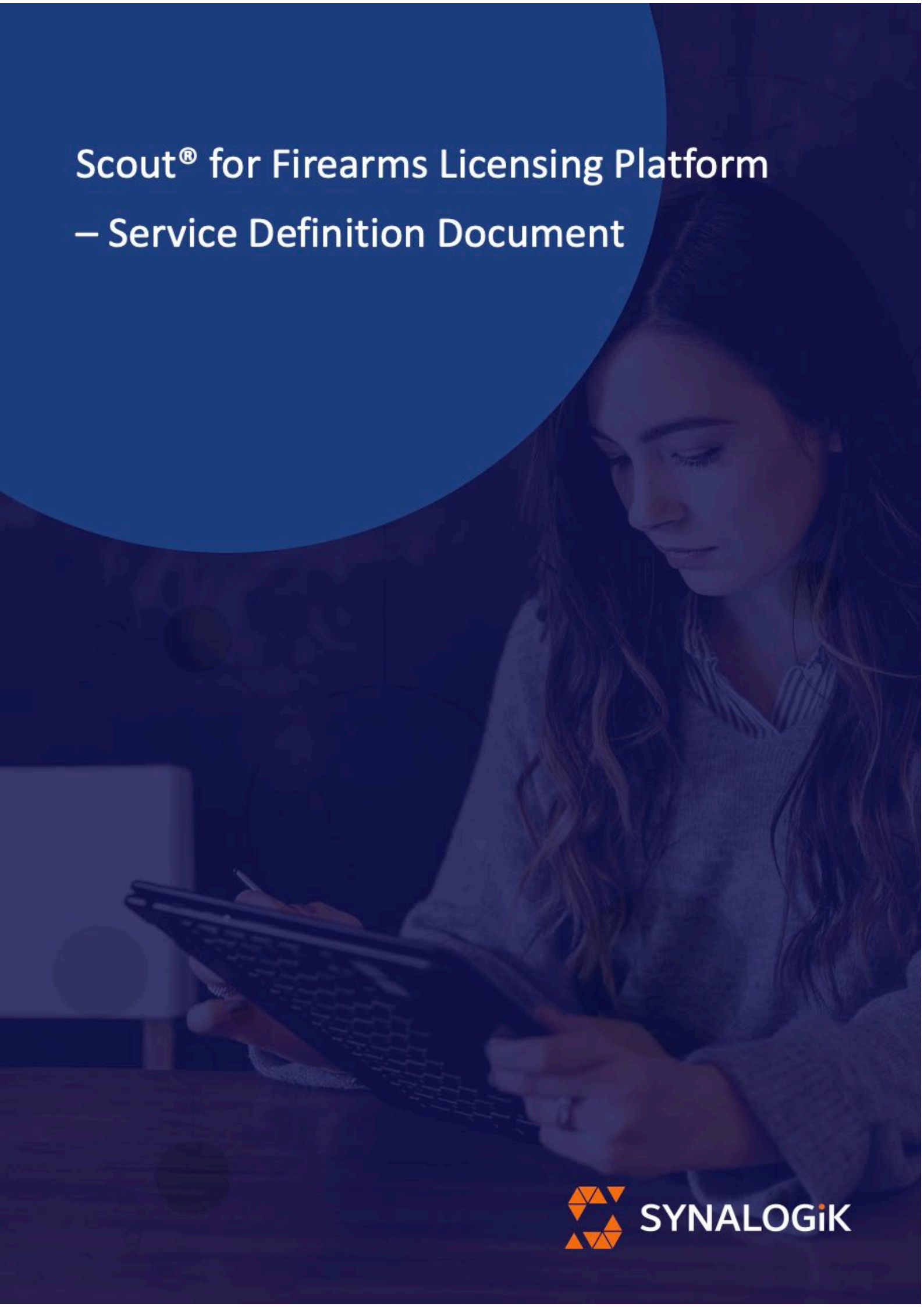
Scout® for Firearms Licensing Platform – Service Definition Document



SYNALOGiK

Solution Overview – Scout® Firearms Licensing platform

Meet Scout® by Synalogik, a one-of-a-kind, auditable, and evidential vetting platform for discovering hidden risks and providing firearms licensing teams with the ability to automate checks across third-party, sensitive policing and open-source data sets. Scout® automates checks for individuals or organisations seeking all kinds of UK Firearms Certificates.

Having gathered and merged the data sources relating to that application as part of an automated workflow, the licensing officer can view the RAG rated results within auditable reports, node view charts, on a map or combined within a spreadsheet. The applications can be ingested into the system individually or via our bulk uploader. A bespoke "firearms check" template can be constructed to allow the same search parameters to be used each time a check is made - ensuring consistency in the checks, time saved constructing the search and an auditable log for each search.

The Scout® Firearms Licensing platform harnesses the power of automated data aggregation, robot process automation, and a sophisticated graph database providing swift, clear and auditable reports for every applicant. It can reduce manual investigation times per enquiry to a matter of minutes for any individual case; saving up to 85% of your teams' time.

Scout® comes as a cloud-based software platform. All Synalogik platforms can be deployed upon a variety of cloud-based providers or on premise, however our standard platform is hosted upon AWS. The system has been deployed with a variety of police forces, Government Departments and Law Enforcement Agencies in a way that meets with their Data Protection, Information Security and all other requirements.

Background and Legislative Guidance for Chief Officers relating to Firearms Licensing Checks

The inspection of police firearms licensing by Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services in 2014-2015 highlighted the need for more consistency in the application of firearms licensing law by police forces and recommended that existing Home Office guidance be put on a statutory footing. This was supported by HM Inspectorate of Constabulary in Scotland in its March 2018 inspection of firearms licensing. The Government subsequently introduced a power for the Secretary of State to issue statutory guidance to chief officers of police through an amendment to the Firearms Act 1968 ('the 1968 Act') made by the Policing and Crime Act 2017.

The Policing and Crime Act 2017 inserted section 55A in to the 1968 Act, allowing the Secretary of State to issue guidance to chief officers of police as to the exercise of their functions under, or in connection with, the 1968 Act. Chief officers of police in England, Wales and Scotland must have regard to such guidance and be able to justify any departure on a case-by-case basis.

The guidance is to be applied to all applications received, and licensing decisions made, on or after its publication, including reviews of suitability of existing certificate holders and registered firearms dealers.

The guidance set out below is taken directly from the Statutory guidance and is to "assist chief officers in interpreting the law and setting operational practices respectively." It sets out the checks that chief officers should complete to assess whether a person can be permitted to possess firearms without danger to public safety or to the peace. The checks apply to the grant or renewal of a shotgun or firearm certificate, or for certification as an RFD. They also highlight the standards which must be applied to ensure a thorough and consistent approach to assessing the risk to public safety.

A firearm certificate shall be granted where the chief officer of police is satisfied:

(a) that the applicant is fit to be entrusted with a firearm to which section 1 of this Act applies and is not a person prohibited by this Act from possessing such a firearm;
(b) that he has a good reason for having in his possession, or for purchasing or acquiring, the firearm or ammunition in respect of which the application is made; and
(c) that in all the circumstances the applicant can be permitted to have the firearm or ammunition in his possession without danger to the public safety or to the peace.

Key takeaways from the statutory guidance:

1. "All applicants should be checked against **the widest relevant databases** to gather conviction, intelligence and counter terrorism data",
2. If any **new information comes to light** as a result of background checks, for example if the applicant's circumstances have changed materially since the original grant or last renewal, or if they are otherwise considered higher risk, for example due to relevant information about behaviour or a medical condition, it is likely that **more extensive enquiries will be necessary** than if none of the above apply,
3. All records found relating to the applicant should be recorded on the application file. This will include instances where the applicant is a victim, witness or associate rather than a suspect,
4. Background checks and medical checks apply to renewals as to grants,
5. Chief officers should ensure that information about applicants, servants, or other individuals subject to checks is processed in accordance with the provisions of data protection legislation and the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002,
6. **Each case should be subject to a risk assessment**, considering **all the available information** in line with the factors for consideration set out in this Chapter. The chief officer must additionally be satisfied that the applicant has good reason for possessing firearms,

7. The chief officer should, when assessing the grant, renewal, or revocation of a firearm or shotgun certificate or RFD registration, ensure that all the available information that may be relevant to the case is considered,
8. The previous criminal, or allegedly criminal, behaviour of an applicant may indicate a future or ongoing risk to public safety or to the peace in the event that they were to possess a firearm. Information that may be relevant in indicating criminal or possible criminal behaviour will include, but is not limited to:
    - (i) previous convictions, cautions and any other disposal, for any offence (including speeding but not including parking offences or fixed penalty notices);
    - (ii) all overseas convictions and disposals;
    - (iii) arrests, police call-outs and bind-overs;
    - (iv) any civil orders the applicant has been subject to, for example Domestic Violence Protection Notices (DVPN) or Domestic Violence Protection Orders (DVPO) or their Scottish equivalents, and compliance with those orders;[footnote 20]
    - (v) evidence relating to criminal proceedings that resulted in an acquittal.
    - (vi) evidence, including intelligence, of any criminal behaviour where no charges, conviction or other disposal resulted; and
    - (vii) safeguarding assessments, including domestic abuse, stalking and honour-based violence (DASH) assessments or those made by multi-agency safeguarding hubs
9. Other information that may be suggestive of the existence of a danger to the public safety or the peace includes, but is not limited to:
    - (i) associations with known criminals or suspected criminals, including members of gangs or organised crime groups, or associations with terrorist or proscribed groups or organisations; or aggressive, abusive or anti-social behaviour or incitement to hatred against particular groups categorised by, for example, race, gender, disability, sexual orientation, age or religion.
    - (ii) evidence of dishonesty;
    - (iii) evidence of threatening or abusive behaviour;
    - (iv) evidence of anti-social behaviour;
    - (v) evidence of reckless behaviour, lack of self-control or restraint, or disregard for the safety of others;
    - (vi) indications that the individual will not handle the firearm responsibly;
    - (vii) insufficiently secure storage arrangements;
    - (viii) relationship difficulties or other domestic turmoil;
    - (ix) unmanaged debts, financial pressures, abnormal financial activity, or unexplained sources of income;
    - (x) relevant medical conditions including alcohol and drug abuse (see section D below);
    - (xi) previous non-compliance with firearms certificate or other types of licences held; and
    - (xii) any of the above factors in relation to a person other than the certificate holder living at, or with unsupervised access to, the address or addresses.

Lack of time and resource often means that one of the key tenets of the guidance provided to Chief Officers is not adhered to as closely as the public might wish:

*"Chief officers should ensure that processes are in place to allow **continuous assessment of suitability** to possess firearms or to be an RFD between grant and renewal.*

4.2 These processes may consist of either:

- *(i) ensuring other parts of the force, including command and control and domestic violence (or public protection) units, systematically notify the firearms licensing department as soon as possible of any new intelligence or incidents involving certificate holders or RFDs, whether by automated processes or manually; or*
- *(ii) the firearms licensing department completing **cross-checks of certificate holders and RFDs against all relevant local and national databases and intelligence systems on a regular basis**."*

Key Benefits & Features of using the Scout® Firearms Licensing platform

· Live data interrogation across all relevant data sources, allowing for more regular checks to be done upon holders of shot gun licences, Firearms Licences and RFDs

· Discover hidden links in merged data sets –Scout® WorkBench allows users to carry out further investigations on the applicant(s) by visualising links between entities and providing the ability to select and investigate any one of them further at the click of a button.

· The ability to search against sensitive data sources as one, including pre-configured access, where hosting and legal requirements are satisfied, to PNC, Ident1, the prison and probation service intelligence database, HM Passport Office imagery and, from the end of 2022, PND.

· The "Data Clasher" functionality allows users to upload large or small additional repositories of data as a spreadsheet into the platform and thereafter to discover hidden connections between those uploaded sources and your ongoing enquiries. These spreadsheets may be the lists of recently refused applicants, known residences of concern or any other datasets compiled for legitimate licensing purposes which ought to be checked as part of ongoing reviews.

· Avoid bottlenecks and backlogs of applications or renewals by relieving licensing officers of the monotonous task of typing in the same search inputs into multiple databases time and time again – simply create templated searches with fixed risk assessments for firearms applications and renewals, which can be used in bulk or individually; relieving pressure upon scarce resource and giving you the time to focus on decision making, not researching.

· Better customer experiences – members of the public applying for licences rely upon swift decision making, but manual checks logging in and out of different data repositories often create a backlog. Let Scout® change the research time to seconds; ensuring greater customer satisfaction, higher productivity for your team and most importantly compliance with your Chief Officers statutory obligations.

· Reduced reputational risk – Where licensing officers are making decisions which have the ability to impact their forces reputation, they need to know that every stone is being lifted before decisions are made.

· Data agnostic – Scout® is data agnostic and pre-integrated with the majority of relevant data sources; eliminating the learning curve and IT resource required to change data suppliers and giving you the flexibility to choose a provider that best suits your needs.

· Conduct Open-source enquiries in a variety of languages at the click of a button - Scout® can be configured to retrieve precise OSint results relating to people, companies, cars, addresses, email addresses and phone numbers in most major languages, giving you insights into foreign nationals and UK nationals who have been resident outside the UK "for a significant period of residence".

· Configurable access using multi factor authentication, Single Sign On and IP address whitelisting, thereafter providing users with a single search across multiple data sources in one go.

Service Description

Scout® is designed for rapid gathering of information from third party data sources, open-source and even your own internal data sources, including Police sensitive sources where hosting and usage requirements are met. Synalogik has incorporated these data sets into API's that are "called" in real time to give you up to the minute results. The search can be conducted on a person, a telephone number, email address, address, commercial entity, or vehicle. The results can be cleansed and reviewed using risk assessments, then viewed as text, node charts, on street view or upon a map. Scout® can perform your search in a fraction of the time taken to manually log in and out of multiple different data sources.

Scout® is made up of many innovative feature-rich tools, each of which contribute to maximising operational efficiency within your team.

Data Aggregation

In-depth reviews on firearms applications and renewals require data from multiple different sources, which, when collated manually, are incredibly time-consuming to complete.

While some automation solutions exist, they often only include their own proprietary datasets, which are insufficient to conclude the checks satisfactorily and inevitably result in the user having to log back into other data sources internally or on open sources before completing an enquiry.

Our automation platform, Scout®, resolves this with a data agnostic approach to aggregation, integrating all your chosen datasets into a single intelligence environment; allowing you to search once and automatically pull data from all these datasets in an auditable and GDPR compliant manner.

The Scout® platform is pre-configured to interrogate data from all major data aggregators and Open Sources. The list of sources grows weekly, but key integrations include data from:

1. Equifax
2. TransUnion
3. Experian
4. GB Group
5. CreditSafe
6. *CRIF / CUE*
7. LexisNexis
8. CIFAS
9. DVLA
10. DVSA
11. Companies House
12. Google API
13. Bing API
14. Sayari (global commercial data)
15. Land Registry

Policing data sources integrated into the DataHunter platform:

1. Police National Computer (“PNC”)
2. Police National Database (“PND”) *(coming in Q4 of 2022)*
3. NOMIS (HM Prison and Probation Service intelligence database)
4. HM Passport Office
5. Ident 1 (Fingerprint data)

Open-Source Intelligence

Open-source intelligence is the fastest growing source of information and the least used by firearms licensing officers, despite the fact that the statutory guidance for chief officers requires such searches to be performed in all cases.

The Scout® Firearms Licensing platform enables you to create templated, highly configurable searches around keywords, proximity, time-frame and document type from the world wide web.

· Select from, or customise, our tried and tested OSint templates for your Force; benefiting from the experience within our Synalogik team and our wide customer base in both the public and private sectors.

· The Scout® Firearms Licensing platform is sufficiently advanced to allow you to only retrieve results linked to your inputs, by putting filters around the location of the results, the timeframe when they were created and the type of document on the web.

· The Scout® Firearms Licensing platform complies with Data Protection Laws and is configured to protect your teams from reviewing information held behind privacy walls or firewall protected sites.

· If your team are "Googling" applicants for licences as part of their investigations, reviewing potentially millions of results, many of which are prioritised by their browsing preferences not actual relevance, then their time is being wasted and the results they're churning through are affected by irrelevancies such as marketing campaigns and sponsored advertisements. These are eradicated by reviewing results directly through search engine APIs rather than their web interface.

· Retain an auditable log, within a standardised report, for all the open-source search results your team produce.

· Start your search query from the country of origin of the applicant to prioritise the results for foreign nationals.

· Easily create, save and add the searches into Scout® workflows that can be applied to individual, batch or inbound automated API queries.

· Retrieve OSint results from live webpages, cached webpages or via direct link to the Wayback Archive – giving you the chance to review results which have otherwise been removed from the web.

Workflow Templates

Spending time manually logging in and out of different data sets before being able to make decisions is inefficient. With Scout® you can create bespoke workflows to cover differing types of firearms application and renewal checks.

· Chose the data inputs you want to research – name, address, email address, telephone number, commercial entity, vehicle registration or IP address.

· Select how Scout® compares inputs to potential results using “fuzzy”, “exact”, “contains” or “begins with” as search filters.

· Filter potential results by name spelling, age or proximity to help remove false positives.

· View and select from a list of all data sources which you want Scout® to interrogate.

· Create bespoke Open-Source searches designed to target keywords, document types, countries or time frames for that type of application and its associated risks.

· Save these configurations as templated workflows to your Scout® home screen for your team to use time and time again.

· Initiate your workflow via API, individually or in bulk.

Risk Assessment

Decisions about firearms licensing are complex and subject to human error when numerous datasets are involved. Manually reviewing risk from multiple data sources is extremely time consuming and the consequences of getting it wrong can result in huge reputational damage or worse.

The Scout® risk assessment tool allows you to create sophisticated rules that automatically look for specific risks, and then score them to get an overall assessment of their level, helping you to make the right decision, save you money and reduce investigation times.

· Build any number of negative or positive risk rules and weight the results to build out a holistic risk view.

· Highlight risk as a score or Red, Amber, Green rating (“RAG”).

· View risk assessments in your Workbench or embedded within reports.

· Get an auditable, transparent and detailed assessment on people, companies, vehicles, addresses, email addresses and phone numbers.

Synalogik Knowledge base

The Scout® Firearms Licensing platform has the optional and highly configurable capability to automatically identify disparate links between seemingly disassociated licensing checks, when requested. Each time a search is initiated, Scout® cross references the findings against the existing "knowledge base" and highlights where searched entities are linked. These "flags" are seen within the report providing the most recent user with the contact details for the previous user who created the linked report - subject to access management rules.

When selected, the "Synalogik Knowledge Base" searches across your database to automatically find if anyone has looked at these search inputs before; providing you with unrivalled insight into the holistic risk this application presents.

How Scout Works

Technical Description

Scout® is an Open-Source Intelligence (OSInt) and data aggregation investigation platform which retrieves data from the web, third party APIs and sensitive 'internal' data sources usually only available on standalone systems. The platform will require firewall access configuration within organisational security policies.

Scout® is accessed using via all standard web browsers, including but not limited to Firefox, Chrome and Internet Explorer. Appropriate internet bandwidth must be available. Our cloud service and resources are provided in the eu-west-2 (London) region within data centres that are accredited to the PASF (Police Assured Secure Facility) standard.

We create a separate environment (or VPC, Virtual Private Cloud) for each customer, there are no shared resources and no opportunities for data to leak between customer systems.

Synalogik provide our customers with access to Scout® via a URL, meaning that no on-premise infrastructure is required within your organisation. If the highest levels of security are required for specific customers or projects, Scout® can be deployed on premise or within secure private clouds. Scout's rules and risk algorithms are customisable, meaning clients can refine and tag certain results or types of data to suit the investigation.

Scout® was designed and built by law enforcement officers and specialist criminal and regulatory barristers, ensuring that it automates the capturing of all evidence in a manner that is compliant with the Criminal Procedure and Investigations Act 1996 (CPIA) and all Data Protection Laws. Every search is auditable, and every node of data brought into the platform is time and date stamped down to the second. Scout® also captures individual users' activity for internal audit ability from a legislative and professional standards perspective. Users access

Scout® via their existing hardware and IT infrastructure. Everything in the onboarding process has been designed to ensure that cost efficiencies are maximised for the client.

Scout® is accessed via a secure, pre-authorised, URL at fixed IP addresses; allowing users to login via a username and password - in addition to SSO and MFA, where requested. Once within the investigation console, users can search unlimited internal, third party or open-source data sets for information relating to: people; postal addresses; email addresses; commercial businesses; telephone numbers; and vehicles. Searches can be completed individually, on bulk via the spreadsheet uploader, or automated API.

Purposefully designed to increase the capacity and capability of teams, Scout® is a secure, real-time investigation platform that enables the user to automate the laborious, manual searching and re-searching of internal, third party or open-source data. Scout® reports can be retained within our auditable case management system (Scout® WorkBench) or the results can be exported into a pdf or spreadsheet. The data sources for all results are clearly attributed within the report. If sensitive data sources are used, these can separately be retained within a different report and form part of a sensitive unused schedule.

The abundance of data provides a real opportunity for users within strategic, operational and intelligence teams to make evidenced based decisions more swiftly. Whether you're looking to investigate more cases or make a more informed decisions, Scout® allows you to look under every stone in a fraction of the time.

Levels of Access

Access, Data Protection and System Security are paramount design features of the platform and its operational deployment. The system is capable of operating to Official Sensitive and is fully compliant with Data Protection, Criminal Procedure and Investigations Act 1996 (CPIA), Information Commissioners Office (ICO) and Information Security standards.

User and system access is provided at four levels:

Admin	Synalogik Administration & Helpdesk	Ability to reset passwords, unlock accounts, disable user access.
Super User	Investigator functionality with admin functionality.	Ability for investigators to also reset passwords & unlock accounts.
General User	Investigator / Analyst	Ability to use full functionality of Scout platform.
Audit	Professional Standards / Compliance	Ability to view user activity.

User Management

Scout® provides users with a platform to interrogate data sets rapidly and whilst it can be procured as a commercial-off-the-shelf capability, it has also been designed in a way that allows Synalogik to work with customers to identify and ingest additional data sets and complement existing in-house technologies to bring further efficiencies in the investigation process and to solve a wider range of user cases.

Individual users have the capability to: customise OSINT search 'wizards' for individual cases, create bespoke search templates into all our headline types of search and proactively monitor any changes to commercial entities in near real time.

User Reports

Custom activity report can be created detailing user activity and itemised searches on a monthly basis, if requested. This functionality is designed to aid organisations with compliance in respect of The Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Criminal Procedure and Investigations Act 1996, The Data Protection Act 2018 and The General Data Protection Regulation. Organisations trust Scout® to ensure their users are not only operating

lawfully, ethically and within the parameters of their role, but so that they can prove they are should the need arise.

Management Reports

Management Information reports are available showing usage of Scout®, thus enabling managers to identify any non-usage and respond accordingly. The reports can also help to identify training and tradecraft gaps and weaknesses, which can then be addressed in learning and development sessions – all of which are delivered by Synalogik as part of our commitment to best-in-class investigations and customer support.

Reporting consists of a monthly emailed "MI" report setting out the required information - names of users, API calls, and search inputs. If a particular instantiation has been deployed to Official Sensitive or above, the Synalogik team cannot gain access to this information and as such MI reporting is not available, however, it can be retrieved by internal users directly from the system.

Security

The Company operates to ISO 27001. Scout® is regularly PEN tested by Crest accredited third parties as part of this certification requirement.

The Synalogik team are vetted to NPPV Level 3 and have a minimum of SC Clearance. Many of the Professional Services team have heightened levels of clearance. Details of which can be provided upon application.

Synalogik also have Cyber Essentials Plus certification.

Professional Accreditations

1. ISO 27 001
2. Cyber Essentials Plus

Data Location

All Scout® Data is held in AWS Servers solely within the UK.

All system backups are retained within the UK.

All data is encrypted at rest and in transit.

Backup/Restore and Disaster Recovery

Synalogik has complete internal plans, processes and systems in place regarding business continuity and resilience of a client's unique data store.

Any specific requirements for backup, restoration and disaster recovery, where appropriate, would be discussed and agreed with the customer prior to an order being placed.

GDPR compliant investigations

Scout and DataHunter platforms interrogate the databases which our clients are lawfully entitled to access. Platform users are trained upon the system and each time they access it they agree to its terms of use, forming part of the auditable log of activity.

The system minimises volumes of personal data processed, by cleansing potential results prior to processing them into reports - this is done by filtering potential results by name spelling, date of birth and proximity.

Each platform is created with specific data retention periods put in place and replicating the Clients Data Protection needs.

Individual users can delete individual reports or OSint results if they prove to be false positives.

The platforms retain an auditable log of every search, data set interrogated, user details and results ensuring you can evidence every step of your data processing for non-punitive, civil or criminal enquiries.

Onboarding

User onboarding and training is available as part of minimum licence package arrangements or separately as requested.

Support Services

Synalogik operate a standard business hours UK-based support service providing telephone and email support. Typically, this is second line support working with the customer's local technical team, although other options are available as required. Support is included as part of the Scout® licence.

Support Helpdesk

Contact details for the service desk will be provided during the onboarding process, and users are encouraged to user either email or telephone to log questions, queries or requests for support

When logging a call by email the following information should be provided as a minimum, and sent to: helpdesk@synalogik.com

- Contact Name
- Contact Number
- Contact email
- Priority
- Username experiencing the issue
- Nature of the problem experienced
- Telephone number

Fault Priority

The Fault Management SLA specifies that faults will be assigned a priority, upon which the response to complete the diagnosis of the fault is as detailed by the Key Performance Indicator (KPI) for that category of fault.

For reference, the SLA categorises the different fault priorities as follows:

Priority	Description
Priority 1 (P1)	Scout® is inaccessible or unusable with the potential of causing critical impact to the customer's business operations if service is not restored quickly. The customer is willing to commit substantial resources around the clock to resolve the situation. For any Incident to be assigned Priority 1, the Customer must guarantee the necessary access & resource required to help diagnose and resolve the incident.
Priority 2 (P2)	Scout® is severely degraded, impacting significant aspects of the Customer's business operations. The Customer is willing to commit full-time resources during business hours to resolve the situation.
Priority 3 (P3)	Scout® performance is degraded. Functionality is noticeably impaired, but most business operations continue.
Priority 4 (P4)	The Customer needs information concerning product capabilities, installation advice, or the creation/deletion of users.

Service Level Agreements

Severity	Contact method	Response Time	Resolution Time	Customer Updates (email or phone)
Priority 1	Phone	1 working hour	24 hrs	Every 2 working hours
Priority 2	Phone / Email	2 working hours	48 hrs	Every 4 working hours
Priority 3	Phone / Email	4 working hours	3 working days	Every 8 working hours
Priority 4	Phone / Email	48 hrs	5 working days	Daily

Availability and Planned Maintenance

For a service of this nature, it is important that the solution is kept up to date with the latest patches released by Operating System and Software / Hardware vendors. In most cases this work will be carried out without disruption to the user, however, disruption may be unavoidable from time to time.

For this type of maintenance Synalogik will notify the customer 5 days in advance of any planned maintenance windows unless deemed critical to the security of the platform. Work will be completed outside of normal business hours e.g. 18:00hrs to 06:00hrs to minimise any impact this may have.

Training

Synalogik provide standard new user training packages. Further training can be customised to suit client need, including: SuperUser Training, Risk Assessment Training and Search Templates Training.

User Guides

- Online self-help portal - with search functionality for the user
- Business Hours Helpdesk - to answer any queries about the product
- 1 x 90-minute basic user session giving introduction to the functions and capability within the Scout® platform
- 1 x 30-minute extension to the 90-minute basic user session for super-users to deal with managing users' permissions
- Videos in the self-help portal, covering all aspects of the platform's functionality
- Regular user clinics hosted online on various new areas of functionality

Synalogik can also provide training on any aspect of intelligence, investigation or internet-based enquiries, including bespoke courses designed to your needs.

Proof of Concepts and Trials

Synalogik usually offer a new customers a complimentary 20-day trial of the core Scout® platform (for up to 5 Users) to demonstrate functionality and operational value. In advance of any trial, appropriate contracts for Data Protection purposes need to be agreed and signed.

Related Scout Products

Scout® Supporting Services

Scout® Training

Acceptable Use

The customer responsibilities include:

· Completing any whitelisting, firewall and security accreditations required for the use of the platform

· Data ownership / agreement with relevant third-party data providers, if required,

· Identify users and contact email addresses

· Ensuring user logins and passwords are kept secure are not shared

· Ensuring that users are appropriately available to be trained

· Ensuring appropriate Internet bandwidth is available

In addition to the Data Protection requirements of Scout®, when each user logs into Scout®, purchasing organisation shall adhere to the following acceptable use policy for the management of the licence software:

· Each Scout® licence is for a named individual and cannot be shared or used in a concurrent model

· Scout® licences can be revoked by the customer and re-issued to another user during the contract period

· You may not share, rent or lease Scout® access credentials to any other individual or entity, for any reason

· You may not sub-license Scout® access credentials to any other individual or entity, for any reason

· You may not issue our access credentials licences to any third party's that are not employed by your Organisation, without written authorisation from Synalogik Innovative Solutions Ltd.

Company Overview

Synalogik Innovative Solutions Ltd ("Synalogik") is a privately-owned company that was formed to deliver solutions, to both the public and private sectors, based around the process automation of data gathering, analysis, risk scoring and report writing for the intelligence and investigation communities

or indeed any role or department that complete the laborious manual researching of databases.

Founded in 2018, Synalogik was conceived with a specific objective: to undertake intelligence and investigations differently, to empower investigators to exploit data to prevent and detect non-compliant behaviour and criminality. As the volume of data available to investigators has continued to expand, Synalogik has continued to evolve our product offering to combat current tactics; every Synalogik customer gets the most updated version of Scout® at no extras cost, throughout the contract term.

Synalogik's proprietary intelligence and investigation platform Scout® is based in AWS, highly secure and operationally proven to lead to significant efficiencies in time and investigation success.

Scout® is the market leader in providing an automated Open-Source Intelligence & Investigation platform for HMG, law enforcement agencies and other public sector authorities.

Synalogik Innovative Solutions Ltd

Unit A, The Courtyard

Tewkesbury Business Park,

Tewksbury

United Kingdom

Company Registration number 11601168

For more information on the services we offer please consult our secure website at the following URL: WWW.SYNALOGIK.COM or email public.sector@synalogik.com