Home Office

Child Abuse Image Database (CAID)

Force Business and Technical Guidance

Version 1.12

Handling Instructions

This document has a classification of OFFICIAL-SENSITIVE under the Government Security Classification scheme. The intended audience for this document is:

- Members of the CAID Project Team
- Individuals within police forces and other law enforcement agencies involved in the implementation or use of CAID in force used for investigation of crimes involving child sexual exploitation
- CAID Solution Supplier Companies

This document should not be disclosed to anyone outside this intended audience without the permission of the CAID Project Management (see Annex A CAID Project Contacts)

This document may be transmitted via email across secure Government networks such as GSI, CJX or PSN. It may be transmitted via email across the Internet only if encrypted in accordance with HMG policy (e.g., AES-256 encryption). It may only be stored on computer system that employs user authentication and access controls to limit access to known authorised individuals (i.e., no anonymous user access) and the system must comply with either ISO27001 control requirements or CESG IS1&2 Baseline Control Set (Deter segment) requirements.

When this document has been superseded, or is no longer required by the recipient, it must be deleted from any storage media and any printed copies disposed of through waste disposal processes suitable for sensitive information.

Change History

Version No.	Date	Details of Changes included in Update	Author(s)
0.1-0.13	14-Aug-2014 01-Dec-2014	CAID Early Adopter Force releases	Charles Spinks
1.0	23-Dec-2014	Document updated see Annex K - Version 1.	Charles Spinks
1.1	15-Jan-2015	Document updated see Annex K - Version 1.1	Charles Spinks
1.2	16-Jan-2015	Document updated see Annex K - Version 1.2	Charles Spinks
1.3	09-Mar-2015	Document updated see Annex K - Version 1.3	Charles Spinks
1.4	28-April-2015	Document updated see Annex K - Version 1.4	Charles Spinks
1.5	11-May-2015	Document updated see Annex K - Version 1.5	Charles Spinks
1.6	09-Jun-2015	Document updated see Annex K - Version 1.6	Charles Spinks
1.7	31-July-2015	Document updated see Annex K - Version 1.7	Charles Spinks
1.8	06-Aug-2015	Document updated see Annex K - Version 1.8	Charles Spinks
1.9	28-Aug-2015	Document updated see Annex K - Version 1.9	Charles Spinks
1.10	30-Sep-2015	Document updated see Annex K – Version 1.10	Frank Lambert
1.11	28-Oct-2015	Document updated see Annex K – Version 1.11	Frank Lambert
1.12	05-Nov-2015	Document updated see Annex K – Version 1.12	Frank Lambert

Table of Contents

1. Introduction 6

1.1 Purpose of this Document 6

1.2 Child Abuse Image Database (CAID) 6

1.3 The Purpose of the CAID 6

1.4 Who can have access to the CAID? 7

1.5 Releases of CAID software 8

1.6 Status of CAID 8

1.7 CAID Governance 8

2. Implementing CAID in Force 10

2.1 Introduction 10

2.2 Force Single Point of Contact 10

2.3 Activities for forces to undertake to connect to CAID 10

2.4 Force Project Timelines 12

2.5 Suggested Force CAID Implementation Team 12

2.6 Support and Communication 13

2.7 Costs 14

3. Roles 17

3.1 Force Roles 17

3.2 Other CAID roles 20

4. Force Hardware and Software 23

4.1 Introduction 23

4.2 Data and Image Transfer Server 23

4.3 CAID User Workstations 25

4.4 Software required to support CAID roles 29

4.5 Compatible Force Categorisation Tools 30

4.6 Connection Details for Administrators 31

4.7 PNN3 Migration to PSN 32

4.8 IIOC Categorisation Workflow 33

4.9 Hash/Fingerprint Technology Supported 34

5. Security Considerations 35

5.1 CAID Government Security Classifications 35

5.2 Connection to CAID 35

5.3 Security Vetting 36

5.4 Business Impact Assessment 37

5.5 Suggested Network Architecture 38

6. CAID Business Rules 43

6.1 CAID Business Processes 43

6.2 Trusted categorisation 43

6.3 IIOC Guidance on Categorisation 44

6.4 Standardisation of Case Naming 45

7. Service Management 46

7.1 User account management: 46

7.2 Business Support 47

7.3 Connecting to CAID 47

7.4 Support 47

8. IIOC Information Exchange with CAID 49

8.1 Receiving CAID Updates 49

8.2 Uploading Force IIOC Information 50

Annex A **CAID Project Contacts 53**

Annex B **Glossary 54**

Annex C **Odata schema 56**

Annex D **Import and Export To CAID. 58**

D.1 Griffeye ..... **Error! Bookmark not defined.**

D.2 C4ALL (ver 1.1) 62

D.3 C4ALL (v2.0) 65

D.4 LACE 69

D.5 Ziuz – VizX 73

Annex E **Software Installation 74**

E.1 Introduction 74

E.2 SSL Certificates 74

E.3 Domain Name Service / Hosts File 78

E.4 Hubstream Intelligence Agent 79

E.5 FTPS Client 82

E.6 Hubstream Web Interface 84

E.7 Griffeye Analyze CS Web Interface 84

E.8 Remote Desktop Connection (to access Griffeye Analyze CS Desktop Client) 84

Annex F **Connectivity Testing 85**

F.1 Introduction 85

F.2 Prerequisites 85

F.3 Support 85

F.4 Process 85

F.5 Issue resolution 88
F.6 Reporting of results 88
Annex G **Force Support Desk Instructions 89**
G.1 Introduction 89
Annex H **Hubstream Griffeye Product Roadmap 90**
H.1 Griffeye Analyze 90
H.2 Version: 15.2.0 90
H.3 Version: 15.3.0 90
H.4 Hubstream Intelligence 91
H.5 Version: 2.5 SP1 91
H.6 Version: 2.5 SP2 92
Annex I **Force Numbers 93**
Annex J **Quick Fix Guide 94**
J.1 Griffeye and Hubstream Web User Interfaces 94
J.2 Hubstream Log File Error Messages 94
Annex K **Change Log 96**
Annex L **Referenced Documents 99**

1. Introduction

1.1 Purpose of this Document

This document is solely for the Audience in the handling instructions on page 1; this document should not be disclosed to anyone outside this intended audience without the permission of the CAID Project Management (see Appendix A for contact details).

The document provides the technical and business information necessary to implement and configure the local CAID solution. This document has been validated by the early adopter forces.

1.2 Child Abuse Image Database (CAID)

In July 2013, the Prime Minister committed to delivering a single secure database of indecent images of children (IIOC) by the end of 2014. CAID is the resulting project, which is built upon initial work by National Crime Agency – CEOP and the Home Office Cyber Crime Programme.

1.3 The Purpose of the CAID

The Child Abuse Image Database project or CAID provides UK law enforcement with new capability to significantly improve investigations into indecent images of children (IIOC).

Use of CAID by UK law enforcement will:

- provide consistent quality of grading for prosecution purposes
- increase the number of abusers identified as a result of IIOC investigations
- increase the number of children safeguarded as a result of IIOC investigations
- increase the throughput of IIOC cases – seized devices are Analyzed more quickly enabling officers to action more cases
- reduce the amount of police time and duplication of effort used categorising images
- reduce/prevent duplication of victim ID effort through signposting information
- increase our ability to protect children who are victims of sexual abuse from repeat victimisation and public identification
- increase the distribution of image metadata used for victim ID
- disrupt the availability of child sexual abuse content hosted anywhere in the world
- reduce the number of IIOC readily available on the internet
- increase the number of distribution networks identified and disrupted.

CAID will improve forces' ability to:

- identify recent images of abuse, increasing the likelihood of finding the victim
- Analyze images and extract information to locate the child or abuser
- identify and disrupt distribution networks
- to share information within the UK.

In addition, CAID will:

- free up police time from repetitive, time consuming and distressing viewing of images
- support and enhance the capability of the police and NCA to investigate efficiently cases of online CSE
- improve the ability of forces to share information within the UK or internationally
- enable communication service providers to filter, block or remove IIOC from the internet.

At the force level:

- Every force can check image hashes from seized devices against known illegal image hashes and common non-illegal hashes.

- Officers can distinguish never-seen-before images, non-validated images (which have been seen before, but as yet, have less than three grading votes), and images with a trusted grade.
- Forces can upload data to the central image database, including:
  - new (never seen before) illegal images
  - grades for non-validated images
  - case relevant metadata against image hashes
  - update images where victim has been identified and safe guarded.
- Officers responsible for the case can upload the data to national database – so officers do not have to see the same images once a trusted grade received, and the metadata becomes available for all forces.
- Officers can build intelligence on their case by referring to images and metadata held on the central image database.

At the national and international level:

- Hashes and metadata will be able to be imported and exported across international policing boundaries – including to Interpol.
- Officers across police forces can collaborate by flagging images of relevance to other forces to support:
  - identifying and stopping producers of images
  - identifying and closing down distributors of images
  - identifying and safeguarding victims of child abuse and rape.
  - Forces can work towards validating the categorisation of images so that we build a trusted set of hashes to support prosecution.

1.4 Who can have access to the CAID?

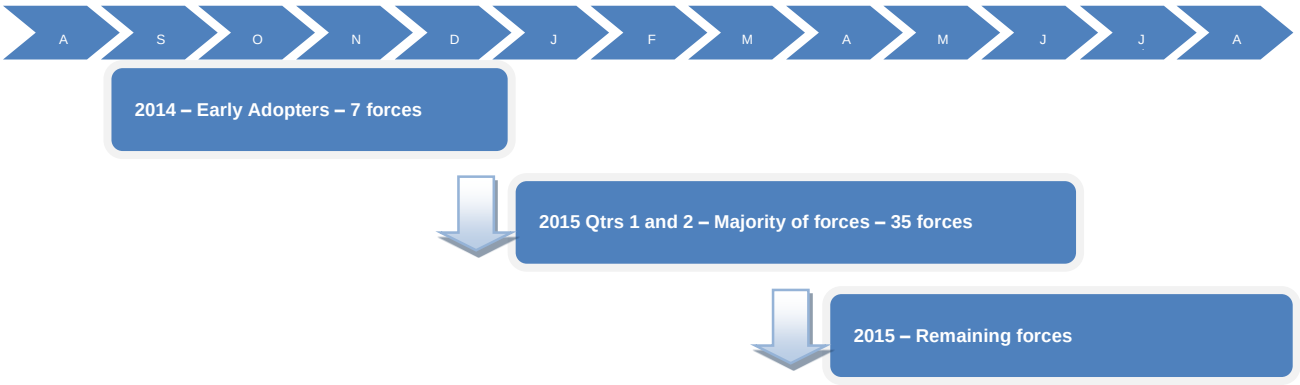
Seven forces have participated in the testing of the CAID database and are the early adopters;

Avon and Somerset Constabulary	Cheshire Constabulary	Lancashire Constabulary
Metropolitan Police Service	Norfolk Constabulary	Suffolk Constabulary
West Yorkshire Police		

All forces in the UK and other law enforcement agencies such as the NCA can have access to CAID

1.4.1 Roll-out of CAID

CAID is being rolled-out to forces in three tranches.



The rollout is managed and assisted by the CAID Implementation team for more details please contact caid-implementation@homeoffice.gsi.gov.uk

1.5 Releases of CAID software

The CAID software is being released in three phases:

1.5.1 Phase 1 (Dec 2014)

Provides the seven early adopter forces with:

- Secure access to 23 million hashes of which 1.5 million are undisputed, graded hashes, and to over 4.4 million images.
- The ability to upload images and hashes and download hashes for comparison.
- A secure web-based user interface.
- The ability to mark images where the victim has been identified so that other forces can concentrate on identifying other victims.
- Compliance with OData standard and latest Project VIC data specification, enabling data sharing with international partners.
- Extended searching capability including geo location.

1.5.2 Phase 2 (April 2015)

Will bring more forces on board and provide:

- The ability to handle additional categories of images.

1.5.3 Phase 3 (Aug- Nov 2015)

1.5.3.1 3.1 (August 15)

Will bring the remaining forces on board, and provide:

- A secure desktop-based user interface.
- Improved reporting features.
- The ability to send alerts and notifications to other forces.

1.5.3.2 Phase 3.2 (November 15)

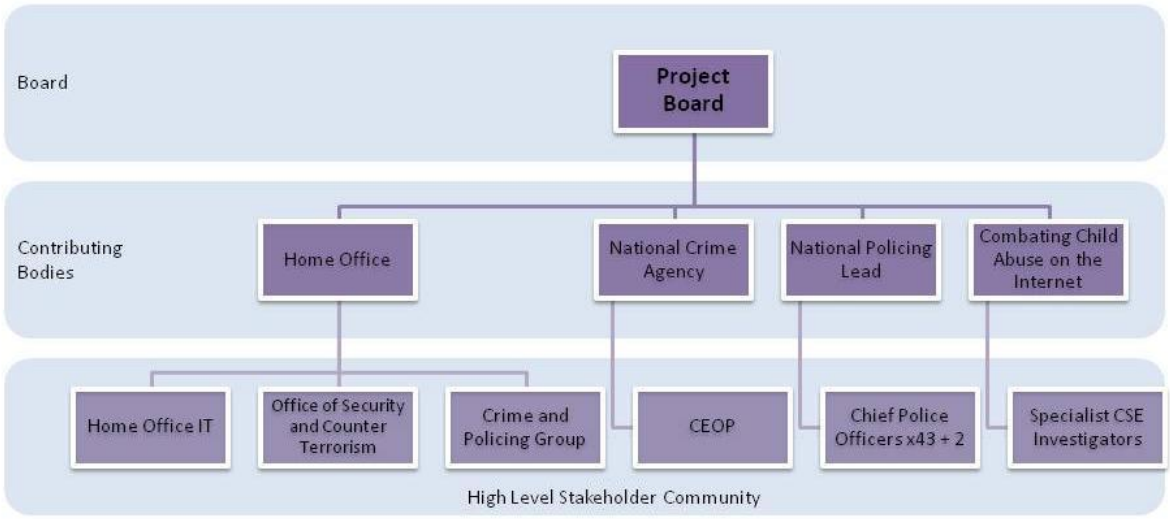
- The ability and support to handle video.

1.6 Status of CAID

- CAID is in live operation
- 1.5 million hashes have been brought to “trusted grade” status with the help of the Internet Watch Foundation. Together with over 4.4 million images, these form the core of the central database.
- The central database has been through intensive user acceptance testing.
- The seven early adopter forces have all successfully connected to the central database.
- Early adopter forces have all received training in the use of the central database and wider training on image categorisation and victim identification.
- A national victim ID strategy to ensure consistent processes for gathering and disseminating intelligence on Victim Identification work is being developed by the National Crime Agency (NCA).

1.7 CAID Governance

The diagram below outlines the governance structure for CAID at the national level, and illustrates how different elements of this structure interact.


Board
Project Board
Contributing Bodies
Home Office
National Crime Agency
National Policing Lead
Combating Child Abuse on the Internet
Home Office IT
Office of Security and Counter Terrorism
Crime and Policing Group
CEOP
Chief Police Officers x43 + 2
Specialist CSE Investigators
High Level Stakeholder Community

2. Implementing CAID in Force

2.1 Introduction

CAID has two separate services designed to assist with different process in the forces IIOC, Online Child Sexual Exploitation and Victim Identification areas

- A Data Exchange Service (Hash, metadata and image transfer)
- A Service for CAID user interface (Victim ID, Intel)

The **Data Exchange** service allows you to:

- Regularly download the CAID hashset, categorisations and metadata for use within your forces existing categorisation tools for example C4ALL, Lace, Griffeye Analyze DI or VizX
- Regularly upload new images, hashes, categorisations and metadata from your IIOC cases

This service is provided via the Hubstream Intelligence Agent Software

The **CAID user interface** allows you to support your victim identification and online child sexual exploitation investigators by (for example);

- Providing image search capability on the national library for images either by the content of an image or by any of the metadata such as camera serial number
- Identifying other forces who have seen the exact or similar images
- Allowing you to flag images of relevance to other forces:
- Providing information on whether the victim has been identified or the image distributed
- Allowing you to Analyze images and extract information to locate the child or abuser

This is provided via the Griffeye Analyze CS software

There are other components that are used to support specialist roles

If you currently don't have victim identification or online child sexual exploitation roles in your force then this is one of the aims of the programme - to create this capability within your force. Further details will be released upon the publishing by NCA CEOP of the National VID Strategy.

2.2 Force Single Point of Contact

Each force has nominated a single point of contact for the project. The Single Point of contact is the focal point for each force's CAID implementation efforts and will be the point of receipt for all communications between the Implementation team and the Force. The list of CAID SPOCS is available on POLKA at

https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Contacts

2.3 Activities for forces to undertake to connect to CAID

A Force Action Plan detailing the products and key activities that should be delivered locally by forces in order to implement CAID, has been produced. It is also comprised of a checklist template for you to develop your local plans for delivery.

The Force Action Plan template can be found on POLKA at

https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Resources

This FAP is for use by forces to plan for and support the local implementation of CAID. It will also be used to measure implementation progress to self-assess how ready forces are for CAID.

2.3.1 The Force Action Plan Structure

The products and key activities are grouped into two components;

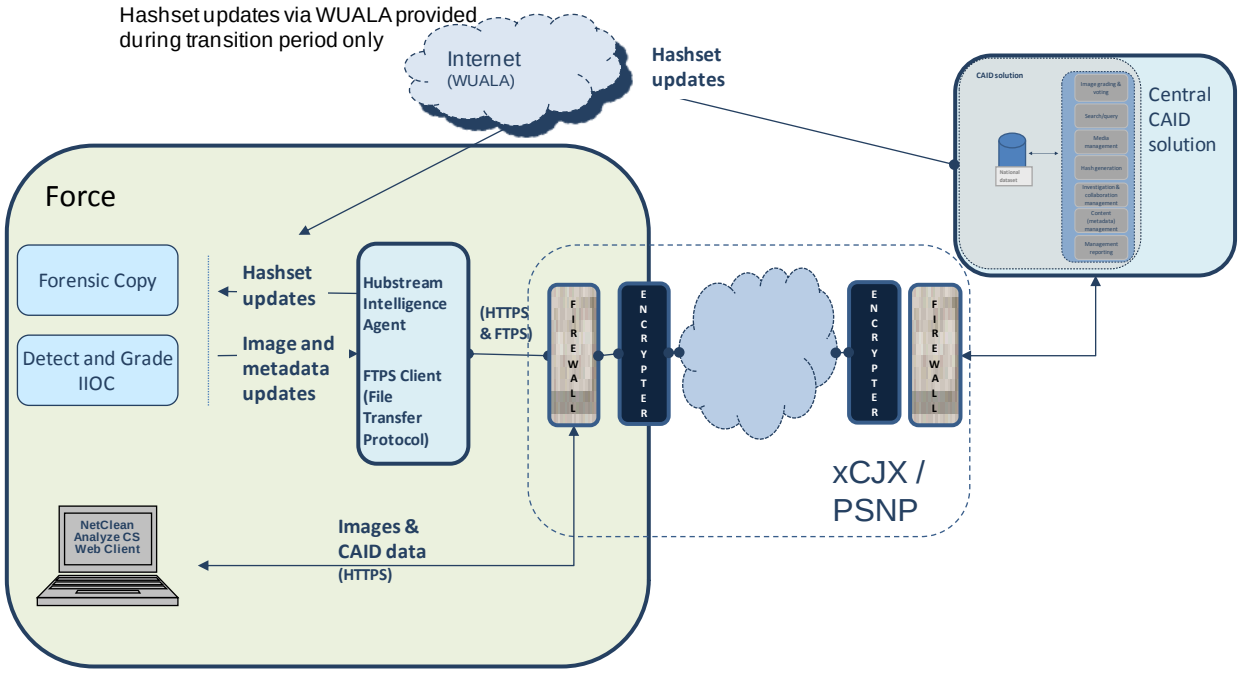
- High Level milestones, for project reporting;
- Checklist for day-to-day force project management monitoring;

Within these groups, where the products and key activities are relevant to only one element of CAID, this has been identified:

- Data Exchange – via the CAID Local element to transfer Hashset updates, image and metadata updates between forces and CAID
- CAID User Interface – to allow force investigators access to the CAID central database to conduct searches etc.

2.3.2 Scope of force local deployment

The elements marked within the force boundary are the responsibility of the force to procure and implement. The software components provided by the CAID Project within that boundary are the Hubstream Intelligence Agent and CAID Application Software.



2.4 Force Project Timelines

Using the Early Adopter Forces as a benchmark the anticipated timelines to implement are shown below

FAP URN	Startup / Initiation
1 / 8 / 9	Startup and initiate the project e.g. Appoint the project board, identify and secure the key resources, commitment and finance

FAP URN	Planning
21 / 22	Identify the locations where CAID is to be deployed in force
31	Identify CAID Users
6	Create force CAID deployment model
27	Ensure the forces current IIOC detection and grading software is compatible
7	Develop Communications Strategy
9	Create the delivery (project) plan

FAP URN	Delivery
2 / 10 / 11 / 24 / 28	Begin the development of the policies and procedures
19	Assess the network / storage requirements
16 / 17 / 18 / 20	Create the secure network access between the CAID components
23	Assess and ensure Code of Connection Compliance
32	Ensure appropriate vetting in place
13 / 14 / 15	Provision CAID force infrastructure / hardware
25 / 26	Install, configure and test the CAID local software elements
30	Undertake CAID Training
29	Undertake Testing - connectivity / user acceptance

FAP URN	Go - Live
12	Go Live Implementation

3

2.5 Suggested Force CAID Implementation Team

The roles outlined below provide a suggested project structure within forces. This is based on lessons learned from the Early Adopter forces and is suggested as good practice for the implementation of CAID. The specific roles may vary depending on force circumstance and change over time as implementation progresses. It is anticipated that the roles below would be part time over a three to four month period.

It is possible that the Force's nominated CAID Single Point of Contact (SPoC) would be either the SRO or Child Abuse Investigation Lead.

- ACPO lead / Force Senior Responsible Owner (SRO)

  The force ACPO Lead is the SRO for CAID at the force level. The SRO will have responsibility for the implementation of CAID within the force. This includes responsibility for the implementation of change and for the achievement of targeted benefits that meet the objectives of the project.

- Project Board

  The project board should include senior stakeholders at the force level and it is responsible for the direction of the project within the force. The board will take decisions on local funding, priorities and delivery options. The project board has overall responsibility for the leadership, direction and delivery of CAID, and for ensuring legal compliance of all CAID-related policies and procedures in the force.

- Project Manager

  The Project Manager is responsible to the force SRO for delivering CAID within the force. This will include defining the targeted benefits and identifying and implementing necessary changes in business operations. The Project Manager will 'own' the CAID Action Plan for the force, oversee all project related activities and report to the Project Board on progress. The Project Manager will deliver the targeted benefits, assess and report on progress, lead and manage change.

- Child Abuse Investigation Business Lead

  The Child Abuse Investigation Business Lead should be an individual who wants the change and will attempt to obtain commitment and resources for it. They will be key to influencing others and gaining commitment to change from within the Child Investigation and High Tech Crime Unit Area.

- IT Lead

  The IT Lead will be responsible for technical implementation leading up to, during and after transition to CAID. They will ensure that the force is technically ready for CAID, service levels are maintained and IT requirements are met.

- Information Security Lead

  The Force Information Security Lead (ISO) will be responsible for ensuring the force local implementation meets all local security policies and national code of connections. The ISO is required to make a connection request to the national accreditor.

  From the Early Adopter phase this was identified as a key role to engage early

2.6 Support and Communication

2.6.1 Support

Support to implement CAID is provided by the CAID Implementation Team.

The team can support you and answer questions by;

- Email
  The CAID Implementation team provide regular updates by email these are sent out by email to SPoCs. You can request to be added to the mailing list by emailing caidbusinesssupport@westyorkshire.pnn.police.uk

- Police OnLine Knowledge Area (POLKA)
  There is a CAID implementation community on POLKA where all the documents and other resources are made available. Please register with POLKA and the CAID: Implementation community https://polka.pnn.police.uk

- Onsite Visits
  The Implementation Team can visit your force at all stages of your project from initiation to go-live to give briefings on the project, answer questions directly and assist in the implementation activities where necessary

2.6.2 Useful documents and resources

Document	Description	Link
Force Action Plan	The Force Action Plan (FAP) supports the delivery of CAID in forces. It details the key activities that should be undertaken by forces in order to implement CAID and provides a checklist of tasks.	https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Resources
CAID Frequently Asked Questions	Frequently Asked Questions (FAQs) on the Child Abuse Image Database (CAID)	https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Briefings%2band%2bFAQs
CAID User Security Operating Procedures (SyOps)	The SyOPs set out the procedures to be followed by users of the CAID system regarding access to, and use of, system facilities. Authorised users of the CAID system should read the whole document and then sign the declaration in Appendix B.	https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Resources
CAID Force Connection Application	The purpose of this document is to ensure that police forces are ready to connect to the Central CAID system via the xCJX or PSNP Secured national network. The Force ISO Should complete and submit this to the Home Office	https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Resources
CAID Force Initial Users Template	This template should be used by a force for creating the initial force users for CAID. Please complete the form for each user required on CAID or requiring access to the helpdesk	https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Resources

2.7 Costs

To assist forces in calculating the costs involved in deploying and using CAID we have produced a simple cost estimate. These should not be used directly as a forces own costs as costs will vary based on the deployment model and complexity. The costs are based on the following assumptions;

- Deployment solution
  - The Force has a single High Tech Crime Unit (HTCU) running on an un-assured network.
  - The CAID Data Exchange component will be deployed within that HTCU.
  - To connect the Secured CAID Data Exchange component to the un-assured HTCU Network an air-gap and separate computer to undertake malware protection will be deployed (see section 5.5 Suggested Network Architecture)
  - The CAID user workstations are deployed within the HTCU

- Other Assumptions
  - HTCU has sufficient physical security to ensure that no further security measures are required. For example additional smart card access would not required.
  - No additional AEP encryptors are needed.
  - No further staff required in order to undertake Victim Id and/or additional grading work
  - No additional machines are required for additional grading work.

Note: Where any of the above assumptions are not correct for your Force or you have a different deployment model from the above for example more than one grading location - then your costs will vary from this estimate.

Total estimated costs for 1st year implementation of CAID	Estimated Cost	Number Required	Total
Cap-Ex Costs			
Hardware			**Total**
Server for Hubstream	£3500	1	£3500
Machines to access CAID (Griffeye Analyze CS Webclient)	£800	2	£1600
Cisco (to protect network leg from HTCU to xCJX or PSNP entry point)	£500	2	£1000
Machine to undertake Malware Scan	£800	1	£800
Removable media for air gapped solution	£50	2	£100
			£7000
Op Ex costs			
Software			
Windows Server Licensing cost (Hubstream machine)	£500	1	£500
PSNP bandwidth (costs for additional bandwidth)	0		0
Anti-virus / Malware protection	£100	1	£100
FTP licensing costs	£150	1	£150
			£750
Force network accreditation			
Pen testing	£3000	1	£3000
Syops/RMADS	£7500	1	£7500
			£10500
Total estimated costs for 1st year implementation of CAID excluding resource costs.			£18250

Total estimated costs for 1st year implementation of CAID	Estimated Cost	Number Required	Total
Cost Recovery			
Costs Recovery from Force	£24500		£24500
The annual cost has been revised from the one notified by Simon Bailey in a letter to Chief Constables on the 15th of September 2014. The annual cost to each force for connecting to the CAID is now £24.5K p/a for the first two years. These costs include funding for the software contract, implementation costs, the costs associated with the central hosting of the database and a reserve to fund further software developments as required. Whilst the figure has not been set for year three, forces should budget for similar cost £24.5K. After this point the CAID contract will be subject to re-procurement			

Costs of implementing a Gateway Solution

Where a force is deploying a gateway solution as described in section 5.5 Suggested Network Architecture then actual costs have been provided by the early adopter force West Yorkshire Police. Please note that not all costs may be relevant to your implementation and your costs for individual items may vary from these. Where a gateway solution is being deployed some costs from the table **above** will no longer be relevant for example “Machine to undertake Malware Scan“ as this is undertaken by the “Dell R620- sever” below

Description	Cost
Hardware	
Dell R620- sever	£3,409.53
Cisco firewalls and switches	£12,596.90
Security and pen testing of the system	
Pen testing	£3,000
Upgrade of Cabinets to Confidential	£5,086.00

3. Roles

To operate, manage and use CAID a number of roles have been identified some of which are mandatory for use of the CAID system. A force should identify the relevant staff who will be undertaking the roles.

3.1 Force Roles

Role Name	Description	Mandatory

Police Investigator
 	
(Formally Online Child Sexual Exploitation (OCSE) Investigators)
	• Investigators are responsible for querying CAID for the purposes querying CAID in relation to active investigation of online child sexual exploitation and of pro-actively identifying new leads of online child sexual exploitation
	• Investigators will be able to upload, query and edit data on CAID as well as export search results
	• Investigators can flag images for action to Police Investigators and Victim ID Officers in other forces
	• Investigators can receive flagged images for action
	• Link images
	• They can add tags to images and hash values
	  ○ Where the victim is identified
	  ○ Where there is a need for a concerted effort to identify the victim
	  ○ Images of interest
	  ○ Where the perpetrator is identified
	  ○ Where there is a need to a concerted effort of identify the perpetrator
	  ○ Group images based on series
	• This role can be split into two business roles or one specialist role dependant on how local enforcement agencies handle online child sexual exploitation within their forces.
	• There must be at least one assigned officer per force with this role to receive images for action from other forces. As a user role, this will be a force implemented role which may link into NCA-CEOP or a central online child sexual exploitation policing function
		Yes

Force Business Administrator	• This user will have no access to view or edit data within CAID • Their responsibility lies in: • Adding new users to the system at a local force level • Providing first line support to officers in a local force • Raising support calls to Claritas • Monitoring any diagnostic tools installed locally on CAID • Viewing audit logs for local use • This role will be held by local IT support desks who need to be fully aware of CAID and how to support the product	Yes

Role Name	Description	Mandatory

Image and Video Graders – *(No direct access to CAID)*	***Existing Force Role***
	• This role is carried out by the police officer responsible for the Online Child Sexual Exploitation (OCSE) case.
	• The officer is responsible for assigning a category to images seized from their suspect's devices
	• The officer will need to have completed a national standard for grading online course and hold an up to date certificate before being allowed to grade images and videos
	• The officer will need to tag images where a victim has been identified in the case they are working on
	• The officer will not have access to CAID but will complete their grading using the local grading tool available in their forces
	• The results of what the officer has graded will added into CAID
	• Where possible, this will include:
	  ○ New Images graded at Categories 1-6 and 9
	  ○ Known hashes graded at Categories 1-6
	  ○ Case reference and force identifier
	  ○ Officer identifier (this may not be feasible in the first delivery of CAID)	

Victim Identification Investigators	• Victim ID Investigators are responsible for querying CAID for the purposes of identifying victims and ensuring victims are safeguarded. • Victim ID Investigators will be able to upload, query and edit data on CAID • Investigators will not be able to change categories on images* • Victim ID Investigators can flag images for action to Police Investigators and Victim ID Officers in other forces • Victim ID Investigators can link images • Victim ID Investigators can receive flagged images for action especially images taken outside UK Force Boundaries • They can add tags to images and hash values • Where the victim is identified • Where there is a need for a concerted effort to identify the victim • Images of interest • Group images based on series • As a user role, this may be managed by the NCA Victim Identification Unit with specialist Victim Identification officers based in Police Forces	Yes

Role Name	Description	Mandatory

Force Auditor	• It is anticipated Forces have existing auditors who audit access and use of National Systems and their remit should be extended to include auditing access of and use of CAID.
	• It should be noted that the requirements for the Local CAID Auditing role, in particular, is in addition to auditing requirements on police forces arising from:
	  ○ HMG Security Policy Framework (SPF), which is mandatory on all Government departments and agencies.
	  ○ ACPO, which publishes guidance on auditing.
	  ○ PSNP, which includes auditing requirements in its Code of Connection.
	• It is important that whoever fulfils an auditing role is independent of the CAID operational, administrative, user roles – nobody, especially privileged users, should audit themselves.
	• Local CAID Auditors may review logs of their Local CAID system components, where applicable.
	• Local CAID Auditors will ensure compliance of the CAID users on their site(s) with CAID User SyOPs. This involves checking that CAID users are following procedures as specified in SyOPs.
	• The Local CAID Auditors Local will perform CAID compliance audits periodically (anticipated quarterly or annually – to be decided).
	  ○ The Local CAID Auditor will produce a report, which is sent to the National CAID Auditor, outlining what was checked, any deviances from SyOPs found and any remedial actions taken.
		Yes

Role Name	Description	Mandatory
Data Transfer Administrator (formally Local CAID)	• This is a system and user role which is responsible for ensuring CAID updates on hash values are received by law enforcement agencies to be used for grading and sends new images and categorised hash values back to CAID • It is expected that this role will sit within High Tech Crime Units or in the secure physical location where IIOC content is viewed and graded • Data Transfer Administrator will monitor new updates received into the force and ensure images and hashes graded by Image and Video Graders are sent to National CAID • Data Transfer Administrator will add data with a time, date and force stamp of when any data was sent and received. • Whilst CAID transitions to a live service and potentially for some time after, this role may require some 'human' effort to upload a file location and pull off the hash values to a local grading tool. This user role would sit within a High Tech Crime Unit where the local CAID service is situated. • Data Transfer Administrator will identify images from a case that are new to CAID to be sent and send new Categories against hashes known by CAID • Data Transfer Administrator will not be able to change/ delete any categories, hash values or tags created within the local grading tool.*	Yes

3.2 Other CAID roles

Role Name	Description	Mandatory
Grading Adjudicator	• This role is specifically for managing grading conflicts only • Grading Panel Adjudicators will have access to the National CAID for the purposes of resolving conflicts on images of IIOC which are either indicative/ borderline IIOC due to age determination or where an image has been categorised by LEAs as IIOC but a category cannot be agreed on. • Grading Panel Adjudicators will be presented with a report of disputed images with the image • A Grading Panel Adjudicator will assign a category of either 1: A, 2:B, 3:C or 6: Borderline (not possible to resolve) • Images that have been assigned a category by a Grading Panel Adjudicator will be determined to have a trusted category that cannot be overridden • Members of the Grading Panel Adjudicator must be specialists at victim analysis and have received training specific to grading images based on the category	

Role Name	Description	Mandatory
	• Users in the first instance will be based within the National Business Administration Function. Depending on volumes needed to be handled, the role may also go to specialists within forces once the functionality can be made available	

System Administrator	• This user will have no access to view or edit data within CAID
	• Their responsibility lies in:
	  ○ Add new users to CAID and inform the business administrator function to allocate a role to the new user
	  ○ Authenticating existing users of CAID
	  ○ Carrying out password resets for existing users of CAID
	  ○ Performing admin tasks including upgrades/ patches etc
	  ○ Viewing audit logs
	• This role will be held by the service provider for CAID on behalf of West Yorkshire Police – in this instance, Claritas	

NCA Bureau	• The Bureau will be based in Warrington and will have all the same user rights as Local Graders and Police Investigators.
	• They will be responsible for:
	  ○ Loading images from NCMEC and other sources on to CAID
	  ○ Check whether NCMEC images are known to CAID
	  ○ Categorise new images using a local grading tool (either using the categories mentioned previously or in time critical situations with a Cat9 CETS case specific and include the CETS case reference number)
	  ○ Allocate new or known images/ meta data to a police force for action
	  ○ Tag images where victim, perpetrator or distributor has been identified or needs to be identified
	  ○ Link images
	  ○ They will have some additional metadata to be added along with the images including IP address and email address for any chat logs where images were found from
	  ○ Chat logs themselves will not be loaded onto CAID and remain in CETS (Child Exploitation Tracking System)	

National Business Administrator (Application Manager)	• In addition to the roles specified above, the business administrator will be capable of deleting images deemed no longer relevant to CAID, archiving images and data from being searchable. • The business administrator will also be responsible for any new user role definition as required by the business and subject to the functionality CAID will allow	

Role Name	Description	Mandatory
	• The business administrator will confirm which role a new user will be assigned to • The Business Administrator role will report into the SRO for CAID – [To be confirmed] • Please see separate Business Administrator Function for more information	
National Auditor	• The National CAID Auditor will review the Griffeye and Hubstream application logs who will notify appropriate Local CAID Auditors of anything relevant to them. • The National CAID Auditor will ensure compliance of CAID administrators and privileged users with CAID Admin SyOPs. • The National CAID Auditor will undertake National CAID compliance audits periodically and produce a report. This report will include highlights from Local CAID audits, as well as National audit findings. This report will be sent to the CAID Security Working Group (SWG). The CAID system has a number of sources of protective monitoring collected via monitoring agents on the servers, system logs and a QinetiQ facility that meets the Detect & Resist segment requirements. The System and network logs are reviewed by Vodafone for PSNP/xCJX for wide area networking and Claritas/WYP for Central CAID infrastructure. More detail on auditing is provided in the CAID RMADS Section 5.1.7, Protective Monitoring & Auditing (Awaiting Publication)	
NCA CEOP Victim ID	TBA	

4. Force Hardware and Software

4.1 Introduction

Two types of environment are required in force to support the two types of service:

- Data and Image Transfer

  Infrastructure required to perform data synchronisation with the CAID central database

- CAID User Workstations

  Infrastructure required allowing various force users to connect interactively to CAID to perform roles[1] such as;

  - *Grading Panel Adjudicator*
  - *Victim Identification*
  - *Online Child Sexual Exploitation Investigators*

Both these environments should be:

- Supported via the forces local support arrangements.
- Part of the forces accredited secured environment - Accredited "Secure" machine with user authentication and access controls

4.2 Data and Image Transfer Server

Purpose

- Download
  - Hashset, Categorisations and Metadata for use within the forces triage / categorisation tools
- Upload
  - Hashset, Categorisations and Metadata from new IIOC cases
  - New images categorised in one of the in-scope for image upload categories

Two Software Components perform the data transfer

- Hubstream Intelligence Agent
- FTPS

FTPS is only required to support a process to upload images missing from the CAID library.

The two software components should be located on a single physical or virtual machine to support the future transition to using the Hubstream Intelligence Agent

Requirements

Data and Image Transfer		
Component	**Hubstream Service Agent**	**FTPS**
Version	2.5.210.0 (CAID Release 2)	N/A
Purpose / Function	Windows Application - Upload of the OData JSON File case exports - Download of the OData JSON File Hashset Deltas	- Upload of new images and video categorised in one of the in-scope categories

[1] These roles are to be confirmed

	Communicates with the CAID Hubstream Web Server to update the Hubstream Intelligence Database	
Hardware	***Minimum Requirements***	***Minimum Requirements***
- Memory	1GB	N/A - Client Specific
- Processor	1ghz	N/A - Client Specific
- Disk space	100Mb plus storage space for - incoming hashset 20GB - outgoing hashset and metadata files (force Specific)	Force Specific sufficient for outgoing new IIOC image and video files
- Screen	No minimum	N/A - Client Specific
- Other	Virtualisation of Hardware is possible	N/A - Client Specific
Software pre-requisites	Windows Installer 4.5 Microsoft .NET Framework 4.5	N/A - Client Specific
Operating systems Supported	Windows 8.1 Windows 8.0 Windows 7 SP1 Windows Server 2012 R2	N/A - Client Specific
Protocols	HTTPS (recommended)	FTPS
Connection Details		
- Service End Point		
- xCJX IP Address		
- Port(s)	443 (Default HTTPS)	990 (Control) TBA (Data)
Max installations / Licenses per force	Unlimited	
Software Distribution	Updates via HTTPS to the server from http://caid-1.x.pnn.police.uk	N/A
File transfer management to manage network load?	Yes	N/A
Security		
- Controls required on the computer	Accredited "Secure" machine with user authentication and access controls	
- How will users be created and managed	Via Active Directory, and registration with Intelligence Server	TBA
- Computer part of the central CAID domain	No	No
Software Maintenance		
- Release Cycle	Intelligence Server cycle (TBA)	
- Who will Install Patches	N/A	
- What is the notification mechanism	N/A	

4.3 CAID User Workstations

Purpose

To allow various force users to connect interactively to CAID to undertake management of the intelligence data, querying of database via free text, single fields or batches of search attributes and images searching in undertaking the roles

- *Online Child Sexual Exploitation Investigators*
- *Victim Identification*
- *NCA Bureau*
- *Grading Panel Adjudicator*

Software Components

- Griffeye Analyze CS Web Client
- Hubstream Web Client
- Remote Desktop Connection
- Griffeye Analyze CS Desktop Client[2]

Remote Desktop Connection

Remote Desktop Connection (terminal services) is required to access the 10 available sessions of Griffeye Analyze CS Desktop Client available via Remote Desktop Services.

This is only available for limited roles see.4.4 Software required to support CAID roles The only standard force role requiring this is the “Auditor”

[2] The Griffeye Analyze Desktop Client will be available in release 3 of CAID due for release in November 2015

Requirements

	CAID User machines		
Component	**Griffeye Analyze CS Web**	**Hubstream WebClient**	**Griffeye Analyze CS Desktop**
Version for CAID deployment	v14.1.2 (x64)	n/a	15.2
Purpose / Function	Communicates with the CS Web Server - Management of the intelligence data (e.g. category, series, identification status, persons and roles, distributed status, comments, attachments). - Search intelligence / metadata via free text or fields - Search Images - EXIF data analysis - File download - Charts of meta data- and intelligence statistics	Web Application Communicates with the Hubstream Web Server Allows management of the intelligence data (in Hubstream Intelligence Database) Search intelligence data Notifications	Windows Application Communicates with the CS Application Server / CS File Storage - Management of the intelligence data (e.g. category, series, identification status, persons and roles, distributed status, comments, attachments) - Search intelligence / metadata via free text or fields - Search Images - Image Grading - Grading conflict resolution (Grading Panel) - Reporting & statistics - Review audit log and CS server status - Administrate cases and media files (add, remove, edit) - Configure user roles - File and data exports - EXIF data analysis
Hardware	***Minimum Requirements***	***Minimum Requirements***	***Minimum Requirements***
- Memory	OS recommendations	OS recommendations	8GB
- Processor	OS recommendations	OS recommendations	Multi core CPU recommended
- Disk space	OS recommendations	OS recommendations	500 Mb plus storage for local hash sets
- Screen	No minimum	No minimum	Twin monitor with a resolution of 1680x1050 or higher recommended
- Other	Virtualisation of Hardware is possible	Virtualisation of Hardware is possible	Virtualisation of Hardware is possible
Software pre-requisites	Web browser - Chrome (version 27 or higher)	Web browser - Chrome (version 27 or higher)	Microsoft .NET Framework 4.5

	- IE (version 9 and higher, version 7 and 8 results in limited functionality), - Firefox (version 22 or higher) - Safari (version 6)	- IE (version 9 and higher) - Safari (version 6)	
Operating systems supported	Platform independent	Platform independent	Windows Vista 64 bit OS Windows 7 64 bit OS Windows 8 64 bit OS
Ports and Protocols	HTTPS SOAP over HTTPS	HTTPS (recommended)	AES 128 Encrypted TCP/IP **17000 (Data, AES 192 Encrypted)** **17001 (File Streaming, TLS - preferably ver. 1.2)**
Connection Details			
- Service End Point			
Max installations / Licenses per force	Unlimited	Unlimited	Unlimited
Software Distribution	Analyze CS Web server		The MyGriffeye portal (Restricted part of www.Griffeye.com)
Web Clients			
- Java Applets or other components download to the users machine?	None	None	N/A
- Are browser add-ins used?	No	No	N/A
- Any non standard browser settings	No	No	N/A
Security			

- Controls required on the computer	Accredited "Secure" machine with user authentication and access controls		
- How will users be created and managed	There will be a manual process to provide new, amended or changed users to the CAID central administration function		Users are assigned to roles in the user and role management module of the Analyze CS client
- Computer part of the central CAID domain	No	No	No
Software Maintenance			
- Release Cycle	2 major releases / year + additional minor updates when required (e.g. hotfix)	Intelligence Server cycle	2 major releases / year + additional minor updates when required (e.g. hotfix)
- Who will Install Patches	System admin with assistance from Griffeye	Only Server-side patches	Manual download (MyGriffeye portal) and install
- What is the notification mechanism	Server updates are communicated directly by Griffeye.	N/A	Griffeye Analyze Newsletter for client updates or when logging on to CS. Server updates are communicated directly by Griffeye.

4.4 Software required to support CAID roles

A force may choose to deploy and support multiple versions of the “CAID User Workstations” depending on the role(s) each of their users undertakes for CAID. The table below shows the access required to perform each role.

The Griffeye Analyze CS Desktop Client is only available initially via Remote Desktop Connection (terminal services). It is anticipated that the users and roles accessing the Griffeye Analyze CS Desktop Client initially via terminal services will migrate to using a local Griffeye Analyze CS Desktop Client when these become available in 2015 Quarter 3.

Roles	**Requires Access To**		
Standard Force Roles	**Griffeye Analyze CS Desktop Client**	**Griffeye Analyze CS Web Client**	**Hubstream Web Access**
• Image and Video Graders	Local access required to grading tools		
• Auditor	via terminal service		Yes
• Data Transfer Administrator			Yes
• Local Business Administrator			
• Police Investigator	Desktop Client (when available in Q3 2015)	Yes	Yes
• Victim Identification Investigators	Desktop Client (when available in Q3 2015)	Yes	Yes
Specialist Roles			
• National Business Administrator	via terminal service	Yes	Yes
• Grading Panel Adjudicator	via terminal service		Yes
• National Auditor	via terminal service	Yes	Yes
• NCA Co-Ordination and Tasking Bureau	Desktop Client (when available in Q3 2015)	Yes	Yes (when v2.5 available in Q1 2015)
• System Administrator Roles	via terminal service		Yes

4.5 Compatible Force Categorisation Tools

Introduction

Project Vic publishes a standard for compliance to the interface format utilised by the CAID Project. During the User Acceptance Test (UAT) phase of the CAID Project the following categorisation tools were installed and tested:

- BlueBear LACE
- ZIUZ - VizX
- Griffeye Analyze DI
- C4ALL Version 1 and 2

Note: The inclusion of a software component in the UAT is not a recommendation of that software product

BlueBear LACE

- Tested Version 12.1.92
- This release is compliant with ODATA 1.1

ZIUZ VizX

- Tested Version 2.3.0.3
- This release is compliant with ODATA 1.0 so is not fully CAID compliant, the vendor is working on the new release version and we recommend VizX users waiting for the new release before upgrading

Griffeye Analyze DI

- Tested Version 14.2.0 (14.2.14.352)
- This release is compliant with ODATA 1.1 and is CAID compliant

C4ALL

There are two major releases of C4ALL available; both versions were tested during the CAID UAT;

- Version 1
- Version 2

C4ALL Version 1

- Tested Components/Versions
  - C4ALL 1.1.4
  - C4P Review Right Click Properties 1.0.3250.23043 (Date Modified 23/3/10) [1.6a]
  - ODatatoCSV 1.0
- With the use of a workaround this release is compliant with ODATA 1.1 and thus is CAID compliant; it can natively create the exports for upload into CAID but requires the use of a Hubstream provided utility that converts ODATA 1.1 Files into C4ALL Hash files.
- The workaround is permanent; we recommend C4ALL Version 1 users upgrade to this release
- The ODatatoCSV utility can be obtained from;
  - http://c4all.e-crime.on.ca/links/ODataToCSV_Encrypted.zip
  - It is encrypted the password is “Salary Attack Bank=5128”

C4ALL Version 2

- Tested Components/Versions
  - C4ALL 2.0.1
  - Strategy Management Studio 2.0.2 (Contact the CAID-Implementation team to get this version)

4.6 Connection Details for Administrators

Component	Function	Service	URL	PSNP IP Addresses	
				LIVE	DR
Hubstream Intelligence Agent	Installation	tcp/80	http://caid-1.x.pnn.police.uk	psnp.psnp.226.101	psnp.psnp.226.161
Hubstream Web Interface	Web Client UI	tcp/443	https://caid-1.x.pnn.police.uk/CAID	psnp.psnp.226.101	psnp.psnp.226.161
Griffeye Analyze CS Web Client	Web Client UI	tcp/443	https://caid-2.x.pnn.police.uk	psnp.psnp.226.102	psnp.psnp.226.162
Hubstream Intelligence Agent	Media Files	tcp/8739	https://caid-2.x.pnn.police.uk:8739/webapi/upload/	psnp.psnp.226.102	psnp.psnp.226.162
Hubstream Web Interface	Reports	tcp/80	http://caid-1.x.pnn.police.uk/ReportServer/	psnp.psnp.226.101	psnp.psnp.226.161
Hubstream Intelligence Agent	OData	tcp/443	https://caid-3.x.pnn.police.uk/CEServiceInterfaces/Media.svc	psnp.psnp.226.103	psnp.psnp.226.163
Remote CS Desktop Clients	Terminal Services	tcp/3389	Caid-4.x.pnn.police.uk	psnp.psnp.226.104	psnp.psnp.226.164
User Password Portal	Password Reset	tcp/443	https://caid-4.x.pnn.police.uk/rdweb https://caid-4.x.pnn.police.uk/rdweb/pages/en-us/password.aspx	psnp.psnp.226.104	psnp.psnp.226.164
File Transfer (missing images only)	FTPS	tcp/FTPS 990 (Control) 50000-50049 (Data)	Caid-5.x.pnn.police.uk	psnp.psnp.226.105	psnp.psnp.226.165
Griffeye Analyze CS Desktop	Data	AES256/17000	https://caid-2.x.pnn.police.uk	psnp.psnp.226.102	psnp.psnp.226.162
Griffeye Analyze CS Desktop	File	TLS/17001	https://caid-2.x.pnn.police.uk	psnp.psnp.226.102	psnp.psnp.226.162

4.7 PNN3 Migration to PSN

To assist in the transition from PNN3 to PSN the PSNP Programme has a Public Services Network in Policing (PSNP) community on POLKA. This contains useful information on the migration. Technical documents can be found on that community at the following link

https://polka.pnn.police.uk/en/Communities/Documents/?clubId=345&folder=Technical

4.7.1 *CAID Migrating to PSN*

The planned date for migration of the CAID central service to PSNP is the 21st of September 2015.

By that date, you must have configured your relevant force firewall to allow access to the PSNP IP addresses listed in section 4.6 Connection Details for Administrators. There are recommendations on how this may be undertaken in the documents provided by the PSNP Programme.

There is separate guidance on the steps to undertake when your force migrates to PSN these are in section

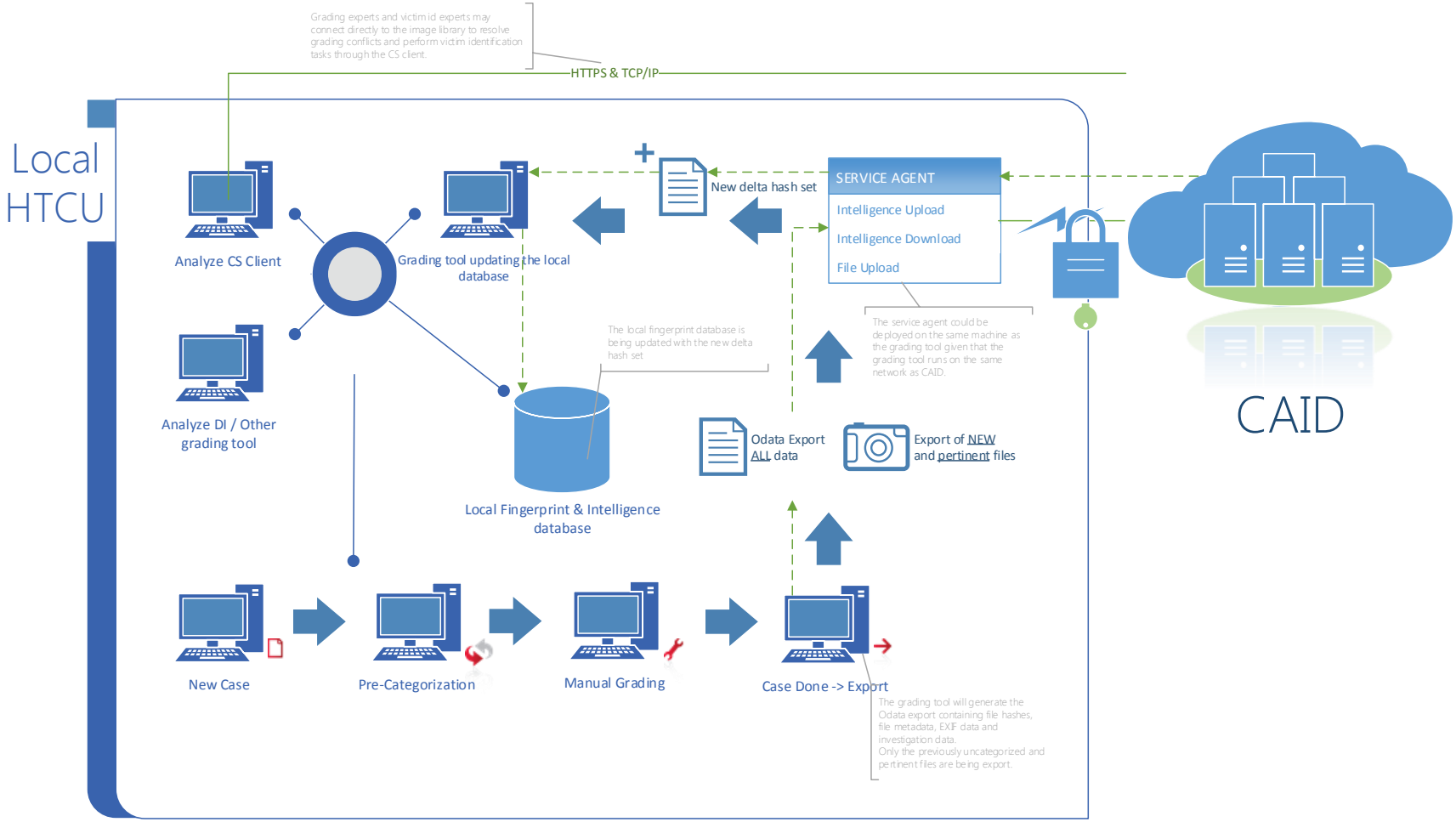
4.7.2 *Force Migrating to PSN*

Prior to a Force Migrating to PSN you should follow the instructions below;

- To migrate your connection from xCJX to PSNP
    - Raise a help desk call with the request to Claritas to migrate the IP addresses
    - Please redact the first two pairs of octets when providing addresses for example psnp.psnp.123.456
- Claritas will confirm the forces PSNP status with the Home Office accreditor team
    - If the connection has been approved then both sets of IP addresses will be enabled in the firewall until the force requests disconnection of the xCJX ones
    - You will receive an email when this has been completed
    - If the connection has not been approved then you will be advised to resubmit your request when your PSNP connection has been approved by the accreditors.
- Requesting disconnection of the xCJX addresses
    - You should requests disconnection of the xCJX by raising a help desk call with Claritas once the new PSNP connection is operational

4.8 IIOC Categorisation Workflow

Supplier provided workflow diagram –. Terminology on this diagram may differ to that used in the remainder of the document; “Local HTCU” refers to any force group or department that is using grading tools, “Service Agent” is the Data and Image Transfer Server specified in section 4.2, “Analyze CS Client” is the CAID User Workstations specified in section 4.3. We are not mandating that forces follow the diagram as a deployment model.



4.9 Hash/Fingerprint Technology Supported

To supply images and information to CAID, a categorisation tool must be project Vic ODATA 1.1 compliant and as part of this provide the mandatory MD5 “fingerprint” for the image file. There are other hashes supported and provided by CAID

Image Hashing

On receiving image files to CAID the central system will generate / regenerate the

- MD5 hash
- SHA 1 hash
- Microsoft PhotoDNA hash

Video Hashing

Friend MTS have donated their F1 video technology to IMEC and the community of categorisation tool vendors have agreed to adopt this as the standard for video hashing.

More information can be obtained from the press release;

https://www.friendmts.com/press-release/first-step-taking-control/

Video will not be adopted by CAID however until at least CAID Phase 3.2 due to be deployed in November 2015

5. Security Considerations

5.1 CAID Government Security Classifications

CAID is classified under the Government Security Classifications (GSC) as 'OFFICIAL-SENSITIVE' (OFFICIAL with the handling caveat SENSITIVE)

Whilst the statement "current infrastructure accredited for RESTRICTED material should be assumed to be secure enough for OFFICIAL" is OK as a general rule of thumb, an important feature of the new classification scheme is that security controls need to be appropriate to the information being processed and the threats to which it may be exposed.

In the case of CAID, we are processing particularly sensitive information (i.e., images of children being sexually abused) and have substantial threats from organised criminals and hackers. The impact of a security breach could potentially be devastating for victims and their families. Consequently, additional controls are deemed necessary to provide adequate protection. The outcome is a level of protection roughly equivalent to CONFIDENTIAL in the previous Government Protective Marking Scheme (GPMS). In particular, we need Enhanced grade CAPS encryption and strong network controls for wide area communications, which equates to xCJX / PSNP Secured.

5.2 Connection to CAID

In order to connect to CAID;

- The force SIRO is aware of the connection of CAID to xCJX / PSNP Secured and has accepted the local risks.
- Local CAID system components are installed in physically secure locations with appropriate security controls as defined by the NPC CoCo.
- CAID users are subject to vetting in accordance with the NPC CoCo.
- CAID users receive appropriate training and welfare services in accordance with the CAID Security Operating Procedures.
- CAID users are provided with access to the appropriate Security Operating Procedures, which they are required to acknowledge they have read and agree to comply with.
- Persons have been assigned to fulfil the roles of CAID Local Business Administrator and CAID Local Auditor. Note that the same individual cannot undertake both roles.

Force Assurance Statement

The force solution must be accredited or otherwise assured by the force Accreditor / Information Security Officer and a CAID Force Connection Application submitted to the CAID National Accreditor.

Completed connection applications should be submitted to Antony Holland the Lead Accreditor for CAID by email to Antony.Holland@homeoffice.pnn.police.uk copying in CAID-implementation@homeoffice.gsi.gov.uk

The "CAID Force Connection Application" is available via POLKA at

https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Resources

CAID Security Operating Procedures / Code of Connection

As part of the RMADS, CAID Security Operating Procedures (SyOPs) have been produced by the CAID Project, which individual police forces may adapt or extend to suit their own particular situation. Where customised versions of the CAID SyOPs are produced, you will need to get them approved by your local Accreditor.

The document set consists of;

- Risk Management and Accreditation Document Set [Not yet released]
  - Annex I. CAID Risk Assessment (IS1&2 Forms 1 – 6) [Not yet released]
  - Annex II. CAID Administrator SyOPs [Not yet released]
  - Annex III. CAID User SyOPs [Draft on POLKA]

These will be available (when released) via POLKA at

- https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Resources

There will be no CAID Code of Connection (CoCo) in accordance with instructions from NPIRMT. Individual forces will have to comply with the xCJX or PSNP Secured CoCo, as appropriate.

When a force has moved to PSNP full compliance is required, however for xCJX a Risk Managed Approach is acceptable

External Media USB/CD/DVD

Force solutions may include an air-gap necessitating the use of external media to transport information.

Whilst this is normally not allowed via the Codes of Connection for secure environments it is allowed where there is a legitimate business reason to connect and use physical media

There must be a managed risk approach to the malware threat this introduces, this may include;

- Protective measures implemented during the image carving process
- Additional malware defence including – Anti Virus, Validation, White Listing
  - For the central system Symantec we are looking at malware protection regimes which may include validation / white listing or AV

Deep Secure Web Guard is being investigated however if the decision is to implement, this it will be a phase two enhancement in 2015

Protective Monitoring

When a force is connected via PSNP Secure complete Protective Monitoring (PM) including an intrusion detection system (IDS) and security information and event management (SIEM) will be required

When a force is connected via xCJX full PM is not required and a risk based approach would be acceptable encompassing basic monitoring including the monitoring of firewalls and logs.

5.3 Security Vetting

Staff accessing the CAID require security vetting;

- For standard roles - Equivalent of Police Vetting (RV) or Non Police Personnel Vetting (NPPV) level 2
- Administrator / Audit Roles – Management Vetting (MV) or Non Police Personnel Vetting (NPPV) level 3

The following vetting levels are not appropriate for CAID roles

- Baseline Personnel Security Standard (BPSS)
- Counter-Terrorist Check (CTC)
- NPPV level 1

5.4 Business Impact Assessment

The executive summary from the “Child Abuse Image Database Business Impact Assessment” is contained below

A Business Impact Assessment (BIA) workshop was held on 6 February 2014 to determine the potential impacts of a breach of security affecting the Child Abuse Image Database (CAID). It was attended by representatives of both the business and the CAID project.

The workshop used the current method of expressing impacts using Business Impact Levels (BILs). These may be replaced by an alternative method when the new Government Security Classification (GSC) scheme is introduced in April 2014.

For the purposes of the assessment, the information handled by CAID was divided into seven groups:

- Media – IIOC images and video.
- Metadata – media details including EXIF and series data.
- Hash values, grade and action data.
- Case related data.
- Victim investigation related data.
- Intelligence and collaboration data.
- Data relating to Politically Exposed Persons (PEPs).

For each information group, the potential impact of a compromise of confidentiality or integrity was assessed. In each case, a BIL value was assigned for a compromise of a single record or item, and then for a compromise of the entire data set. The values were arrived at by discussion within the workshop, drawing especially on the expertise and experience of the business representatives.

It is important to note that impact assessment considers only the impact on the business or citizen if a breach of security were to occur. It does not consider the effects of any security controls that may be in place to mitigate the likelihood or impact of a breach.

Overall, the results of the workshop can be summarised as:

- IIOC media and metadata, victim data and intelligence data attracted BIL levels of IL4 to IL5.
- The BIL value of IL4 for metadata was derived from the sensitivity of location data.
- PEP data, which may or may not be held in CAID, was assessed as IL5 due to its sensitivity.
- Hash set data was assigned a Confidentiality BIL of IL0 but an Integrity BIL of IL3.
- Compromise of case related data was assessed as having a negligible (IL0) impact.

The importance of the information held by CAID to on-going investigations, and especially to protecting victims, was considered by the workshop in determining impact levels for the availability of the system. The workshop considered the potential impact of short-term unavailability (say, a couple of days) and long-term unavailability (a couple of months), and arrived at the following:

- Impact of short-term unavailability: IL4.
- Impact of long-term unavailability: IL5.

Two factors played an important part in determining impact levels throughout the workshop. These were:

- The devastating effect that sexual abuse could have on the lives of victims; and
- The urgent need to identify victims and protect them from further abuse.

5.5 Suggested Network Architecture

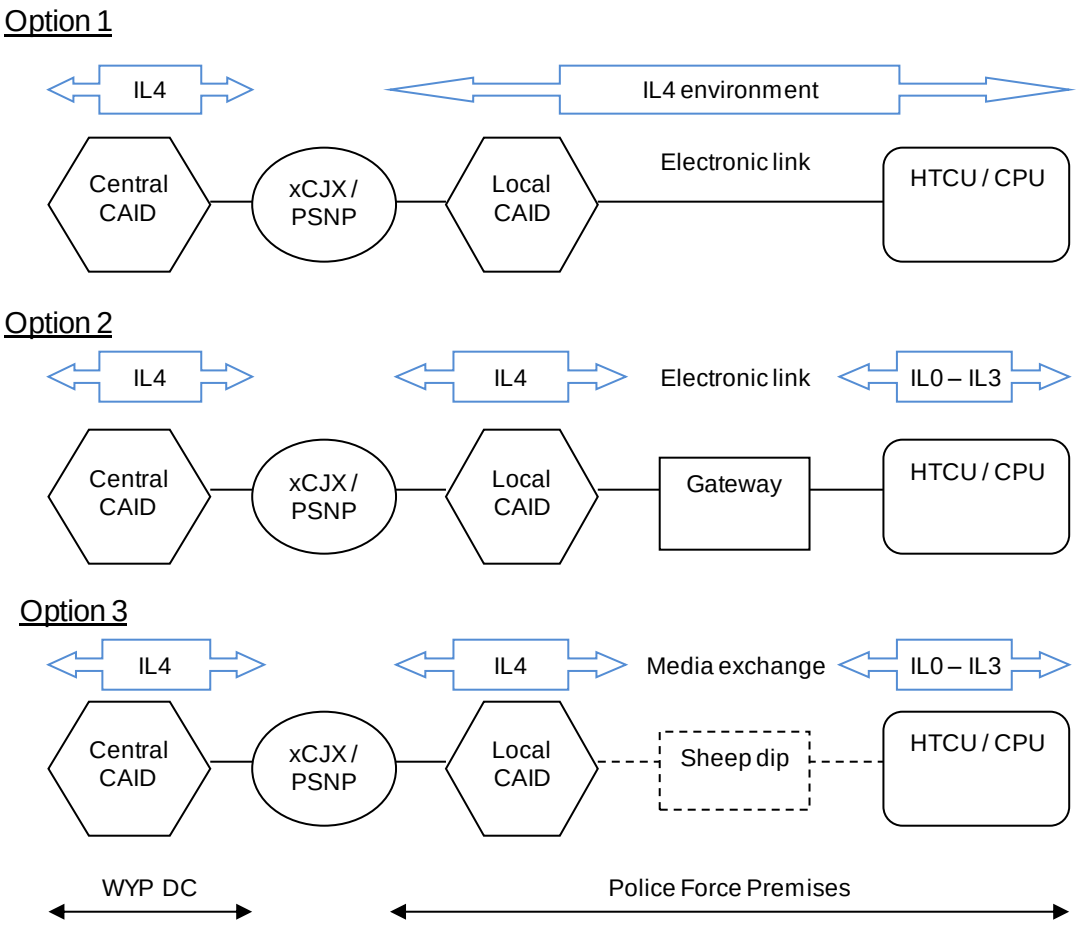
This section focuses primarily on forces connecting HTCU networks to the "Data and Image Transfer Server" described in section 4.2

From a high-level IA viewpoint, police force solutions for connection to CAID fall into one of three types:

- Option (1) IL4 HTCU/CPU system direct network link to Local CAID and xCJX/PSNP Secured
- IL0 – IL3 HTCU/CPU system either:
  - Option (2) electronic link via a gateway
  - Option (3) media exchange via an air gap

  to Local CAID and xCJX/PSNP Secured

These options are illustrated in the following diagram.



5.5.1 *HTCU/CPU system is accredited to process data at IL4*

Where the force HTCU/CPU system is accredited to process data at IL4 (option 1), it may be connected directly to Local CAID with no need for a gateway or air gap. In this situation, the HTCU/CPU system must be covered by a National Policing Community Code of Connection submission from the force covering the HTCU/CPU

5.5.2 *HTCU/CPU system is not accredited to process data at IL4*

Where the force HTCU/CPU system is not accredited to process data at IL4 and the force wants to

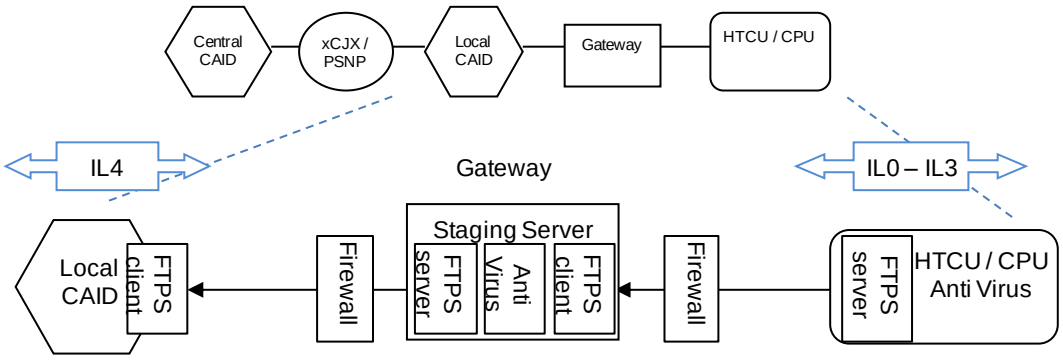
a) Connect it electronically to Local CAID (option 2)
    a. it must implement a secure gateway such as CESG's Architectural Pattern 2 "Walled Garden" DMZ (AP2). It is a force responsibility to assure the security of their connection.
b) Connect it via an air gap (Media Exchange)

The information exchange between Local CAID and the HTCU/CPU system includes security controls that endeavour to block the transmission of malware.

5.5.3 *An example of a suitable Secure Gateway*

Whilst it is not possible to provide a readymade solution for the Secure Gateway, a potential solution that is accepted as mitigating the risks / threats is below. Whether this is suitable for an individual force is for the force Accreditor / Information Security Officer to determine

Secure Gateway Example for Option (2)



FTPS is used to transport media and JSON Files

Transfers are always initiated from the "high side"

- Staging Server initiates transfers to and from the HTCU
- Local CAID initiates transfers to and from the Staging Server

The firewalls ensure only;

- Traffic from the correct endpoints are allowed
- The correct protocol / ports are allowed (FTPS)
- Traffic initiated from the high end is allowed.

Virus Scanning takes place

- In the HTCU prior to placing in the upload folder
- In the Staging Server prior to placing in the upload folder

It is assumed the components in this example are connected via physical network infrastructure that provides suitable protection and separation for handling Illegal Images of Children classified at Secured (IL4).

5.5.4 *Gateway Solution Scripts / Software*

DataLynx has software and scripts available to support forces wishing to implement a gateway solution. These scripts have been deployed at two early adopters; West Yorkshire Police and Avon & Somerset and where used in conjunction with correctly configured Firewalls and intermediate server has been accepted by the National Accreditor for CAID. The scripts and software are both

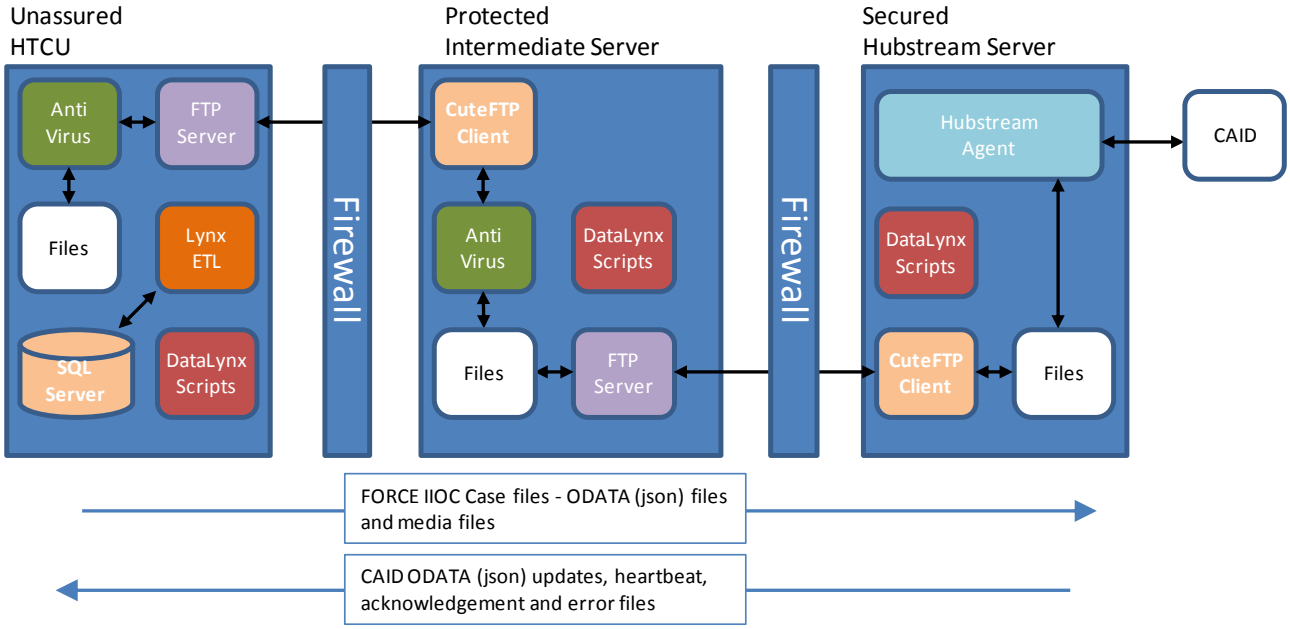
free. The CAID-Implementation team supports the implementation and use of the scripts and software whilst that team is in place. The solution comprises two components;

- LynxETL - Commercial Data and File migration software
- Scripts – DOS Batch Files

For the solution to function the force needs to provide

- CuteFTP Client (2 Licences)
- FTP Server for example FileZilla Server, Cerberus FTP (2 Licences)
- 2 Anti Virus Software packages from different vendors (must have command line support)
- Microsoft SQL Server (any version 2005 onwards including express editions)

5.5.4.1 Solution Overview



The solution moves;

- FORCE IIOC Case files consisting of ODATA (json) files and media files up to the Secured Hubstream Server for transmission by the Hubstream Agent to CAID
- CAID updates ODATA (json) files, Heartbeat files, Acknowledgement files and Error Files from the Secured and Protected down to the unassured Environment

Transfers are initiated from the higher assurance environment to the lower assurance areas i.e. from the Secured area to the Protected environment and from the Protected Environment to the Unassured environment.

Files are virus scanned twice – once in the unassured environment and once in the intermediate server

Scripts and Software

- The LynxETL Software
  - Provides scheduling
  - Health check mechanism for the send receive process
  - Email alerting
- The “Protected” environment scripts
  - Control the push and pull of material to the unassured area
  - Pass files through the Anti Virus software
- The “Secured” Scripts
  - Control the push and pull of material to the Protected environment.

- Create “link” file(s) to instruct Hubstream to upload cases to CAID
- Remove media and odata files once sent
- Recognise when a successful transfer to CAID has taken place and create an acknowledgement file

- Scripts create heartbeat files when they run, and error files if they or a component they call fails, these are passed by the system back down to the LynxETL Software.
- Acknowledgement files are created by the DataLynx scripts in the protected environment once a case has been successfully transmitted to CAID these are passed by the system back down to the LynxETL Software

5.5.5 *Network Infrastructure Considerations*

5.5.5.1 All network links

- The network used to connect the components in these suggested network architectures should be suitable for handling Secured (IL4) information.
- Due to the nature of the information being transmitted consideration should also be given to separating the traffic from other Secured traffic

5.5.5.2 Cross site links that aren’t fully encrypted

- Where the traffic is traversing protected (IL3) infrastructure CPA level – Crypto would be sufficient for example e.g. CISCO’s at each end of the network run
- Where the traffic is traversing unassured networks then CAPS level protection would be required

Some notes on terminology and the data being handled by HTCU / CSE units and CAID.

1. Images of child abuse have been assessed as IL4 and classified as OFFICIAL – SENSITIVE under the new Government Security Classification (GSC) scheme. IL4 equates to CONFIDENTIAL under the old Government Protective Marking Scheme (GPMS).

2. The IL4 assessment for child abuse images does not change because they are being processed on an unassured HTCU system or because they were found on the Internet. The impact of, say, unauthorised disclosure remains the same.

3. An Unassured system is one where we can have no confidence in its security (it may have security controls, it may not, but the security of the system has not been formally assessed). Such a system should only be used to process IL0 data. If it is being used to process IL4 data (e.g., child abuse images), it must be assumed there is considerable risk of a compromise.

4. An Assured system is one that has been formally assessed as providing adequate security to connect to networks such as PSN. Such a system should only be used to process data up to IL2 for confidentiality or integrity. If it is being used to process IL4 data, there is significant risk that the security controls are inadequate to protect the data.

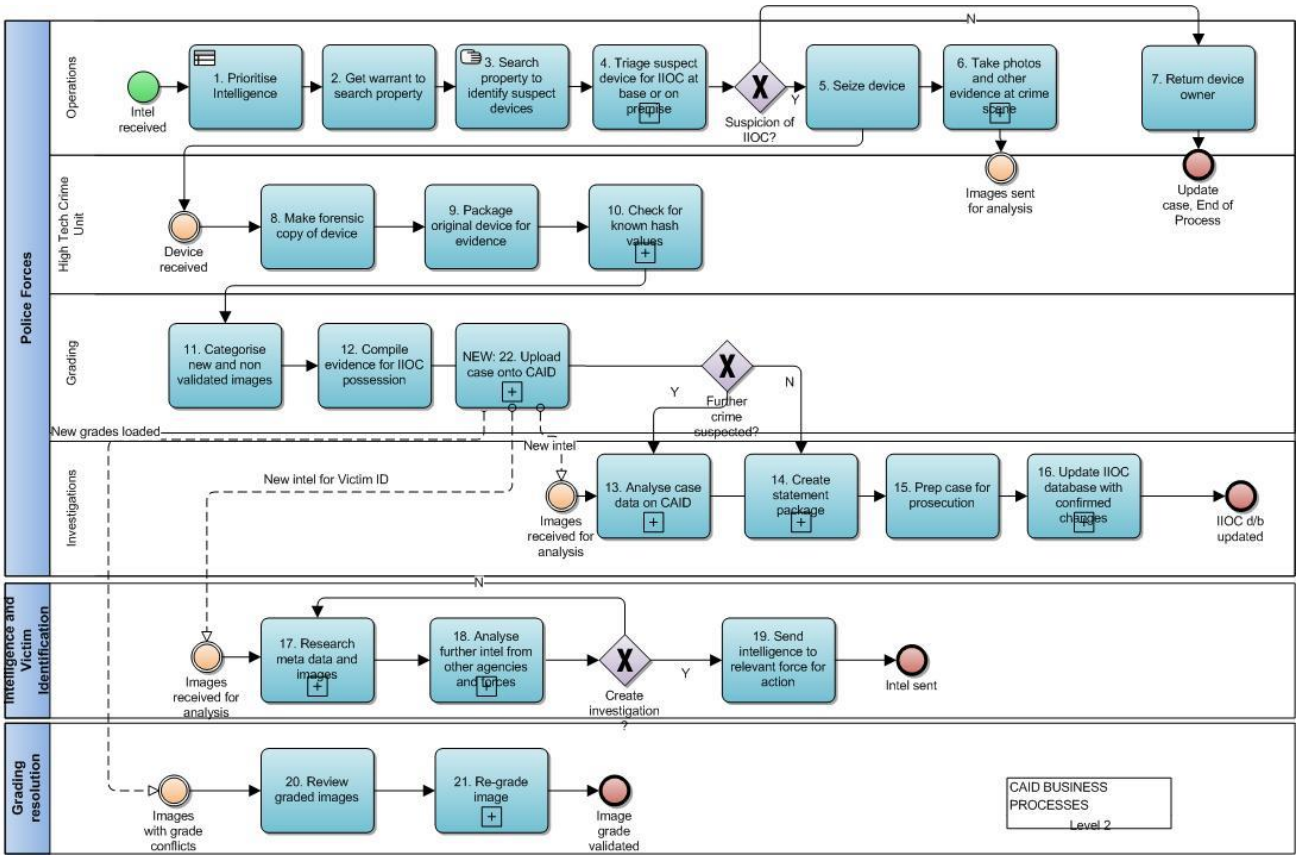
5. A Protected system is one that has been formally accredited as meeting the security objectives for processing IL3 data. If it is being used to process IL4 data, there is some risk that the security controls are inadequate to protect the data.

6. A Secured system is one that has been formally accredited as meeting the security objectives for processing IL4 data.

6. CAID Business Rules

6.1 CAID Business Processes

The CAID Business Process is below; this shows the processes and interaction with CAID.



6.2 Trusted categorisation

To ensure everyone involved can be confident of the categorisation of images held in CAID, the central system employs a trust model;

- An image needs to be independently categorised three or more times, and 80% of the categorisations for an image must agree before the image category is trusted.
- An image categorisation may also achieve trusted status where a Grading Adjudicator reviewed and set the image and categorisation.

The table in section 8.2.1 Categories for Upload and Download lists the categories for which the trust process applies to

6.2.1 *Category 7 - IIOC "un-confirmed"*

When the CAID system publishes new information including categorisations to forces, for images where a trusted status has not been reached the categorisation will be set to 7 - IIOC "un-trusted".

Where pre-categorisation of a case results in images being assigned a category of 7, the force should review and categorise the images.

Forces must not manually categorise an image as '7' during the viewing and categorisation process.

6.2.2 *Grading Panel*

Where seven or more categorisations have been received for an image but the image has not achieved the criteria for trust, then the grading panel will review and assign the image a trusted categorisation or categorise the images as a permanently disputed category 6.

6.3 IIOC Guidance on Categorisation

The main guidance on categorising indecent photographs of children is contained in the document "Guidance on categorising indecent photographs of children", this document was compiled under the NHSD Project in collaboration with the National Grading Panel as per the ABC categories (April 2014 onwards)

This guidance should be used for categories 1 through 5 and is available on POLKA

https://polka.pnn.police.uk/en/Communities/Documents/?clubId=607&folder=Guidance

The CAID Project has developed new guidance for categories 6 / 7 / 8 / 9

Category	Guidance
6	▪ **Indicative / Borderline / Other notable** ▪ Images that do not meet the beyond reasonable doubt test to be included in Category A-C (e.g. some doubt as to age or indecency) ▪ Banners from sites known for illegal child content and images in a series that are not indecent in themselves ▪ Images from known Child Abuse Series (e.g. fully clothed children that were shared with IIOC)
7	▪ **IIOC "un-confirmed"** ▪ When the CAID system publishes new information including categorisations to forces, for images where a trusted status has not been reached the categorisation will be set to 7 - IIOC "un-confirmed". ▪ Where pre-categorisation of case results in images being assigned a category of 7, the force should review and categorise the images. ▪ Forces must not manually categorise an image as 7 during the viewing and categorisation process
8	▪ **Ignorable / Discounted (including adult pornography)** ▪ Lawfully held images of all descriptions ▪ Unique ignorable images (e.g. family or holiday snaps) ▪ Common ignorable images (e.g. corporate logos, web site banners) ▪ Includes lawfully held adult pornography
9	▪ **Supports Identification** ▪ images that are not illegal but can support the identification of a victim or offender only. These images can be taken by a police officer or from images seized from a suspect's property. This category will not be subject to the voting system.

6.4 Standardisation of Case Naming

To avoid conflicts and enable CAID to function correctly it is necessary for each case submitted to CAID to have a unique name.

Forces should follow the standard

- "[FORCEID]-[CASE REF]-[UNIQUE STAFF NO]"

For example

- 01-10/24/2014 IIOC 4-67891

6.4.1 *Grading Tools Guidance*

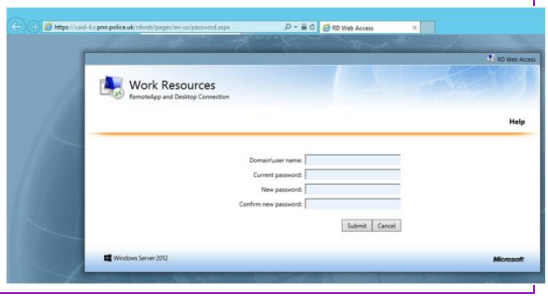
To assist forces in the provision of this information we have identified which field needs to be completed during the preparation or export of a case.

Categorisation Tool	Version	Guidance
C4ALL	V1.1.4	Complete the “Hubstream Case Details : Case Number” (entered during the export of the case)
C4ALL	V2.0.2	Complete the “Hubstream Case Details : Case Number” (entered during the export of the case)
Griffeye Analyze DI	14.1.4	Complete the “Case Name” during the creation of the case when the Administrative Options for the case are displayed.
BlueBear Lace	TBA	Complete the Police ID when prompted by the “New Case Wizard”
ZuiZ VizX	2.3	Complete the “Case Name” during the creation of a new case when the Create Case screen is displayed

7. Service Management

7.1 User account management:

- Provisioning of new user accounts
  - During initial force on boarding;
    - The ***Local Business Admin*** or ***CAID SPOC*** should complete the "CAID Force Initial Users template .xlsx" (email CAID-Implementation@homeoffice.gsi.gov.uk to request a copy)
    - Once complete the form should be emailed to CAID-Implementation@homeoffice.gsi.gov.uk
    - Users will be emailed their credentials
    - There is a 24 hour SLA for these requests
  - For business as usual
    - The ***Local Business Admin*** should complete the "CAID Force Initial Users template .xlsx" for the new users and email supportcjsm@claritas-solutions.com.cjsm.net
    - Users will be emailed their credentials
    - There is a 24 hour SLA for these requests
- User password change
    - ***Users*** may change their passwords by using the password portal

Step	Screenshot
1. Using one of the supported browsers enter the URL enter https://caid-4.x.pnn.police.uk/rdweb	
2. Enter your CAID username with the CAID domain prefix e.g. CAID\john.doe 3. Enter existing and new passwords 4. Click Submit	

    - Passwords are changed immediately
- User password reset / User account unlocking
  - If the user has forgotten their password then the password may be changed by;
    - The **user** emailing supportcjsm@claritas-solutions.com.cjsm.net requesting a reset of the password
    - There is a 24 hour SLA for these requests
    - A self-service facility for these requests is being developed
- Removal of existing user accounts
    - The ***Local Business Admin*** should email supportcjsm@claritas-solutions.com.cjsm.net requesting the removal of the account

    - There is a 24 hour SLA for these requests
- Changing user roles
    - The ***Local Business Admin*** should email supportcjsm@claritas-solutions.com.cjsm.net with details of the user and new roles
    - There is a 24 hour SLA for these requests

7.2 Business Support

- Grading Adjudication
    - If a ***CAID user*** or ***Person undertaking categorisation*** identifies that in their opinion a trusted category has been assigned incorrectly they should request adjudication by emailing email caidbusinesssupport@westyorkshire.pnn.police.uk with the hash in question and the reasons for disputing the categorisation
    - There is a best endeavours turn round for these requests

7.3 Connecting to CAID

- Once the prerequisite steps to implement the CAID local elements have been completed a connection to CAID is obtained by
    - The Force ISO and HTCU manager or equivalent should submit a completed “CAID Force Connection Application” to NPIRMT see section 5.2 Connection to CAID
    - You will receive a confirmation of approval from the NPIRMT
    - Send the xCJX IP address or range of IP addresses you wish to connect to CAID on to Caid-implementation@homeoffice.gsi.gov.uk
      Please redact the first two octets of the IP address e.g. xCJX.xCJX.123.123
    - The CAID Implementation team will advise you by email when the connection has been configured.
    - Undertake the connectivity tests as outlined in Annex F Connectivity Testing

7.4 Support

Support is provided by various support organisations depending on the nature of the support required and the stage the support request has reached.

For support using your categorisation and grading tools for instance C4ALL, Bluebear Lace, Griffeye Analyze DI, Ziuz VizX you should refer to the suppliers own support arrangements.

You should use the support process below for the following products;

- Griffeye Analyze CS Web
- Griffeye Analyze CS Desktop (via Terminal Services)
- Hubstream WebClient
- Hubstream Intelligence Agent

7.4.1 *First Line Support*

Initially all force ***users*** should refer issues to their local support arrangements either their IT Support Desk or their nominated CAID Business Administrator (see section 3.1 Force Roles)

If an issue has been resolved by first line support, it should not be raised with second line support.

7.4.2 *Second Line Support*

Claritas who manage and run the CAID Data centre provide second line support.

- Telephone – 0113 318 1227
- Email – supportcjsm@claritas-solutions.com.cjsm.net

Access to second line support is restricted and each force should nominate key users and members of their IT Support team to be able to call / email the second line support facility (see section 7.1 User account management:).

A challenge/response that nominated users will be required to setup will ensure only authorised users contact second line support

Issues should only be raised with Claritas if first line support cannot resolve the issue.

7.4.3 *Third Line Support*

- Griffeye and Hubstream will provide third line technical support for the CAID components this should only be requested by Claritas
  - Griffeye Analyze CS Web
  - Griffeye Analyze CS Desktop (via Terminal Services)
  - Hubstream WebClient
  - Hubstream Intelligence Agent
- West Yorkshire Police in their role as National Business Administrators will provide third line business support for CAID this should only be requested by Claritas

8. IIOC Information Exchange with CAID

CAID will receive updates from forces containing information and selected images relating to IIOC cases within that force. CAID will then publish regular updates to the hashset, categorisations and metadata for forces.

8.1 Receiving CAID Updates

CAID will publish regular updates to the hashset, categorisations and metadata for forces to use in their local categorisation tools.

This update will be provided in the Project Vic (http://www.projectvic.org/) agreed format. More information on the structure and content of the files is contained in Annex C Odata schema

The definition of which categories will be provided within an update is in section 8.2.1 Categories for Upload and Download.

The Hubstream Intelligence Agent software provided as part of the solution performs the download of the update from CAID (see section 4.2 Data and Image Transfer Server)

The download frequency can be configured within the Hubstream Intelligence Agent software, initially this will be set to Daily i.e. forces will receive a daily update to the hashset, categorisations and metadata held centrally.

It is the Force's responsibility to ensure that these updates are imported into the Force's specific grading tool database.

Project Vic publishes a list of tools that are compatible with the standard these include the common UK force grading tools

- BlueBear (LACE)
- ZIUZ (Vizx)
- Griffeye (Analyze DI)
- C4ALL / C4P

8.1.1 *CAID "Gold Disk"*

As the initial download of the hashset, categorisations and metadata would be large we provide that information on DVD known as the "Gold Disk" the gold disk contains packages for each of the grading tools with the file split into suitable sized smaller files where necessary.

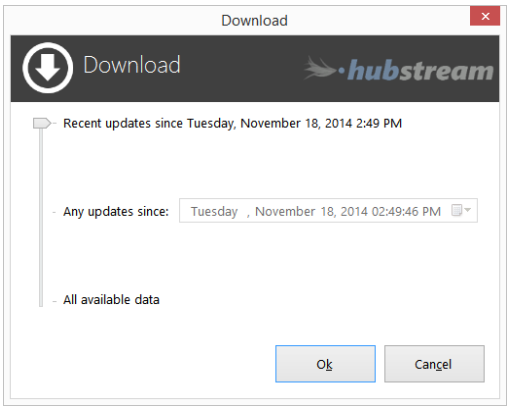
The Hubstream agent automatically downloads from the end of the period covered by the Gold Disk

To receive your "Gold Disk" please contact the National Business Administration team at caidbusinesssupport@westyorkshire.pnn.police.uk

8.1.2 *Instructions for download via Hubstream Agent*

Once the Hubstream Intelligence Agent is installed and configured correctly (see section E.4 Hubstream Intelligence Agent) the instructions bellow can be followed for downloading the first update a new update to hashset which will then be available in your local "\Inbox" Folder.

Step	Screenshot
Only the force users who have the "Data Transfer Administrator" role should undertake the download 1. Open the Hubstream Intelligence Agent User Interface	

Step	Screenshot
2. Choose Download	
3. Move the Slider to select one of the top two updates options or select “All Available data” a) Press OK	
4. The odata file should be downloaded to the Inbox Folder	

More information on how the Hubstream Intelligence Agent works is contained in Section E.4 Hubstream Intelligence Agent

8.2 Uploading Force IIOC Information

Only the force staff who are undertaking the “Data Transfer Administrator” role should upload information

After a force has categorised an IIOC case, the force should transmit the in-scope information and images relating to IIOC cases to CAID.

The scope of information and images required to be uploaded are contained in section 8.2.1 Categories for Upload and Download. **It is important to ensure that only categories 0-6 and 8 are uploaded to CAID** until the next release of CAID – in practice this is controlled during the export of the cases

Project Vic publishes a list of software that is compatible and hence that can create the necessary exports these include the common UK force grading tools

- BlueBear (LACE)
- ZIUZ (Vizx)
- Griffeye (Analyze DI)
- C4ALL / C4P

You may need to upgrade your grading tool to the latest version, for C4ALL users for example a release of C4All 1.1 has been released that contains the required functionality.

Each tool has specific instructions on how to undertake perform the export – simple instructions are included for each in Annex D Import and Export To CAID.

Transferring the files for upload

The Hubstream Intelligence Agent software provided as part of the solution will perform the upload of the information and images to CAID (see section 4.2 Data and Image Transfer Server).

The method of transfer between the High Tech Crime Unit network and this server will vary between forces as this is dependent upon the solution implemented by the Force.

Each case will typically consist of

- A single data file – this will have the extension .json
- Many images usually in a folder or folder
-

When these are exported from the categorisation tools they will usually be saved into a single folder

Copying the files

The image files should be kept in the same relative location to the json file as initially exported.

i.e. in the example above, once copied across, both the “files.20141130.104007” image folder and the “Export. 20141130.104007.json” file should be in the same folder

The order to copy files

An important consideration for forces utilising Automatic Sync, where files are sent automatically when they are placed in the “Outbox” folder is

- Regardless of whether the transfer is automated or manual from the HTCU, All the images should be transferred into the Outbox folder prior to transferring the JSON File

Hubstream Intelligence Agent Upload Options

There are both automatic and manual upload options available, we would recommend automatic

Automatic - The information and images will be uploaded automatically once they have been transferred to the local upload server

Manual – via the Hubstream Intelligence Agent User Interface

More information on how the Hubstream Intelligence Agent works is contained in Section E.4 Hubstream Intelligence Agent

8.2.1 *Categories for Upload and Download*

The following table identifies for which categories of image the information (including hash, categorisations and metadata) and images are to be sent to CAID and which information (including hash, categorisations and metadata) will be published by CAID.

The final business rules and processing are being supplied in release 3 of the Griffeye and Hubstream Software – This will allow Category 9 hashes and images to be uploaded and Category 0 Hashes – At this point you must not upload Category 9 and 0

When Exporting Data and Images from your grading tools you must ensure only the categories marked "Yes" in the "Upload to CAID column" are exported – CATEGORY 0, 7 and 9 should not be uploaded to CAID

Release 2 Rules		Upload to CAID		Download from CAID	Categories subjected to Trust	
Cat	Definition of Category	Hash	New Image	Hash	Result before a 3-vote process?	Result after a 3-vote process?
0	Ungraded Images - not included in any voting process	No	No	No	N/A	N/A
1	IIOC - images involving penetrative sexual activity, sexual activity with an animal or sadism	Yes	Yes	Yes	7	1 - trusted
2	IIOC - images involving non-penetrative sexual activity	Yes	Yes	Yes	7	2 - trusted
3	IIOC - other indecent images not falling within categories A or B	Yes	Yes	Yes	7	3 - trusted
4	Prohibited Images (animation/ depictions of IIOC)	Yes	Yes	Yes	7	4 - trusted
5	Non IIOC - Extreme Content	Yes	Yes	Yes	7	5 - trusted
6	Indicative of IIOC content/ Borderline IIOC content where age cannot be determined	Yes	Yes	Yes	7	6 - trusted
7	CAID Generated Number - Images indicating possible IIOC content – but it has not received trusted grade status due to the image having less than 3 confirmed votes or at least one other force has disputed the IIOC category. - Images should be graded by officers.	No	No	Yes	N/A	N/A
8	Ignorable / Discounted/ Legal images (including Adult pornography)	Yes	No	Yes (Common only)	excluded from download	8 - Common Ignorable
9	Supports Identification - Any non illegal image that may support the identification of a Victim or Offender of Online Child Sexual Exploitation	No	No	No	N/A	N/A

Annex A CAID Project Contacts

CAID Project Management	
Senior Project Manager	Steve Thomson Steve.Thomson2@homeoffice.gsi.gov.uk 07525 407887
CAID Project Manager	Kieran O'Callaghan Kieran.O'Callaghan@homeoffice.gsi.gov.uk 07584 004078
CAID Senior Stakeholders	
Senior Information Risk Owner (SIRO) for CAID	Chief Constable Simon Parr Cambridgeshire Police
Senior Responsible Owner (SRO) for CAID	Jeremy Oppenheim Home Office
Information Asset Owner (IAO) & National Policing Lead for CAID	Chief Constable Simon Bailey Norfolk Police
Data Controller	Chief Constable Simon Parr Cambridgeshire Police
CAID Security & Accreditation	
Lead Accreditor for CAID	Antony Holland Antony.Holland@homeoffice.pnn.police.uk 07785 714130
CAID Security Consultant (CLAS)	Nigel Ball Nigel.Ball2@homeoffice.gsi.gov.uk 07557 906275
CAID Implementation Team	
CAID Implementation	Caidbusinesssupport@westyorkshire.pnn.police.uk POLKA https://polka.pnn.police.uk/en/Communities/Home/?clubId=607
CAID Implementation Team Manager	Charles Spinks Charles.Spinks@homeoffice.gsi.gov.uk 07811 106749
CAID Implementation Specialist	Mark Walker Mark.Walker8@homeoffice.gsi.gov.uk 07921 842 646

Annex B Glossary

Abbreviation, acronym or term	Full text or description
AES	The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data
BPSS	Baseline Personnel Security Standard
CEOP	Child Exploitation and Online Protection command within the NCA
CESG	Communications: Electronic Security Group, the UK National Technical Authority
CLAS	CESG Listed Advisor Scheme
CSE	Child Sexual Exploitation
CSP	Commercial Service Provider
CJX	Criminal Justice Extranet
DNS	Domain Name System - The Domain Name System is a hierarchical distributed naming system for computers it associates IP Addresses with domain names.
DPA	Data Protection Act
EXIF	Exchangeable Image File (extended JPEG format)
FTPS	FTP over SSL, another name used to encompass a number of ways in which FTP software can perform secure file transfers
GPS	Government Procurement Service or Global Positioning System
GSC	Government Security Classification scheme
GSI	Government Secure intranet
HMG	Her Majesty's Government
HMIC	Her Majesty's Inspectorate of Constabulary
HO	Home Office
HOIT	HO Information Technology
HRA	Human Rights Act
IA	Information Assurance
IAO	Information Asset Owner
ICO	Information Commissioner's Office
ICSE	International Child Sexual Exploitation database
ICT	Information and Communication Technology

Abbreviation, acronym or term	Full text or description
ID systems	ICT systems that identify citizens and hold PII data
IIoC	Indecent Images of Children
iNHSD	interim National Hash Set Database
IP	Internet Protocol
IPTC	International Press & Telecommunications Council
IS1	HMG Information Assurance Standard No.1
IS2	HMG Information Assurance Standard No.2
IWF	Internet Watch Foundation
JPEG	Joint Photographic Expert Group
LEA	Law Enforcement Agency (a term that covers CEOP and police forces)
MD5	Message Digest algorithm version 5
NCA	National Crime Agency
NPC	National Policing Community
PCG	PIA Consultative Group
PhotoDNA	Microsoft algorithm for identifying photographic images
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information (i.e., private information relating to identifiable individuals)
PSN	Public Services Network
SAR	DPA Subject Access Request
SC	Security Check, level of security clearance
SCOC	Strategic Centre for Organised Crime (Home Office)
SSL	Secure Sockets Layer (SSL), is a cryptographic protocol designed to provide communication security
SHA1	Secure Hash Algorithm version 1
SIRO	Senior Information Risk Owner
XMP	Adobe Extensible Metadata Platform

Annex C Odata schema

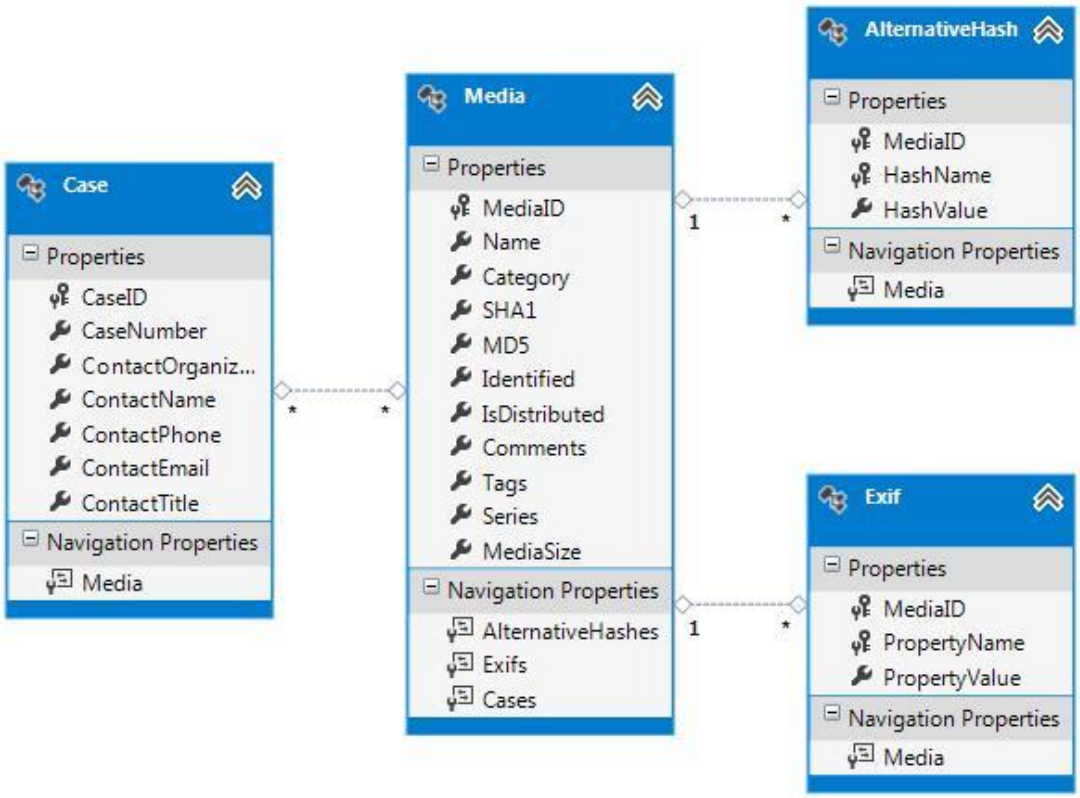
More information on the project Victim schema is available from the website http://www.projectvic.org/project-vic-odata-protocal/

The following schema diagram illustrates the Odata data model v1.0

> Presently in development is version 1.1 of the schema, which is extended to contain a reference to the associated images enabling the Hubstream Intelligence Agent to Upload the image file to the Central CAID database.

This schema describes the content of a 'Case export' from the compatible grading tools, (into the JSON file output).

Note: Not all grading tools may export the entire set of fields, a matrix is being developed in order to identify which tool cannot export which fields.



Data Dictionary

The following table describes the fields within the OData schema (v1.0)

Table Name	Field Name	Description
Case	CaseID.	Internal system identifier
	CaseNumber	Force Case Number (Force internal identifier)
	ContactOrganization	Force / Law Enforcement Authority who are exporting the Case
	ContactName	System User's name

Table Name	Field Name	Description
	ContactPhone	User's contact telephone number
	ContactEmail	User's contact email address
	ContactTitle	User's title
Properties	MediaID	Unique Id for the image
	Name	Name of the image
	Category	Grading applied to hash (1-8)
	Sha1	Sh1 Hash Value
	MD5	MD5 Hash value
	Identified	Indicator as to whether the victim has been identified
	IsDistributed	Inidicator (Y/N) as to whether the image
	Comments	Free text field for grade comments
	Tags*	Field can hold a number of items e.g. Victim Identified, Perpetrator of Abuse Identified, Case and Force Identifier, (Grading Officer identifier if feasible)
	Series	Indicator to indentify whether an image is part of a series (Y/N)
	MediaSize	field holds size of the image
AlternativeHash	MediaID	Unique Id for the Image
	HashName	Should be populated with Hashvalue type where the type is something other than MD5 or Sha1 (e.g. PhotoDNA)
	HashValue	Hashvalue for image (in the format of the field above)
Exif	MediaID	Unique Id for the Image
	PropertyName*	Field will hold descriptor of Exif value E.g. Camera (type)
	PropertyValue	Corresponding value for above PropertyName e.g. Nikon-D3100

Notes

***PropertyName** - Cameras / Devices can hold a variety of exif data e.g. Geo-location, Camera type, Camera Model number etc.

Annex D Import and Export To CAID.

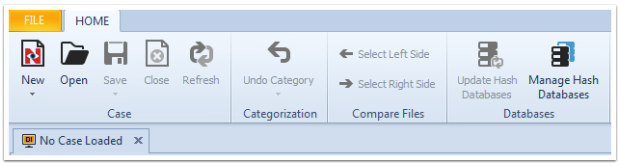
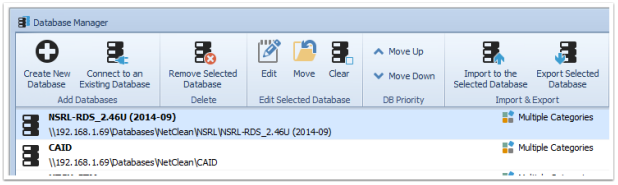
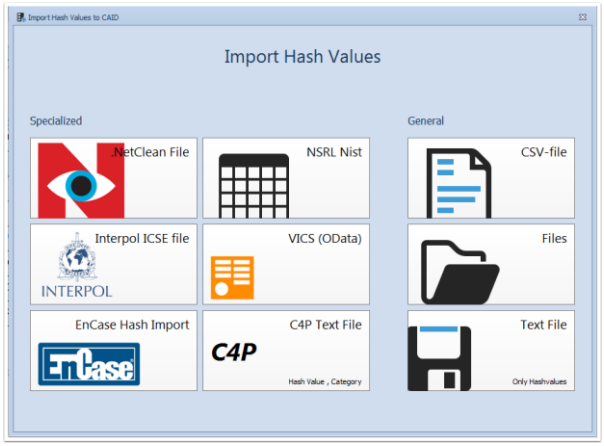
The following section details the steps to be followed when sending case files and associated images for upload into CAID and the steps required when importing hashset updates received from CAID. The section is broken down by tool and details import and export for each tool.

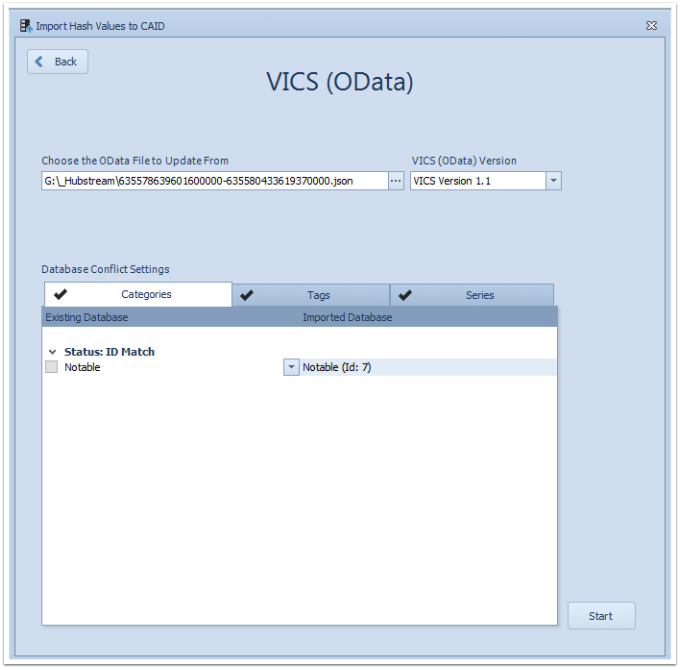
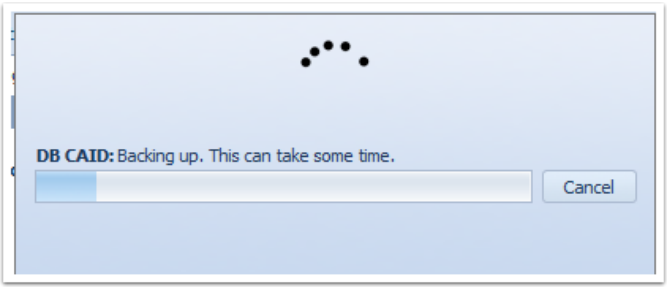
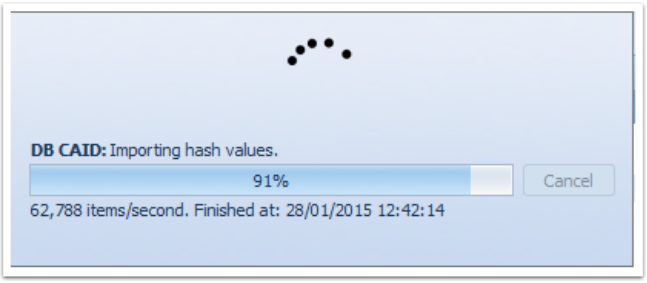
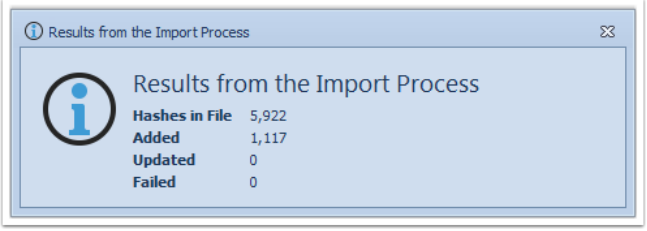
D.1 Griffeye

The following instructions relate to Griffeye version 14.1.4

Note ! - To import or export ODATA you need to activate it from the Griffeye Forensic Market Apps available on the Home Tab.

How to import the CAID Hashset update

Step	Screenshot
It is anticipated that only the force users who perform the "Data Transfer Administrator" role will undertake the Import 1. Using Griffeye Analyze DI	
2. Choose [Home] [Manage Hash Databases]	
3. Highlight the database you wish to import the Hashset to and select [Import to Selected Database]	
4. Press the VICS (Odata) button ***If the VICS (Odata) button does not appear from the 'Import Hash Values' Tab;*** a) Click the Griffeye Forensic Marker Apps Button. b) Click on the VICS (OData) Import and Export c) Press the Activate button	

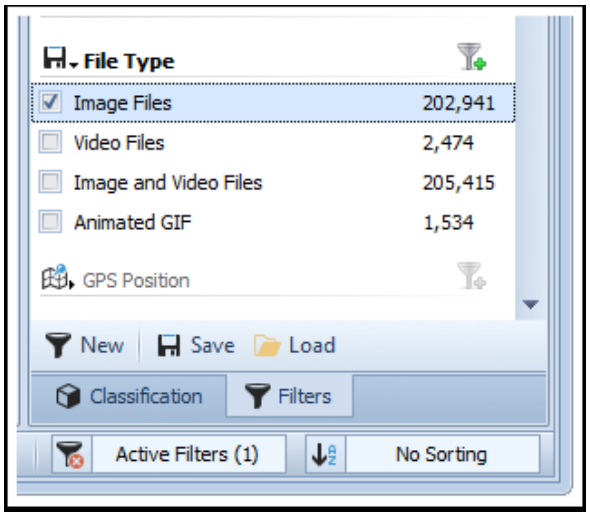
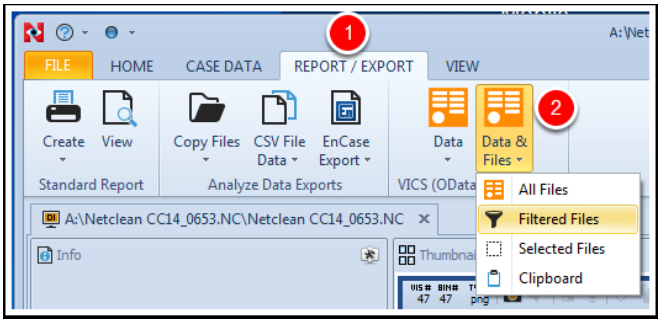
Step	Screenshot
5. Select the file from the location where it has been saved	
6. Check and fix any category mappings.	
7. Database will backup	
8. Dialog will be displayed for the import	
9. You will see a results file (click x in the top right corner to close the dialog)	
10. Say “No” to the "do you want to import another file?" dialog	

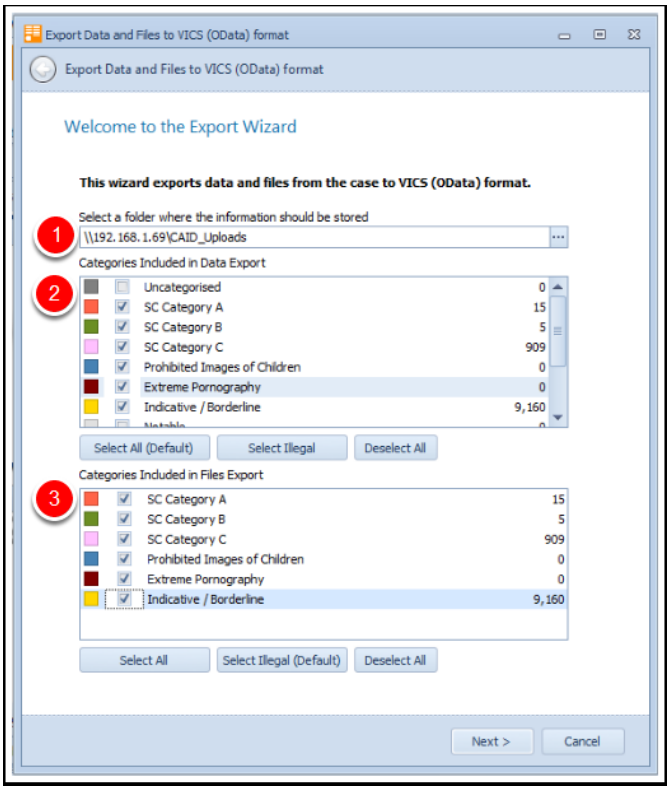
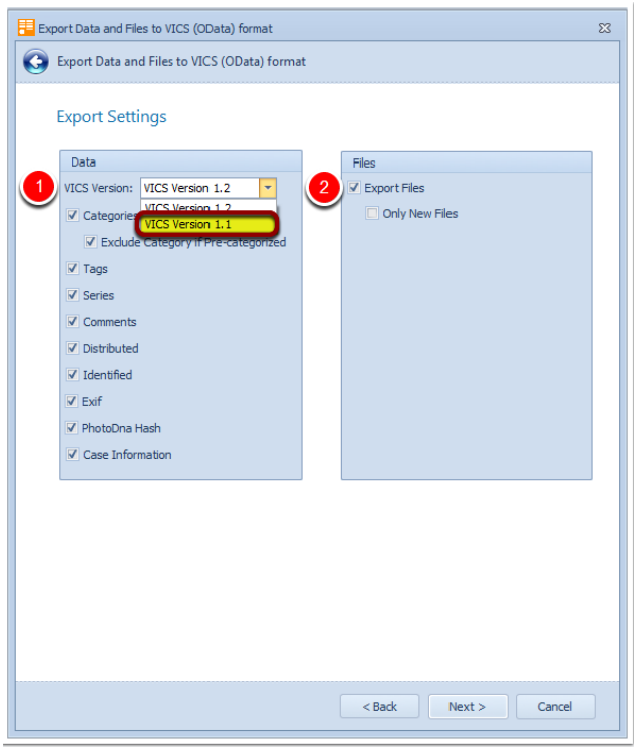
How to export a case for upload to CAID

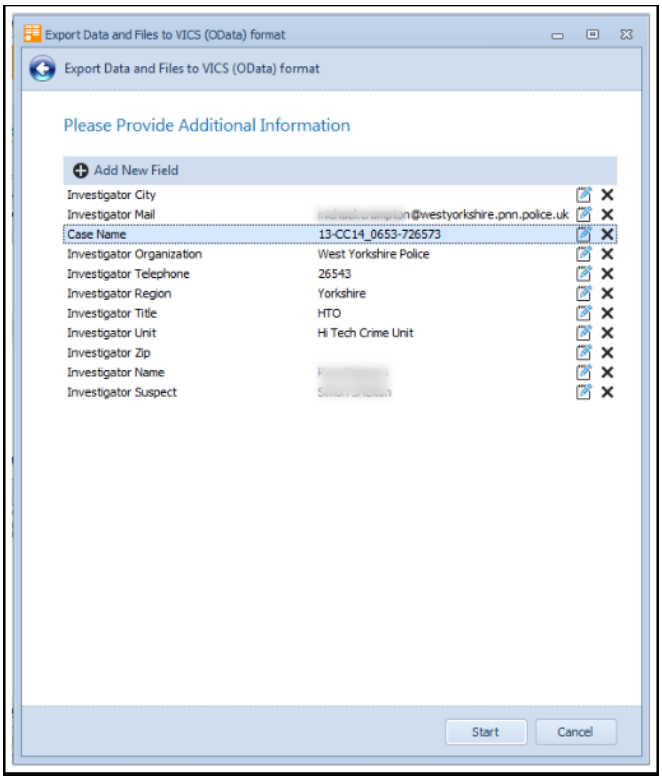
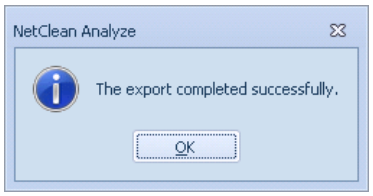
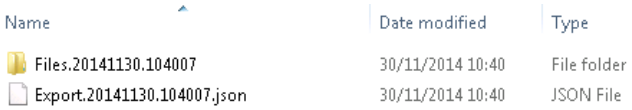
This export process is for Release 2 of CAID and is to export hashes and images for categories 1 to 6 and hashes only for category 8.

No other categories or videos are to be exported at this time.

The process has been tested on Griffeye v 14.2.

Step	Screenshot
1. Clear all existing filters a) Filter on File Types -> Image Files	
2. With the case open that you want to export Select [REPORT / EXPORT]	
3. Select “Data & Files” → Filtered Files ***If the Data & Files icon does not appear from the 'HOME' Tab;*** d) Click the Griffeye Forensic Marker Apps Button. e) Click on the VICS (OData) Import and Export f) Press the Activate button	

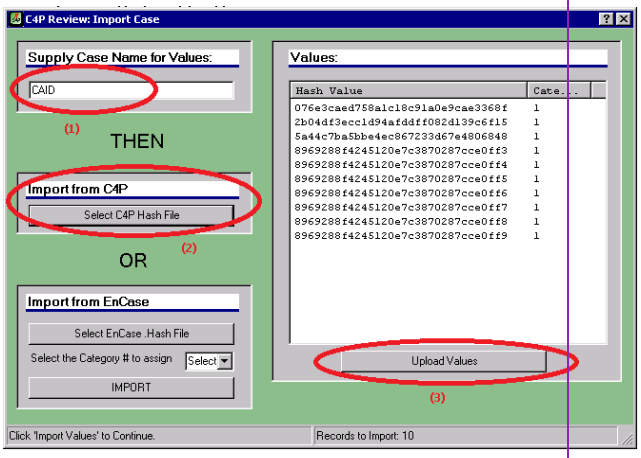
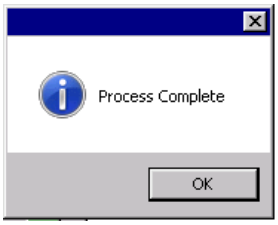
Step	Screenshot
4. The Export Wizard will display a) (1) Select the location to export the data and images (please refer to the person(s) within your force who are responsible for uploading to CAID) b) (2) From the Categories included in Data Export - Select Categories 1 to 6 and 8 c) (3) From the Categories included in Files Export - Select Categories 1 to 6 *Do **not** use the 'Select Illegal' Button as this will not include Category 6*	
5. The Export Settings options will display a) Make sure you select 1.1 as the VICS version b) All settings should be selected – however deselect “Only New Files”. [This is a temporary measure to help populate the CAID database with missing images where the hash value already exists]. c) Select [Next >]	

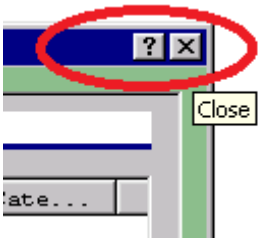
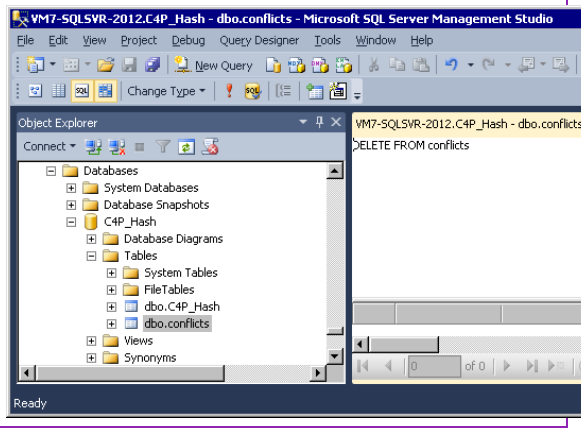
Step	Screenshot
6. The “Additional Information” options will be displayed a) Please provide all information **except** any information which contains the personal details of the suspect or victim for example do **not** provide Investigator Suspect b) Select [Start] **Important:** **Case Name** must be of the format <Force Code>-<Case Number>-<Staff Number> For Example 13-CC14_0653-726573 This information is recorded in the CAID system.	
7. The success dialog will display a) Select [OK]	
8. A dialog to open the folder will display b) select [YES]	
9. The exported files should be in the folder a) At this point please liaise with the person(s) within your force who are responsible for uploading information to CAID for further instructions	

D.2 C4ALL (ver 1.1)

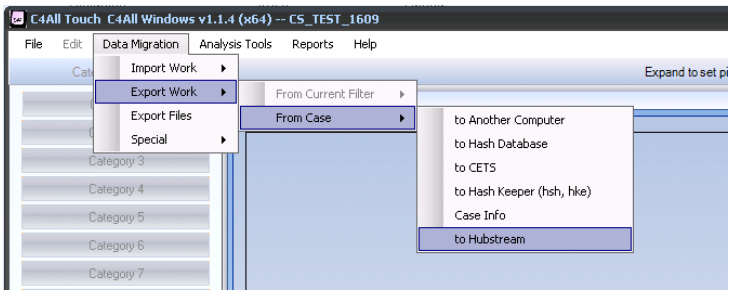
The following instructions relate to version 1.1 of C4ALL. Note: The json Files are imported using a separate utility called C4P Review

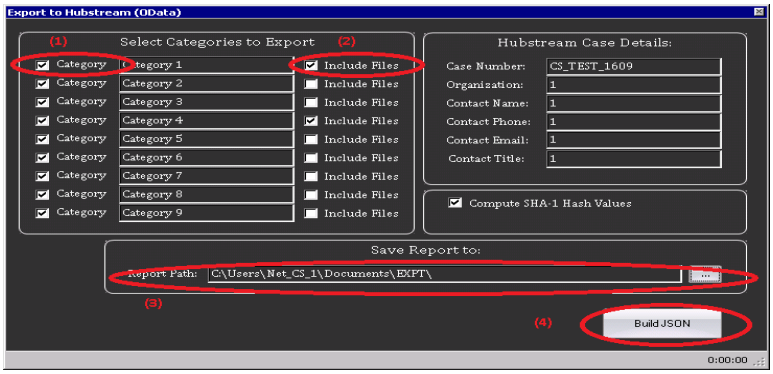
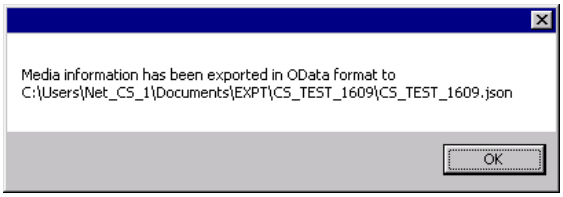
How to import the CAID Hashset update

Step	Screenshot
It is anticipated that only the force users who perform the “Data Transfer Administrator” role will undertake the Import	
1. Using the command line to convert the JSON file to CSV ODataToCSV sourcefilename targetfilename For example ODataToCSV C:\Users\John\Documents\ProjectVicCase.json c:\temp\test.csv	
2. Start C4P Review by double clicking the icon	
3. Press [Import New Case]	
4. In the Import Case Dialog a) Supply Case Name for Values - Enter Force case identifier see section 6.4 Standardisation of Case Naming b) Select C4P Hash File Note C4P Review does NOT import JSON Files. There is a utility supplied by Hubstream that converts JSON TO C4P Hash Files see step 1 c) press [Upload Values]	
5. You will receive a Process Complete dialog a) Press [OK]	

Step	Screenshot
6. EACH CAID UPDATE FILE NEEDS LOADING TWICE a) The C4ALL product has a conflicts process which interferes with the update process for CAID b) To ensure the CAID updates are loaded successfully you need to repeat Steps 4 and 5 again.	
7. Click on the [X] in the top right to close the Import Case Dialog	
8. Conflict Resolution a) Do not undertake any of the cleanse conflicts or other options to resolve conflicts b) Periodically you will need to delete the conflicts from the conflicts table by issuing the command “Delete from Conflicts” using SQL Server Management Studio or similar NOTE This should only be performed by someone experienced in SQL commands	

How to export a case for upload to CAID

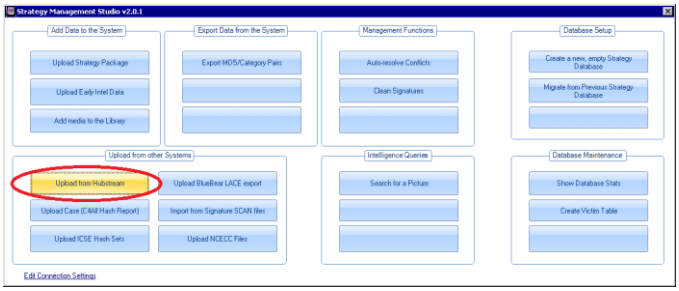
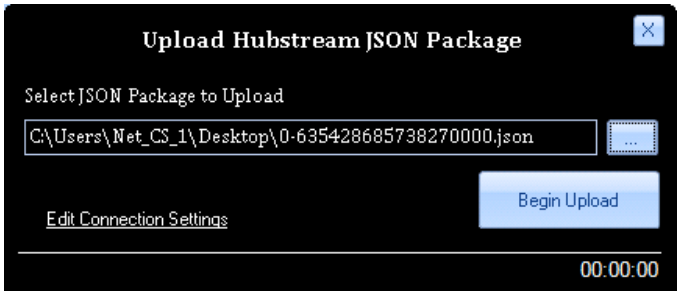
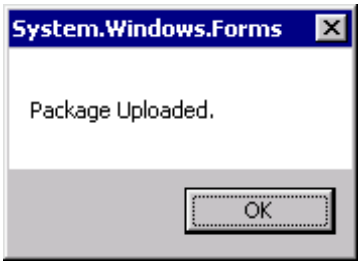
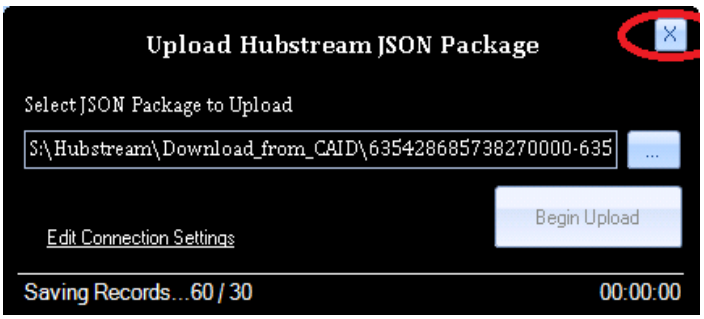
Step	Screenshot
1. Select Data Migration --> Export Work --> From case --> to Hubstream	

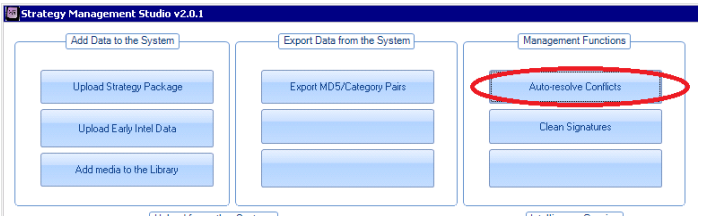
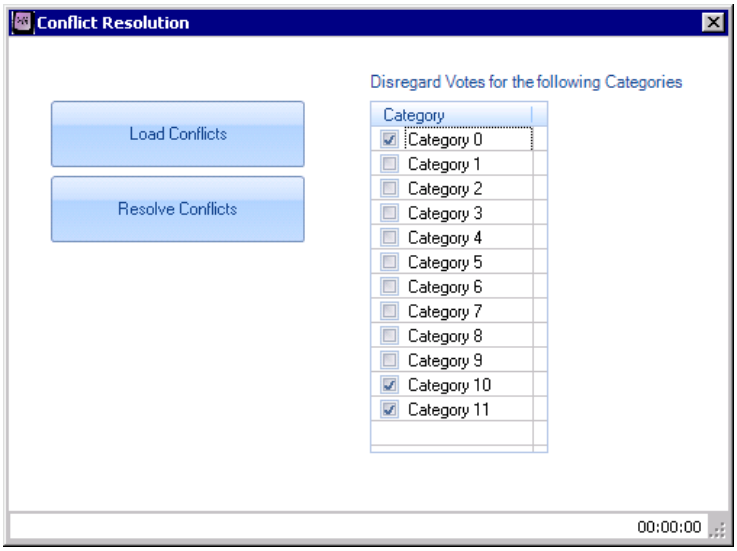
Step	Screenshot
2. The "Export to Hubstream" dialog is shown a. Select the categories of hash and images to export b. (1) From the “Category” - Select Categories 1 to 6 and 8 c. (2) From the “Include Files” - Select Categories 1 to 6 d. Select the destination folder to export the images and JSON File e. press [Build JSON] **Important:** **Case Number** must be of the format <Force Code>-<Case Number>-<Staff Number> For Example 13-CC14_0653-726573 This information is recorded in the CAID system	
3. An export success Dialog is displayed - Press [OK]	
4. At this point please liaise with the person(s) within your force who are responsible for uploading information to CAID for further instructions	

D.3 C4ALL (v2.0)

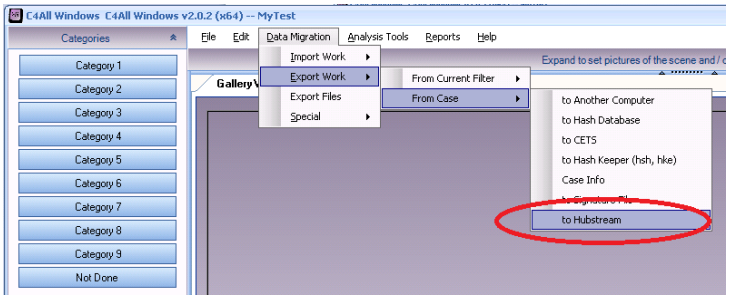
How to import the CAID Hashset update

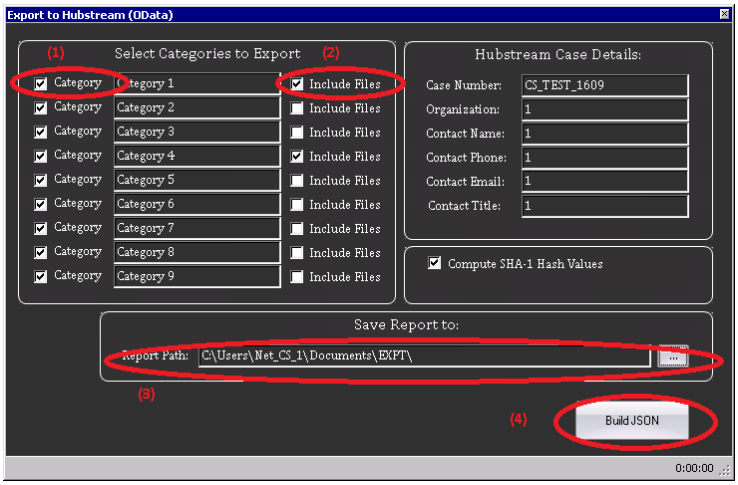
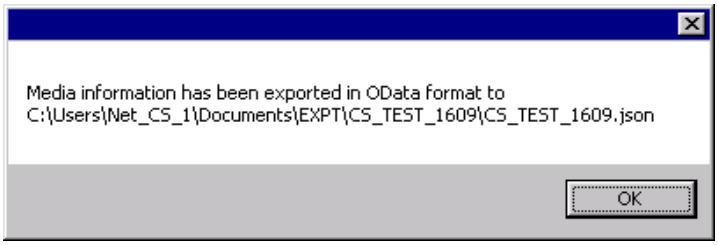
The CAID Hashfile updates are imported using a separate utility “Strategy Management Studio” (SMS)

Step	Screenshot
It is anticipated that only the force users who perform the “Data Transfer Administrator” role will undertake the Import 1. Start SMS Review by double clicking the icon	
2. Click on [Upload From Hubstream]	
3. Select the CAID Hashfile File to upload Then press [Begin Upload]	
4. Confirmation Message Displayed Press [Package Uploaded]	
5. Press [X] in the top right corner to close the dialog	

Step	Screenshot
6. EACH CAID UPDATE FILE NEEDS LOADING TWICE a) The C4ALL product has a conflicts process which interferes with the update process for CAID b) To ensure the CAID updates are loaded successfully you need to repeat Steps 2, 3, 4 and 5 again.	
7. WHEN THE FILE HAS BEEN LOADED TWICE a) Press [Auto resolve Conflicts]	
8. Set the correct categories to ignore then 9. press [Load Conflicts] 10. press [Resolve Conflicts]	

How to export a case for upload to CAID

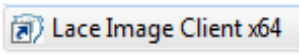
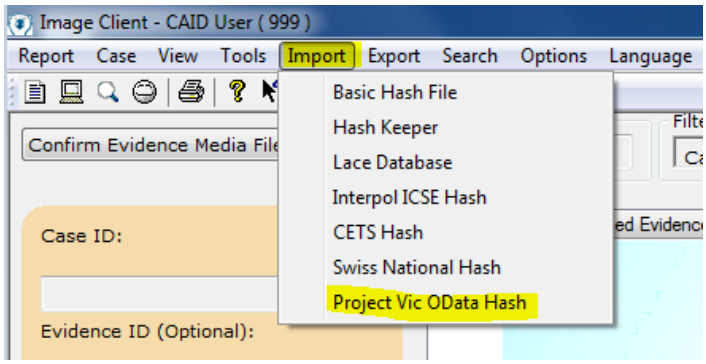
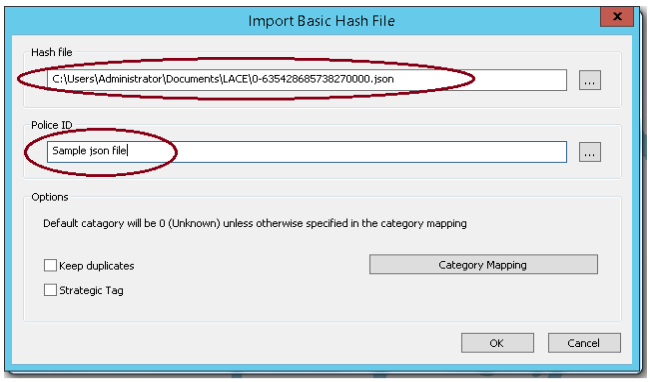
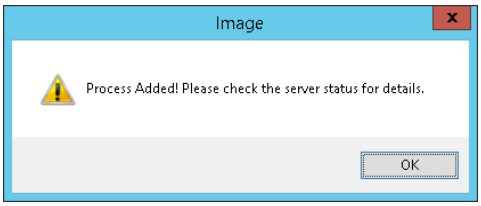
Step	Screenshot
1. WORKAROUND An issue has been identified where the incorrect value for case names is being exported to CAID Until a fix has been identified please locate and rename the *.C4P* file to prior to exporting the OData and images from C4All (Versions 2.0.2 and 2.0.3) The file name must be of the format <Force Code>-<Case Number>-<Staff Number> For Example 13-CC14_0653-726573 This information is recorded in the CAID system	
2. Select Data Migration → Export Work → From case → to Hubstream	

Step	Screenshot
3. The "Export to Hubstream" dialog is shown a. Select the categories to export b. (1) From the “Category” - Select Categories 1 to 6 and 8 c. (2) From the “Include Files” - Select Categories 1 to 6 d. Select the images to export e. Select the destination folder to export the images and JSON File f. Press [Build JSON] **Important:** **Case Number** must be of the format <Force Code>-<Case Number>-<Staff Number> For Example 13-CC14_0653-726573 This information is recorded in the CAID system	
4. Dialog is displayed - Press [OK]	
5. At this point please liaise with the person(s) within your force who are responsible for uploading information to CAID for further instructions	

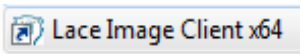
D.4 LACE

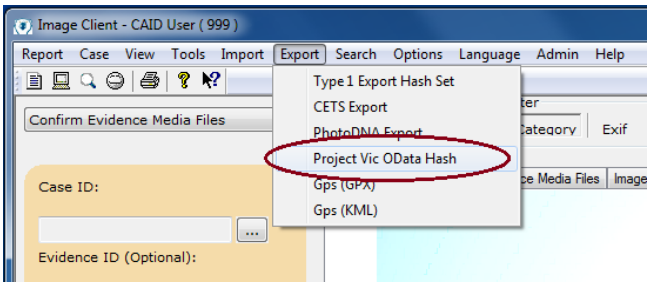
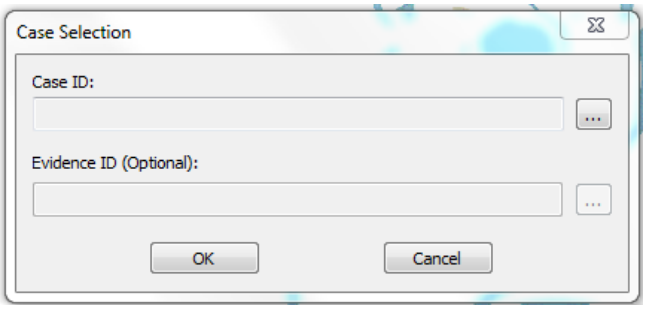
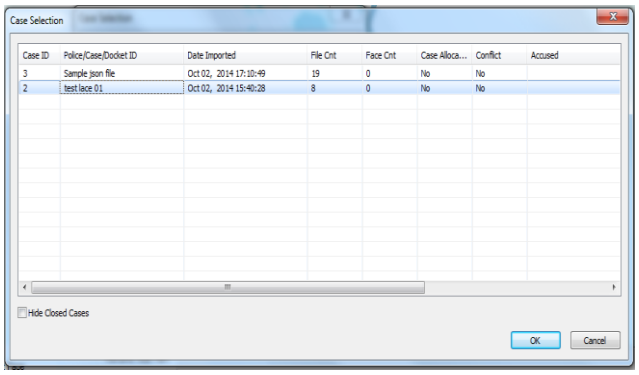
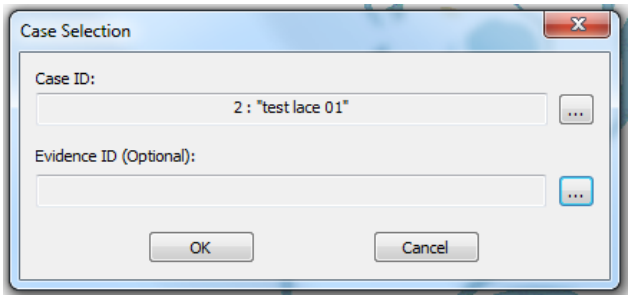
How to import the CAID Hashset update

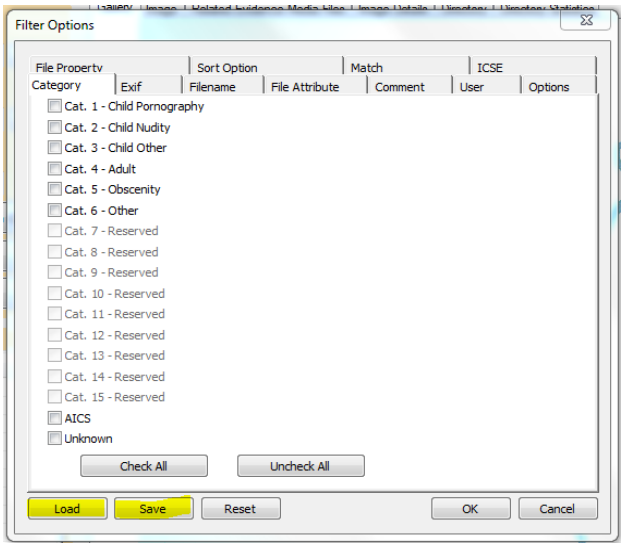
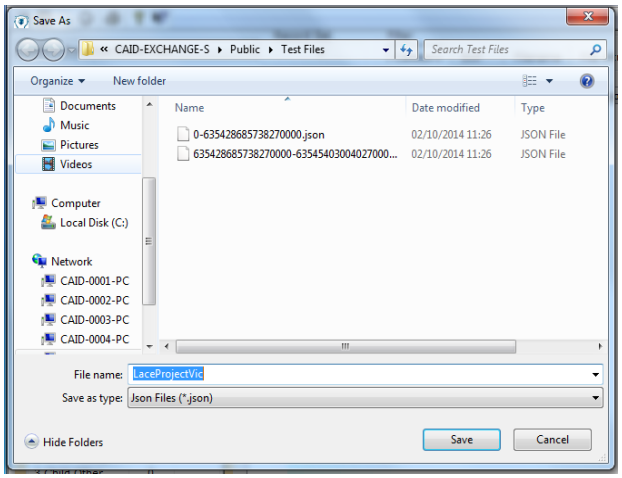
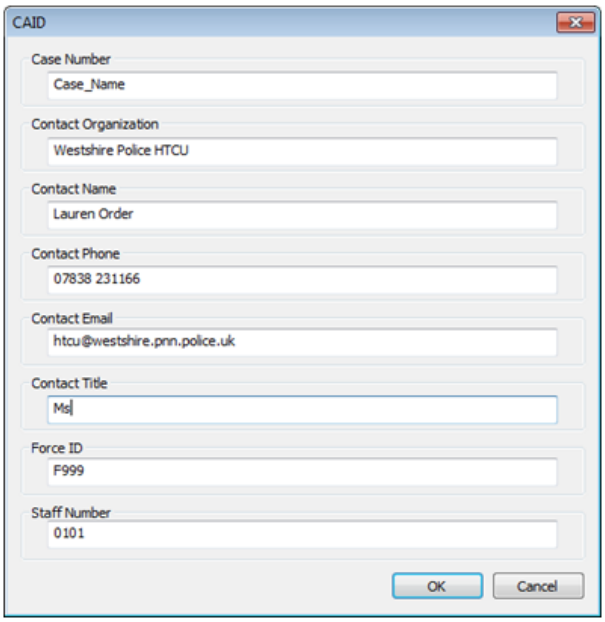
NOTE: to import json files into LACE you must run the process on the machine that is running the LACE server itself although it uses the LACE client software to perform the import.

Step	Screenshot
It is anticipated that only the force users who perform the “Data Transfer Administrator” role will undertake the Import 1. Log into the lace server and start the "Lace Image Client x64" by double clicking the icon	
2. Log in using your usual credentials	
3. On the "Import" menu, choose "Project Vic OData Hash"	
4. In the Import Basic Hash File Dialog a. Select Hash File (use the "..." button to browse for the file) b. Enter “CAID” under "Police ID" c. press [OK]	
5. If successful you should get the following confirmation dialog; a. press [OK]	

How to export a case for upload to CAID

Step	Screenshot
1. Start the "Lace Image Client x64" by double clicking the icon	
2. Log in using your usual credentials	

Step	Screenshot
3. On the "Export" menu, choose "Project Vic OData Hash"	
4. Choose the case you wish to export by clicking on the "..." button	
5. Select the case to export, and click "OK"	
6. You can restrict the export to specific pieces of evidence in the Optional "Evidence ID". If you do not restrict the export the entire case will be exported.	

Step	Screenshot
7. Click "OK" and you will see the filter options dialog; a. You can save and reload previous filter settings using the "Load" and "Save" buttons. b. Select the correct categories of hashes and images to export c. Select Categories 1 to 6 and 8 d. Select images for Categories 1 to 6 e. Once you have selected the categories you wish to export, click "OK"	
8. Choose a suitable name and location for the Export file and click "Save"	
9. Complete the meta data and click OK. Note that the “Case_Number” field will have been completed automatically with the Case ID. **Important:** **Case Number** must be of the format <Force Code>-<Case Number>-<Staff Number> For Example 13-CC14_0653-726573 This information is recorded in the CAID system	

Step	Screenshot
10. At this point please liaise with the person(s) within your force who are responsible for uploading information to CAID for further instructions	

D.5 Ziuz – VizX

TBA

Annex E Software Installation

E.1 Introduction

Whilst it is anticipated forces will have a common build for each of the two environments

- Data and Image Transfer
- CAID User Workstations

It is possible to have different Installations dependent on the local force deployment of machines and the role(s) each user will have.

The table in section 4.4 Software required to support CAID roles determines which software is required to perform each role

The hardware and software pre-requisites for each component is provided in sections 4.2 Data and Image Transfer Server and 4.3 CAID User Workstations

E.2 SSL Certificates

The CAID Trusted Root Certificate will need installing this will be provided to you via your CAID Implementation Consultant.

Delivery

- Email - Where your email system allows; the certificate can be delivered to a secure email address (.pnn .gsi etc);
  - The certificate will be contained in a zip archive (**without** password) to prevent mail clients stripping the attachment type
  - Please send an email request to caid-implementation@homeoffice.gsi.gov.uk from the email account you wish to receive the certificate.
- Post / Delivered - The certificate can be delivered via post;
  - Please send an email request to caid-implementation@homeoffice.gsi.gov.uk with the full name of the recipient and postal address from the recipients email account
  - A WinZip (AES-256) archive will be created for the Certificate using Passwords of at least nine (9) characters, used one time only and communicated to the recipient of the CD / DVD via a different mechanism (e.g. email).
  - The password will only be transmitted to the recipient once they have confirmed receipt of the CD
  - The CD / DVD will be virus scanned using commercial virus scan software which is kept up-to-date.
  - The CD / DVD will be marked OFFICIAL SENSITIVE
  - The Creation of the CD/DVD will be recorded in the
  - The CD/DVD will be double enveloped.
  - The protective marking will not be displayed on the outer envelope.
  - The inner envelope will be marked OFFICIAL SENSITIVE
  - Both envelopes will be fully addressed to the named recipient
  - Both envelopes will include return address details.
  - The CD/DVD will be sent by royal mail post using the “signed-for” service or hand delivered by a member of the CAID Implementation Team

Certificate security

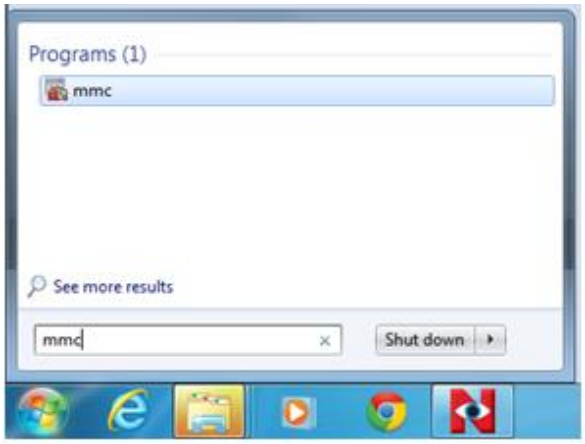
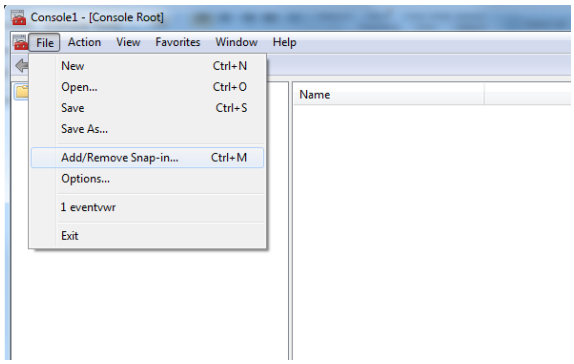
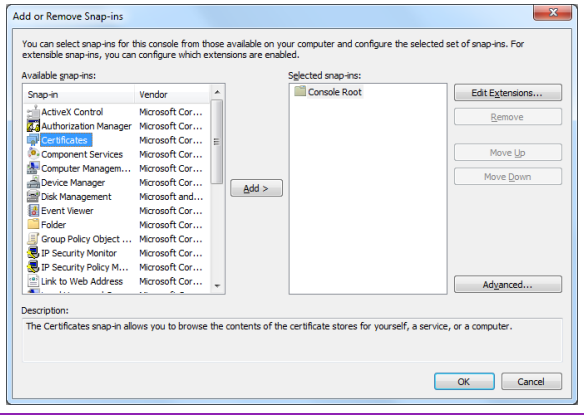
- The certificates are OFFICIAL SENSITIVE Assets
- Forces are responsible for controlling and managing the physical certificate files, including any passwords.

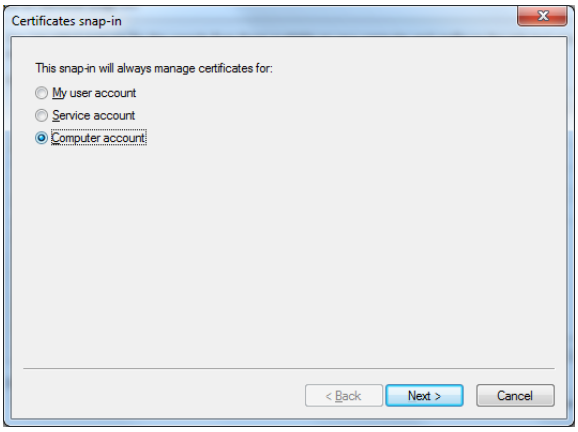
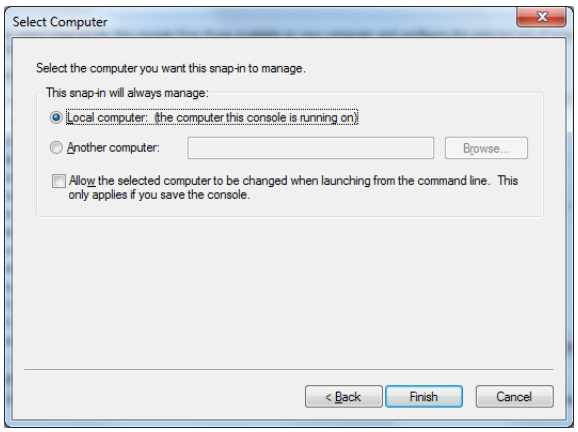
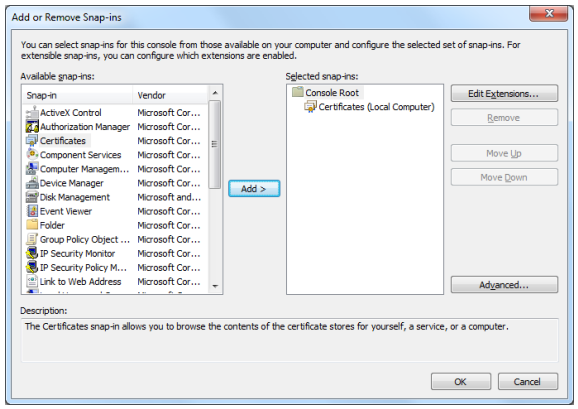
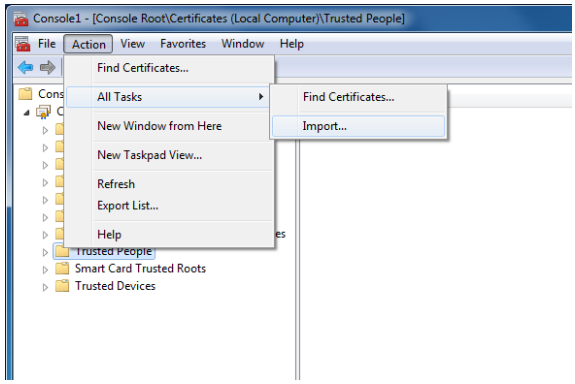
- Simple guidance to protect the assets are
  - delete the physical certificate file from each machine once imported
  - If received by email delete the email once the installation process is complete
  - A copy can be held locally but this should be protected by encryption
- Ultimately, the responsibility for safeguarding the certificate resides with the force.

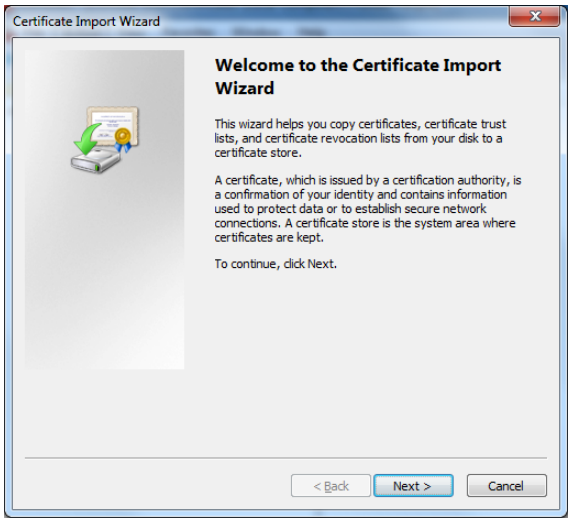
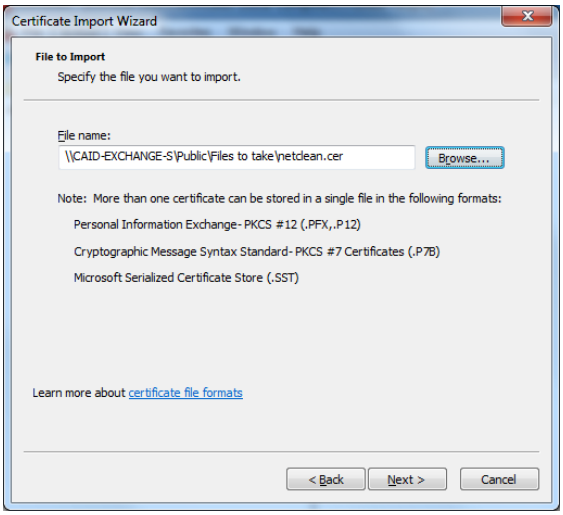
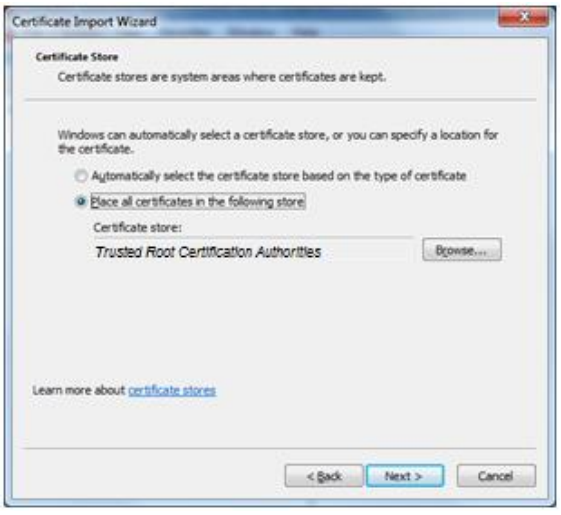
The certificates need installing on all force machines that will run the following CAID Components;

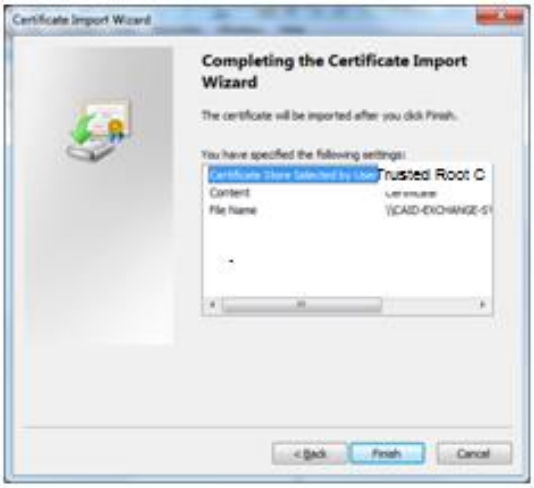
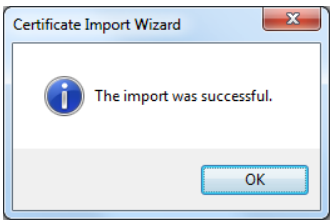
- Hubstream Intelligence Agent
- Hubstream Web User Interface
- Griffeye Web User Interface

To install the certificates please follow the instructions below on each relevant machine;

Step	Screenshot
1. Click the windows icon in the bottom left of your computer screen a. type "mmc" in the search box (see below) and select the ”mmc” application from the list b. If the dialog ""Do you want to allow the following program to make changes to this computer" is displayed press [Yes]	
2. The Microsoft Management Console should display a. select File→Add/Remove Snap-in...	
3. The Add or Remove Snap-ins should display; b. Select "Certificates" from the left hand pane c. Click the central [Add >] button	

Step	Screenshot
4. The Certificates snap-in should display; d. Select Computer account e. Press [Next >]	
5. The Select Computer dialog will be displayed; f. Select the radio button "Local computer" g. Press [Finish]	
6. The “Add or Remove Snap-ins” Dialog will be displayed again h. Press [OK]	
7. The “Console1” window will display i. Select " *Trusted Root Certification Authorities*" by left clicking under "Console" j. from the menu select Action→All Tasks→Import	

Step	Screenshot
8. The import wizard should display k. press [Next]	
9. The File To Import dialog will be displayed a. Click [Browse] b. Select the correct certificate c. Press [Next]	
10. " Trusted Root Certification Authorities" should be preselected in the "Certificate Store" (see below) if not press browse and select " *Trusted Root Certification Authorities*" d. Select [Next >]	

Step	Screenshot
11. The completion screen is displayed a. press [Finish]	
12. After a short while you will see the success dialog a. press [OK]	
13. Exit the Console by select File→Exit	

E.3 Domain Name Service / Hosts File

The Domain Names required for CAID have been registered with Vodafone's standard policing Domain Name System DNS. The entries will be managed and propagated via the standard process. we would recommend that computers connecting to CAID utilise the standard DNS.

Where this is not possible forces should provide a local DNS or hosts file. The entries required are below (please substitute the "xCJX.xCJX." with the correct xCJX IP addresses;

Details for xCJX

xCJX.xCJX.103.21	caid-4.x.pnn.police.uk
xCJX.xCJX.103.22	caid-5.x.pnn.police.uk
xCJX.xCJX.103.23	caid-1.x.pnn.police.uk
xCJX.xCJX.103.24	caid-2.x.pnn.police.uk
xCJX.xCJX.103.25	caid-3.x.pnn.police.uk

Vodafone's standard policing Domain Name System DNS for xCJX are

Primary xcjx.xcjx.55.98
Backup xcjx.xcjx.66.98

These allow UDP/53 only no TCP

Details for PSN

psnp.psnp.226.101	caid-1.x.pnn.police.uk
psnp.psnp.226.102	caid-2.x.pnn.police.uk
psnp.psnp.226.103	caid-3.x.pnn.police.uk
psnp.psnp.226.104	caid-4.x.pnn.police.uk
psnp.psnp.226.105	caid-5.x.pnn.police.uk

E.4 Hubstream Intelligence Agent

Intelligence Agent uses ClickOnce, a Microsoft deployment technology. This allows the client to be updated automatically when the server installation of Intelligence Server updates the Agent to a newer version.

Each time the web URL or UNC path for the Hubstream.Intelligence.Agent.installer file is run, it interacts with files in the user's profile. It will either download and install the application, or process any application updates from the CAID server (caid-1.x.pnn.police.uk)

The Hubstream Intelligence Agent can be installed or updated from the following URL which can only be accessed from a secure environment

- http://caid-1.x.pnn.police.uk

We recommend keeping the connection between Hubstream Agent and the CAID Server intact, and installing the Agent application via the web URL. This will allow ensure all installations run updated versions without additional maintenance overhead.

Should operational or other requirements necessitate an offline or disconnected installation, this can be supported using the offline process below; you should contact caid-implementation@homeoffice.gsi.gov.uk to discuss this process

Deploy Intelligence Agent using an offline process

For manual deployments of the Hubstream Agent a Server Installation Package is available on DVD please contact the National Business Administration team at caidbusinesssupport@westyorkshire.pnn.police.uk to receive it.

When updates are made to the central Hubstream Server that would necessitate a new agent a new DVD will be produced and distributed to you.

In a typically single workstation deployment, unzip the archive and run Hubstream.Intelligence.Agent.application.

In a multi-user organizational environment, we highly recommend hosting the files (after unzipping the archive) on a network file share or web server location so that future updates are centralized. To do this, unzip the archive in the network share or web application and access Hubstream.Intelligence.Agent.application using the UNC file path (such as \\files\Agent) or HTTP/HTTPS URL (such as http://internalserver/Agent).

Either process will install Agent to a local profile location on the workstation.

Locating the Hubstream Install Directory

The location of each installation follows a pattern that differs by installation. An example is below. The ultimate location is in the last directory that starts with "hubs" (for Hubstream).

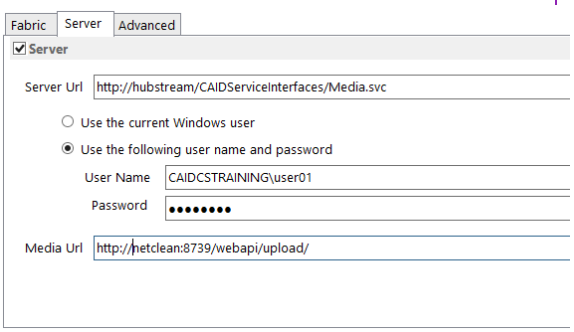
- C:\Users\<USER>\AppData\Local\Apps\2.0\D0MZ2ZRR.V2M\NK1JC0K3.AT8

The recommended method of navigating to the directory is to open the user profile directory, navigate to the AppData subdirectory (this is a hidden directory so it may be required to turn on visibility of hidden files and folders), and then navigate down the path.

Installing Hubstream

Please use Microsoft Internet Explorer to perform the install. During user acceptance testing it was observed that browsers other than Internet Explorer encountered issues so we recommend the use of Internet Explorer for this purpose.

Step	Screenshot
1. Using Microsoft Internet Explorer enter • http://caid-1.x.pnn.police.uk or if deploying the Intelligence Agent using an offline process run; • Hubstream.Intelligence.Agent.application	
2. Follow prompts to install the Hubstream Agent	
3. Start Hubstream Intelligence Agent	

4. Select the Server" tab then enter the following;
• *Server URL:*
  • https://caid-3.x.pnn.police.uk/CEServiceInterfaces/Media.svc
• *Media URL:*
  • https://caid-2.x.pnn.police.uk:8739/webapi/upload/
• *Use the following user name and password*
  • User credentials for a user who has been granted the "Data Transfer Administrator" role should be entered please prefix the user with CAID e.g.
  • *CAID\firstname.lastname*
	

5. Select the Advanced tab • Set the advanced settings (see table below)	

Hubstream Intelligence Agent Advanced Settings

Setting	Recommended	Description
Folder	Blank	Which folder to use for Hubstream downloads
Model version	Default	Which data model version to use for local grading tools
Automatic synch	On	If on, downloads and uploads happen automatically. If off, user must manually initiate download and upload

Setting	Recommended	Description
Download interval	1440 minutes	How often to automatically download the latest hashes
Autostart hour	0	If bandwidth during business hours is an issue, set this to an hour e.g. 20 or 8PM to delay auto upload/download start time

Hubstream Folders

Folders	Description
\Inbox	Folder where JSON file downloads are stored by the intelligence agent
\Outbox	Folder where JSON files and Images should be placed for upload when “Automatic synch” is on – Please follow
\Log	Contains log files of all communication and operation of the Hubstream Agent
\Temp	
\Sent	Contains all json files transferred to the server
\TimeStamp	Contains a single file with the timestamp of the last download

Configure Intelligence Agent To Use The Default System Web Proxy

When connecting to Intelligence Server or Intelligence Fabric from a secure environment, some configurations may need to be explicitly configured to use the default system proxy.

There is Hubstream knowledge base article https://hubstream.zendesk.com/hc/en-us/articles/206355608 the contents of which are below

Here are the steps to implement this option:

1. Find the installation location of Intelligence Agent

2. Open Notepad using "Run as Administrator"

3. Open the file file Hubstream.Intelligence.Agent.exe.config from the installation location.

4. Find the section <basicHttpBinding>. Underneath that, add an attribute to the <binding> element for the default setting

useDefaultWebProxy="true"

The section should now look like this, although your other settings may be different.

<basicHttpBinding>

<binding useDefaultWebProxy="true" name="ServerBinding" openTimeout="00:50:00" receiveTimeout="00:50:00" sendTimeout="00:50:00" maxReceivedMessageSize="2147483647">

<security mode="Transport">

<transport clientCredentialType="Windows" />

</security>

</binding>

</basicHttpBinding>

5. [Removed not required]

6. Exit Intelligence Agent. Ensure that the application is not minimized in the taskbar.

7. Restart Intelligence Agent

More information on these settings and other configuration options is available on MSDN.

E.5 FTPS Client

The supply of FTP client software is outside of the scope of CAID supply but, to ensure compatibility with the CAID File Transfer solution, any client used by a force must conform to the protocols specified in the following memorandum published by the Internet Engineering Task Force [IETF]:

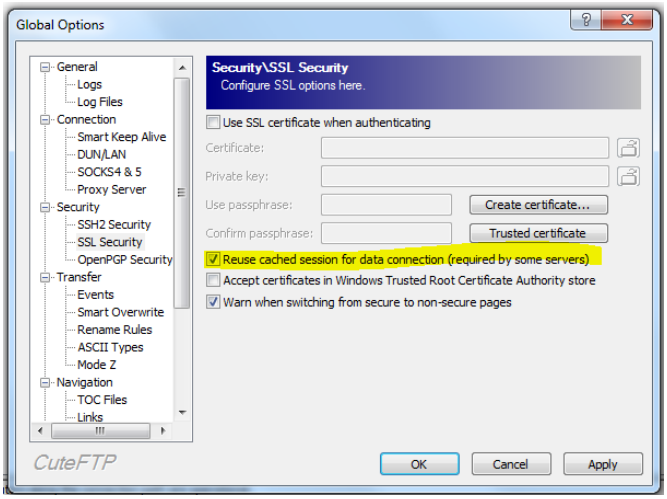
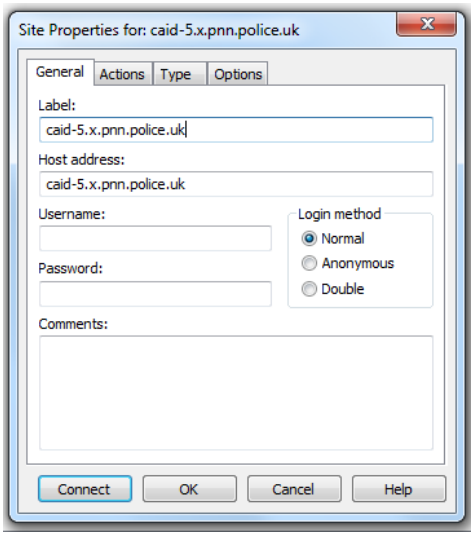
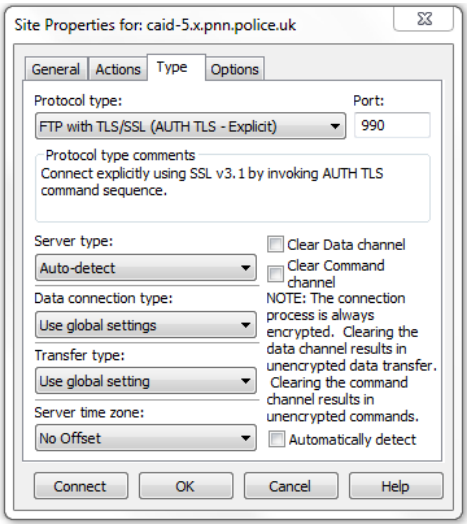
- The FTP client must support FTPs mode of Implicit and Explicit connection and FTP over TLS.
- The FTP client must support client certificate authentication.
- The FTP client must support configuration of specific ports used for data channel connection - “Passive Mode FTP”

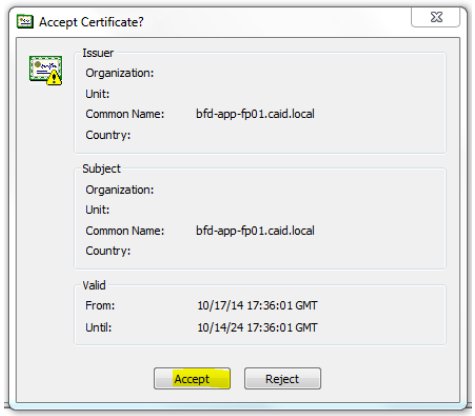
The FTPS Service is Caid-5.x.pnn.police.uk

Useful Configuration Settings

During User Acceptance Testing CuteFTP Pro was used as the FTP client software – this is not a recommendation or endorsement of that product.

The options required to connect to CAID using CuteFTP were recorded – it is anticipated that similar options will be available in most FTP Client software and should be set

Setting	Screenshot
1. Reuse Cached Session for Data Connection (required by some servers)	
2. Configure the Site Properties	
3. Configure the Protocol Type	

Setting	Screenshot
4. On first connect accept the Certificate	

E.6 Hubstream Web Interface

The Hubstream web interface has no locally installed components

E.7 Griffeye Analyze CS Web Interface

The Griffeye Analyze CS Web Interface has no locally installed components

E.8 Remote Desktop Connection (to access Griffeye Analyze CS Desktop Client)

The Remote Desktop Connection required to access the remote Griffeye Analyze CS Desktop Client does not require any additional software components however users will need access to Remote Desktop Connection provided by Microsoft

Annex F Connectivity Testing

F.1 Introduction

This section covers the full connectivity testing.

The connection testing provides confirmation for the correct configuration of the Firewall/Proxy routing of traffic to the CAID Hubstream Server (IP address, Control Port Number, Data Channel Port Numbers) – this applies at both ends of the xCJX connections.

The connectivity tests listed in this document only cover the connection from the CAID Client Software Components to CAID;

- Hubstream Intelligence Agent
- Hubstream Web Interface
- Griffeye Analyze CS Web Interface
- FTPS Client
- Remote Desktop
- Password Portal

The connectivity to the Forces grading and categorisation tools is out of scope for this document.

F.2 Prerequisites

- Forces should ensure that the SSL Certificates and where appropriate FTPS client software have been installed and correctly configured within their IL4 CONFIDENTIAL environment.
- Forces should ensure the pre-requisites for each software component have been met.
- Forces should ensure they have the correct resources available to support the connectivity testing including Networking Engineers, Firewall experts and System Administration (operating systems and infrastructure).
- Forces should have completed and had confirmation of successful acceptance of the following;
    - CAID Force Initial Users Template
    - CAID Force Connection Request (see section 5.2 Connection to CAID)

F.3 Support

- Your Connectivity Testing should be arranged with your CAID Implementation Specialist to ensure they will be onsite to support the process.

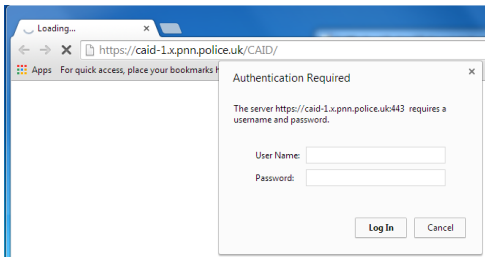
F.4 Process

Each force will undergo Connectivity Testing for new connections to CAID as follows:

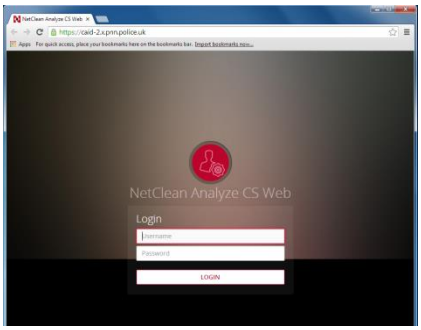
1. Hubstream Intelligence Agent Installation

Step	Screenshot
1. Follow the installation instructions in section E.4 Hubstream Intelligence Agent to install the agent direct from the CAID Hubstream Server	n/a
2. Expected Result - Confirmation that the download was successfully complete	n/a

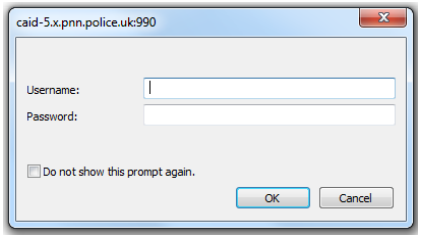
2. Hubstream Web Interface

Step	Screenshot
1. Using one of the supported browsers enter the URL https://caid-1.x.pnn.police.uk/CAID	
2. Expected Result – The Hubstream Login Page is displayed	

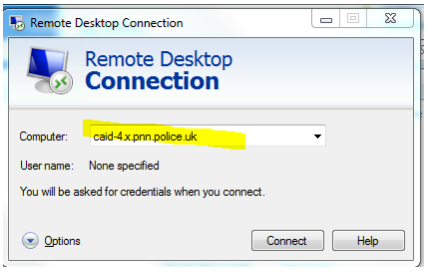
3. Griffeye Analyze CS Web Interface

Step	Screenshot
1. Using one of the supported browsers enter the URL https://caid-2.x.pnn.police.uk	
2. Expected Result – The Griffeye Login Page is displayed	

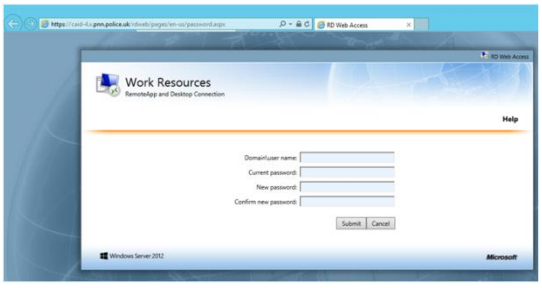
4. FTPS Client

Step	Screenshot
1. Using your compatible FTP Client user interface attempt to open a connection to the Caid-5.x.pnn.police.uk	
2. Expected Result – The FTP Server Login Page will displayed	

5. Remote Desktop

Step	Screenshot
1. Open Remote Desktop Connection by clicking the Start button. In the search box, type Remote Desktop Connection, and then, in the list of results, click Remote Desktop Connection	
2. In the Computer box, type “Caid-4.x.pnn.police.uk”, and then click Connect	
3. If presented with the dialog to trust the connection click Connect	
4. Expected Result – The Remote Desktop Login Page will displayed	

6. Password Portal

Step	Screenshot
1. Using one of the supported browsers enter the URL enter https://caid-4.x.pnn.police.uk/rdweb	
2. Expected Result – The Change Password screen is displayed	

F.5 Issue resolution

During connectivity testing:

- The force should manage the resolution of issues direct with their CAID Implementation Specialist.

During business as usual:

- Any connectivity issues during normal operations should be assessed via the standard internal force operational process.

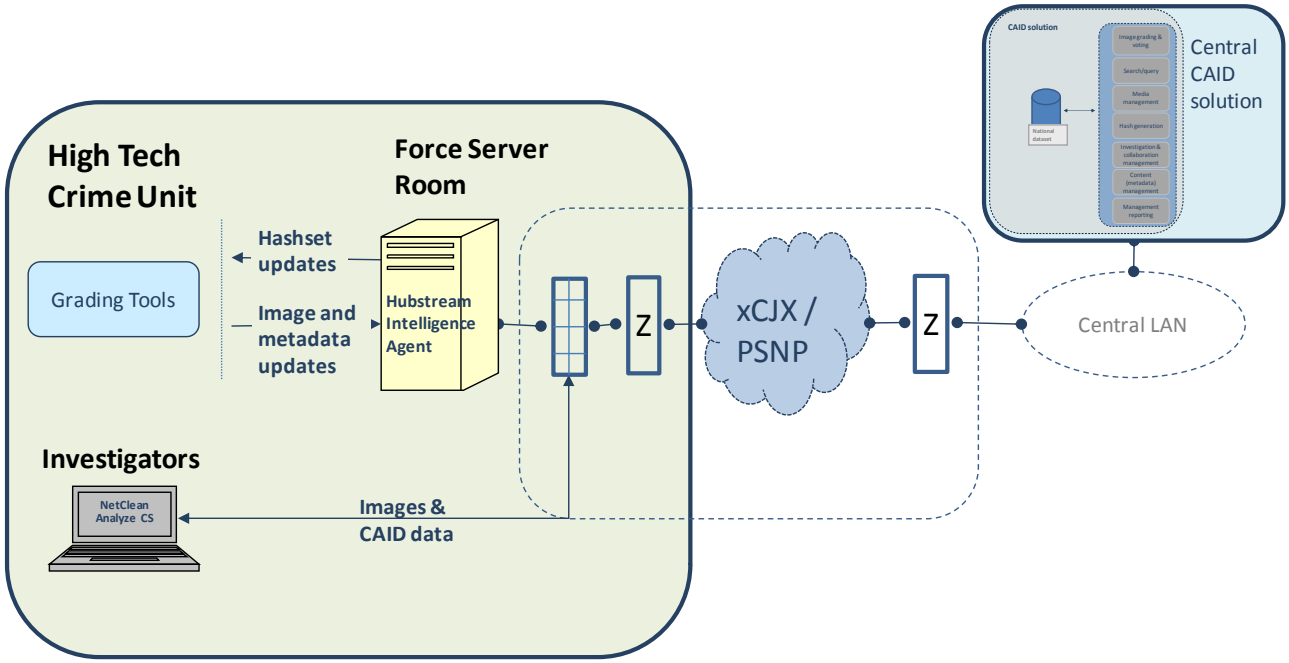
F.6 Reporting of results

Please email a summary of the tests conducted and the results to caid-implementation@homeoffice.gsi.gov.uk

Annex G Force Support Desk Instructions

G.1 Introduction

The CAID system integrates with a forces existing systems for categorising and processing illegal images of Children. A template architecture diagram is show below to show the systems and components involved however a force will have implementation differences to this.



Support may be provided by various support teams dependent on the incident type including;

- Force IT Helpdesk
- Force High Tech Crime Unit
- CAID Support Desk (Claritas)
    - National Business Administrators
    - Griffeye / Hubstream / L3

[TO BE COMPLETED]

Annex H Hubstream Griffeye Product Roadmap

Note that this roadmap is a subject to changes. Features marked with a D are decided and features marked with a P are planned for a specific release but that could also mean that a planned feature could be postponed if more urgent matters show up.

Note: Version 15.2 includes a lot of improvements to the many new features introduced in 15.1 on both server and clients.

H.1 Griffeye Analyze

H.2 Version: 15.2.0

Release date: June 29th - 2015

Griffeye Analyze CS Server

- Low level feature descriptor matching using SIFT technology D
- Support for the VICS data model version 1.2 D
  - Adaptations to CS and IS API (File & vote sync improvements) D
  - OData VICS data model updates D
- Eliminate SMB dependency D
  - Stream image and video data from server to client D

Griffeye Analyze CS Client

- Low level feature descriptor matching in Analyze relations UI D
- VICS Case export

Griffeye Analyze CS Web Client

- Download page
- Additional search and filter capabilities
- Vast UI improvements

Griffeye Analyze DI

- Support VICS data model version 1.2 D
  - Export and import case data based on new data model D
  - Integrate Analyze with yet to be announced commercial forensic software using the new data model (NUIX was announced in May using VICS 1.1) D
- Annotations D
  - Extend data model with annotations concept together with a subset of annotations properties
  - New UI (Annotations view) to annotate images
  - Link annotations to bookmarks
  - Export annotations
  - C4All Case export P

H.3 Version: 15.3.0

Release date: October 5th – 2015

Note: Version 15.3 includes a great UI “clean-up” effort on both CS thick client and DI.

▪ Griffeye Analyze CS Server

- Video fingerprinting capabilities with the F1 technology D
  - Video matching with the F1 signature D
  - Calculate and store Friend MTS F1 signature D
  - Share (import/export) the Friend MTS F1 signature D

▪ Griffeye Analyze CS Client

- New video review and analysis capabilities D
  - Video scene view based on new scene detection algorithm D
  - New video playback control D
  - Automated video filters based on visual content or motion D
  - New Video overview control D
  - Extensive video bookmarking capabilities P

▪ Griffeye Analyze CS Web Client

Yet to be decided but most likely enhanced collaborative capabilities through an activity board and add support for alerts and notifications.

▪ Griffeye Analyze DI

- Extended support for VICS data model version 1.2 D
  - Add support for the repository flag for missing files D
- New video review and analysis capabilities D
  - Fully compatible with the F1 video matching fingerprint D
  - Video scene view based on new scene detection algorithm D
  - Great improvements to the video playback control D
  - Automated video filters based on visual content or motion D
  - New Video overview control D
  - New Video playback control D
  - Extensive video bookmarking capabilities P
  - Integrate CS frame server D
- Analyze API

H.4 Hubstream Intelligence

Version 2.5 will be followed by service packs (SP1 and SP2) in 2015. Service packs are a roll-up of fixes and improvements where the goal is to respond to customer requests and improve quality, while not changing the functionality of the server enough to require extensive UAT or end user re-training before deployment. Large functional changes are included in major releases, the next planned release for Intelligence Server is version 3.0 which is targeted for a beta in third quarter 2015 and release the following year.

H.5 Version: 2.5 SP1

Release date: May 30th - 2015

▪ Hubstream Intelligence Agent

- Improved error reporting and retries for understanding and correcting any errors during upload/download D
- Performance enhancements D
- Support for VICS data model 1.2 D

▪ Hubstream Intelligence Server

- Improvements to synchronization with CS D
  - Vote history sent to CS
  - Only data for files where the media is stored is sent to CS
  - Support for visual duplicates
  - Performance improvements
- Improvements to investigation features D
- Performance enhancements D
- Support for VICS data model 1.2 D
  - Support for extended case metadata
  - Support for repository flag for missing files
- Improvements to standard reports D

H.6 Version: 2.5 SP2

Release date: October 15th - 2015

▪ Hubstream Intelligence Agent

- Substantially redesigned user interface P

▪ Hubstream Intelligence Server

- Support for F1 video signature D
- Integration with Intelligence Fabric cloud service for sharing with international agencies and private sector partners D

Annex I Force Numbers

Number	Name	Number	Name
52	Avon & Somerset	01	Metropolitan
40	Bedfordshire	02	Metropolitan
93	BTP	24	Ministry of Defence
35	Cambridgeshire	91	National Crime Agency
07	Cheshire	36	Norfolk
48	City of London	60	North Wales
17	Cleveland	12	North Yorkshire
03	Cumbria	34	Northamptonshire
30	Derbyshire	10	Northumbria
50	Devon & Cornwall	31	Nottinghamshire
55	Dorset	98	PSNI
11	Durham	96	Scotland
63	Dyfed-Powys	90	Scottish Criminal Intel. Office
42	Essex	15	Service Crime Bureau
53	Gloucestershire	62	South Wales
06	GMP	14	South Yorkshire
56	Guernsey	21	Staffordshire
61	Gwent	57	States of Jersey
44	Hampshire	37	Suffolk
41	Hertfordshire	45	Surrey
16	Humberside	47	Sussex
97	Isle of Man	43	Thames Valley
57	Jersey (States Of)	23	Warwickshire
46	Kent	22	West Mercia
04	Lancashire	20	West Midlands
33	Leicestershire	13	West Yorkshire
32	Lincolnshire	54	Wiltshire
05	Merseyside		

Annex J Quick Fix Guide

J.1 Griffeye and Hubstream Web User Interfaces

Error Message	Remedy
Receive the message “Cannot Resolve Hostname” when trying to enter the CAID web addresses	Please contact your internal IT support desk referring them to section E.3 Domain Name Service / Hosts File
Login page seen but “not authorised to access the system” message is displayed	Please contact Claritas IT support desk and request they check the account is authorised for access to the application

J.2 Hubstream Log File Error Messages

Error Message	Remedy
Hubstream.Intelligence.Agent.exe Error: 0 : Error occured in download agent. The provided URI scheme 'https' is invalid; expected 'http'.	Please check both the Username and Password in particular check and remove spaces at the end of either Reset the password using the password Portal
Hubstream.Intelligence.Agent.exe Error: 0 : Error occured in download agent. The HTTP request is unauthorized with client authentication scheme 'Negotiate'. The authentication header received from the server was 'NTLM,Negotiate'.	Please check both the Username and Password in particular check and remove spaces at the end of either! Reset the password using the password Portal
Hubstream.Intelligence.Agent.exe Error: 0 : Error occured in download agent. There was no endpoint listening at https://caid-3.uat.claritas-solutions.com/ceserviceInterfaces/media.svc%20/Media.svc that could accept the message. This is often caused by an incorrect address or SOAP action. See InnerException, if present, for more details.	Please check the “Server URL:” and “Media URL” in particular check and remove spaces at the end of either
Hubstream.Intelligence.Agent.exe Error: 0 : Error occured in download agent. Could not establish trust relationship for the SSL/TLS secure channel with authority 'caid-3.uat.claritas-solutions.com'.	Please check you have installed the SSL Certificate correctly on the machine. If in doubt reinstall

Skipping Download due to no changes	This is not an error it indicates there are no new downloads to retrieve

Annex K Change Log

Description
K.1 Version 1.0
○ Updated post early adopter go-live to be used by all forces and connecting law enforcement agencies
K.2 Version 1.1
○ Section 4.2 “Connection to CAID” removed “And National Accreditor??”
○ Section 3.4 “Compatible Force Categorisation Tools” – updated the compatible versions
K.3 Version 1.2
○ Section E.4 Hubstream Intelligence Agent – removed unnecessary instructions to setting the TimeStamp date
○ Section D.4 LACE – updated the export instructions
K.4 Version 1.3
○ Added Annex G Force Support Desk Instructions [TO BE COMPLETED]
○ Added Annex H Hubstream Griffeye Product Roadmap
○ Added Annex J Quick Fix Guide [TO BE COMPLETED]
○ Amended Annex D Import and Export To CAID. **Error! Reference source not ound.** to provide guidance on enabling via the Digital Market Place
K.5 Version 1.4
○ Added Section 4.7.2 Force Migrating to PSN ○ Added Annex I Force Numbers ○ Updated Annex D Import and Export To CAID. To include a workaround for C4ALL case naming and to reinforce the case name/number in all tools. ○ Updated section 4.4 Software required to support CAID roles to reflect the availability of the Hubstream UI and the new role names ○ Updated Section 1.5 Releases of CAID software to reflect new release schedule ○ Moved Section 8 to Section 3 updated Section 3 Roles to remove Researcher (also removed from the entire document) modified some role names and added the new “NCA CEOP Victim ID” Role ○ Updated 8.2.1 Categories for Upload and Download – Category 8 hashes (not images) can now be included for upload (Cat 0 and 9 are still excluded) ○ Added Section 5.5.4 Gateway Solution Scripts / Software ○ Added Section 8.1.1 CAID “Gold Disk”
K.6 Version 1.5

Description
○ Amended Section 5.5.4 Gateway Solution Scripts / Software ▪ Clarified the scripts are only compatible with the FTP Client “CuteFTP” ▪ Added a prerequisite for SQL Server ▪ Amended the overview diagram to reflect points 1 and 2 ○ Amended section 4.2 Data and Image Transfer Server ▪ Updated the version of Hubstream required in line with CAID R2 ○ Amended Section 4.3 CAID User Workstations ▪ Removed the roles from the table as these are provided in section 4.4 Software required to support CAID roles ○ Amended 2.7 Costs ▪ Revised the cost of Pen Tests ▪ Included West Yorkshire Police costs for the gateway solution ○ Amended Section Annex D Import and Export To CAID. ▪ Improved the instructions on the categories and images to export (Defect 231) • Categories 1 to 6 and 8 • Files - Categories 1 to 6 ○ Altered the description for category 7 to 'Unconfirmed' (Defect 217) ○ Added Section 6.1 CAID Business Processes
K.7 Version 1.6
○ Updated Annex H Hubstream Griffeye Product Roadmap ▪ Updated to reflect new roadmap from vendors ○ Updated section 7 Service Management ▪ Updated section 7.1 User account management: completed all TBA Sections ▪ Inserted section 7.2 Business Support ○ Updated 4.5 Compatible Force Categorisation Tools ▪ Provided a link to the ODatatoCSV utility ○ Updated Annex J Quick Fix Guide ▪ Added the known Hubstream Error Messages ○ Updated Annex D Import and Export To CAID. ▪ Amended D.2 C4ALL (ver 1.1) to reflect the correct process for loading files from CAID including conflict resolution ▪ Amended D.3 C4ALL (v2.0) to reflect the correct process for loading files from CAID including conflict resolution
K.8 Version 1.7
○ Updated all sections to ▪ Rename both “CAID Local” and “Local CAID” roles to “Data Transfer Administrator” ▪ Change the contact from the CAID Implementation team to the National Business Administration team at caidbusinesssupport@westyorkshire.pnn.police.uk for relevant tasks ○ Updated Section 4.6 Connection Details for Administrators ▪ Added PSNP IP Addresses ○ Updated Section Annex A CAID Project Contacts ▪ Updated the implementation team contacts ○ Added section 4.7 PNN3 Migration to PSN

Description
K.9 Version 1.8
○ Updated 8.2.1 Categories for Upload and Download ▪ Modified the text for category 7 ○ Updated Section 4.6 Connection Details for Administrators ▪ Corrected the Password Portal from 433 to 443
K.10 Version 1.9
○ Updated Section E.3 Domain Name Service / Hosts File ▪ Provided PSN Hosts file ○ Updated Section E.4 Hubstream Intelligence Agent ▪ added a section on configuring the intelligence agent to use the default system web proxy
K.11 Version 1.10
○ Updated Section D.1 Import and Export to CAID - Griffeye ▪ Changed step 5 in “How to export a case for upload to CAID” to reflect additional steps.
K.12 Version 1.11
○ Changed all references to “NetClean” to the new name of “Griffeye” ○ Added details of ports and protocols for use with the Griffeye Analyze CS desktop client due for release in November 2015 (page 27)
K.13 Version 1.12
○ Amended table in section 4.6. Added entries that relate to Griffeye Analyze CS Desktop, and removed references to the xCJX network ○ Changed some references to the e-mail address caid-implementation@homeoffice.gsi.gov.uk

Annex L Referenced Documents

Document	Version	Description
CAID User Roles and Responsibilities	1.1	Document describing role titles and activities expected to be carried out (.ppt)
Child Abuse Image Database Business Impact Assessment	1.0	Outcomes of the Business Impact Assessment (BIA) workshop held on 6 February 2014 to determine the potential impacts of a breach of security affecting the Child Abuse Image Database (CAID).
CAID RMADS Annex III User SyOPs	0.4	The SyOPs set out the procedures to be followed by users of the CAID system regarding access to, and use of, system facilities.
Product Roadmap - Hubstream IS 2 5 Griffeye Analyze 15 2 15 3.pdf		Griffeye and Hubstream Product Roadmap