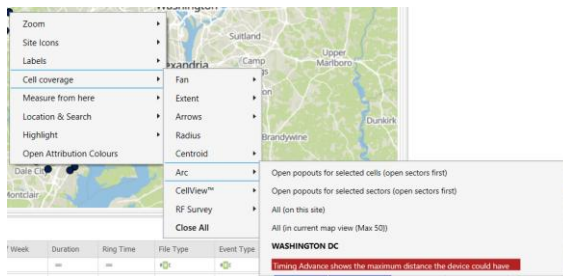
Each timing advance disclosure shows the subject device's approximate distance from the serving cell site or tower at the stated time (inferred from the delay experienced by the device's transmissions). Timing advance (TA) doesn't offer a precise measurement of distance; it instead provides measurements that are organised into 'bands'. Different technologies have different sized bands – 2G GSM networks, for example, report TA distance in bands that are each 550m deep, whereas 4G networks report TA distance in bands that just 78m deep and 5G has a number of configurations with band options of 78m, 39m and 19m. TA therefore isn't offering an exact measurement of the device's distance from the reporting tower; it's instead reporting the approximate arc or area within which the device was likely to have been located.

It should be noted that a device's actual distance from the tower and the distance inferred by Timing Advance may differ. TA is calculated based on delay – factors such as tower/antenna height and whether the device has clear line of sight to the tower can affect delay and therefore affect the distance calculated by TA. A device can be closer to the tower than TA data indicates but is unlikely to be further away than the outer edge of the TA band.



310-260-12600577 (30°) PHILADELPHIA						
Ref	Type	S/E	Date	Time	Calling	Called
11	U	(SE)	17/03	08:48:39	ANCE	
8	U	(E)	17/03	08:48:46	ANCE	
12	U	(SE)	17/03	08:48:47	ANCE	

TA reports show location in relation to the reporting cell site or tower; CSAS shows tower locations in the usual way on the map. Cell sites and arcs take on the subject phone's attribution colours.



The timing advance arcs associated with the cell site can be viewed via the right-click menu using the Cell Visualisation > Arc options.

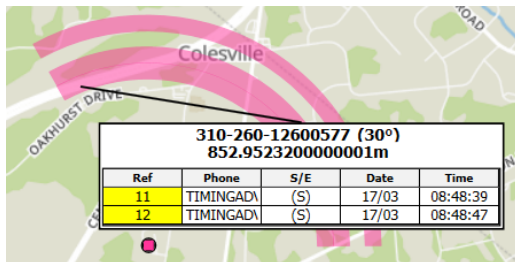
Clicking on a cell ID in the list activates the TA arcs associated with that cell.

It is also possible, from the same menu, to activate all arcs on the same site and all arcs on all sites that are currently viewable on the map (up to a maximum of 50 sites).



Each arc extends across the area that the cell is assumed to cover, based on the stated azimuth and the assumed sector arc, which defaults to 120°.

If multiple TA events have been presented for the same cell, multiple arcs will be displayed.



Left clicking on an individual arc activates a popup label that shows details of the TA events that have been reported within the selected TA band distance, showing the date/time of each event and the band distance.

Individual timing advance arcs can be shown on their own by applying appropriate date/time filters to the map.

Both ping and timing advance data provide device location information which have a variable degree of accuracy, sometimes better accuracy can be obtained by overlaying details of multiple location events that happened in quick succession.



In this example, there were two timing advance events within 30 seconds of each other with TA arcs that just overlapped (in an area just to the north of Oakhurst Drive). There was also a ping location events at around the same time that had a 600m accuracy radius.

By overlaying the intersecting TA arcs and the ping data it is possible to provide a more exact estimate of the subject device's location at that time.

Some providers (T-Mobile and Verizon, for example) disclose TA data as a set of distances. This can be interpreted as the distance from the used tower to the inner edge of the associated TA band. These distances are disclosed in imperial units (miles, to two decimal places) and must be converted to metric to determine the appropriate TA band.

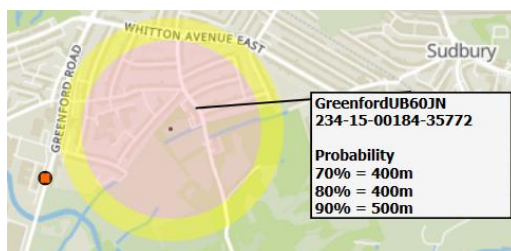
The conversion process entails a degree of rounding error, so CSAS converts the imperial distances to the closest metric band distance before displaying that data, meaning that there may be a small apparent discrepancy between the stated distance in the source file and distance displayed on the map – CSAS is correcting the rounding error rather than introducing an error of its own in these circumstances.

14.6.17 Centroids

Mathematically, a 'centroid' is the centre or 'arithmetic mean' of a shape or area, in cellular networks the term is used to indicate the predicted centre of a cell's coverage area.

Most cellular networks provide estimated cell coverage indications in the form of an azimuth, which indicates the direction in which a cell's antenna is facing. Some networks, including Vodafone UK, also provide centroid details for their cells and the azimuth and centroid data can be used to draw different conclusions about the coverage area of a cell and the likely locations of any phones using that cell.

The centroid data provided by Vodafone, as an example, consists of a point location (based on map coordinates) which represents the centre of the area within which the associated cell is predicted to offer the best or most attractive coverage. There are then a set of three radius values that are associated with probabilities that a phone using that would have been located within one of those radius areas.

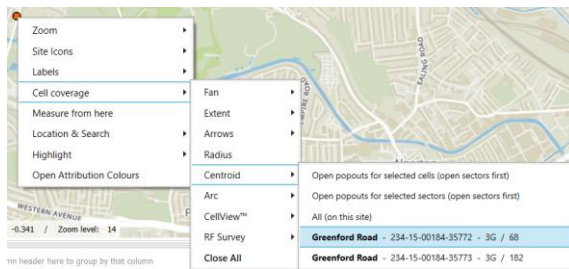


In this example, the data is indicating that the centre of the coverage area of cell 35772 transmitted by the Greenford site is in an area a few hundred metres to the north-east of the site (represented by the dot at the centre of the concentric circles)

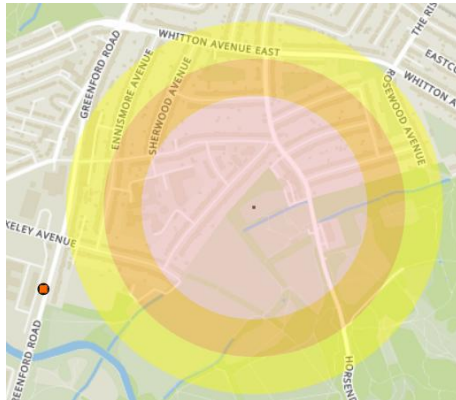
The concentric circles represent the probability radius values – indicating that is a 90% probability that a phone using that cell would have been located within the largest circle (500m in radius from the centroid point), and lower probabilities of a phone having been within one of the smaller radius areas (of 400m).

Centroids do not offer proof of a cell's actual coverage area and are not considered to be an alternative to a forensic RF survey for establishing a cells' serving footprint, instead they provide a further indication of the predicted coverage area of a cell and are designed to offer a suggested starting point for any searches conducted that are looking for the user of a phone that has connected to that cell.

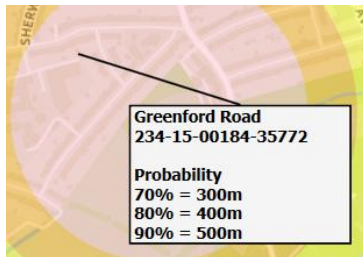
If a source CDR contains centroid data, it can be displayed on a CSAS map.



A cell's centroids can be viewed via the cell site right-click context menu Cell Coverage > Centroid > select cell ID.

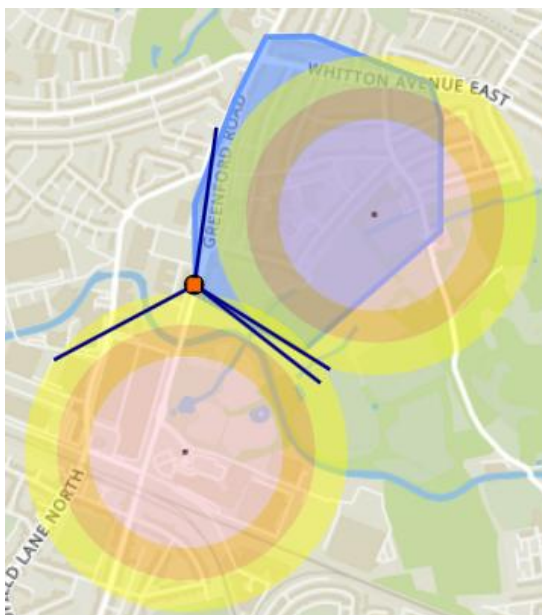


The centroid for an individual cell will be displayed as a set of three concentric rings, conforming to the probability radius values provided in the source data.



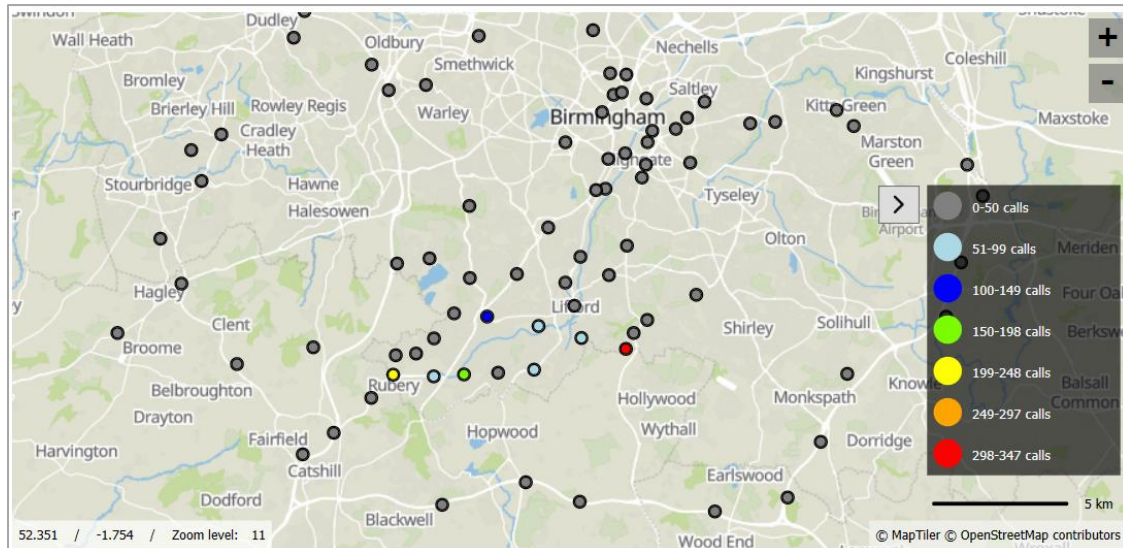
Clicking anywhere within the centroid rings activates an information popup, which confirms the cell and site details and provides values for that centroid's probability radius values.

The centroid visualisation can be overlaid with other cell coverage visualisation types, such as sector fan or extent arms, or if CellView data is available for the cell that can also be overlaid.



14.6.18 Heatmap Mode

Heatmap mode is a site icon choice option (see [Cell Site Icons](#)). When selected, the map shows cell site locations as coloured discs, but the colouring of the discs is based on the level of usage rather than on attribution colour.



Cells with higher levels of usage are shown with 'hotter' colours, those with lower levels are shown using 'cooler' colours.

When Heatmap Mode is activated, a key or legend panel appears on the right of the map, this shows the usage levels (i.e. the call count) that equate to each colour. The correlation is recalculated whenever the current dataset is updated, so the key always reflects the proportions for the current data.

The key can be dismissed by clicking on the small grey arrow to the top right of the box and can be revealed again by clicking on the same arrow. The key is included if the map is exported to PowerPoint.

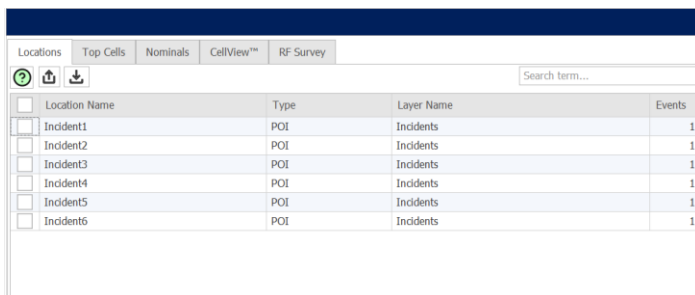
14.7 Using the Details Panel

Next to the Grid, there is a pane from which you can select the following tabs/controls:

- » Locations
- » Top Cells
- » Nominals
- » CellView
- » RF Survey

14.7.1 Locations

Locations, both ANPR and POI, from the currently selected set of files and layers, are displayed in the 'Locations' tab:

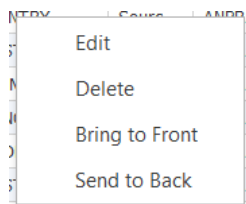


Location Name	Type	Layer Name	Events
☐ Incident1	POI	Incidents	1
☐ Incident2	POI	Incidents	1
☐ Incident3	POI	Incidents	1
☐ Incident4	POI	Incidents	1
☐ Incident5	POI	Incidents	1
☐ Incident6	POI	Incidents	1

The 'Locations' grid shows the name of each location, its type (ANPR or POI), the File or Layer it belongs to and the number of events that each Location has associated with it.

Note: You can hide/unhide a Location on the map by checking/unchecking the necessary checkbox against the Location Name.

You can export and import location data using the buttons at the top of the Locations tab.



The Locations tab supports a right-click menu function. You can Edit the selected Location (which launches the Edit POI popup), Delete the Location (which is not reversible) and can send the Location icon to the back (further away from the viewer) or bring it to the front.

The Locations tab will also include one or more rows for each Timing Advance file that is loaded into the map, if that TA file also includes point location data (as per T-Mobile and AT&T formats). The Location table row offers the option to show or hide the point locations in the map, as they are generally regarded as not being evidentially accurate. Check the row to see the associated point locations on the Case Hub map.

14.7.2 Top Cells

This tab provides you with analytics information of the top N cells (ranked by number of events) in the selected case data. If the data in the 'Case Hub' grid gets filtered, clicking the  button within the 'Top Cells' tab refreshes the data to show the 'Top Cells' in the current dataset:

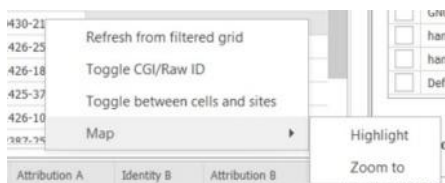
Locations	Top Cells	Nominals	CellView™	RF Survey
Display Top	10	Search Term	☒ Cells ☐ Sites	
Cgi	Site Name			
234-10-07187-31692	HOLLYWOOD			
234-10-21429-17365	BURNHAM-ON-SEA TA82DE			
234-10-21429-31279	Highbridge TA94JU			
234-10-30430-21741	BURNHAM SEAFRONT			
234-10-21426-25378	NORTHFIELD B312JR			
234-10-21426-18637	LONGBRIDGE B314JP			
234-10-21425-37842	DRUIDS HEATH B145LQ			
234-10-21426-10894	RUBERY B459RU			
234-10-07187-31692	WIMBORNE WEST			

The list is restricted by default to show the top 10 cells/sites, but by selecting from the drop-down in the tool bar, can be expanded all the way up to 'All' cells/sites.

Note: In large cases it's recommended to keep this setting at 10 to avoid a performance drag on the grid when the list is refreshed.

The 'Cells' and 'Sites' radio buttons toggle the list from showing the top cells (based on individual cell IDs) to top sites (based on site name). The 'search' box allows you to search for a specific cell or cell ID.

A right-click option allows you to:



- » Refresh the data.
- » Toggle between cell ID formats (raw and CGI).
- » Toggle between cell ID and site name.
- » Select a site and highlight it or zoom the map to focus on it.

14.7.3 Nominals

The Nominals tab lists the attributed nominals in the case and provides an indication as to whether each of those nominals has active events in the current dataset.

The Nominals tab provides a quick way of understanding which significant nominals were active at different points in time during the period covered by a case. The grid shows, for each nominal, their name, the set of identifiers that are associated with them and the count of events in the current dataset:

Locations	Top Cells	Nominals	CellView™	RF Survey
☒ Targets	☒ Non-Targets	☐ Include Inactive		
Name	Identifier	Filtered Events		
Dessi Khan	07700902421, 07700907268	205		
Jim Smith	07700902421	285		
Jorden Miller	07700905100	1		
Unknown 2	07700903852	5		

Using the checkboxes, the Nominals grid can be filtered to show 'Target' nominals and/or

'Non-Target' nominals; it can also be set to include or exclude details of nominals who are not active in the current dataset – e.g. if the 'Case Hub' data is filtered to cover just one day and the nominal, for example 'Jorden Miller', has no call records on that day, he would be regarded as being 'inactive' in the current dataset.

Stepped Procedure

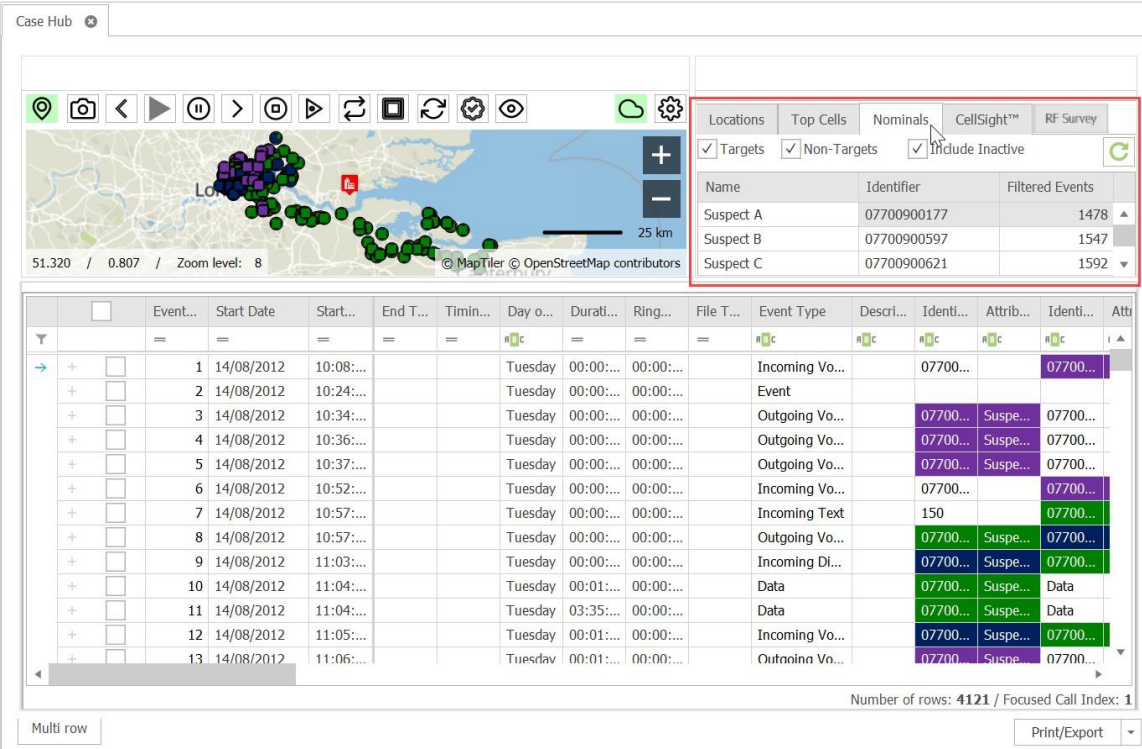
The following stepped procedures are broken down into:

- Filtering the grid to the required dataset.
- Refreshing the Nominals panel.

Filtering the Grid to the Required Dataset

From the sidebar, click the  icon then from the 'Filters' panel, select the necessary source data files and prefilters from 'Source data', 'Date & Time', 'Locations' and 'Event types' panels using the drop-down menus, checkboxes and radio buttons and click on the **Apply** button; the data grid populates:

Note: Nominal(s) which have previously been attributed within the selected dataset are listed in the Nominals details panel:



The screenshot shows the CSAS Case Hub interface. At the top, there's a 'Case Hub' tab. Below it, a map displays a cluster of green and purple location markers. To the right of the map is a 'Filters' panel with tabs for 'Locations', 'Top Cells', 'Nominals', 'CellSight™', and 'RF Survey'. The 'Nominals' tab is active, showing checkboxes for 'Targets' (checked), 'Non-Targets' (checked), and 'Include Inactive' (checked). Below these is a table of filtered events:

Name	Identifier	Filtered Events
Suspect A	07700900177	1478
Suspect B	07700900597	1547
Suspect C	07700900621	1592

Below the filters is a large data grid with columns: Event..., Start Date, Start..., End T..., Timin..., Day o..., Durati..., Ring..., File T..., Event Type, Descri..., Identi..., Attrib..., Identi..., and Att. The grid contains 13 rows of data, each representing an event. At the bottom right, it says 'Number of rows: 4121 / Focused Call Index: 1'. There are also buttons for 'Multi row' and 'Print/Export'.

Refreshing the Nominals Panel

If any changes are made to the filtered data set, you can refresh the nominals 'Details' panel by clicking either the  button located to the right of the panel or the **Apply** button from the bottom of the 'Filters' panel.

14.7.4 CellView

Note: CellView is an optional feature and requires an additional licence to activate it. If you don't have a licence and you are authorised to get one, ask your CSAS administrator for a Licence Code. To add a licence, see About/Licensing.

Note: CellView data is not evidential and is for intel use only.

If licensed, this feature gives you access to crowd-sourced cell coverage data, that when plotted on a map can provide a realistic indication of the coverage area of each cell:

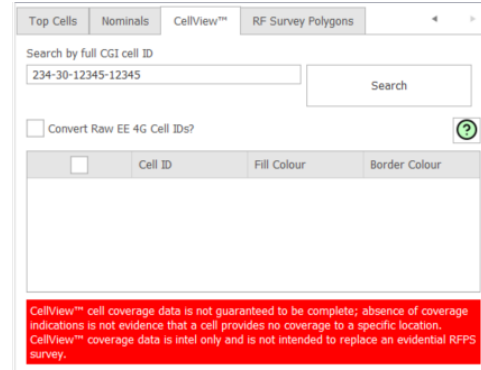


The panel provides a view of all 'CellView' cell coverage polygons that are currently available in the map and offers the opportunity to show/hide and recolour coverage polygons. There's also an option to search for additional cells' coverage areas.

Please see [Using CellView](#) for more details of this feature.

CellView coverage details can be displayed on a CSAS map by selecting the CellView option from a cell site right-click menu's cell coverage option. Alternatively, the CellView tab allows you to search for CellView data, where available, linked to a particular cell by entering the necessary CGI cell ID you want to display on the map.

From the Details Panel, when you click on the CellView tab, a panel with a search field is displayed into which you can enter the necessary CGI cell ID you want to show on the map:



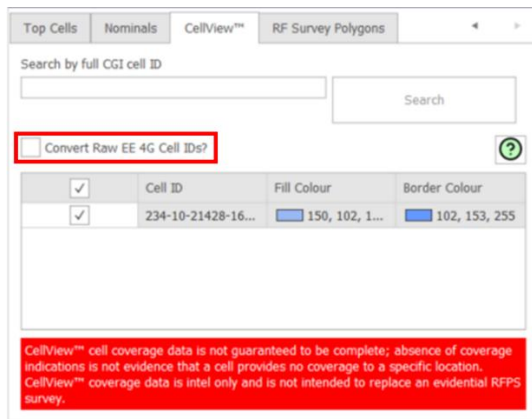
Note: The CellView database is not comprehensive and some cell ID searches may not result in cell coverage details being provided.

You must enter the Cell ID in one of the following formats:

- » MCC-MNC-LAC/TAC-CID
- » MCC-MNC-ECI/NCI

Clicking the button creates a list of matching Cell IDs for you to choose from, if any cells in the CellView database match the ID you entered. Selected cell IDs are listed in the grid with a randomly assigned Fill Colour and a Border Colour, which are used to colour the polygon that represents the cell's coverage on the map.

The 'Convert Raw EE 4G Cell IDs?' checkbox option is intended to be used for the UK EE 4G cell network, as they have a non-standard format for 4G/5G cell IDs:



Top Cells | Nominals | CellView™ | RF Survey Polygons

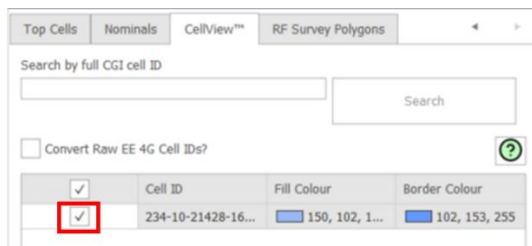
Search by full CGI cell ID

☐ Convert Raw EE 4G Cell IDs?

	Cell ID	Fill Colour	Border Colour
☒	234-10-21428-16...	150, 102, 1...	102, 153, 255

CellView™ cell coverage data is not guaranteed to be complete; absence of coverage indications is not evidence that a cell provides no coverage to a specific location. CellView™ coverage data is intel only and is not intended to replace an evidential RFPS survey.

Selecting the checkbox forces CellView to toggle between formats in the event that an EE 4G/5G cell ID isn't recognised, and to interpret 4G/5G cells beginning with '234-30' using the specific EE 4G/5G cell ID format.



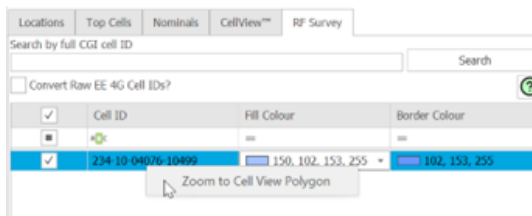
Top Cells | Nominals | CellView™ | RF Survey Polygons

Search by full CGI cell ID

☐ Convert Raw EE 4G Cell IDs?

	Cell ID	Fill Colour	Border Colour
☒	234-10-21428-16...	150, 102, 1...	102, 153, 255

You can turn on/off each Cell ID for which CellView data is being displayed in the map using the checkbox against each search result:



Locations | Top Cells | Nominals | CellView™ | RF Survey

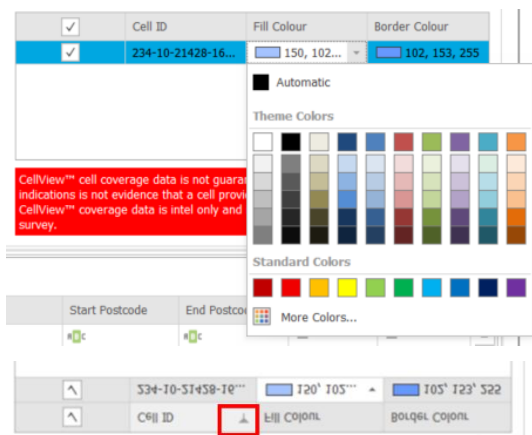
Search by full CGI cell ID

☐ Convert Raw EE 4G Cell IDs?

	Cell ID	Fill Colour	Border Colour
☒	234-10-04076-10499	150, 102, 153, 255	102, 153, 255

Zoom to Cell View Polygon

You can zoom to the cell coverage displayed in the map by right-clicking over the Cell ID you want to zoom to:



	Cell ID	Fill Colour	Border Colour
☒	234-10-21428-16...	150, 102...	102, 153, 255

CellView™ cell coverage data is not guaranteed to be complete; absence of coverage indications is not evidence that a cell provides no coverage to a specific location. CellView™ coverage data is intel only and is not intended to replace an evidential RFPS survey.

Start Postcode: End Postcode

Cell ID: Fill Colour: Border Colour:

You can select a different Fill Colour and Back Colour for the cell coverage visualisation using the drop-down menus:

You can filter the search results in the grid using the filter control in the 'Cell ID' column.

Please note that CellView cell coverage data should only be used for intel purposes, it should not be used as evidence of a cell's coverage area. The CellView tab includes the following warning text:

CellView™ cell coverage data is not guaranteed to be complete; absence of coverage indications is not evidence that a cell provides no coverage to a specific location. CellView™ coverage data is intel only and is not intended to replace an evidential RFPS survey.

14.7.5 RF Survey

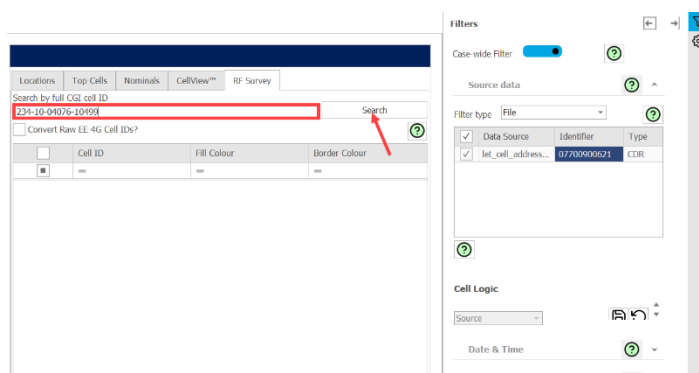
The CSAS RF Survey tab is activated when the optional RF Survey Module add-on is licensed for CSAS v3. If you don't have one and you are authorised to get one, ask your CSAS administrator for a Licence Code. To add a licence, see *About/Licensing*.

Once activated, the RF Survey Module add-on can be used to import raw survey data from a variety of popular forensic survey devices. Evidential cell coverage data, gained from imported RF Survey data, can be viewed in Case Hub maps – details of activated RF Survey coverage visualisations are displayed in the RF Survey tab.

Detailed information about what the RF Survey Module does and how it does it is given in the CSAS v3 RF User Guide. Details information about the use of RF Survey in Case Hub is provided in the [RF Survey](#) section.

RF Survey coverage details can be displayed on a CSAS map by selecting the RF Survey option from a cell site right-click menu's cell coverage option. Alternatively, the RF Survey tab allows you to search for RF Survey data, where available, linked to a particular cell by entering the necessary CGI cell ID you want to display on the map.

From the Details Panel, when you click on the 'RF Survey' tab, a panel with a search field is displayed into which you can enter the necessary CGI cell ID you want to show on the map:



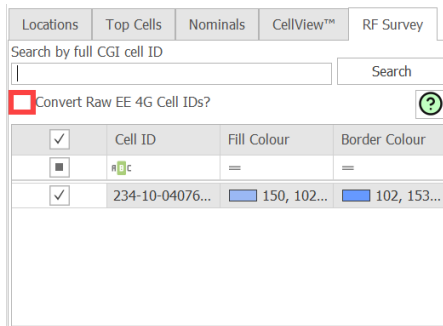
Note: You can only use this feature if RF Survey coverage data is available in your case.

You must enter the Cell ID in one of the following formats for search to be possible:

- » MCC-MNC-LAC/TAC-CID
- » MCC-MNC-ECI/NCI

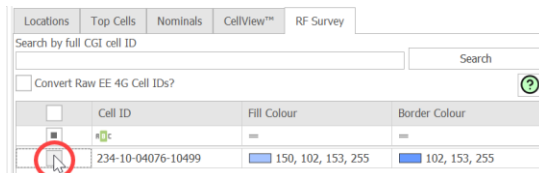
Clicking the button creates a list of matching Cell IDs for you to choose from, if any cells in the imported RF Survey data in the case match the ID you entered. Selected cell IDs are listed in the grid with a randomly assigned Fill Colour and a Border Colour, which are used to colour the polygon that represents the cell's coverage on the map.

The 'Convert Raw EE 4G Cell IDs?' checkbox option is intended to be used for the UK EE 4G cell network, as they have a non-standard format for 4G/5G cell IDs:



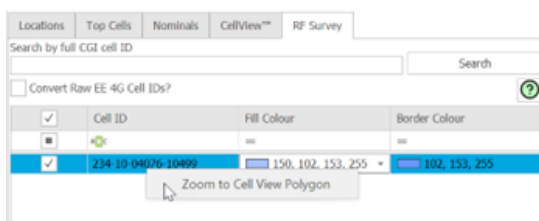
Cell ID	Fill Colour	Border Colour
234-10-04076-10499	150, 102...	102, 153...

Selecting the checkbox forces RF Survey to toggle between formats in the event that an EE 4G/5G cell ID isn't recognised, and to interpret 4G/5G cells beginning with '234-30' using the specific EE 4G/5G cell ID format.



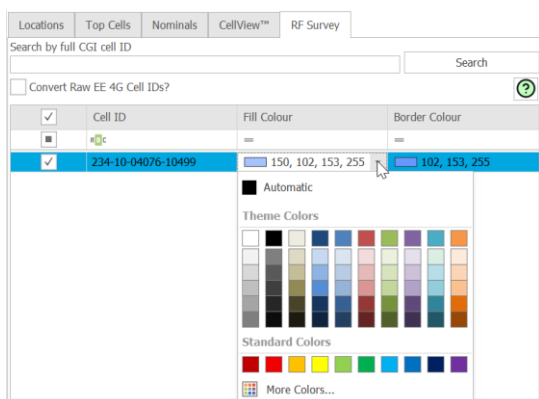
Cell ID	Fill Colour	Border Colour
234-10-04076-10499	150, 102, 153, 255	102, 153, 255

You can turn on/off each Cell ID for which RF Survey data is being displayed in the map using the checkbox against each search result:



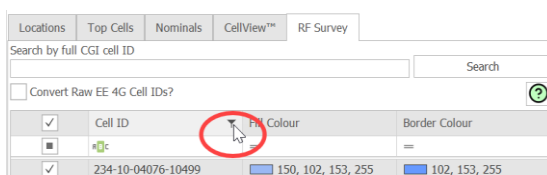
Cell ID	Fill Colour	Border Colour
234-10-04076-10499	150, 102, 153, 255	102, 153, 255

You can zoom to the cell coverage displayed in the map by right-clicking over the Cell ID you want to zoom to:



Cell ID	Fill Colour	Border Colour
234-10-04076-10499	150, 102, 153, 255	102, 153, 255

You can select a different Fill Colour and Back Colour for the cell coverage visualisation using the drop-down menus:

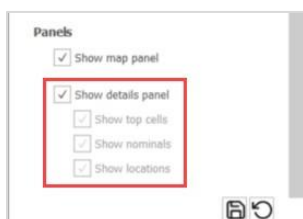


Cell ID	Fill Colour	Border Colour
234-10-04076-10499	150, 102, 153, 255	102, 153, 255

You can filter the search results in the grid using the filter control in the 'Cell ID' column:

14.7.6 Show/Hide Tabs

This function allows you to select which tabs are visible in the 'Details' panel. The checkboxes can be found in the 'Settings' sidebar, at the bottom of the 'Case Hub' panel:



Unticking a tab in the list removes it from the Details panel.

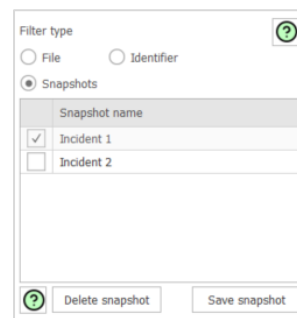
Note: Further tabs will be added over time as additional functionality is requested by users.

14.8 Using Case Snapshots

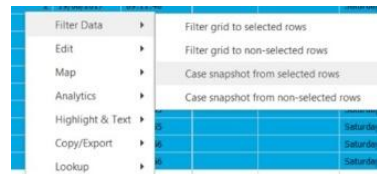
This function allows you to instruct CSAS to save the current dataset as a Case Snapshot, including all data currently selected to be viewed in the grid, plus any filters you've applied.

Case Snapshots are often used as way of saving a snapshot of case data that relates to a particular location, incident or time period. The Case Snapshot also saves the state of the map (if one is enabled) at the point where the snapshot was saved – this means that the map should reopen in the same state (i.e. same set of map objects in view and each object the same configuration) as when the snapshot was saved.

Case Snapshots can be saved, reviewed, reopened and deleted all from the Case Hub > Filters sidebar, in the 'Source data' section:



You can also save Case Snapshots from the Case Hub grid right-click menu:



You can also create a Case Snapshot within a CSAS map from the 'measure from here' and 'marquee select' controls:



Once it has been reopened, the data in a Case Snapshot can be exported via Case Outputs, Case Export and the other usual methods.

Why, When, Who



This function is necessary to create, edit, save and reopen a Case Snapshot. The intention is that if you save a Case Snapshot, when you reopen it, you will get back to the dataset in the same state it was in when you saved it, meaning you won't have to remember which source files and filter options you selected previously.



This function is undertaken whenever you want a snapshot of certain case details to revisit at another time.



This function is typically carried out by the following users:

» CSAS User

*Stepped Procedure****Saving a new Case Snapshot***

1. Compile your required dataset by selecting the appropriate source files and setting the necessary filters.
2. Trigger the saving of a new snapshot using one of the three methods outlined above:
 - Go to Filters sidebar > Source data > Snapshots and click 'Save snapshot'.
 - Go to Case Hub grid right-click menu > Save Snapshot section and look for your snapshot in the list.
 - Using the map's 'measure from here' or 'marquee select' features, click on the 'cog' icon in the popup label and select one of the filter options, then select the 'filter grid and create case snapshot' option.
3. Name and save your new snapshot by clicking the button. You'll be asked to provide a unique snapshot name (unique within the current case).

Open and use an existing snapshot

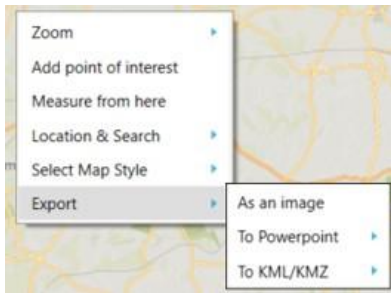
1. To reopen/edit/save a snapshot, go to Filters sidebar and scroll to the 'Source data' section, then select the 'Snapshots' option and look for your snapshot in the list.
2. To open the necessary snapshot, tick it's checkbox and click the button.

Delete a snapshot

1. To delete a snapshot, go to Filters sidebar and scroll to the 'Source data' section, then select the 'Snapshots' option and look for your snapshot in the list.
2. To delete a snapshot, tick it's checkbox and click the button. Any deleted snapshots are unrecoverable.
3. If data from the deleted snapshot was loaded in the Case Hub grid at the time, you may need to click the Reset or Apply buttons to clear the data from the grid before progressing.

14.9 Using Map Exports

This function allows you to export CSAS maps and content in a number of ways using the map background right-click menu 'Export' option drill-down:



14.9.1 Export As an image

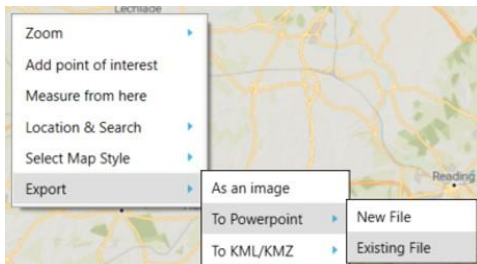
The 'export as an image' option provides an alternative method for saving a screengrab of the current map panel.

After selecting this option, you will be asked to select the 'save to' location for the screengrab. The image will be saved in .png format.

14.9.2 Export To Powerpoint

This option allows you to export the contents of the map to a Powerpoint slide in a selected file. This isn't simply a screengrab being exported, CSAS exports the map content along with the north arrow (if activated), the scale and the map copyright information, but it doesn't copy the zoom in/out buttons.

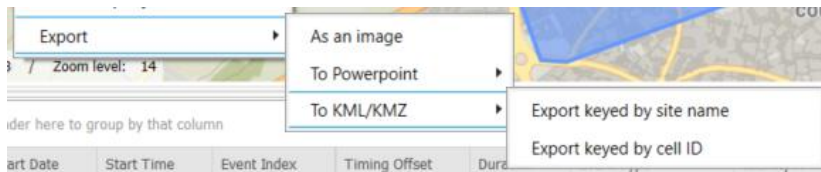
You can choose to send the data to a new Powerpoint file (which opens automatically) or to an existing file (which you can select):



This feature is designed to make the process of compiling a mapping presentation using CSAS simpler. It often works best if you create a preferred Powerpoint presentation template first, then make a copy of that template for each new case and export map data to it slide by slide as required.

14.9.3 Export To KML/KMZ

This option sends the current set of map objects and their details to a standard KML mapping file. KML is a widely used open format used to exchange map information between applications, allowing you to compile a map in CSAS and export it to view in another application (such as Google Earth).



When exporting to KML, you can choose what the key piece of identifying data for each location is, which has implications for how each location is labelled in the other mapping application, with options of:

- » Export keyed by site name – locations are identified by cell site, camera or POI name.
- » Export keyed by cell ID – cellular locations are identified by cell ID; other types of location continue to be identified by location name.

When triggered, the 'export to KML/KMZ' function asks where the exported file should be saved and then exports the data to a .kmz file.

The exported KMZ file is really just a zipped folder, that contains the KML file, itself containing the exported location and event data, plus any icons that were included in the original map, so they can be reproduced in another application.

☐ Name ^	Type
 ANPR1.png	PNG File
 doc.kml	KML File
 radiostation.png	PNG File

Why, When, Who



This function is necessary to export maps and their layers to create screengrabs, mapping presentations and to view in other applications.



This function is undertaken whenever mapping data needs to be reviewed, presented or viewed in other applications.



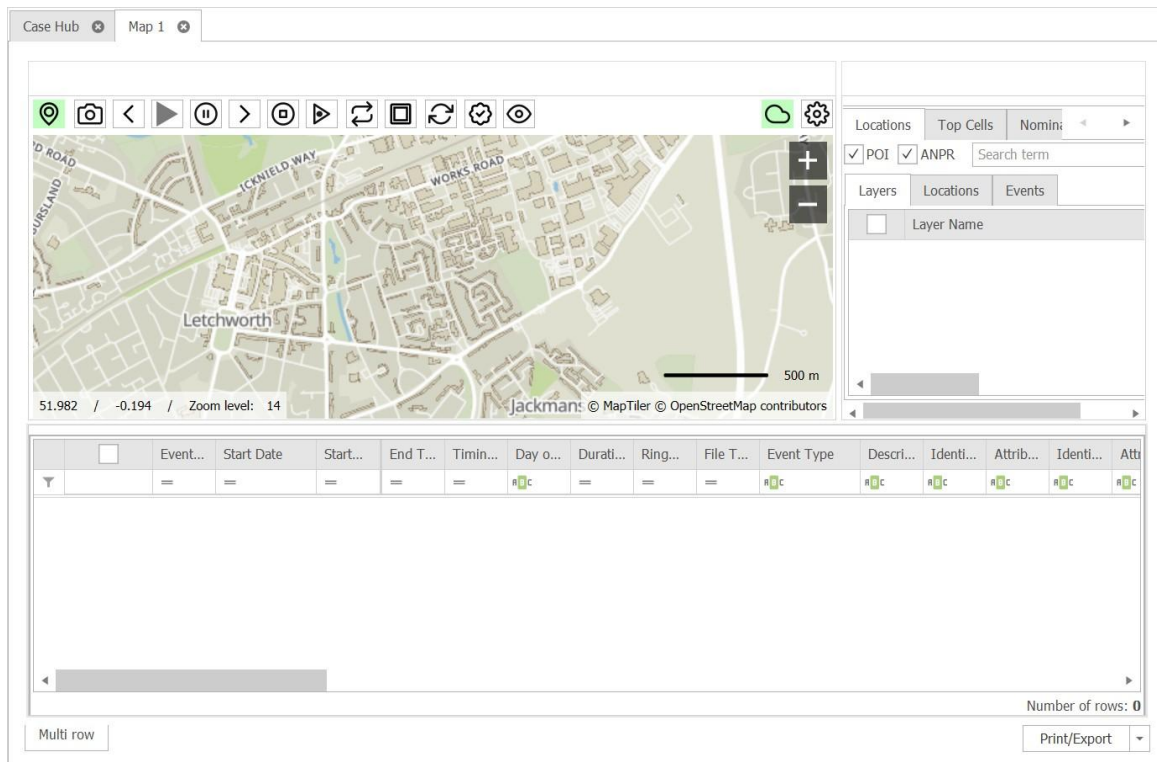
This function is typically carried out by the following users:

- » CSAS User

14.10 Using New Map

This function allows you to open an additional map as a new tab (a New Map tab) and load necessary source data files into the map. This function allows you to open multiple maps, in addition to the 'Case Hub' map, up to the maximum number of open tabs allowable.

To open a new map tab, go to the CSAS Home Navigation Panel and click on the  button. The New Map tab opens:



A Map Tab is really just an additional instance of 'Case Hub' and works in exactly the same way. The idea is that it gives you the opportunity to open additional maps alongside 'Case Hub'; they're called 'map tabs' to differentiate them from 'Case Hub' and avoid confusion.

From the new 'Map Tab', you can use:

- » All 'Case Hub' features.
- » Animate the map- see *Using Mapping*.

You can also open a new map tab by sending data to a map from:

- » Dashboard
- » Case Hub
- » Analytics
- » Case Cells

You can send data to a new map by right-clicking in any row of the Case Hub grid and selecting 'Send to map'.

Each new map tab is opened with the 'Case wide filters' and 'Case wide settings' disabled – the rationale for this is that the new map tab would have been created to view a specific

subset of data, if the tab is synced to the rest of the case, the data in view would also be synced to the rest of the case and wouldn't show the specific selected subset of data, which would defeat the purpose of opening the map tab in the first place.

Note: The functionality of the Details panel, Filters panel and Data Grid are the same as in the Case Hub screen. For information about how to use these panels and how to filter and import data into the map, refer to *Using Case Hub*.

Why, When, Who



This function is necessary to map important data using a separate map tab(s).



This function is undertaken any time you want to display a full dataset or a subset of data on a map.



This function is typically carried out by the following users:

» CSAS User

14.11 Using CellView

This function offers you a 'desktop RF survey' service that allows cell coverage areas to be viewed on a CSAS map as graphical images, based on crowd-sourced cell coverage data. This is made possible by expanding CSAS's RF (Radio Frequency) survey capabilities.

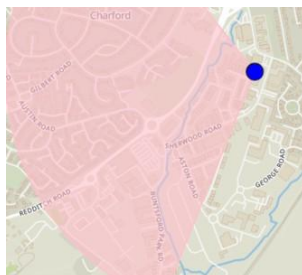
14.11.1 How is the Data Gathered

The service that provides the source data for 'CellView' has deployed a widget in a variety of popular smartphone apps that anonymously captures the geolocation of the host mobile, device along with details of the Cell ID that is currently being used. This data is transmitted to the provider's database where it becomes available to be queried by CellView users. The resulting database collates millions of readings from partner apps and offers instant access to maps showing the general coverage area of cells across the world.

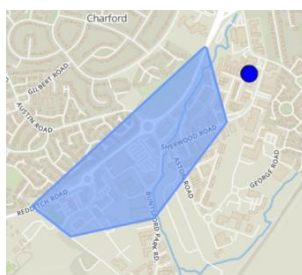
It must be stressed that CellView does not provide the ability to track an individual phone and cannot be used to provide any insight into the movement or location of specific subject phones in an investigation. Its sole purpose is to provide a general indication of the coverage area of cells, based on information provided by multiple contributing phones over an extended period of time.

14.11.2 Output Examples

The diagrams below provide examples of the results of a CellView cell coverage lookup:



Traditional indicative coverage - gives you a traditional coverage visualisation based on the provided azimuth with an expected coverage arc and an estimated cell reach or radius.



CellView reported coverage - shows you the actual coverage for the cell as reported by the phones that host the partner apps.

Knowledge of the approximate coverage area of a cell could be used as a starting point when formulating a search strategy or could drive a decision to despatch units to a particular area.

14.11.3 Caveats and Limitations

CellView data is gathered from partner smartphone apps and other sources, therefore cell measurement data will only be available for areas in which partner apps have been used. This may further mean that high volumes of cell data have been captured along major road and rail routes and in places where partner app users are likely to visit, but lower volumes of cell coverage data might be collected in less popular locations.

In light of this, there are several caveats associated with the use of CellView cell coverage data:

- » CellView cell coverage data is not guaranteed to be complete.
- » Coverage indications that encompass a specific point on the map are not evidence that a measurement of the associated cell was obtained at that exact location.
- » Absence of coverage indications at a specific point is not evidence that a cell provides no coverage at that exact location.
- » CellView coverage data is intel only and is not intended to replace an evidential RF survey.

Note: Coverage data is sourced from partner companies therefore Forensic Analytics Ltd offers no guarantees as to the accuracy or completeness of the data.

There are also some data protection aspects to be aware of:

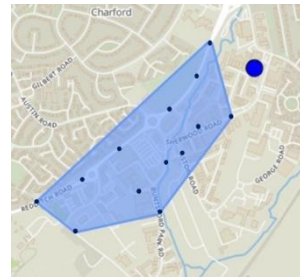
The measurement data collected by the partner apps is reported anonymously – there are no device (IMEI) or user (IMSI, MSISDN) details reported – and it is therefore not possible to use this data to identify or track individual phones or their users.

CellView data does not show the usage of cells by the specific subject phones in a case – there is no direct correlation between the usage of cells by subject phones in a case and the cell coverage data provided by CellView. CellView is merely indicating areas in which certain cell IDs have been reported as having been measured by multiple contributing phones over time.

The information reported to CSAS consists only of the details required to draw the coverage 'polygon' on the map; no details of individual phones or measurements are provided to us.

The measurement data provided by the partner apps indicates that one or more phones have reported their use of each individual cell ID in a combination of locations which, when they have been joined by an outline, produce a polygon that covers a particular area - just because a specific point on the map is covered by the polygon does not mean that a measurement of the associated cell was obtained at that exact location.

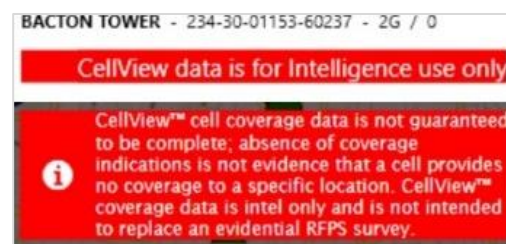
In this example, the small dark blue dots indicate the hypothetical location of phones that reported measurements for the associated cell ID via the partner apps:



- » The coverage polygon is calculated by joining the outermost points (using a mathematical technique called a 'convex hull'); the resulting coverage polygon bounds an area within which measurement points have been reported but offers no indication of the likelihood or otherwise of coverage at any specific point within that area.
- » The dots shown in the image are for illustrative purposes only, CSAS is not provided with details of actual measurement points and therefore cannot provide real images that contain this level of detail.

The source database contains measurements dating back several years, and initially all coverage data will be exposed to 'CellView' queries.

Each 'CellView' map contains the following caveat text.



This is shown in the *Cell Coverage* > *CellView* drop-down (from the map cell site right-click menu) which opens when you attempt to activate a CellView coverage polygon:

Note: The larger CellView panel also contains a longer string of caveat text which all recipients of CellView data or maps must be made aware of. These caveats, along with the anonymised nature of the reporting process and the lack of an audit trail for the crowd-sourced cell measurements combine to ensure that **CellView cell coverage visualisations should only be used for intel purposes and should not be used in evidence.**

CellView coverage data is provided 'as is'.

Caution: Although Forensic Analytics Ltd are prepared to provide statements or wording to explain how CellView works and what its limitations are, we will also make it clear that we regard this data as being for 'intel only' use. Forensic Analytics Ltd will not provide statements that attempt to explain any one particular set of CellView results and will offer no interpretation of those results. By using CellView within CSAS, you're agreeing that you've read and understand these caveats. Forensic Analytics Ltd will not be held liable for any consequences arising from the use of the cell coverage data provided by this feature.

14.11.4 Preparation

Prerequisites

CellView is an add-on to CSAS and is separately licensed, you must therefore have existing CSAS licences to add a CellView licence to.

CSAS instances must have access to the Internet to be able to use this facility, it's not available offline or to non-networked host machines. There is an option to have a CellView server deployed within an organisation's internal network, which would avoid the need to connect via the Internet; please contact your CSAS account manager if you would like to discuss this option.

Comms and Whitelisting

CSAS CellView looks up cell coverage details via an API call to the following domain:
<https://apiv2.combain.com>

This destination and any URLs that use it as a stem might need to be whitelisted in your organisation's firewall, proxy or other network edge equipment to enable lookups to take place.

CellView replicates CSAS's general ability to interwork with network proxies, which is based on inheriting the host PC's network settings, there is no additional interface in which to add proxy details, usernames or passwords, although it is possible to select the network security protocol to be used (via the *Help > About/Licensing > Web Request Settings* menu).

Note: CellView lookups are usually very quick but may take up to 30 seconds to complete and could take longer if multiple cell IDs are sent in the same request.

14.11.5 Using CellView

CellView cell coverage lookups can be triggered from two places within CSAS, once the feature is licensed:

- » A search bar in the Case Hub CellView panel.
- » A right-click menu option when clicking on a cell site icon in the map.

Acceptable Cell ID Formats

The CellView panel search bar option needs you to enter one or more cell IDs to search for – to ensure that the results for the correct cell are returned, the cell ID must be entered in the CGI format. The traditional CGI format is:

- » MCC (country code) – MNC (network code) – LAC (2G/3G only) – Cell ID.

An example for a 2G/3G cell:

- » 234-10-21001-18886

An example for a 4G cell:

- » 234-10-130140787'

CellView will not be able to lookup cells without the leading MCC-MNC component as it wouldn't know which network to query. For 2G/3G cells, the CGI must also contain the

correct LAC (location area) as 2G/3G cell IDs are only unique within a LAC and there may be multiple cells nationally that have the same cell number.

4G/5G CGIs don't specifically contain the TAC (Tracking Area Code) and so typically only contain three elements – 'MCC-MNC-Cell ID'. The cell ID component is referred to as the ECI (EUTRAN Cell ID) for 4G cells and the NCI (NR Cell ID) for 5G cells.

CellView will also accept lookup requests for 4G/5G cells where the TAC *has* been included – so requests for 234-10-130140787 and 234-10-04288-130140787 would return the same results.

Network-specific Anomalies

EE UK use an adapted version of the 4G/5G cell ID that doesn't match the CGI format transmitted by EE cells – this means that entering the 4G/5G cell ID format found in EE CDRs will not get the correct result as the CellView database is populated with measurements taken by phones based on what is transmitted by the cells. CSAS automatically creates a standardised 4G/5G CGI for EE cells, which will provide the cell ID in a format that CellView can work with.

The CellView tab search bar has a checkbox that forces CSAS into interpreting EE 4G/5G cell IDs (prefixed with 234-30) in either 'EE format' or 'CGI format', but it's your responsibility to switch between modes as necessary.

O2 UK have a similar issue with some of their older 3G cells. 3G networks are optionally able to refer to one or more cells with a combined identifier called a SAC (Service Area Code), O2 choose to use a single SAC to describe all individual cells on the same sector/azimuth of their 3G sites, so up to three cells (each with their own unique cell ID) can be grouped and collectively referred to by the same SAC. The SAC is what gets captured in CDRs, instead of a cell ID, but the SAC is not transmitted by the cells. This means that SAC-only 3G cell IDs will not be recognised by CellView, as the database is populated with CGI data transmitted by O2 cells, which does not contain the SAC.

The O2 Sort Cellular database is able to provide a lookup of the cell IDs that relate to each SAC, so you may be able to find an identifier there that can be used to lookup cell coverage in CellView.

14.11.6 Using CellView Lookup Process

CellView coverage data can be added to a CSAS map in two ways:

Map Right-click Menu

If a location for the cell ID you want to search for is already visible in a CSAS map, for example if a cell icon for the site that hosts the cell ID is shown on a map, CellView cell coverage details can be requested from the cell icon right-click menu.

To open a CellView lookup: right-click on the necessary cell site and select Cell coverage > CellView and then the cell ID of interest:

Not all cells will be eligible for CellView lookups – see *Acceptable Cell ID Formats*.

If the cell is found in the CellView database, the coverage details are displayed on the map.

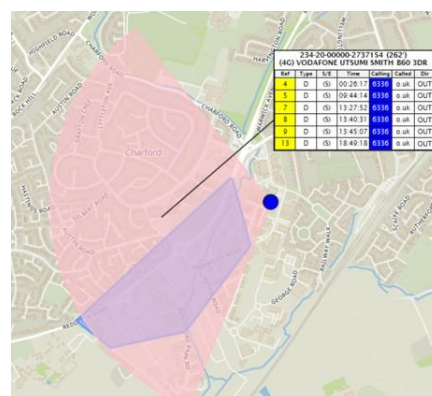
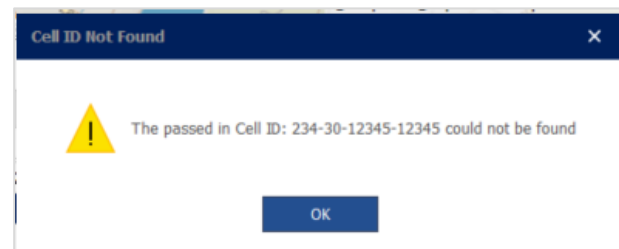
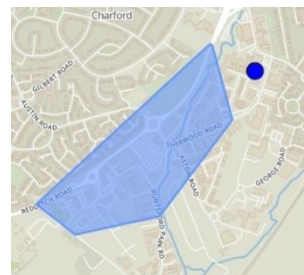
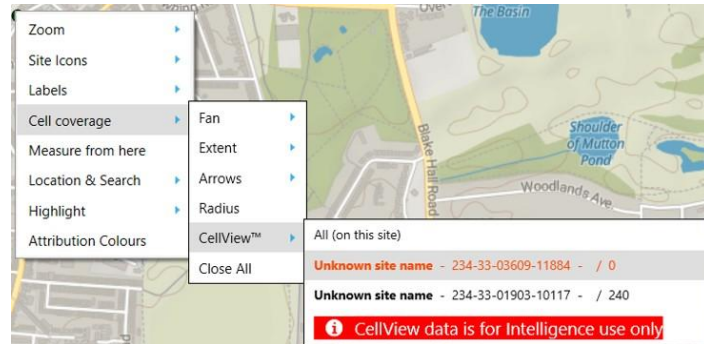
If the cell you've searched for is not found in the CellView database, an error message is posted indicating a negative result.

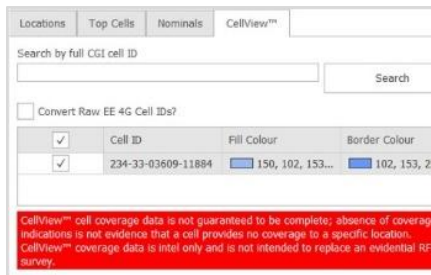
As the cell location was already being displayed in the map, details of its azimuth and calls should be available, so the usual CSAS map features (fan/extent/arrow and call label) should also be available, allowing users to view a mix of CellView coverage and other cell visualisations:

Note: CellView coverage details are not currently stored if a map is saved, they will need to be requested again when a map is reopened to be able to be viewed.

CellView Panel Search Bar

It's also possible to search for CellView cell coverage data from within Case Hub:





If you know the cell ID you want to search for, but is not currently displayed on the CSAS map, you can search by typing the cell ID into the search bar - see *Acceptable Cell ID Formats*.

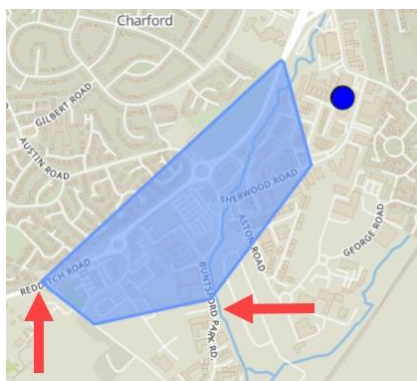
- » If the cell is found in the CellView database, the coverage details are displayed on the map.
- » If the cell is not found in the CellView database, an error message is posted indicating a negative result.
- » If cell coverage details are displayed in a map, the cell IDs are listed in the CellView panel. You can:
 - Show or hide individual cells by clicking the 'View' checkbox.
 - Change the fill/outline colours or fill opacity of the highlighting used for an individual cell by clicking the 'Colour' drop-down menu.

CellView Settings

Currently there are no user-accessible settings for CellView.

14.11.7 Understanding Coverage Visualisation

CellView cell coverage visualisations provide an indication of the approximate coverage area of a given cell ID. As the data is collected from 'partner' smartphone apps, it must be understood that the coverage data will only be gathered from places visited by users of those apps.



In this example, the fact that the coverage of the cell (shown in blue) is mostly shown clustered along two main roads (Redditch Rd and Buntsford Park Rd) doesn't mean that the cell in question only serves along those two roads, but that users of the apps were travelling along those roads (and a few of the surrounding side streets in the town of Charford) when measurements were reported by apps running on their phones.

Note: Forensic Analytics Ltd have undertaken extensive validation of the CellView data, as have several CSAS customers, and have found that where CellView data is available, there generally appears to be a good correlation between the coverage areas indicated by CellView and those obtained from physical RFPS surveys. We find that, in general,

between 85% and 95% of CellView requests for UK cell are successful, but there will also be a proportion of cells for which the service has no coverage data. CellView data is not guaranteed to be complete, however, and absence of coverage indicated by Cell View cannot be assumed to mean that a cell does not provide coverage in a given area, only that no measurements for that cell have been reported by partner apps in that area. These caveats, along with the anonymised nature of the reporting process and the lack of an audit trail for the crowd-sourced cell measurements combine to ensure that CellView cell coverage visualisations should only be used for intel purposes and should not be used in evidence.

14.11.8 Getting the Best Results

The cell coverage images produced by the CellView service are bounded polygons; Forensic Analytics Ltd recommend using a light colour with reasonable opacity for the infill and a stronger colour for the border.

If the 'CellView' coverage is of a cell for which a site icon and azimuth data are available, we recommend showing the cell 'extent' arms in the map and also the cell site label, as these details will add context to the image.

It's possible to show details for multiple cells in the same map, but we generally recommend including a maximum of only 3 or 4 cells on any one map to avoid overloading the viewer and losing the impact of the coverage visualisations.

Why, When, Who

	This function is necessary to view cell coverage areas on a CSAS map as graphical images, based on crowd-sourced cell coverage data.
	This function is undertaken anytime you want to view a subset of data from Case Hub on a map; however, you must have existing CSAS licences to add a 'CellView' licence to.
	This function is typically carried out by the following users: » CSAS User

Troubleshooting

Not every CellView lookup will result in a populated map; there are several possible reasons for this:

- » Coverage data is only available from areas visited by users of the partner apps – if no users have visited an area, the database will not contain details of any cells that provide coverage there.
- » CellView lookups can only be performed using full (CGI) cell IDs; abbreviated cell ID formats (e.g. cell ID only or LAC/Cell ID only) are potentially ambiguous and a lookup cannot be performed using them.
- » Lookups of O2 'SAC-only' cell IDs will not work – the SAC is not broadcast by the cell and therefore won't be picked up measurements captured by partner apps and further won't appear in the CellView database and so can't be looked up

- » Lookups of non-standard cell ID formats (raw EE 4G cell IDs, for example) won't work unless the request is made with the 'Convert EE 4G cell IDs' option enabled, as the EE-specific 4G format is not broadcast by the cells (it's only used in the CDRs) and won't be picked up by the partner apps or stored in the CellView database.
- » The CellView database is contacted via the Internet – if your PC is not connected to the Internet, you will not be able to access the facility.
- » Some police or organisational networks may block access to the CellView service – you'll need to confirm with your IT team whether you'd be permitted to access the CellView service.

14.12 Time Offset, Merging and Adjustment

CSAS Case Hub presents imported data in a grid organised in date/time order. For the data to be presented correctly, the dates and times of the events must be shown in the correct sequence. Some data sources – cellular CDRs, for example – are linked to very accurate time sources and so the timestamps related to the disclosed events can be trusted to also be accurate. Some data sources – handset downloads, for example – may not have such rigorously accurate timestamps.

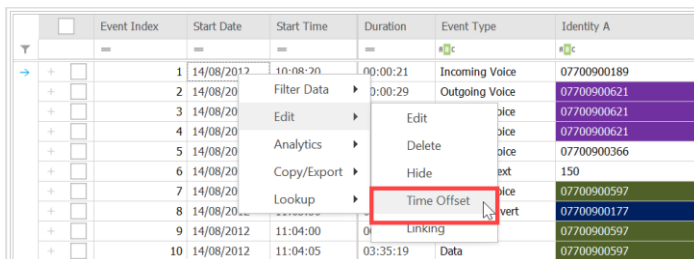
Although most mobile handsets default to obtaining their date/time reference from the network, there is nothing to stop a handset user manually setting the date/time on their phone to something other than the 'real' time. It's not unheard of for criminals to manually set their phones to a different date/time in order to confuse any evidence that might be captured from their device at a later date. There may also be instances where data in a file was captured across multiple time zones. In these circumstances, it is useful to be able to adjust the 'displayed' time of case events by applying an offset to them.

The 'time offset' feature in Case Hub exists for this purpose.

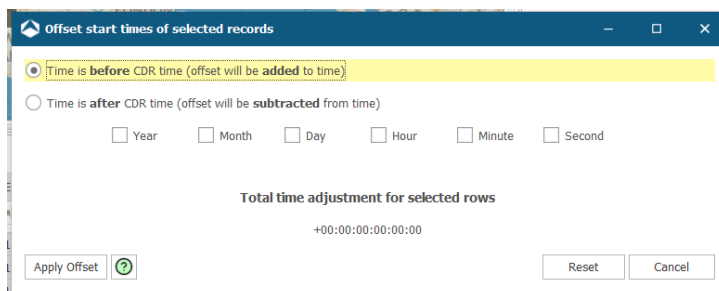
Time Offsets are often useful if a case includes CDRs and handset download data for the same device – the CDR events will usually have accurate timestamps, whereas the handset events may not. It may be useful to be able to add a time offset to allow duplicate records, where both a CDR and a handset record for the same event exist, to be time aligned.

Applying an offset

When you work in 'Multi row' grid view in Case Hub, the Time Offset function allows you to add a date/time offset to an event or group of events so that you can compensate for any differences between the event timestamps and 'real' time, effectively giving you manual control over the order in which case events are displayed. When you right-click on the grid, a drop-down menu opens from which you can select 'Time Offset':



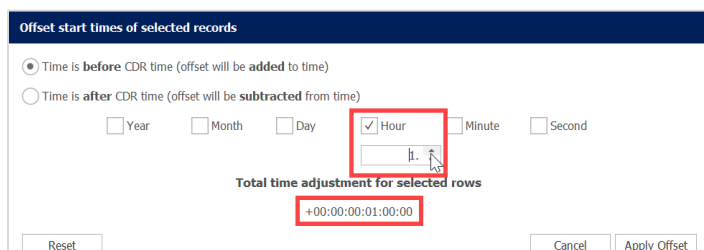
When you select 'Time Offset' a pop-up window opens from which you can set the date/time offset using the radio buttons, checkboxes and drop-down boxes:



You are asked to indicate whether you wish to **add a positive** offset to create a displayed time that is earlier than real time into alignment, or to subject a negative offset to create a displayed time that is later than real time into alignment.

You can then select the time units (years, months, days, hours, minutes and seconds) and the value of the offset.

In this example, the 'Hour' checkbox is selected and a time offset of '1' hour is applied.



The 'total time adjustment...' value indicates the total value of the offset that is to be applied.

When you click the Apply Offset button, the pop-up window closes and the grid adjusts to apply the selected offset.

The value of the applied offset, if any, for each row in the Case Hub grid can be viewed in the 'Timing Offset' column, which is displayed in the 'full' grid layout. Any time offset actions are captured in Case Audit.

An example of the application of a time offset is shown below, which presents the same dataset with and without an offset applied.

In this version, no offset has been applied – the first event timestamp is 19:00:52 and the Timing Offset column is set to 0 for all events:

Start Date	Start Time	...	Timing Offset	Duration	Event Type	Identity A	Attribution A	Identity B	Attribution B
12/08/2017	19:00:52	1	0	00:00:00	Incoming Text	0EB88E038D87A0398B22		07700902421	Unknown 1
12/08/2017	19:00:59	2	0	00:00:00	Outgoing Text	07700902421	Unknown 1	3535	
12/08/2017	19:01:01	3	0	00:00:00	Incoming Text	3535		07700902421	Unknown 1
12/08/2017	19:02:53	4	0	00:00:02	Outgoing Voice	07700902421	Unknown 1	07700907514	
12/08/2017	19:08:20	5	0	00:17:07	Incoming Voice	07700907514		07700902421	Unknown 1
12/08/2017	19:36:06	6	0	00:01:05	Outgoing Voice	07700902421	Unknown 1	07700907514	
12/08/2017	19:46:25	7	0	00:00:00	Incoming Text	0EB88F838D87A830BE23		07700902421	Unknown 1
12/08/2017	20:28:41	8	0	00:00:05	Outgoing Voice	07700902421	Unknown 1	07700907514	
12/08/2017	20:29:46	9	0	00:00:20	Incoming Voice	07700907514		07700902421	Unknown 1
12/08/2017	20:44:35	10	0	00:00:15	Outgoing Voice	07700902421	Unknown 1	07700907514	

Whereas, in this version, a positive one-hour offset has been applied – the first record is now at 20:00:52 and the Timing Offset column indicates that a 1h offset has been applied.

Start Date	Start Time	E...	Timing Offset	Duration	Event Type	Identity A	Attribution A	Identity B	Attribution B
==	==	==	==	==					
12/08/2017	20:00:52	1	1h	00:00:00	Incoming Text	0E88BE038D87A0398B22		07700902421	Unknown 1
12/08/2017	20:00:59	2	1h	00:00:00	Outgoing Text	07700902421	Unknown 1	3535	
12/08/2017	20:01:01	3	1h	00:00:00	Incoming Text	3535		07700902421	Unknown 1
12/08/2017	20:02:53	4	1h	00:00:02	Outgoing Voice	07700902421	Unknown 1	07700907514	
12/08/2017	20:08:20	5	1h	00:17:07	Incoming Voice	07700907514		07700902421	Unknown 1
12/08/2017	20:36:06	6	1h	00:01:05	Outgoing Voice	07700902421	Unknown 1	07700907514	
12/08/2017	20:46:25	7	1h	00:00:00	Incoming Text	0E88BF838D87A83DBE23		07700902421	Unknown 1
12/08/2017	21:28:41	8	1h	00:00:05	Outgoing Voice	07700902421	Unknown 1	07700907514	
12/08/2017	21:29:46	9	1h	00:00:20	Incoming Voice	07700907514		07700902421	Unknown 1
12/08/2017	21:44:35	10	1h	00:00:15	Outgoing Voice	07700902421	Unknown 1	07700907514	

Note: This can be applied to single row or multiple rows in the grid.

Removing an offset

To remove an offset, use the same process as outlined above but deselect all time units – you will be warned that you’re trying to apply a zero offset and will be asked if you want to clear any applied offsets – click ‘yes’.

All selected records will be returned to their original timestamp.

Why, When, Who



This function is necessary to change the displayed timestamp for one or more events and to bring records that relate to the same event into time alignment.



This function is undertaken any time there is a justifiable need to apply an offset to source data.



This function is typically carried out by the following users:

» CSAS User

14.13 Using Cell Confidence

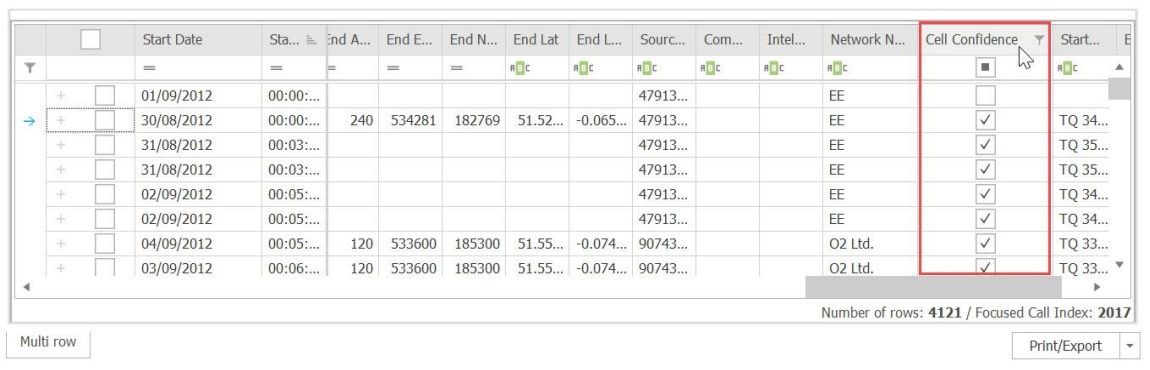
Voice and SMS connections are handled in such a way as to ensure that the CDR record captured for each event provides details of the cell that was in use by the subject phone at the start time stated in the record. This kind of certainty is sometimes referred to as being an 'at conclusion', because if a record's start timestamp and start cell correlate, it is possible to state that the subject phone was somewhere within the coverage area of the cell 'at' the time stated in the timestamp.

Due to the more periodic nature of mobile Internet connectivity, where phones can be active but not connected to a cell for long periods of time, GPRS (or mobile data) records are captured in a different way to voice or SMS records. This makes them difficult to use evidentially, as there is often a less definite correlation between a record's start time and its start cell. This means that it is not always possible for analysts to draw a conclusion that Phone A was within the coverage area of Cell B at Time C. GPRS events, when included in a cell site analysis report, are often presented with an 'at or before' conclusion, to highlight the fact that the start cell and start timestamp do not necessarily correlate.

There are however some scenarios where it is possible to have confidence that the start time and start cell on a GPRS record do correlate. For these records we can say that 'cell confidence' (e.g. confidence that the record's start time and start cell correlate) is 'true'.

The 'Cell Confidence' column in the Case Hub grid is a simple Boolean (True/False) column. Records for which cell confidence is true will be ticked, those for which cell confidence is false will not be ticked.

You can look for GPRS record correlations using the 'Cell Confidence' column in the Data Grid:



	Start Date	Sta...	End A...	End E...	End N...	End Lat	End Lon	Sourc...	Com...	Intel...	Network N...	Cell Confidence	Start...
	01/09/2012	00:00:...						47913...			EE	☐	
	30/08/2012	00:00:...	240	534281	182769	51.52...	-0.065...	47913...			EE	☒	TQ 34...
	31/08/2012	00:03:...						47913...			EE	☒	TQ 35...
	31/08/2012	00:03:...						47913...			EE	☒	TQ 35...
	02/09/2012	00:05:...						47913...			EE	☒	TQ 34...
	02/09/2012	00:05:...						47913...			EE	☒	TQ 34...
	04/09/2012	00:05:...	120	533600	185300	51.55...	-0.074...	90743...			O2 Ltd.	☒	TQ 33...
	03/09/2012	00:06:...	120	533600	185300	51.55...	-0.074...	90743...			O2 Ltd.	☒	TQ 33...

Number of rows: 4121 / Focused Call Index: 2017

Multi row Print/Export

Cell confidence will always be 'true' for voice and SMS events and will always be set to 'false' for GPRS/mobile data events unless a specific set of circumstances is detected.

Note: Cell Confidence can only be used with the records provided by certain networks, not all GPRS CDRs provide enough information to make a cell confidence determination.

It may be possible to use an 'at' conclusion with GPRS CDR records in some circumstances, amongst which are:

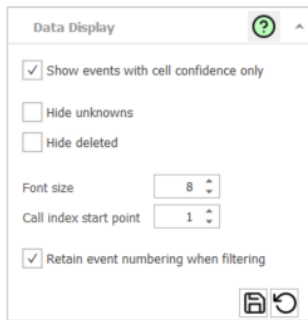
- » Start of a new session denoted by change of Charging ID or a gap of more than 10 seconds between the end of the previous record and the start of a new one for the same network element (Access Point Name (APN)).
- » Change of technology for follow-on records.

Not all networks' GPRS CDRs include the necessary information to allow CSAS to make a cell confidence determination – it is helpful if the CDR contains data fields such as Charging ID, end time or duration and APN. If some of all of those data types are excluded from the CDR, CSAS will assume that all GPRS record have cell confidence = false.

If a CDR does provide enough information in the GPRS/data records, CSAS can attempt to determine if a user can have confidence that a record's start cell correlates with its start time. The method is as follows:

- » Always assume that an 'at or before' conclusion is good enough for a GPRS record unless you need to place the phone in a cell coverage 'at' a specific time and can't do it with voice or SMS records.
- » Compile reports and identify the GPRS events for which you need to use an 'at' conclusion (those for which an 'at or before' conclusion isn't good enough).
- » If you decide not to use any 'at' conclusions for GPRS events, then there's no need to determine the cell confidence.
- » Check if a Charging ID is available in the CDR. The change of Charging ID denotes the start of a new session and you should have confidence in the correlation of the start time and start cell for the CDR record that is recorded at the start of a new session:
 - If a Charging ID isn't available, then you can look at the gaps between the end time of one GPRS record and the start time of the next GPRS record **for the same APN**. If there is a gap of 10 seconds or more then it is reasonable to assume that the old session ended and a new session has started therefore you can have confidence in the correlation of start time and start cell.
 - If the Charging ID doesn't change and/or the gap between the end of one record and the start of the next **for the same APN** is less than 10 seconds, check the technology. If the technology changes between two records for the same APN, then it is reasonable to assume that the start cell on the new record correlates to the start time therefore giving the 'at' conclusion.

Case Hub can be set to only display records where cell confidence is true, if required.



The 'Data Display' settings panel includes the following options:

- ☒ Show events with cell confidence only
- ☐ Hide unknowns
- ☐ Hide deleted
- Font size: 8
- Call index start point: 1
- ☒ Retain event numbering when filtering

In the Settings sidebar, Data Display section, select the 'Show events with cell confidence only'.

With this option selected all voice/SMS and other types of events will be shown as usual, but only GPRS/mobile data events where cell confidence is 'true' will be displayed, events where cell confidence is 'false' will be hidden and ignored.

Why, When, Who



This function is necessary to indicate whether the start cell of each record can be expected to correlate with the start time, making it far easier for analysts and investigators to make full use of this important type of evidence.



This function is undertaken whenever you want to correlate the start time and start cell on a GPRS record.

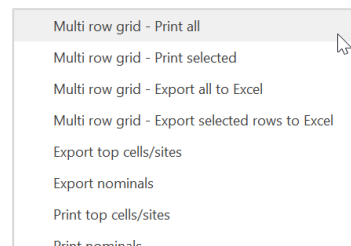


This function is typically carried out by the following users:

» CSAS User

14.14 Printing / Exporting

This function provides you with options for printing and exporting the contents of the Case Hub grid via the **Print/Export** button which opens the following drop-down menu:



The dropdown menu contains the following options:

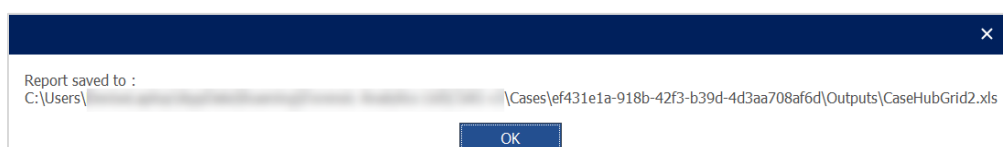
- Multi row grid - Print all
- Multi row grid - Print selected
- Multi row grid - Export all to Excel
- Multi row grid - Export selected rows to Excel
- Export top cells/sites
- Export nominals
- Print top cells/sites
- Print nominals

The 'Export' and 'Print' facilities offer several options:

- » Print/export all – the entire contents of the Case Hub grid will be output.
- » Print/export selected – only the ticked Case Hub rows will be output.
- » It is also possible to print/export the grids for two of the Details panels.

If selecting to Export, a status bar and pop-up message window will be displayed as the report is generated and saved.

The following message pop-up window opens stating where the generated report has been saved to:



The message pop-up window displays the following information:

Report saved to : C:\Users\... \Cases\ef431e1a-918b-42f3-b39d-4d3aa708af6d\Outputs\CaseHubGrid2.xls

OK

When the user clicks on the **OK** button, the message pop-up window closes and the

If selecting to Print the Grid, you'll see a similar pop-up message showing you the print progress, then a 'Preview' pop-up window opens:

Preview																										
File View Background																										
Selection	Event Index	Start Date	Start Time	id	Prog	Cal	Grating	End Point	Temperature	Substrate	Incident beam	EMF	EMPC	C Cell	in Cell	5 mm	LACAT	Set T	Asst	Em	Normal	in Cell	Cal	Cal Speed	AC	
☒	1	1/14/09/2012	10:24:00		15	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	2	2/29/09/2012	10:04:04		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	3	3/26/09/2012	10:54:37		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	4	4/29/09/2012	11:14:00		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	5	5/29/09/2012	11:26:22		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	6	6/29/09/2012	11:33:10		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	7	7/29/09/2012	12:08:38		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	8	8/29/09/2012	12:09:03		Val	00	00		Inv	24	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	9	9/29/09/2012	12:19:19		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	10	10/29/09/2012	12:27:15		Val	00	00		Inv	15	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	11	11/29/09/2012	12:27:23		Val	00	00		Inv	15	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	12	12/29/09/2012	12:40:24		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	13	1/29/09/2012	13:49:08		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	14	4/29/09/2012	14:17:20		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	15	15/29/09/2012	14:20:18		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	16	16/29/09/2012	14:25:39		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	17	17/29/09/2012	14:28:26		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	18	18/29/09/2012	14:38:07		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	19	19/29/09/2012	14:42:03		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	20	20/29/09/2012	14:44:17		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	21	21/29/09/2012	14:48:21		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	22	22/29/09/2012	14:53:56		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	23	23/29/09/2012	15:08:32		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07
☒	24	24/29/09/2012	15:19:12		Val	00	00		Inv	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07	07

Page 1 of 20

100%

Page 1 of 20

Why, When, Who

-  This function is necessary to print or export the user's completed dataset for review.
-  This function is undertaken any time Case Hub is used.
-  This function is typically carried out by the following users:
 -  CSAS User

15 Using Case Outputs

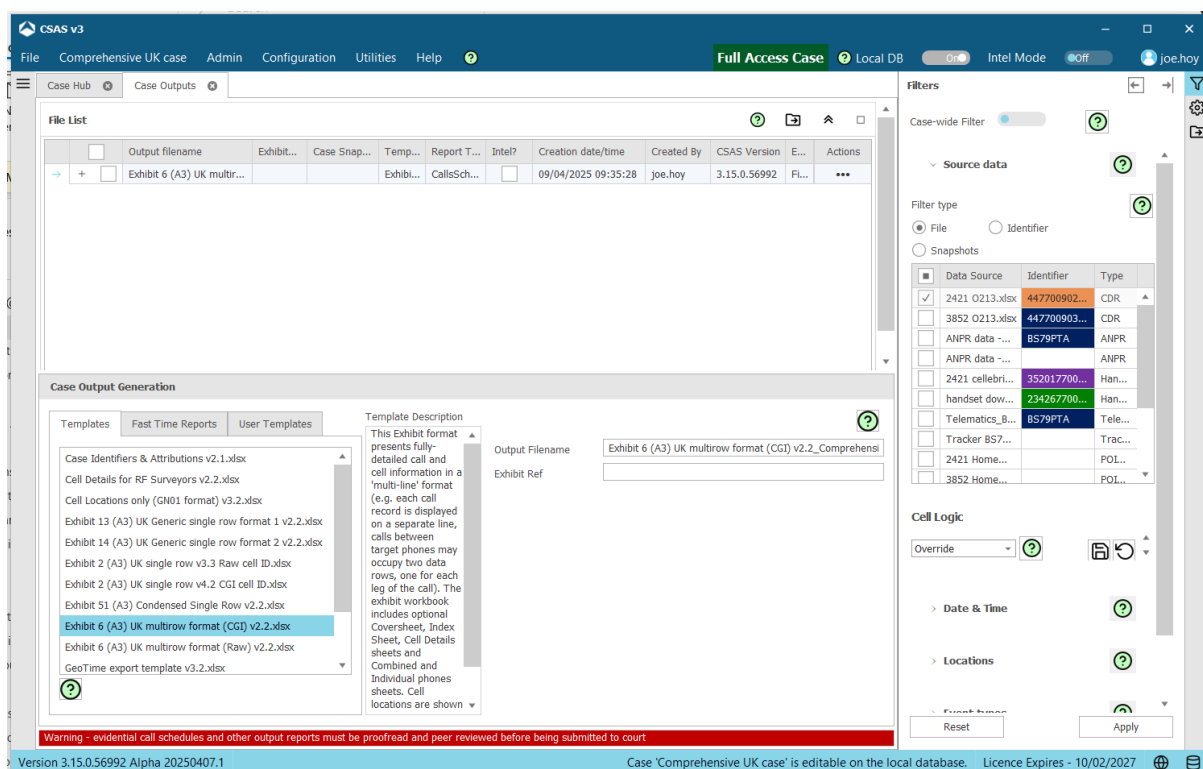
The Case Outputs function allows you to output processed source data (either a 'basic' dataset created from an unfiltered set of source files or 'filtered' snapshot dataset in which the data has been filtered by date/time or some other criteria) and export to an Excel workbook in either the Investigation format or one of the Exhibit formats.

The Case Outputs grid lists all outputs created in a case, not just those exported via the Case Outputs screen, this includes reports generated in Analytics, Case Hub and other screens. This provides the opportunity to view and manage all case outputs in one place.

15.1 Layout

The Case Outputs screen is split up into windows and panes:

- » File List grid
- » Template list
- » Template description
- » Options.



The content of the output file from Case Outputs is selected using the Filters sidebar 'Source data' tab.

Case Outputs functions are available by clicking on the  Case Outputs button from the Case Home screen (or by other screen prompts) which opens the 'Case Outputs' screen.

WARNING: AS HARD AS FORENSIC ANALYTICS LTD TRY TO ENSURE THAT CSAS OUTPUTS ARE ACCURATE, WE CANNOT IN GOOD FAITH GUARANTEE THAT ERRORS WILL NEVER BE MADE, ALTHOUGH IT IS VERY RARE. FOR THIS REASON, WE HAVE ALWAYS SUGGESTED THAT CALL SCHEDULES AND OTHER PRODUCT OUTPUT FROM CSAS IS PROOFREAD AFTER IT HAS BEEN CREATED AND IS PEER REVIEWED BEFORE BEING SUBMITTED TO COURT.

Please note the following WARNING text stated at the bottom of the Case Outputs screen:

“Warning - evidential call schedules and other output reports must be proofread and peer reviewed before being submitted to court.”

15.2 Creating a New Output File

Output workbooks can be created directly from the case source data files or from any Snapshots you have saved in the Case.

Why, When, Who



This function is necessary to create a new output file to be used to exhibit data for a case or to export data to enable further analysis outside of CSAS.



This function is undertaken at any time Case Outputs is selected and a new output file is required.



This function is typically carried out by the following users:

 CSAS User

Stepped Procedure

1. From the Filters sidebar, select the source files or Case Snapshot you want to export.
2. Set any filters or settings options, such as Redaction that are required.
3. Select the required output or Fast Time template.
4. Set any required Options and assign an Exhibit Reference if required.
5. To start the export, click the Apply button.
6. The exported template will be added to the Case Outputs file list grid and will be opened automatically if Excel (or a compatible open office product) is available.

15.3 Grids and Controls

The Files List grid shows all output files that have been created for a Case:

Case Hub Case Outputs

File List

	Output filename	Exhibit Ref	Case Snapshot	Template	Rep...	In...	Creation dat...	CSAS...	Error	Acti...
→	☐ Case Identifiers & Attributions v2...			Case Identifiers & Attri...	Call...	☐	15/09/2021...	3.3.0.9...		***
	☐ Top Cells (1).xlsx				Anal...	☐	21/09/2021...	3.3.0.9...		***
	☐ Top Contacts (1).xlsx				Anal...	☐	21/09/2021...	3.3.0.9...		***
	☐ Case Outputs (1).xlsx				Anal...	☐	22/09/2021...	3.3.0.9...		***
	☐ CaseHubGrid1.xls				Call...	☐	23/09/2021...	3.3.0.9...		***
	☐ CaseHubGrid2.xls				Call...	☐	23/09/2021...	3.3.0.9...		***

The grid contains the following information about each file:

- » 'Output filename' – this column shows the filename without the 'folder path' information. The default name for each file will be [< template type > _ < case name > _ < index > .xlsx] but this can be replaced with a custom file name by selecting 'Output File Name' from the Options panel and entering the required details.
- » 'Exhibit Ref' – this column shows the optional Exhibit Ref you assigned to each output file – listing the Exhibit Ref here might make it easier to keep track of the exhibits that you've created.
- » 'Case Snapshot' – this column shows the name of the case snapshot you used to create the output, if any.
- » 'Template' – this column shows which template was used to create the output file.
- » 'Report Type' – this column shows you what has been output, in this example a fully-detailed, multi-row call and cell schedule has been created e.g. each call record is displayed on a separate line. The Report Type is dictated by the type of Template you select.
- » 'Intel?' – this column shows if any intel records have been included in the output data; if any intel records were included, the box will be ticked.

Note: Updated templates that contain the intel records column have the template filename suffixed with '_INTEL' and have 'INTEL ONLY' in the sheet headers).
- » 'Creation date/time' – this column shows the date/time that the file was created by CSAS (or the time at which CSAS first became aware of it, in the case of files that were copied into the 'Output' folder from elsewhere).
- » 'Created By' – this column shows the user who generated the report.
- » 'CSAS Version' – this column shows the version of CSAS that created the output report.
- » 'Error' – this column will be populated with a message if any errors or issues are detected with any listed output files
- » 'Actions' – see [Grid Right-click and Actions Menu](#).

Note: You can double-click on any output file in the list which automatically opens the file in the appropriate application or viewer.

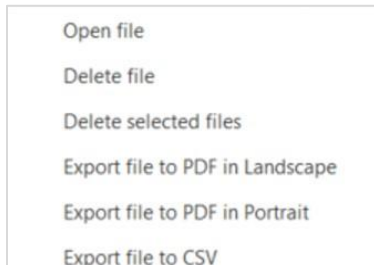
15.3.1 Grid and Column Controls

The Case Outputs grid shares a common set of filtering and layout controls with the other grids in CSAS. Details of how to apply filters, customise the column layout and other grid control options are given in [Grid Filtering and Controls](#).

15.3.2 Grid Right-click and Actions Menu

Right-click menu

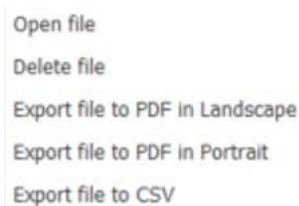
The grid supports a right-click menu that hosts additional options, most of which are replicated in the 'Actions' menu, which is accessible from the last column in each row in the grid:



- » Open file – opens the selected file in the appropriate viewer, for example, xlsx files will be opened in Excel (or an equivalent open office application) if available on the host machine.
- » Delete file – deletes the selected file. The file must be closed for this complete this action.
- » Delete selected files – multi-selects several files and delete them all in one action.
- » Export file to PDF in landscape – exports an Excel file to PDF with the page orientation set to landscape.
- » Export file to PDF in portrait – exports an Excel file to PDF with the page orientation set to portrait.
- » Export file to CSV – exports an Excel file to CSV. The contents of multi-tab Excel files are all exported sequentially into one CSV file.

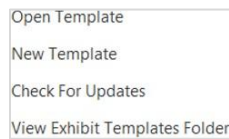
Actions menu

The 'Actions' menu offers a similar set of options, except the option to delete multiple files - as the Action menu works on a row-by-row rather than a multiple row basis:



15.3.3 Template Panel Right-click Menus

Templates and Fast Time Reports panels



- » Open Template – opens the selected template in the Template Builder for editing.
- » New Template – opens a blank template in the template builder ready to be created.
- » Check for updates – checks the templates folder to see if any new templates have been added, if any are found they are added to the templates list.
- » View Exhibit Templates Folder – opens the CSAS templates folder so the current set of templates can be viewed and new templates can be copied in.

User Templates panel

This offers the same set of options apart from 'Check for Updates', as user templates are created locally and there is no opportunity to import them from elsewhere.

15.3.4 Options Tab

Gives output-specific options:



- » 'Exhibit Output Filename' – allows you to select a name for an output file rather than accepting the automatically generated one.
- » 'Exhibit Ref' – allows you to add an Exhibit Reference that will be added to the output file (if the 'exhibit ref' field was included in the template).

15.3.5 Sidebars

Filter Sidebar

Case Outputs uses the same standard 'Filters' sidebar as other screens:

- » The data to be output is selected using the 'Source data' tab and either File, Identifier or Case Snapshot options.
- » You can choose to output the data from just one source file or from a set of source files.
- » You could choose to output the data for one or more identifiers, or you could choose to out the data from a Case Snapshot (currently you can only select one Snapshot at a time to output).
- » The Cell Logic setting governs whether 'source' cell details or the potentially more comprehensive 'override' cell details will be included in the output.
- » You can also choose to use any of the other filters in the sidebar (date/time, time slice, location or event types) to edit the dataset before outputting it.

Settings Sidebar

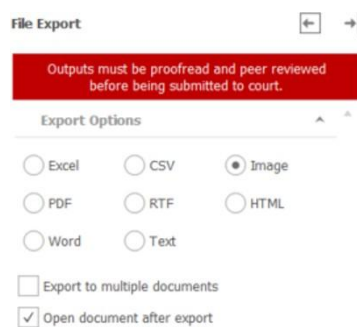
The 'Data Display' tab includes the 'Call index start point' control, which specifies that the first event in the dataset be given a specific sequence number rather than starting at 1 – this feature can be set to apply to the created output.

The Matching settings, both duplicate matching and single row matching, will be applied to the created output.

The Redaction settings will be applied to the created if you need some or all personally identifiable details to be redacted.

Export Sidebar

The 'Export' sidebar provides options to output the contents of the File List grid in a variety of formats:

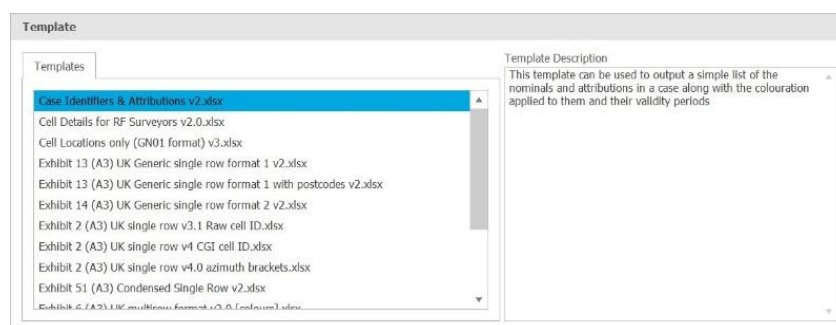


15.4 Output Formats

CSAS can output the selected data in one of several 'exhibit' or 'intel' templates or it can output a more analytical set of reports using one of the Fast Time Reports templates.

15.4.1 Selecting Templates

This function allows you to select a Template into which your chosen source files or case filter is output. Typically, the standard set of Templates (or formats) bundled with each CSAS installer package includes:



» 'Exhibit' formats - specifically created to be court-ready formats that can be printed as exhibits.

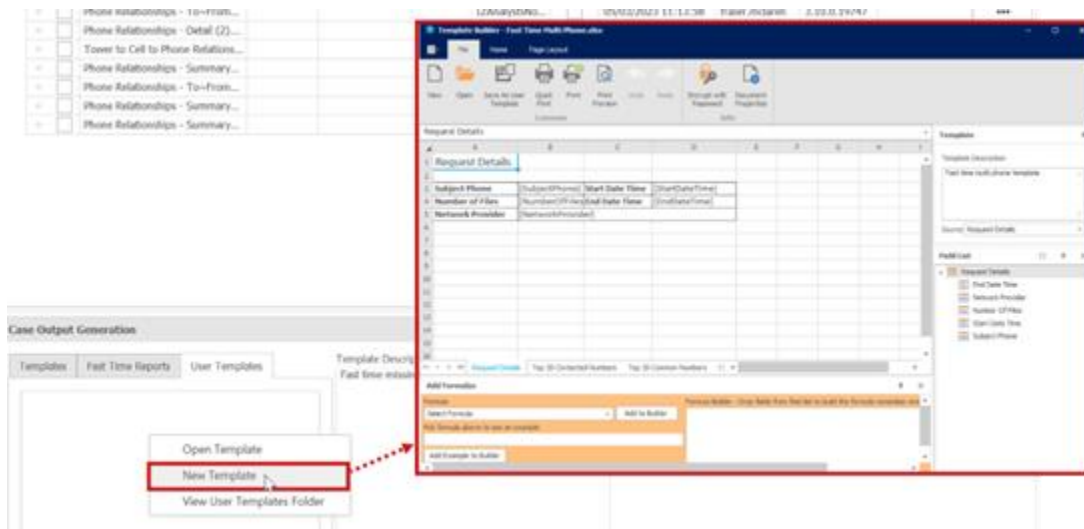
- 'Exhibit Format 2' – 3 format based on the single line format favoured by some police forces, displays both legs of a call (outbound and inbound) on a single line.
- 'Exhibit Format 6' - CSAS-specific 3 format, multi-line, full cell details designed for UK use with easting/northing for site locations.

- 'Exhibit 13 UK Generic 1' – 3 single-row format that matches the preferred style of many UK police agencies (with date/time columns on left of form).
- 'Exhibit 14 UK Generic 2' – 3 single-row format, same as Generic 1 but with date/time columns in centre of form.
- » 'Intel' formats – which provide full details of all call records, though not particularly suitable for printing once output to Excel due to the large number of data columns.
 - 'Cell Details for RF Surveyors' format - outputs cell details with additional information of use the RFPS surveyors.
 - 'GN01' format (generic cell details import form) - this template will only output the case cell details into the standard CSAS rescue format for cell addresses. This allows the form to be manually updated, if additional cell address details are available, and then reimported back into the CSAS case.
 - 'GN02' (or 'Rescue') format - the GN02 generic call details import format can be used as a generic 'rescue' format to import data from unrecognised formats and can also be used to export & reimport data into CSAS 'Full' information formats display content such as Cell ID, Cell Site Name, Azimuth and Site OSG, 'abbreviated' formats typically show only Cell ID and Site Name format. This format can be reimported back into CSAS if necessary.
 - 'Large Case' format (a minimal template with a single worksheet designed to allow very large cases to be output without crashing Excel).
 - 'Case Phones' format (produces an A4 sheet that lists the set of target phones in a case).
 - 'Cell Locations' only format (produces an A4 sheet that lists the cells in the case).
- » 'Intel Mode' formats (a set of output templates especially for Intel Mode that contain an extra column for an 'Intel?' indicator – if a record is an intel record it will have a 'Y', if it is an evidential record it will have an 'N'. Templates that contain the intel records column have the template file name suffixed with '_INTEL' and have 'INTEL ONLY' in the sheet headers):

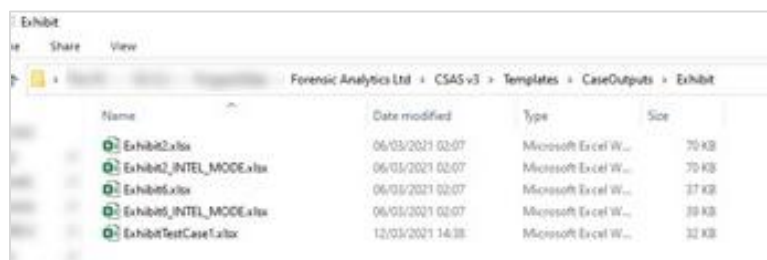
Note: When clicking on a Template, the 'Template Description' pane automatically provides a short description of each selected Template.

The Template panel has a right-click menu option from which you can select:

- » Open Template and New Template - both menu options open the Template Builder screen:



- » Check For Updates – this option allows CSAS to check to see if any new or update Case Outputs templates have been copied to the Templates folder and to add them to the Templates list if so.
- » View Templates Folder – this option opens a new screen displaying the location for all Case Outputs templates:



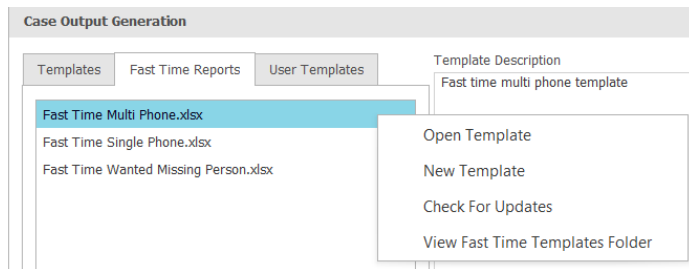
When new or updated template files are released, they need to be stored in the appropriate Templates folder, there are several ways in which this can be achieved:

- » Updated template files can be downloaded from the Forensic Analytics secure support website; we will issue email alerts when new files are available.
- » CSAS Support can email updated template files directly to users who have requested them.

After receiving or downloading updated templates, you just have to right-click in the Templates panel and select 'View Templates folder' and then paste the new file into the templates folder, then click 'Check for Updates' and the newly imported templates will then be available for use.

15.4.2 Selecting Fast Time Reports

This tab allows you to quickly create a customised report which only includes relevant source data about the requested subject identifiers. You can right-click inside this tab to edit an existing template or create a new template:



Once you select the Source data you want to include in your report, you can select a Fast Time template to export it in.

Fast Time reports give the ability to mix 'call schedule' type outputs, that provide formatted lists of selected case events, with 'analytics' style queries, such as 'top 10 contacts' or 'top 10 cells'.

Each element is output to a different tab of a multi-tab Excel workbook. It's possible to create customised Fast Time Report templates using the Template Builder.

Currently, there are three Fast Time Report templates, that have the following tabs:

- » Wanted Missing Person report:
 - Coversheet – request details
 - Linked IMEIs & IMSIs
 - Last 20 contacted numbers
 - Top 20 contacted numbers
 - Last 20 billing records
 - Wide area map
 - Last 10 cell locations map & data
 - Last 4 cell locations map & data
 - Call Distribution over Time
 - Most used cells
 - Glossary

- » Multi phone report:
 - Coversheet – request details
 - Top 20 contacted numbers
 - Top 20 common numbers
 - Event counts
 - SIM Swapping
 - Wide area map
 - Detail map
 - Location Detail maps

- Time of Day activity
- Most used cells
- Billing file details
- Glossary

» Single phone report:

- Coversheet – request details
- Linked IMEIs & IMSIs
- Top 20 contacted numbers
- Top 10 landline numbers
- Wide area map
- Top 10 cells
- Top 10 cell sites
- Call Distribution over Time
- Most used cells
- Glossary

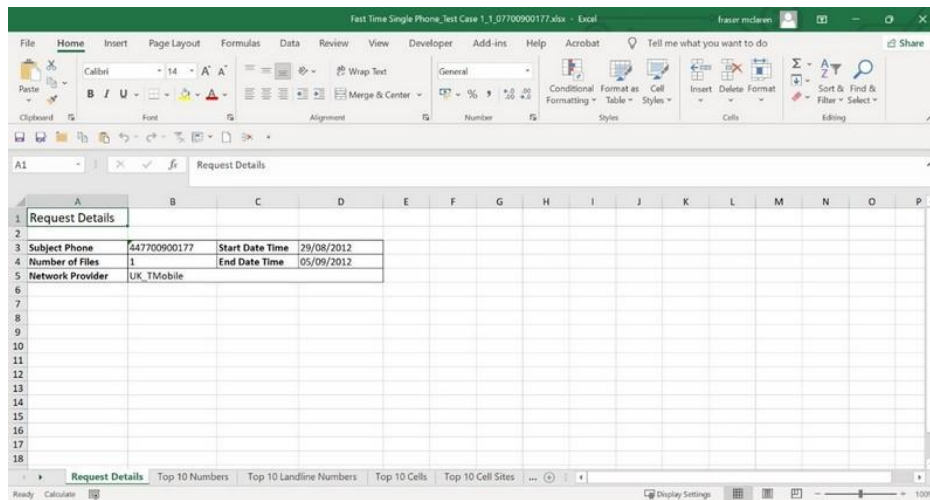
Note: Using the Template Builder, you can build your own bespoke template; however, we suggest you contact CSAS Support first for more information.

Why, When, Who

	This function is necessary to create analytical reports for specific subject phones.
	This function is undertaken whenever you want to create an analytical fast Time report in a case.
	This function is typically carried out by the following users: » CSAS User

Stepped Procedure

1. From the sidebar, select 'Filters' then from the 'Source data' pane, select the file(s) you want to export in a Fast Time Report.
2. From the 'Template' panel, select the Fast Time tab and select the required Fast Time template.
3. In the 'Options' panel, if you want a different filename to the one generated for you, in the 'Exhibit Output Filename' text field, enter the necessary filename.
4. From the 'Options' panel, if you have an exhibit reference number you want to add, enter it in the 'Exhibit Ref' text field.
5. To generate your Fast Time Report, click the button. A "Please Wait" pop-up message opens whilst your report is generating, then your report opens in the selected format:



In the 'File List' grid, your report is listed:



- In the 'File List' grid, at the end of the applicable row, you can Open or Delete a report by clicking in the 'Actions' column and from the drop-down menu select the necessary action:



- Case Outputs are created in Excel by default, if you would prefer your report to be saved in PDF format, find the report in the File List, click on the Actions button and select 'Export file to PDF in Landscape' or 'Export file to PDF in Portrait' as required.

15.4.3 Selecting User Templates

If, using the Template Builder, you edit an existing standard template or create a new one, the bespoke template gets added in the User Templates list. Custom templates get saved to your user profile and, in Server mode, should be available even if you log in to CSAS via a different machine.

15.5 Deleting a Case Output

This function allows you to delete a case output.

Files listed in the file list grid can be deleted using the grid right-click menu or the 'Actions' menu, both of which have an option to 'Delete file'.

The right-click menu has an additional option of 'Deleted selected files', which will work with a multiselect set of files from the list.

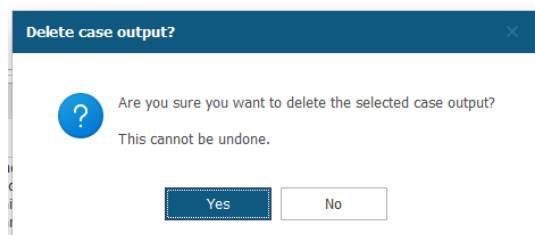
Output file deletion cannot be undone.

Why, When, Who

	This function is necessary to delete an existing case output.
	This function is undertaken anytime you need to delete a case output.
	This function is typically carried out by the following users: ➤ CSAS User

Stepped Procedure

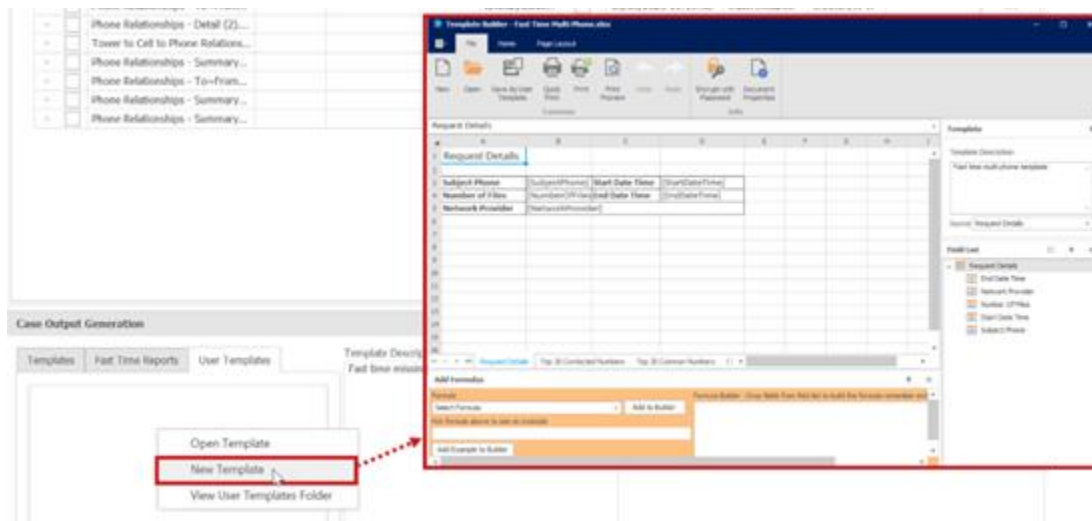
1. Before you try and delete an output, make sure the file isn't open, for example, in Excel.
2. In the grid, select the file you want to delete, right-click then select 'Delete file'. A pop-up message opens:



3. To delete the file, click on the **Yes** button. The selected file is removed from the File list Grid. The record of the file will be deleted from the CSAS database and the output file itself will be deleted from the Case folder.

15.6 Template Builder

Selecting the 'Open Template' or 'New template' options from any of the Templates panel right-click menus opens the Template Builder:



The Template Builder is designed to make it simpler for users to create and edit CSAS case outputs templates.

15.6.1 CSAS Templates

CSAS case outputs templates are created in Excel – the layout and design of each template is achieved using standard Excel formatting and editing techniques, where the column headers and other layout features are created using ordinary Excel text, fill colours and formatting.

The CSAS-specific content is added using a set of 'field tags'.

Field tags are linked to specific data fields in the CSAS case database – the use of a field tag essentially instructs CSAS to place the data from the relevant database field in a particular Excel cell.

	A	B	C	D
1	Call Ref	Start Date	Start Time	End Date
2	=@FIELD("Index")	=@FIELD("EventStartDateString")	=@FIELD("EventStartTimeString")	=@FIELD("EventEndDateString")

Standard Excel text, fill colours and formatting

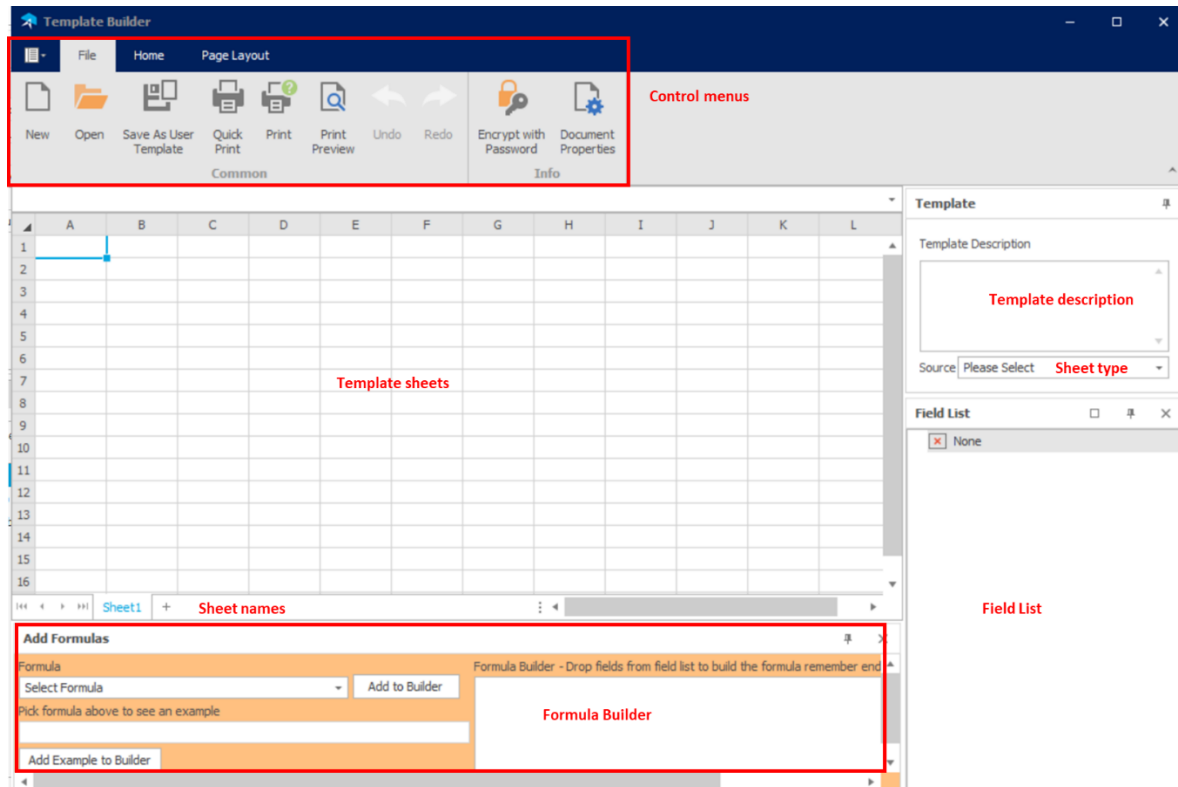
CSAS content 'field tags'

In the above example, the column headers in Row 1 of a template spreadsheet have been created using standard Excel text, filled in blue and had box lines placed around them. Row 2 hosts the field tags – cell A2 has the tag '`=@FIELD("Index")`', which instructs CSAS to add the event index number for each row in that column; cell B2 has the tag '`=@FIELD("EventStartDateString")`', which instructs CSAS to add each event's start date in that column; and so on.

The Template Builder offers a list of relevant field tags that can be used for different types of template, making it simpler to select the correct tag for the required type of output.

15.6.2 Template Builder Layout & Controls

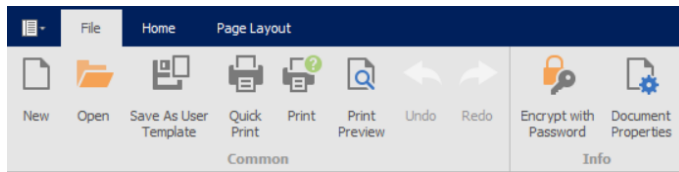
The Template Builder consist of the following elements:



- » Control menus – designed to mirror Excel controls to allow template files to be saved and formatted.
- » Template sheets – sheet contents can be viewed and edited in the main window.
- » Sheet names – in multi-sheet templates, each sheet has a tab, allowing you to switch between sheets when editing.
- » Formula Builder – helps you to build and insert Excel formulas into your template.
- » Template description – provides an opportunity to add text to describe a template and its intended purpose.
- » Sheet type – the 'source' menu allows you to define the use a sheet is designed to support.
- » Field List – provides a pick list of the data fields that are available for each source sheet type.

File menu

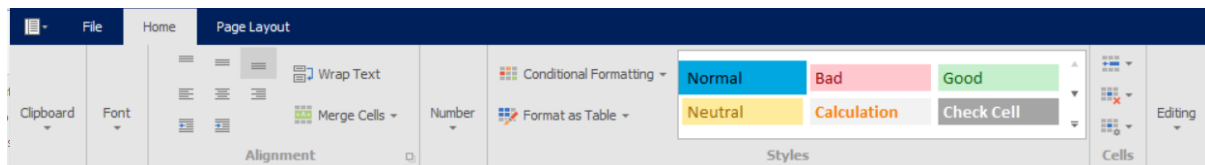
The File menu offers options for managing the template file, including:



- » New – create a brand-new template.
- » Open – open an existing template for editing.
- » Save as User Template – if you edit a prebuilt template, the edited version gets saved to your user profile as a 'user template'.

Home menu

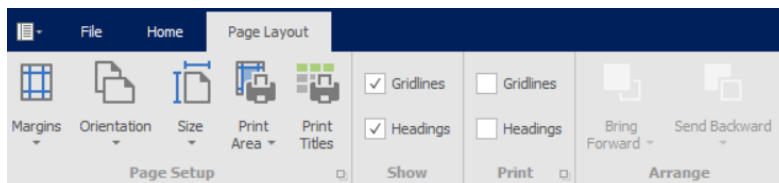
The Home menu offers some basic formatting controls, including:



- » Font – select a font for highlighted text.
- » Alignment – set text justification and set word wrap and cell merging options.

Page Layout

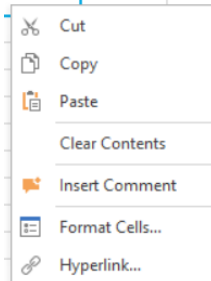
The Page Layout menu offers further editing options:



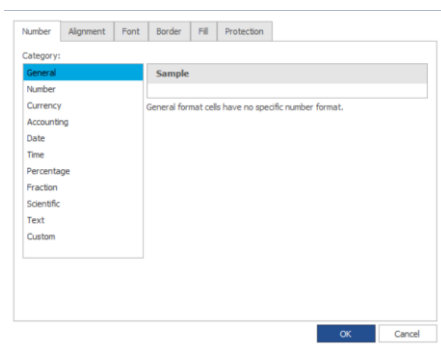
- » Margins – set page margins.
- » Orientation – select portrait or landscape.
- » Size – select page size – case outputs templates are often formatted as A3 size.

15.6.3 Template Formatting

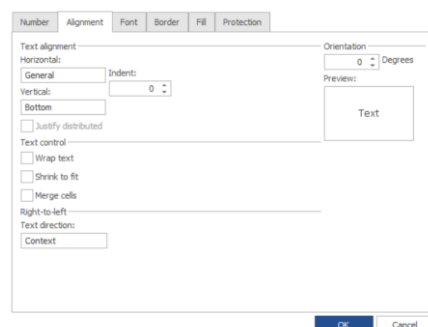
The Template Builder grid works in exactly the same way as an Excel spreadsheet (indeed, the output of the Template Builder *is* an Excel spreadsheet), so before you add fields, you may want to create the column layout and column headers for your worksheet the same as you would in a 'normal' spreadsheet.



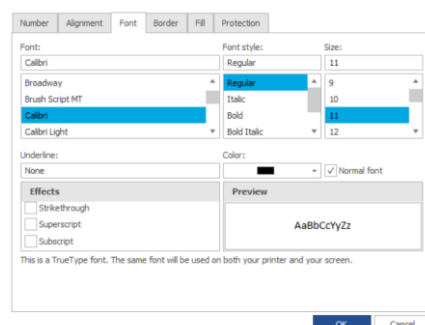
The template grid supports a right-click menu with a set of options that includes the Format Cells control, which in turn supports a number of useful formatting options.



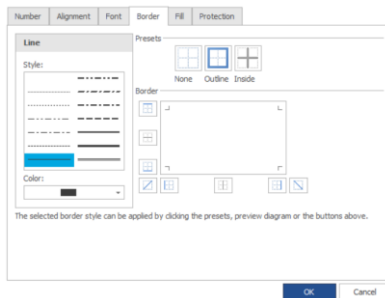
Number – as in the Excel equivalent, allows you to specify the format of a cell or column. It is useful to set the column type in a CSAS template, especially for date, time and numerical columns, to ensure that data is displayed correctly.



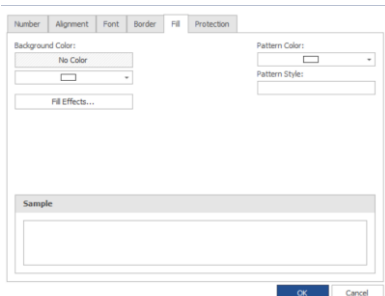
Alignment – these options are useful for formatting text in column header rows, especially if there is a requirement for text to shown in vertical alignment.



Font – this allows you to set the required font, font colour and text size, again, this is especially useful for formatting column header rows.



Border – this option provides control of the formatting of any boxing or borders applied in the template.

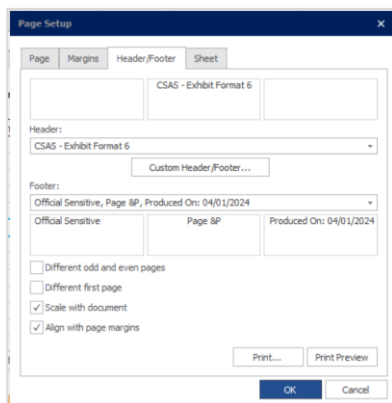


Fill – this option allows you to set in fill colour for cells, which is also useful for formatting the template's column header row.

15.6.4 Headers & Footers

CSAS case outputs templates often have specific header and footer data added to their layout. Headers can be used to show the case name or exhibit reference or to give each sheet in a report a title and footers are often used to show page numbers and security markings.

The Headers & Footers control is accessed via the Page Layout ribbon – click on the 'expand' button at the bottom right of the Page Setup section in the ribbon, then open the Headers & Footers tab in resulting popup.



The Excel header and footer each have three zones (left/middle/right), click on the zone you wish to edit.

Use the Header dropdown to select predefined fields, such as 'page number' and 'produced on date' or click 'Custom Header/Footer' to manually add text to a zone.

The header & footer details must be set separately for each sheet in the template.

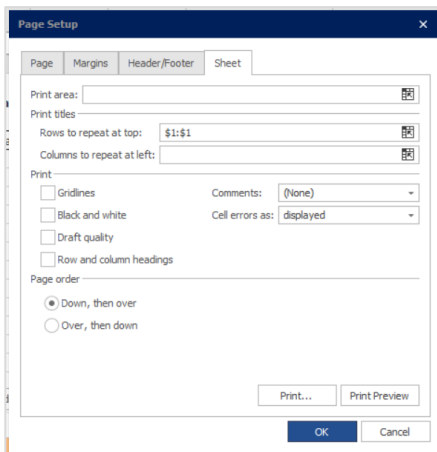
A subset of field tags (see below) from the Case Details source sheet type can be used to insert case specific information in the Excel sheet headers or footers, including

- » =FIELD("CaseName") to display the case name
- » =FIELD("ExhibitRef") to display any reference you've set for the output
- » =FIELD("OrganisationName") to display your organisation's name as a title

15.6.5 Repeat Column Header Row

Sheets that contain data grids can be set so that the column header row is repeated on

each new page.



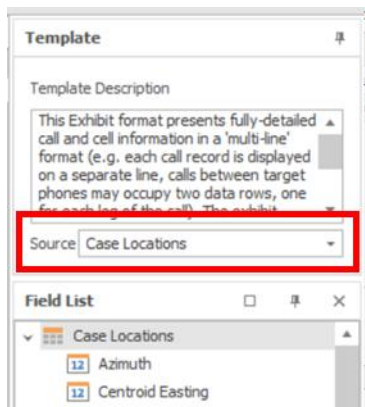
This option is accessed via the Page Layout ribbon – click on the 'expand' button at the bottom right of the Page Setup section in the ribbon, then open the Sheet tab in the resulting popup.

Click on the icon on the right of the 'rows to repeat at top' option and select the rows in the sheet that you wish to see repeated on each new page.

This must be repeated for each individual sheet in the template.

15.6.6 Sheet Types

CSAS templates can support a variety of different types of Excel worksheet and one template file can consist of multiple sheets.



The CSAS Template Builder lists the various supported types of sheet in the 'Source' dropdown.

When you create a new worksheet for a template, you need to select the required source sheet type, which will then prime the 'field list' with the correct set of field tag options for you to choose from.

Excel call schedule templates can support the following source sheet types:

- » Attributions – lists the subject identifiers in a case along with their assigned attributions and any validity period dates.
- » Case Details – lists details such as case name, organisation name, exhibit reference, etc.
- » Case Locations – lists the unique cells and cell IDs found in the case.
- » Multirow Case Events – lists cellular events for all selected subject phones in a 'multirow' format, where each call record is listed on a separate row.
- » Multirow Case Events by Target – creates a separate multirow output sheet for each individual selected subject phone.
- » Singlerow Case Events – lists cellular events for all selected subject phones in a 'singlerow' format, where the outgoing and incoming records for each event are merged on to a single row in the output.
- » Request Details – lists details of the source files that were selected for the output.

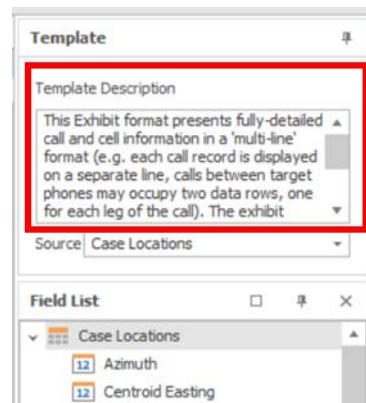
Fast Time report templates can support a number of analytical query types – these can be placed on a separate sheet per by selecting the appropriate 'source' option per sheet. The set of support Fast Time queries includes:

Coversheet – request details - o Billing file details - o Call Distribution over Time - o Detail map - o Event counts - o Last 10 cell locations map & data - o Last 20 billing records - o Last 20 contacted numbers - o Last 4 cell locations map & data - o Linked IMEIs & IMSIs - o Location Detail maps	- o Most used cells - o SIM Swapping - o Time of Day activity - o Top 10 cell sites - o Top 10 cells - o Top 10 landline numbers - o Top 20 common numbers - o Top 20 contacted numbers - o Wide area map - o Glossary
--	---

15.6.7 Template Description

When you create a new template, you can add a description to inform other users about the features available in the template or its intended use.

The description panel is in the top right of the Template Builder – simply enter the required description text in the panel and it will be saved with the template and displayed within Case Outputs.



15.6.8 Field Lists

Each source sheet type supports a limited set of field tags – each tag represents a CSAS case database field that is relevant to the source sheet.

The field tag names generally reflect in plain language the type of data the field represents, for example:

=@FIELD("CaseName") inserts the case name

=@FIELD("AttributionA") inserts the A or calling number's assigned attribution

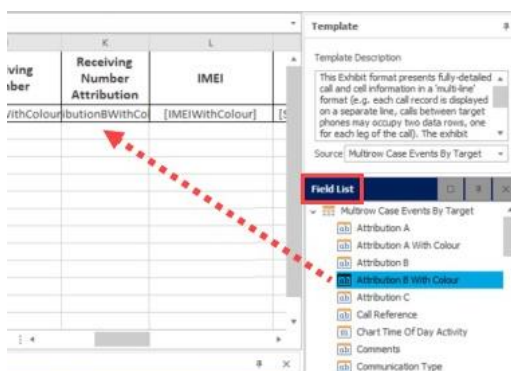
Some fields are available to be infilled with attribution colours – phone numbers, attributions, IMEIs, etc. These field tags have a version with a suffix of 'WithColour' added them, '=@FIELD("AttributionAWithColour")', for example.

Some fields that contain date or time data have tag versions that are suffixed with the word 'String' – '=@FIELD("DurationTimeString")', for example. The 'string' versions of these fields are designed to overcome Excel's occasional desire to format dates or times in a numerical format (e.g. converting the date 04/01/2024 to the number 45295). Specifying that the date or time is written as 'string' should prevent unwanted conversions.

Note – if a field tag for a required type of data doesn't exist, please contact CSAS Support to request it – it might be available to be added in a later release.

Once the correct 'source' sheet type has been selected, the Field List displays the set of available tags.

To use a tag in a template, click and hold on the tag in the field list and drag it to the required column and row in the template, then release the mouse button. The name of the tag will be shown in the selected Excel cell.



Receiving Number Attribution	Receiving Number	Receiving Number Attribution
	07700900177	Unknown 4
	07700900177	Unknown 4
own 6	07700900177	Unknown 4
own 5	07700900177	Unknown 4

In this example, the user wishes to populate a column in their template called 'Receiving Number Attribution' and they wish the column to show the attribution colour associated with each identifier.

The user selects the 'Attribution B with Colour' option from the Field list and drags it to cell K2 in the template.

The resulting output using that template looks like this, with the appropriate attribution name for the B number for each record shown in column K.

15.6.9 Excel Formula Field Tags

The Field Lists available for each source sheet type support many of the most commonly used CSAS data fields, but the list is not exhaustive – there may be fields or other content that isn't directly catered for with a field tag. CSAS templates support a limited number of Excel formula fields, that can be used to combine or separate data found in other fields. For example, if you wanted to have one column in a template that combined a record's cell ID, site name and azimuth in one column (rather than having three separate columns), the Template Builder allows the use of the Excel 'Concatenate' formula to merge several fields together. Alternatively, if for some reason you wished to only show the last 10 (least significant) digits of a phone number in a template, you could use the Excel 'Right' formula.

The 'Formula' dropdown lists the available formula types:

- » =CONCAT - concatenates or merges two or more fields together
- » =IF - builds an if/then statement
- » =LEFT - displays just the leftmost N characters from a field
- » =RIGHT - displays just the rightmost characters from a field
- » =MID - displays N characters starting from character M in a field
- » =VLOOKUP - performs a lookup on a list somewhere in the spreadsheet
- » =FILL - adds specific text to an Excel cell

The formulas are designed to work with the existing set of field tags or with specific text and you can also include separators in text fields.

For example, the CONCAT formula can be constructed using field tags like this:

=CONCAT(field1,field2,field3)

Or with separators, like this, with spaces and a comma between the merged fields:

=CONCAT(field1," , ",field2," , ", field3)

If you wished to view the start cell ID, site name and site postcode for a record merged into the same column, you would use the CONCAT formula as follows:

=CONCAT(FIELD("StartCGI")," , ",FIELD("StartSite")," , ",Field(StartPostcode"))

Which would result in a merged field that looked like this when populated:

First Cell ID	Last Cell Location
234-10-12049-38036 CANONBURY	234-10-12049-38036 CANONBURY
234-30-01153-14431 YATES HOUSE E2 6NU	234-30-01153-14431 YATES HOUSE E2 6NU

Alternatively, if wanted to show only the last 10 digits of the calling number in a column, you could use the RIGHT formula like this:

=RIGHT(FIELD("IdentityA"),10)

Which would result in a truncated field like this when populated:

Calling Number
7700900189
7700900621
7700900621
7700900621

Representative examples of each formula type are as follows:

CONCAT (fields)	=CONCAT(FIELD("StartCGI"),",",FIELD("StartSite"),",",FIELD("StartPostcode"))
CONCAT (text)	=CONCAT("Calls starting at ",FIELD("EventStartTime")," was made by ",FIELD("IdentityA")," and lasted ",FIELD("DurationTime"))
IF (fields)	=IF(FIELD("IdentityA")=FIELD("TargetIdentifier"),"Target","Other")
IF (text)	=IF(FIELD("IdentityA")="447700900123","Target","Other")
LEFT	=LEFT(FIELD("CommunicationType"),3)
RIGHT	=RIGHT(FIELD("StartPostcode"),4)
MID	=MID(FIELD("StartSite"),3,4)
VLOOKUP	=VLOOKUP(FIELD("Postcode"),Postcodes!A:D,4,FALSE),"")
FILL (empty cell)	=@FILL("")
FILL (specific text)	=@FILL("CDR")

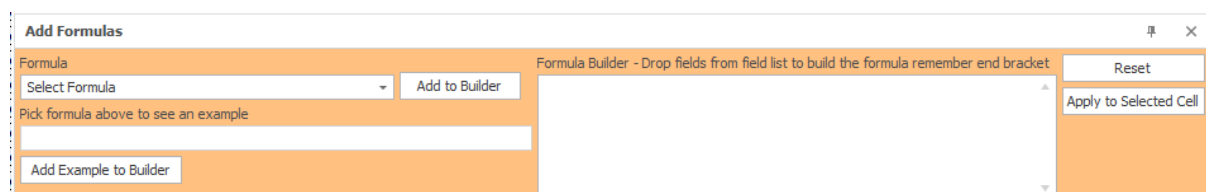
It is also possible to create formulas that combine two or more formula types, for example:

=IF(FIELD("Postcode")<>"", (VLOOKUP(LEFT(FIELD("Postcode"),LEN(FIELD("Postcode"))-2),Postcodes!A:D,4,FALSE)), "")

Which combines an IF and a VLOOKUP formula.

15.6.10 Add Formulas Panel

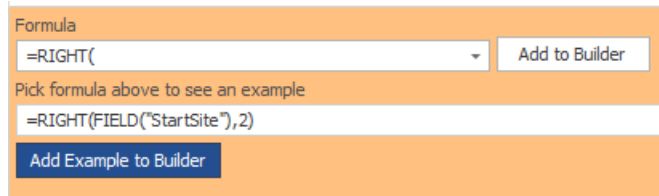
The Add Formulas panel in the Template Builder helps you to organise the elements that comprise an Excel formula.



Select the formula type to be used from the dropdown.

If you're confident that you understand the format or the required format, click 'Add to Builder' to add the basic version of the formula to the builder window – e.g. for the IF formula this would add just '=IF(' to the builder, ready for you to add the rest of the text.

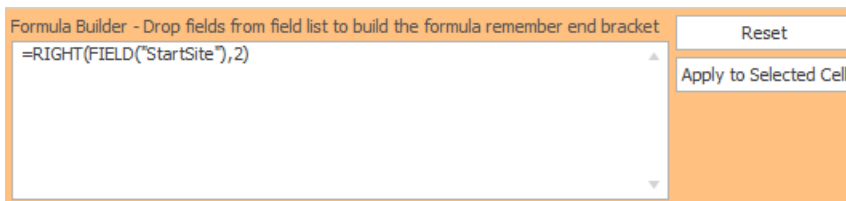
For users who are less familiar with Excel formulas, when you select a formula type, the template builder adds an example of a complete formula to the examples box:



Clicking 'Add Example to Builder' copies the entire example version to the builder box, you can then adapt it to your requirements by following the example provided.

Note - the example version of the formula may not contain the correct field tag(s) or other values for your specific requirement, so it will usually need to be edited before being used.

The 'builder box' is where you can construct and edit the full formula before sending it to the template.



As it says at the top of the builder box – do not forget to add the end bracket on the formula or the template will fail to run correctly, for example:

=MID(FIELD("StartSite"),3,4)

=CONCAT(FIELD("StartCGI"),",",FIELD("StartSite"),",",Field(StartPostcode"))

Unlike Excel, the Template Builder will not warn you if a formula is not correctly constructed.

When your formula is complete, click on the template cell you wish it to populate and click 'Apply to selected cell'.

Click Reset to clear the Formula Builder.

Why, When, Who

	This function is necessary to modify or create an output template which accommodates your requirements.
	This function is undertaken at any time you want to output a dataset into a template not provided by Forensic Analytics Ltd.
	This function is typically carried out by the following users:  CSAS User

Stepped Procedure

Create a New Template

To create a new template:

1. In Case Outputs, right-click anywhere in the appropriate Templates panel tab (i.e. if you wish to create a template, click in the Templates tab, if you wish to create a Fast Time report template, click in the Fast Time tab) and select 'New Template' – the Template Builder will open.
2. Select the required sheet type using the 'source' dropdown – if you are creating a multi-sheet template you'll be asked to return to this point for each new sheet.
3. Use the Excel editing facilities in the Template Builder to set the column header row text and formatting, including borders and fill colours. Also set the header & footer content and the 'rows to repeat'.
4. Use the Field List to select the required content for each column – select the field tag, click and hold, drag it to the appropriate column in the content row and release.
5. Repeat for all columns in the sheet.
6. If any columns require formulas, use the Formula Builder to create and add the required text.
7. If you need to create additional sheets in the template, return to step 2 for the next sheet.
8. Once all sheets have been formatted, add a template description, if required.
9. Save the template – give it a meaningful name. It will be saved to your 'User Templates' folder and will be available from that tab in Case Outputs.
10. Test the new template by selecting it in Case Outputs and outputting some case data.
11. If you wish to share the new template with colleagues, right-click within the User Templates tab and select 'View User Templates Folder'. Copy the Excel template file ready and distribute it using your preferred method.

Edit an Existing Template

To edit an existing template:

1. In Case Outputs, right-click on the template to be edited in the appropriate Templates panel tab (i.e. if you wish to edit a standard template, click in the Templates tab, if you wish to create a Fast Time report template, click in the Fast Time tab, if you wish to edit an existing custom template, click in the User Templates tab) and select 'Open Template' – the Template Builder will open.
2. Select the required sheet to be edited – if you are creating a multi-sheet template you'll be asked to return to this point for each new sheet.
3. If the sheet layout requires editing, use the Excel editing facilities in the Template Builder to adjust the content, layout or formatting.

4. Use the Field List to add or change select the required content for each column – select the field tag, click and hold, drag it to the appropriate column in the content row and release.
5. Repeat for all columns in the sheet that need editing or adding.
6. If any columns require formulas, use the Formula Builder to create and add the required text.
7. If you need to create or edit additional sheets in the template, return to step 2 for the next sheet.
8. Edit the template description, if required.
9. Save the template – custom and edited templates are saved to the User Templates folder and will be available from that tab in Case Outputs.
10. Test the updated template by selecting it in Case Outputs and outputting some case data.
11. If you wish to share the updated template with colleagues, right-click within the User Templates tab and select 'View User Templates Folder'. Copy the Excel template file ready and distribute it using your preferred method.

15.7 Exporting / Printing

This function allows you to Export or Print the contents of the output files grid. The ribbon at the top of the output list grid offers options to export the grid to Excel and to print the grid:



When you click on the  icon, the contents of the grid are exported to Excel.

When you click on the  icon, a print 'Preview' pop-up window opens. Clicking on 'File', 'View' and 'Background' gives you various options for page setup, tool bar, status bar, colour and watermark options.

The Export tab offers additional options for outputting the File List grid.

Why, When, Who

	This function is necessary to save a list of the output files created in a case.
	This function is undertaken at any time you need a list of the output files created in a case.
	This function is typically carried out by the following users: >> CSAS User

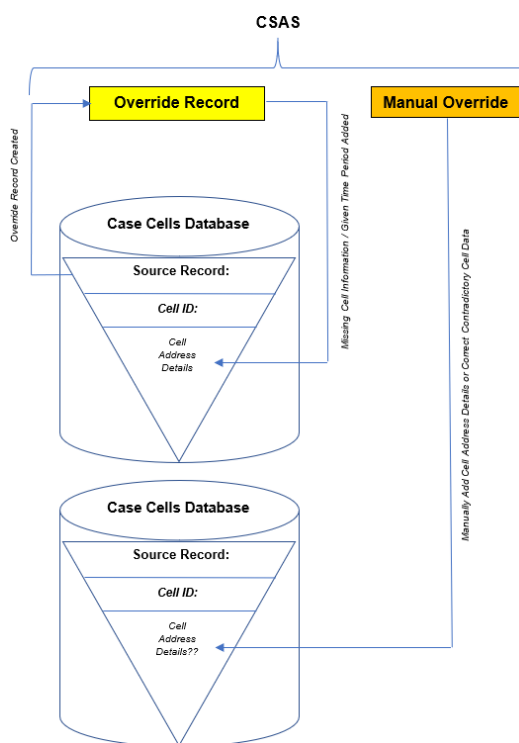
16 Using Case Cells

This function allows you to:

- » View details of the cells that are included in the call data in a case, so you can manage those cells in the event of data issues.
- » View details of other case locations, such as ANPR/ALPR cameras.
- » Manage Source Records and Override Records effectively and to manually create Master Records.
- » Create a Manual Cell record for a cell ID to replace the imported cell data in the event that CSAS is provided with contradictory data.
- » Manage the settings used by the case cells control, so you can vary the way that cell details are handled in different scenarios.

16.1 Hierarchical View of Cell Records

Case Cells comprise a three-layer structure:



- » Source Records - Each unique and different set of cell address details (even if the address details are all blank) found for a cell ID within the imported data for a case has a Source Record created for it in the case cells database; call records are linked to a Source Record to add cell address details to Case Hub and other screens. Source Records for a cell ID are sequentially numbered in the order in which they were encountered in the source data files.
- » Override Records - When a new Source record is created for a cell ID, CSAS also creates an 'Override' record.

This is used to fill in any missing cell information in Source records for a given time period, which is known as the override record's 'validity period'. If CSAS is operating in 'override' mode and if a source record is to be used that has missing details (e.g. missing postcode or azimuth), CSAS will attempt to fill in the missing information from an Override record.

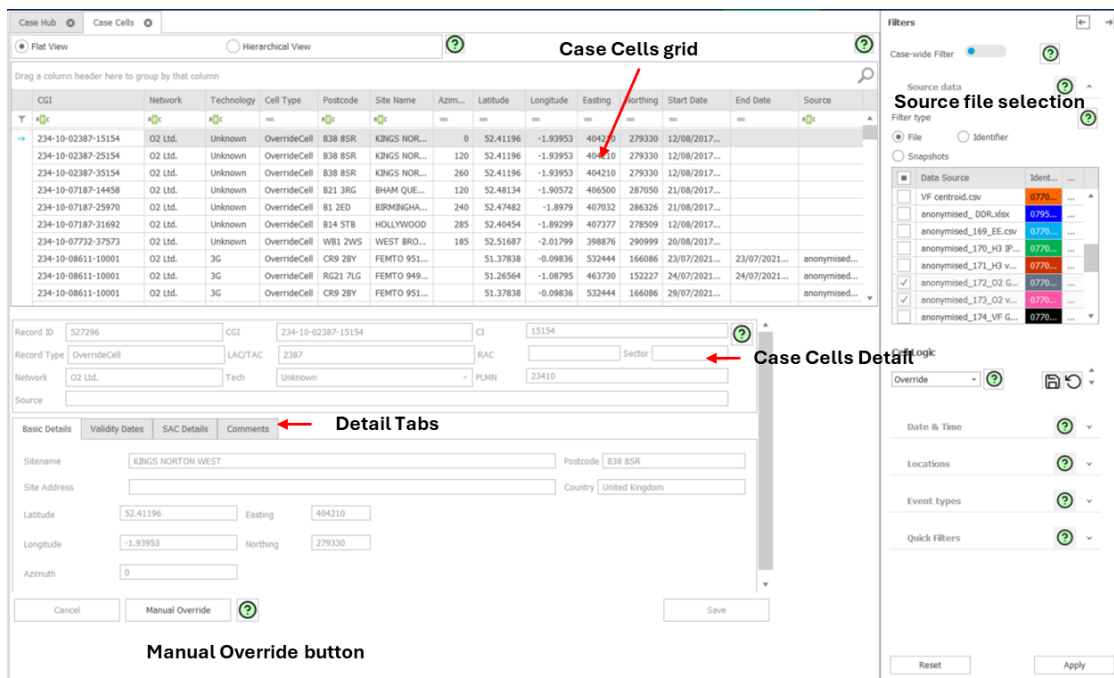
If, over time, the information provided for a cell ID changes, an Override record is created for each distinct and different set of details. When applying override data, CSAS will choose the override record that covers the period of time in

which the associated call was made.

- Manual Override – A Manual Override record can be created when you want to manually override the imported details for a cell. This would only usually be required if there were either no cell address details provided for a cell in a format that could be imported into CSAS or if the cell details that were provided in different files or records were too fragmentary or contradictory to be used automatically. The manual override process is also used for some operator-specific purposes, for example, to add a specific cell ID in place of an O2 3G SAC. If there is a Manual Override record created for a cell it will always be used in the viewing and analysis of event data and any Source or Override records created for that cell ID will be ignored.

16.2 Layout

The Case Cells screen is a single window with two panes housing tabs, option boxes, buttons and various right click filters:



The screenshot displays the CSAS Case Cells interface. At the top, there are tabs for 'Case Hub' and 'Case Cells'. Below this, a 'Case Cells grid' is shown with columns for CGI, Network, Technology, Cell Type, Postcode, Site Name, Azim..., Latitude, Longitude, Easting, Northing, Start Date, End Date, and Source. A red arrow points to the 'Case Cells Details' section, which contains fields for Record ID, Record Type, Network, and Source. Below this, 'Detail Tabs' are visible, including 'Basic Details', 'Validity Dates', 'SAC Details', and 'Comments'. A red arrow points to the 'Manual Override' button. On the right side, there are 'Filters' and a 'Source file selection' panel with a list of data sources and a 'Filter type' dropdown. At the bottom right, there are 'Reset' and 'Apply' buttons.

- Case Cells Window:
 - 'Flat View' and 'Hierarchical View' radio buttons.
- Case Cells Grid.
- Case Cell Details.
- Detail Tabs
 - Basic Details tab
 - 'Validity Dates' tab
 - SAC Details tab
 - Comments tab

The content of Case Cells is controlled using the sidebar filters. Select the source files for which you wish to see cell details from the Filters sidebar – if you wish to see details of all case cells, select all case files.

Case Cells functions are available by clicking on the  button from the Case Home screen (or by other screen prompts). The 'Case Cells' screen opens:

16.3 Viewing and Updating Cell Records

Clicking on any row in the (upper) Case Cells Grid will change the cell details displayed in the (lower) Case Cells Detail panel.

A subset of cell details shown in the Case Cells Detail panel can be edited or added if required, but if a cell record is edited in this way it creates a Manual Cell record that replaces all imported data for the cell.

16.4 Grids and Controls

16.4.1 Grid and Column Controls

The Case Cells grid shares a common set of filtering and layout controls with the other grids in CSAS. Details of how to apply filters, customise the column layout and other grid control options are provided in [Grid Filtering and Controls](#).

The grid can be filtered to show the details of a single cell ID or site name by using the 'auto-filter' bar at the top of the grid (and entering the name of the cell ID/site you wish to view) or by using the column filter in each column (using the 'filter' icon and drop-down menu in each column header).

16.4.2 Grid

The 'Case Cells' grid contains the following columns:

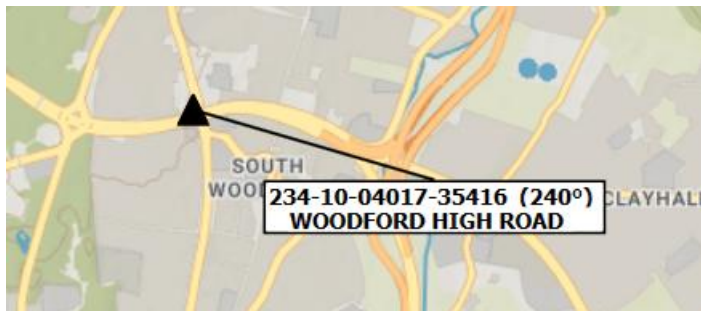
- » CGI – lists the unique cell ID for each cell detected in the case data. This forms the database 'key' for each record and cannot be edited.
- » Network – shows the network the cell belongs to (if known).
- » Technology – shows the technology used by the cell – for example 2G, 3G, 4G, 5G (if known).
- » Cell Type – shows the cell record type Manual, Override or Source.
- » Postcode – shows the cell site postcode (if known).
- » Site Name – shows the name assigned to the cell site in the source data (if known)
- » Azimuth – shows the cell azimuth for the current record (if known).
- » Latitude/Longitude/Easting/Northing – show the map coordinates for the cell site.
- » Start Date/End Date – shows the 'validity period' for the record, especially important for Override records.
- » Source – shows the file the record was captured in.

16.4.3 Right-click and Actions menus

The Case Cells grid supports a right-click menu with one option:

234-10-04017-14719	O2 Ltd.	2G	Over
234-10-04017-14719	O2 Ltd.	Unknown	Sou
234-10-04017-24	Send cell(s) ONLY to map		
234-10-04017-24	O2 Ltd.	2G	Over

This options sends the location of the selected cell(s) to a CSAS map tab – this option works as a multi-select, so details of multiple cells can be sent in one go.



As only details of the cell locations (and no details of any calls made via those cells) are sent to the map, it is not possible to include any attribution colours in the map, so the cell sites are represented using the Black Triangle option.

Other usual map features, such as the cell coverage visualisation option, will work normally.

16.4.4 Case Cells Detail panel

The lower half of the Case Cells screen displays detailed information for a selected cell ID.

Record ID	527296	CGI	234-10-02387-15154	CI	15154
Record Type	OverrideCell	LAC/TAC	2387	RAC	
Network	O2 Ltd.	Tech	Unknown	PLMN	23410
Source					

Basic Details		Validity Dates		SAC Details		Comments	
Sitename	KINGS NORTON WEST			Postcode	B38 8SR		
Site Address				Country	United Kingdom		
Latitude	52.41196	Easting	404210				
Longitude	-1.93953	Northing	279330				
Azimuth	0						
Cancel		Manual Override		Save			

The details in the grid are usually greyed out and cannot be altered, unless you elect to create a Manual Override record, see below.

The top section of the Case Cells Detail panel provides general information for the selected cell, including cell ID, and network and also details of the imported source file from which the details were captured.

Below this, there are a set of tabs, each displaying a specific set of cell information:

- » Basic Details tab – displays the site name and any site location information (address, map coordinates) along with the cell's azimuth.
- » Validity Dates tab – shows the date period within which this set of details is

valid.

- » SAC Details – provides an opportunity to manually add cell IDs to be used in place of the SAC (Service Area Code) for some 3G cells.
- » Comments – provides an opportunity to add cell-specific notes.

16.4.5 Choosing Different Views

This function allows you to choose between:

- » Flat View.
- » Hierarchical View.

The 'Case Cells' screen opens with the Case Cell Details grid in 'Flat View':

Flat view shows all types of record (source, override and master) for all cell IDs in one list, meaning that the same cell ID might be listed multiple times if there are multiple different records and types of record for it. The list can be filtered to view only source or override or master records if required. Flat View is generally more useful for comparing changing address values for a cell over time.

Selecting 'Hierarchical View' changes the layout.

The Hierarchical View segments the cell records into their different types and shows only Override records initially. An Override record can be opened (by clicking on the small + symbol to the left of each cell ID). A 'child' menu opens to show the corresponding Source records that are associated with each Override.

Hierarchical View shows you how the changing data for the same cell ID is related over time.

16.4.6 Sidebars

Case Cells uses the same standard 'Filters' sidebar as other screens. The cell details to be viewed are selected via the 'Source data' tab using the File, Identifier or Case Snapshot options.

You can choose to view the cell details from just one source file or from a set of source files; you could choose to view the cell details associated with just one identifier or with many/all identifiers, or you could choose to view the cell details associated with a Case Snapshot (currently you can only select one Case Snapshot at a time to view).

You can also choose to use any of the other filters in the sidebar (date/time, timeslice, location or event types) to edit the dataset before viewing the associated cell details. For example, you may want to apply a date/time filter and view only details of the cells that were used during that period, or you might apply a Location filter and view only details of cells found within that area.

Note: The Cell Logic setting has no effect in this screen.

16.5 Editing Case Cell Records

Cell records can be edited, for example, to provide information that was missing from any automatically imported data. The editing process for any cell record creates a Manual Cell record that then replaces all other instances of cell data for that cell ID.

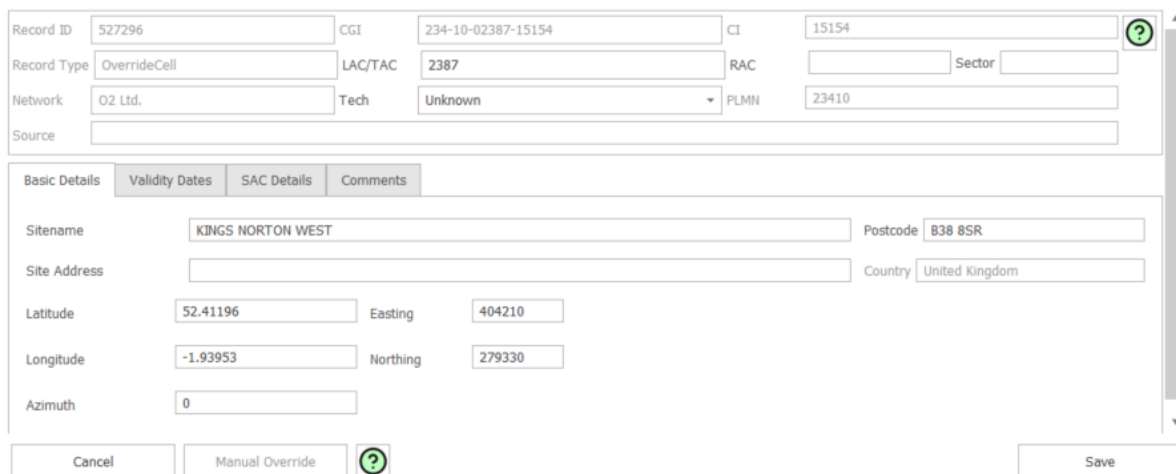
16.6 Manual Override Records

A Manual Override record can be created when you want to manually update the details of a cell.

This would only usually be required if there were either no cell address details provided for a cell in an importable format, or if the cell details that were provided in different files or records were too contradictory to be used automatically. If there is a Manual Override record created for a cell, it will always be used in the viewing and analysis of event data, and any Source or Override records created for that cell ID will be ignored.

When a ManualCell record is created, it is imposed on every call record that references that cell ID in place of the original cell data. If used inappropriately, a ManualCell could be classed as 'manufactured' evidence. If a ManualCell is created and is used in a case that goes to court, we strongly recommend detailing the reasons for the use of the ManualCell in a statement to be submitted along with the call schedule.

You can select a cell to edit by highlighting it in the main grid and then clicking on the **Manual Override** button, the stored details for that cell record are then shown in the lower part of the control screen, you can then edit the information using the text fields and drop-down menus to create a manually edited set of cell address details. If a Manual Override has been created it will override all Source and Override records for the associated cell ID, only the Manual Override details will be displayed for that cell ID:



Note: The 'CGI' (Cell Global Identifier) field cannot be edited as this is a database 'key' field for the record.

You can also edit the information in the 'Validity Dates' tab by unchecking the box; the fields become 'live' and you can then use the drop-down menus and calendars to amend the dates:

To ensure any edits made are saved in the database, click on the **Save** button. Details of any edits made will be captured in the Audit log.

Why, When, Who



This function is necessary to manually update details for cells that have been discovered as part of the case data.



This function is undertaken only if the automatically discovered address data for a cell is incorrect or if there are contradictory sets of address data for the same cell – we recommend speaking to CSAS Support before using this feature for the first time.



This function is typically carried out by the following users:

» CSAS User

16.7 Defining O2 3G SAC Cells

This function allows you to deal with a specific issue experienced with O2 UK 3G cell data – as 3G is in the process of being decommissioned, this is unlikely to be an ongoing issue. Uniquely, O2 UK originally decided to describe its 3G cells using a value called the SAC (Service Area Code) and instead of capturing a cell ID for each 3G cell in their CDRs they instead showed a shared SAC, which could generally relate to up to 3 individual cells. This has meant that it is sometimes not possible to determine which 3G cell carried a call from O2 CDRs. It is possible to perform a lookup on O2's 'sort cellar' database and get the details of the individual cell IDs that share each SAC and from that it is also possible to manually select one of those specific cell IDs to display in CSAS, but this requires the creation of a Manual Cell record.

This issue is particularly pertinent if a user wishes to link O2 CDR records with RF Survey data. The SAC is not broadcast on a cell's control channels, only the cell ID gets broadcast. If a CDR record only contains a SAC and not a cell ID, it is not possible to link RF Survey data that includes that cell with CDR records for connections that used that cell. By setting a specific cell ID for the 'SAC-only' cell, it gives CSAS an identifier it can use to link to RF Survey data. Generally, cells that share the same SAC are transmitted from the same site and the same antenna and can be expected to share a common coverage area, so if the correct cell IDs for the SAC are used, it generally doesn't make a huge amount of difference which of the cell IDs is selected in CSAS, the resulting plotted RF Survey coverage area will be applicable to either cell ID.

An example of how this would be used:

- » A source CDR contains details of 3G calls made via a cell of the Broadgate North cell site.

234-10-21001-00000-10261	O2 Ltd.	3G	SourceCell	EC2A 4LB	BROADGATE NORTH (OFFLOAD 1801_S1)
--------------------------	---------	----	------------	----------	------------------------------------

- » The individual cell ID wasn't captured, just the shared SAC assigned to both cells on the same sector of that site. The SAC is 10261 and the cells' LAC is 21001.
- » Initially, CSAS would create a CGI of 234-10-21001-00000-10261 – with the cell ID portion blank (00000) and the SAC (10261) added to the end.

End CGI	End Site
	= BROADGATE NORTH (OFFLOAD 1801_S1)
234-10-21001-00000-10261	BROADGATE NORTH (OFFLOAD 1801_S1)
234-10-21001-00000-10261	BROADGATE NORTH (OFFLOAD 1801_S1)
234-10-21001-00000-10261	BROADGATE NORTH (OFFLOAD 1801_S1)

234-10-21001-00000-10261 (90°)						
BROADGATE NORTH (OFFLOAD 1801S1) EC2A 4I						
Ref	Type	S/E	Date	Time	Calling	Called
4520	D	(E)	31/07	18:22:52	5091	Data
4519	D	(E)	31/07	18:22:59	5091	Data
4521	D	(E)	31/07	18:23:36	5091	Data

If the user has searched in 'sort cellar' and has determined that the two possible cell IDs for that SAC are 10098 and 22098 and they want to use one of those cell IDs in their CSAS data, in place of the supplied SAC, they can use the Manual Cell process to select it.

Who, When, Why

	This function is necessary to define a particular 3G cell ID rather than a 'shared' 3G SAC.
	This function is undertaken at any time Case Cells is selected.
	This function is typically carried out by the following users: >> CSAS User.

Stepped Procedure

The SAC Cell fields on the Case Cells screen allows you to add the 'missing' cell IDs to be associated with a SAC:

- For each SAC cell that needs to be updated, select the required cell from the Case Cells grid.

CGI	Network	Tech...	Cell Type	Postcode	Site Name	Azim...
		= 3G	=			=
234-10-09311-10001	O2 Ltd.	3G	SourceCell	SE8 4AF	FEMTO 949511	
234-10-21001-00000-10261	O2 Ltd.	3G	SourceCell	EC2A 4LB	BROADGATE NORTH (OFFLOAD 1801_S1)	90
234-10-21001-00000-24491	O2 Ltd.	3G	SourceCell	EC2A 3QA	CURTAIN RD (4523 REPL)	350

- Click on Manual Override to open the record for editing.
- Open the SAC Details tab for the record.
- Add the specific cell IDs to the 'SAC Cell' fields for that cell.

Record ID	525410	CGI	234-10-21001-00000-10261	CI	
Record Type	SourceCell	LAC/TAC	21001	RAC	
Network	O2 Ltd.	Tech	3G	PLMN	23410
Source	anonymised_172_O2 GPRS.csv				

Basic Details	Validity Dates	SAC Details	Comments
---------------	----------------	-------------	----------

SAC	10261
SAC cell 1	10098 ☐ Use cell 1 as part of CGI
SAC cell 2	20098 ☐ Use cell 2 as part of CGI
SAC cell 3	☐ Use cell 3 as part of CGI

- Optionally, add comments to the Comments tab to indicate the source of the additional information.

Basic Details	Validity Dates	SAC Details	Comments
SAC details obtained from O2 SortCellar 03/06/2024			

- Save the Manual Override record.
- Select the ManualCell record in the Case Cells Grid again and open the SAC Details tab.
- Select which cell ID(s) will be displayed for the cell by ticking the required SAC Cell entries.

Basic Details	Validity Dates	SAC Details	Comments
SAC 10261			
SAC cell 1	10098	☒	Use cell 1 as part of CGI
SAC cell 2	20098	☐	Use cell 2 as part of CGI
SAC cell 3		☐	Use cell 3 as part of CGI

- Click **Save**.
- The ManualCell record for that cell will be updated to show the selected cell ID instead of the original SAC.

CGI	Network	Tech...	Cell Type	Postcode	Site Name
		= 3G	=		= BROADGATE NORTH (OFFLOAD 1801_S1)
234-10-21001-00000-10261	O2 Ltd.	3G	SourceCell	EC2A 4LB	BROADGATE NORTH (OFFLOAD 1801_S1)
234-10-21001-10098	O2 Ltd.	3G	ManualCell	EC2A 4LB	BROADGATE NORTH (OFFLOAD 1801_S1)

- View the cell's data in Case Hub and confirm that the required cell ID is being displayed in place of the original SAC.

End CGI	End Site
	= BROADGATE NORTH (OFFLOAD 1801_S1)
234-10-21001-10098	BROADGATE NORTH (OFFLOAD 1801_S1)
234-10-21001-10098	BROADGATE NORTH (OFFLOAD 1801_S1)
234-10-21001-10098	BROADGATE NORTH (OFFLOAD 1801_S1)

234-10-21001-10098 (90°)						
BROADGATE NORTH (OFFLOAD 1801S1) EC2A 4L						
Ref	Type	S/E	Date	Time	Calling	Called
4520	D	(E)	31/07	18:22:52	5091	Data
4519	D	(E)	31/07	18:22:59	5091	Data
4521	D	(E)	31/07	18:23:36	5091	Data

If any RF Survey data for the associated cell has been imported, it should now be possible to view that RF coverage data in Case Hub.

16.8 Printing and Exporting

Currently there is no Print/Export option available in this screen.

17 Using Analytics

This function allows you to choose various Analytics functions and further filter the selected source data displayed before running the query and getting analytical results.

In CSAS v2, Analytics queries were grouped by the scope of the source data – queries were grouped into sets that related to Target Phone, Target Pair, Target Group, etc.

In CSAS v3, those distinctions have been removed and most queries are able to use any mix of source data – a single file for one phone, all files for one phone, a mix of files for several phones, all files for all phones.

There are some queries where it's probably not sensible to mix data for multiple phones (IMEI Summary, for example, unless you're looking at data for different SIMs that all used the same handset) and there are some queries that will ignore some kinds of data (First Cell Last Cell only works with CDRs, for example, and will ignore ANPR or handset data).

CSAS can also work from previously saved Case Snapshots, allowing you to create complex datasets in Case Hub before opening an Analytics query.

Finally, it is also possible to send selected data from Case Hub directly to a selected Analytics query via the right-click menu.

CSAS Analytics queries are intended to offer answers to the most frequently asked questions concerning digital forensics data, the current set of queries are:

- » **Activity Hotspot** – This query provides a simple visual indication of the levels of activity for the selected subject phones over time. The call activity grid is colour coded in accordance with the frequency of calls, with periods with low call volumes shown in light colours and periods with heavier usage shown in darker colours.
- » **Average Event Distribution** – This function window displays an event distribution graph, showing the average amount of activity recorded for the selected target phone(s) in particular time periods. The graph is switchable between different units of time – hour of day, day of week, month of year - which alters the data the graph displays and shows, for example, what on average is the busiest hour of the day for the selected subject phones.
- » **Cell Usage** - This query populates three panes:
 - The 'Summary List' pane lists the unique cell IDs found in the selected dataset ordered by those that are most heavily used, to offer a view of the cells used most often by the selected subject phone(s).
 - The 'Top 10 Cells' bar chart highlights the top ten cells with the highest event counts.
 - The 'Hotspot Chart' pane contains a time-based grid (hours vs days) that seeks to expose any patterns associated with the use of particular cells – for example, the subject phone only ever uses Call 1 on Saturday afternoons.

Note: The data displayed in all three panes is selectable between cell ID

(CGI and Raw) and it can also be switched to aggregate the cell counts by site and by sector (site + azimuth).

- » **Concurrent Calls** – This query provides details of times when two phones (or members of two groups of phones) were in use concurrently and can be used as a way of determining whether those phones could have been in use by the same person (if there were few concurrent calls) or by different people (if there were many concurrent calls).
- » **Contact Summary** – This query lists the set of other identifiers that have been in contact with the selected subject identifiers and itemises the details of those contacts in the form of the total number of Outgoing and Incoming connections of various types.
- » **Contact Summary by Date Range** – This query lists the 'other' contacted numbers for the selected subject identifiers and summarises those contacts by time period – hours/days/week/months – to expose any time-based patterns of contact, such as 'who did the subject contact the most during this time period?'.
- » **Contacts Between** – This query provides details of the levels of contact (a count of calls and texts) between different identifiers in the selected CDR files. The 'New Details View' drill-down provides a detailed breakdown of the contacts between two selected numbers – showing the number of incoming/outgoing contacts between them for each date on which contact took place.
- » **Correlation Query** – this query is designed to search for common information across a large dataset, e.g. looking for phone numbers that appear in multiple cell dumps.
- » **Drug Line Analysis** – This query uses a methodology developed by UK narcotics investigators to estimate the number of 'deals' being done and the resulting volumes of drugs being distributed by a drugs gang based on an analysis of the cellular data associated with the gang's mobile devices. The Drug Line Analysis window has two main parts: a control ribbon where you can select different filter options and a report grid.
- » **First Cell Last Cell** – This function window displays two panes:
 - The 'Activity' pane displays a grid showing the 'First Cell' used in each contiguous period of activity and the 'Last Cell' used in each period for the selected subject phones.
 - The 'Summary' pane displays a grid that summarises the set of cells used for first or last call during the period.
- » **IMEI Summary** – This function window displays three panes:
 - The 'Summary List' pane displays the detected International Mobile Equipment Identity (IMEI) numbers that have been used in conjunctions with the selected target phone(s).
 - The 'Chronological List' pane provides an indication of the time periods and numbers of calls that were recorded whilst each pair of IMEI and MSISDN were in use together.

- The 'Unique List' pane displays a simple list of the unique IMEIs that were used by each target phone, listed by 'First used' and 'Last used' dates/times and a count of the number of events registered for each pairing.

Note: The data displayed in all panes is selectable between being focused on the IMEIs and being focused on the associated MSISDNs via two radio buttons at the top of the window.

- » **Inactivity Chart** – Understanding the periods of inactivity for a subject phone can sometimes be as instructive as analysing their periods of activity. This query highlights configurable periods of inactivity for the selected subject identifiers and provides details of the last event for the selected phone(s) before the inactive period and the first event after the inactive period ends.
- » **Pivot Builder** – This query allows you to build a variety of reports using a set of prebuilt templates, each of which can be customised using the various fields and tab filter drop-down menus. The queries include versions that deal with ANPR data, with CDR data and with POI Location data and also include specialised queries such as the Courier Fraud query.
- » **Potential Colocation** – This query detects times when two or more target identifiers (phones or vehicles) could have been close to each other or to any case locations, based on comparing the records in the selected dataset against two parameters: 'Time (seconds)' - which refers to the time difference between events for the subject identifiers being considered by the query, and 'Distance (km)' - which refers to the geographical distance within which the comparison is made, based on the location of cell site(s).

17.1 Layout

Each Analytics function opens in a separate tab and allows you to analyse the selected source data files.

Each pane in a given Analytics query opens in a separate window and allows you to analyse the selected source data files.

Queries have one or more information panes, each of which can be exported, printed, minimised and maximised. All Analytics queries can be accessed via the Case Home navigation panel.

You can select each Analytics query by clicking on the relevant icon in the drop-down menu. The selected function will open in a new CSAS tab.

To populate the grid, you will need to open the Sidebar Filters tab and select the required files, identifiers or Case Snapshots; it's also possible to send data directly from Case Hub into a selected Analytics query, by using the grid right-click 'Analytics' option.

17.2 Grids and Controls

17.2.1 Grid Columns and Layout Controls

The Analytics grids share a common set of filtering and layout controls with the other grids in CSAS. Details of how to apply filters, customise the column layout and other grid control options are provided in *Grid Filtering and Controls*.

17.2.2 Controls

At the top right-hand side of each Analytics function window is a series of shortcut buttons:



Each shortcut button allows you to:

- » **Export** – clicking on the  button exports the query results into Excel.
- » **Print** – clicking on the  button allows you to print the query results via the 'Print Preview' pop-up window.
- » **Collapse** – clicking on the  button closes the associated query pane to allow other panes to be more easily viewed. Clicking on the  button again unrolls and restores the pane.
- » **Maximise** – clicking on the  button maximises the display so the query occupies the whole window. Clicking on the  button again restores the query to its original size.

17.2.3 Sidebar Tabs

The sidebar has 3 tabs. Selecting checkboxes and options in each tab changes what information is displayed by the Grid. From the sidebar, you can select the following tabs:

- » Filters tab
- » Settings tab
- » Export tab.

Filters Tab

All Analytics queries use the same standard 'Filters' tab as other screens. The data you want to query is selected using the 'Source data' panel using the File, Identifier or Case Snapshot options:

- » You can choose to query the data from just one source file or from a set of source files.
- » You could choose to query the data for one or more identifiers.
- » You could choose to query the data from a Case Snapshot (currently you can only select one Snapshot at a time to query).

The Cell Logic setting governs whether 'source' cell details or the potentially more comprehensive 'override' cell details will be included in the query.

You can also choose to use any of the other filters in the sidebar (date/time, timeslice, location or event types) to edit the dataset before querying it; this opens the possibility of running 'location specific' queries, for example, by using 'Location' filters.

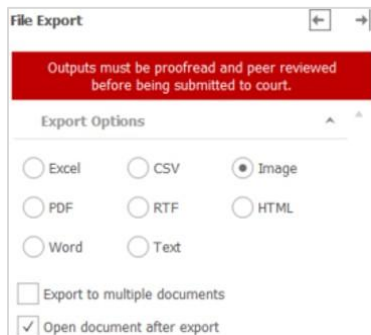
Settings Tab

The 'Matching' settings - duplicate matching, SMS concatenation and singlerow matching - will be applied to all queries.

The 'Redaction' settings will be applied to the displayed and exported data if you require some or all personally identifiable details to be redacted.

Export Tab

Provides options to output the query results in a variety of formats.



This output method can be termed 'what you see is what you get' and provides no additional formatting, it simply exports the selected data in the selected format. It's also possible to export query results to Excel or print them using the controls in the top bar of each query window.

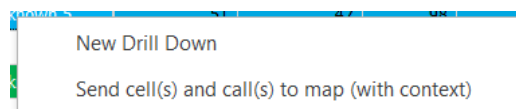
Note: It is recommended you first use the 'Filters' tab to select what data to load and display.

17.2.4 Using Drilldowns

Most Analytics queries offer the opportunity to 'drill down' into the data behind the query results. If a drilldown option is available, you can open it from a right-click menu in the main grid or chart of each query; it may be necessary to minimise other panels in the query screen to bring the drill-down panel into view.

17.2.5 Report Grid Right-click Menus

Most query results and drilldown grids support a right-click menu function with two options

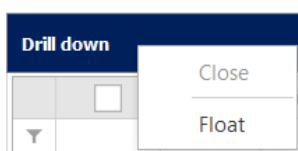
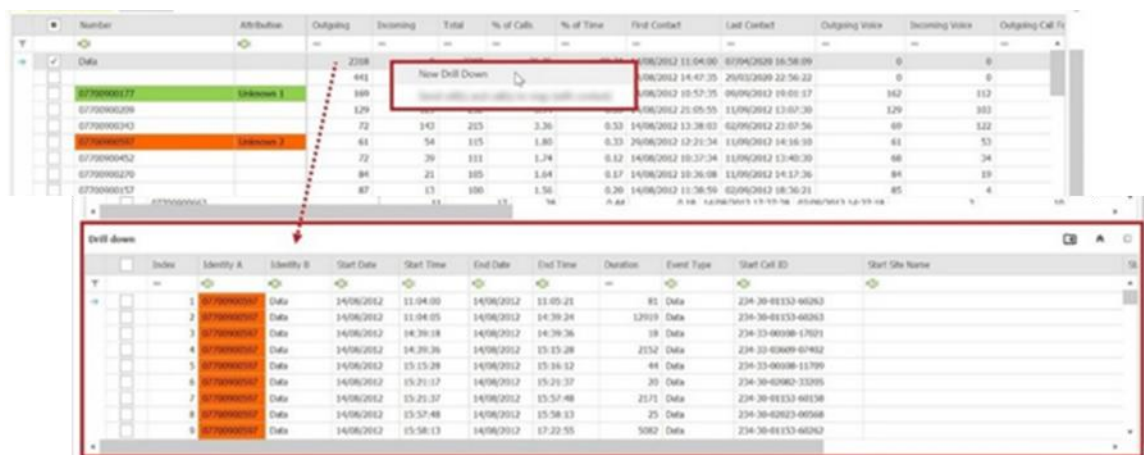


You can select a single row or multiple rows to send to drilldown or to a map. When selecting multiple rows you can either click & drag to highlight a contiguous set of required rows or you can use the checkbox column to select non-contiguous rows to send.

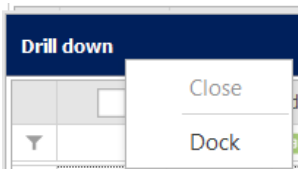
New Drilldown

Most query results grids support a drilldown function, where any/all rows in the report can be sent to a drilldown grid which provides access to the raw data events that are summarised in the analysis.

You can open the drill down grid by selecting a single cell in a column, or clicking and dragging to cover multiple cells, then right-clicking and selecting 'New Drill Down':



Once the drilldown pane has opened, you can right click in the header and select to 'Float' which opens the 'Drill down' as a new window so all information can be reviewed.



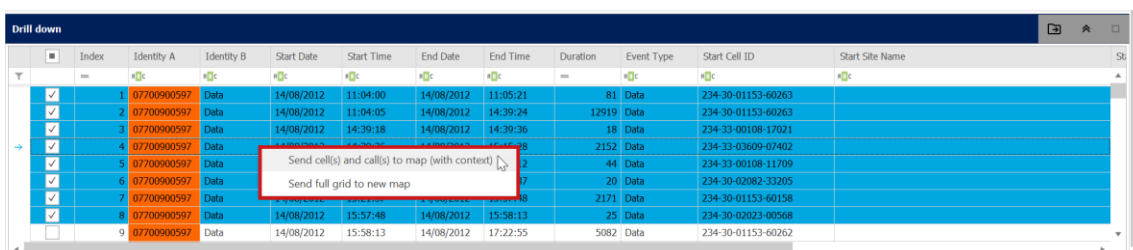
In the same way, you can select to locate the floated window back into the main window by selecting 'Dock'.

The 'float & dock' option also works for any other pane in any CSAS window that has a dark blue border along the top of the pane.

The Drill down grid supports the usual CSAS in-column filtering options.

Send to Map

In most query results and drilldown grids, you can right-click in any row (multiselect a set of rows) and send the data to a new Map Tab:



Once loaded, the new Map Tab opens, you can then review and process the data as described in:

» Using the New Map Button

» Using Mapping

Alternatively, you can send the whole data grid to a new Map Tab, which opens in the same way with the same functions.

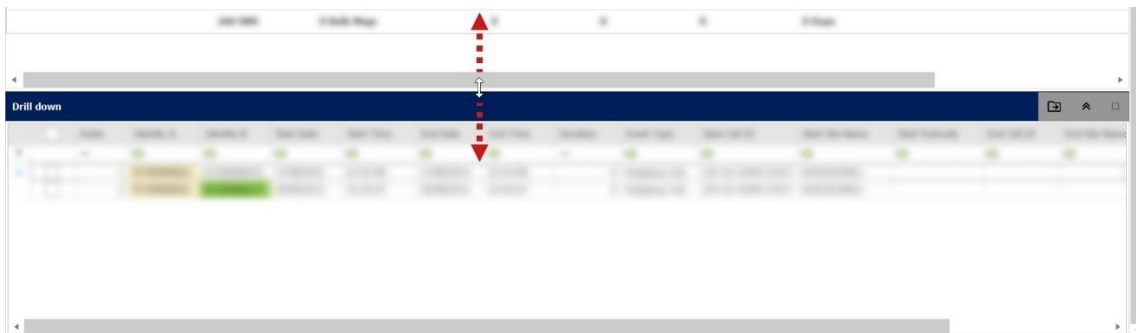
17.2.6 Selecting and resizing panes

Each pane can be Collapsed and Maximised using the buttons and controls at the top right side of the window; you can also get more information about the window by clicking the '?' hints & tips icon:



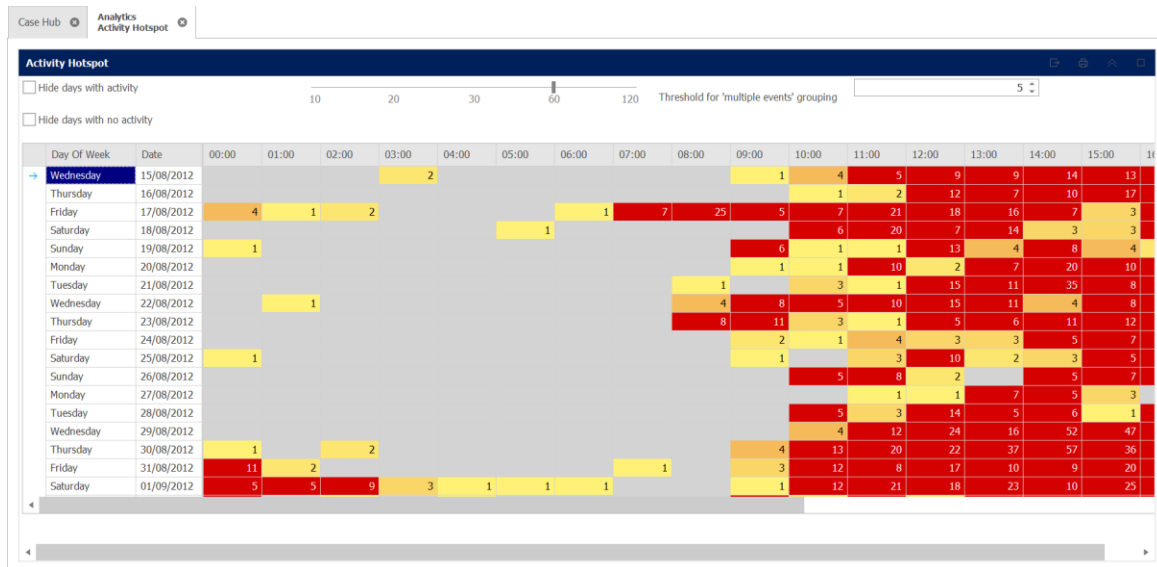
You can show/hide individual panes using the  button in the pane header. It is often useful to close the main pane after launching a drilldown grid, to ensure that drilldown pane has the maximum amount of space to be viewed.

Panes can be resized as required by using the mouse and grabbing / dragging the edge of the pane up / down:



17.3 Using the Activity Hotspot query

The Activity Hotspot query displays activity levels over time for the selected data using a colour code to represent the different levels of activity. You can use this function to determine trends in activity for a subject and also to the levels of activity around the times of significant events.



17.3.1 Supported Data Types

The Activity Hotspot query can be used with any imported data or file type that includes time-ordered event data, including CDR, ANPR, handset download, telematics, tracker and others.

17.3.2 Layout

The results grid displays days/dates in rows (with a row header showing date and day name) and time periods across each day (defaulting to 24 one-hour periods) in columns (with column headers showing the start time of each period). Each intersection of a row and column represents an 'analysis period', a selectable period of time (one hour, for example) in a day.

The count in each grid cell indicates the number of events that were active during each analysis period. An analysis period will have its event count incremented for each connection that is active during that period – this means that, of course, each new call, text or data session that is set up during a period increments the count, but long duration events that span across multiple periods will also increment the count.

For example, with the analysis period duration set to 60 minutes, imagine the subject phone makes a call that starts at 15:50, the event count for the hour 15:00-15:59 on that day will be incremented. If the call lasts for 30 minutes, the event count for the hour 16:00-16:59 will also be incremented, as the call was also active during that hour. The same applies to long running GPRS/mobile data events.

The query follows this methodology as a way of detecting ongoing activity and to avoid incorrectly assuming that the subject phone was 'inactive' when it was actually in use, just with a long-lasting connection.

If you wish to concentrate on voice & SMS activity and avoid issues caused by long-lasting GPRS sessions, you can elect to remove GPRS events from the analysis using the right sidebar 'Event Type' filter. If you do remove GPRS events from the dataset, please remember to disable the event type filter again before moving on to undertake more general analysis.

Key:

 Highest value	 2nd highest	 3rd highest	 4th highest	 5th highest
--	---	--	---	--

The results grid is colour-coded to ensure that periods with the highest event counts get highlighted and are more easily visible. This employs a five-tier colour code system, with red (hottest) indicating the periods with the highest event count, graduating down through a cooler set of oranges and yellows to indicate periods with lower event counts. Inactive periods, with no active connections, are coloured grey. The colours used for the colour codes are not user selectable.

17.3.3 Filters & Controls

The data to be analysed is selected from the right sidebar 'Source Data' menu in the normal way and is sent into the query when the 'Apply' button is clicked. Any filters or options applied within the query take effect immediately, there is no separate 'run' button and the 'Apply' button only needs to be clicked if you change the set of selected files or sidebar filters.

The length of the 'analysis period' used by the query can be varied using the slider at the top of the pane – this offers five options for period length of 10, 20, 30, 60 (default) and 120-minute intervals as required.

The colour-coding feature colours grid cells for analysis periods with the highest events count in red. The scale for specifying what constitutes the 'highest' event count values can be customised using the 'threshold for multiple events grouping' option. The default threshold for the highest (red coloured) grouping is 5 events, but this can be set to higher values in steps of 5. Setting to a higher value, say '20', means that only cells with 20 or more events in will be coloured red and the other groupings are evenly distributed up to that value. So, with a red group threshold of 20, the other group thresholds are yellow 1-4, light orange 5-9, mid orange 10-15, dark orange 15-19, red 20+.

It can be useful to adjust the threshold for 'multiple events' in cases with large amounts of data, where each subject phone in an analysis is very busy at key times. If, for example, you were interested in quickly identifying times when the selected subject phone(s) engaged in more than 30 events in one hour, you could set the time slider to '60 minutes' and the 'multiple events' threshold to '30'. Analysis periods that had 30 or more events would be coloured red and would stand out clearly in the results grid.

There are also two checkboxes for controlling visibility of 'day' rows: 'hide days with activity' hides days that have at least one active event registered to them, leaving only inactive days. This offers an alternative method for creating an inactivity report. 'Hide days with no activity' does the opposite and hides days that have zero active events. This is useful for condensing results grids that cover long periods of time, allowing the

analysis to skip days with no activity. Obviously, if both tickboxes are checked, the results grid will display no data, which isn't recommended.

The results grid supports the standard Analytics right click menu options of 'drilldown' and 'send to map', as outlined in the [Grids and Controls](#) section.

17.3.4 Understanding the results

The Activity Hotspot query offers a visual method for differentiating between less busy and more busy periods. The colour codes allow the extremes (inactive is grey, highest event count is red) and then the event counts in the individual analysis periods allow the relative levels of busyness to be determined.

DayOfWeek	Date	2:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00
Saturday	12/08/2017																	
Sunday	13/08/2017					1	1	9	4	1			7	2	3		6	9
Monday	14/08/2017							1		1		3	8	4		19	3	1
Tuesday	15/08/2017							1	2					4	2	5	4	
Wednesday	16/08/2017								5	3	4	2	5	1	1	3	1	5
Thursday	17/08/2017								1	2		1	3	6	3	4	5	2
Friday	18/08/2017						1		3				2	3		2	14	5
Saturday	19/08/2017						3	6	3	6	8	3		9		3	6	8
Sunday	20/08/2017									1	1	2	16		1			
Monday	21/08/2017	1						4		3		2	6	1	2	2	5	12

In the above example, which happens to be analysing CDR data, the subject phone wasn't used at during 12th August (the first date in the dataset). Other days have a general level of activity, with occasional periods with higher levels of activity.

For example, the one-hour period starting 07:00 on 18/08 had one active event, whereas the one-hour period starting 13:00 on 20/08 had an event count of 16.

The analysis period in the example was set to 60 minutes and the threshold for 'multiple events' was set to 10.

Why, When, Who



This function is necessary to analyse event activity trends and to determine the levels of activity at significant times.



This function is undertaken as required.



This function is typically carried out by the following users:

» CSAS User.

Stepped Procedure

To launch the Activity Hotspot query:

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters. Due to the fact that long-lasting GPRS session records may confuse the view of actual user-initiated activity levels, you may wish to exclude GPRS/mobile Internet events using the Filters > Event Types option.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query.
4. The results chart will update to show the data for the selected source data.
5. If necessary, you can change the analysis period value to something other than 60 minutes. There is no need to click 'Apply' again after making changes to the query controls or filters, the results will update automatically.
6. You can change the threshold value for applying the highest/hottest red colour to analysis periods with the highest event counts.
7. You can hide days with activity and those with no activity by checking the checkboxes.
8. Review the results grid to gain an understanding of the activity levels across the analysed time span for the selected subject identifiers.
9. Sending the top few Summary List rows to a map may help to identify the general area in which the subject was staying during the analysed period.
10. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
11. If you wish to view any of the results in a map, select the required row(s), right-click and select Send to Map.
12. If you filtered GPRS/data events from the dataset when launching this query, remember to restore them to the dataset, by cancelling the Event Type filter, before continuing with your analysis.

17.4 Using the Average Event Distribution query

This query displays average event distribution data on a colour coded graph. Analytics Average Event Distribution provides an indication of when the selected identifier is busy or idle, by showing the average activity levels over a period of time thereby establishing trends in activity.

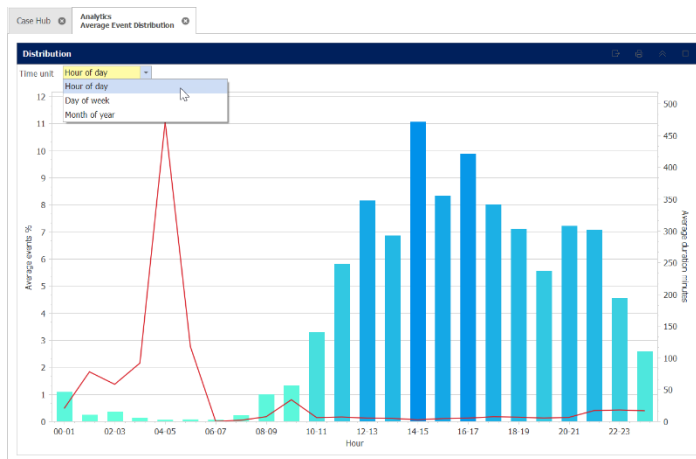
This query is general and can be used to show activity levels for all types of identifiers, not just phones.

17.4.1 Supported Data Types

The Average Event Distribution query can be used with any imported data or file type that includes time-ordered event data, including CDR, ANPR, handset download, telematics, tracker and others.

17.4.2 Layout

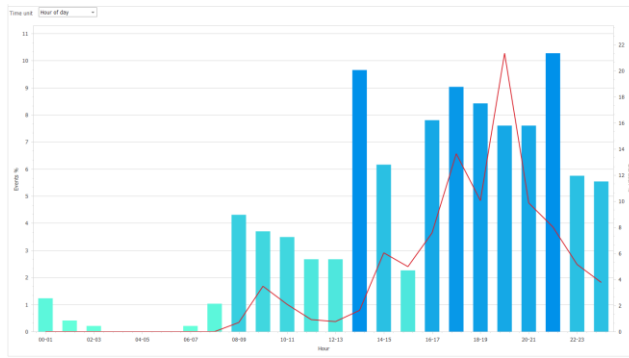
The query displays target identifier activity in terms of average number of events (the bars) and average event duration (the line):



17.4.3 Filters & Controls

The data to be analysed is selected from the right sidebar 'Source Data' menu in the normal way and is sent into the query when the 'Apply' button is clicked. Any filters or options applied within the query take effect immediately, there is no separate 'run' button and the 'Apply' button only needs to be clicked if you change the set of selected files or sidebar filters.

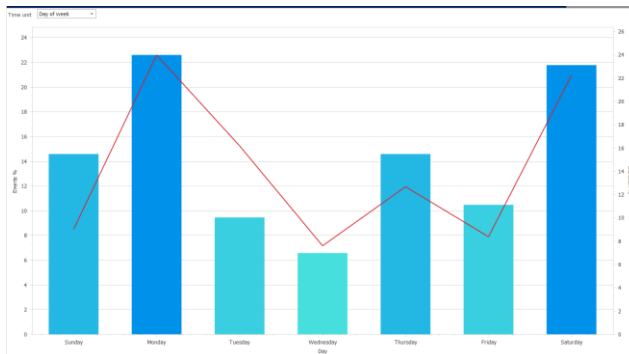
The graph can be set to show average event levels over a 24-hour period (highlighting when the selected identifier of dataset is on average busiest), or over the days of the week or the months of the year.



In 'hour of day' mode, the scale along the bottom of the chart shows the 24-hour day.

The scale on the left side shows percentage of overall events.

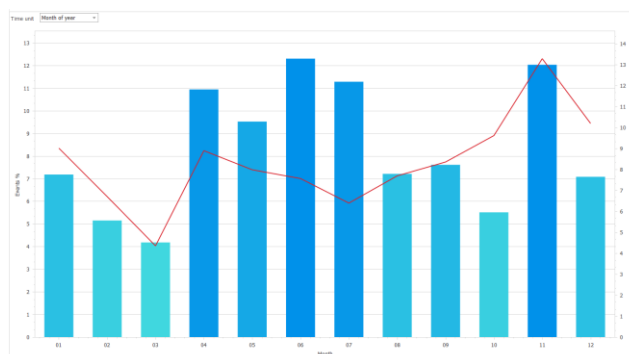
The scale on the right side shows percentage of event duration.



In 'day of week' mode, the scale along the bottom of the chart shows the 7-day week.

The scale on the left side shows percentage of overall events.

The scale on the right side shows percentage of event duration.

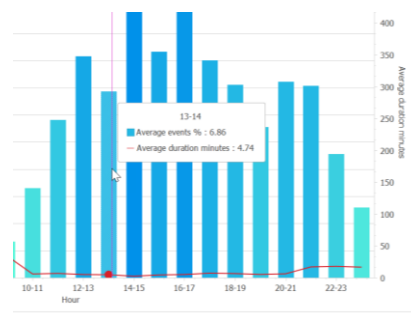


In 'month of year' mode, the scale along the bottom of the chart shows the 12-month year.

The scale on the left side shows percentage of overall events.

The scale on the right side shows percentage of event duration.

Moving the cursor over the graph shows data for each bar:



Data is colour-coded depending upon frequency, with higher event counts being coloured a darker shade of blue. You can select the data to be displayed in the grid via the sidebar prefilters.

Double-clicking on a bar in the chart launches the drill down view for that data.

17.4.4 Understanding the results

The Average Event Distribution query provides information about the average number of events that were active in each period (hour, day, month) in the selected dataset.

This can provide an indication of, for example, a suspect's lifestyle, showing whether they have a conventional lifestyle (sleep at night, awake during the day), an inverted lifestyle (awake at night, asleep during the day) or a chaotic lifestyle with no fixed patterns of activity or inactivity.

Why, When, Who

	This function is necessary to summarise the average levels of activity of a particular identifier.
	This function is undertaken as required.
	This function is typically carried out by the following users: ➤ CSAS User

Stepped Procedure

To launch the Average Event Distribution query:

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query.
4. The results chart will update to show the data for the selected source data.
5. You can switch the query mode by changing the 'Time Unit' setting, so show average distribution per hour, day or month.
6. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required bar in the bar chart and double click.

17.5 Using the Cell Usage query

Cellular records, usually obtained in the form of CDR (Call Details Records) files, provide details of the cells used to carry each call, text or data session.

Typically, SMS text message events are carried by just one cell, as there is no mechanism that allows a handover to take place during a text transmission. Voice call records usually contain details of two cells – the 'start' cell used at the beginning of a call and the 'end' cell that was in use when the connection was closed. GPRS/mobile data sessions typically include details of just one cell, either the start cell or end cell depending upon the network, but it is possible that some networks might supply details of both start and end cells for mobile data records. Voice calls that were handled using VoWiFi (Voice over WiFi) techniques might capture details of the WiFi access point used for each call, but this is uncommon. Some records, for a variety of reasons, don't capture any details of the cells that were used.

When analysing cellular data, it can be useful to determine the overall cell or set of cells that a subject phone uses most often, this can help to indicate the general geographic areas the user of the phone frequents most often. Alternatively, it might be useful to under the 'top cells' a phone used during a particular period of time.

The Cell Usage query attempts to aid this form of analysis by providing a list of the unique set of cells found in the selected source data files, showing a usage count for each cell and listing them in order of those that are used most often. This can be used to answer the question 'which cells or cell sites does this phone use most often?'

17.5.1 Supported Data Types

The Activity Hotspot query can be used with CDR and cellular data only.

17.5.2 Layout

Data is presented in three panes:

- » Summary List pane
- » Top 10 Cells pane
- » Hotspot Chart pane.

Summary List

Display by Cell ID

Cell Id	Site Name	Postcode	Network	Technology	Azimuth	Event Count	Percentage (Call Count)	Percentage (Usage Count)	Phone Count
+ 234-30-01153-60263	YATES HOUSE	E2 6NU	EE	2G	240	158	19.41	14.98	1
+ 234-30-01153-14431	YATES HOUSE	E2 6NU	EE	2G	240	131	16.09	12.42	1
+ 234-30-01153-60262	YATES HOUSE	E2 6NU	EE	2G	120	99	12.16	9.38	1
+ 234-30-01153-14450	YATES HOUSE	E2 6NU	EE	2G	120	61	7.49	5.78	1
+ 234-30-02023-00569	YATES HOUSE	E2 6NU	EE	2G	240	21	2.58	1.99	1
+ 234-30-01153-60235	BACTON TOWER	E2 0LT	EE	2G	120	19	2.33	1.80	1
+ 234-30-01078-00786	LONDON POST	W1D 4FR	EE	2G	240	17	2.09	1.61	1

The 'Summary List' displays key information for each unique cell or cell site such as Cell ID, cell Site Name, cell Postcode and the Network the cell belongs to.

The main metrics computed by the query are the 'event count' per cell and two different

values for the percentage of overall cellular activity that each count represents.

The grid can be sorted/resorted by any of these values by clicking on a column header.

Event Count

The compilation of the 'Event Count' value requires some explanation – this value is not calculated as a simple count of the number of occasions on which the cell ID appears in the source data as that could be misleading. Instead, it's a count of the number of calls/connections in which the cell features – so if Call A uses Cell 123 as both the start and end cell in a call record (which means that Cell ID 123 appears twice in the record), the query will only count that as 1 call and Cell 123 will only have its count incremented by 1; whereas if a record shows that Call B used Cell 123 as the start cell and Cell 234 as the end cell, then both cells get a count of 1 added to their totals.

The proportion of overall usage associates with each cell can also be calculated in two different ways (or, more accurately, we have been asked to calculate it in two different ways by CSAS users), hence the need for two 'percentage' columns.

Percentage (Call Count)

In this calculation, the event count for each cell is divided by the total number of events (the total number of individual call/text/data records) in the analysed dataset:

$$\text{cell event count} / \text{event total} * 100.$$

This provides a value that shows the proportion of total cell usage that handled by each cell.

Percentage (Usage Count)

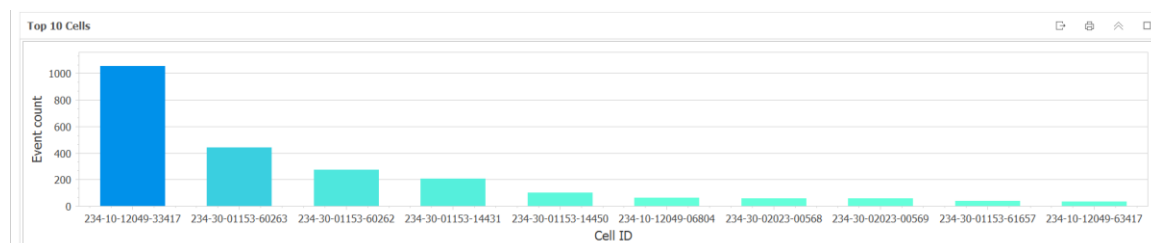
In this calculation, the event or usage count for each cell is divided by the sum of all the event usage counts for all cells in the analysis:

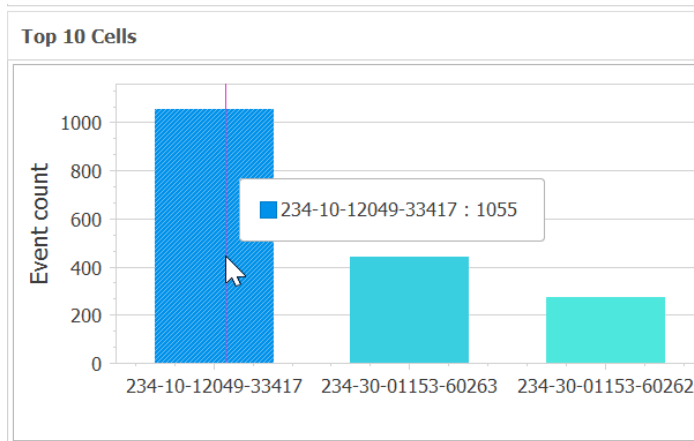
$$\text{cell event count} / \text{sum of all cell event counts} * 100.$$

This provides a value that shows the proportion of total calls/connections that handled by each cell.

Top 10 Cells

Data for the top 10 rows in the 'Summary List' are displayed in a graphical form, to make the proportions of usage between those top 10 cells/sites more immediately obvious:





Hovering over any bar will display the data represented by that bar over the top of the graph:

Hotspot Chart



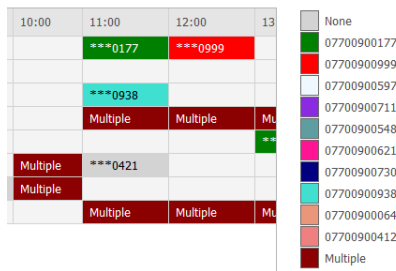
The Summary List shows how often each cell/site/sector was used, which is useful for understanding where a phone might have been most commonly located, but the Hotspot Chart can show 'when' each cell was used. It can also show details of the other numbers that were involved in those calls. Both of these pieces of information could be useful, as they could show that there is a specific pattern to the usage of a particular cell site, which may be relevant to an investigation. For example, the Hotspot Chart could show that a subject phone only uses a particular cell on Saturday afternoons, or it could show that the cell was only used to contact a specific other number.

You can elect to show details for individual or multiple cells on the 'Hotspot Chart' by navigating to the 'Summary List' and selecting an individual row, clicking and dragging to select a contiguous set of rows, or using 'control & click' to select a set of non-contiguous rows, then right-clicking and selecting 'Show in Hotspot Usage Chart'.

The Hotspot Chart displays a date/time grid, with each row representing a day and each column representing a selectable time period across each day. The intersection of a row and a column provides information for one time period of one day.

The Hotspot Chart has two modes:

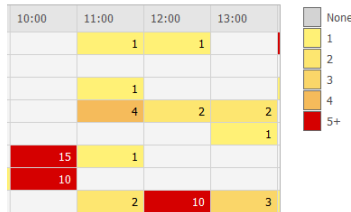
- » Individual Cells – where the populated intersections in the hotspot grid represent a time period in which connections were made that used the selected cell(s).



The detail in each intersection box shows the 'other' numbers that were contacted. If more than one other number was in contact during a time period, the intersection will show 'multiple'.

A legend beside the grid shows the colour coding applied to the other numbers.

» Group Cells – where the populated intersections show the time distribution of the events that used the selected cell(s) during that time period.



The detail in each intersection box shows the event count for that time period.

A legend beside the grid shows the colour coding applied to the event counts, with the highest counts being coloured red.

17.5.3 Filters & Controls

The data to be analysed is selected from the right sidebar 'Source Data' menu in the normal way and is sent into the query when the 'Apply' button is clicked. Any filters or options applied within the query take effect immediately, there is no separate 'run' button and the 'Apply' button only needs to be clicked if you change the set of selected files or sidebar filters.

The Summary List and Hotspot Chart panes have a small set of controls:

Summary List

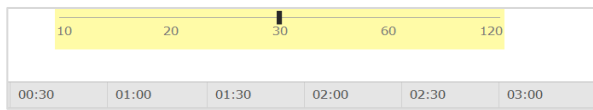
The 'Display By' drop-down optionally allows the data in the grid to be aggregated.

- » If set to 'Cell ID' the list shows one row and count for each individual cell ID found in the selected data.
- » If set to 'site name' there is one row for each site name and counts for all cells on that site are aggregated into that row.
- » If set to 'site name and azimuth/sector' there is one row for each different azimuth found on each site (so, for example, all of the cells with a 120 azimuth on the same site are aggregated together) and the counts for those cells are aggregated into that row.

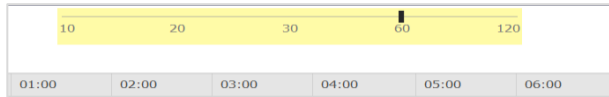
The 'Cell ID' drop-down allows the format of the cell IDs to be changed from the standardised CGI format, to whatever the format the raw data was presented in.

Hotspot Chart

The Hotspot Chart time period can be adjusted (with values of 10, 20, 30, 60 and 120 minutes) by sliding the bar at the top of the pane.



For example, when you slide the bar to 30 [minutes] the time values change to half-hour intervals:



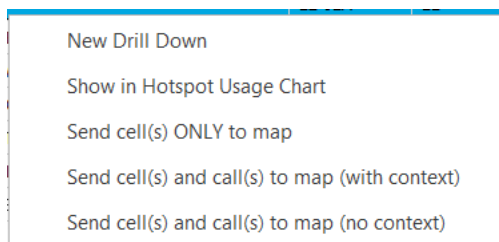
If you slide the bar to 60, the values will change to hourly intervals:

- ☐ Hide days with activity
- ☒ Hide days with no activity

You can select to hide days with or with no activity to compress the data as required.

Right-click menus

The Summary List supports an extended right-click menu, offering more than the usual Analytics right-click options:

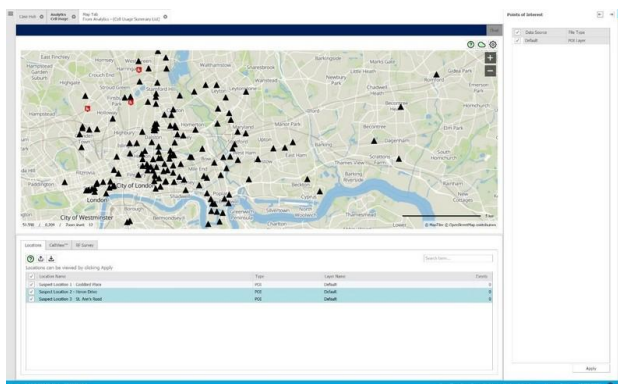


The New Drilldown option works in the usual way, as described in the *Grids and Controls* section.

The 'Show in Hotspot Usage Chart' option sends data for the selected row(s) to the Hotspot Chart.

There are three 'send to map' options.

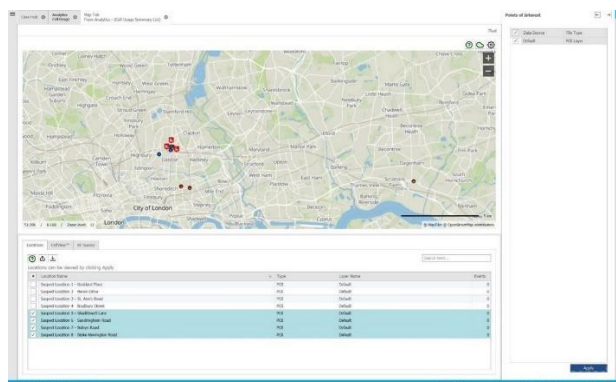
» If you select to 'Send cell(s) ONLY to map', a simplified Map Tab opens:



As this only sends the cell locations and no event details to the map, the simplified tab displays cell sites as black triangles and map labels will not show any event details.

-

» If you select to 'Send cell(s) and call(s) to map (no context)', the following new Map Tab opens:



17.5.4 Understanding the results

The data provided in the query results grid lists cells or cell sites in order of how heavily they were used and also allows the data to be aggregated to show 'top cells', 'top cell sites' and 'top sectors of cell sites'.

Display by

Cell ID

Cell ID

 CGI

Summary List										
Cell Id	Site Name	Postcode	Network	Technology	Azimuth	Event Count	Percentage (Call Count)	Percentage (Usage Count)	Phone Count	
					=	=	=	=	=	
234-30-01153-60263	YATES HOUSE	E2 6NU	EE	2G	240	158	19.41	14.98	1	
234-30-01153-14431	YATES HOUSE	E2 6NU	EE	2G	240	131	16.09	12.42	1	
234-30-01153-60262	YATES HOUSE	E2 6NU	EE	2G	120	99	12.16	9.38	1	
234-30-01153-14450	YATES HOUSE	E2 6NU	EE	2G	120	61	7.49	5.78	1	
234-30-02023-00569	YATES HOUSE	E2 6NU	EE	2G	240	21	2.58	1.99	1	
234-30-01153-60235	BACTON TOWER	E2 0LT	EE	2G	120	19	2.33	1.80	1	
234-30-01078-00786	LONDON POST	W1D 4PR	EE	2G	240	17	2.09	1.61	1	
234-30-01153-61657	LUPIN HOUSE	E2 0EA	EE	2G	240	17	2.09	1.61	1	

In the above example, cell ID 234-30-01153-60263 (connected to the Yates House site in the E2 area of London) was the most frequently used cell, with 158 events connecting via that cell, which represents 19.41% of total call/connections and 14.98% of total cell usage.

The next four top cells were also from the Yates House site, so switching the 'Display By' option to 'Site':

Display by

Site

 Cell ID

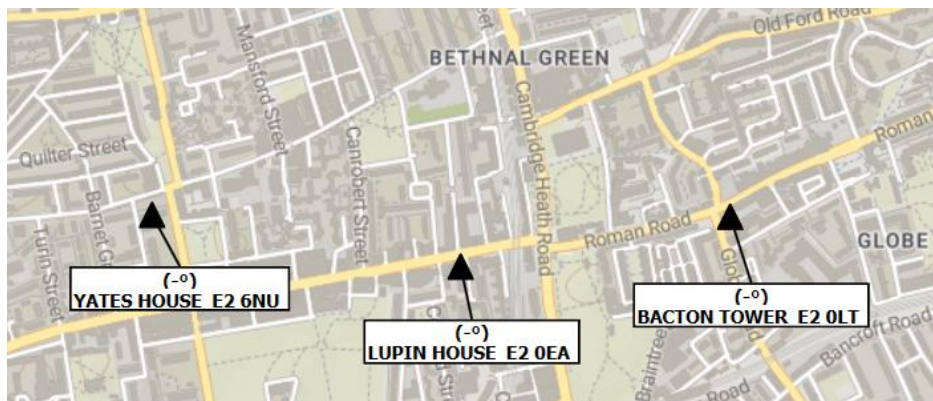
CGI

Summary List

	Site Name	Postcode	Network	Sector Count	Cell Count	Event Count	Percentage (Call Count)	Percentage (Usage Count)	Phone Count
▼				=	=	=	=	=	=
→	+ YATES HOUSE	E2 6NU	EE	3	9	496	60.91	47.00	1
	+		EE	3	65	97	11.83	8.96	1
	+ LUPIN HOUSE	E2 0EA	EE	3	6	57	7.00	5.39	1
	+ BACTON TOWER	E2 0LT	EE	3	8	42	5.15	3.96	1
	+ LONDON POST	W1D 4PR	EE	3	4	31	3.81	2.93	1

Reveals that over 60% of all connections were handled by Yates House and two more of the top 5 sites were also in the E2 area.

The conclusion to draw from the is that the user of the subject phone lived or spent a lot of time in the E2 area. Sending the data to a map confirms this assumption:



Sending data for one selected cell to the Hotspot Chart reveals that the subject phone's user only appears to use that particular cell in the early afternoon and not at other times. This may or may not be significant.

DayOfWeek	Date	10:00	11:00	12:00	13:00	14:00	15:00
Monday	30/08/2021					7	
Saturday	04/09/2021			8	9	4	

Why, When, Who

	This function is necessary to display, at a glance, which cell has the highest use during an analysed period.
	This function is undertaken as required.
	This function is typically carried out by the following users:  CSAS User.

Stepped Procedure

To launch the Cell Usage query:

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query.
4. The results default to being displayed with one row per unique cell ID, but you can elect to aggregate the results by site or sector by changing the Display By option.
5. Review the results grid to gain an understanding of the cells or sites the subject phone(s) visited most frequently and the cells used most often.
6. The Top 10 Sites bar chart will display data for the top 10 rows of the grid, whatever format the grid is set to.
7. If you wish to view data for a specific cell or set of cells looking for time-based usage patterns, you can select the required row(s), right-click and 'send to hotspot chart'.
8. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
9. If you wish to view any of the results in a map, select the required row(s), right-click and select the required Send to Map option.

17.6 Using the Concurrent Calls query

The Concurrent Calls Query is designed to list instances where the selected subject phones were both in use simultaneously with concurrent or overlapping calls.

This query is useful in scenarios where, for example, investigators are alleging that both phones were being used by the same individual; assuming that one individual can generally only use one phone at a time, a large number of concurrent calls could cast doubt upon the allegation being made.

The contents of the Concurrent Calls are available for export to Excel via the Print/Export menu and drilldown is available. When any cell in a row is double-clicked the drilldown screen provides details of the set of concurrent calls made at that time.

It is also possible to select/multiselect rows in the grid, right-click and send the data to a map.

Concurrent Calls

Group A CDR Identifiers

07700903852

Group B CDR Identifiers

447700902421

Min. overlap (seconds)

5

Max. overlap (seconds)

20

☒ Match events once

☒ Voice only

☒ Restrict Overlap

Run

Column chooser

Group A CDR Events							Group B CDR Events				
Overlap (seconds)	Start date	Identifier	Attribution	Start time	End time	Event type	Identifier	Attribution	Start time	End time	Event type
=	=			=					=	=	
17	14/03/2024	07700903852	Unknown 9	17:36:35	17:38:07	Outgoing Voice	447700902421	Unknown 10	17:37:50	17:41:05	Outgoing Voice
7	15/03/2024	07700903852	Unknown 9	21:48:14	21:48:32	Incoming Voice	447700902421	Unknown 10	21:48:25	21:54:14	Incoming Voice

The query allows users to select a set of source data files from the right sidebar; those files can then be assigned into two groups – Group A and Group B – the query will then compare the Group A records against the Group B records and highlight pairs of records that overlap.

Each group could contain just one phone (so the query would be comparing the records for just two phones), or they could each contain data for multiple phones – for example, if the intention of running the query was to look for overlapping events for two suspect individuals who both used multiple phones, Group A could be set up to contain all phones linked to Suspect A and Group B the same but for Suspect B. The query would then highlight any overlapping calls for Suspect A and B across all of their devices.

17.6.1 Supported Data Types

The Concurrent Calls query can be used with CDR files only.

17.6.2 Layout

The Concurrent Calls query is divided into two panes, with an additional drilldown pane that can be triggered if required.

Concurrent Calls

Group A CDR Identifiers

07700903852

Group B CDR Identifiers

447700902421

Min. overlap (seconds)

5

Max. overlap (seconds)

20

☒ Match events once

☒ Voice only

☒ Restrict Overlap

Run

Column chooser

Filters & Controls

Group A CDR Events							Group B CDR Events				
Overlap (seconds)	Start date	Identifier	Attribution	Start time	End time	Event type	Identifier	Attribution	Start time	End time	Event type
=	=			=	=				=	=	
17	14/03/2024	07700903852	Unknown 9	17:36:35	17:38:07	Outgoing Voice	447700902421	Unknown 10	17:37:50	17:41:05	Outgoing Voice
7	15/03/2024	07700903852	Unknown 9	21:48:14	21:48:32	Incoming Voice	447700902421	Unknown 10	21:48:25	21:54:14	Incoming Voice

Results Grid

Filters & Controls

Results Grid

Filters & Controls

These are used to select the phones to compare against each other, set the parameters and values used by the query that are outlined below. It also hosts the 'Run' button used

to trigger or cancel the running of the query and the 'column chooser' button.

Results Grid

The results grid lists the results of the query – it lists details of the overlapping events for 'Group A' and 'Group B' phones that match the filter criteria.

The columns in the default layout are:

- » Overlap (seconds) – which shows the amount of time the two events overlap for
- » Group A CDR events
 - Start date
 - Identifier (phone number)
 - Attribution
 - Start time
 - End time
 - Event type
- » Group B CDR events – columns match those for group A

Via the column chooser (which can be accessed by right clicking in the results grid column header row) a number of other column options are available, including details of the cells used by the phones in each group.

17.6.3 Filters & Controls

The filters and controls section consists of the following elements:

- » Group A CDR Identifiers – a dropdown menu that lists the subject identifiers from all selected source files and allows the user to indicate which of them should be included in Group A
- » Group B CDR Identifiers – the same but for Group B
- » Min overlap (seconds) – sets the minimum amount of time a pair of events would need to have overlapped for to be included in the results. This value defaults to 5 seconds but can be wound down to 0 seconds or increased to a higher value
- » Max overlap (seconds) – sets the maximum amount of time a pair of events could overlap for to appear in the results. This value defaults to 20 seconds but can be adjusted up or down as required.
- » Match events once – if enabled (the default) it only includes an individual event in once in the results. For example, if Phone A has a call at 12:00:10 that lasts for 2 minutes and Phone B has two calls at 12:00:10 and 12:01:15, the Phone A event will only be shown once in the grid (associated with the Phone B event at 12:00:30), it will not also be listed for the event at 12:01:15. If the option is disabled, all correlating pairs of events are shown.
- » Restrict Overlap – if enabled the query takes the min and max overlap settings into account; if disabled (the default), these settings are ignored.
- » Voice only – if enabled (the default), the analysis is restricted to voice calls; if disabled, all events in the selected CDRs (including SMS and data sessions) will be included.

The Run button initiates the query and the Column Chooser button offers an alternative method for opening the additional columns list.

17.6.4 Understanding the results

The Concurrent Calls query offers a quick and simple method for determining whether two phones (or members of two groups of phones) were regularly in use at the same time – one of the main uses of the query to help to check for 'clean phone/dirty phone' usage.

The proposition is that an individual who is engaged in criminal activity and who is aware that their phone records might be examined by the police, will use one phone (the 'clean' phone) for all of their legitimate activities and a different phone (the 'dirty' phone), which will usually be an unregistered 'burner' phone, for all of their criminal activities.

The purpose of the analysis would be to see if the events captured for each phone could be correlated – one option is to use the Potential Colocation query to see whether the two phones could be seen to be geolocated or moving together on a regular basis. Another technique would be to see whether there are regular overlapping calls for the two phones – based on the assumption that if they're both held by the same person, they will only be engaged in one call at a time. A high level of overlapping calls might argue against the idea that both phones were being used by the same individual.

The min/max overlap filters can be used to focus the query for different scenarios – for example, setting a higher 'min overlap' value means that only pairs of calls where there is a substantial overlap would be included in the results, which would filter out situations where the suspect was on a call on their clean phone, answered a concurrent call on their dirty phone, found out who it was, then ended the first call on the clean phone. Such a short overlap would mean that the two calls were excluded from the results.

Group A CDR Events							Group B CDR Events				
Overlap (secon...	Start date	Identifier	Attribution	Start time	End time	Event type	Identifier	Attribution	Start time	End time	Event type
=	=			=	=				=	=	
17	14/03/2024	07700903852	Unknown 9	17:36:35	17:38:07	Outgoing Voice	447700902421	Unknown 10	17:37:50	17:41:05	Outgoing Voice
7	15/03/2024	07700903852	Unknown 9	21:48:14	21:48:32	Incoming Voice	447700902421	Unknown 10	21:48:25	21:54:14	Incoming Voice

In the example results grid above, the first result shows an overlapping pair of call records. The calls overlap by 17 seconds (the Phone B call started at 17:37:50 and the Phone A call didn't end until 17:38:07).

Why, When, Who

This function identifies the number of concurrent calls between selected phones and may help to indicate whether it is likely that those phones were used by the same or different people



This function is undertaken as required.



This function is typically carried out by the following users:

» CSAS User.

Stepped Procedure

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected datasets into the query.
4. In the filters & control section, use the Group A CDR Identifiers to select the phone (or phones) that comprise Group A, then do the same for Group B.
5. If the 'Restrict Overlap' setting is enabled, select the required 'min overlap' and 'max overlap' values to filter the results.
6. Check that the other settings (match events once, restrict overlap and voice only) are set as required and when ready, click 'Run'
7. The results grid will list the pairs of events that meet the criteria.
8. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
9. If you wish to view any of the results in a map, select the required row(s), right-click and select Send to Map.
10. If you wish to output the results grid, click on the export button in the query header.
11. View the details provided in the results grid,

17.7 Using the Contact Summary query

This query displays contact summary data for the selected target phone(s) in a tabulated form that counts the total number of Outgoing and Incoming connection events (calls, texts, data session, etc) for the selected date and time span:

Summary List

Event Totals

Total Events	1,158	Outgoing Text	156
Incoming Text	140	Data	343
Incoming Voice	187	Outgoing Forward	1
Outgoing Voice	331		

☐ Display top rows only 50

	Number	Attribution	Outgoing	Incoming	Total	% of Calls	% of Time	First Contact	Last Contact	Outgoing Voice	Incoming Voice	Outgoing Call Forward
	Data		343	0	343	29.62	92.00	29/08/2021 12:32:53	05/09/2021 17:01:45	0	0	
	07700900597	Unknown 3	51	47	98	8.46	0.75	29/08/2021 12:21:34	05/09/2021 16:45:36	51	47	
	07700900938		41	30	71	6.13	0.99	29/08/2021 15:38:43	04/09/2021 17:57:23	21	18	
	07700900621	Unknown 1	34	26	60	5.18	0.52	29/08/2021 11:26:22	05/09/2021 12:18:34	33	25	
	07700900938		22	17	39	3.37	0.41	03/09/2021 20:00:38	04/09/2021 00:32:12	1	0	
	07700900599		25	9	34	2.94	0.17	29/08/2021 13:09:39	04/09/2021 18:10:19	22	8	
	07700900441		28	0	28	2.42	0.06	03/09/2021 18:00:29	05/09/2021 16:39:21	21	0	
	07700900381		16	11	27	2.33	0.13	31/08/2021 14:50:53	05/09/2021 14:38:58	11	6	
	07700900999		14	9	23	1.99	0.32	29/08/2021 10:54:37	05/09/2021 11:47:15	8	3	
	07700900412		13	10	23	1.99	0.05	29/08/2021 18:30:26	05/09/2021 11:36:24	6	1	
	07700900954		18	5	23	1.99	0.20	04/09/2021 17:41:20	05/09/2021 16:42:00	15	5	
	07700900767		15	7	22	1.90	0.00	29/08/2021 13:07:11	05/09/2021 15:08:55	0	0	
	07700900964		10	11	21	1.81	0.09	29/08/2021 14:17:32	05/09/2021 14:59:42	6	1	
	07700900711		13	5	18	1.55	0.15	29/08/2021 13:13:04	05/09/2021 13:32:31	12	5	
	07700900566		8	10	18	1.55	0.12	29/08/2021 16:49:51	05/09/2021 16:19:18	6	6	
	07700900254		11	5	16	1.38	0.37	29/08/2021 17:04:46	05/09/2021 15:05:16	10	4	
	07700900421		6	10	16	1.38	0.07	30/08/2021 16:09:12	04/09/2021 10:55:13	2	5	
	07700900245		3	12	15	1.30	0.03	30/08/2021 21:34:43	04/09/2021 11:56:04	0	4	
	07700900173		8	6	14	1.21	0.01	31/08/2021 14:24:46	04/09/2021 11:11:58	1	0	
	07700900267		6	7	13	1.12	0.55	01/09/2021 12:53:58	04/09/2021 09:50:38	6	7	
	07700900434		11	1	12	1.04	0.06	29/08/2021 15:15:49	05/09/2021 14:51:43	8	1	

The Contact Summary screen summarises the set of 'other' numbers that were in contact with the selected subject phone(s) during the selected period. This function can provide aggregated results for multiple subject phones (selectable via the 'Filters' tab) however it is recommended that only one phone is selected at a time as the results for multiple phones combined could be misleading. There are scenarios in which selecting multiple subject phones might be beneficial, however, for example if a case has several phone numbers that are attributed to the same individual or the same group, this query can provide an idea of the overall pattern of contact that group of phones has with others.

The selected phone(s) data is presented in a grid showing the number of outgoing and incoming calls and percentages (of total events and of total connected time) for each contacted identifier and the date and time of first and last contact.

The 'outgoing' columns summarise calls/texts outgoing from the target phone to the listed contact; the 'incoming' columns summarise calls/texts incoming to the target from the listed contact.

17.7.1 Supported Data Types

The Contact Summary query only works with CDR files.

17.7.2 Layout

The query results pane consists of two sections – a summary panel and a results grid.

Summary Panel

The summary panel provides totals for the various main event types listed in the results grid.

^ Event Totals			
Total Events	1,158	Outgoing Text	156
Incoming Text	140	Data	343
Incoming Voice	187	Outgoing Forward	1
Outgoing Voice	331		

There are no filters, drilldowns or other features associated with the summary panel and it is not included in the Excel export for this query.

Results Grid

The results grid contains the following columns:

- » Checkbox – used for the selecting a specific row or rows for drilldown or sending to a map.
- » Number – an 'other' number the selected subject(s) have been in contact with – this also includes a count of any GPRS/mobile data activity grouped as 'Data'.
- » Attribution – any Attributed nominal associated with the number.
- » Outgoing – total count of events (calls, texts, data, etc.) in the selected dataset outgoing *from* the subject phone(s) *to* the listed number.
- » Incoming – total count of events (calls, texts, etc. but not data) in the selected dataset incoming *to* the subject phone(s) *from* the listed number.
- » Total – total count of all events that included the listed number.
- » % of calls – percentage of total events in the dataset represented by the total count for the listed contact. Highlights the other number contacted most by the selected subject(s).
- » % of Time – percentage of total connected time for all events in the dataset represented by the connected duration for the listed contact. Highlights the other number the selected subject(s) spoke to for the longest amount of time.
- » First Contact – date/time of the start of the first record in the dataset where a subject number was in contact the listed number.
- » Last Contact – date/time of the end of the last record in the dataset where a subject number was in contact with the listed number.
- » Individual event type columns – each column summarises the event count for the specified type of event – e.g. Outgoing Voice counts the number of records that show a subject phone calling the listed number.

17.7.3 Filters & Controls

Filters

The Contact Summary grid has one filter option, 'Display top rows only' which is designed to filter the number of results provided.

☐ Display top rows only 50

If unchecked, the filter is inactive and details of all contacted numbers are listed.

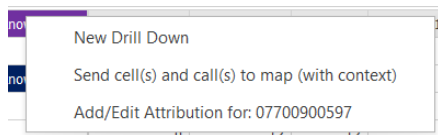
☒ Display top rows only 10

If checked, the results grid is limited to the selected number of rows – in the example, only to the top 10 results will be listed.

Controls

The grid controls are as outlined in the [Grids and Controls](#) section.

The Contact Summary has an additional right-click option that opens an Attributions popout to allow attribution names to be added and edited directly in the Analytic grid.



17.7.4 Understanding the results

The Contact Summary grid provides a simple count of the number of contacts between a selected subject number and a listed 'other' number.

☐	Number	Attribution	Outgoing	Incoming	Total	% of Calls	% of Time	First Contact	Last Contact
☐	c	c	=	=	=	=	=	=	=
☐	Data		343	0	343	29.65	92.00	29/08/2021 12:32:53	05/09/2021 17:01:45
☐	07700900597	Unknown 5	51	47	98	8.47	0.75	29/08/2021 12:21:34	05/09/2021 16:45:36
☐	07700900938		41	30	71	6.14	0.99	29/08/2021 15:38:43	04/09/2021 17:57:23
☐	07700900621	Unknown 6	34	26	60	5.19	0.52	29/08/2021 11:26:22	05/09/2021 12:18:34

In the above example, which has a selected subject number of 07700900177, the most frequently contacted 'other' is 'data', which means that Subject 177 connected to GPRS/mobile Internet services 343 times in the analysed period. Looking at row 2, which has details of contact with a 'real' other number:

- » The 'other' number is 07700900597.
- » It has been attributed to a 'dummy' nominal of 'Unknown 5'.
- » Subject 177 made outgoing contacts (outgoing calls or texts) to 597 51 times.
- » Subject 177 received incoming contacts (incoming calls or texts) from 597 47 times.
- » The total number of contacts between 177 and 597 was 98.
- » This represents 8.47% of all analysed contacts for Subject 177.
- » This represents 0.75% of all connect time (e.g. talk time) for Subject 177.
- » Subject 177 was first in contact (e.g. the start of the first phone call) with 597 on 29/08/2021 at 12:21:34 and the last contact (e.g. the end of the last phone call) between those numbers ended on 05/09/2021 at 16:45:36.
- » Leaving data sessions aside, 597 is the number that Subject 177 was in

contact with the most during that analysed period.

Why, When, Who

	This function is necessary to summarise top contacts for an identifier.
	This function is undertaken as required.
	This function is typically carried out by the following users:  CSAS User

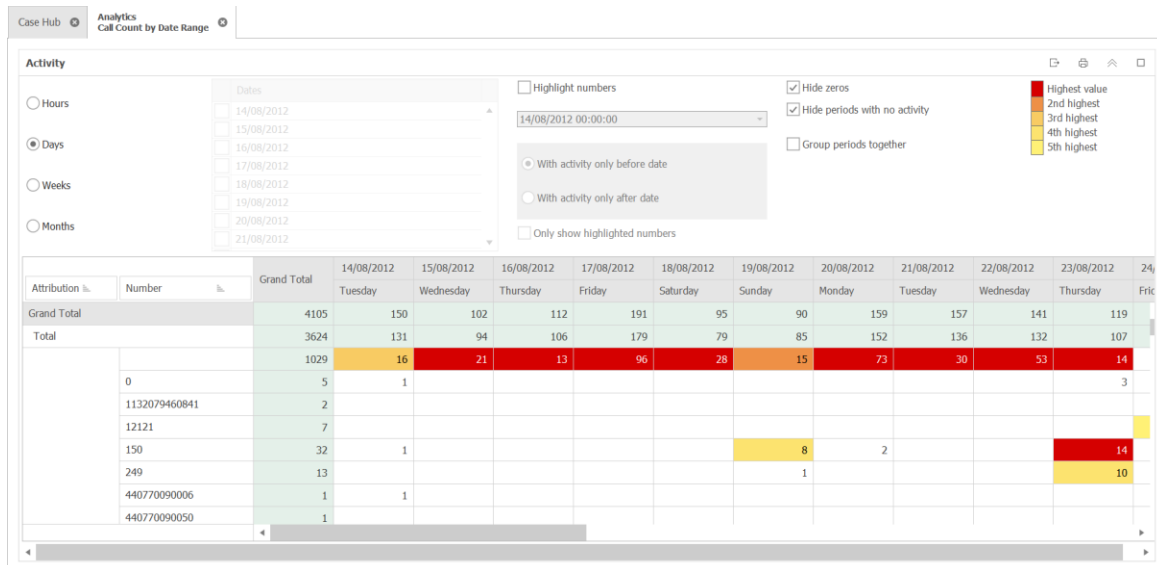
Stepped Procedure

To analyse data using the Contact Summary query:

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters. If your primary interest is in the set of call and text contacts for the subject phones, you may wish to exclude GPRS/mobile Internet events using the Filters > Event Types option.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query.
4. Filter the query results table, if required, to show only the 'Top N' results.
5. The results table will provide a list of the top N contacts for the selected subject phone(s).
6. The results can be sorted or resorted by clicking on the relevant column header and can be filtered using the grid filtering features.
7. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
8. If you wish to view any of the results in a map, select the required row(s), right-click and select Send to Map.
9. If you filtered GPRS/data events from the dataset when launching this query, remember to restore them to the dataset, by cancelling the Event Type filter, before continuing with your analysis.

17.8 Using the Contact Summary by Date Range query

The Contact Summary by Date Range query – which could also be called the 'event record count.' query, as it deals with more than just call data, it also analyses SMS and mobile Internet events as well - displays mobile phone activity (calls, SMS and data sessions) for selected subject phones during a selected date and time range, the results can be grouped into selectable time periods of hours, days, weeks, or months.



The data grid has the selected target phone(s)'s contacted numbers down the left side for the rows and the selected time periods (hour, day, week or month) along the top for the columns. The intersection for each row and column shows the count of connected events between the selected subject phone(s) and the 'other' number represented in that row during the time period represented by that column.

The purpose of this query is to summarise the levels of contact between the subject phone and other numbers and to show the changes in connection levels per period of time. This could show, for example, the number the subject was most in contact with on a day-by-day or week-by-week basis.

17.8.1 Supported Data Types

The Contact Summary by Date Range query can only be used with CDR data.

17.8.2 Layout

The query screen is divided into two main sections:

- » Filters & controls – in the top half of the screen.
- » Results grid – in the lower half of the screen.

		Grand Total	29/08/2021 Sunday	30/08/2021 Monday	31/08/2021 Tuesday	01/09/2021 Wednesday	02/09/2021 Thursday	03/09/2021 Friday	04/09/2021 Saturday	05/09/2021 Sunday
Grand Total		504	81	128	45	41	61	54	50	44
Total		346	50	86	34	22	58	37	31	28
150		3	2					1		
Data		343	48	86	34	22	58	36	31	28
Unknown 5	07700900597	98	13	28	9	12	1	8	12	15
Unknown 6	07700900621	60	18	14	2	7	2	9	7	1

The top two rows of the results grid specify the time divisions used in the analysis:

- » If set to 'hours' each column will show the hour of the 24 hours of the day and will show an aggregate count for all events that took place in each hour across all selected days. It is recommended that the 'hour's option is only used with data from one day at a time.
- » If set to 'days', each column will show the date and day of the week and will show a separate column for each individual date included in the analysis.
- » If set to 'weeks', each column will show the date and the day name of the start of the week. This query defaults to showing Monday as the start of the week, but the first column will contain the name and date of the first day for which data is included.
- » If set to 'months', each column will show the day and date of the first day in each month, except the first column, which will show the day and date of the first day for which data is included.

The event counts are summarised in totals rows (that summarise the contents of each column) and totals columns (that summarise the contents of each row).

There are two totals rows at the top of the grid.

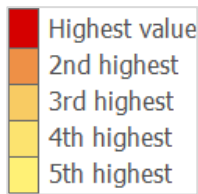
		Grand Total	29/08/2021 Sunday	30/08/2021 Monday	31/08/2021 Tuesday	01/09/2021 Wednesday	02/09/2021 Thursday	03/09/2021 Friday	04/09/2021 Saturday	05/09/2021 Sunday
Grand Total		504	81	128	45	41	61	54	50	44
Total		346	50	86	34	22	58	37	31	28
150		3	2					1		
Data		343	48	86	34	22	58	36	31	28
Unknown 5	07700900597	98	13	28	9	12	1	8	12	15
Unknown 6	07700900621	60	18	14	2	7	2	9	7	1

The 'Grand Total' value shows the total count of all events in each column, including those linked to both attributed and non-attributed identifiers. The 'Total' value shows the event count only for non-attributed identifiers (e.g. only for the rows for identifiers 'Data' and '150' in the example).

		Grand Total	29/08/2021 Sunday	30/08/2021 Monday	31/08/2021 Tuesday	01/09/2021 Wednesday	02/09/2021 Thursday	03/09/2021 Friday	04/09/2021 Saturday	05/09/2021 Sunday
Grand Total		504	81	128	45	41	61	54	50	44
Total		346	50	86	34	22	58	37	31	28
150		3	2					1		
Data		343	48	86	34	22	58	36	31	28
Unknown 5	07700900597	98	13	28	9	12	1	8	12	15
Unknown 6	07700900621	60	18	14	2	7	2	9	7	1

The 'Grand Total' column shows the total number of events in each row – therefore it

shows the total number of connections associated with each 'other' number.



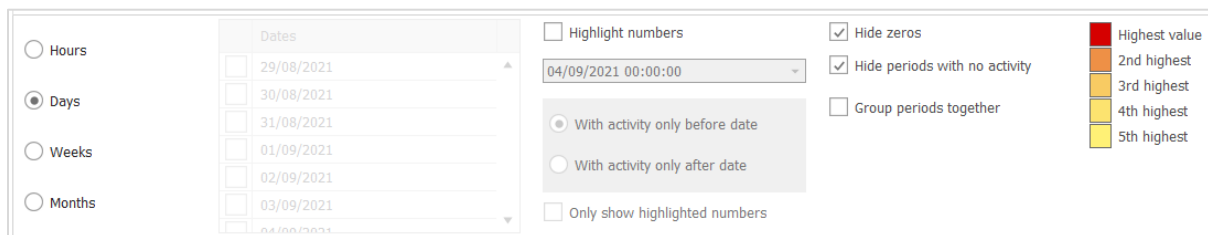
Colour coding is used to highlight the top five contacted numbers in each time period (column), with red equating to the highest count for the time period and shades of orange and yellow denoting the next four highest counts.

If multiple identifiers share the same event count, they will all be coloured with the same infill. For example, if two identifiers had the highest call count for the same day, they would both be coloured red.

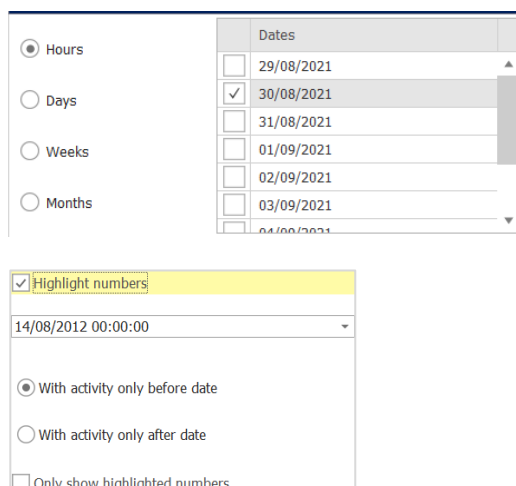
17.8.3 Filters & Controls

Controls

The data to be analysed is selected from the right sidebar 'Source Data' menu in the normal way and is sent into the query when the 'Apply' button is clicked. Any filters or options applied within the query take effect immediately, there is no separate 'run' button and the 'Apply' button only needs to be clicked if you change the set of selected files or sidebar filters.



The control area for the query allows you to vary the granularity of the analysis time period. It defaults to 'days', but the radio buttons allow the time period to be changed to hours, weeks or months, as required.



If the scope is set to 'hours' then you are required to select the specific date you wish to view data for. Although it is possible to select multiple dates, this is not recommended, as in this mode, the results aggregate the count for all selected days into the same 24 columns.

The Highlight Numbers option is designed to provide so-called 'dropped phones' analysis and instructs the query to indicate contacted numbers that drop in or drop out of the dataset over time.

Dropped Phone analysis is sometimes used to analyse the data of suspects who may be aware that they are the subject of an investigation. Such 'forensically aware' subjects are known to use unregistered 'pay as you go' SIMs and cheap handsets that they 'drop' (or stop using) at regular intervals and start using a new number. Ongoing analysis of such subject is difficult until the investigators gain knowledge of the new number, which can

sometimes be gained by analysing the call records for numbers the subject is known to be in regular contact with -a friend, girlfriend or family member, for example.

The 'highlight number's feature allows an investigator to, for example, analyse the call records for one of a suspect's regular contacts looking for new numbers that have started to contact them after the suspect was known to have dropped their old phone. To use this feature, set the Highlighted numbers date value to the date (and time, if it is known) that the suspect is assumed to have dropped their old phone and select the 'with activity only after date' option.

Attribution	Number	Grand Total	29/08/2021	30/08/2021
			Sunday	Monday
Grand Total		1157	169	210
Total		989	137	163
	00770090050	1		
	01623960686	1		
	02079460220	1		1
	02079460800	1		

Any numbers that only started being listed in the data after the specified date/time are shown in bold in the contacted numbers list. One of these numbers might be the new number being used by the suspect, especially if it has a high event count.

The other option, 'With activity only before date', is used to highlight contacted numbers that stopped being in contact with the selected subject phone(s) before the specified date/time. This feature might be used to analyse, for example, a murder victim's call records, using the assumed date/time of the murder as the analysis date and looking to see which regular contacts stopped calling them, possibly providing an indication of who knew the victim had died before it became common knowledge.

The 'only show highlighted numbers' option hides any identifiers that don't meet the current 'highlight numbers' criteria - meaning that any non-highlighted numbers are hidden.

The filters and control zone also hosts three further tickboxes:

- » Hide zeros - if enabled, any intersection cells with a zero event count will be shown as empty cells, if disabled, the cell will contain a zero. Enabling this feature may make cells with actual event counts easier to view.
- » Hide periods with no activity - if enabled, time period columns with no event counts will be hidden. For example, if the grid shows results for five days, but one of those had no events, the column for that day would be hidden.
- » Group periods together - reorders the results grid to group similar time periods together. For example, in 'days' mode, this option would group all the columns for Mondays together and provide a specific Grand Total column just for events that happened on Mondays.

Right-click Menu

The results grid supports two right-click menus, depending on where you click:

Number	Grand Total	14/08/2021	15/08/2021
		Saturday	Sunday
07700900000	3		
07700900000			
07700900000			
07700900000			

Right-clicking in the 'number' column launches asset of sorting options, as shown.

'Sort Time Period value by this row' resorts the grid, based on the selected row – the columns are resorted based on the count values in that row, from lowest to highest.

For example, with no sorting applied, the data for the 157 phone, as shown below, is ordered sequentially, in date order from left to right, starting on 14/08/2021.

	Grand Total	14/08/2021	15/08/2021	16/08/2021	17/08/2021	18/08/2021	19/08/2021	20/08/2021	21/08/2021	22/08/2021	23/08/2021	24/08/2021
Number		Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Monday	Tuesday
07700900157	100	6	4	1	1	5	6	12	9	9	10	

After applying the sort function, however, the columns are now ordered based on the various counts for the 157 phone, starting with 24/08/2021 and other dates on which the event count was zero, then 16/08/2021 and other dates on which the event count was 1 and so on up to 29/08/2021, which had the highest event count for the row with 16 events.

	Grand Total	24/08/2021	25/08/2021	26/08/2021	27/08/2021	16/08/2021	17/08/2021	01/09/2021	28/08/2021	31/08/2021	02/09/2021	15/08/2021
Number		Tuesday	Wednesday	Thursday	Friday	Monday	Tuesday	Wednesday	Saturday	Tuesday	Thursday	Sunday
07700900157	100					1	1	1	3	3	3	4

The 'Sort Time Period text by this row' has no effect in this grid, as there is no text content, only numbers.

The 'Remove all sorting' option cancels the filter and returns the grid to date sequential ordering.

The main results grid supports the usual Analytics right-click menu, with options to drilldown and 'send to map'. See the Analytics [Grids and Controls](#) section for more details.

17.8.4 Understanding the Results

The Contact Summary by Date Range query is designed to expand the 'contact summary' provided by the Contact Summary query, by breaking the data up into time periods, allowing changes and patterns in contacts for the subject phone(s) to be viewed.

The colour coding applied to the results allows the contacts with the highest event counts per period to be readily identified and any changes in highest contacts over time can also be clearly tracked.

Attribution	Number	Grand Total	14/08/2021	15/08/2021	16/08/2021	17/08/2021
			Saturday	Sunday	Monday	Tuesday
Grand Total		882	37	29	19	108
Total		702	18	21	13	96
	249	11				
	Data	691	18	21	13	96
Landline1	02079460677	2				
Unknown 4	07700900177	178	19	8	6	12

In this example, the selected subject phone has been in contact with four other numbers (including 'Data' which is an aggregate of all GPRS/mobile Internet sessions).

On 14/08/2021, the first data in the time span, the contact with the highest event count was the 177 phone, with 19 connections. If you want to see details of those 19 connections, simply right-click in the event count cell and launch a drilldown.

The second highest contact on 14/08 was 'data'.

On 15/08 the roles were reversed, data was the highest contact (21) and 177 was the

second highest (8), and so on.

If you want to exclude GPRS/mobile Internet records from this analysis, they can be deselected using the right sidebar 'Event Type' filter.

Datasets for subjects with a regular pattern of contacts will generally show the same small number of contacts vying to have the top contact count over time. Subjects with complex or chaotic contact patterns may have a constantly changing set of top contacts. This query is particularly useful in identifying periods of time when the subject has an unusual contact pattern.

For example, if the subject's data generally shows a consistent pattern of contact, with the same numbers being contacted in roughly the same proportions over time, but then, around the time of an incident that is under investigation, their contact patterns change radically, that could be taken as evidence of their involvement in the incident.

Alternatively, a sudden change of top contact can be seen to be out of character for a subject, by comparing that time period with the contact patterns in the rest of the period under analysis.

Longer time period divisions (weeks, months) are useful for looking at long term variations in contact patterns, whereas short term divisions (hours, days) are better suited to looking at changing contact patterns as the events under investigation unfold.

Why, When, Who



This function is necessary to identify changing patterns of total contact activity (Contact Summary) across a period time.



This function is undertaken as required.



This function is typically carried out by the following users:

» CSAS User.

Stepped Procedure

To run the Contact Summary by Date Range query:

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters. If your primary interest is in the set of call and text contacts for the subject phones, you may wish to exclude GPRS/mobile Internet events using the Filters > Event Types option.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query.
4. Select the required time period type (hours, days, weeks, months) – if 'hours' are selected then you'll also need to select the specific date(s) to be queried. It is recommended to run the 'hours' query for a single date at a time.
5. If you are attempting to view numbers that only contact the subject before or after a certain date, then select the 'highlight numbers' option, select the cut-off date/time and select whether to highlight numbers that were only in contact before or after the cut off.
6. The results will update automatically as filter/control options are selected, there is no need to click 'Apply' again to run the query.
7. The results grid will provide an event count per contacted number per time division. The five highest ranking event counts per time division will be highlighted using a colour code.
8. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
9. If you wish to view any of the results in a map, select the required row(s), right-click and select Send to Map.

17.9 Using the Contacts Between query

A common request to communications analysts is for them to examine data for two or more phones and answer the questions 'have these phones been in contact with each other and if so when and how frequently?'.

The Contacts Between query summarises the set of contacts for each selected and provides a count showing the number of contacts for each. For each 'other' number, it also shows the date/times when that number was in contact with any of the selected subject numbers, shows the total count of all contacts for the number with all subjects and highlights the number of selected subject phones each 'other' number was in touch with.

The query can also be filtered to, for example, only show details of the selected subjects and their contacts with each other.

Further options allow you to select one or more specific pairs of identifiers (e.g. one subject phone and one 'other' phone) and get a graphical view of the patterns of contact and a detailed itemisation of exactly what types of contact were made (calls, texts, etc) on which dates.

The query is useful for showing the level of contact between different numbers, but also for highlighting 'other' numbers that have been in contact with more than one selected subject number.

17.9.1 Supported Data Types

The Activity Hotspot query can be used with CDR and cellular data only.

17.9.2 Layout

The query has three sections, plus a drilldown grid.

Results Grid

The results grid is laid out in rows and columns.

Each row represents one of the 'other' numbers that were in contact with at least one of the selected subject phones – if there has been contact between subject phones, then a subject phone number could also appear as a row.

The columns in the report are divided into two sections.

Analytics

Calls between

Call Between Contacts Grid

☒ Target Phones
☒ Non-Target Phones
☒ Attributed
☐ Unattributed

Minimum Number Of Targets Contacted

All

☒ Rank By Most Common
☐ Rank By Highest Count

Reset

StartDate

Start Time

Call Type

Hour

Evts...

Tar...

First Co...

Last Co...

Target Attribution %

Target MSISDN %

Other MSISDN

Other Attribution

07700000177

Suspect A

07700000007

Suspect B

07700000001

Suspect C

07700000177

Suspect A

07700000007

Suspect B

07700000001

Suspect C

Events

Targets Contacted

First Contact

Last Contact

306

2

14/08/2012 10:57:35

09/09/2012 19:00:42

115

2

29/08/2012 12:21:34

11/09/2012 14:15:48

60

1

29/08/2012 11:26:22

05/09/2012 12:17:43

The first section lists the selected subject phones – the intersection of rows and columns in this section show a count of the number of contacts between the two phone numbers. Looking down one column (which is dedicated to one selected subject number) therefore provides details of the set of other numbers each subject number was in

contact with in the selected dataset.

The second section provides a detailed summary of the events associated with each row's 'other' number, including:

- » **Events:** The overall number of contacts between this number and any of the selected subject numbers.
- » **Targets Contacted:** The number of selected subject phones this number has been in contact with.
- » **First Contact / Last Contact:** These columns show the earliest contact and the latest contact each 'other' number had with any of the selected subject numbers.

Details View – Diagram

The Details View offers a deeper insight into the level and frequency of communication between a selected set of identifiers.

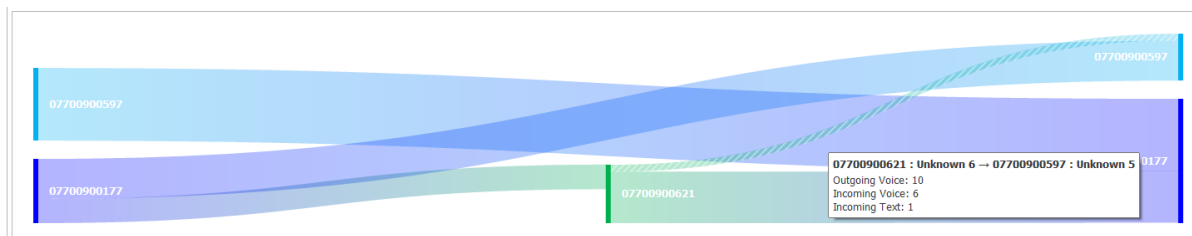
From the results grid, select the intersection grid cells for the identifiers you wish to view in more details, right-click and select New Details View.

Other MSISDN	Other Attribution	Unknown 4	Unknown 5	Unknown 6	Events	Targets Contacted	First Contact
07700900177	Unknown 4		178	128	306	2	14/08/2021 10:57:30
07700900597	Unknown 5	98		17	115	2	29/08/2021 12:21:30
07700900621	Unknown 6	60					

New Drill Down
New Details View
Send cell(s) and call(s) to map (with context)

In this example, the intersections between the subject numbers have been selected, to provide a Details View highlighting the contacts between all subject phones.

The Details View diagram is based on a type of visualisation known as a 'Sankey' diagram, which shows the connections between a set of elements as lines and indicates the volume of connections by carrying the thickness of the line – e.g. the line between identifiers that haven't communicated very much will be thin, that between identifiers that communicate a lot will be thicker.



The diagram separately identifies communications that travel in different directions. In the example, outgoing communications travel left-right and incoming communications travel right-left. This indicates that 597 contacted 177 (the larger blue line at the top of the diagram) more often than 177 contacted 597 (the smaller purple line in the middle of the diagram).

Click anywhere on the Sankey diagram to bring it into focus and then hover on any line to

see more details.

Details View – Grid

The grid displays more details about the set of data that was sent into the Details View.

In this example, only the intersection between two subject phones has been selected.

Other MSISDN	Other Attribution	Unknown 4	Unknown 5	Unknown 6	Events	Targets Contacted
07700900177	Unknown 4		178	128	306	2
07700900597	Unknown 5	98		17	115	2
07700900621	Unknown 6	60				

New Drill Down
New Details View
Send cell(s) and call(s) to map (with context)

The resulting Details View grid itemises the contacts that took place on each day in the selected date range on which contact occurred. Each different type of contact (incoming voice, outgoing voice, incoming text, etc) is itemised separately and a Grand Total in each row shows the total number of contacts for each day. Only communication types that were found in the dataset are listed – in the example below, only incoming and outgoing voice are listed as the selected dataset shows no text messages being exchanged between the selected identifiers.

Start Date	Other MSISDN	Other Attribution	Target MSISDN	Target Attribution	Incoming Voice	Outgoing Voice	Grand Total
29/08/2021	07700900597	Unknown 5	07700900177	Unknown 4	5	8	13
30/08/2021	07700900597	Unknown 5	07700900177	Unknown 4	15	13	28
31/08/2021	07700900597	Unknown 5	07700900177	Unknown 4	7	2	9
01/09/2021	07700900597	Unknown 5	07700900177	Unknown 4	7	5	12
02/09/2021	07700900597	Unknown 5	07700900177	Unknown 4		1	1
03/09/2021	07700900597	Unknown 5	07700900177	Unknown 4	2	6	8
04/09/2021	07700900597	Unknown 5	07700900177	Unknown 4	3	9	12
05/09/2021	07700900597	Unknown 5	07700900177	Unknown 4	8	7	15

17.9.3 Filters & Controls

The results grid and Details View grid offer some basic controls.

Results Grid

☒ Target Phones
☒ Non-Target Phones
☒ Attributed
☒ Unattributed

Minimum Number Of Targets Contacted: All
☐ Rank By Most Common
☐ Rank By Highest Count
Reset

- » Target Phones: select this checkbox to include only target/subject phones in the grid results.
- » Non-Target Phones: select this checkbox to include non-target (or 'other') phones in the grid results.
- » Attributed: select this checkbox to include attributed phone data in the grid results.
- » Unattributed: select this checkbox to include non-attributed phone data in the grid results.
- » Minimum Number of Targets Contacted: filters the grid to show only 'other' numbers that have been in contact with at least the selected minimum

number of subject phones – e.g., in a grid showing data for 4 selected subject phones, if this option was set to '2', the grid would filter to only show other numbers that had been in contact with two or more of the subject phones, numbers that had only been in contact with one of the subject numbers would be excluded. If this option was set to '4' then the grid would consist only of phones that had been in contact with all of the selected subject phones.

- » Rank By Most Common: select this checkbox to order the grid results by the other numbers that had been in contact with the highest number of subject phones.
- » Rank By Highest Count: select this checkbox to order the grid results by the other numbers that had the highest event counts – e.g. those that were in contact with one or more of the subject phones most frequently.
- » Reset button - reset the filters to their default settings by selecting the button.

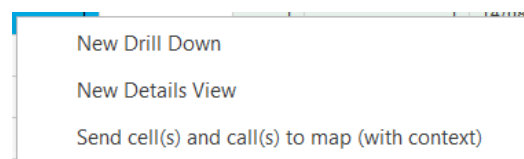
Just like the Pivot Builder query, the Contacts Between results grid offers the opportunity to select additional criteria to add extra detail to the results grid. The set of additional criteria that can be dragged into the results grid are listed below, see [Prebuilt Query Options](#) for more details of how to use the additional criteria feature:

- » Start Date: a filter with checkboxes from which you can select / deselect different start date periods.
- » Start Time: a drop-down menu from which you can select different call start times given by the data set.
- » Call Type: a filter with checkboxes from which you can select / deselect different incoming and outgoing call types.
- » Hour: a sliding filter to adjust the timespan between calls from 0-23 hours.

Right-click Menus

The results grid and Details View grid support right-click menus.

The results grid menu supports the standard Analytics options plus an option to send the selected data to a New Details View.



The Details View grid supports just the standard Analytics right-click menu options, as outlined in the [Grids and Controls](#) section.

17.9.4 Understanding the results

The Contacts Between query offers the opportunity to view the communications relationships between selected subject phones and the other numbers they are in contact with. In that sense it is similar to the results offered by the Call Summary query but can also show that summary for multiple subject phones side by side.

When looking at the data for a single subject phone, the query can highlight the other numbers the subject is in contact with most often.

When looking at the data for multiple subject phones, the query can provide an indication

of the other numbers that were in contact with the greatest number of subject phones or even highlight only the numbers that were in contact with *all* subject phones or with a minimum number of subject phones.

The results of this query generally relate to understanding the circles of association for the selected subjects, who they are in contact with and how often. This can potentially be used to, for example, detect phone numbers of previously unknown suspects or associates.

Why, When, Who



This function helps to find relationships between target and contacted phones and how often contact has been made.



This function is undertaken as required.

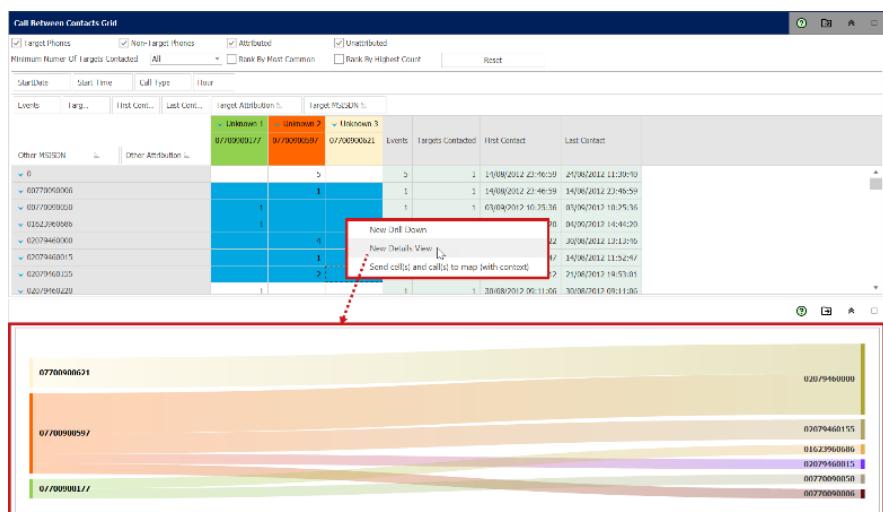


This function is typically carried out by the following users:

»» CSAS User.

Stepped Procedure

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query results grid.
4. View the details provided in the results grid, using the various filters to ensure that data for the required set of phones is displayed.
5. If you wish to see more details for a subset of phones in the Details View, from the 'Contacts Between Contacts Grid', select the required data by clicking on the intersection between the subject and contacted phones you wish to examine. You can click on just one intersection or click and drag a set of contiguous intersections. Right-click and select 'New Details View' send the data to the view.



6. The Sankey Diagram and 'Contacts Between Details Grid' open:

7. In the Sankey diagram, you can hover the cursor over the any relationship between target and other Identifiers for more information about that relationship.
8. The Details View grid provides further details about the mix of communication types that made up the contact between the selected numbers on days on which contact took place.
9. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
10. If you wish to view any of the results in a map, select the required row(s), right-click and select Send to Map.

17.10 Using the Correlation query

The Correlation Query is designed to provide tools for searching for common items in large datasets – for example, looking for phones that appear in multiple cell/tower dumps or looking for 'contacted numbers' that are common to multiple subject phones.

The initial release of the Correlation query supports two use cases:

- » Cell/tower dump – which searches for common numbers across multiple files, also works with timing advance area dump and RTT files.
- » CDR Other phone – which searches for common 'other' numbers across multiple files

17.10.1 Supported Data Types

The Correlation query can be used with CDRs, cell/tower dumps, timing advance area dump, RTT and cellular data only.

17.10.2 Layout

The query has three sections, plus a drilldown grid.

Correlation Query

Query Settings

Correlation Type: Cell/Tower Dump
Data to Correlate: Phone Number

Data Sources

File Name	Time Range
1h3anonymised_S-NEWCELLDUMP_0000545324_3..csv	23/08/2
1h3anonymised_S-NEWCELLDUMP_0000545328_3..csv	23/08/2
1h3anonymised_S-NEWCELLDUMP_0000545329_3..csv	23/08/2
1h3anonymised_S-NEWCELLDUMP_0000545330_3..csv	23/08/2
1h3anonymised_S-NEWCELLDUMP_0000545331_3..csv	23/08/2
1h3anonymised_S-NEWCELLDUMP_0000545332_3..csv	23/08/2

Groups

Group	Files

Results Details

Number of groups	Common Identifiers

Run

Data Sources

The Data Sources section automatically lists all qualifying imported files in the case, without them needing to be selected from the right-sidebar – this is different to all other CSAS Analytics queries, where files need to be explicitly selected in the right-sidebar menu before the query can run, and was implemented as a time-saving measure. Cases that involve cell/tower dumps often import large numbers of source files (one file for each serving cell at each significant location) and all imported files are usually included in the analysis, so imposing a step where all required files had to be separately selected before the analysis could be performed would be an unnecessary additional step.

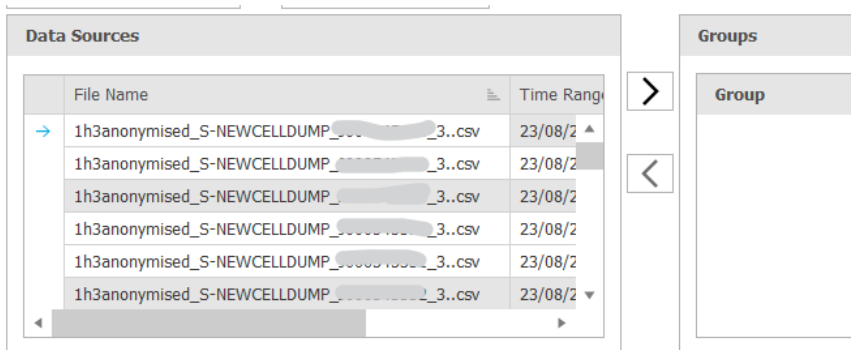
The underlying assumption for the Correlation query options is that the imported files relate to different offences, incidents or locations and that the files need to be grouped to represent those that relate to each separate offence, incident or location.

Files are selected for analysis by first assigning them to a group.

For example, imagine that a cell/tower dump has been undertaken to search for phones that were in use in the area of three linked offences – three robberies that took place on different days at different locations, for example. The investigators have requested cell/tower dumps for the cells that are expected to provide coverage at the three offence locations for the periods that cover each offence.

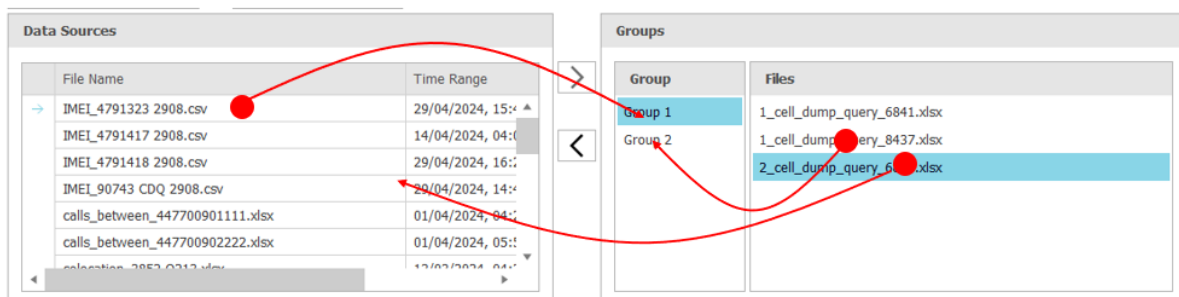
All of the source files that relate to cells that cover offence location 1 should be selected as part of the same analysis group – to do this, select the files that relate to offence location 1 from the file list in the Data Sources section. Use 'click & shift' to select a contiguous set of files or 'click & ctrl' to select non-contiguous files. Once all the files for

offence/location 1 have been selected, click on the right chevron button  to send those files to the Groups window as Group 1.



Perform the same action with the remaining files and assign them to Groups.

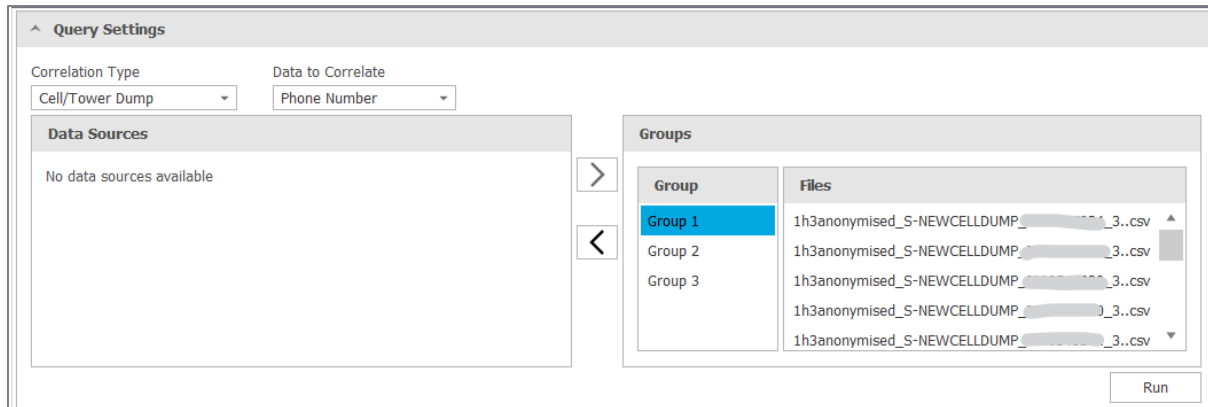
If you make a mistake and send a file to an incorrect Group, or you miss a file that should have been included in a Group, you can click and drag files between the Data Sources list and the Group List and you can drag a file from the Files list associated with a Group and drop it in a different Group or drag it back to the Data Sources list.



It may be an idea to edit the source file names before the files are imported into CSAS to include the intended group number in the filename – for example, all files that are intended to be included in Group 1 could have '1' added to the front of the file name.

Groups

The Groups window lists the set of file groups that have been created – clicking on a name in the Group column causes the files that have been selected as part of that group to be displayed in the Files window.



Once all groups have been correctly selected, click the 'Run' button to run the Correlation query.

Results Details

The Results Details window lists identifiers that have been found in multiple Groups.

Results Details						
Number of groups	Common Identifiers	Identifier	Attribution	Group 1	Group 2	Group 3
3	5	[REDACTED]		23/08/2017 18:30:27 - 18:45:58	23/08/2017 18:45:10	23/08/2017 18:32:20 - 18:34:37
2	54	[REDACTED]		23/08/2017 18:30:42 - 18:34:50	23/08/2017 18:30:16 - 18:46:57	23/08/2017 18:42:32 - 19:13:49
1	361	[REDACTED]		23/08/2017 18:32:47 - 18:33:51	23/08/2017 18:30:36 - 18:31:07	23/08/2017 18:41:00
		[REDACTED]		23/08/2017 18:30:36 - 18:47:11	23/08/2017 18:44:31	23/08/2017 18:41:18 - 18:42:44
		[REDACTED]		23/08/2017 18:35:17	23/08/2017 18:33:21 - 18:43:31	23/08/2017 18:36:20 - 18:42:37

In this example, three Groups were created relating to cell/tower dumps captured for three different offence locations.

The 'number of groups' and 'common identifiers' columns summarise the common identifiers that have been detected – in this example, there were 361 identifiers that appeared in only one location, there were 54 identifiers that appeared at two locations and there were 5 identifiers that appeared at all three locations.

Clicking on a row in that table causes the details of the correlating identifiers to be shown in the results window. The results grid lists the correlating identifiers and summarises the date/time span during which each was detected as being active at each Group location.

Right-clicking on any row in the results grid and selecting 'New drilldown' causes the full details of the events summarised in that row to be shown in the Drilldown window.

17.10.3 Filters & Controls

The Correlation query offers two query options via the Correlation Type dropdown menu and those query types can be set to display three types of identifier – phone number, IMEI or IMSI:

Correlation Type Cell/Tower Dump	Data to Correlate Phone Number	Correlation Type Cell/Tower Dump	Data to Correlate Imei
Correlation Type CDR Other Phone	Data to Correlate Phone Number		

- » Cell/Tower Dump – searches for common identifiers across different cell dump Groups – it can be set to search for phone numbers, IMEIs or IMSIs
- » CDR Other Phone – looks for common contacted numbers across different cell dump Groups – i.e. do any of the phones that are active during different cell dumps contact the same 'other' number? This analysis is performed only on phone numbers.

The Correlation query is able to also make use of the standard right-sidebar filters, such as Date/Time, Location and Event type.

17.10.4 Understanding the results

The Correlation query offers a quick and simple method for determining whether any identifiers appear in multiple sets of data – for example, if the same phone appears in multiple cell dumps.

The query results list all numbers found in the source data and summarise them based on how many Groups each number appears in – it then lists the set of numbers that appear in one Group, two Groups, etc up to all Groups.

In this example, there was only one number that appeared in the data for all three cell dumps. Whilst that isn't proof that the holder of that phone was involved in the incidents that occurred at each cell dump location, it does offer a viable line of enquiry for further investigations, either for phones that were active in the area of each incident or for 'other' numbers that were contacted at around the time of each incident.

17.11 Using the Drug Line Analysis query

Many drugs gangs run a significant part of their business via mobile phones, in fact, many drugs gangs use a well-known phone number to advertise their product and take orders from their customers – this is commonly known as a 'drugs line' and the associated phone number can be a valuable asset for an established drugs gang.

The drugs line number is often used to send out 'bursts' of text message adverts to customers; a proportion of those customers respond to the SMS adverts by texting or calling the drugs line number to place an order, which is known as a 'deal'.

The Drug Line Analysis query supports a method that has been developed for estimating the volume of drug deals handled via a drugs line phone by analysing the pattern of outgoing SMS 'burst' adverts and incoming voice or text responses from the recipients of those adverts. The query tabulates the number of qualifying responses and offers an

estimate for the number of deals arranged through the drugs line over a period of time.

Separately, a drugs expert witness can use the output of the query to estimate the volume of product and the associated amount of cash those deals represent.

Note: The process that this function has automated was originally developed by specialist drugs officers in the UK. The methodology that the query is a component of has been approved for use as a part of a prosecution by the Crown Prosecution Service and the overall methodology, including the use of CSAS and the drug line query, has been upheld as being valid and reasonable by the UK Court of Appeal (in R v Akrofi-Daniels).

One of the benefits of this methodology is that it has enabled the prosecution of 'drugless' cases – cases where the defendants did not need to be caught in possession of drugs or even be observed physically selling any drugs. As long as the individual(s) can be shown to be in control of the analysed drug line phone line, they can be prosecuted for the deals that are alleged to have been arranged via that phone line.

How the query works

The query works through a dataset in a series of stages, outlined below. The query generally works best when analysing data for just one phone, a drugs line phone, that has been used for sending burst SMS adverts and receiving calls and texts to place orders for drugs. It can also work well in cases where different phone numbers are used consecutively – i.e. the original number is used for a period of time but then switch to a different number. In scenarios in which the process is split between two phones – e.g. one phone sends out the SMS adverts but a different number receives the orders – please contact CSAS Support to discuss other forms of analysis that could be performed.

The basic process is as follows:

1. The selected subject data is divided into weeks – meaning that the events are grouped by the week in which the event timestamp falls. This is done so that a weekly running total of qualifying events can be calculated.
2. The event data for each week is analysed looking for 'bursts' of outgoing SMS records. Filtering can be used to vary the definition of what constitutes a 'burst', but the default definition is if 10 or more outgoing SMS were sent to different recipients within a 60 second period.
3. If a burst is detected, the query captures details of the recipients of the SMS messages and adds them to a list of overall recipients. The process ignores incoming calls or messages from numbers that haven't been detected as recipients of a burst SMS, so the list of recipients is an important component in the analysis.
4. The process then checks to see if any of the recipients of a burst SMS responded by calling or texting the subject phone in the period after a burst was sent. Any recipient that responds is added to the list of respondents.
5. At the end of each week's worth of data, the query will have compiled a list of SMS burst recipients and another list showing the subset of recipients who responded.

6. The list of respondents is then further filtered to remove those that responded less than a minimum number of times. This is done to remove people who, for example, only responded to say, 'please take me off of this list, I don't wish to receive these messages anymore'. This just leaves responders who have contacted the drugs line multiple times – these are classed as being 'qualified respondents'.
7. The query then counts the number of days during the week that each qualified respondent contacted the drugs line – it doesn't count the number of individual contacts, it just counts the number of days on which there was a contact. Each contact is assumed to represent a 'deal' but the process is deliberately conservative in that it only counts one assumed deal per day per qualified respondent.
8. For each analysed week, the query therefore ends up with a count of 'deal days' (e.g. days on which a deal was done) per qualified respondent which, following the assumption the method is based on, gives a count of the number of deals arranged via the drugs lines in each week.
9. The process is repeated for each further week covered by the selected data and provides an overall count of suspected deals across the analysed period.
10. The output of the query should then be passed to a drugs expert witness, who can provide evidence of the average volume and value of a 'deal', allowing them to comment on the estimated volume of business arranged via the drugs line.

17.11.1 Supported Data Types

The Drug Line Analysis query can only be used with CDR data that has been obtained for a phone used by a drug line.

17.11.2 Layout

The Drug Line Analysis window has two main parts:

- Controls ribbon you can select different options and filters from.
- A results grid:

Drug Line Analysis							
Use Manual Burst	☒	Use Auto Burst Detection	☐	Exclude SMS reply	☐	Calculate across period	☐
Min. Message #	10	Min. Messages	10	Exclude AUTO reply	☒	Show footers	☒
Duration (secs)	60	Max Interval (secs)	5	Min. Responses	2	Min. Call Duration	4
Week commencing date	Total # o/g SMS	Count of outgoing messages included in a bulk event	Total bulk event recipients (over entire period) in this week	Number of bulk msg recipients that responded	Number of qualifying repeat respondents	Count of days on which each qualifying respondent responded	
27/03/2023	54	50	10	7	6	12	
03/04/2023	140	130	10	7	7	38	
10/04/2023	143	130	10	7	6	34	
17/04/2023	112	90	10	7	7	28	
24/04/2023	153	140	10	7	7	38	
01/05/2023	152	140	10	7	7	39	
08/05/2023	142	130	10	7	7	39	
15/05/2023	129	110	10	7	7	30	
22/05/2023	136	120	10	7	7	36	
29/05/2023	139	130	10	6	6	29	
05/06/2023	131	120	10	6	6	34	
12/06/2023	156	140	10	6	5	33	
3612 SMS 3240 Bulk Msgs 270 159 155 822 Days							

A separate Drill down grid can be opened from the results grid, if required.

The results grid displays a row for each analysed week – with the date of the start of the week shown. It also displays the following columns, which show the steps of the query process:

- » Total # o/g SMS – this is the total number of outgoing SMS events during that week, irrespective of whether the messages were in a burst or not.
- » Count of outgoing messages included in a bulk event – the subset of outgoing SMS that were assumed to be included in one or more SMS bursts.
- » Total bulk event recipients (over entire period) in this week – the number of unique recipients of burst SMS messages during the week.
- » Number of bulk msg recipients that responded – the subset of recipients that responded to the analysed phone during the week.
- » Number of qualifying repeat respondents – the subset of respondents who responded at or above the minimum number of qualifying responses threshold.
- » Count of days on which each qualifying respondent responded – count of 'deal days per respondent', which provides an estimate for the number of assumed deals arranged that week.

Each column has an overall total at the foot of the query:

178 SMS	178 Bulk Msgs	31	23	23	66 Days
---------	---------------	----	----	----	---------

The 'days' count on the extreme right shows the overall number of assumed deals arranged during the analysed period.

17.11.3 Filters & Controls

As with all analytics queries, using the 'Filters' and 'Settings' tabs located on the sidebar, you can filter the case data, for example 'From' and 'To' dates and times, and therefore control the output of the query.

Drug Line Analysis

Use Manual Burst	☒	Use Auto Burst Detection	☐	Exclude SMS reply	☐	Calculate across period	☐
Min. Message #	10	Min. Messages	10	Exclude AUTO reply	☒	Show footers	☒
Duration (secs)	60	Max Interval (secs)	5	Min. Responses	2	Min. Call Duration	4

In the Drug Line Analysis window, there are various options and filters you can select to change what information is output in the results grid:

Using the checkboxes, you can select from two burst detection modes:

- » 'Use Manual Burst' - using this mode, you can manually define the parameters that constitute an individual 'burst SMS' event – this may be based on analysing the data for a specific drug line as the length of a burst will be mainly determined by the number of recipients the messages are sent to each time. If the bursts in the analysed data are reasonably uniform (e.g. sent to a similar number of recipients with each burst taking a similar amount of time to transmit), you could manually define the burst parameters.

- 'Min Message #' - selecting this option allows you to choose the minimum number of outgoing SMS messages that can constitute a burst.
- 'Duration (secs)' - selecting this option allows you to choose the maximum time period over which the SMS messages must have been sent to be part of the same burst.

Use Manual Burst	☒	Use Auto Burst Detection	☐
Min. Message #	10	Min. Messages	10
Duration (secs)	60	Max Interval (secs)	5

» 'Use Auto Burst Detection' – this mode is designed to be used if the parameters of the SMS bursts in the data vary over time – for example, if initially there are 10 recipients and a burst takes 15 seconds to transmit, but later in the period there are 100 recipients and the burst takes 2 minutes to transmit. Fixed manual burst definitions don't work well if the data varies, but automatic burst detection can be used instead. Using this mode, you enter the minimum number of messages a burst must contain and the maximum time interval between each message (5 seconds is default). Using these settings, the query will detect the end of each burst if the interval between messages exceeds the maximum interval.

- 'Min Messages' - selecting this option allows you to choose the minimum number of outgoing SMS messages that can constitute a burst.
- 'Max Interval (secs)' - selecting this option allows you to choose the maximum time period allowed between messages before the current burst is deemed to have ended.

Another set of filters handle the ways in which responses are interpreted or how the data is displayed:

Exclude SMS reply	☐	Calculate across period	☐
Exclude AUTO reply	☒	Show footers	☒
Min. Responses	2	Min. Call Duration	4

- » 'Exclude SMS reply' – selecting this option ensures that only respondent phone calls are counted.
- » 'Exclude AUTO reply' – if SMS responses are permitted, selecting this option will look for responses that arrive within 1 or 2 seconds of the outgoing text being sent, on the assumption that they are automated responses and shouldn't be counted.
- » 'Min. Responses' – selecting this option sets the threshold for a 'qualifying' respondent. This option defaults to '2', meaning that a recipient must

respond twice (on different days) within the week to qualify as a potential customer.

- » 'Calculate across period' – when disabled (the default), a number must have received a burst SMS in each week to be considered as a recipient during that week; if enabled (not recommended), if a number receives a burst SMS in any week, they are considered to be a valid recipient in all weeks. The default value for this setting ensures that the 'burst SMS - response' relationship between the drug line and the recipient must be refreshed every week in order for that recipient's responses to be counted.
- » 'Show footers' – selecting this option controls whether the totals are displayed at the foot of the query grid.
- » 'Min Call Duration' – this sets the minimum duration of a respondent's phone call to the drugs line to allow it to qualify as being long enough to carry the conversation necessary to place an order. Calls shorter than this value are assumed to have disconnected or gone to voicemail and won't be counted.

When you have selected all necessary options and filters, to start the query click the button. The query runs and the results are shown in the grid.

Each of these options has a default value but can also be changed to some other value. Changing filters values is often based on the specific nature of the data for a particular drug line phone, the size of the 'customer list' the SMS adverts are sent to and the contact preferences of the respondents, so the filters may need to be adapted for each case based on the specifics of the analysed data for each case.

The results grid supports the standard Analytics right click menu options of 'drilldown' and 'send to map', as outlined in the [Grids and Controls](#) section.

17.11.4 Understanding the results

The form of analysis provided by this query is specifically designed to work with one scenario, which involves call data obtained for a drug line phone, one that is involved in sending out drug adverts via SMS and receiving orders for drugs from customers via calls and texts.

Week commencing date	Total # o/g SMS	Count of outgoing messages included in a bulk event	Total bulk event recipients (over entire period) in this week	Number of bulk msg recipients that responded	Number of qualifying repeat respondents	Count of days on which each qualifying respondent responded
04/09/2023	40	40	5	2	2	8

Looking in detail at the example results data provided above:

- » The data covers the week beginning 04/09/2023.
- » There was a total of 40 outgoing SMS for this phone in that week.
- » All 40 SMS events were deemed to be part of one or more bulk SMS bursts – meaning that the subject phone wasn't used for any non-burst outgoing SMS events.
- » The 40 burst SMS messages were sent to 5 different recipients across all bursts that week.
- » Only 2 of those recipients responded.
- » Both of those 2 recipients responded on more than one day, so both of them

were classed as 'qualified respondents'.

- » The 2 qualified respondents responded on 8 different days between them – this might mean that each respondent responded on four days each that week or it might mean some other permutation of responses.
- » The inference that can be drawn from this is that the drug line made 8 sales or deals that week.
- » A drugs expert witness could now testify as to the average volume and value of each deal and give an estimate for the amount of product moved by the line in that period.

It must be stressed that the CSAS Drug Line query is not attempting to estimate the volume or value of the drugs that may have been sold via the analysed drug line phone, that is a job for a suitably qualified and experienced drugs expert witness. The CSAS query is merely using the analysed data to provide evidence of the number of contacts the analysed phone received that met certain criteria.

This query and its output can be used as part of a wider process that follows a methodology developed by UK police. If you would like further information about the wider methodology or are considering using the query and would like details of a drugs expert witness or if you have any other questions relating to this query, please contact CSAS Support or your Forensic Analytics account manager.

Why, When, Who



This function is necessary to help estimate the number of deals arranged via a drug line phone.



This function is undertaken as required.



This function is typically carried out by the following users:

>> CSAS User.

Stepped Procedure

To launch the Drug Line Analysis query:

1. Manually analyse the required dataset first to determine aspects such as the number of recipients and time taken to send the largest SMS burst, the average duration of respondents' calls. Also determine your preference for the day that each week starts and the minimum number of responses that constitute a qualified respondent. If you are unsure about the values to use, run the query with default values and then examine the results to see if they provide a reasonable interpretation of the data.
2. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters. GPRS/data events are ignored by the query, so there is no need to filter those events from the dataset.
3. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
4. Click 'Apply' to send the selected dataset to the query.
5. If necessary, you can change any of the filter and control settings. If you change any of the filters you must click 'Apply' again to rerun the query.
6. Click the query specific 'Apply' button to run the analysis. You'll only need to click the right sidebar 'Apply' button again after making changes to the sidebar controls or filters and the results chart will update to show the data for the selected source data.
7. Review the results grid to gain an understanding of the weekly and overall numbers of 'deal days' handled by the drug line.
8. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
9. If you wish to view any of the results in a map, select the required row(s), right-click and select Send to Map.
10. The results should be provided to a drugs expert witness, who can use them as the basis for an estimate of the volume and value associated with the deals indicated by the query.

17.12 Using the First Cell Last Cell query

This query, often known as 'bed & breakfast', 'bedding calls' or 'heads up heads down' analysis, displays the cells used by the selected subject phone(s) which were recorded as being used to carry the first connection and last connection for each contiguous period of activity during a selected time period.

The 'First Cell Last Cell' screen summarises the selected source data files into a chart showing the cells used for the first and last cellular connections (e.g. calls, SMS, data sessions, etc) for each period of continuous activity. This is usually employed as a form of 'lifestyle analysis' and is a method of potentially attributing a phone to a suspect by determining whether the cells primarily used for that phone's first and last calls are located close to a known home address or other significant address. The technique can also be used to identify possible locations of unknown significant addresses for a subject.

This type of analysis is based on two fundamental assumptions: first, that periods of inactivity equate to periods of sleep; second, that the subject always or generally sleeps at the same address. If either of those assumptions is incorrect, this form of analysis will not necessarily provide usable intelligence.

It is generally recommended that this analysis is performed on the data for one subject at a time – data for multiple phones could be analysed together, if those phones were all attributed to the same subject. The results could become very confusing if data for several subjects was analysed together.

17.12.1 Supported Data Types

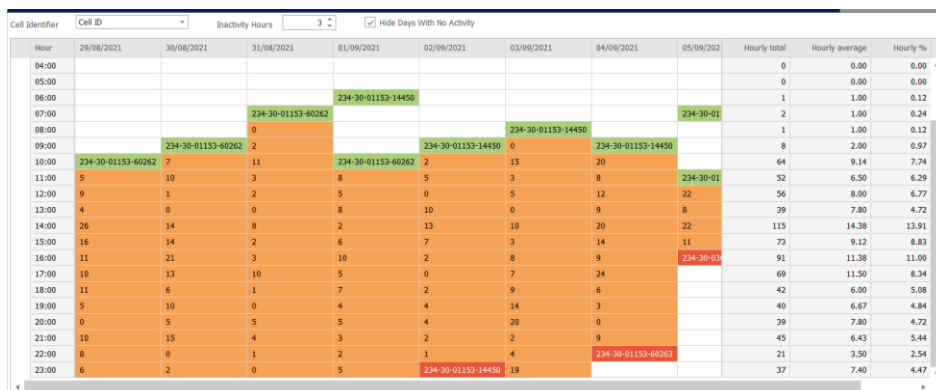
The First Cell Last Cell query can only be used CDR data.

17.12.2 Layout

This Analytics function comprises of two panes:

- » Activity
- » Summary

Activity Pane



The Activity pane is designed to highlight call usage activity patterns, which are organised into 'contiguous periods of activity'.

The results grid is laid out with each column representing a day (with a column header showing the date) and each row representing an hour (with the row header showing the time) – the intersection of a column and a row therefore represents one hour of one day. The grid is filled as follows:

- » Hours during which the selected subject phone(s) had no active connections are blank and uncoloured.
- » Hours during which a new connection is established after a period inactivity are coloured green and details of the first used cell during that period are displayed.
- » Hours during a period of activity are coloured orange and a count of the number of connections that were active during that hour is provided.
- » Hours during which the last connection for a period of activity was made are coloured red and details of the last used cell during that period are displayed.
- » If the first and last event for a period time occur in the same one-hour period, the cell will show the details of the first cell only and will be coloured green. Activating a drilldown can provide details of the last cell used during that hour.

An hour within a period of activity will have its event count incremented for each connection that is active during that hour – this means that, of course, each new call, text or data session that is set up increments the count, but long duration events that span across multiple hours will also increment the count.

For example, imagine the subject phone makes a call that starts at 15:50, the event count for the hour 15:00-15:59 on that day will be incremented. If the call lasts for 30 minutes, the event count for the hour 16:00-16:59 will also be incremented, as the call was also active during that hour. The same applies to long running GPRS/mobile data events.

The query follows this methodology as a way of detecting ongoing activity and to avoid incorrectly assuming that the subject phone was 'inactive' when it was actually in use, just with a long-lasting connection.

If you wish to concentrate on voice & SMS activity and avoid issues caused by long-lasting GPRS sessions, you can elect to remove GPRS events from the analysis using the right sidebar 'Event Type' filter. If you do remove GPRS events from the dataset, please remember to disable the event type filter again before moving on to undertake more general analysis.

The rightmost three columns provide a set of totals for each row, summarising:

- » Hourly total – the total number of events registered for the selected subject phone(s) in each hour across the whole analysed period.
- » Hourly average – the average number of events per hour, averaged across the whole analysis period.
- » Hourly percentage – the percentage of overall events that took place during each hour.

Summary Pane

Summary					
Cell Identifier		Cell ID	Inactivity Hours		
			4		
Index	Cell Identifier	First	Last	Total	
→ 1	234-10-12049-33417	8	11	19	
2	234-30-01153-60262	3	1	4	
3	234-10-04017-55416	0	1	1	
4	234-10-12049-18036	1	0	1	

The Summary pane is designed to give a simple summary of the information provided in the 'Activity' grid. The Summary grid displays a simple list of the unique set of cells that were detected as being used as a First and/or Last cell in the main Activity grid.

Each individual detected first/last cell is listed, along with a count of the number of times each cell was detected as a first cell and a last cell, along with an overall total of number of times the cell was detected as either. The list initially sorted by the 'total' column.

The summary can make it easier to understand the area (or areas) in which a subject phone is most likely to be used at the start and at the end of each period of activity, which may in turn provide an insight into the where the user of the phone might have been living or staying during the analysed period.

Note: This information is also shown in the 'General Investigation' Dashboard.

17.12.3 Filters & Controls

The data to be analysed is selected from the right sidebar 'Source Data' menu in the normal way and is sent into the query when the 'Apply' button is clicked. Any filters or options applied within the query take effect immediately, there is no separate 'run' button and the 'Apply' button only needs to be clicked if you change the set of selected files or sidebar filters.

Both Activity and Summary panes have a set of filter and control options:

Activity Pane

Cell Identifier		Cell ID	Inactivity Hours		☒ Hide Days With No Activity
		Cell ID			
Hour	SiteName		01/09/2021	02/09/2021	03/
04:00	Postcode				
05:00	Count				

The 'Cell Identifier' control allows you to select the information shown in the 'first cell' (green) and 'last cell' (red) grid cells. It defaults to showing the CGI cell ID of each first or last cell but can also be set to display the first/last sitename or site postcode and there is also an option to display an hourly event count instead of first/last cell details.

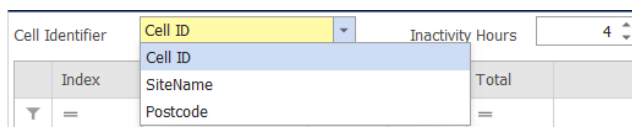
The length of a qualifying 'period of inactivity' can be set using the 'Inactivity Hours' spin box (1-24 hours). This setting defaults to 4 hours, meaning that a 'period of contiguous activity' can still be regarded as being 'contiguous' (i.e. continuous) even if there are gaps in activity of up to 4 hours. The value of this filter can be changed depending on the perceived lifestyle of the subject. When analysing a subject who follows a fixed routine and has a regular wake/sleep cycle, it might be useful to set a longer inactivity period or 6 or even 8 hours, to ensure that you capture the real first and last cells for that subject. Conversely, for subjects who lead chaotic lifestyles, who maybe snatch short bursts of

sleep at irregular intervals, shorter inactivity periods might be needed to narrow down the set of cells that provide coverage in the area where they were staying during the period being analysed. The 'Inactivity Hours' values in the Activity and Summary panels are linked, changing the value in one spin box automatically changes the value in the other one.

The 'Hide days with no activity' checkbox can be used to, as the filter name suggests, hide columns that represent days on which there was no activity for the selected subject phone(s). It is recommended to use this setting for datasets that cover a long period of time and where there are frequent long periods of inactivity.

The Activity pane supports a standard Analytics right-click menu, which operates as outlined in the [Grids and Controls](#) section.

Summary Pane



The Summary Pane controls allow you to set the type of information that is displayed in the 'cell identifier' column – with options of cell ID (CGI), sitename and site postcode. There is also an opportunity to set the qualifying value for the 'inactive hours' filter separately to the filter used by the main grid.

The Summary pane supports a standard Analytics right-click menu, which operates as outlined in the [Grids and Controls](#) section.

17.12.4 Understanding the results

The 'First Cell Last Cell' query is designed to help narrow down or confirm that area in which the user of a subject phone was staying by highlighting the cell used by the phone last thing at night and first thing in the morning (or at whatever other time intervals the subject sleeps).

The Activity pane provides a graphical overview of the subject phone's daily activities over the analysed period and can be used to help spot repeating patterns of usage. The activity chart can help to show if the subject has a fixed routine and if they sleep regularly. It can also be used to highlight subjects who have chaotic lifestyles.

Hour	1	30/08/2021	31/08/2021	01/09/2021	02/09/2021	03/09/2021	04/09/2021	05/09/2021
00:00		1	234-30-01153-60235	2	234-30-01153-60262		234-30-01153-60262	
01:00		0		1				
02:00		234-30-01153-60263		234-30-01153-60262				
03:00								
04:00								
05:00								
06:00				234-30-01153-14450				
07:00			234-30-01153-60262					234-30-01153-14450
08:00			0			234-30-01153-14450		
09:00		234-30-01153-60262	2		234-30-01153-14450	0	234-30-01153-14450	
10:00	153-60262	7	11	234-30-01153-60262	2	15	20	
11:00		10	3	8	5	3	8	234-30-01153-14431
12:00		1	2	5	0	5	12	22
13:00		0	0	8	10	0	9	8
14:00		14	8	2	13	10	20	22

The subject in the above example seems to lead a relatively conventional lifestyle (based on the underlying assumption that periods of inactivity equate to periods of sleep),

where they regularly wake up mid-morning and go to bed in the early hours of the following day.

Index	Cell Identifier	First	Last	Total	
=	=	=	=	=	
+	1 234-30-01153-60262	2	2	6	
+	2 234-30-01153-1	New Drill Down			
+	3 234-30-01153-6	Send cell(s) and call(s) to map (with context)			
+	4 234-30-01153-60235	0	1	1	
+	5 234-30-03609-61156	0	1	1	

The Summary pane offers the opportunity to determine the cells the subject phone uses most often for first/last events. If the assumptions stated at the start of this section are valid for the selected subject (e.g. that periods of inactivity equate to periods of sleep and that the subject generally sleeps at the same location most days), then the top one or two results in the Summary list should relate to cells that provide serving coverage at the subject's home address. The right-click 'send to map' function can be used to provide a visual indication of the area a subject may have been staying in.

Why, When, Who



This function is necessary to summarise imported source data files into a table showing the cells used for the first and last calls for a specific day or period of activity to develop usage/location/lifestyle patterns for a nominal.



This function is undertaken as required.



This function is typically carried out by the following users:

» CSAS User.

Stepped Procedure

To launch the First Cell Last Cell query:

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters. Due to the fact that long-lasting GPRS session records may obscure some inactivity periods, you may wish to exclude GPRS/mobile Internet events using the Filters > Event Types option.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query.
4. The results chart will update to show the data for the selected source data.
5. If necessary, you can change the inactivity period value for both the Activity and Summary panels. There is no need to click 'Apply' again after making changes to the query controls or filters, the results will update automatically.
6. You can change the value displayed in the 'hour' grids and in the Summary List for first and last cells using the Cell Identifier dropdown menus.
7. You can hide days with no activity by checking the checkbox.

8. Review the Activity and Summary panes to gain an understanding of the lifestyle and calling patterns displayed for the selected subject phone(s) and to see a list of cells that were used for first and last connections.
9. Sending the top few Summary List rows to a map may help to identify the general area in which the subject was staying during the analysed period.
10. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
11. If you wish to view any of the results in a map, select the required row(s), right-click and select Send to Map.
12. If you filtered GPRS/data events from the dataset when launching this query, remember to restore them to the dataset, by cancelling the Event Type filter, before continuing with your analysis.

17.13 Using the IMEI Summary query

CDR data generally captures details of the subscriber and mobile number (IMSI and MSISDN) for the subject account and often also provide details of the handset (IMEI) used for each contact. It is possible to swap physical SIM cards between handsets, so a dataset in which this kind of SIM swapping has taken place will link different IMEIs to the IMSI/MSISDN over time.

Analysis of when SIM swaps have taken place and which handsets the SIM has been used with can be investigatively significant. For example, the fact that a suspect swaps their SIM out of an expensive smartphone into a cheap feature phone just before each burglary that suspect is accused of could be significant. Or the fact that the same handset IMEI appears in the data for a group of phone numbers alleged to belong to members of the same gang, could be used as proof of association between those individuals.

This IMEI Summary query provides a set of results grids that highlight and summarised the set of IMEIs associated with the selected subject data files and provides event count totals and association periods for each of them, with the objective of indicating whether SIM swapping and/or handset sharing has taken place.

17.13.1 Supported Data Types

The IMEI Summary query can only be used with CDR data.

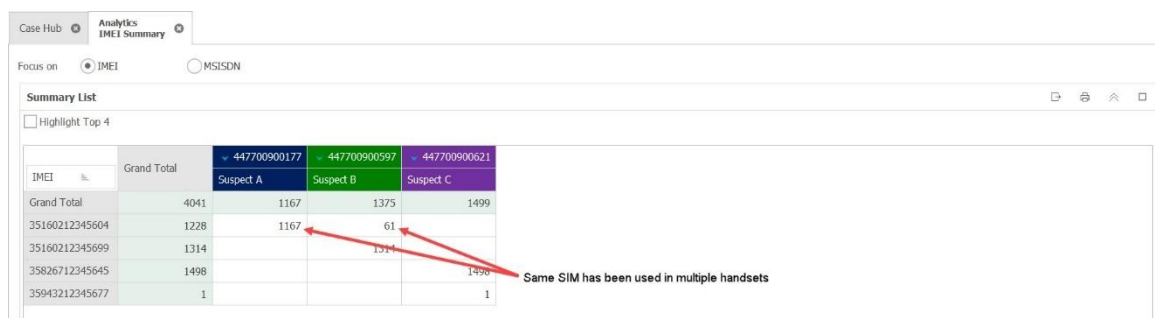
17.13.2 Layout

The IMEI Summary query supports three results grids:

- » Summary List – provides a pivot table listing the set of detected IMEIs against the set of associated subject phone numbers.
- » Chronological List – if multiple IMEIs are detected and SIM swapping has taken place, this list shows the time span that each IMEI and MSISDN were paired for, plus a count of events that took place during each period.
- » Unique List – provides a simple list of the unique IMEIs found in the dataset.

Summary List

The Summary List results grid shows detected IMEIs in rows and associated subject phone numbers in column. The count shown at the intersection of a row (IMEI) and column (MSISDN) indicates the number of events that were recorded in the selected dataset when that IMEI was paired with that phone number.



IMEI	Grand Total	447700900177 Suspect A	447700900597 Suspect B	447700900621 Suspect C
Grand Total	4041	1167	1375	1499
35160212345604	1228	1167	61	
35160212345699	1314		1314	
35826712345645	1498			1498
35943212345677	1			1

Same SIM has been used in multiple handsets

Chronological List

Chronological List						
	IMEI	Nominal	MSISDN	Start Date	End Date	Event Co...
+	35160212345604	Unknown 1	447700900177	29/08/2012 10:04:04	29/08/2012 16:00:04	52
+	35160212345699	Unknown 1	447700900177	29/08/2012 15:05:23	29/08/2012 21:02:10	81
→	35412412345691	Unknown 1	447700900177	29/08/2012 21:02:09	30/08/2012 10:24:37	37

The 'Chronological List' results grid displays a different view of the same data; in this report the results are grouped to show the time periods covered by each IMEI and MSISDN pairing plus the event count. In the example above, the subject phone number (ending 177) has been used with three different IMEIs during the period under analysis.

If the same IMEI has been used multiple times with a phone number and/or if the same phone number has been used with multiple handsets, each separate period of association between the subject number and an IMEI will have its own row listing in the results.

The columns in the results grid provide details of the set of IMEIs, the attribution and phone number for each associated subject identifier, the start and end dates of each period of association, the event count for each period of association.

Double-clicking on a row launches the drill down view for that data.

The Chronological List often works best if data for only one subject phone at a time is selected, results for multiple subject phones, where each period of association between each pair of IMEI and MSISDN is listed separately, can be confusing when multiple subject phones are viewed together.

Unique List

Unique List						
	IMEI	Nominal	MSISDN	First used	Last used	Event...
→	358267...	Suspect C	4477009006...	14/08/2012...	11/09/2012...	1498
+	351602...	Suspect B	4477009005...	14/08/2012...	02/09/2012...	1314
+	351602...	Suspect A	4477009001...	29/08/2012...	05/09/2012...	1167
+	351602...	Suspect B	4477009005...	29/08/2012...	30/08/2012...	61
+	359432...	Suspect C	4477009006...	29/08/2012...	29/08/2012...	1

The 'Unique List' grid displays a list of all unique IMEIs that were found in the data and shows the overall period within which the IMEI was in use with each target number, even if that overall period is non-contiguous, and the overall number of events that were captured for each pairing.

17.13.3 Filters & Controls

The data to be analysed is selected from the right sidebar 'Source Data' menu in the normal way and is sent into the query when the 'Apply' button is clicked. Any filters or options applied within the query take effect immediately, there is no separate 'run' button and the 'Apply' button only needs to be clicked if you change the set of selected files or sidebar filters.

The Summary List results can have their focus switched between IMEI focus and MSISDN focus using the radio buttons at the top of the results pane. When switching between IMEI and MSISDN the configuration of the grid in the panel changes.

In IMEI focus mode, the grid is focusing on the set of selected target numbers (shown along the top) that each unique IMEI (shown along the side) has been paired with in the current dataset – it answers the question ‘which phone numbers have each IMEI been used with?’.

IMEI	Grand Total	447700900177	447700900597
		Unknown 1	Unknown 2
Grand Total	262	170	92
35160212345604	113	52	61
35160212345699	112	81	31
35412412345691	37	37	

IMEI focus

MSISDN	Nominal	Grand Total	35160212345604	35160212345699	35412412345691
Grand Total		350	113	112	37
447700900177	Unknown 1	170	52	81	37
447700900597	Unknown 2	92	61	31	

MSISDN focus

Whereas, in MSISDN focus mode, the grid is focusing on the set of IMEIs (shown along the top) that each selected target number (shown along the side) has been paired with in the current dataset – it answers the question ‘which IMEIs have each target phone number been used with?’:

The Summary List also has a control option to ‘Highlight top 4’ count values. This is useful in very busy results grids, where there are lots of IMEIs and subject phone numbers and evidence of lots of SIM swapping or phone swapping. When enabled, the top 4 highest event counts in the grid are highlighted (highest count is red, next highest is orange, etc) to ensure that the highest values are immediately visible.

The main results grid supports the usual Analytics right-click menu, with options to drilldown and ‘send to map’. See the Analytics [Grids and Controls](#) section for more details. Double-clicking on a row or grid cell also launches the drill down view for that data.

17.13.4 Understanding the Results

Single phone number analysis

If data for a single subject phone number is analysed, possibly looking for evidence of SIM swapping, the results could be interpreted as follows:

The Summary List provides an overview of the set of IMEIs with which the subject number was associated.

IMEI	447700900177
	Unknown 1
Grand Total	170
35160212345604	52
35160212345699	81
35412412345691	37

In this example, there are clearly multiple IMEIs listed, each with a significant event count, which can be seen as evidence of SIM swapping.

Evidence of SIM swapping isn’t necessarily evidence of criminal intent, of course, so it may be useful to understand when each instance of SIM swapping took, to see if those times match up to the times of significant events in a case.

The Chronological List provides details of when any instances of SIM swapping took place. The example results grid below, for a subject phone number ending 177, shows the following information:

Chronological List						
	IMEI	Nominal	MSISDN	Start Date	End Date	Event Co...
+	35160212345604	Unknown 1	447700900177	29/08/2012 10:04:04	29/08/2012 16:00:04	52
+	35160212345699	Unknown 1	447700900177	29/08/2012 15:05:23	29/08/2012 21:02:10	81
+	35412412345691	Unknown 1	447700900177	29/08/2012 21:02:09	30/08/2012 10:24:37	37

This can be interpreted as follows:

- » 177 was used with IMEI ending 604 for 52 events between 10:04:04 (start of first paired event) and 16:00:04 (end of last paired event).
- » 177 was used with IMEI ending 699 between 15:05:23 and 21:02:10.
- » 177 was used with IMEI ending 691 between 21:02:09 and 10:24:37 the next day.
- » SIM swapping has clearly taken place, with the SIM linked to the 177-phone number being swapped in and out of three different handsets over a 24-hour period.

In very complex cases, where there are multiple and repeated instances of SIM swapping, it can be useful to compile a simple list of each unique IMEI that has been paired with a subject phone, rather than focusing in detail on each individual time period during which they were associated. The Unique List provides this simplified set of information.

Complex Multiple phone number analysis

A more complex analysis might include data for multiple phones – often, this form of analysis is used to see if there is evidence of the SIM/phone numbers associated with a group of individuals have been used in any common handsets. Even if those individuals deny knowing each other, evidence that they have regular shared the same handsets over a period of time could be used to refute those denials.

In this example, the users of the 177 and 597 phones are suspected of being associated with each other for criminal purposes but have so far denied knowing each other.

IMEI	Grand Total	447700900177	447700900597
		Unknown 1	Unknown 2
Grand Total	262	170	92
35160212345604	113	52	61
35160212345699	112	81	31
35412412345691	37	37	

The IMEI Summary List for the two phones clearly shows that have both used the same two handsets (with IMEIs ending 604 and 699).

The suspects may claim that this is coincidental, that maybe one of them bought an old handset on eBay that just happened to have been used by the other suspect.

The Chronological List can be used to show that the usage of the handsets by the two phone numbers overlapped and interleaved across a period of time, with a pattern of usage that doesn't fit with the content they've put forward.

Chronological List						
	IMEI	Nominal	MSISDN	Start Date	End Date	Event Count
Y	IMEI	Nominal	MSISDN	=	=	=
	+ 35160212345604	Unknown 1	447700900177	29/08/2012 10:04:04	29/08/2012 16:00:04	52
	+ 35160212345699	Unknown 2	447700900597	29/08/2012 10:19:03	29/08/2012 15:01:10	31
	+ 35160212345604	Unknown 2	447700900597	29/08/2012 15:01:06	30/08/2012 10:37:52	61
→	+ 35160212345699	Unknown 1	447700900177	29/08/2012 15:05:23	29/08/2012 21:02:10	81
	+ 35412412345691	Unknown 1	447700900177	29/08/2012 21:02:09	30/08/2012 10:24:37	37

The Unique list can be used to provide a simple list of the three IMEIs found in the case data and their overall set of associations with the two subject numbers.

	IMEI	Nominal	MSISDN	First used	Last used	Event Count
Y	IMEI	Nominal	MSISDN	=	=	=
	+ 35160212345604	Unknown 1	447700900177	29/08/2012 10:04:04	29/08/2012 16:00:04	52
→	+ 35160212345699	Unknown 2	447700900597	29/08/2012 10:19:03	29/08/2012 15:01:10	31
	+ 35160212345604	Unknown 2	447700900597	29/08/2012 15:01:06	30/08/2012 10:37:52	61
	+ 35160212345699	Unknown 1	447700900177	29/08/2012 15:05:23	29/08/2012 21:02:10	81
	+ 35412412345691	Unknown 1	447700900177	29/08/2012 21:02:09	30/08/2012 10:24:37	37

Why, When, Who



This function is necessary to analyse a dataset to see if SIM swapping or handset sharing has taken place.



This function is undertaken as required.



This function is typically carried out by the following users:

» CSAS User.

Stepped Procedure

To run the IMEI Summary query:

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query.
4. The results grids will update to show the data for the selected source data.
5. You can switch the Summary List view from 'IMEI focus' to 'MSISDN focus' if required and also active the 'highlight top 4' feature in complex datasets.
6. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
7. If you wish to view any of the results in a map, select the required row(s), right-click and select Send to Map.

17.14 Using the Inactivity Chart query

For some forms of digital forensics analysis, it can be as important to understand when a phone or other device is not being used as it is to understand when it is being used. As criminals become more forensically aware, for example, there is a growing understanding that they should leave their phones at home or switch them off when they plan to undertake activities at locations, they may not wish the authorities to be able to track them to. This type of obfuscation leaves periods of inactivity in a subject's data records. Analysis of those records can indicate whether any periods of inactivity coincide with significant events in a case and whether such inactivity is usual or unusual in the context of the subject's normal levels of activity.

The Inactivity Chart query is designed to highlight periods of inactivity for a phone or vehicle, with the option to specify the qualifying minimum period of inactivity. The results grid then adds context by displaying details of the last event captured before the period of inactivity started and of the first event captured after each period of inactivity ended.

If you wish to concentrate on voice & SMS activity and avoid issues caused by long-lasting GPRS sessions, you can elect to remove GPRS events from the analysis using the right sidebar 'Event Type' filter. If you do remove GPRS events from the dataset, please remember to disable the event type filter again before moving on to undertake more general analysis.

The analysis can be performed using data for just one subject, if you're interested in whether that one individual has periods of inactivity, or it can be performed on the data for a group of subjects, if you're interested in whether there were periods of time where some or all of the group went inactive at the same time.

17.14.1 Supported Data Types

The Inactivity Chart query can currently be only used with CDR and ANPR data, other data types could possibly be added to the set if required.

17.14.2 Layout

The Inactivity Chart results grid is laid out in three sections:

- » Left side – shows details of the last event before a period of inactivity.
- » Centre section – shows the length of each qualifying period of inactivity.
- » Right side – shows details of the first event after a period of inactivity.

The left (before) and right (after) sections display basic information about the events:

Last event before inactivity							
EventType	Calling	CallingAttribution	Called	CalledAttribution	EventStart	EventEnd	StartPostcode

First event after inactivity							
Event Start	Event End	Calling	Calling Attribution	Called	Called Attribution	Start Postcode	Event Type

For CDR data, the 'Calling' and 'Calling Attribution' column columns display details of the calling (A) phone and the 'Called' and 'Called Attribution' columns details the called (B) phone; for ANPR data, the 'Calling' columns contain details about the vehicle captured in each event and the 'Called' columns are left blank.

InactivityDuration
00:56:04
00:31:09
00:24:16
00:32:01

The Duration value shows the time difference between the end of the 'before' event and the start of the 'after' event. The Duration column is usually formatted to show Hours:Minutes:Seconds, but if you select 'Days' as the inactivity period, then the format is expanded to show 'Days.Hours:Minutes:Seconds'.

17.14.3 Filters & Controls

The data to be analysed is selected from the right sidebar 'Source Data' menu in the normal way and is sent into the query when the 'Apply' button is clicked. Unlike most other queries, the Inactivity Chart query has an additional 'Apply' button in the query window. After selecting the source data files to view and clicking the right sidebar 'Apply' button, you can set the required value for the qualifying inactivity period and hit the specific 'Apply' button to run the query.

Inactivity Trigger Time

20

☐ Days
 ☐ Hours
 ☒ Minutes

Reset

Apply

You can adjust the inactivity duration by selecting from the Days, Hours or Minutes check boxes and by adjusting the 'Inactivity Trigger Time' then clicking on the query-specific **Apply** button.

You can exclude certain types of event (for example, GPRS/mobile data events) in the 'Filters' sidebar, using the 'Event Types' filter.

You can clear the grid by clicking on the **Reset** button.

The results grid supports the standard Analytics right click menu options of 'drilldown' and 'send to map', as outlined in the [Grids and Controls](#) section.

17.14.4 Understand the results

The Inactivity Chart query is designed to quickly highlight periods of time when the selected subjects were inactive for more than a minimum duration and is especially useful in investigating suspects who are forensically aware enough to switch their phones off when they are doing some illegal.

The results grid shows details of the events that bookend each qualifying period of inactivity. For example, if you select an 'Inactivity Trigger Time' of 25, tick the 'Minutes' checkbox and click on the query-specific **Apply** button, each row in the results grid will show details of the last event before and the first event after each period where the selected data has an inactive gap in records of 25 minutes or more:

Inactivity Chart											
Inactivity Trigger Time: 25 ☐ Days ☐ Hours ☒ Minutes Reset Apply											
Last event before inactivity											
Index	Event Type	Calling	Calling Attribution	Called	Called Attribution	Event Start	Event End	Start Postcode	Inactivity Duration	Event Start	Event End
1	Incoming Voice	07700900...		07700900...	Suspect C	14/08/2012 10:08	14/08/2012 10:08		00:25:54	14/08/2012 10:34	14/08/2012 10:34
2	Outgoing Voice	07700900...	Suspect C	07700900...		14/08/2012 16:37	14/08/2012 16:38		00:44:55	14/08/2012 17:22	14/08/2012 17:22
3	Incoming Voice	07700900...		07700900...	Suspect C	14/08/2012 18:57	14/08/2012 18:58		01:26:11	14/08/2012 20:24	14/08/2012 20:24
4	Outgoing Text	07700900...	Suspect B	07700900...		14/08/2012 22:20	14/08/2012 22:20	E2 6NU	01:23:46	14/08/2012 23:44	14/08/2012 23:44
5	Outgoing Text	07700900...	Suspect B	44077009...		14/08/2012 23:46	14/08/2012 23:46	E2 6NU	04:09:03	15/08/2012 03:56	15/08/2012 03:56
6	Incoming Divert	07700900...		07700900...	Suspect C	15/08/2012 09:37	15/08/2012 09:37		00:51:37	15/08/2012 10:29	15/08/2012 10:29
7	Incoming Voice	07700900...	Suspect A	07700900...	Suspect B	15/08/2012 10:33	15/08/2012 10:36		00:47:29	15/08/2012 11:23	15/08/2012 11:23
8	Outgoing Voice	07700900...	Suspect C	07700900...		15/08/2012 13:06	15/08/2012 13:07		00:27:13	15/08/2012 13:34	15/08/2012 13:34

It might be that an inactivity duration of 25 minutes isn't particularly uncommon or significant for the subject(s) being investigated, so the 'trigger period' duration could be

varied to see if there are inactive periods that are either of unusually long duration or that coincide with the date/time of any of the significant events that are under investigation.

As a further example, imagine that the data for a burglary suspect shows that their phone is usually used almost continuously through the day and evening across the analysed days, even having excluded GPRS/data from the analysis using the Event Type filter. However, the Inactivity Chart indicates that there were two qualifying periods of inactivity of over 2 hours each that coincided with two of the burglaries that were under investigation. This analysis doesn't provide proof, on its own, that the suspect was involved in those burglaries, but it does highlight that the periods of inactivity were out of character and the coincident timing of the inactivity and the burglaries adds weight to the contention that the suspect may have been involved.

Why, When, Who

	This function is necessary to develop detect significant periods of inactivity in analysed data.
	This function is undertaken as required.
	This function is typically carried out by the following users: » CSAS User.

Stepped Procedure

To launch the Inactivity Chart query:

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters. Due to the fact that long-lasting GPRS session records may confuse the view of actual user-initiated activity levels, you may wish to exclude GPRS/mobile Internet events using the Filters > Event Types option.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query.
4. If necessary, you can change the inactivity trigger period value to something other than 20 minutes.
5. Click the query specific 'Apply' button to run the analysis. You'll only need to click the right sidebar 'Apply' button again after making changes to the sidebar controls or filters.
6. The results chart will update to show the data for the selected source data.
7. Review the results grid to gain an understanding of any qualifying periods of inactivity across the analysed time span for the selected subject identifiers.
8. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
9. If you wish to view any of the results in a map, select the required row(s), right-

click and select Send to Map.

10. If you filtered GPRS/data events from the dataset when launching this query, remember to restore them to the dataset, by cancelling the Event Type filter, before continuing with your analysis.

17.15 Using the Pivot Builder query

There are multiple forms of analysis covering many different formats of source data available to digital forensics investigations, but many of these types of data can be adequately analysed using a simple pivot chart.

The Pivot Builder query provides a set of prebuilt pivot templates that are dedicated to particular data types and/or forms of analysis, which you can optionally customise using the various fields and tab filter drop-down menus.

Pivot Tables

A pivot table offers a form of analysis that contrasts two sets of criteria and performs an action for each interaction.

The selected criteria are displayed in row and columns – one set of criteria make up the rows and the other set make up the columns.

At each intersection of row and column, an action will be performed on the data from that row and that column. Typical actions include showing a count of the instances where the row contents are found in each instance of the column data.

A simple example of a pivot table could be like this:

Day	Date	Employee	Count of Employee	Column 1					
Sunday	01/12/2023	Dave	Row Labels	Dave	Phil	Rosie	Sharon	(blank)	Grand Total
Monday	02/12/2023	Phil	Monday		2				2
Tuesday	03/12/2023	Rosie	Tuesday	1		1			2
Wednesday	04/12/2023	Phil	Wednesday		1		1		2
Thursday	05/12/2023	Dave	Thursday	1		1			2
Friday	06/12/2023	Dave	Friday	1					1
Saturday	07/12/2023	Sharon	Saturday	1	1		1		3
Sunday	08/12/2023	Rosie	Sunday	1		1			2
Monday	09/12/2023	Phil	(blank)						
Tuesday	10/12/2023	Dave	Grand Total	5	4	3	2		14
Wednesday	11/12/2023	Sharon							
Thursday	12/12/2023	Rosie							
Friday	13/12/2023	Dave							
Saturday	14/12/2023	Phil							

The source data shows which employee performed a certain task on each of the days in a two-week period. The pivot table has columns for each 'employee' and 'day of week' for each row.

The intersection of each row and column shows the count of the number of times each employee performed the task on each day of the week.

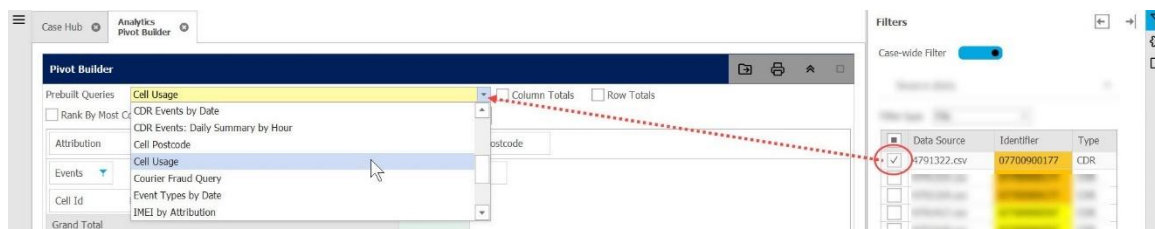
From this we can see that Dave performed the task most often and Sharon the least.

The CSAS Pivot Builder offers a set of prebuilt pivots, based on the selected source files,

where the contents of the rows and columns have been preselected, but where additional criteria could be added to expand or add more depth to the query.

Prebuilt Query Options

You start the query by selecting the Source Data you want to include in your report, and click on the button:



You can then choose the type of prebuilt query you want to build:

Type of Prebuilt Query	Function of Prebuilt Query
ANPR Cameras by Date	A pivot table of dates vs ANPR cameras showing the count of ANPR captures for each camera on each date.
ANPR Events by Date	A pivot table of dates vs vehicle registrations showing the number of ANPR captures for each registration on each date.
ANPR: Day of Week	A pivot table of ANPR cameras vs day of the week showing the count of ANPR captures per camera per day. This may help to identify the camera that a given vehicle might be expected to close to on a given day of the week.
ANPR: Postcode	A pivot table of ANPR camera postcode vs vehicle registrations showing the count of ANPR captures per postcode. This query has additional controls that allow the size of the area over which the count is made to be altered by adding/ removing parts of the postcode to aggregate areas together.
ANPR: Time of Day	A pivot table of ANPR Cameras vs hours of the day showing a count of the ANPR captures per camera per hour of the day. This may help to identify the camera that a given vehicle might be expected to close to on a given hour of the day.
ANPR: Vehicles	A pivot table of ANPR cameras vs vehicle registrations showing a count of the times each vehicle has been captured by each camera. This may help to identify the camera that a given vehicle is captured by most often.
Call Summary by Attribution	A pivot table of case subject attributions vs other numbers, allowing the most frequent contacts for each subject to be determined.
Call Summary	A pivot table of case subject phone numbers vs other numbers, allowing the most frequent contacts for each subject to be determined.
Calls Between	A pivot table of case subject numbers vs each other, allowing the frequency of contacts between subjects to be determined. To

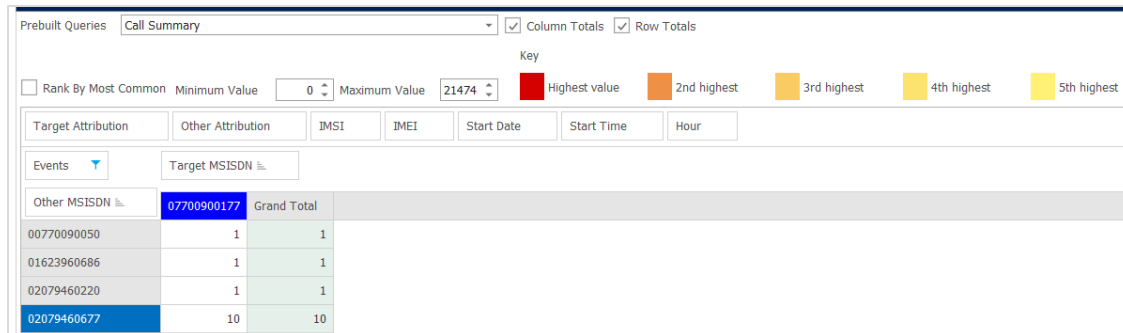
	avoid double-counting target-target events, this query only counts outgoing voice/call records.
CDR Events by Date	A pivot table of dates vs subject numbers, showing a count of the number of events recorded for each subject number per date.
CDR Events: Daily Summary by Hour	A pivot table of dates vs hours of the day showing a count of the number of events recorded for the selected set of files per hour of each date.
Cell Postcode	A pivot table of cell postcode vs subject phone showing a count of the number of times an identifier used a cell in each postcode. This query has additional controls that allow the size of the area over which the count is made to be altered by adding / removing parts of the postcode to aggregate areas together.
Cell Usage	A pivot table of cell ID / cell site vs subject identifier showing a count of the number of times each identifier used each cell.
Courier Fraud Query	A pivot table of subject identifiers vs other numbers, showing the total duration of calls made between each subject identifier and the other numbers they contacted. This query is designed to work with call data from phones suspected of being involved in courier fraud, where victims are persuaded to hand money over to bogus police officers or bank officials. In theory, other numbers that the suspects speak to for the longest are likely to have been drawn further through the fraud process, so this query can provide evidence of the fraudulent contact and may be helpful in identifying victims who haven't previously come forward.
IMEI by Attribution	A pivot table of case IMEIs vs subject attributions showing a count of the number of events where each attribution used the device associated with each IMEI.
IMEI by IMSI	A pivot table of case IMEIs vs case IMSIs showing a count of the number of events where each IMSI used the devices associated with each IMEI.
IMSI by MSISDN	A pivot table of case IMSIs vs subject identifiers showing a count of the number of events where each subject identifier used the SIM account associated with each IMSI.
IMSI by Attribution	A pivot table of case IMSIs vs subject attribution showing a count of the number of events where each subject attribution was associated with each IMSI.
IMSI vs MSISDN	A pivot table of case IMSIs vs subject identifiers showing a count of the number of events where each subject identifier was associated with each IMSI.
Locations by Date	A pivot table of case location vs dates showing a count of the case events recorded at each location on each date.

17.15.1 Supported Data Types

The Pivot Builder query can be used with any imported data or file type, including CDR, ANPR, handset download, telematics, tracker and others, although particular queries are more suited to some data types than others and some queries may not produce results for some combinations of source data.

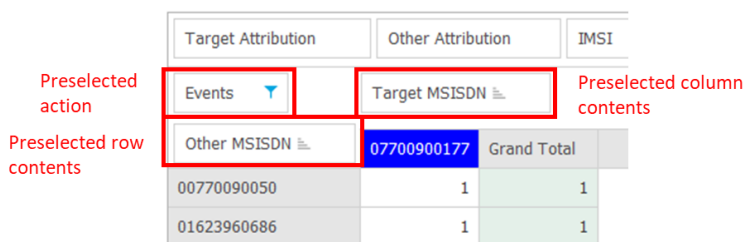
17.15.2 Layout

The pivot queries all share the same fundamental layout but might each have differences suited to the type of data or form of analysis provided. Generic features include:



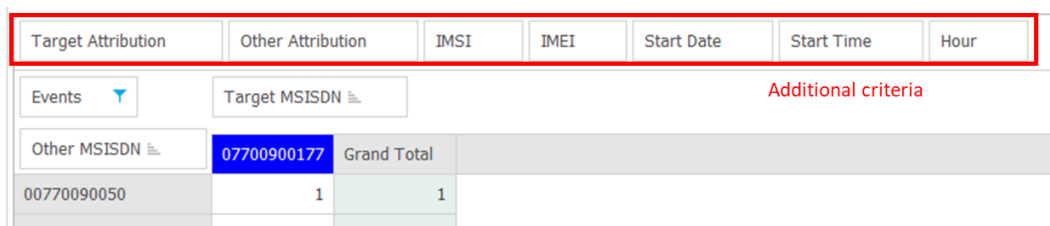
- » The 'Prebuilt Queries' dropdown menu lists the available set of pivot queries, select the required query type from the list.
- » There are several basic filter and control options, which are described below.
- » The result pivot grid displays the results for the required query.
- » Each Prebuilt Query has a default results grid, with a selected set of column and row criteria and a selected action.

In this example, the pivot is contrasting 'Target MSISDN' (in columns) against 'Other MSISDN' (in rows) with an action of 'count of events'.



Resulting in a pivot table that counts the number of contacts between each specific pair of phone numbers – e.g. the 177 phone was in contact with the 050 phone 1 time, with the 686 phone 1 time, and so on.

Most CSAS pivot queries have a set of additional criteria that can be dragged into the pivot by adding them to the rows or columns or by replacing the current 'action' criteria.



For example, the 'Target MSISDN vs Other MSISDN' pivot could be expanded by dragging the 'Start Date' criteria into the column definition, which has the effect of breaking the count for each Target MSISDN up into separate columns per date. Like this:

Target Attribution

Other Attribution

IMSI

IMEI

Start Time

Hour

Events

Target MSISDN

Start Date

Criterion dragged to 'columns' definition

	07700900177								Grand Total	
Other MSISDN	29/08/2021	30/08/2021	31/08/2021	01/09/2021	02/09/2021	03/09/2021	04/09/2021	05/09/2021		
00770090050						1			1	
01623960686							1		1	

Resulting in a grid that now has a set of sub-columns for the Target MSISDN, one for each date on which there were call records. This turns a simple aggregated call count query into a more complex call count by date' query.

The order in which the criteria are placed controls the order in which the criteria are applied. In the example above, the 'Target MSISDN' criterion is applied first, creating a separate section for each selected subject number, the 'Start Date' criterion is applied next, creating sub-sections for each date.

Target Attribution	Other Attribution	IMSI	IMEI	Start Time	Hour					
Events 	Start Date 	Target MSISDN 								
	▼ 29/08/2021			▼ 30/08/2021						
Other MSISDN 	07700900177	07700900597	07700900621	07700900177	07700900597	07700900621				
0										
00770090006										

If more than one Target MSISDN was selected, there would be a separate set of date columns for each additional subject number. If the 'Start Date' criterion had been placed first, there would be a separate section for each date, each of which had its own set of sub-sections for each subject number.

Any of the available additional criteria can be dragged in to and out of the pivot builder, as can any default criteria that were included in the query originally. This allows a wide degree of variation to be applied to the prebuilt query selections.

17.15.3 Filters & Controls

There are a generic set of filters and controls used by all pivot builder queries and some queries have their own specific additional controls.

Prebuilt Queries: ANPR Cameras by Date ☒ Column Totals ☒ Row Totals

☐ Rank By Most Common Minimum Value: Maximum Value: ANPR Key

☒ Highest value ☐ 2nd highest ☐ 3rd highest ☐ 4th highest ☐ 5th highest

The generic controls are as follows:

- » 'Column Totals' - this checkbox adds a 'Grand Total' column to the pivot builder results grid.
- » 'Row Totals' - this checkbox adds a 'Grand Total' row at the bottom of the pivot table:
- » 'Rank by Most Common' - this checkbox filters the column so the most common used cell tower is at the top of the pivot table:
- » 'Minimum Value' / 'Maximum Value' - these fields allow you to set the minimum / maximum number of results shown in each column.
- » Most query results grids also include colour coding to highlight the top 5 values in each grid

Analytics Pivot Builder

Pivot Builder

Prebuilt Queries: ANPR Cameras by Date ☒ Column Totals ☐ Row Totals

☐ Rank By Most Common Minimum Value: Maximum Value: ANPR Key

☒ Highest value ☐ 2nd highest ☐ 3rd highest ☐ 4th highest ☐ 5th highest

Attribution	IMEI	Start Date	Start Time	Hour	Altitude	Postcode	Target MSISDN	Grand Total
234-10-04017-14719	LYPTON WELAND						07/00000177	30
234-10-04017-34517	LYPTON 3559_364						07/00000099	5
234-10-04017-35416	WOODFORD HIGH ROAD						07/00000021	3
234-10-04017-05243	WEST GREEN PARK						07/00000021	1
234-10-04017-11348	WOODBERRY						07/00000021	1
234-10-04017-20525	WEST GREEN PARK						07/00000021	1
234-10-04017-21348	WOODBERRY						07/00000021	1
							Grand Total	80

Analytics Pivot Builder

Pivot Builder

Prebuilt Queries: ANPR Cameras by Date ☐ Column Totals ☒ Row Totals

☐ Rank By Most Common Minimum Value: Maximum Value: ANPR Key

☒ Highest value ☐ 2nd highest ☐ 3rd highest ☐ 4th highest ☐ 5th highest

Attribution	IMEI	Start Date	Start Time	Hour	Altitude	Postcode	Target MSISDN	Grand Total
234-33-03605-61784							07/00000021	2
234-33-03605-61786							07/00000021	1
234-33-03605-61881	MARCON PLACE						07/00000021	2
234-33-03605-62285							07/00000021	1
234-33-03605-62360	41 STAMFORD HILL						07/00000021	1
234-33-03605-62413							07/00000021	1
234-33-03605-63387							07/00000021	1
							Grand Total	1181

Analytics Pivot Builder

Pivot Builder

Prebuilt Queries: ANPR Cameras by Date ☐ Column Totals ☐ Row Totals

☒ Rank By Most Common Minimum Value: Maximum Value: ANPR Key

☒ Highest value ☐ 2nd highest ☐ 3rd highest ☐ 4th highest ☐ 5th highest

Attribution	IMEI	Start Date	Start Time	Hour	Altitude	Postcode	Target MSISDN	Grand Total
234-10-12049-33417	SHACKLEWELL						07/00000021	1054
234-30-01153-60263	YATES HOUSE						07/00000021	249
234-30-01153-60262	YATES HOUSE						07/00000021	122
234-30-01153-14431	YATES HOUSE						07/00000021	44
234-30-01153-14431	YATES HOUSE						07/00000021	70

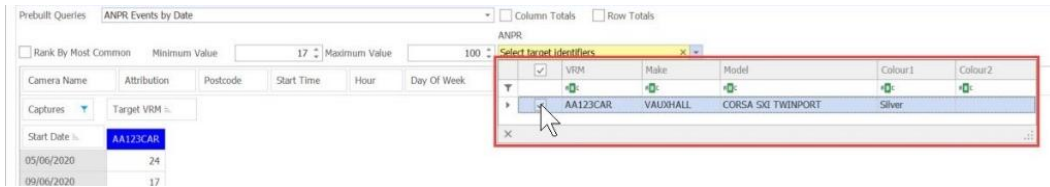
Minimum Value: Maximum Value:

Key

☒ Highest value ☐ 2nd highest ☐ 3rd highest ☐ 4th highest ☐ 5th highest

Some queries have additional specific filters or controls.

- » 'Select target identifiers' - some prebuilt queries such as 'ANPR...' include a drop-down menu from which you can select which Identifiers you want to include in the pivot table:



- » Postcode Matching - queries that deal with location data organised by postcode can be filtered to use all or just some of the postcode (this is a UK-specific feature). UK postcodes consist of 4 sections (Area, District, Sector, Unit, with unit being the smallest division).

Postcode Matching

☒ Area ☒ District ☒ Sector ☒ Unit

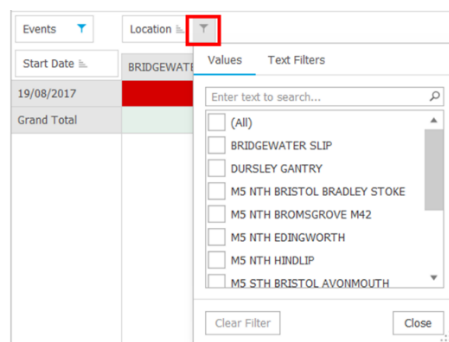
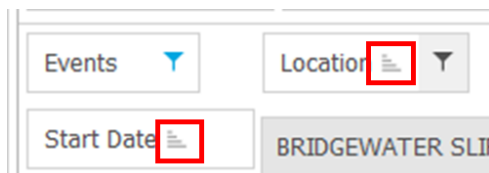
The Postcode Matching filter works from smallest upwards and instructs the query to aggregate smaller areas together. For example, with the 'unit' option selected, CSAS would see the two postcodes E2 2NU and E2 2FD as being different areas, but with the 'unit' option deselected it would regard them as aggregated into the same 'E2 2' area.

In Grid Filtering

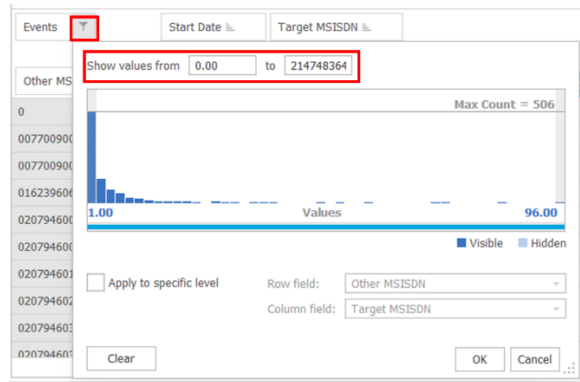
The boxes for each selected criterion offer sorting and filtering options of their own.

The ordering of the columns can be changed by clicking the 'sort' icon in the column criterion box and the order of the rows can be changed by clicking the icon in the row criterion box.

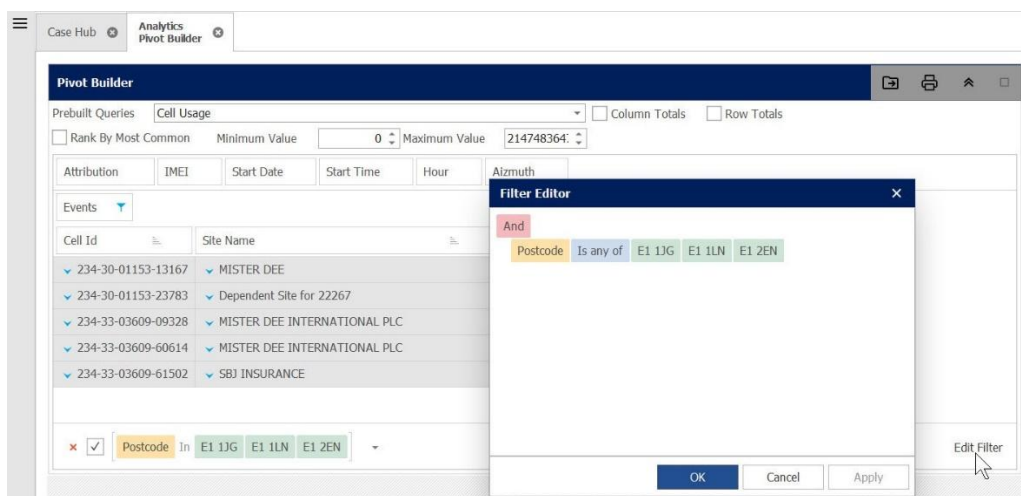
Rows and columns can be filtered to show only specific values using the 'filter' icons that appear when the criterion box is moused over.



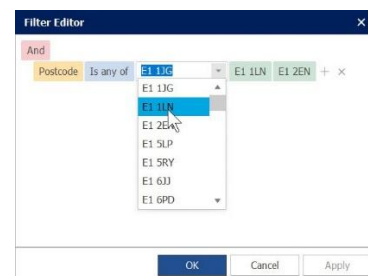
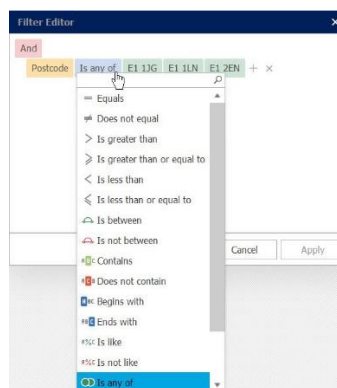
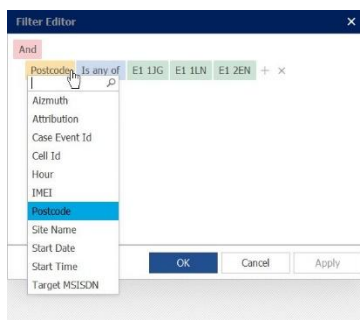
The 'action' box also supports a filtering option, allowing you to filter the results to only show results that fall within a specific range of values.



If any filters are applied, details of the filter will be shown at the bottom of the Pivot Builder panel. On the right side of the filter bar there is an 'Edit Filter' button which when clicked, opens the 'Filter Editor' pop-up window:



From the 'Filter Editor' pop-up window, you can edit the filter, changing the selected values or adding additional clauses as required.



Right-click menus

The results grid supports the standard Analytics right click menu options of 'drilldown' and 'send to map', as outlined in the [Grids and Controls](#) section.

17.15.4 Understanding the results

There are multiple pivot queries in the Pivot Builder feature, meaning that it's not possible to provide one description of how to understand the results. All pivot tables share a common set of features, however, so all of the CSAS pivot query examples can be interpreted in roughly the same way.

A pivot table contrasts a set of data in rows and against data in columns – the intersection between each row and column provides information about the correspondence between the value for the row and the value for the column. Most often a pivot table provides a count of the number of events shared by the pair of identifiers that intersect at each square in the results grid.

Why, When, Who

	This function is necessary to analyse case data using one of the methods supported by the Pivot Builder.
	This function is undertaken whenever you want to analyse data using one of the supported methods.
	This function is typically carried out by the following users:  CSAS User.

Stepped Procedure

Each pivot query is different, but the procedure to use any of them is similar – this example will use the Call Summary pivot option.

1. Select the required set of source data files for the subject identifier(s) you wish to analyse, apply any required right sidebar Filters.
2. Remember that right sidebar Settings apply to Analytics queries, meaning that duplicate matching, SMS concatenation and redaction will be applied if enabled.
3. Click 'Apply' to send the selected dataset to the query.
4. From the 'Pivot Builder' screen, go to 'Prebuilt Queries' and select from the drop-down menu the type of query you want to build.
5. To customise your pivot table, go to the row of additional criteria boxes above the pivot table and drag and drop any required additional criteria into the pivot table, remembering that the order in which the criteria are positioned affects the order in which they are applied.
6. In the pivot table, use the icons in the row, column and action criteria boxes to filter and sort the data as necessary.
7. If you wish to drilldown into any of the results rows, to view the raw data that sits behind the results, select the required row(s), right-click and select New Drilldown.
8. If you wish to view any of the results in a map, select the required row(s), right-click and select Send to Map.

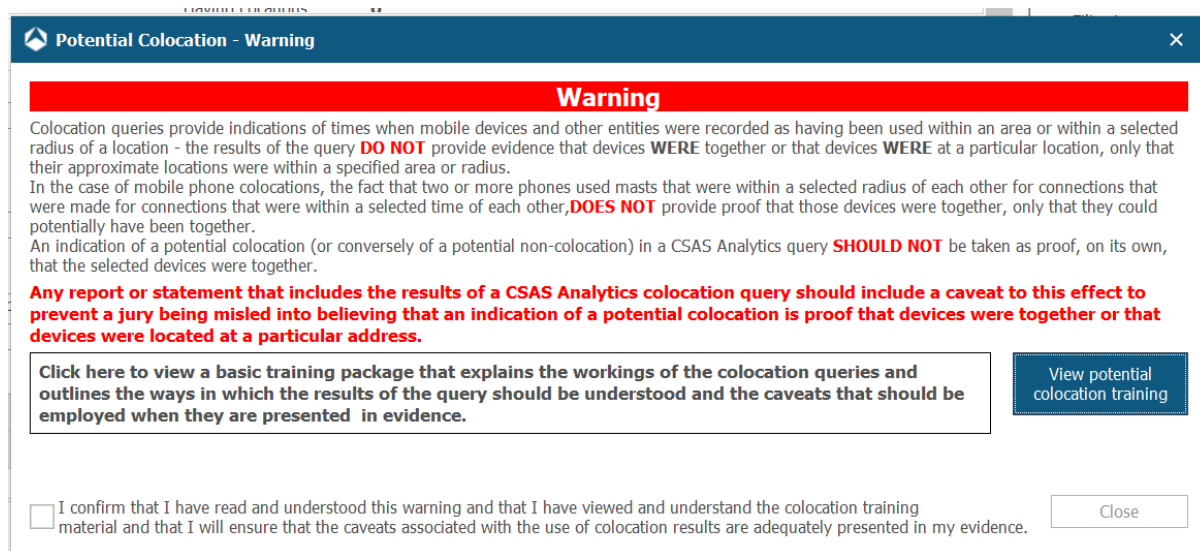
17.16 Using the Potential Colocation query

The Potential Colocation query identifies points in time when subject devices could have been in the approximate area as each other. As the source data for this analysis is often cellular billing records, which generally provide a location for the cell tower a phone was connected to, rather than providing a location for the phone itself, there exists the potential for a large degree of uncertainty in any results obtained. Use of the Potential Colocation query therefore has the following caveats associated with it:

WARNING: THE POTENTIAL COLOCATION QUERY PROVIDES AN INDICATION OF TIMES WHEN DIFFERENT DEVICES WERE LINKED TO LOCATIONS (CELL MASTS, ANPR CAMERAS, ETC) THAT ARE WITHIN A SELECTED DISTANCE OF EACH OTHER AND THAT WERE USED WITHIN A SELECTED TIME PERIOD - THE RESULTS OF THE QUERY DO NOT PROVIDE EVIDENCE THAT THE DEVICES WERE TOGETHER, ONLY THAT THE PROXIMITY OF THE LOCATIONS LINKED TO THEM RAISES THE POSSIBILITY THAT THEY COULD HAVE BEEN TOGETHER AT A POINT IN TIME.

THE UNCERTAINTY ASSOCIATED WITH THE QUERY INCREASES IF CELL DATA FOR GPRS/MOBILE DATA EVENTS OR ANPR DATA WHERE THE CAMERA IS LOCATED ONLY BY POSTCODE IS USED, AS THE CORRELATION BETWEEN EVENT START TIMES AND START LOCATION IS LESS CERTAIN, OR THE ACCURACY WITH WHICH THE LOCATION CAN BE DETERMINED IS LIMITED.

Whenever you open the Potential Colocation screen, you will see the following warning message:



Potential Colocation - Warning

Warning

Colocation queries provide indications of times when mobile devices and other entities were recorded as having been used within an area or within a selected radius of a location - the results of the query **DO NOT** provide evidence that devices **WERE** together or that devices **WERE** at a particular location, only that their approximate locations were within a specified area or radius.

In the case of mobile phone colocations, the fact that two or more phones used masts that were within a selected radius of each other for connections that were made for connections that were within a selected time of each other, **DOES NOT** provide proof that those devices were together, only that they could potentially have been together.

An indication of a potential colocation (or conversely of a potential non-colocation) in a CSAS Analytics query **SHOULD NOT** be taken as proof, on its own, that the selected devices were together.

Any report or statement that includes the results of a CSAS Analytics colocation query should include a caveat to this effect to prevent a jury being misled into believing that an indication of a potential colocation is proof that devices were together or that devices were located at a particular address.

[Click here to view a basic training package that explains the workings of the colocation queries and outlines the ways in which the results of the query should be understood and the caveats that should be employed when they are presented in evidence.](#)

[View potential colocation training](#)

☐ I confirm that I have read and understood this warning and that I have viewed and understand the colocation training material and that I will ensure that the caveats associated with the use of colocation results are adequately presented in my evidence.

[Close](#)

To close the warning message, you must select the checkbox to **confirm** you have read and understand the warning – a record of your acceptance is saved to the Case Audit. The window will close and the Potential Colocation screen is fully displayed.

The warning popup includes a link to a basic training package that outlines the benefits of the colocation query and also the caveats within which its results should be viewed. To get information about further training for this type of query, see [Where to Get Help](#).

17.16.1 Potential Colocation

This query allows you to look for times when two or more subject phones or vehicles could have been located near to each other or near to a case location, based on comparing the selected datasets against two parameters:

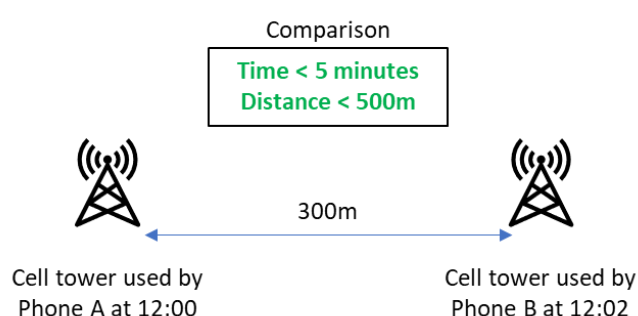
- » 'Time (seconds)' - refers to the time difference between events for the subject devices being considered by the query.
- » 'Distance (km)' - refers to the geographical distance within which the comparison is made, based on the location of cell site(s), cameras or case locations associated with each event.

Potential Colocation Events

A colocation event is when two or more groups of vehicles, target phones or POI events can be identified as potentially being near to one another at around the same time. For example, when you look for a colocation event, you might ask yourself the following question:

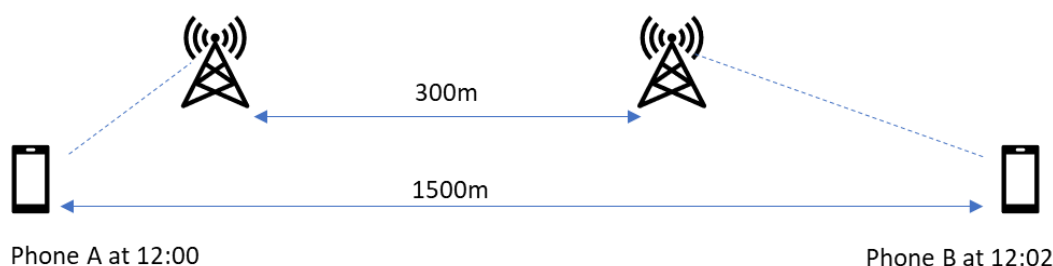
- » "Does an event for Phone A match with any events for Phone B that were active within Time (T) seconds of each other and if so, were the masts used by the two calls within Distance (D) of each other?"

For a potential colocation event to be indicated, the answers to both questions must be YES.



In this example, Phone A and Phone B were both in use within 2 minutes of each other, which is within the comparison time (T) of 5 minutes, and the towers used by the two phones are 300m apart, which is within the comparison distance (D) of 500m.

Phone A and Phone B could be said to be potentially collocating at this time. They are only 'potentially' collocating however – cell towers provide coverage across a wide area, as shown below, Phone A could have been at one extreme of the coverage area of its cell, whilst Phone B could have been at the extreme edge of its cell, meaning that the phones themselves could have been much further then 300m apart.



As, from cellular billing data alone, it is not generally possible to determine exactly where each subject phone was located, the analysis must be performed based on knowledge of the locations of the towers the subject phones used, which introduces the uncertainty that requires us to label this as a 'potential' colocation.

The reverse calculation is called a non-colocation event.

Non-colocation Events

A non-colocation event is when you look for points in time when the phones couldn't have been together. This is not as simple as thinking "I can calculate the collocating events and then show all the other events as non-colocating events".

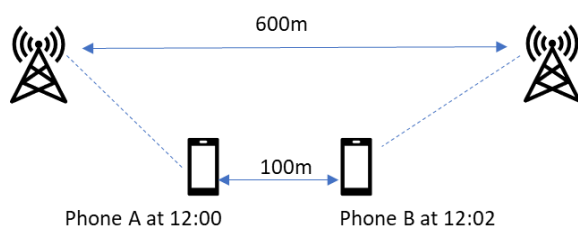
To be classed as a collocating event, two events must be within the D distance and within the T time but to be classed as a non-colocating event, the events must be greater than D distance apart but still within T time; events that are less than D distance but more than T time are classed as non-qualifying events (or 'All other events'):



In this example, Phone A and Phone B were both in use within 2 minutes of each other, which is within the comparison time (T) of 5 minutes, but the towers used by the two phones are 600m apart, which is outside the comparison distance (D) of 500m.

CSAS only outputs a non-colocation event if the distance between the cell site(s) is greater than the comparison distance and the time between the event(s) is within the time parameter; events where the time difference is greater than the time parameter are ignored because the comparison the query is attempting to show is whether the subject phones can be shown to be apart at a particular point in time. The query does not look for all occasions when the phones cannot be shown to be together but instead shows times when the phones must have been apart.

The uncertainties associated with using cellular billing data and tower locations for the comparison, means that it is also possible that the phones themselves could have been closer than the comparison distance, even if the towers they were using were further away.

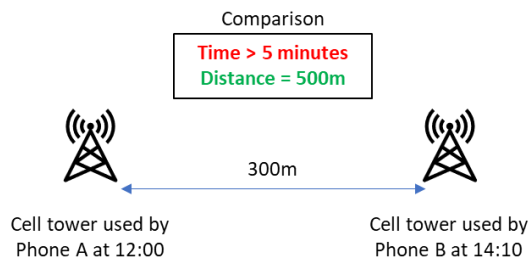


For this reason, non-colocation queries are usually run with much larger comparison distances than colocation queries use. A typical distance value for a colocation query

would be 500-1500m in urban areas, whereas a non-colocation query in the same area might be set to look for towers that 2500-5000m or more apart.

Non-Qualifying Events

Events where the time difference is greater than the time parameter are ignored because the comparison the query is attempting to show is whether the subject phones can be shown to be apart at a particular point in time. These events are known as 'non-qualifying' as they don't meet the basic requirements for either colocation or non-colocation.



In this example, although the cell towers used by the phones are within the distance value, the calls made by the phones are outside of the time comparison – there is a nearly two-hour time difference, so it's not possible to show that the phones were in the same area at the same time.

To ensure that CSAS offers a complete picture of potential colocation, the query can be set to count and report on the number of non-qualifying events in a dataset, to offer the ability to view the proportion of colocation/non-colocating events against the proportion of non-qualifying events.

The table below summarises the comparison that are made for the three classifications of events:

Time $\leq$ T Distance $\leq$ D	Potential colocation
Time $\leq$ T Distance $>$ D	Non-colocation
Time $>$ T Distance $\leq$ D	Non-qualifying

17.16.2 Use Cases

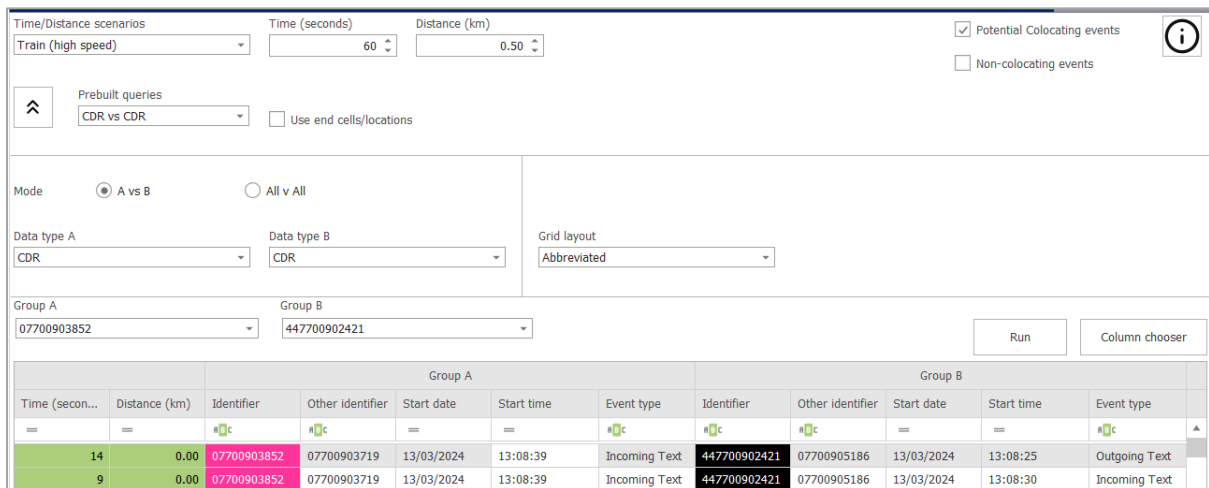
The CSAS Potential Colocation query currently works with three types of case data – CDRs, ANPR and POI locations. CSAS therefore supports the following basic forms of analysis:

- » CDR vs CDR
- » CDR vs ANPR.
- » CDR vs Layer
- » ANPR vs ANPR
- » ANPR vs Layer

CDR vs CDR

This option is used to look for potential colocations between mobile devices, with the intention of seeing if there are times when two or more mobile devices can be seen to be operating in the same general area at around the same time. Remember, this is not evidence that the two phones WERE together, only that they could potentially have been. This query allows you to select the mobile devices you want to compare against the configurable distance (D) and time (T) parameters. The question being asked by the query in this configuration is:

- » "Were any of the selected phones using cell masts within D distance of each other whilst making calls/texts/data connections that were active within T time of each other?"



The screenshot shows the CSAS Potential Colocation query interface. At the top, there are dropdowns for 'Time/Distance scenarios' (set to 'Train (high speed)'), 'Time (seconds)' (set to 60), and 'Distance (km)' (set to 0.50). There are checkboxes for 'Potential Colocating events' (checked) and 'Non-colocating events' (unchecked). Below this, there are 'Prebuilt queries' (set to 'CDR vs CDR') and a checkbox for 'Use end cells/locations'. The 'Mode' section has 'A vs B' selected. 'Data type A' and 'Data type B' are both set to 'CDR'. 'Grid layout' is set to 'Abbreviated'. 'Group A' is set to '07700903852' and 'Group B' is set to '447700902421'. There are 'Run' and 'Column chooser' buttons. Below the form is a table with columns for Time, Distance, Identifier, Other identifier, Start date, Start time, Event type, and then the same columns for Group B. The table shows two rows of data for Group A and Group B.

Group A							Group B					
Time (secon...	Distance (km)	Identifier	Other identifier	Start date	Start time	Event type	Identifier	Other identifier	Start date	Start time	Event type	
14	0.00	07700903852	07700903719	13/03/2024	13:08:39	Incoming Text	447700902421	07700905186	13/03/2024	13:08:25	Outgoing Text	
9	0.00	07700903852	07700903719	13/03/2024	13:08:39	Incoming Text	447700902421	07700905186	13/03/2024	13:08:30	Incoming Text	

CDR vs ANPR

This option is used to look for potential colocations between mobile devices and vehicles, with the intention of seeing if there are times when one or more mobile devices can be seen to be operating in the same general area at around the same time as a vehicle that was captured by an ANPR camera. This query allows you to select the mobile devices and the ANPR data files to be compared against distance (D) and time (T) parameters. The question being asked by the query in this configuration is:

- » "Were any of the selected phones using cell masts within D distance of any

of the ANPR cameras that captured details of any of the selected vehicles and were any of those devices active within T time of the captures taking place?"

Time/Distance scenarios
Train (high speed)
Time (seconds)
60
Distance (km)
0.50

☒ Potential Colocating events
☐ Non-colocating events

Prebuilt queries
CDR vs ANPR

☐ Use end cells/locations

Mode
☒ A vs B
☐ All v All

Data type A
CDR
Data type B
ANPR
Grid layout
Abbreviated

Group A
447700902421
Group B
BS79PTA

Run
Column chooser

		Group A					Group B				
Time (seconds)	Distance (km)	Identifier	Other identifier	Start date	Start time	Event type	Identifier	Other identifier	Start date	Start time	Event type
30	0.26	447700902421	07700900963	19/03/2024	09:19:22	Incoming Voice	BS79PTA		19/03/2024	09:18:52	ANPR
39	0.42	447700902421	07700900963	19/03/2024	14:01:59	Incoming Voice	BS79PTA		19/03/2024	14:02:38	ANPR

CDR vs Layer

This option is used to look for potential colocations between mobile devices and case events/locations (which are saved as POI 'layers' in the case database), with the intention of seeing if there are times when one or more mobile devices can be seen to be operating in the same general area at around the same time as a case event that took place at a specific location. This query allows you to select the mobile devices and the case event/location layers to be compared against distance (D) and time (T) parameters. The question being asked by the query in this configuration is:

» "Were any of the selected phones using cell masts within D distance of any of the locations at which case events took place and were any of those devices active within T time of any of the case events?"

Time/Distance scenarios
Train (high speed)
Time (seconds)
240
Distance (km)
2.50

☒ Potential Colocating events
☐ Non-colocating events

Prebuilt queries
CDR vs Layer

☐ Use end cells/locations

Mode
☒ A vs B
☐ All v All

Data type A
CDR
Data type B
Layer
Grid layout
Abbreviated

Group A
447700902421
Group B
Shooting (1)

Run
Column chooser

		Group A					Group B				
Time (seconds)	Distance (km)	Identifier	Other identifier	Start date	Start time	Event type	Identifier	Other identifier	Start date	Start time	Event type
141	0.69	447700902421	07700900963	19/03/2024	12:52:21	Outgoing Voice	Shooting (1)	Shooting (1)	19/03/2024	12:50:00	Event

ANPR vs ANPR

This option is used to look for potential colocations between significant vehicles, with the intention of seeing if there are times when one or more vehicles can be seen to be in the same general area at around the same time as each other. This query allows you to select the ANPR data files to be compared against the distance (D) and time (T)

parameters. The question being asked by the query in this configuration is:

- » "Were any of the vehicles detailed in the ANPR files captured by ANPR cameras that were within D distance of each other and did any of those captures take place within T time of each other?"

Total Records Read : 12	First Group : 11	Second Group : 1	Having Locations : 11	Having Locations : 1	All AvB Matches : 1	Potential Colocations : 1	Non Colocations : 0
-------------------------	------------------	------------------	-----------------------	----------------------	---------------------	---------------------------	---------------------

Potential Colocation

Time/Distance scenarios
Train (high speed)
Time (seconds)
130
Distance (km)
2.50

☒ Potential Colocating events
☐ Non-colocating events

Prebuilt queries
ANPR vs ANPR
☐ Use end cells/locations

Group A
BS79PTA
Group B
AA28HHD

Run
Column chooser

Group A							Group B				
Time (seconds)	Distance (km)	Identifier	Other identifier	Start date	Start time	Event type	Identifier	Other identifier	Start date	Start time	Event type
20	0.00	BS79PTA		19/03/2024	15:00:02	ANPR	AA28HHD		19/03/2024	15:00:22	ANPR

ANPR vs Layer

This option is used to look for potential colocations between significant vehicles and case events/locations (which are saved as POI 'layers' in the case database), with the intention of seeing if there are times when one or more vehicles can be seen to be operating in the same general area at around the same time as a case event that took place at a specific location. This query allows you to select the ANPR files and the case event/location layers to be compared against the distance (D) and time (T) parameters. The question being asked by the query in this configuration is:

- » "Were any of the significant vehicles captured by ANPR cameras within D distance of any of the locations at which case events took place and were any of those captures within T time of any of the case events?"

Time/Distance scenarios Train (high speed)	Time (seconds) 6000	Distance (km) 20.00	☒ Potential Colocating events ☐ Non-colocating events
---	------------------------	------------------------	---

Prebuilt queries
ANPR vs Layer
☐ Use end cells/locations

Group A
BS79PTA
Group B
Shooting

Run
Column chooser

Group A							Group B				
Time (seconds)	Distance (km)	Identifier	Other identifier	Start date	Start time	Event type	Identifier	Other identifier	Start date	Start time	Event type
4645	11.80	BS79PTA		19/03/2024	11:32:35	ANPR	Shooting	Shooting	19/03/2024	12:50:00	Event
1177	11.74	BS79PTA		19/03/2024	12:30:23	ANPR	Shooting	Shooting	19/03/2024	12:50:00	Event

Bespoke Queries

Using the controls available in the query, it's possible to build bespoke queries that compare a mix of CDR, ANPR and Location data against each other. For example, if you wanted to compare the mobile phone and the vehicle attributed to an individual against a case event/location (to see if that individual can be placed near to that location at a significant time), you could configure the query so that 'Group A' consisted of the phone and vehicle and 'Group B' was the location layer. This would then show if either the phone or the vehicle could be placed near the location at the time of the event:

Time/Distance scenarios
Train (high speed)

Time (seconds)
240

Distance (km)
2.00

☒ Potential Colocating events
☐ Non-colocating events

Prebuilt queries
ANPR vs Layer

☐ Use end cells/locations

Mode
☒ A vs B ☐ All v All

Data type A
CDR, ANPR

Data type B
Layer

Grid layout
Abbreviated

Group A
447700902421, B579PTA

Group B
Shooting

Run

Column chooser

Group A							Group B				
Time (seconds)	Distance (km)	Identifier	Other identifier	Start date	Start time	Event type	Identifier	Other identifier	Start date	Start time	Event type
=	=	447700902421	07700900963	19/03/2024	12:52:21	Outgoing Voice	Shooting	Shooting	19/03/2024	12:50:00	Event

17.16.3 Supported Data Types

The Potential Colocation query can only be used with CDR, ANPR and POI event & location data.

17.16.4 Layout

The Potential Colocation query is divided into three panes, with an additional drilldown pane that can be triggered if required.

Potential Colocation Summary

Total Records Read : 1801
First Group : 1314
Second Group : 487

Having Locations : 1314
Having Locations : 487

All Av8 Matches : 61
Potential Colocations : 61
Non Colocations : 0

Time/Distance scenarios
Train (high speed)

Time (seconds)
60

Distance (km)
0.50

☒ Potential Colocating events
☐ Non-colocating events

Prebuilt queries
CDR vs CDR

☐ Use end cells/locations

Group A
07700903852

Group B
447700902421

Run

Column chooser

Group A							Group B				
Time (se...	Distance (...)	Identifier	Other ide...	Start date	Start time	Event type	Identifier	Other ide...	Start date	Start time	Event type
14	0.00	07700903...	07700903...	13/03/2024	13:08:39	Incoming...	44770090...	07700905...	13/03/2024	13:08:25	Outgoing...
9	0.00	07700903...	07700903...	13/03/2024	13:08:39	Incoming...	44770090...	07700905...	13/03/2024	13:08:30	Incoming...
32	0.00	07700903...	07700903...	13/03/2024	13:08:57	Outgoing...	44770090...	07700905...	13/03/2024	13:08:25	Outgoing...

This potential colocation query provides an indication of times when different devices were linked to locations (cell masts, ANPR cameras, etc) that are within a selected distance of each other – the results of the query **DO NOT** provide evidence that the devices **WERE** together, only that the proximity of the locations linked to them raises the possibility that they **COULD** have been together....

Colocation Summary

Filters & Controls

Results Grid

Warning Text

Colocation Summary

This provides context for the analysis by showing the counts for the total number of compared events, the numbers of events for 'group A' and 'group B' identifiers and also indicates the number of each that were excluded from the analysis for having no associated location data. The main purpose of the summary table to show the counts for each comparison type – colocating, non-colocating and non-qualifying.

The purpose of providing the summary is to show the results in context – for example, if an analysis shows that out of 10,000 events, there were two potential colocations, that puts the potentially colocating events into perspective and may mean that the two phone were not potential together regularly. If, instead, the summary showed that out of

10,000 events there were 5,000 potential colocations, it could indicate that the phones potentially spend lots of time together.

Filters & Controls

These are used to set the parameters and values used by the query and are outlined below.

Results Grid

In A vs B mode, the results grid is divided into two sections – the left side shows events for a Group A identifier and the right side shows any correlating events for a Group B identifier. In All vs All mode, the grid can be interpreted as showing Phone A and Phone B records on each row.

There are three preloaded column layout options for the results grid – abbreviated, standard, full – and also a set of user selectable additional columns that can be added to the grid via the column chooser. For brevity, only the 'abbreviated' grid layout will be explained in detail:

- » Comparison columns:
 - Time (seconds) – shows the time difference between the measured timestamp for each correlating record.
 - Distance (km) – shows the geographical distance between the compared locations for each correlating record.
- » Group A columns:
 - Identifier – shows the Group A subject identifier used for this comparison.
 - Other identifier – shows the other number the subject identifier was in contact with for this record.
 - Start date – start date for the record.
 - Start time – start time for the record.
 - Event type – call, text, data session, ANPR capture, POI event, etc.
- » Group B columns:
 - Identifier – shows the Group B subject identifier used for this comparison.
 - Other identifier – shows the other number the subject identifier was in contact with for this record.
 - Start date – start date for the record.
 - Start time – start time for the record.
 - Event type – call, text, data session, ANPR capture, POI event, etc.

It cannot be stressed enough how important it is to remember that the Potential Colocation query does not necessarily indicate that the analysed identifiers were actually together – a repetition of the warning text is shown at the foot of the results grid, just to reinforce the message.

17.16.5 Filters & Controls

The Potential Colocation query requires a complex set of filters and controls.

Source Data selection

The source data – either from source files or from a case snapshot – to be analysed is selected using the right sidebar Filters > Source Data control in the usual way.

As with most analytics queries, using the 'Filters' and 'Settings' tabs located on the right sidebar, you can filter the overall dataset to be queried, for example 'From' and 'To' dates and times, and therefore control the output of the colocation calculation.

Select the required source data and hit the Apply button to send the data into the query – clicking Apply does not run the query, it merely passes the required data to it.

If you want to change the set of data being analysed, select a different set of source data and again click 'Apply' to send it into the query.

For processing a colocation query, each event included in the dataset should be treated as being the equivalent, irrespective of whether it's a call, a text, an ANPR hit or POI event, as all events have:

- » Identifier
- » Start time
- » Start location (lat/long)
- » End time
- » End location (lat/long)

For most types of data, the end time/end location will be the same as the start time/start location. You can choose to disable the comparison against end time/location so only the start time/location would be considered by the query (this is the default).

Filters

In the 'Potential Colocation' Filters & Controls section, there are various options and filters you can select to change what information is output in the report grid:

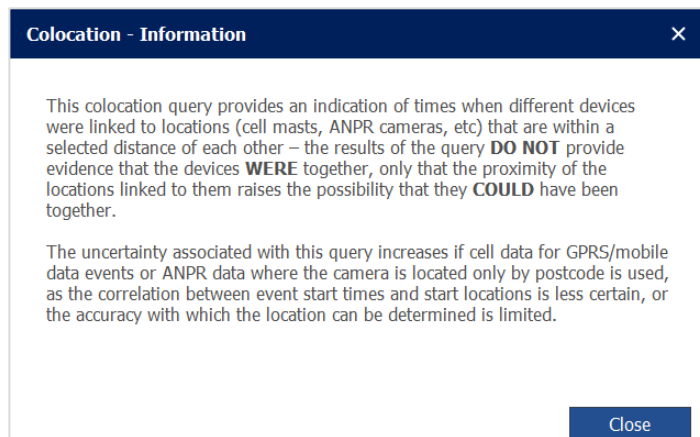
The filters section defaults to a minimised state, where the mode, data type and grid layout options are hidden – click on the  button to view the additional options and on  to hide them again. The screenshot above shows this section maximised.

The elements in the filters section are:

- » 'Time/Distance scenarios' - selectable using the drop-down menu. Each scenario populates the 'Time (seconds)' and 'Distance (km)' fields with different parameters to run the query against for different analytical scenarios; for example, if you select 'Pedestrian (low speed)', these fields will show a shorter comparison time and distance than if you select 'Train (high speed)'. You can also set the time/distance values manually by typing in the relevant boxes.
- » 'Time (seconds)' - selectable using the up/down arrows or by typing in the box. Increasing or decreasing the time adjusts the time in which comparisons are made. Shorter time spans produce more feasible potential colocations – setting a time period of 5 minutes might find realistic potential colocations, whereas setting a value of 12 hours would generally provide few realistic results.
- » 'Distance (km)' - selectable using the up/down arrows or by typing in the box. Increasing or decreasing the distance adjusts the range in which a colocation might exist. Shorter distances (for colocation) and longer distance (for non-colocation) produce more feasible potential colocations – setting a colocation distance of 100km, where the entities could be 100km or more apart, generally wouldn't be accepted as evidence of the entities potentially being together at a location.
- » 'Prebuilt queries' - various standard 'data type vs data types' scenarios are selectable from a drop-down menu and have built-in assumptions to make outputting a query report quicker. For more information see *Running a Prebuilt Query*
- » 'Use end cells/locations' - selecting this option, which is only applicable for CDR events, compares all cells used in each compared set of records (start-start, start-end, end-end) to determine if any of those distances fall within the comparison value. For more information, see *Comparing using End Cells / Locations*.
- » 'Colocating events' - selecting this option displays only colocation events in the report grid (coloured green).
- » 'Non-colocating events' - selecting this option displays only non-colocation events in the report grid (coloured red).
- » 'Mode' - 'A vs B' and 'All vs All' are available. For more information see *Selecting Different Modes*.
- » 'Data type A' and 'Data type B' - selecting these options allows you to choose the type(s) of data that will be analysed in 'Group A' and 'Group B' (or just 'Group A' for 'All vs All'). A mix of data types – CDR and ANPR, for example – can be selected for each group if required.
- » 'Group A' and 'Group B' - from the drop-down menu you can select all identifiers for each group you want to run a report against, in All vs All mode

there is only a Group A dropdown. For more information see *Selecting Data and Group Options*.

- » 'Grid layout' - from the drop-down menu you can select from Abbreviated, Standard or Full output layouts. For more information see *Selecting View Options*.
- » 'Run' - runs the query using the selected dataset and filter options. Generates co-location data in the form of a grid, which displays any 'Potential Colocating events' and/or 'Non-colocating events'. For more information see *Generating Co-location Data*.
- » 'Column chooser' - clicking on the Column chooser button opens the 'Customization' pop-up window. From the window you can select from two tabs: 'Columns' and 'Bands' to customize the grid layout. For more information see *Customising the Grid Layout*.
- »  clicking this icon shows a pop-up message explaining about colocations:

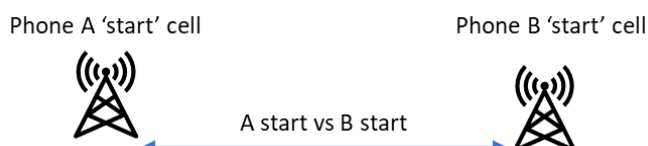


17.16.6 Comparing using End Cells / Locations

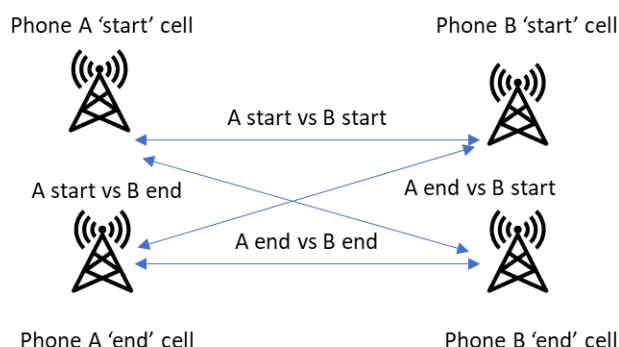
In A vs B mode, the Potential Colocation query compares the times and locations for 'Group A' events against the times and locations for 'Group B' events. In 'All vs All' mode, the query compares data for all selected identifiers against each other.



With the 'use end cells/locations' checkbox unselected, for CDR data, CSAS only compares the start time of one call with the start time of another call, meaning that there will only be one 'qualifying comparison' (A start vs B start) for each pair of compared events.



When you select the 'Use end cells/locations' checkbox, CSAS must compare all possible permutations of time and distance for each pair of compared records (A-Start vs B-Start; A-Start vs B-End; A-End vs B-Start; A-End vs B-End) – meaning that there could be up to four qualifying comparisons for each pair of compared events.



This leads to a complex set of results from the comparisons for D distance and T time:

Start/End Time	Start/End Location
Potential Colocation	
A start time vs B start time $\leq T$	A start location vs B start location $\leq D$
A start time vs B end time $\leq T$	A start location vs B end location $\leq D$
A end time vs B start time $\leq T$	A end location vs B start location $\leq D$
A end time vs B end time $\leq T$	A end location vs B end location $\leq D$
Potential Non-colocation	
A start time vs B start time $\leq T$	A start location vs B start location $\geq D$
A start time vs B end time $\leq T$	A start location vs B end location $\geq D$
A end time vs B start time $\leq T$	A end location vs B start location $\geq D$
A end time vs B end time $\leq T$	A end location vs B end location $\geq D$

Multiple comparisons for each pair of compared events could potentially collocate or non-colocate, so to keep the results table simple (and not show four rows of results for every pair of compared records), the query chooses the 'best comparison' for each pair of compared records, instead of showing up to four results for each compared pair of records.

For potential colocation, the 'qualifying comparisons' will be those where time $\leq T$ and distance is $\leq D$, but the 'best comparison' will be the one with the shortest distance (e.g. showing details of when the selected devices were potentially closest to each other). If all four comparisons were potentially collocating, the best comparison will be coloured green; if only some of the results were potentially colocation (e.g. if A-Start vs B-Start was collocating but the other three comparisons weren't) then the best comparison will be coloured orange.

For potential non-colocation, the 'qualifying comparisons' will be those where time $\leq T$ and distance $\geq D$, but the 'best comparison' will be the one with the largest distance (e.g. showing details of when the devices were potentially furthest apart). If all four comparisons were potentially non-collocating, the 'best comparison' will be coloured red; if only some of the comparisons were non-collocating (e.g. if A-End vs B-Start was non-collocating but the other three weren't) then the best comparison will be coloured orange.

17.16.7 Colouring

Query results in the report grid are coloured. Colouring helps to make the query results easier to understand:

- Colocating events are coloured green.
- Non-colocating events are colour red.
- When end cell comparison is enabled, 'partial' events, where only some comparisons associated with the events correlate, are coloured orange:

Time/Distance scenarios

Train (high speed)

Time (seconds)

60

Distance (km)

0.50

☒ Colocating events

☐ Non-colocating events

☐ All other events

Prebuilt queries

CDR vs CDR

☒ Use end cells/locations

Mode

A vs B

Data type A

CDR

Data type B

CDR

Grid layout

Abbreviated

Group A

07700900111, 07700900177, 07...

Group B

07700900111, 07700900177, 07...

Run

Column chooser

Group A							Group B						
Time (seconds)	Distance (km)	Identifier	Other identifier	Start date	Start time	Event type	Identifier	Other identifier	Start date	Start time	Event type		
15	0.00	07700900597		29/08/2...	21:09:29	Data	07700900177		29/08/2012	21:09:14	Data		
1	0.00	07700900597	07700900343	29/08/2...	21:40:06	Outgoing Voice	07700900177	07700900597	29/08/2012	21:41:23	Outgoing Voice		
9	0.00	07700900597	07700900343	29/08/2...	21:40:06	Outgoing Voice	07700900177	07700900597	29/08/2012	21:41:23	Outgoing Voice		
1	0.00	07700900597	07700900177	29/08/2...	21:41:22	Incoming Voice	07700900177	07700900597	29/08/2012	21:41:23	Outgoing Voice		
9	0.00	07700900597	07700900177	29/08/2...	21:41:22	Incoming Voice	07700900177	07700900597	29/08/2012	21:41:23	Outgoing Voice		
7	0.00	07700900597	07700900177	29/08/2...	21:41:22	Incoming Voice	07700900177	07700900597	29/08/2012	21:41:23	Outgoing Voice		
1	0.00	07700900597	07700900177	29/08/2...	21:41:22	Incoming Voice	07700900177	07700900597	29/08/2012	21:41:23	Outgoing Voice		
1	0.00	07700900177	07700900597	29/08/2...	21:41:23	Outgoing Voice	07700900597	07700900343	29/08/2012	21:40:06	Outgoing Voice		

This location query provides an indication of times when different devices were linked to locations (cell masts, ANPR cameras, etc) that are within a selected distance of each other - the results of the query **DO NOT** provide evidence that the devices were linked.

The uncertainty associated with this query increases if cell data for GPS/mobile data events or ANPR data where the camera is located only by postcode is used, as the correlation between event start times and start locations is less certain, or the accuracy.

There are multiple scenarios catered for in the query and the colouration is there to help summarise the results. For example:

- With 'End cells/locations' disabled and 'Non-colocating events' selected: if time $\leq T$ and distance $> D$ then there will be one qualifying comparison (A start vs B start) which will be coloured red.
- With 'End cells/locations' enabled and 'Potential Colocating events' selected: there will be four possible comparisons, if all four comparisons have time $\leq T$ and distance $\leq D$, then there will be four qualifying comparisons; the query will select the 'best' comparison (with the lowest distance) to display and will colour it green.
- With 'End cells/locations' enabled and 'Potential Colocating events' selected: there will be four possible comparisons, if only some but not all of the comparisons have time $\leq T$ and distance $\leq D$ (e.g. if the start cells are $< D$ apart but the end cells are $> D$ apart), then there will be less than four qualifying comparisons; the query will select the 'best' comparison (with the lowest distance) to display and will colour it orange.
- With 'End cells/locations' enabled and 'Non-colocating events' selected: there will be four possible comparisons, if all four comparisons have time $\leq T$ and distance $> D$, then there will be four qualifying comparisons; the query will select the 'best' comparison (with the largest distance) to display and will colour it red.
- With 'End cells/locations' enabled and 'Non-colocating events' selected:

there will be four possible comparisons, if only some but not all of the comparisons have time $\leq T$ and distance $> D$ (e.g. if the start cells are $< D$ apart but the end cells are $> D$ apart), then there will be less than four qualifying comparisons; the query will select the 'best' comparison (with the largest distance) to display and will colour it orange.

Note: The choice of colours used is not user selectable.

17.16.8 Selecting Different Modes

CSAS supports two Potential Colocation modes – A vs B mode and All vs All mode.

This is selected in the expanded filters section.

A vs B

In this mode, you will select one or more identifiers to be in Group A (for example all of the phones attributed to the same individual) and one or more identifiers to be in Group B.

The query then works sequentially through every record in the dataset and looks for pairs of records (one record from Group A and one from Group B) where the compared timestamps of the two records are within the T.

If time $> T$ then the pair of records are classed as non-qualifying and the process moves on, if time $\leq T$ the process checks the distances between the locations in the two records.

If any distances are $\leq D$ the records are classed as potentially collocating, if any distances are $> D$ the record are classed as non-colocating.

The A vs B results table lists the 'best comparison' for each individual pair of qualifying records.

All vs All

In this mode, there is only one group (Group A), that contains all selected identifiers.

The query then works sequentially through all events for all identifiers and compares them. This means that the results will show all potential colocations for all identifiers against all other identifiers, without filtering them by group. This mode may produce many more records than A vs B mode, as it will also show potential colocations between identifiers that might belong to the same group or individual.

17.16.9 Selecting Data and Group Options

Potential Colocation Summary

Total Records Read :	1801	All Av8 Matches :	61
First Group :	1314	Potential Colocations :	61
Second Group :	487	Non Colocations :	0
Having Locations :	1314		
Having Locations :	487		

Potential Colocation

Time/Distance scenarios: Train (high speed) | Time (seconds): 60 | Distance (km): 0.50

☒ Potential Colocating events | ☐ Non-colocating events

Prebuilt queries: CDR vs CDR | ☐ Use end cells/locations

Mode: ☒ A vs B | ☐ All v All

Data type A: CDR | Data type B: CDR | Grid layout: Abbreviated

Group A: 07700903852 | Group B: 447700902421

You can select different data types from the 'Data type [X]' and 'Group [X]' drop-down menus:

- From both 'Data type [X]' drop-down menus, you can select one or multiple dataset types you have imported, for example 'CDR', 'ANPR', 'Layers' etc. to run the query against.
- From both the 'Group [X]' drop-down menus, you can select one or more Identifiers to run the query against.

For information on how these options change the query, see *Use Cases*.

17.16.10 Running a Prebuilt Query

To make it easier and quicker to run a query, you can select to run a Prebuilt query. This function is intended to save you time, by having built-in assumptions and criteria and automatically setting the 'Mode' and the 'Data type [X]' options for you.

The Mode defaults to A vs B mode.

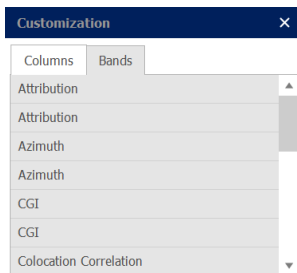
The Data Type options are outlined in the Use Cases above and offer various permutations of CDR, ANPR and POI Layer analysis.

Selecting 'CDR vs CDR', for example, loads only phone numbers into Group A and Group B selection dropdowns.

17.16.11 Customising the Grid Layout

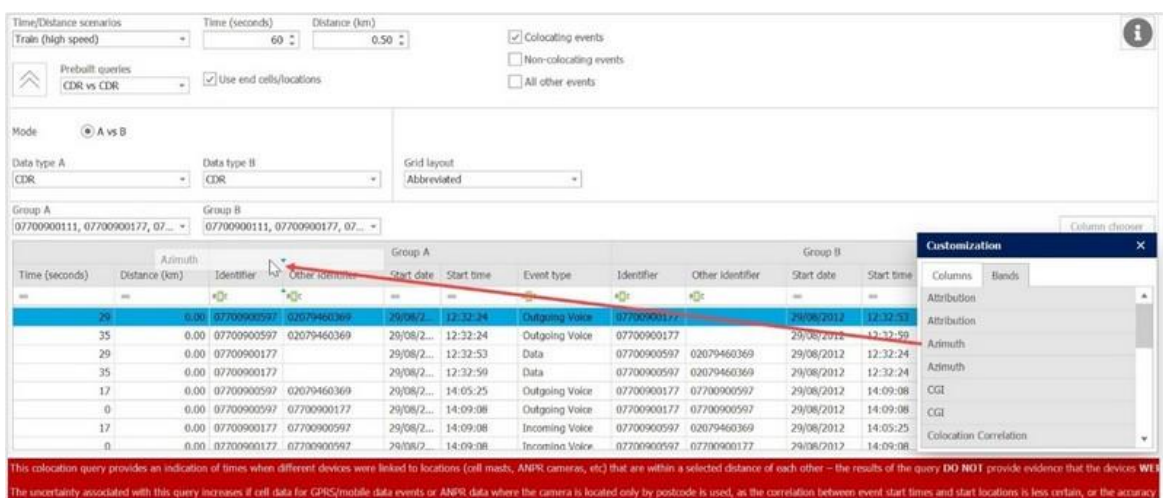
The Grid Layout option offers three preloaded grid layout options. If you wish to customise a layout or add more columns to it than are provided, you can use the Column Chooser.

Clicking on the button opens the 'Customization' pop-up window:



From this pop-up window, select the 'Columns' tab.

- The 'Columns' tab allows you to drag and drop different columns into the grid. Select a column name, for example 'Event ID', left click on the name and hold the mouse button, then drag your selection up to the header row of the grid to the position you want the column:



- To place the column, let go of the left mouse button - the column docks in the grid.

Note: You can drag columns in and out of the 'Customization' pop-up window as necessary.

17.16.12 Generating Co-location Data

Clicking the Run button generates a grid which displays any 'Potential Colocating events' and/or 'Non-colocating events', as selected using the checkboxes in the controls section of the window.

The grid is generated using the files selected from the 'Source data' panel.

The grid opens in the 'Potential Colocation' window:

17.16.13 Understanding the results

The Potential Colocation query is designed to provide an indication of events that show that two identifiers could be together (for example, to try to support an allegation that two suspects met up) or not together (for example, to undermine a suspect's alibi statement that he was with another individual at a certain time).

The key parameters for the query at the time (T) and distance (D) values.

A potential colocation is indicated if the difference in the timestamps of two compared

records is less than time T and the geographical distance between the locations in the records is less than distance D.

A non-colocation is indicated if the time difference is less than T and geographical distance is greater than D.

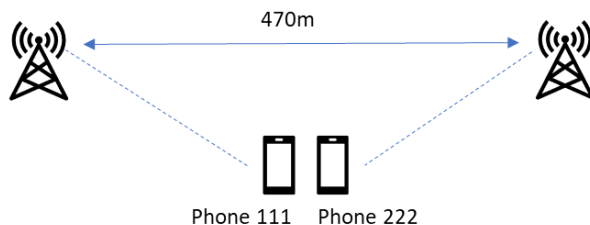
Non-qualifying records have a time difference greater than T, which therefore means that it doesn't matter what the geographical difference is.

Potential Colocation Example

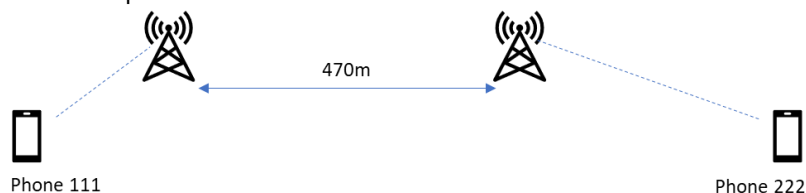
In this example, the 111 phone is being compared to the 222 phone with comparison values of T=60s and D=500m and 'compare end cells' disabled.

Time (seconds)	Distance (km)	Identifier	Start date	Start time	Identifier	Start date	Start time	Event type
=	=		=	=		=	=	
20	0.47	07700900111	02/04/2020	07:04:57	07700900222	02/04/2020	07:05:17	Incoming Voice
20	0.47	07700900111	02/04/2020	09:04:57	07700900222	02/04/2020	09:05:17	Incoming Voice
20	0.31	07700900111	02/04/2020	15:04:57	07700900222	02/04/2020	15:05:17	Incoming Voice
20	0.47	07700900111	02/04/2020	17:04:57	07700900222	02/04/2020	17:05:17	Incoming Voice

- » On 02/04/2020 at 07:04:57 the 111-phone connected to the network – within 20 seconds the 222 connected using a cell tower that was 470m away.
- » Remember that the locations provided in the source data show the location of the cell towers used by the phones, not the locations of the phones themselves.
- » A favourable interpretation of this results is that the phones were located near their cell towers and may even have been closer together than 470m.



- » A less favourable interpretation is that the phones could have been anywhere in the coverage areas of the two cell and may have been much further apart than 470m.



- » Since it is not possible, with CDR data, to be any more definite about the location of the phones, we accept that the data tells us the phone could 'potentially' have been colocating.
- » The results indicate that the two phones had several instances where they were potentially colocating during the day on 02/04/2020. Multiple potential colocations across multiple days strengthens support for an allegation that, for example, the two phones are being carried by the same person (a 'clean' phone and a 'dirty' phone, possibly). Whereas comparisons that look at a long

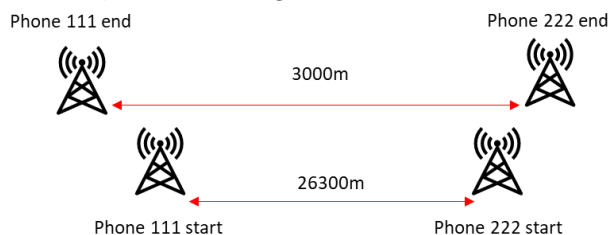
period of time where there are only a few potential colocations might not support an allegation of colocation and might be dismissed as mere coincidence.

Non-Colocation Example

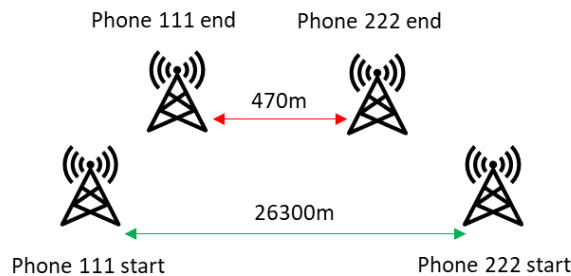
In this example, the 111 phone is being compared to the 222 phone with comparison values of $T=60s$ and $D=500m$ and 'compare end cells' enabled.

Time (seconds)	Distance (km)	Identifier	Start date	Start time	Identifier	Start date	Start time
=	=		=	=		=	=
50	2.63	07700900111	01/04/2020	11:04:57	07700900222	01/04/2020	11:05:17
50	2.63	07700900111	01/04/2020	13:04:57	07700900222	01/04/2020	13:05:17
50	2.63	07700900111	01/04/2020	15:04:57	07700900222	01/04/2020	15:05:17
50	2.63	07700900111	01/04/2020	17:04:57	07700900222	01/04/2020	17:05:17
50	2.63	07700900111	01/04/2020	19:04:57	07700900222	01/04/2020	19:05:17
20	2.63	07700900111	01/04/2020	21:04:57	07700900222	01/04/2020	21:05:17
50	2.63	07700900111	01/04/2020	23:04:57	07700900222	01/04/2020	23:05:17

- On 01/04/2020 at 11:04:57, the 111phone connected to the network, 50 seconds later the 222-phone connected to the network using a cell tower that was 2630m away. Time was $< T$ and distance was $> D$, so we can class this as a non-colocation.
- As 'compare end cells' is enabled, for each of the correlating records displayed in the grid, CSAS undertook eight separate calculations – for both T and D it compared A start vs B start, A start vs B end, A end vs B start, A end vs B end.
- For the first 5 rows in the grid, all four T calculations must have shown that time was less than T and all four D calculations must have shown that distance was less than D – we can tell this because those rows are coloured red, which means that all 8 comparisons were 'qualifying comparisons'. An example of this might look like this:



- For the last two rows, at least of the comparisons must have been non-qualifying – meaning that at least one of the Time comparisons had a time difference greater than T , or one of the distance comparisons had a distance less than D – as the rows are coloured orange to indicate 'partial correlations'. An example of this might look like this:



- » Non-colocation analysis generally works better with longer values for D – at 500m, the distance between towers is small enough to allow phones using those towers to potentially still colocate. Values of several km are considered to be better.

Why, When, Who



This function is necessary to provide an indication of times when two or more Identifiers could have been in the same general area as each other ('colocating'). The function provides a 'potential' colocation query as it's not possible for CSAS to tell if the phones actually were together, or if they just happened to be using nearby cell towers at the same time however, from this query it can be inferred that those phones and their users may have had an opportunity to be colocating.



This function is undertaken at any time.



This function is typically carried out by the following users:

- » CSAS User

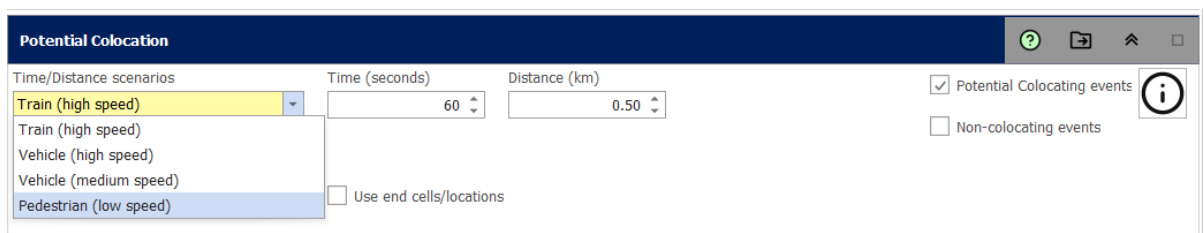
Stepped Procedure

There are multiple permutations of ways to run Potential Colocation queries. This section outlines two examples, a very simple query using the preloaded scenarios option, and a more complex option that mixes different data types together.

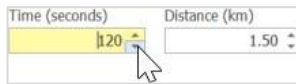
Simple Scenario

In this scenario you want to run a simple colocation analysis on the data for two phones using start cell information only:

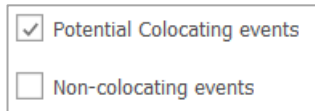
1. Select the source data you wish to analyse from the right sidebar, select any sidebar Filters or Settings you wish to use and hit 'Apply' to load the data into the query.
2. From the 'Time/Distance scenarios' field, select the appropriate scenario:



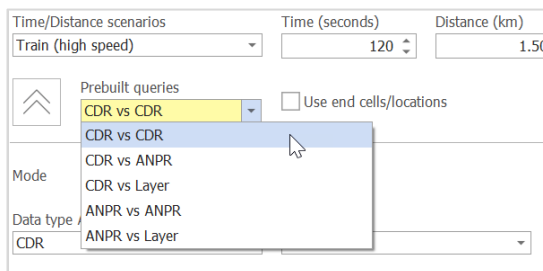
- The values in the 'Time (seconds)' and 'Distance (km)' fields will be automatically populated however you can use the controls to select different values if required:



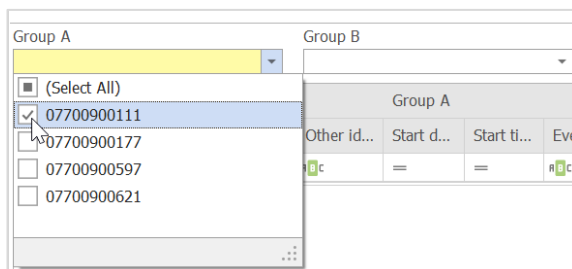
- Select the type of event you want the query to output result for:



- From the 'Prebuilt queries' drop-down, select the type of query you want to run such as 'CDR vs CDR', 'CDR vs Layer' etc:



- From the 'Group [A/B]' fields, you can select one or multiple Identifiers you want the query to work on for each group. Note – you must select at least one identifier for Group A and at least one identifier for Group B:



- To run the query, click on the Run button. The report grid will display the query results.
- You can send one or more rows from the results grid to the drilldown pane using the right-click option and get export the grid using the Export and Print options in the pane header.

Complex Scenario

In this scenario you want to run a complex colocation analysis on the data for three phones and two vehicles using start and end cell information:

- Select the source data you wish to analyse from the right sidebar, select any sidebar Filters or Settings you wish to use and hit 'Apply' to load the data into the query.
- Set Time as 120s and Distance as 1500m.
- Tick the 'use end cells/locations' box.
- Click on the down chevron button to maximise the additional filters section.

5. For Data Type A, select CDR and ANPR and do the same for Data Type B.

Data type A

CDR, ANPR

(Select All)

☒ CDR

☒ ANPR

☐ Layer

6. Select the required mix of phone numbers and number/licence plate numbers for Group A and do the same for Group B.

Group A

07700900111

Group B

07700900222

	☒	Value	AttributedTo
	☒	07700900111	Unknown 1
	☒	ABCDEFGF	Unknown 3

7. Select 'Potential Colocating events' as the query type.
8. Hit the Run button.
9. The results will show instances where any of the records for the phones/cars in Group A have Time $\leq T$ and Distance $\leq D$ when compared to any of the records for the phones/cars in Group B.

Time (seconds)	Distance (km)	Identifier	Start date	Start time	Identifier	Start date	Start time
==	==		==	==		==	==
30	1.10	ABCDEFGF	01/04/2020	10:06:02	07700900222	01/04/2020	10:06:02
30	1.10	ABCDEFGF	01/04/2020	10:06:02	07700900222	01/04/2020	10:06:02
30	1.10	ABCDEFGF	01/04/2020	10:06:02	07700900222	01/04/2020	10:06:02
30	1.10	ABCDEFGF	01/04/2020	10:06:02	07700900222	01/04/2020	10:06:02

10. Correlations between entities within each group are ignored – for example if phone A1 and vehicle A2 can be seen to be colocating, this will not be reported in A vs B mode.

18 Case Reports

The Case Reports feature offers a set of pre-built report types or templates that are designed to simplify and streamline some of the administrative chores associated with building a case.

There are three Case Reports options:

- » Disclosure Report
- » Phone/Attribution/File Summary
- » Continuity Log

The report types currently included in the Case Reports set are largely based on the requirements of UK users, additional reports and templates can be added that conform to the requirements of other jurisdictions if required; please contact your CSAS account manager or CSAS Support if you wish to discuss the creation of additional report types.

18.1 Disclosure Report

In many jurisdictions, it is a requirement that the prosecution provide to the defence full details of all objects and items that came into their possession during an investigation, whether those items were used as part of the investigation or not. In the UK, this process is known as 'disclosure' and requires the prosecuting agency to provide a list of all materials, used or unused, to the defence, except in situations where the materials contain information that is regarded as 'sensitive' – e.g. that could identify a vulnerable witness or an undercover asset.

This requirement is also imposed on the less tangible items employed in a digital forensics investigation, such as the source files that were obtained for analysis.

In some parts of the UK, the prosecution is required to complete MG6 forms that contain lists of the items to be disclosed – in a cell site analysis investigation, this is usually a list of the source data files that have been analysed. Manually compiling an MG6 form can be a long and tedious process, but the CSAS Case Reports feature can automate this process and reduce the time required to minutes instead of hours.

The CSAS Disclosure report supports two file status options:

- Used – means the file was imported into the case and data from the file was included in the analysis
- Unused – means that the contents of file were not used as part of the analysis

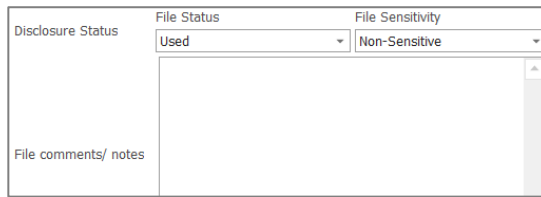
There are also two 'sensitivity' markings for files – a file marked 'non-sensitive' contains no data that could, for example, identify a vulnerable witness or an undercover asset, and disclosure of that file would not pose a risk to individuals or other investigations. A file marked 'sensitive' might contain information of that sort and may be judged too risky to disclose.

18.1.1 Setting Disclosure Status

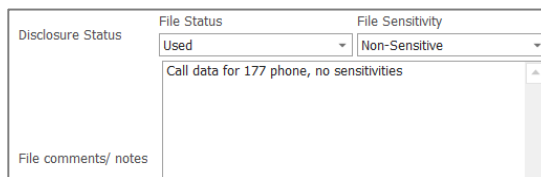
The disclosure status of each file imported into a CSAS case is set in the Import Files tab, specifically in the Update File Details menu.

To set the disclosure status of an imported file:

1. Select the file in the Import Files grid, right-click and select Update File Details.



2. The Disclosure section of the Update menu allows users to set the file's Disclosure status (used/unused), its sensitivity (sensitive/non-sensitive) and also allows any file-specific Disclosure comments to be added.



3. Once the details of the file have been updated, click 'Save' to save the data and close the Update File Details menu.
4. Repeat for all other files in the case.

18.1.2 Reviewing Disclosure Data

The Disclosure settings for a case can be reviewed in the Import Files grid (via the Disclosure radio button) or in the Case Reports > Disclosure screen.

☒ Disclosure ☐ Date Range 

	Call/Event count	Format ID	Provider	Data from	Data to	File Status	Sensitivity	Comments/notes	Cell/Location count
	=	#[c]	#[c]	=	=	=	=	#[c]	=
	334	CDR23-UK2...	UK_TMobile	29/08/2021	05/09/2021	Used	Non-Sensitive	Call data for 177 phone, no sensitivities	147
	504	CDR23-UK2...	UK_TMobile	29/08/2021	05/09/2021	Used	Non-Sensitive		190
	343	CDR24-UK2...	UK_TMobile	29/08/2021	05/09/2021	Used	Non-Sensitive		180

18.1.3 Creating a Disclosure Report

To output a Disclosure Report, open the Case Reports > Disclosure Report screen.

Import 		Disclosure Report 									
		File Status	Any								
		Sensitivity	Any								
		Report Template	MG6C	Create							
		Filename	Subject Ident...	Attribution	Type	Provider	Start Date	End Date	File Status	Sensitivity	Comments/ Not...
+	☐	4791322 2021...	07700900177	James SMITH	CDR	UK_TMobile	29/08/2021	05/09/2021	Used	Non-Sensitive	Call data for 17...
+	☐	4791323 2021...	07700900177	James SMITH	CDR	UK_TMobile	29/08/2021	05/09/2021	Used	Non-Sensitive	
+	☐	4791324 2021...	07700900177	James SMITH	CDR	UK_TMobile	29/08/2021	05/09/2021	Used	Non-Sensitive	
+	☐	4791417 2021...	07700900597	David WILLIAMS	CDR	UK_TMobile	14/08/2021	02/09/2021	Used	Non-Sensitive	
+	☐	4791418 2021...	07700900597	David WILLIAMS	CDR	UK_TMobile	14/08/2021	02/09/2021	Used	Non-Sensitive	
+	☐	4791422 2021...	07700900597	David WILLIAMS	CDR	UK_TMobile	14/08/2021	02/09/2021	Used	Non-Sensitive	
+	☐	90743 CDQ 20...	07700900621	Paul TAYLOR	CDR	UK_O2	14/08/2021	11/09/2021	Used	Non-Sensitive	
+	☐	Cell Address...			Cell data	UK_Generic	01/01/0001	31/12/9999	Used	Non-Sensitive	

With no filters applied, the Disclosure Report grid lists all files that have been imported into the case. Filtering options at the top of the grid allow users to filter the grid by File Status (used/unused) and Sensitivity (sensitive/non-sensitive).

Filter the grid to show only the set of files to be included in a specific Disclosure Report – it is often the case that separate MG6 reports will be created to show each permutation

of status and sensitivity. Select the files from the filtered list to be included in the report by ticking the required rows in the grid.

Once the required set of files is displayed in the list, select the required output template (MG6C is used to list non-sensitive disclosures, MG6D is for sensitive disclosures, please see https://www.cps.gov.uk/sites/default/files/documents/legal_guidance/National-Disclosure-Standards-2018.pdf for more details), and hit 'Create'. The report will be created in using the recommended Word template and will be available to be further edited and annotated once it has been exported from CSAS.

POLICE SCHEDULE OF RELEVANT NON-SENSITIVE UNUSED MATERIAL			
R v Crippen The Disclosure Officer believes the following RELEVANT MATERIAL which does not form part of the prosecution case is NOT SENSITIVE. For further detailed guidance refer to the Disclosure Manual and Attorney General's Guidelines		URN FOR CPS USE: * Enter D = Disclose to defence I = Item disclosable and defence may inspect CND = Clearly not disclosable (by description) ND = Document viewed and not disclosable	
Item No	Record below Material of any kind, including information and objects, which is obtained in the course of a criminal investigation and which may be relevant to the investigation and RELEVANCE is that it has some bearing on any offence under investigation or any person being investigated or on the surrounding circumstances of the case, unless it is incapable of having any impact on the case. Do not speculate if it is not considered relevant do not record it on the schedule. Give a sufficiently detailed DESCRIPTION of the relevant material for the prosecutor to make a decision on whether or not it should be examined.	LOCATION State precisely where the item can be found/located	* REASON FOR DECISION
	The relevant is: Filename: 4791322 2021.csv Subject Identifier: 07700900177 Attribution: James SMITH Type: CDR	Within OIC case on CSAS	

18.2 Phone/Attribution/File Summary

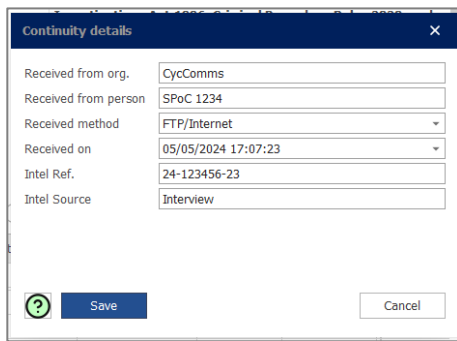
If the product of a CSAS case is submitted to court, it is usually combined with some form of statement or analytical report that summarises the findings. These statements often list the source files that were analysed and show relevant details about them, such as the filename, the associated subject identifier, the linked attribution and so on. This report offers a simple way of gathering that kind of administrative information in one place, from where it can be copied or inserted into a report or statement.

Attribution	Target Identity	Short File Name	Data Start Date	Data End Date	Event Count	Location Count
James SMITH	07700900177	4791322 2021.csv	29/08/2021 10:04	05/09/2021 16:19	334	147
James SMITH	07700900177	4791323 2021.csv	29/08/2021 11:47	05/09/2021 16:55	504	190
James SMITH	07700900177	4791324 2021.csv	29/08/2021 12:32	05/09/2021 17:01	343	180
David WILLIAMS	07700900597	4791417 2021.csv	14/08/2021 10:57	02/09/2021 22:51	373	82
David WILLIAMS	07700900597	4791418 2021.csv	14/08/2021 10:57	02/09/2021 23:07	369	132
David WILLIAMS	07700900597	4791422 2021.csv	14/08/2021 00:00	02/09/2021 22:38	686	351
Paul TAYLOR	07700900621	90743 CDQ 2021.csv	14/08/2021 10:08	11/09/2021 16:35	1530	127
		Cell Address Data - GN01.xls	01/01/0001 00:00	31/12/9999 23:59	0	741

There are no filters or controls associated with the report, it simply lists all imported files in the case and shows relevant information, as indicated in the screengrab.

The report can be output in a variety of formats (including Excel, Word, CSV and PDF) via the Print/Export button.

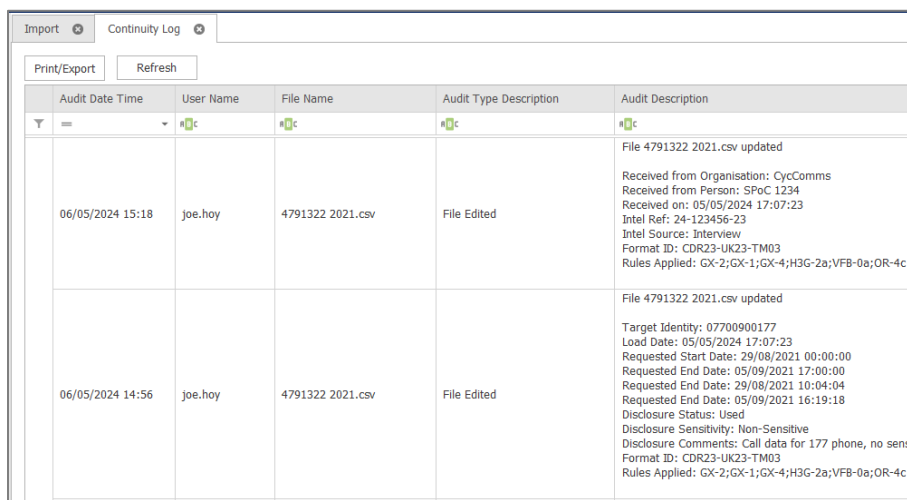
18.3 Continuity Log



A dialog box titled 'Continuity details' with a close button (X) in the top right corner. It contains several input fields: 'Received from org.' with the value 'CycComms', 'Received from person' with 'SPoC 1234', 'Received method' with a dropdown menu showing 'FTP/Internet', 'Received on' with a date/time dropdown showing '05/05/2024 17:07:23', 'Intel Ref.' with '24-123456-23', and 'Intel Source' with 'Interview'. At the bottom left is a green question mark icon, and at the bottom right are 'Save' and 'Cancel' buttons.

Case continuity information can be optionally added to a CSAS case via the 'Set continuity details' option in the Import Files grid right-click menu; the types of continuity information that can be added include details of the source of each file, when it was received, how it was received and so on.

Manually added continuity details and details that are added automatically (relating to the import/deletion of files, any Update File Details actions that are taken, etc), are displayed in the Continuity Log.



A screenshot of the 'Continuity Log' window. It has a tabbed interface with 'Import' and 'Continuity Log' tabs. Below the tabs are 'Print/Export' and 'Refresh' buttons. The main area is a table with the following columns: 'Audit Date Time', 'User Name', 'File Name', 'Audit Type Description', and 'Audit Description'. There are two rows of data.

Audit Date Time	User Name	File Name	Audit Type Description	Audit Description
06/05/2024 15:18	joe.hoy	4791322 2021.csv	File Edited	File 4791322 2021.csv updated Received from Organisation: CycComms Received from Person: SPoC 1234 Received on: 05/05/2024 17:07:23 Intel Ref: 24-123456-23 Intel Source: Interview Format ID: CDR23-UK23-TM03 Rules Applied: GX-2;GX-1;GX-4;H3G-2a;VFB-0a;OR-4c
06/05/2024 14:56	joe.hoy	4791322 2021.csv	File Edited	File 4791322 2021.csv updated Target Identity: 07700900177 Load Date: 05/05/2024 17:07:23 Requested Start Date: 29/08/2021 00:00:00 Requested End Date: 05/09/2021 17:00:00 Requested End Date: 29/08/2021 10:04:04 Requested End Date: 05/09/2021 16:19:18 Disclosure Status: Used Disclosure Sensitivity: Non-Sensitive Disclosure Comments: Call data for 177 phone, no sens Format ID: CDR23-UK23-TM03 Rules Applied: GX-2;GX-1;GX-4;H3G-2a;VFB-0a;OR-4c

There are no filters or controls associated with the log, it simply lists all continuity events, as indicated in the screenshot.

The report can be output in a variety of formats (including Excel, Word, CSV and PDF) via the Print/Export button.

19 Case Audit

Criminal investigators and analysts are required to maintain activity logs and 'contemporaneous notes' of the actions they take during an investigation. These logs and notes might be requested to be submitted to court to prove that the correct steps and processes were followed.

CSAS maintains logs of all significant actions undertaken by a user while a case is being worked on and those logs can be viewed in the Case Audit screen.

Case Audit data begins to be captured when a case is first opened and is added to each the case is accessed and each time significant work is done. The types of action that are captured by Case Audit include importing new files, deleting case files, adding/amending/deleting attributions, creating Case Outputs documents, running Analytics queries and so on.

The 'Audit' function is accessed via the  button from the CSAS home pane. Click on the  button to open the 'Audit' screen:

19.1 Layout

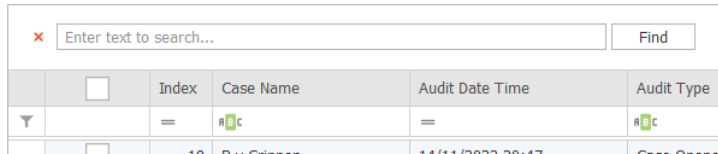
		I...	Case Name	Audit Date Tl...	Audit Type	Audit Description	User N...	Team N...	Case Mode	Source Data
			1 R v Crippen	08/11/2023 1...	Case Added	Case: R v Crippen has been added	joe.hoy	Default...	Local	
			2 R v Crippen	08/11/2023 1...	Case Opened	Case R v Crippen has been opened	joe.hoy		Local	
			3 R v Crippen	08/11/2023 1...	File Loaded	File 90743 CDQ 2021.csv has been loaded	joe.hoy		Local	
			4 R v Crippen	08/11/2023 1...	File Loaded	File 4791322 2021.csv has been loaded	joe.hoy		Local	
			5 R v Crippen	08/11/2023 1...	File Loaded	File 4791323 2021.csv has been loaded	joe.hoy		Local	
			6 R v Crippen	08/11/2023 1...	File Loaded	File 4791324 2021.csv has been loaded	joe.hoy		Local	
			7 R v Crippen	08/11/2023 1...	File Loaded	File 4791417 2021.csv has been loaded	joe.hoy		Local	

The Case Audit screen provides a simple list showing the actions taken, who by and when, with columns showing:

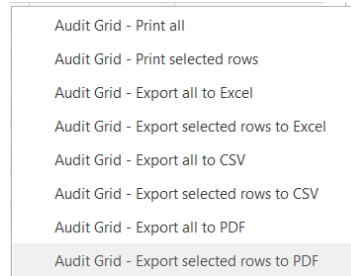
- » Event index number – each event is sequentially numbered within a case.
- » Audit Date Time – the date/time of the event.
- » Audit Type – the type of event.
- » Audit Description – additional narrative details of the action.
- » Username – the logged in user who performed the action.
- » Team name – the user's team (in standalone deployments this will always be set to 'default team').
- » Case Mode – shows whether CSAS was operating in standalone (local) mode or server mode at the time the action was performed.
- » Source Data – lists the names of any files that were imported or deleted.

19.2 Filters & Controls

In addition to the standard CSAS grid controls (see [Grid Filtering and Controls](#)), the Case Audit screen has the Find Panel permanently displayed, making it simpler to run searches of the audit data.



At the bottom right of the screen there is a Print/Export button, which allows audit content to be exported in a variety of formats, including Excel, CSV and PDF.



To use any of the 'export selected...' options, first use the checkbox column at the left of the grid to select the rows to export.

The 'Refresh' button updates the audit grid with any new events that have been captured since the Case Audit screen was opened.

As with other grids in CSAS, the Case Audit grid is flexible, allowing you to:

- » Drag individual columns around the window to manipulate the grid display.
- » Sort a column to display in an ascending order or descending order.
- » Open a filter menu by right-clicking in the header of any column.

It is not possible to save customised layouts for future use.

Why, When, Who

	This function is necessary to audit the application.
	This function is undertaken as required.
	This function is typically carried out by the following users:
	» CSAS User.

Stepped Procedure

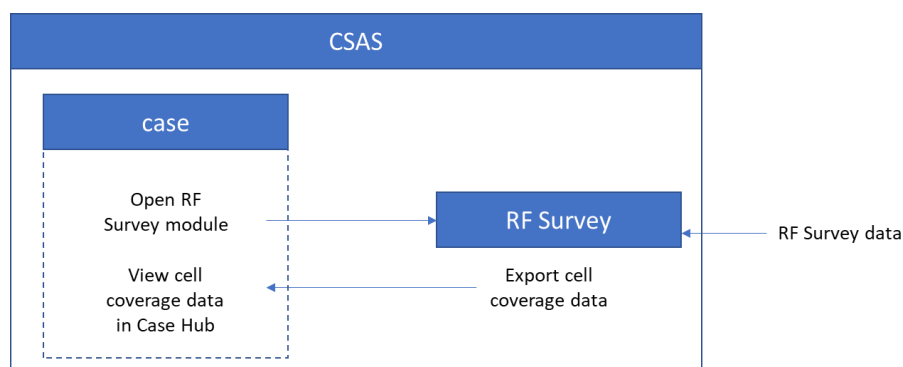
None.

20 RF Survey

CSAS is able to visualise cell coverage areas in several different ways, one of which involves importing RF Survey data and linking it to the cells displayed in Case Hub maps.

The import and filtering of RF Survey data is handled by the separate CSAS RF Survey module, which is a separately licensed add-on feature in CSAS. If licensed, the CSAS RF Survey module can be launched from within a CSAS case via the navigation dropdown menu - the last item on which will be 'RF Survey'.

Once RF Survey data has been imported into a case, it can be viewed in Case Hub maps as another option from the cell site right-click menu, cell coverage options.



Instances of CSAS with a valid RF Survey licence also provide access to an RF Survey tab in the Case Hub details panel, from where you can view details of cells that have had RF coverage details in the map and can also search for coverage of cells via their cell ID.

If you don't have CSAS RF Survey licence and you are authorised to get one, talk to your CSAS administrator or Forensic Analytics account manager to discuss obtaining an RF Survey Licence Code. To add a licence once you've received a code, see *About/Licensing*.

20.1 RF Survey Module

Once activated, the RF Survey Module add-on can be used to import raw survey data from a variety of popular forensic survey devices, including:

- » Group 2000 Lima cell monitor
- » Rohde & Schwarz TSMA*
- » Keysight NEMO*
- » First Forensics Forensic Compass
- » QRC ICS
- » 3GForensics CSurv MuNST
- » Network Cell Info (Android app).

*TSMA has many combinations of output column formats, CSAS does not accept all possible column layouts

**Raw NEMO data must be mediated using a macro before importing.

The CSAS RF Survey Module imports, processes, tabulates and summarises raw forensic survey data before outputting it into a variety of report types and maps. The main types of survey scenario that are supported include:

- » Location surveys – which seek to show the set of cells that serve at and around a specific location.
- » Cell coverage surveys – which seek to show the serving footprint area of individual cells.
- » Route (or scenario) coverage surveys – which seek to show the progression of cells that provide coverage along a route or in other specific scenarios.

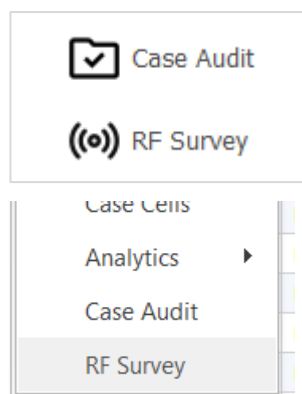
Reports can be generated for specific network/technology combinations, or CSAS RF Survey can produce 'all network/technology' profiles, which capture details of all cells, from all networks that were detected at a surveyed location.

Detailed information about what the RF Survey Module does and how it does it is given in the CSAS v3 RF Survey Module User Guide.

20.1.1 Opening the RF Survey module

To open the RF Survey, first open the CSAS case associated with the RF Survey data.

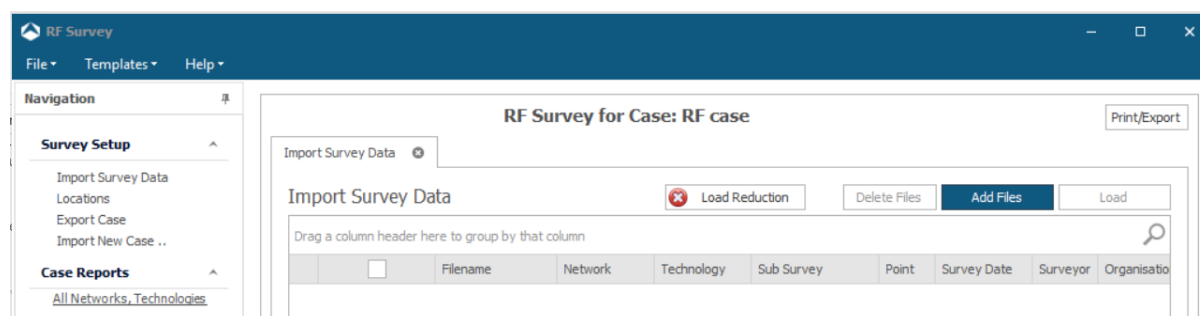
The click on the RF Survey icon in the left sidebar case navigation panel...



... or open the case navigation dropdown in the top row menu list and select 'RF Survey'.

If RF Survey isn't listed in the case navigation menu it means that the RF Survey feature is not licensed on that instance of CSAS.

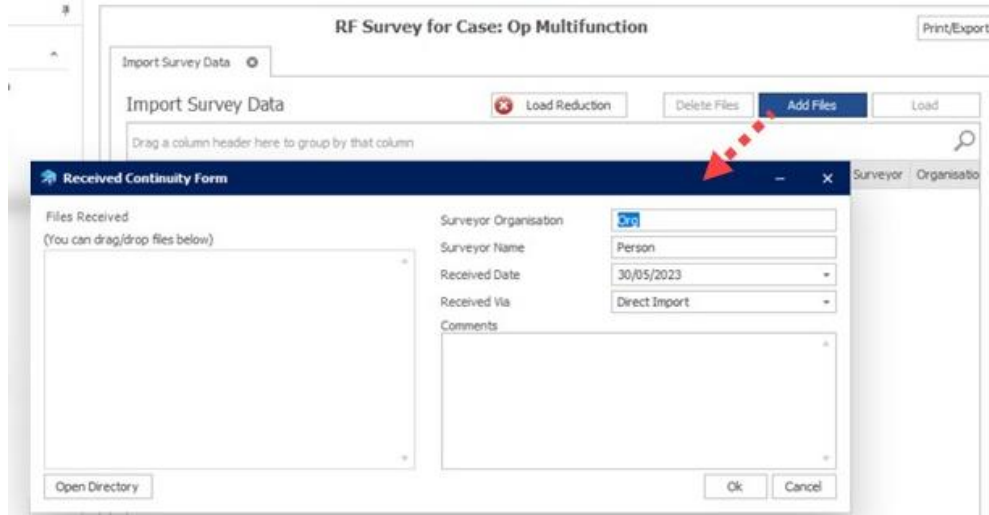
If it is available, the CSAS RF Survey module will open directly into the Import Survey Data screen.



20.1.2 Importing RF Survey Data

Stepped Procedure

1. From the 'Import Survey Data' tab, click the **Add Files** button. The 'Received Continuity Form' pop-up window opens:

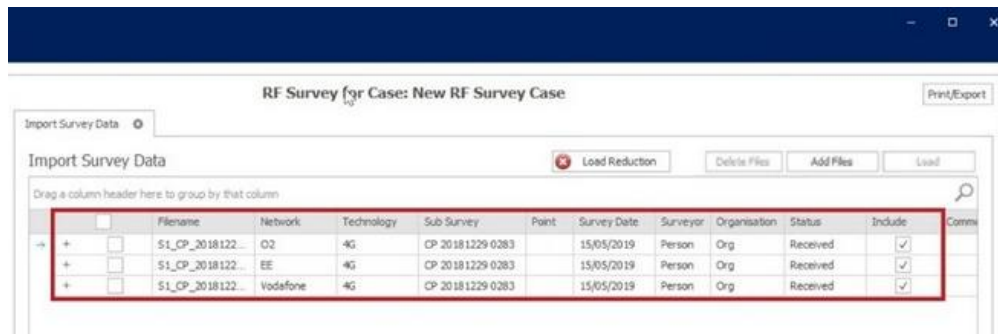


2. From the 'Received Continuity Form' pop-up window, click the **Open Directory** button. A Windows File Explorer pop-up window opens.
3. From the file Explorer pop-up window, select the RF Survey source data file(s) you want to Import into the case then click the **Open** button. The file Explorer pop-up window closes and the 'Received Continuity Form' is displayed showing the file(s) you selected in the 'Files Received' panel:



Note: You can also drag-and-drop the selected file(s) from an open File Explorer window directly into the 'Files Received' pane.

4. For the RF Survey source data file(s) you have imported, using the fields and drop-down calendar and menus, you can optionally enter the necessary continuity details - Surveyor Organisation, the Surveyor Name, the Received Date, the Received Via type (for example, email, memory card, CD/DVD etc.), and any Comments – if required.
5. Click the **Ok** button. The 'Received Continuity Form' closes, the file import process begins and a timer is displayed.
6. Once the file(s) have been selected they are listed in the grid – any issues with the imported files will be highlighted at this stage:



7. To start loading the Survey Data, click the **Load Files** button.
8. The RF Survey data will be parsed and added to the case database. The progress of the import process is indicated in the bottom left of the RF Survey screen.
9. Once the process is complete, the imported files will be listed in the Import Survey Data grid with a status of 'loaded'.

20.1.3 Exporting Data to View in Case Hub

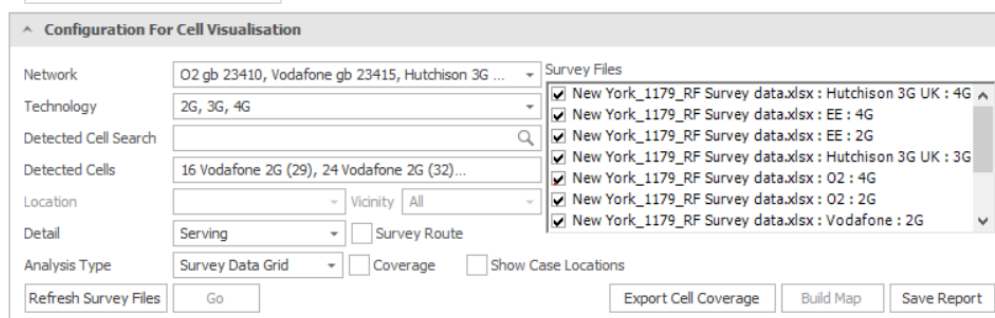
The imported data is now available to be viewed and mapped in the RF Survey Module, please see the CSAS RF Survey Module user guide for more details of the features available in that product. These instructions focus only on the process required to view RF Survey data in case Hub.

Stepped Procedure

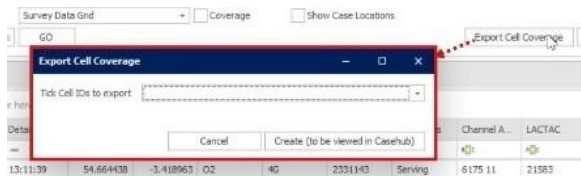
1. Still in the RF Survey module and in the same case that the data was imported into – in the RF Survey left sidebar, go to 'Cell Visualisations' section and select 'Custom Reports':



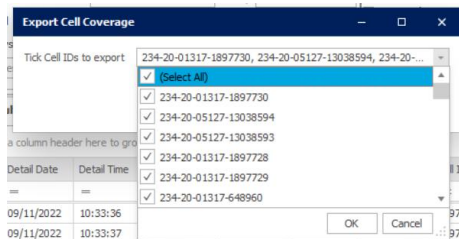
This option opens a menu that allows you to select cell coverage data for all detected cells across all networks and all technologies – this is the simplest way of ensuring that data for all detected cells is exported for viewing in Case Hub.



2. Click the **Refresh Survey Files** button and then the **GO** button. The grid in the RF screen populates with the selected source data.
3. Click the **Export Cell Coverage** button. The 'Export Cell Coverage' pop-up window opens:



- From the 'Export Cell Coverage' pop-up window, select the 'Tick Cell IDs to export' drop-down menu, and tick the 'Select All' checkbox:



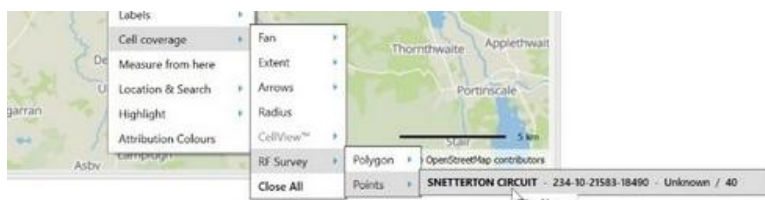
- Click the **OK** button to confirm your selection.
- Click the **Create (to be viewed in Casehub)** button. Cell coverage data for all detected cells will be exported in a format that Case Hub can use.

20.1.4 Viewing RF Survey coverage data in Case Hub

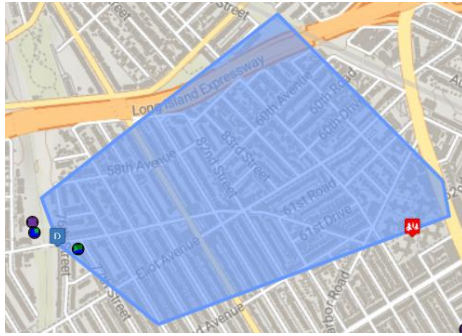
The expectation is that the RF Survey data you imported in the previous section is linked to the CDR data you've imported into your CSAS case – meaning that some of the cells found in your CDR data will have been surveyed as part of the RF Survey data and that coverage details of those cells can be viewed in Case Hub.

Stepped Procedure

- Select the file(s) to be viewed in Case Hub from the Source Data menu in the right sidebar, click 'Apply' to send the data into Case Hub and, if necessary, click the manual or auto sync buttons to view the data in the map.
- If you wish to view the RF Survey coverage for a specific cell, find the cell site icon in the map, right-click and select Cell Coverage > RF Survey.
- The RF Survey sub-menu offers two options – 'polygon' and 'points' – from which you can then select and individual cell to view:

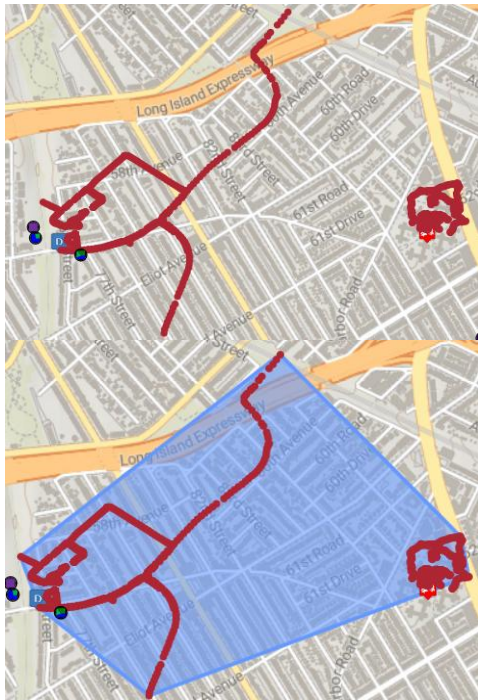


- The 'polygon' option displays cell coverage data in much the same way as CellView does.



The process calculates the total area within which the selected cell was detected in the associated RF Survey files and draws an outline around it. This option offers a simple visualisation of cell coverage, that provides an indication of the general coverage area for non-technical reports.

5. The 'points' option displays more detailed cell coverage data.



The process indicates each spot where the RF Survey device detected the selected cell as a serving cell. The sequence of dots provides an exact representation of the places where the selected cell was detected as serving. This option is more appropriate for more technical reports and examinations.

It's also possible to select both options and view the survey points enclosed in a polygon:

6. Details of the currently visible set of RF coverage visualisations are displayed in the RF Survey tab in Case Hub. A visualisation can be dismissed by rerunning the process and clicking on the menu option in the points or polygons sub-menu or by deselecting the cell ID in the list in the RF Survey tab.

20.2 RF Survey Tab

If your instance of CSAS has been licensed to use the RF Survey capabilities, the RF Survey tab will be visible in the Case Hub details panel.

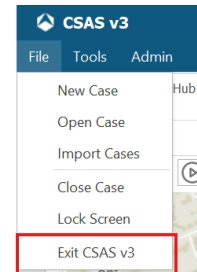
To view the details of the RF Survey tab, please see [RF Survey](#).

21 Logging Out and Closing CSAS

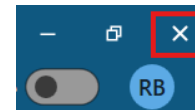
This function allows you to log out of CSAS, release the current floating licence if you have one and close the software.

There are three ways you can log out of and close CSAS:

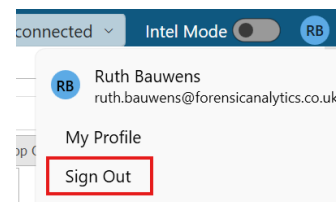
Using the 'File' tab in the top left of the application window:



Using the 'X' in the top right of the application window:



Using the profile icon in the top right of the application window:



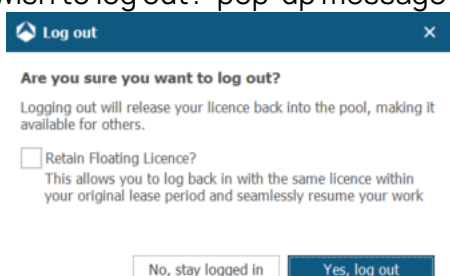
If you have a case open when you exit CSAS, all case data will be saved before the exit happens, so there should be no opportunity for unsaved data to be lost.

Why, When, Who

	This function is necessary to enable you to log out and close CSAS
	This function is undertaken whenever you log out of and close CSAS and for users who are using a floating licence.
	This function is typically carried out by the following users: >> CSAS User.

Stepped Procedure

1. To sign out of CSAS, select one of three ways shown above. The 'Are you sure you wish to log out?' pop-up message window opens:



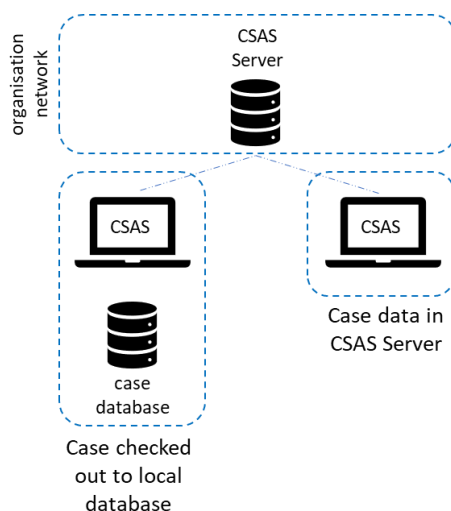
2. Optionally select to retain the floating licence if applicable.
3. Click on the “Yes, log out” button. The pop-up message window closes and the CSAS application closes.

22 Hybrid Mode

CSAS can currently be deployed in two main configurations:

- » Standalone mode – where all processing is undertaken on the local machine and data is held locally in a CSAS database created on the user's local machine.
- » Hybrid mode – where all processing takes place locally, but the user has the choice to keep cases saved to their local CSAS database or to upload them to their organisation's CSAS Server, where they can be centrally archived or shared with other authorised users.

In Hybrid mode, a shared case database is stored on CSAS Server and the main user, team and case administration functions are handled via CSAS Server, but cases can also be downloaded and stored on the user's local machine, which can be beneficial in the event of slow network connections or congested servers.



The 'hybrid' aspect of this mode refers to the ability to choose where the data for specific cases is stored – either centrally in the organisation's CSAS Server or locally, with the case checked out and the data stored on the user's PC.

Running cases with the data stored on the server allows cases to be shared – the case owner has full read/write permissions for the case and other authorised users can have concurrent read only access – this makes case sharing simpler.

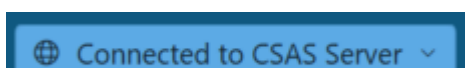
However, if the organisation has a slow or congested network, working in 'online' mode in this way can be frustrating, as there may be delays associated with uploading and downloading case data.

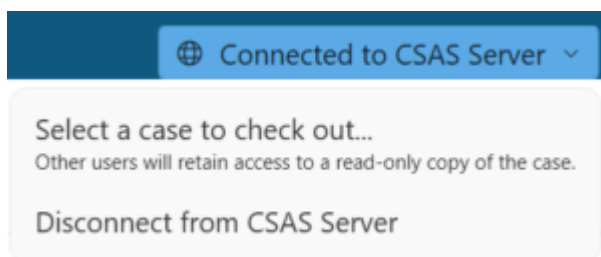
The other hybrid option is to work 'offline' on cases with the data stored in the local CSAS database – the case can be worked on without suffering delays, but working offline also means that the case cannot be concurrently shared with other users.

22.1 Switching Modes

Users can switch between modes using the CSAS Server connection controls in the top row of the CSAS application window.

The control indicates if users are currently connected to CSAS Server and able to access case data in CSAS Server or disconnected and using a local database.





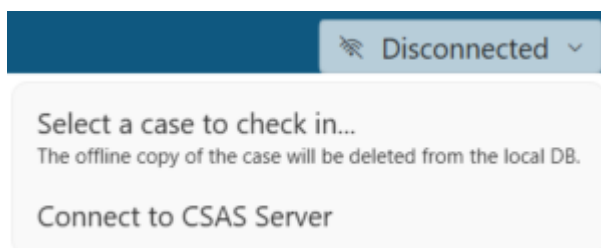
When selected, two options are offered:

- » Select case to check out
- » Disconnect without a case

If 'Select a case to take check out' is chosen, a list of available server cases is presented for the user to choose from – check the box for the required case and click 'Take offline' – the selected case will be downloaded to the local CSAS database ready to be worked on offline.

If 'Disconnect from CSAS Server' is selected, CSAS simply disconnects from CSAS Server without downloading any cases – any cases that have previously been downloaded or that were created offline will be available to be worked on.

When disconnected from CSAS Server, use the same control to connect to CSAS Server again.



Two options are offered:

- » Select a case to check in
- » Connect to CSAS Server (Without checking in a case)

If 'Select a case to check in' is chosen, a list of available local cases is presented for the user to choose from – the selected case will be uploaded to the CSAS Server database ready to be worked on online.

If 'Connect to CSAS Server' is chosen, CSAS simply connects to CSAS Server without uploading any cases – any cases that have previously been uploaded or that were created online will be available to be worked on.

CSAS instances that are configured to work in Hybrid mode will initially open connected to CSAS Server – users will need to select to disconnect to work locally. Once CSAS switches disconnects from CSAS Server, it stays in that configuration, even if CSAS is closed and reopened, until the user elects to return to online mode again.

22.2 Online Mode

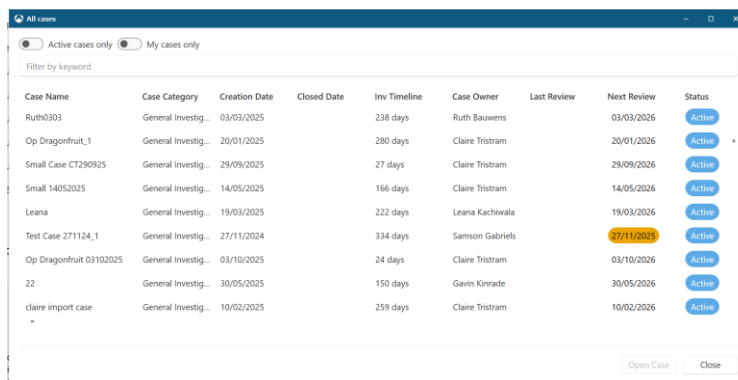
When operating in online or 'Server' mode, CSAS is connected to the organisation's CSAS Server and functions related to the storing of case data and administration are managed via the server. This means that some functions operate slightly differently than they do in offline or Standalone mode.

22.2.1 CSAS Login

Initial log in is handled via the server, also deployments that operate in online/server mode often also use floating licences. This means that there may be a slight delay during log in as CSAS contacts both servers (CSAS Server and Floating Licence server) to exchange details. CSAS login in server mode is only possible if the host PC is connected to a network that provides access to the server, so users operating away from their office may need to use their organisation's VPN or other remote access method to gain access to CSAS Server cases and features.

22.2.2 Open Cases

When connected to CSAS Server, the Open Cases screen displays details of all cases you have access to.



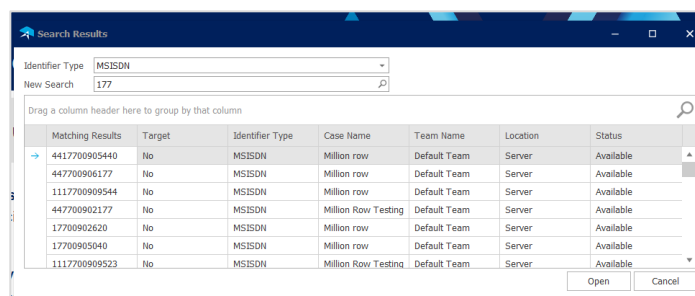
Case Name	Case Category	Creation Date	Closed Date	Inv Timeline	Case Owner	Last Review	Next Review	Status
Ruth0303	General Investig...	03/03/2025		238 days	Ruth Bauwens		03/03/2026	Active
Op Dragonfruit_1	General Investig...	20/01/2025		280 days	Claire Tristram		20/01/2026	Active
Small Case CT290925	General Investig...	29/09/2025		27 days	Claire Tristram		29/09/2026	Active
Small 14052025	General Investig...	14/05/2025		166 days	Claire Tristram		14/05/2026	Active
Leana	General Investig...	19/03/2025		222 days	Leana Kachiwala		19/03/2026	Active
Test Case 271124_1	General Investig...	27/11/2024		334 days	Samson Gabriels		27/11/2025	Active
Op Dragonfruit 03102025	General Investig...	03/10/2025		24 days	Claire Tristram		03/10/2026	Active
22	General Investig...	30/05/2025		150 days	Gavin Kinnade		30/05/2026	Active
claire import case	General Investig...	10/02/2025		259 days	Claire Tristram		10/02/2026	Active

Users can use the two toggles at the top of the screen to restrict the list to their own cases or two active cases.

They can also search for a specific case using the filter bar.

22.2.3 Case Search

The Case Search results popup will display details of cases that you have access to in which the search term was found, whether they're checked out and saved to the local database or if they're saved to the server database.



Matching Results	Target	Identifier Type	Case Name	Team Name	Location	Status
4417700905440	No	MSISON	Million row	Default Team	Server	Available
447700906177	No	MSISON	Million row	Default Team	Server	Available
1117700909544	No	MSISON	Million row	Default Team	Server	Available
447700902177	No	MSISON	Million Row Testing	Default Team	Server	Available
17700902620	No	MSISON	Million row	Default Team	Server	Available
17700905040	No	MSISON	Million row	Default Team	Server	Available
1117700909523	No	MSISON	Million Row Testing	Default Team	Server	Available

The 'Location' column indicates the database the case is saved to, with options of 'Local' and 'Server'.

22.2.4 Creating a New Case

When creating a new case in server mode, the selected Team and Security Level are potentially more important than they are in Standalone mode. Please ensure that you choose the correct Team and SL for each case.

22.2.5 Opening an Existing Case

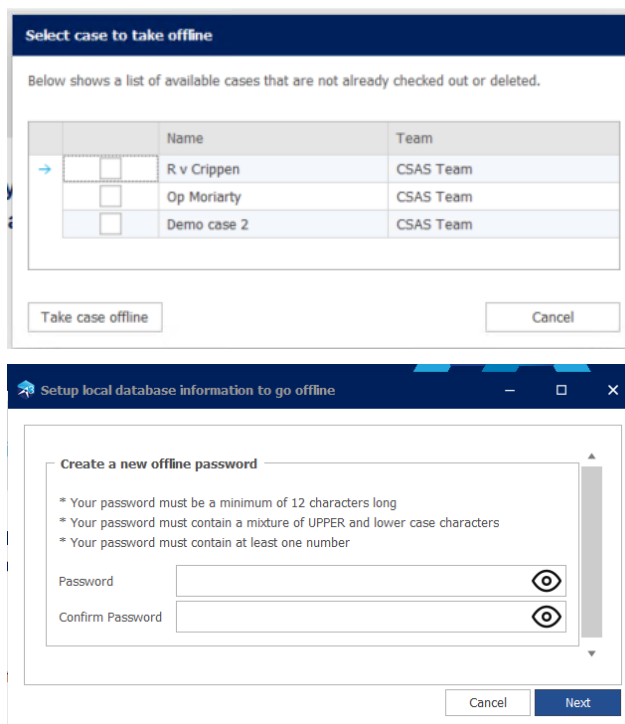
When opening an existing case, CSAS will access the server and download the selected case data ready to be worked on. Any imported data will be parsed locally, in your copy of CSAS, and the parsed data will be uploaded to the server database. Depending on the speed of your network connection, these actions may take slightly longer to complete

than they would in Standalone mode.

22.2.6 Checking Out a case

If your user profile and CSAS Server configuration allow it, it may be possible to check a case out, which entails downloading it from the server database to your PC and running it from the local CSAS case database. You must be the case owner to take a case offline.

Case download can be triggered using the CSAS Server connection drop down button and selecting 'Select a case to check out'. This launches the 'select case to take offline' popup, which lists the cases that are available for you to take offline – you can only take one case offline at a time.



Select case to take offline

Below shows a list of available cases that are not already checked out or deleted.

	Name	Team
☐	R v Crippen	CSAS Team
☐	Op Moriarty	CSAS Team
☐	Demo case 2	CSAS Team

Take case offline Cancel

Setup local database information to go offline

Create a new offline password

- * Your password must be a minimum of 12 characters long
- * Your password must contain a mixture of UPPER and lower case characters
- * Your password must contain at least one number

Password

Confirm Password

Cancel Next

Select the case to download by checking the appropriate checkbox and clicking 'take case offline'.

If you have never worked offline before, CSAS will create a new local database for the downloaded case, the username will be the same as the one you use to access CSAS in server mode, which will usually be your organisational email address but you'll be asked to set the password to use to access CSAS in offline mode.

In the interests of operational security, please do not reuse your CSAS Server password. You'll also be asked to set three password reset questions, to be used if you forget the password to the local database.

The case will then be downloaded. You'll be asked to log in to CSAS again, using the local database password you've just created, when the case is ready to work on.

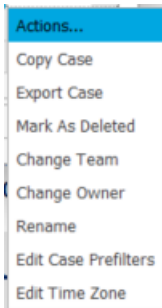
Once the local database has been created, it will persist, allowing you to create new offline cases and download additional server cases to the local database.

22.2.7 Managing Cases

The Admin > Manage Cases menu offers a range of options that allow you to manage the cases you control.

In online mode, the Manage Cases menu lists all cases that you have access to, whether as case owner or as a team member with read only access.

Case Name	Creation Date	Owner Username	Owner Fullname	Security Level	Team	Time Zone	Checked out?	Marked for deletion?	Deletion After	Actions
Investigation Case	08/05/2025	Ruth.bauwens@fore...	Ruth Bauwens	5	Default Team	Europe/London	☐	☐		Actions...
Op Dragonfruit 5	20/01/2025	Ruth.bauwens@fore...	Ruth Bauwens	1	Default Team	Europe/London	☒	☒		Actions...



For cases that you own and have full control of, the Actions dropdown offers the full range of administrative functions, allowing you to copy, export, delete and rename cases, to assign the case to a new Team or case owner and to edit any case prefilters and its timezone.



If you are not the case owner, you have a more abbreviated set of case management options, which allow you to create a copy of the case (which you would then be the owner of and have full control of) or export the case to a zip folder.

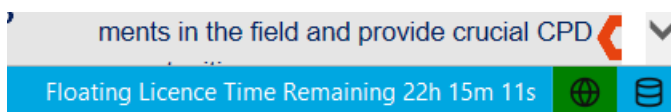
A similarly limited set of options exist for cases that you are the owner of but which have been downloaded to your local database. Full control is only possible once the case has been uploaded to CSAS Server again.

22.2.8 Checking out a Floating Licence

If you downloaded the case to be able to work on it offline, you may also need to check out a floating licence (if your instance of CSAS isn't using a dedicated licence). Please see [Floating Licence Checkout](#) for more details.

22.2.9 Checking server connection & case status

In server mode, you can check the state of your connection to CSAS Server and the states of the cases you have access to by clicking on the 'globe' icon at the right of the bottom CSAS taskbar.



The globe icon is green when you are connected to CSAS Server and orange when you are disconnected or are working on a downloaded case.

File	Local File Availability	Server File Availability
ID test case R v Crippen data	Read Only - not available locally	Read Only
Import GN02	Read Only - not available locally	Read Only
intel mode case	Downloaded - available locally	Full Access
keith test 1	Read Only - not available locally	Read Only
MDE 2	Read Only - not available locally	Read Only
Million row	Read Only - not available locally	Read Only
Million Row Testing	Read Only - not available locally	Read Only
NMPR Demo	Read Only - not available locally	Read Only
NWROCU TEST	Read Only - not available locally	Read Only
Ogilvie	Read Only - not available locally	Read Only

Clicking on the globe icon launches the CSAS Resources popup.

The 'test connection' button reports the status of the server connection.

The 'refresh' button refreshes the case list.

The 'download templates and patches' button triggers CSAS to check for parsing and

template updates.

The case list shows the set of cases to which you have access and shows the availability of each case in both the local database and the server database.

Cases that have been checked out will be shown as 'downloaded – available locally', cases that are saved to the server will be shown as 'not available locally'. If you are the case owner you will be shown as having 'full access', if you are not the case owner, you will be shown as having 'read only' access.

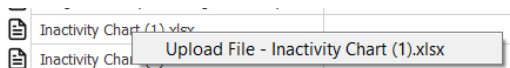
Clicking on the arrow to the left of a case name, opens the list to show details of the subfolder and files associated with the case.

File	Local File Availability	Server File Availability
intel mode case	Downloaded - available locally	Full Access
Images		
Imports		
EE intel mode examples.xls	✓	✓
VF intel mode examples.xls	✓	✓
Outputs		

Files that are available for you to view either locally or on the server are shown with a green tick.

File	Local File Availability	Server File Availability
taunton Shooting (Copy)	Read Only - not available locally	Read Only
Images		
ANPR1.png		!
Imports		
anonymised_CDR_2.xls		!
handset download 3852.xlsx		!

Files that aren't available for you to view, either because you have 'read only' access or because they haven't been downloaded, are shown with a red exclamation mark.



If a file exists locally but isn't saved to the server, you can trigger the manual upload of the file by right-clicking and selecting 'upload file'.

If you work in a hybrid mode, with some server-based cases worked on and some downloaded cases worked on, the CSAS Resources popup offers a set of options that allow you to manage their synchronisation state. If, for whatever reason, some imported source files or created outputs for a case haven't been uploaded to the server, the upload can be manually triggered from here.

22.3 Offline Mode

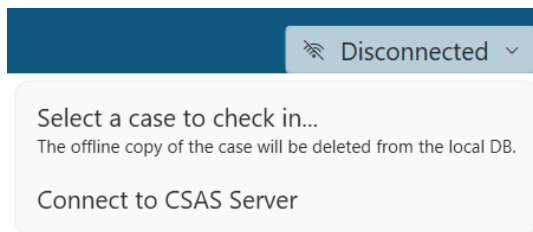
When CSAS is in offline mode, all user administration and case management is handled locally, using the local CSAS database.

The operation of CSAS will be essentially the same as for a copy that was deployed in Standalone mode, which is described elsewhere in this user guide.

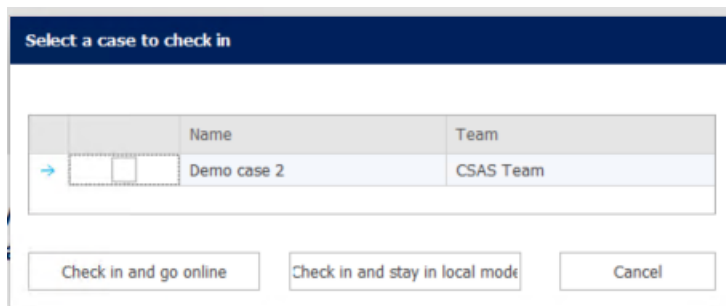
22.3.1 Switching back to online mode

When you've finished working in offline mode, whether you wish to check a case in or not,

you can begin to connect to CSAS Server using the CSAS Server connection drop down button.



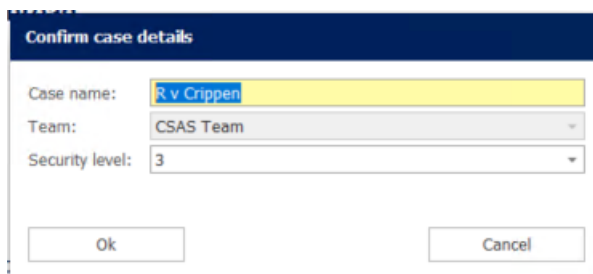
You'll be asked whether you want to check a case in or just connect to CSAS Server without checking in case.



If you have an offline case that you wish to check back into the server, select it from the popup list by checking the appropriate row.

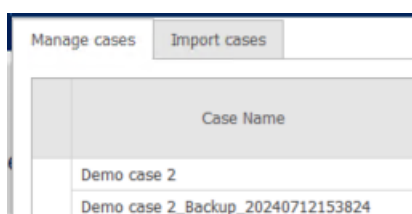
If you're checking the case back in because you wish to work on it online, or because you've finished working on that case and want to save it to the server, select 'Check in and go online'.

If you want to check the case in to save it to the server but wish to continue working offline on a different case, select 'Check in and stay in local mode'.



If you elected to check a case in, you'll be asked to confirm the case name, Team and security level for the case.

If the case name is not unique (i.e. if the server already contains a case with the same name), you'll be warned and asked if you want the uploaded case to overwrite the existing server case. If you don't want to overwrite the existing server case, you can choose a different name for the case you are checking in.



If you do elect to overwrite the existing case, a copy of the current server version will be stored on the server suffixed with '_backup' and the current date.

The case data will then be uploaded to the server and the case will be checked back in. Once the upload is complete, CSAS will restart back in server mode.

22.4 CSAS Server Administration

CSAS Server is used to administer users and Teams and will eventually also be able to

manage cases.

22.4.1 Logging in to CSAS Server

The administrative interface for CSAS Server is accessed via a browser – you can either type the server address directly into the browser or you can go via the Admin > Server Admin menu option. You will need to be connected to a network that has access to your instance of CSAS Server.

You will need to log in to CSAS Server using the authentication method employed by your deployment (local username password, Active Directory, Azure AD). Only authorised CSAS admins will be provided with access to CSAS Server, please contact your local IT support team to arrange this. CSAS Support has no access to customers' CSAS Server deployments.

The CSAS Server home page offers three options – home, admin and help.

The Home option returns to the home page. There are no other options on the home page.

Admin offers two submenus – User Admin and IT Admin.

User Admin (individual users)

The User Admin screen supports three controls and an information panel.

Users						View all users
Username	Name	Locked?	CSAS Server Access	CSAS Desktop Access	Actions	
user1@forensicanalytics.co.uk	user1	☐	☒	☒	Edit User Suspend User	
username123@forensicanalytics.co.uk	username123	☐	☒	☒	Edit User Suspend User	
username234@forensicanalytics.co.uk	username234	☐	☒	☒	Edit User Suspend User	

Showing 5 of 36 active users

[Add a user](#)

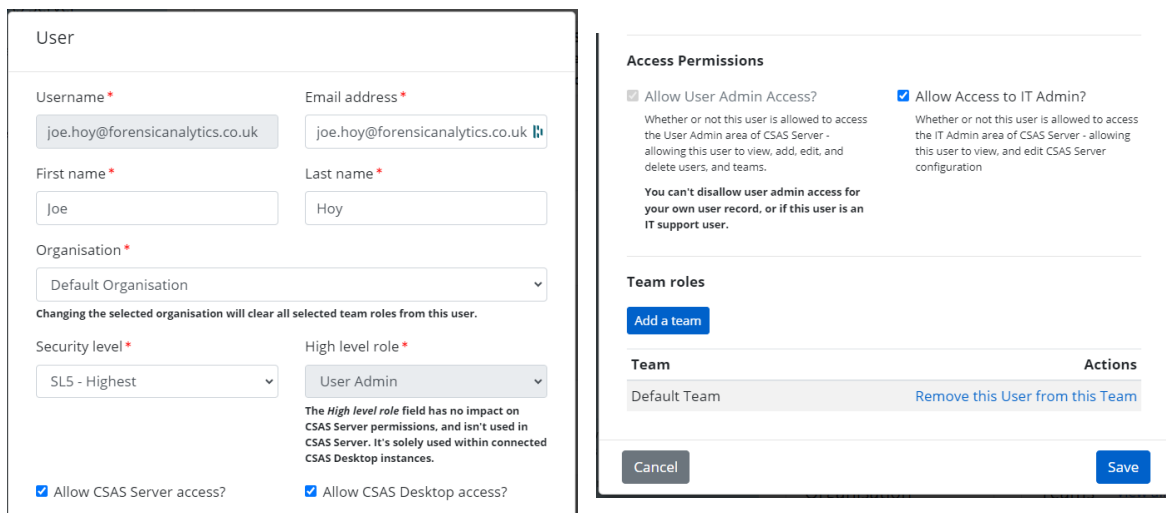
Users

The Users menu lists the set of registered users for the server – only users who are listed here will be able to access this instance of CSAS Server from their copies of CSAS.

- » The list by default shows the first 5 user accounts, to view all user accounts, click 'View all users'.
- » Each registered user is listed in their own row.
- » To edit a user, click 'Edit User', see below.
- » To temporarily prevent a user from accessing their CSAS and CSAS Server service, click 'Suspend User' – you'll be asked which services you wish to suspend them from.
- » In 'View all users' mode, the edit/suspend links are replaced by an Actions menu button, which provides access to a further option of 'Reset identity questions'. Selecting this will cause the user to have to re-enter their 'forgotten password' hints the next time they log in.
- » To Add a new user click 'Add a user'.

Add/Edit User

If you select to Add a new user or Edit an existing one, you'll see the following screen, which has been split in two halves to fit the page:



User

Username * Email address *

First name * Last name *

Organisation *

Changing the selected organisation will clear all selected team roles from this user.

Security level * High level role *

The High level role field has no impact on CSAS Server permissions, and isn't used in CSAS Server. It's solely used within connected CSAS Desktop instances.

☒ Allow CSAS Server access? ☒ Allow CSAS Desktop access?

Access Permissions

☐ Allow User Admin Access? ☒ Allow Access to IT Admin?

Whether or not this user is allowed to access the User Admin area of CSAS Server - allowing this user to view, add, edit, and delete users, and teams.

Whether or not this user is allowed to access the IT Admin area of CSAS Server - allowing this user to view, and edit CSAS Server configuration

You can't disallow user admin access for your own user record, or if this user is an IT support user.

Team roles

Team	Actions
Default Team	Remove this User from this Team

- » Username – the name the user will log in with, this is often their organizational email address.
- » Email address – the address to send administrative emails to.
- » First name/last name – used to identify the user in audit logs, etc.
- » Organisation – currently one instance of CSAS Server can be support one 'organisation', in later versions multiple organisations will be able to share one server deployment. Currently there will only be one option for this dropdown menu.
- » Security Level – the SL assigned to this user. They will not be able to access Teams or Cases with a higher SL, but be able to access resources with this or a lower SL.
- High Level Role – the main job this user is intended to do – it determines the actions that are available for the user within CSAS. Most users will be set as

'Standard' users. The set of role options are:

- User Admin – a CSAS Administrator with permissions to create and manage users.
 - CSAS Case Admin – an admin with permissions to manage specific cases – set case owner, unlock downloaded cases, etc.
 - Standard – a standard CSAS user.
 - Intelligence Only User – A standard user advised to use CSAS for non-evidential purposes only, in accordance with FSA - DIG 101 of the Forensic Science Regulator's Code of Practice.
 - CSAS View Only – a specific type of read-only user, who can never be a case owner.
 - IT Support – local support or CSAS Support user.
- » Allow CSAS Server access – if ticked, the user can log in to the CSAS Sever admin pages.
 - » Allow CSAS Desktop Access – if ticked, the user will be able to access the CSAS case database.
 - » Allow User Admin Access – the user will be able access the CSAS Server › Admin page to manage CSAS users.
 - » Allow Access to IT Admin – the user will be able to access the CSAS Server › IT Admin page to manage server settings.
 - » Teams – a list of the Teams the user belongs to – every user must belong to at least one Team.
 - » For each listed Team, there is the option to 'Remove user from this Team'.

Organisation

This panel displays details for the Organisation (i.e. the customer) that CSAS Server is owned by. CSAS Server currently one supports only one 'organisation', in later versions multiple organisations will be able to share one server deployment.

Organisation	
Name	Actions
Default Organisation	Edit Organisation

The organisation that is created when CSAS Server is installed is called 'Default Organisation', by clicking on 'Edit Organisation', this can be changed to a specific name (e.g. the police force name) and it also offers the opportunity set a minimum security level.

Teams

This panel lists the Teams that have been created within the Organisation. A basic team (Default Team) is created automatically, but this can be edited and additional Teams can be added via this control.

Teams [View all teams](#)

Name	Actions
Default Team	View Users Edit Team Delete Team
Ops	View Users Edit Team Delete Team
RF	View Users Edit Team Delete Team
Sales	View Users Edit Team Delete Team
SOCU	View Users Edit Team Delete Team

Showing 5 of 6 teams

[Add a team](#)

- » View all Teams opens a popup that lists all Teams, not just the top 5.
- » View Users – shows a list of CSAS Server users who have been associated with that Team.
- » Edit Team – opens the Team details for editing, see below.
- » Delete Team – deletes the Team. **WARNING** – as cases are associated with a specific Team, deleting a Team effectively deletes all cases associated with that Team (by making it impossible to access them). Please ensure that any cases that need to be retained are moved to a different Team before a Team is deleted.
- » Add a team – adds a new Team.

Add/Edit a Team

If you need to Edit and existing Team and Create a new one, the following popup appears:

Team

Name *

Default Team

Organisation *

Default Organisation

Minimum security level *

SL1 - Lowest

This is the minimum security level that users have to be to belong to this team. As an example if the minimum security level is SL3, only users who have a security level of SL3, SL4 or SL5 can be a member of this team.

Cancel

Save

The team name must be unique within the set of Teams within the organisation.

The Organisation cannot currently be selected and defaults to the only organisation for the deployment.

The minimum SL limits the Team to users and cases with at least that security level.

Active Users

This panel provides details of admin users who are currently logged in to this instance of CSAS Server.

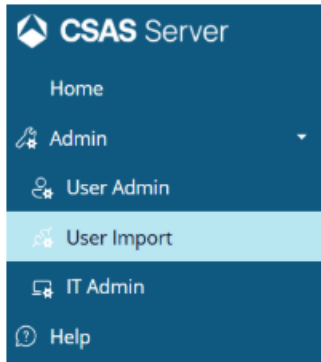
User Import (multiple users)

The User Import option provides a method for adding multiple users at once, by uploading a csv file containing the user details.

The csv file needs to be structured as follows:

Firstname, LastName, EmailAddress, Username, TeamName, HighLevelRole, SecurityLevel

With one row per user and no blank rows.



Trigger the upload by selecting User Import from the CSAS Server admin menu, this opens a Windows file explorer popup, navigate to the csv file and select it.

If the contents of the file are invalid, it will be rejected. If the contents of the file are valid, they will be displayed in the User Imports grid and any missing data will be highlighted.

Errors have been found and are displayed against the rows. Please correct and re-upload the file.

Firstname	LastName	EmailAddress	TeamName	HighLevelRole	SecurityLevel	Errors
User	One	one@forensicanalytics.co.uk	Team 1	Standard	SL5	
User	Two	two@forensicanalytics.co.uk	Team 2	Standard	SL3	
User	Three	three@forensicanalytics.co.uk	Team 4	User Admin	SL1	Invalid Team Name
User	Four	four@forensicanalytics.co.uk	Team 1	CSAS Case Admin	SL2	
User	Five	five@forensicanalytics.co.uk	Team 2	CSAS View Only	SL5	
User	Six	six@forensicanalytics.co.uk	Team 3	Standard	SL3	
User	Seven	seven@forensicanalytics.co.uk	Team 1	Standard	SL1	
User	Eight		Team 2	Standard	SL2	Empty columns found

Once all required data has been added, click 'import' to complete the process.

The imported users will be displayed onscreen and can be individually managed via the User Admin screen.

23 Training & Support

23.1 Training

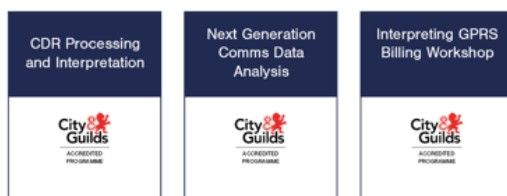
Full user training for CSAS users can be provided, as can 'train the trainer' sessions to allow organisations to manage their user training on an in-house basis. Both onsite and remote training options are offered, with remote online sessions provided via Microsoft Teams.

Initial, self-paced online training is typically offered for free as part of the CSAS licensing agreement, additional charges may apply for onsite courses.

Additional training material, online help videos and access to regular training webinars are available to registered users via the Forensic Analytics website – training.forensicanalytics.co.uk.

23.1.1 Recommended Technical Pre-requisite courses

Forensic Analytics offer a set of pre-requisite courses that provide the underpinning technical knowledge for users who are new to digital forensics and cell site analysis.



- » CDR Processing & Interpretation – provides an in-depth overview of the formatting and meaning of cellular call data records and introduces a set of hands-on methods for processing, analysing and interpreting this vital form of digital evidence.
- » Next Generation Comms Data Analysis – builds on the CDR Processing course and introduces details of the interpretation of more complex data types, such as mobile Internet data.
- » Interpreting GPRS Billing Workshop – provides a deep dive into the construction of mobile Internet billing data and offers a level of understanding of the interpretation and analysis of this data type.

23.1.2 Training Pathway for New CSAS users

The recommended training pathway for users who are entirely new to CSAS includes a suite of courses that offer progression to the CSAS 'certified user' accreditation and some of which have additional City & Guilds certification.



- » CSAS V3 Lite e-learning – a self-paced interactive e-learning course offering a basic overview of CSAS and its use.

- » CSAS V3 New User Essentials – a more in-depth introduction e-learning course that mixes a set of preparatory videos with a detailed self-paced interactive e-learning module.
- » Investigate with CSAS V3 – this course offers a mix of self-paced modules and instruction videos with a live online practical session led by a Forensic Analytics data analysis expert.
- » CSAS V3 Advanced User – this course offers a mix of self-paced modules and instruction videos with a live online practical session led by a Forensic Analytics data analysis expert.

23.1.3 Training Pathways for Existing CSAS users

The training pathway for existing CAS users, who have previous experience of using CSAS v2 and are converting to CSAS v3, is similar to that for new users but also includes an optional 'conversion' course, that highlights the similarities and differences between the old and new versions of CSAS.

23.2 Support

CSAS has been designed and developed to be simple and robust but situations may arise where users need help.

The Forensic Analytics website offers tips, advice and FAQs that should help solve most issues but if these do not help solve a problem then the CSAS Support team is available via our website or email.

CSAS Support will respond in working hours within the SLA agreed in the user's licence agreement.

The default support package included with a CSAS licence provides telephone and remote support, onsite support can be arranged via a separate maintenance agreement.

CSAS uses a variety of tools for remote support including, where permitted, Microsoft Teams and Quick Support sessions.

We recognise that remote access may not always be an appropriate support solution in cases where CSAS is being run on a computer in a sensitive location and we will endeavour to tailor the support we provide to each user's requirements.

In cases where users encounter a call data format that CSAS doesn't recognise or where call data processing is thought to be inaccurate, CSAS Support will endeavour to provide new or updated data parsing functionality as quickly as possible.

24 Troubleshooting

24.1 Help & Support

24.1.1 Where to Get Help

Help and guidance on the use of CSAS is primarily provided via this User Guide, and there are also help resources of the Forensic Analytics secure support website, including 'How To...' guides, online training courses and videos that demonstrate basic CSAS activities.

Larger customer organisations will usually have a CSAS Administrator and some also have in-house trainers who have been trained by us to support our software.

We offer basic CSAS end-user training free with each licence sale and further refresher or advanced training can be provided if required.

We also have a network of regional support associates who can be called in to offer on-site support, on-the-job training and guidance.

The first port of call for help is the CSAS website, then try the local CSAS Administrator and finally contact CSAS Support, we'll help to work through any issues and get the right support or training deployed to resolve them.

For further Help information view the Help menu options in *Top Row Buttons and Controls*.

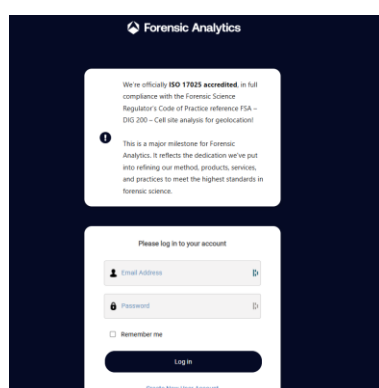
24.1.2 How To...Contact CSAS Support

CSAS Support can be contacted via our secure support website at [secure.forensicanalytics.co.uk](https://support.forensicanalytics.co.uk) (log in required). After logging in, navigate to:

<https://support.forensicanalyticscloud.com/login>

We can also be contacted via email: support@forensicanalytics.io

24.1.3 Accessing the Secure Support website



The secure support website is located at:

<https://support.forensicanalyticscloud.com/login>

Users must have a valid username and password to log in. These will have been assigned when the user's organisation signed up for CSAS.

Contact CSAS Support to get log in credentials resent or renewed.

24.2 Common Issues

24.2.1 Updating the CSAS Application

CSAS Application updates are issued at regular intervals and offer improved performance and enhanced functionality.

CSAS copies that are configured to automatically check for updates will alert you when a new version is available and will prompt you to begin the installation. If you aren't using the automated method, registered users will receive an email from CSAS Support announcing a new version and will be instructed to download it from the secure support website.

In most organisations, software updates are managed by the IT Team, so you may not be permitted to run the update process yourself.

To access a new CSAS version:

1. Log in to <https://support.forensicanalyticscloud.com/login>
2. Click on the CSAS link.
3. Click on Downloads & Updates.
4. Click on the file listed under the Application Updates link – it will typically be called 'CSAS_V3_Installer_Version_<version number>.msi'.
5. Save the file and then click to run it when requested.

For details on how to install or update CSAS, please see [Installing CSAS](#).

24.2.2 CSAS Version Numbers

In common with many other software applications, CSAS uses a four-section version number scheme in the format:

v.A.B.C.D e.g. v3.13.0.12345

Where:

- A – is the generation number and will be incremented only when a new generation of CSAS is released (e.g. CSASv3, CSAS v4).
- B – is the major release number and will be incremented when each regular (usually quarterly) version is published.
- C – is the minor release number and will be updated if an incremental release is required between major releases – for example, if a version of the major release with an updated parser is required.
- D – is the build number and will be incremented each time CSAS development engineers save a change to the application; this provides an overall incremented version number across all major/minor/bug fix releases.

24.3 Licensing Issues

Each copy of CSAS needs a valid and non-expired licence in order to operate, without a valid licence CSAS will not start and will instead display the Licensing screen.

Some users will have 'dedicated' licences, that tie a licence to their specific copy of CSAS and which will have been activated by installing a licence code on that copy of CSAS. Other users will use 'floating' or 'concurrent' licences and their copies of CSAS will have been provided with the address of the floating licence server.

24.3.1 Checking Licence Details

Details of the current licence can be found by navigating to the top menu bar, clicking on the  button and selecting from the drop-down menu 'About/Licensing'. The 'About CSAS' pop-up window opens from which details about the current license can be obtained.

24.3.2 Expired Licence

In normal circumstances, Forensic Analytics will be aware of the expiry date of each licence and will contact you (or you're CSAS administrator) well in advance to arrange for licence renewal.

If a user's licence has expired however, you or your CSAS administrator will need to contact CSAS Support to get a new licence issued.

Contact Support via email or the contacts forms on the secure website, selecting 'Licence Management' as the topic.

24.3.3 Online Activation – Licence does not Exist

Occasionally users report that the 'online activation' of a dedicated licence does not work – after copying the activation code into the licensing screen and error message indicates that 'Licence does not exist'.

The cause of this has been found to be that the CSAS licensing server may have been in a 'sleep' state prior to the licensing attempt and takes a few seconds to 'wake up'. If this error message is encountered, wait 10 seconds and try again.

If the process continues to fail after 2 or 3 attempts, then contact CSAS Support.

24.3.4 Floating Licence Unavailable

The floating licence method allows a customer organisation to purchase a small number of activations for a larger population of CSAS users.

A floating licence can be shared by a number of concurrent users in the same organisation. Each floating licence is provided with a number of 'activations', which sets the limit for the number of concurrent users who can share that licence at any one time. For example, if an organisation purchases a floating licence with 10 activations, the first 10 users who attempt to open CAS will get connected, the 11th user will receive a message saying that all activations are in use and will have to wait until one of the original 10 users has logged off.

If this happens regularly, it may be that your organisation doesn't have enough CSAS

activations for their floating licence and might consider purchasing more.

It is also possible to create more than one floating licence 'pool' per organisation, allowing different teams, for example, to have their own separate licence and set of activations. If you would like to discuss purchasing more activations for an existing floating licence or discuss segmenting a single floating licence into separate pools, please contact your Forensic Analytics account manager or CSAS Support.

24.3.5 Floating Licence Server Unavailable

Copies of CSAS that have been configured to use a floating licence will check with the server to obtain an activation when CSAS is opened. Additionally, once a floating licence activation has been granted to a copy of CSAS, it checks in with the server at five-minute intervals to see if the activation is still valid.

If the floating licence server used by your organisation is down or otherwise unavailable, CSAS will not be able to start or if it has started, will close after five minutes if it can't check in.

In most organisations, the floating licence server is deployed within the organisation's network and is managed by their IT Team, so the first port of call when experiencing floating licence issues would be your own IT team. CSAS Support have no access to investigate issues with customer-hosted servers.

A minority of customers use a 'cloud' floating licence service hosted by Forensic Analytics, so for these users only, problems with the floating licence service should be reported to CSAS Support.

24.3.6 Check out a Floating Licence

24.3.7 No access to expected features

Most CSAS features are accessible to all valid users, there are only two separately licensed features namely CellView and RF Survey.

If you expect to be able to access either of these feature but can't, it may be that the required licence hasn't been deployed or has expired.

In the first instance, check the state of the licences for those features – see [Adding Additional Licences](#). If no licences are installed, please contact your local CSAS administrator and check to see whether you have been authorised to access those features. If additional licences are required or existing licences have expired, please contact your Forensic Analytics account manager or CSAS Support. Please note that in most cases the additional licences will attract an additional fee.

24.4 User & Team Management Issues

24.4.1 User can't view expected case(s)

This is generally only an issue in Server mode, as in Standalone mode there is usually only one user and one Team per install. In Server mode, users only have access to cases that are linked to the Teams the user is a member of and that are at or below the Security Level applied to the user's account.

If there are cases on the system that the user knows are there but that they can't see, it is likely that the cases belong to a Team and/or Security Level that the user cannot access.

Speak to the local CSAS or CSAS Server administrator to check the access requirements for the required cases. CSAS Support has no access to individual organisation's CSAS Server, cases or case management function and would not be able to help with this issue.

24.4.2 Expected results not appearing in case search

If you've run a case search for a piece of information (a phone number or other identifier, for example) and do not see the expected cases appearing in the results, there could be several reasons for this:

- The search term may not have been entered correctly or fully.
- In Server mode, the cases in which the search term can be found belong to cases that you don't have the required Team or Security Level to access.
- The cases may have been deleted and are no longer available to be searched.

24.4.3 Moved to a new Team, can't see old cases

This is generally only an issue in Server mode, as in Standalone mode there is usually only one user and one Team per install. In Server mode, users only have access to cases that are linked to the Teams the user is a member of and that are at or below the Security Level applied to the user's account.

If you have been moved to a new Team and removed from your previous Team(s), then any cases associated with those removed Teams will now be unavailable for you.

It is possible, in CSAS Server mode, for an individual user to be a member of more than one Team. If you want to regain access to a previous Team, please contact your local CSAS or CSAS Server administrator to check the access requirements for the required Team(s). CSAS Support has no access to individual organisation's CSAS Server, cases or case management function and would not be able to help with this issue.

24.5 Starting CSAS

24.5.1 Unable to open CSAS

If the CSAS application fails to start, please try the following steps:



- Does the CSAS v3 icon -  - appear on your PC's desktop? If a CSAS icon without the 'v3' in the name appears, that may relate to an older version of CSAS. Please contact your local IT support team to check if CSASv3 is installed on your machine.
- If the CSAS v3 icon appears, but nothing happens when you double click it:
 - is the application already running? Look for the CSAS icon in the taskbar at the foot of the screen.
 - If CSAS isn't already running, restart your PC and try launching the application again when it has restarted, just to see if that resets the application.
 - Are any error or warning message windows open? If so, follow the instructions and see if that allows the application to start.
 - Has CSAS recently been updated, is this the first time you've tried to access it since the update was applied?

If those troubleshooting steps fail, please contact your local IT support team for further assistance. CSAS Support has no access to individual organisation's PCs or virtual machines and would not be able to help with this issue.

24.5.2 Forgotten username or password

CSAS is a secure and robust application and requires all users to have strong and unique passwords to gain access to cases. If you forget your username and/or password you won't be able to access CSAS until those credentials are recovered or reset.

CSAS supports several different user authentication methods and the 'forgot password' process is slightly different for each of them:

- Standalone deployment, local database authentication – standalone deployments do as the name suggests, they 'stand alone' and are not connected to CSAS Server. The username and password for the individual user registered with a standalone deployment will have been saved during initial installation and setup (see [Initial Install](#)) and you will have been urged to save a copy of the credentials.
If you have forgotten your username there are no account recovery options. If you have forgotten your password, you will be asked a series of questions based on the 'password recovery' questions you were asked to complete during the initial install. If you correctly answer the questions, you will be given the opportunity to set a new password and can then gain access to your cases. If you cannot correctly answer the account recovery questions you will not be able to gain access to CSAS or your cases. Please contact CSAS Support in this instance to discuss the options for resetting CSAS and starting again.

- In Server mode, user authentication can be provided in three ways – local Active Directory, Azure Active Directory (also now known as Microsoft Entra ID) and CSAS Server-based authentication.
In all of these options, the username/password combinations are managed by your organisation's IT team, if you cannot log in, please contact them for support. CSAS Support has no access to individual organisation's user authentication systems and would not be able to help with this issue.

24.6 Case Creation & Management Issues

Detailed explanations of the Case Management functions are provided in [Case Management](#).

24.6.1 In Standalone mode, can't see other users' cases

If you're using CSAS in Standalone mode and can't see the cases created by other users in your organisation – for example, when you run a Case Search you don't see results for cases created by your colleagues – then this is the expected behaviour. 'Standalone' deployments do as the name suggests, they 'stand alone' and are not connected to CSAS Server, meaning that there is no mechanism to allow users to automatically share cases with each other. If you wish to view a case created by another standalone CSAS user, you can use the Case Export/Case Import functions (see [Importing and Exporting Cases](#)) to share cases.

In Standalone mode, CSAS only allows one user to be set up per instance of the application. If you are using a shared PC, that several users have access to, CSAS can be made available to multiple users, but only by separately installing and licensing a copy of CSAS in each different Windows account. This effectively means that multiple separate copies of CSAS have been installed on the same machine but are still 'stand alone' from each other. A user logged in to CSAS in one Windows account will not have access to the cases created by users in any of the other Windows accounts, except by using the case Export/case Import functions.

24.6.2 CSAS won't allow a new case to be created

The CSAS case database requires each case to have a unique name, the scope of this restriction is based on the scope of the database.

In Standalone mode, where each copy of CSAS has its own local case database, case names must be unique within the set of cases created on each machine. Different Standalone users on different machines can create cases with the same names if they wish – although this could cause issues if cases get exported/imported between those users.

In CSAS Server mode, all users within an organisation are sharing the same case database, hosted on the server, so case names must be unique across the organisation. This may sometimes be difficult to coordinate, but an agreed format for case names within an organisation could help. If, for example, case names were prefixed with the case reference or the investigating team's name, it would help to keep names organised and unique.

24.6.3 Existing case name clashes with a new case

In scenarios where CSAS declines to create a new case because the case name is already in use, but where the 'new' case takes precedence over the 'old' case, it is possible to change the 'old' case name via the Case Management functions – please see [Rename](#).

24.6.4 Cases no longer needed

In busy organisations multiple CSAS cases can be created over time, which increases the size of the case database, lengthens the time required to complete searches and increases the risk associated with storing personally identifiable data.

If old cases no longer need to be retained within the case database for immediate access, there are two options: delete the old cases or archive them.

The case delete function is available from with the Case Management menu – see [Delete Case](#). Note – the case delete function is irreversible, once deleted a case is gone and cannot be recovered.

The archive option is provided by the Case Export function (see [Importing and Exporting Cases](#)) – there is an option to export and delete cases. The case is deleted from the case database, but the exported zip file can be retained as an archive copy of the case and can be reimported into CSAS at a later time if required.

24.6.5 Change prefilter dates after a case has been created

CSAS offers the option of setting 'prefilter dates' to case when it is created – this limits the Import Files process to only import events that fall within the prefilter dates into the case and to ignore events that fall outside.

If, after initially creating a case and setting prefilter dates, you decide that you need to alter the prefilter date span, this can be done via the case management menu (see [Edit Case Prefilters](#)). Please note that if change prefilter dates you may need to delete and reimport case files – you'll definitely need to reimport files if you widen the date range to include periods that were previously filtered out, as the events for the period will not be available within CSAS.

24.7 Import Files Issues

Detailed explanations of the Import Files functions are provided in [section 9](#) of this guide.

24.7.1 'Unrecognised' Files

The CSAS parser – the element that imports and processes source data files – has been programmed with the details of hundreds of file types and so should process most files automatically. Given the evidential nature of the work that CSAS is often used for, however, we do not allow the parser to engage in any guesswork, it will only process file formats for which it has specific processing instructions. This means that if files are presented to it in a format that it doesn't recognise, it will not attempt to guess how to process them, it will simply state that the files are 'unrecognised'. This doesn't mean that the data cannot be imported into CSAS, it just means that some user intervention may be required.

If source data files are shown with a status of 'unrecognised' after attempting to import them into CSAS, the following steps should be followed:

- Check that the file has not be edited or amended – CSAS works best with 1st generation copies of the 'golden copy' of a file, if files have been edited, had additional worksheets added, had pivot tables created, had header rows removed, had additional header rows added or have had columns added, removed or moved, then CSAS may struggle to automatically recognise the data format.
- The above is especially true of .csv files – see below for an explanation of the issues related to .csv files that have been opened in Excel and resaved.
- If the user has any suspicion that an unrecognised file might be corrupt or badly formatted it is recommended that they reapply to the source of that data (the cellular operator, their client, their organisation's SPoC, etc.) and get fresh, unopened copies of the source data.
- If new copies of files that were originally 'unrecognised' are received, users should ensure that the existing copies are deleted from CSAS before attempting to import the new copies.
- XLS and XLSX files that have been opened/saved many times often have small amounts of format corruption that, although not noticeable when the files are opened manually, cause issues when the files are processed using an automated system like CSAS. The best way to avoid this being an issue is to use a fresh, unopened copy of the golden copy of the file, but if you only have files that have been previously opened to work with, then you might be able to fix the corruption by resaving the file. If possible, XLS files should be resaved in XLSX format, or XLSX files should be resaved as XLS and then resaved again in XLSX format, as swapping between formats forces Excel to review and fix any file issues. After resaving, the new copy of the file should be imported into CSAS (not forgetting to delete the original, unrecognised version first). This process is not recommended for CSV files due to the number format 'exponentialisation' that can occur when CSV files are opened in Excel and resaved.
- If the above process was followed and files are still showing as

'unrecognised' then more advanced users may wish to examine the content of the files (by creating a copy first and examining the copy) and look to see if there are any obvious changes. It might be useful to compare the new file with a 'recognised' copy of a file from the same operator to see if there are any obvious differences (this is what CSAS Support would do in the first instance in any case). If there are obvious differences that can be fixed, the user may wish to edit to copy of the file they are working on and then see if CSAS will accept it.

- Users may wish to try using the CSAS [File Import Wizard](#) or a [CSAS Rescue Format](#) template to see if that helps.
- Ultimately, if you've tried the above steps and still cannot get the data to import into CSAS, you can send the problem file through to CSAS Support for us to look at it. We recommend that users send us copies of files that were unrecognised even if they managed to edit the file to get it through CSAS themselves so that they format can be added to the parser for other users.

24.7.2 'Not Imported' Files

In addition to 'unrecognised' files, which CSAS simply cannot process, there is another class of 'problem' files that have the status 'Not Imported'. There are several reasons why a file may be classed as Not Imported:

- The most common reason is that the file is empty, by which we mean that although it is a properly structured CDR file it contains no call details. In these cases, the file might of a type that is recognised but contains no data to be loaded into the database – hence it's state of Not Imported.
- CDRs may also be Not Imported if they are of too old an Excel format. CSAS only works with .xls files using the format employed Microsoft between 1995 and 2007 and the .xlsx format employed from 2007 onwards – it does not work with any versions earlier than Excel 95. The error comments column will contain a message asking the user to save the source data file as Excel .xls 97-2003 or later and try again. In these situations, the user should delete the offending files from CSAS first, then open them in Excel and resave them as .xls or .xlsx, then import the new versions into CSAS again.
- Encrypted or password protected files might also be shown in this state, as CSAS would not be able to access the data to load it.

24.7.3 'Not Parsed' Files

There can be circumstances in which a file is recognised during CSAS import but fails to load correctly – if the reason for the load failure is understood by CSAS and is it deemed to be acceptable not to load the file (as would be the case with an empty file) then CSAS will move the file into the 'Not Imported' state; if CSAS thinks that data from the file should be loaded but isn't able to it will flag it up as a 'Not Parsed'.

There are a variety of causes of Not Parsed – in some cases it will be because the file is empty but we haven't seen an empty example of that file format before and haven't instructed CSAS on how to deal with it; in others it might be that CSAS was unable to determine the target phone number from the data; in still others it might be that although

the column headers in the data were intact, the data itself was corrupt.

If CSAS understands why the error occurred, it will place a cause in the Error column of the import files list and will usually also suggest a cure.

Many Load Error conditions can be rectified using the [Update File Details](#) control, but some may require intervention from CSAS Support.

24.7.4 How To...Use the Support Rescue Formats

Although we make every effort to keep up to date with the source data formats employed by cellular operators, CSAS users will inevitably encounter files from time to time that CSAS simply cannot process.

In normal circumstances, users only need to contact CSAS Support and provide a copy of the unrecognised data format and should receive updated processing instructions and possibly an automated CSAS parser update shortly thereafter.

If a quick response from CSAS Support is not possible – if the issue occurs out of support hours, for example, or if the fix for the issue requires the distribution of an updated version of CSAS – then users can use the File Import Wizard. Not all file formats are yet supported by the Wizard, though, so the last resort is to employ a Rescue Format template.

The Rescue Formats consist of a set of templates, covering the most commonly imported data types, that have a known column layout that CSAS will recognise. Users are able to reformat the data from the 'unrecognised' source data file to fit into the template to allow it to be imported into CSAS.

Obviously, the effort involved in performing such a procedure would only be required if the user cannot wait for a response from CSAS Support and the Rescue Formats are provided with no guarantee of accuracy or success – it simply offers users an alternative to waiting in cases where time is critical.

If the Rescue Format fails, then users are always able to fall back on to more traditional manual CDR processing methods.

-  GN01 generic cell locations data import v1.6.xlsx
-  GN02 generic call data import v1.3.xlsx
-  GN03 Generic ANPR_ALPR Data Import v1.3.xlsx
-  GN05 generic handset download import template ..
-  GN06 Generic Location Only v3.2.xlsx
-  GN06 Generic Locations & Events v3.2.xlsx
-  GN07 Attributions import template v1.1.xlsx
-  GN08 Generic Tracker Data Import v1.0.xlsx

The rescue formats are accessible via the [Resources > Support](#) top row menu option.

Each rescue template contains in line comments providing instructions about the content and formatting of each column, but general details about each format are provided below:

GN01 – cell address import

This format allows for the manual import of additional cell address information and would be used to add 'missing' cell details to a case – for example, if the source CDRs only

showed Cell ID and Site Name for each cell, a GN01 form could be used to manually add postcode and azimuth details. The CSAS case should be set to use the 'override cells' cell logic option if additional cell details have been imported, otherwise they will not be visible.

The latitude and longitude columns can accept three different formats of lat/long coordinates:

- Decimal – e.g. 51.23456
- Degrees decimal minutes – e.g. 51° 23.456
- Degrees Minutes Seconds – e.g. 51° 23' 456''

The import process is also flexible about how the east/west, north/south direction is handled with either a +/- sign being used or the direction letter (N/S/E/W) being added after the coordinates.

GN02 – call data import

The GN02 format is used to import call records from unrecognised CDR formats. The data from the original CDR needs to be copied over to the appropriate columns of the GN02 form and some columns may need to be reformatted to match the expectations for the GN02 form. The GN02 format is also used by features such as the Encrochat import and the 'file import wizard' feature to reformat imported data into a format that CSAS can understand.

The form supports a large number of columns but there are five mandatory columns (highlighted in yellow in the header row) that must be populated:

- Start Date – must be in dd/mm/yyyy format
- Start Time – must be in hh:mm:ss format
- Duration – must be in hh:mm:ss format
- Event Type – must use the standard CSAS event descriptions:
 - Outgoing/Incoming Voice
 - Outgoing/Incoming Text
 - Outgoing/Incoming MMS
 - Outgoing Data
 - Unknown
- 'A' Number – for Calling phone, must be in international format with leading country code
- 'B' Number – for Called phone, must be in international format with leading country code

Further optional columns are available for importing cell location data, IMEI, IMSI, etc.

Once completed the form can be imported into a case using the standard Import Files screen.

NOTE – this facility does not deal with duplicate events or event types that need to be ignored or combined, it simply imports each row of data as a separate event. This facility is intended to provide a quick workaround in the event that a file is not recognised, we still recommend that unrecognised files are forwarded to CSAS Support so that a long-term fix can be developed for them.

GN03 – ANPR import

Similar to the GN02 format, the GN03 is used to import ANPR/ALPR data from unrecognised files by copy/pasting it from the original (unrecognised) file into the template. The same caveats regarding the potential need to reformat some data columns exist.

GN05 – handset data import

This format is used to import basic handset download data from source files that CSAS does not recognise. It currently only supports the import of text message and call log data.

GN06 – events & locations import

This format is used to import all data types other than CDRs, ANPR or handset data into a case – anything that has a timestamp and/or a location can be mapped into a GN06 form and imported into a case, it can then be viewed in the Advanced Data Browser and in CSAS mapping.

GN07 – attributions import

This format is used to import attribution data – identifier, attributed name, attribution colours, validity periods – via the Import Attributions function. Spreadsheets in other formats can also be imported, but this template uses the default format that CSAS should recognise with no difficulties.

GN08 – tracker data import

This format is used to import GPS vehicle tracker data, which is expected to provide details about the movements of a specific tracked vehicle.

24.7.5 How To...Check Imported File Details

The details associated with successfully imported files are displayed in three places:

- In the Import Files grid – basic view
- In the Import Files grid – advanced view
- In the Import Files grid – 'date range' view

Of these though, the most complete set of details are in the advanced view.

After importing source data files into CSAS it is good practice to scan through the list of files and check that the details displayed in the advanced view for each file matches expectations – two specific things to look for are the numbers of calls/cells that are listed for each file (very low numbers of calls listed for files that should contain many hundreds of calls is a sign to watch out for) and also the date/time span for the file (check that the expected 'from' and 'to' dates/times are listed).

24.7.6 How To...Update File Details

In situations in which the Target Identity data in the imported files list is missing or incorrect, users can make use of the Update File Details feature, which allows users to edit key file attributes such as:

- Target Identity (e.g. target phone number)

- From Date – start date/time of data records
- To Date – end date/time of data records

To access this control, highlight the required row in the imported file list and right-click, a popup with Update File Details appears, click this to access the update control.

If the target phone detected for a file is incorrect – if CSAS has incorrectly determined that the target number is some other number from the data – the Update File Details control can be used to replace the number with the correct one.

To achieve this:

- Highlight the file, right-click and select the Update File Details option.
- Enter the correct phone number in the Target Number box.
- Click 'Save' the data related to the file will be deleted from the case and reimported using the updated details.

24.7.7 How to...add a missing subject for a handset download

Handset downloads (as opposed to SIM downloads) often don't include details of the phone number(s) used with a handset, meaning that those details need to be added manually.

If this happens, CSAS will indicate that the file cannot be imported without a subject identifier and you can use the Update File Details popup to add the missing details.

24.7.8 How to...vary the processing rules for a file

Some more complex data formats (e.g. the Vodafone UK CDR data format) record multiple events that relate to the same transaction – several messages might trace the journey of the same text message through the network, for example.

CSAS, where possible, applies 'post-processing' rules to 'merge' or combine these multiple source records into a single output event that is displayed in Case Hub and presented in output call schedules. This ensures that investigators and, more importantly, juries aren't confused or misled about the number of events (calls, texts, and data sessions) that are being presented.

In some circumstances, it may be beneficial to be able to enable or disable the rules employed for a particular file format to overcome issues with the source data or to accommodate personal or organisational preferences.

For example, most Vodafone UK CDR formats explicitly indicate the azimuth of cells included in a disclosure, but some formats use an alternative method of indicating a cell's general coverage area called a 'centroid'. In these situations, CSAS can be set to calculate an 'assumed azimuth' based on the centroid, which gives a more approximate indication of the direction a cell faces than is provided by a 'real' azimuth. Some organisations prefer to have cell coverage information displayed at all rather than sue an assumed azimuth, so the rule that applies the centroid calculation can be disabled.

Another cause for the occasional need to vary the rules used to process a file relates to deficiencies or errors in the disclosed data. Some networks experience bugs and errors in their data collection and/or disclosure systems, which can mean that disclosed data contains deficiencies or missing data. For example, some CDRs might include a site name

or other location details for a cell, whereas other CDRs, produced by the same network can sometimes omit some of those details. CSAS can be set to search for examples of cell address information found in imported files in a case and use them to 'fill in' the missing details from other files that contain details of the same cell.

In these circumstances, users can elect to make use of the Variable Parsing Rules feature in the right sidebar of the Import Files screen. This feature allows users to specify that specific post-processing rules are enabled or disabled when processing files.

To apply variable parsing rules:

- Identify the file or files that require amended processing. If the files have already been imported into CSAS it will be necessary to delete them first.
- Open the Import Files right sidebar Variable Parsing Rules section.
- The list of rules that are available to be disabled are listed. To change the settings for a rule simply tick/untick the associated tickbox
- The file(s) can then be re-imported into CSAS
- The changes made using this feature are persistent, so the next time a file of that type is processed the varied rules are again applied. If you only varied the rules for a specific file or files, please remember to revert the changed rule(s) back to their original state before importing any more files.

An alternative option for viewing the full set of source data events within CSAS is to launch the required file in the Visual Parser (highlight the file in Import Files grid and right-click), which shows the entire source file alongside the processed output file on the same screen.

24.7.9 'Missing' events

Some CDR data formats (in the UK, Vodafone, EE and occasionally H3/Three) provide details of events from the 'other' or 'non-target' phone's perspective – for example, they might include a record showing a call leaving the 'other' phone and another record showing the same call arriving at the subject phone. Technically, these 'other phone' records are known as 'non-target' and can be disclosed and used only under certain circumstances.

Occasionally, a data set might contain the record of an event that is only shown in non-target data, where there is no 'subject' phone record of the event. For example, the non-target data might show an outgoing record of a phone call being made from the non-target phone to the subject phone but there is no corresponding subject phone record to show the call being connected. In that scenario, it means that there is no evidence that the call was actually connected to the subject phone, either the call failed and wasn't connected, or the call was connected but the network didn't capture a record of it.

In such situations, it is tempting to assume that the fact that there is a 'non-target' record showing that a call attempt was made means that there is evidence that the call was received by the subject phone. This is potentially very dangerous from an evidential integrity point of view, as it means that contact is being assumed without a robust evidential foundation to prove that the contact took place.

For these and other reasons, CSAS by default ignores 'non-target' records and does not

display them in Case Hub or anywhere else. We occasionally get queries about 'missing records' from users who have reviewed the raw data in a case and noticed one or more records that appear to show connections that do not appear in the CSAS version of the data. In most cases, these records would have been classed as 'non-target' data and ignored.

It is possible to view 'non-target' records in CSAS by placing the application into 'Intel Mode' (using the switch in the top right of the CSAS screen).

In 'Intel Mode', CSAS displays any 'non-target' records contained in selected files, but makes it very clear that these records are different – Intel records are shown with their event index and event type columns in-filled in red.

Our recommendation is **NOT** to base significant investigative conclusions on 'non-target' or 'intel mode' data, Intel Mode is purely there to provide a fuller picture of a dataset from an intel point of view.

24.7.10 Unable to View Imported Files

Users have sometimes reported that they have been unable to find or view files in the right sidebar Source Data list after importing them, most often the 'missing' files are 'cell address' files.

The Source Data list only displays files that contain substantive events that can be displayed in the Case Hub grid. Cell address files, which are disclosed by some networks to provide additional address details for cells, usually have no event details, only locations. As they contain no events to be displayed, they aren't listed in the Source Files menu.

24.7.11 Deleting & Re-importing Files

In situations in which a source data file is in the 'Unrecognised' state after importing or the 'Not Imported' or 'Not Parsed' state after loading, there will usually be a resolution of some form for the issue – this may be a local resolution, in which the user fixes the problem via the File Import Wizard or Update File Details controls, or it may be resolved by CSAS Support and could involve them editing the data file, issuing a parsing update or releasing an application update.

In the event that a parsing update or a CSAS update is issued and the 'failed' file is still listed in the Import Files grid, the file should be deleted from CSAS and reimported, to give the updated parser an opportunity to process it.

24.7.12 Special Handling for .csv Files

Many operators issue CDR data and other file types in the .csv (Comma Separated Value) format – if a .csv file is opened in Excel, Excel tries to be 'helpful' and attempts to determine the type of data held in each column. Quite often Excel decides that a phone number, as a string with nine or more digits, should really be displayed in scientific notation (so 07700900123 would become 7.70×10^9 , which Excel would render as '7.70E+09' for example).

If the file is resaved, as .csv is a text-based format, it will save the phone number in text as '7.70E+09' and all details about the original phone number digits after '770' will be

lost.

If the file is then imported into CSAS, the scientific notation form of the phone number is converted back to a numerical telephone number, but to the missing data what was originally 0770900123 becomes 07970000000.

In these circumstances there is no way of recovering the missing digits, except by requesting a fresh copy of the source data. This is why we recommend that users only import 'unopened' 1st generation copies of source data files into CSAS, as if they haven't been opened there won't have been a chance for Excel to be 'helpful'.

One way of avoiding this issue is to change the Windows file association settings for .csv files. By default, Windows associates .csv with Excel (if Excel is installed) and therefore automatically opens .csv files in Excel.

If the file associated for .csv is changed to a different application – Notepad, for example – then the issues related to 'exponential' phone numbers disappears, as the problem is caused by opening the data in Excel rather than being a problem with the source data itself.

24.7.13 Sending Unrecognised/Unloaded Files to CSAS Support

If the various steps outlined above fail to solve a file import or file load issue, or if a user receives a copy of a genuinely new data format, then CSAS Support will need to be informed so we can either fix the problem file or develop a parsing description for the new file format.

CSAS Support can be contacted via our secure support website at secure.forensicanalytics.co.uk (log in required). After logging in, click on the Tickets link and 'Create Ticket'. Outline the issue in the contact form.

If CSAS Support agree that the file should be sent for examination, they will provide you with the email address to use - if your organisation permits source data to be transmitted to third parties.

With the advent of the EU's GDPR regulations in 2018 and for general operational security, we much prefer it if source CDRs are anonymised before being sent to us.

24.7.14 Anonymising Files before sending them to Support

We make an 'anonymisation macro' available to help users anonymise sensitive files before sending them to use – it is available within CSAS in the [Resources > Tools](#) folder, which also includes a document detailing how to use the macro.

24.7.15 Recognising Handset Download files

CSAS will accept Excel and XML extracts from the following handset download software:

- » Cellebrite (Excel only)
- » XRY (Excel and XML)
- » Blue Lights Digital Odyssey (Excel only)

Data Processed by CSAS

CSAS currently imports data from the following tabs:

Cellebrite	XRY/XAMN
Summary *	Summary *
Device Info *	Device General Info *
User Accounts	Case Data *
Contacts	Device Accounts
Call Log	Contacts Contacts
Chats	Calls
MMS Messages	Messages Chat
SMS Messages	Messages MMS
Searched Items	Messages SMS
Web History	Messages Emails
Messages MMS	Web History
Messages SMS	Locations History
Notes	Device Network Info
Locations	
Wireless Networks	
Instant Messages	
Emails	
SIM Data	
Journeys	

Currently, the tabs shown in yellow **must** be present in order for the files to be recognised by CSAS – you may need to speak to your DFU to ensure that these tabs are included in outputs

At least one of the other tabs must be included in order for usable data to be extracted.

It is also a good idea to ask the DFU to create a version of the download that only includes the tabs listed here – CSAS ignores other tabs, so if they are included it just makes the files larger unnecessarily

Recognising Cellebrite Extracts

When importing device download data into CSAS your extract using Cellebrite will need to meet the following criteria for the extract to be recognised and formatted correctly.

The below table identifies the values required for the different versions of Cellebrite extract reports. Please note you only need 1 value in your summary worksheet to match.

Format Name	Sheets that MUST be present	Must Match which Cell Value?
HSD88-UK70-CB01	Summary	On Summary Sheet between Rows 1-20, Column B must be text " Examiner "
HSD88-UK70-CB01V2	Summary	On Summary Sheet between Rows 1-20, Column B must be text " Examining Officer "
HSD88-UK70-CB01V3	Summary	On Summary Sheet between Rows 1-20, Column B must be text " Time zone settings " or " Report creation time "

Device Information tab is also required – if it contains an identifier (IMEI/IMSI) that will be captured as subject identifier, if the tab is present but doesn't contain an identifier, the user will be asked to add one manually

Other Cellebrite hints

Extracts can be extremely large files, if CSAS encounters an "Out of Memory issue", then reduce the size of Workbook by removing the "Timeline" worksheet. (This is not used in CSAS as it is a repeat of all the Voice/Chat/SMS data)

Consider splitting the data into another workbook (Splitting Chats/Messages SMS/Call Log sheets)

XRY/XAMN extracts

The below table identifies the values required for the different versions of XRY Excel-formatted extract reports.

Please note you only need 1 value in your summary worksheet to match.

Format Name	Sheets that MUST be present	Must Match which Cell Value?
HSD89-UK71-XR01	Summary, Device General Information	On the Summary sheet between Rows 2-10, Column A must be text "XRY Version"
HSD89-UK71-XR01V2	Device General Information	On the Device General Information sheet between Rows 1-2, column B must be the text "Attribute"
HSD89-UK71-XR01V3	Device General Information	On the Device General Information sheet between Rows 1-21, column A must be the text "Attribute"
HSD89-UK71-XR01V4	Summary, Device General Information	On the Summary sheet between Rows 2-10, Column B must be text "XRY Version"
HSD89-UK71-XR01V5	Summary, Case Data	On the Summary sheet between Rows 2-10, Column A must be text "XRY Version"
HSD89-UK71-XR01V6	Device General Information	On the Device General Information sheet between Rows 1-21, column D must be the text "Attribute"
HSD89-UK71-XR01V7	Summary	On the Summary sheet between Rows 1-12, Column A must be text "XRY Version"

Other XRY hints

Often XRY has formatted date/times as below (other Formats may cause Start Dates etc NOT to be read and to have 0001/01/01 values)

dd/MM/yyyy HH:mm:ss UTC (Device)	dd/MM/yyyy HH:mm UTC (Device)
dd/MM/yyyy HH:mm:ss UTC	dd/MM/yyyy HH:mm UTC
dd/MM/yyyy HH:mm:ss UTC (Network)	dd/MM/yyyy HH:mm UTC (Network)
dd/MM/yyyy HH:mm:ss UTC+01:00 (Network)	dd/MM/yyyy HH:mm UTC+01:00 (Network)
dd/MM/yyyy HH:mm:ss UTC+01:00 (Device) ,	dd/MM/yyyy HH:mm UTC+01:00 (Device) ,
dd/MM/yyyy HH:mm:ss (Network)	dd/MM/yyyy HH:mm (Network)
dd/MM/yyyy HH:mm:ss (Device) ,	dd/MM/yyyy HH:mm (Device) ,
dd-MM-yyyy HH:mm:ss tt UTC (Device) ,	dd-MM-yyyy HH:mm tt UTC (Device) ,
dd-MM-yyyy HH:mm:ss tt UTC (Network) ,	dd-MM-yyyy HH:mm tt UTC (Network) ,
dd-MM-yyyy HH:mm:ss tt (Network)	dd-MM-yyyy HH:mm tt (Network)
dd-MM-yyyy HH:mm:ss tt (Device) ,	dd-MM-yyyy HH:mm tt (Device) ,

dd-MM-yyyy HH:mm:ss tt UTC	dd-MM-yyyy HH:mm tt UTC
dd-MM-yyyy HH:mm:ss (Network)	dd-MM-yyyy HH:mm (Network)
dd-MM-yyyy HH:mm:ss (Device)	dd-MM-yyyy HH:mm (Device)

Rescue Format

If you are unable to import your download by following the requirements below, the rescue format GN05 generic handset download import template can be used. Simply copy and paste your data from the original download into the relevant tabs.

This rescue document can be found in CSAS in the following location:

Utilities > Resources > Support > GN05 generic handset download import template

Unrecognised Handset Files

What to do if you have a handset file that CSAS doesn't recognise?

First, create a 'working' copy of the golden copy of the file, then:

Cellebrite

- Add 'dummy' tabs to the front of the workbook
- Rename the tabs 'Summary' and 'Device Information'
- In Row 2, Column B of the Summary tab, add the word 'Examiner'
- In Row 11, Column B of the Device Information tab, add either 'IMEI' or 'IMSI', then add the file's subject identifier (IMEI or IMSI) in row 11, column C

XRY/XAMN

- Add two 'dummy' tabs to the front of the workbook
- Rename the tabs 'Summary' and 'Device General Information'
- In Row 2, Column A of the Summary tab, add the word 'XRY Version'

Then try importing the working version of the file into CSAS.

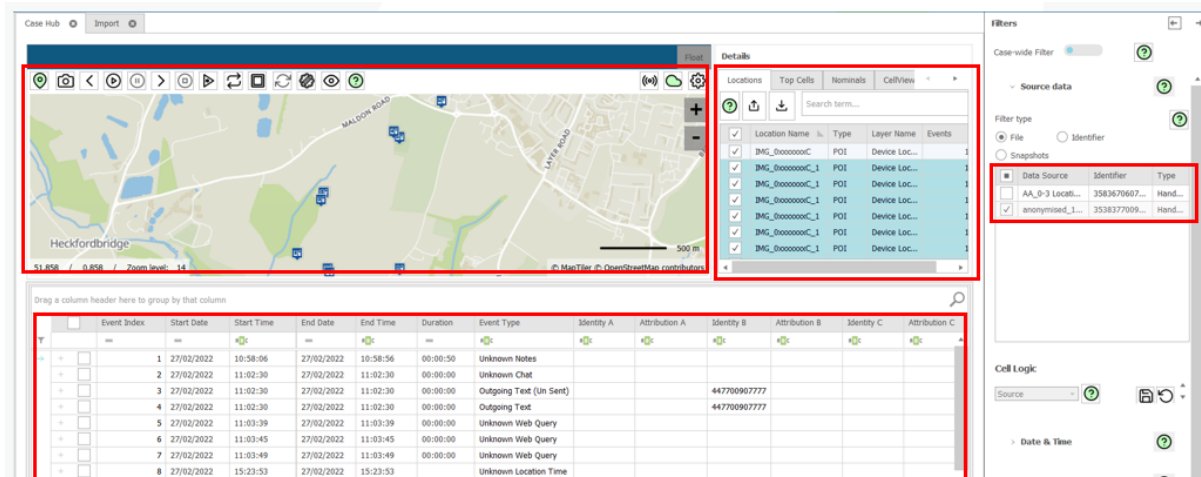
If it still doesn't import, please contact CSAS Support

Common Reasons for handset files failing to import

- File is from an extraction tool that isn't currently supported – Cellebrite & XRY/XAMN currently supported – if support for other tools is required, please let us know (and provide examples)
- File isn't in a format that CSAS handles:
 - Cellebrite – xlsx only - .ufdr not currently imported
 - XRY – xlsx or xml supported
- File doesn't contain required set of tabs/content for recognition – add dummy tabs
 - Cellebrite – Summary & Device Information
 - XRY – Summary & Device General Information

- File doesn't contain any of the tabs CSAS captures substantive information from, so there's no data to import
- File is too large – Excel starts to get unstable when importing files larger than 100MB and the process will be very slow for files above 50MB – make a working copy of the handset file and remove any tabs that CSAS doesn't deal with

Viewing handset data in Case Hub



The screenshot shows the CSAS Case Hub interface. On the left is a map of Heckfordbridge. In the center is a table of events. On the right is a sidebar with filters and a list of locations.

Event Index	Start Date	Start Time	End Date	End Time	Duration	Event Type	Identity A	Attribution A	Identity B	Attribution B	Identity C	Attribution C
1	27/02/2022	10:58:06	27/02/2022	10:58:56	00:00:50	Unknown Notes						
2	27/02/2022	11:02:30	27/02/2022	11:02:30	00:00:00	Unknown Chat						
3	27/02/2022	11:02:30	27/02/2022	11:02:30	00:00:00	Outgoing Text (Un Sent)			447700907777			
4	27/02/2022	11:02:30	27/02/2022	11:02:30	00:00:00	Outgoing Text			447700907777			
5	27/02/2022	11:03:39	27/02/2022	11:03:39	00:00:00	Unknown Web Query						
6	27/02/2022	11:03:45	27/02/2022	11:03:45	00:00:00	Unknown Web Query						
7	27/02/2022	11:03:49	27/02/2022	11:03:49	00:00:00	Unknown Web Query						
8	27/02/2022	15:23:53	27/02/2022	15:23:53	00:00:00	Unknown Location Time						

1. Imported handset files are listed in the file selection window in the right sidebar
2. Select the required handset file(s) and hit 'Apply' to send them to the grid
3. Events with date/times associated with them (including media events) will be listed in the Case Hub grid
4. Locations captured from the selected handset files will be listed in the Locations panel and can be enabled/disabled as required
5. Enabled Locations are visible as icons on the map

24.8 Attributions Issues

Detailed explanations of the Attribution features are provided in [Using Attribution](#).

24.8.1 Clear an incorrect attribution

If an attribution has been applied which later turns out to be incorrect, it can be deleted – highlight the required attribution in the Attributions grid, click on the Actions column for that row and select 'clear attribution' – the linked name and colours will be removed.

24.8.2 Import attributions from a non-standard Excel file

The Import Attributions feature allows you to import attribution details (identifiers, names, validity dates, attribution colours) from an Excel spreadsheet. CSAS includes a standard template, the GN07 Attributions Import template (see [Support](#)) for this purpose, but it is also possible to import attributions from any other single tab spreadsheet.

If the Import Attributions feature (see [Importing Attributions](#)) doesn't automatically recognise the columns in the imported sheet, you can manually define the contents of the worksheet using the dropdown menus at the top of each column – select the columns that contain the required minimum set of data (identifier, attribution name) and any of the other columns that exist and set any columns that contain data that isn't to be imported to 'Not Used' and the process will ignore it.

24.9 Dashboard Issues

Detailed explanations of the Dashboard feature are provided in [Using Case Dashboards](#).

24.9.1 No data appearing in the Dashboard

To view data in the Dashboard, select the required data from the right sidebar Source Data menu, apply any required filters and settings and click 'Apply'. If after following these instructions, no data appears in some or all of the Dashboard widgets, there may be a simple explanation:

- The General Investigation Dashboard (currently the only Dashboard option) works best with CDR and cellular data. Other data types like ANPR, handset download, tracker and telematics data will only populate the Average Event Distribution widget.
- The Dashboard grid displays details of all selected time-bound events, it is highly unlikely that a source file that contains data with no timestamps would be available for display in the Source Data menu, but it is potentially possible that the selected file(s) contained no events to display. Please check the type and content of the selected source files and confirm that event data is included.
- If any right sidebar filters or settings are applied that remove all events from the dataset – for example, if the date/time filter is set to a time period that covers no selected events – again, the Dashboard widgets will not be populated. Check the filters that are applied (see [Using the Right Sidebar](#)) or click on the 'Reset' button and reselect the required files and see if the report data is displayed.

24.10 Case Hub Issues

Detailed explanations of the Case Hub feature are provided in [Using Case Hub](#).

24.10.1 No data appearing in Case Hub

To view data in the Case Hub grid or map, select the required data from the right sidebar Source Data menu, apply any required filters and settings and click 'Apply'. If after following these instructions, no data appears in the grid or map, there may be a simple explanation:

- The Case Hub grid displays details of all selected time-bound events, it is highly unlikely that a source file that contains data with no timestamps would be available for display in the Source Data menu, but it is potentially possible that the selected file(s) contained no events to display. Please check the type and content of the selected source files and confirm that event data is included.
- The Case Hub map can be set into two modes – with auto-sync enabled, any data sent into the grid that has locations associated with it will automatically be displayed in the map; without auto-sync off, the map will need to be manually synced (using the  button in the map ribbon) before location data is visible.
- The Case Hub map displays details of the locations associated with the selected events. Some source data types include events but do not provide locations for them – some forms of financial data, for example. If no locations are populated on the map, it might be that the selected source data files contained no locations to be displayed. Please check the type and content of the selected source files and confirm that location data is included.
- If any right sidebar filters or settings are applied that remove all events from the dataset – for example, if the date/time filter is set to a time period that covers no selected events – again, the Case Hub grid and map will not be populated. Check the filters that are applied or click on the 'Reset' button and reselect the required files and see if the report data is displayed.
- If none of the above work, you could try closing the case and then closing and reopening CSAS to see if the 'missing' data appears.

24.10.2 Cell Address Details Not Being Displayed

Users sometimes report that Case Hub is not displaying full cell address details for cells that they know have full details loaded into the database.

The typical cause of this is related to the Cell Logic setting selected in the right sidebar Filters tab. This option manages the source of the cell details that are displayed in the current selected dataset. The basic options are:

- » **Source** – this forces CSAS to only use cell details that were available in the original source files and ignores any details provided in separate 'cell address' files or supplementary updates. This can lead, for example, to GPRS call records not showing Site Names or for cells not to have azimuth details associated with them. This option ensures that any cell details displayed for

the case exactly match the details that were available in the source CDR, but it means that Case Hub might not offer a complete set of cell details.

- » **Override** – this option allows the original cell details from the source file to be enhanced with any additional or supplementary details that might have been loaded into the case. This is achieved by preserving the data that came from the source CDR (i.e. Cell ID, Site Name) and filling any empty fields with data from the supplementary inputs (i.e. azimuth, map reference). This option should be used if you have loaded a dataset that includes formats that have a separate 'cell address' type of file (e.g. some Vodafone UK formats).

In cases where an insufficient level of cell detail is displayed, the first step would be to check that the Cell Logic dropdown is set to Override (remembering to click 'Apply' after making a change).

24.10.3 Invalid Date Formats

Occasionally users experience call records presented in the Data Browser with invalid dates – such as 01/01/1900 00:00:00.

The cause of this has usually been determined to be corrupted or missing date fields in the source data.

An example: Vodafone UK CDR files show start date/time in one combined column in the format 'dd/mm/yyyy hh:mm:ss' with a single space between the end of the date (yyyy) and the start of the time (hh). Occasionally the data output function in the Vodafone billing system omits the space leading to the date following directly into the time – dd/mm/yyyyhh:mm:ss – or adds more than one space.

CSAS has been instructed to check for a fix these date format issues but there may be other corruption issues or alternative formatting issues with other file types that we are not yet aware of.

If entries with invalid dates are discovered in processed data, CSAS is instructed to add a 'minimum' date, as imported event records must have a timestamp.

If you find one of more 'minimum' dates in imported data, the suggested fix is to use the Edit function in the Case Hub grid right-click menu – this allows you to update the timestamp associated with a record, but it must be performed one record at a time.

If all records or a large number of records in a file have corrupted or badly formatted timestamps, the recommended fix would be to send a copy of the file to CSAS Support to be reviewed for possible parsing update work to be done. If the file needs to be processed more urgently, then it could be possible to review the original source data to attempt to find and fix the problem at source by editing the source file. If problems are found and fixed the file needs to be deleted from CSAS and a copy of the corrected file needs to be imported and a note or statement should be added to the case indicating that the source data was edited.

24.10.4 Incorrect Data Appearing in Columns

Occasionally users have reported instances where the 'wrong' data has been displayed in the Case Hub data grid. For example, Cell IDs have appeared in the postcode column or

azimuths in the Site name column.

The cause of this has usually been determined to be corruption in the original source data files, especially files that were originally supplied in .csv format that have been opened and saved in Excel or in cases where additional commas are inserted into particular rows.

In these circumstances the mapping of data from the original comma-separated columns to Excel columns sometimes goes wrong, meaning that extra columns are created or that data that should be mapped to a specific column gets mapped elsewhere.

One fix for these issues is to make sure that the user is working with a previously unopened 1st generation copy of the 'golden copy' of the data, which hasn't had the opportunity to have been opened and saved in Excel.

A fix for instances where additional commas have been introduced into a row of data (which often happens in 'address' fields, where an address such as 'Pixmore Avenue, Letchworth' is included in one field without putting quotes around the whole field. CSAS would interpret this data as showing 'Pixmore Avenue' in one column and 'Letchworth' in another). If a situation like this is discovered, placing quotes around the text (e.g. "Pixmore Avenue, Letchworth") should fix the issue.

If a 'fresh' version of the offending data file can be sourced or created, then the 'corrupt' version should be deleted from CSAS before the 'clean' version is imported.

See also [Special Handling of CSV Files](#) above.

24.10.5 'Missing' Text Messages

Users occasionally report that a number of text messages are 'missing' from their processed data – this is generally associated with Vodafone UK data.

There are usually one of a number of causes of this:

- » The Vodafone Simplified data format bundles a number of event records together that are associated with the same text message and presents them as either a 'SMS Events' or an 'SMS' record. In some cases, the timestamp captured for incoming 'combined' event records relates to the time that the text message left the non-target phone, rather than the time it arrived at the target phone. Vodafone provide details of the delivery time for incoming text messages in the 'Timestamp SMS Delivery column (Column HY). CSAS uses this information to populate the timestamp field for such events.
- » Vodafone Simplified and Raw formats record details of events that relate to non-target phones if those phones are also on the Vodafone network. Our data processing policy is to only records in processed data that relate to the target phone, CSAS does not (by default) provide details of events that relate to non-target phones. Upon investigation we sometimes find that the 'missing' SMS events reported by users were events that were related to the non-target phone. It is possible to force CSAS to include some of these events by employing the Change Parsing Rules function discussed at 11.5.8 above.

24.10.6 'Incorrect' Timestamps

Users occasionally report that the timestamps presented by CSAS are incorrect by a few seconds.

This is usually reported in association with calls that were recorded with more than one event record – typically something like an incoming call that went to voicemail, where both the incoming call and the voicemail divert were recorded separately.

Our policy in these situations is to combine the separate event records into one processed event and to use the timestamp that relates to an action performed by the target phone.

For example, imagine that Phone A (non-target) calls Phone B (target) at 11:02:01 and Phone B fails to answer, causing a voicemail/divert event to be triggered at 11:02:05. CSAS will combine both event records into a processed Voicemail/Divert event that shows the A number (Phone A), B Number (Phone B) and a C Number (Voicemail platform number) and will use the timestamp from the voicemail/divert event as that relates to an action performed by (or on behalf of) the target phone, Phone B.

We would not capture the timestamp of the original call as that relates to an action performed by the non-target phone several seconds before the target phone became involved in the call.

Details of our other data processing policies can be found in the CSAS Data Processing Policies document available from the CSAS Support website.

24.10.7 Timing Advance 'point locations' not appearing

Point locations (also known as SHILD data) acquired from timing advance files from T-Mobile and Verizon are not generally regarded as being evidentially accurate and so are hidden by default. To view point locations on a CSAS map, check the row in the Details > Locations tab associated with that file and the points should appear in the map.

24.11 Case Outputs Issues

Detailed explanations of the Case Outputs feature are provided in [Using Case Outputs](#).

24.11.1 No data appearing in Case Outputs template

To view data in a Case Outputs template, select the required data from the right sidebar Source Data menu, apply any required filters and settings, select the required output template and click 'Apply'. If after following these instructions, no data appears in the Excel output that is created, there may be a simple explanation:

- Case Output templates display details of all selected time-bound events, it is highly unlikely that a source file that contains data with no timestamps would be available for display in the Source Data menu, but it is potentially possible that the selected file(s) contained no events to display. Please check the type and content of the selected source files and confirm that event data is included.
- If any right sidebar filters or settings are applied that remove all events from the dataset – for example, if the date/time filter is set to a time period that

covers no selected events – again, the Case Outputs template will not be populated. Check the filters that are applied or click on the 'Reset' button and reselect the required files and see if the report data is displayed.

24.11.2 Template Files Corrupted

If one or more output template files has become corrupted or unusable then new copies can be installed.

CSAS runs a check for the default set of templates each time it is restarted. To refresh the templates, you can close CSAS and delete the affected file(s) from the templates folder (see [Grid Right-click and Actions Menu](#)) and then restart CSAS. The application will check the templates, notice that one or more default templates are missing and will automatically reinstall them.

If you have specific or bespoke templates created are advised to keep backup copies elsewhere and copy these back into the User Templates folder in case of problems. If the bespoke templates were created for you by CSAS Support, then copies of the formats should be available to download from the secure support website.

24.12 Analytics Issues

Detailed explanations of the Analytics feature are provided in [Using Analytics](#).

24.12.1 No data appearing in the selected Analytics query

To view data in an Analytics query, select the required query, select the required data from the right sidebar Source Data menu, apply any required filters and settings, select the required output template and click 'Apply' – there may be additional filters and/or a 'run' button within the query that also need to be selected. If after following these instructions, no data appears in the query window, there may be a simple explanation:

- Not all source data types work with all queries – some queries only work with specific data types. Review the appropriate section of this user guide for the query you wish to use; each explanation has a 'Supported Data Types' section that details the types of data that work with each query.
- Analytics queries generally display details of all selected time-bound events, it is highly unlikely that a source file that contains data with no timestamps would be available for display in the Source Data menu, but it is potentially possible that the selected file(s) contained no events to display. Please check the type and content of the selected source files and confirm that event data is included.
- If any right sidebar filters or settings are applied that remove all events from the dataset – for example, if the date/time filter is set to a time period that covers no selected events – again, the Analytics query will not be populated. Check the filters that are applied or click on the 'Reset' button and reselect the required files and see if the report data is displayed.

24.13 CellView Issues

Detailed explanations of the CellView feature are provided in [Using CellView](#).

24.13.1 CellView tab not visible

The Case Hub details panel displays details of any active CellView visualisations and provides the option to manually search for CellView visualisations of specific cells.

If the CellView tab is not visible, or is visible but isn't populated, please check that you have a valid CellView licence installed (see [Adding Additional Licences](#)).

24.13.2 No CellView results returned for a cell

If you have triggered a CellView lookup, either from the cell right click Cell Coverage > CellView menu or from the CellView tab and no results are returned, there is generally a simple explanation:

- The CellView database does not contain details of every possible cell, only cells that have been reported as providing coverage to mobile devices that are running one of the 'partner apps', so it could be that the cell you've selected simply isn't in the CellView database.
- If searching for a cell manually via the CellView tab, was the cell ID entered in one of the required formats – see [Acceptable Cell ID Formats](#).

24.13.3 No CellView results returned for any cells

If CellView returns no results for any cell you've selected, even if you try looking for cells found in different source files and belonging to different networks, it could be that the CellView service is offline – leave it for 10 minutes and try again – or that your PC is offline – check connectivity and try again.

24.14 RF Survey Issues

Detailed explanations of the RF Survey feature are provided in [Using RF Survey](#).

24.14.1 RF Survey tab not visible

The Case Hub details panel displays details of any active RF Survey visualisations and provides the option to manually search for cell coverage visualisations of specific cells.

If the RF Survey tab is not visible, or is visible but isn't populated, please check that you have a valid RF Survey licence installed (see [Adding Additional Licences](#)).

24.14.2 No RF Survey results returned for a cell

If you have triggered an RF Survey lookup, either from the cell right click Cell Coverage > RF Survey menu or from the RF Survey tab and no results are returned, there is generally a simple explanation:

- Have you imported RF Survey data into that specific case and exported RF coverage details from the RF Survey module ready to be used in Case Hub – see [Opening the RF Survey module](#).
- An imported RF Survey dataset will contain details of every possible cell, only cells that were detected and measured during the surveys from which data

has been imported, so it could be that the cell you've selected simply wasn't detected during the imported surveys. Check that you've imported the correct or complete set of survey files and consider undertaking further surveys to capture details of the required cells.

- If searching for a cell manually via the RF Survey tab, was the cell ID entered in one of the required formats – see [RF Survey tab](#).

24.15 Case Cells Issues

24.15.1 Understanding Cell ID Formats

Different operators format their cell IDs in different ways; most present them in decimal (e.g. Cell ID 12345) but a minority elect to present them in hexadecimal (e.g. 1bc4).

To accommodate this, CSAS employs a number of Cell ID format descriptions:

- » Raw – this is the format in which a cell ID loaded into the database from the source CDR. CSAS stores this as an untouched record of the source cell ID data. Selecting 'Raw' as the display format for cell IDs ensures that the displayed data matches the source CDRs.
- » Decimal – CSAS creates and stores a decimal version of each cell ID, in case it is required – this is the default format for displaying cell IDs.
- » Hexadecimal – CSAS also creates and stores a hexadecimal version of the cell ID in case it is required.
- » CGI – the true and unambiguous identifier for a cell is its CGI (Cell Global Identifier). Because the CGI is a globally unique ID for each cell, CSAS uses it as the cell details database key, so a CGI is created for each detected cell too. The CGI consists of:
 - MCC (Mobile Country Code)
 - MNC (Mobile Network Code)
 - LAC (Location Area Code) + CI (Cell ID) for 2G/3G cells
 - Base Station ID + CI for 4G/5G cells

In general, CSAS defaults to identifying cells by their full CGI but the display format is configurable in most screens and functions.

24.15.2 Converting Between Decimal & Hexadecimal

Numbering systems can be devised that can contain any number of unique characters. The decimal system has ten characters 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 and was designed originally because human beings have ten fingers.

As digital equipment such as computers use pulses of electricity or light to represent numbers, they operate using the binary system, which has only two conditions, ON and OFF. These two conditions are represented by the characters 1 and 0.

Large numbers in binary have many 1s and 0s, which can be difficult to represent on paper. For example, 27 in decimal is represented in binary by 11011.

Hexadecimal (or 'hex') is a numbering system of sixteen characters, ten digits and six letters. It is used to condense into a more manageable form, the long strings of zeroes and ones in large binary numbers.

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

This base-16 numeric notation is frequently used to specify addresses in computer memory as it makes life simpler for programmers. The decimal numbers 0-9 are represented by the decimal digits 0-9 and the decimal numbers 10-15 are represented by the letters A-F.

Therefore, if a byte (8 bits) in binary is 01001101 then this is represented as 4D (4=0100 and D=1101) in hex.

Cell ID information is often presented in hex, which can cause confusion.

The CI (Cell ID) component of 2G and 3G CGIs is transmitted on the cell's BCCH in binary and consists of a 16-bit binary number.

When converted to decimal, a 16 field has a range of values from 0 to 65,535 and in hexadecimal, has a range of 0 to FFFF.

Use	Binary	Decimal	Hexadecimal
Lowest possible Cell ID	0000000000000000	0	0
Highest possible Cell ID	1111111111111111	65,535	FFFF

Networks often use Cell ID 65,535/FFFF to mean 'no cell used' or 'cell not known'.

24.15.3 Special handling for Hexadecimal Cell IDs

Excel has problems with hexadecimal cell IDs, especially those with an 'E' in them.

If .csv files containing hexadecimal cell IDs are opened in Excel, cell IDs that contain an 'E' character – e.g. 12e4 or ee87 – are typically interpreted as being exponentials, so '12e4' might get reformatted as '1.2+E4' and 'ee87' would be reworked into 'E+E87'.

If the files containing such 'exponentialed' cell IDs are then imported into CSAS the true cell IDs can be difficult to determine.

As has been previously suggested, the best way of avoiding such problems is to import only unopened, 1st generation copies of source CDR files into CSAS, and also to change user's PC file associations for .csv files to Notepad instead of Excel.

24.16 Miscellaneous

Miscellaneous issues that don't fit into any of the other categories include:

24.16.1 Moving to a new PC

If you are moving to a new PC and wish to ensure that your CSAS cases move with you, please consider the following:

- If the move to the new PC is being managed by your organisation's IT team, ask

them to contact CSAS Support for a more comprehensive guidance document.

- If your instance of CSAS is set up as a Standalone deployment, it means that all of your case data is stored locally on your PC. If you move to a new PC without copying the CSAS folders to the new machine you will lose all of your case data. Your case data will be stored in your personal CSAS folder – by default this is saved to C:\Users\<user>\AppData\Roaming\Forensic Analytics Ltd\CSAS v3\ (but this can be changed to a different location during installation, see [Initial Install](#) for details). The 'appdata\roaming' location was chosen as the default location as it is one that is routinely included when backing up a user's personal data in larger organisations, so there is a strong possibility that, if your organisation undertakes regular automated backups, that your CSAS data will simply be copied across automatically. Please provide details of this folder location to your IT support team and ask them to ensure that the contents are copied over to the new PC.
- In CSAS Server mode, your data may reside in two places – the central CSAS Server case database and, if you have any cases checked out at the point when the move to a new PC is triggered, the local CSAS database. Cases saved in the CSAS Server database will continue to be available to you after you move to a new PC, as long as the new PC uses the same CSAS user account details as the old one. If any cases are checked out when the move is triggered, please check them back in, which uploads them to the server. If this isn't possible, follow the 'standalone mode' instructions provided above to copy the local database to the new PC.
- These instructions should also be followed if you are keeping your existing PC but it is having its hard drive wiped or replaced.

24.16.2 I've moved to a new PC, but can't find my CSAS cases

If you've already moved to a new PC (or had your existing PC's hard drive wiped or replaced), logged into CSAS and can't find any of your existing cases:

- In CSAS Server mode, check that you've logged into the new PC using the same CSAS account details you used on the old PC – CSAS will link you to the set of cases associated with your 'old' account.
- In Standalone mode, check that you or your IT team followed the instructions provided above regarding the preparation to move to a new PC.
- If you have moved to a new PC, using CSAS in Standalone mode, without following the database migration process outlined above and if your 'old' PC is no longer available, it may be that your CSAS database has gone and cannot be recovered. In these circumstances, you could check with your IT team to see if the data can be recovered from backups or archives.

25 Glossary

A	
ANPR	Automatic Number Plate Recognition.
APN	Access Point Name. An element in a cellular network that manages GPRS/mobile data connections to an external network or service, such as the Internet.
Attribution	The linking of a name (or 'nominal') to an Identifier within a case, to provide an indication of the person alleged to have been using that identifier.
Authorisation ID	Allows a user to make an advanced search in CSAS.
Azimuth	Data contained in a cellular record that indicates the compass angle at which a cell is pointing, which provides an indication of where that cell provides coverage.
B	
Begins with	Selects records by matching the character string you specify with the starting characters of the values stored in a specific record field.
C	
CDAN	Communications Data Automated Normalisation
CDR	Call Detail Record. A billing data file disclosed by a communications network.
Cell	The radio coverage area provided by a cell site (or cell tower) that allows mobile devices to connect to a network.
Cell Confidence	Describes the confidence you can estimate that the 'start time' and 'start cell' values in a cellular record correlate. If cell confidence is 'true' it means that you can state that a subject device was within the coverage of the stated 'start cell' at the stated 'start time'.
Cell ID	Cell Identifier. The identifying number used by a cellular operator to reference each of the cells in their network.
CF	Call Forward. A call divert to another phone or a divert to a service such as voicemail.
CGI	Cell Global Identifier. A globally unique identifier for each cell in each network. It consists of a country code, a network code, a location area code (for 2G and 3G cells) and a cell ID.
Charging ID	A data element in a GPRS/mobile data record that allows records for the same 'connectivity session' to be grouped together.
Colocation	A type of analytics query that attempts to determine if there are

	times when two or more entities (phones, vehicles, etc.) could have been in the same general area. The calculations used for colocation are rarely able to provide certainty that the entities WERE together, only that the potentially COULD have been together.
Contains	Selects records by matching the word or phrase you specify with values stored in a specific record field. Records are selected only if the search elements specified appear in the same sequential and contiguous order in the field value.
County Lines	A form of illegal drug dealing where established drugs gangs from cities export their drug supply business out into smaller 'county' towns.
Courier Fraud	A type of fraud where the victim is tricked into handing cash over to a 'courier' for safekeeping, who then disappears with the money.
D	
DB	Database. The file or application that efficiently stores data with a system.
DDR	Device Data Record. A type of cellular data that discloses administrative messages exchanged between a subject device and the network (currently only issued by O2 UK).
DPA	Data Protection Act. Legislation that covers the disclosure and use of most other types of data apart from communications data.
E	
EE	Everything Everywhere. A UK cellular provider, owned by BT.
End Cell	The cell used at the end of a call or other cellular record. Also known as the 'last' cell.
Ends with	In searches, selects records by matching the character string you specify with the ending characters of the values stored in a specific record field.
EULA	End-User Licence Agreement. The contract that exists between an application provider and the end user, that stipulates the limits to the users' rights when using the application.
Export	When analysing the identities returned by CSAS you can choose to Export as plain text (tab delimited), as CSV, as Excel or as PDF files.
F	
FA	Forensic Analytics Ltd
File	The types of files which can be Imported to CSAS: .XLS files / XLSX files / .CSV files and .xml files.
G	

GDPR	General Data Protection Regulation. European legislation that covers the disclosure and use of most other types of data apart from communications data.
GPRS	General Packet Radio Service. Originally the method used to provide Internet and data services in 2G networks, has become a standard shorthand way of describing all mobile Internet services even in later generations.
H	
H3	Hutchison Three. A UK cellular provider.
I	
Identifier	Something that uniquely identifies a device or service – such as a phone number, social media handle, email address, etc.
IMEI	The International Mobile Equipment Identity. The International Mobile Equipment Identity or IMEI is a unique identification or serial number that all mobile phones, smartphones and some satellite phones have. It is usually 15 digits long and has a 1- or 2-digit suffix added when it is transmitted over the cellular network.
IMSI	The International Mobile Subscriber Identity is an internationally standardized unique number to identify a mobile subscriber. The IMSI is defined in ITU-T Recommendation E.212. The IMSI consists of a Mobile Country Code (MCC), a Mobile Network Code (MNC) and a Mobile Station Identification Number (MSIN).
IP Address	Internet Protocol Address. A numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.
IPA	Investigatory Powers Act. UK legislation that provides the framework for the lawful disclosure of communications data to law enforcement agencies.
J	
Job	A static import route to bring source data into the Nexus database (listed by Name, Inquiry, Folder Path, Job Actions, File extensions, Team and Security Level) which, along with imported files (.XLS, .XLSX and CSV files) allows a user to search for target and contacted telephone numbers which may link a suspect to a particular crime(s) in one or more cases to aid prosecution. Also referred to as an Indexer Job. Indexer Jobs ingest data into Nexus so that it can be indexed by Name, Inquiry, Folder Path, File count and Current Status.
K	
KML	Keyhole Markup Language. A standard method of encoding map data

	so you can be passed between applications such as Google Earth. You can create KML files to pinpoint locations, add image overlays, and expose rich data in new ways.
KMZ	A 'zipped' or compressed version of KML.
L	
LAC	Location Area Code. An administrative grouping of cells in 2G and 3G networks.
Layer	A group of CSAS Map objects that are treated as being one unit – for example, all of the ANPR cameras imported from the same source file might be placed on a CSAS map and regarded as being one 'layer'. Layers can be shown/hidden separately.
Login	Sends the user Username and Password for authentication. If you have typed your name and Password assigned to you correctly then the CSAS Home page is displayed. If you have mis-typed or used the wrong Username and/or pass- word then authentication will fail and a message is displayed asking you to re-enter your name and Password details.
M	
MAC Address	Media Access Control Address. A unique identifier assigned to a network interface controller. For communications within a network segment, it is used as a network address for most IEEE 802 network technologies, including Ethernet, Wi-Fi, and Bluetooth.
MMS	Multimedia Messaging Service. The technical name for 'photo messaging' in cellular networks.
MOPI	Management of Police Information regulation. A set of guidelines that control the length of time the police are able to retain data and other information related to a case before they are required to dispose of it.
MSISDN	Mobile Station International Subscriber Directory Number. A number used to identify a mobile phone number inter- nationally. MSISDN is defined by the E.164 numbering plan. This number includes a country code and a National Destination Code which identifies the subscriber's operator.
O	
O2	A UK cellular provider.
OSG	Ordnance Survey Grid reference. A UK-specific type map coordinates system.
OSGB36	The mapping standard, based on surveys conducted in 1936, on which the UK-specific OS Grid map reference system is built.
Override Cell	A cell reference generated by CSAS that collects a unique set of cell

	address details for each cell ID and is used to fill in any 'missing' cell address details in source records.
P	
Parsing	The process employed to process source data into a standard format that can be used within CSAS.
Password	The unique Password provided to you to access CSAS.
POI	Point Of Interest. Can be added to a map to show locations which might be related to another Event(s).
R	
Raw Cell ID	A cell ID in the format it is presented in the source file, before CSAS standardises it into a CGI.
RF	Radio Frequency.
RIPA	Regulation of Investigatory Powers Act. Legislation from 2000 that is the forerunner to the current IPA legislation that governs the disclosure and use of communications data.
S	
SAC	Service Area Code. Used in 3G networks to identify a sector/cell or a group of sectors/cells belonging to the same cell site.
SIM	Subscriber Identity Module.
SIM Swapping	The process of moving a SIM card from one device to another in an attempt to obscure the calls made using that SIM card.
SL	Security Level. An administrative element within CSAS that restricts users' access to certain files or cases.
SMS	Short Message Service. The technical name for text messaging within a cellular network.
Source Cell	A record created in CSAS that captures only the cell address details found in each event record.
Start Cell	The cell used at the beginning or start of a call or other cellular connection.
T	
TAC	Tracking Area Code. An administrative grouping of cells in 4G and 5G networks.
Target	The phone number under investigation (also known as the 'subject' number).
TO	Telecommunications Operator. A communications service provider such as a landline or cellular telephone service.

U	
UserID	UserID lets you associate a persistent ID for a single user with that user's engagement data from one or more sessions initiated from one or more devices. Analytics interprets each unique user ID as a separate user, which provides a more accurate user count in the user reports.
Username	The unique Username provided to you to access CSAS.
V	
VF	Abbreviation of Vodafone, a cellular provider.
VRM	Vehicle Registration Mark.



Forensic Analytics Ltd
Registered in England and Wales.
Company No: 08606475
Pixmore Centre, Pixmore Avenue, Letchworth, SG6 1JG, UK

+44 800 158 3830 | www.forensicanalytics.io

