



# Splunk for Local Government Connect

Comprehensive compliance with the UK Government Connect Secure Extranet (GCSx) Log Management and Monitoring requirements.

## What is Government Connect?

According to the UK Information Commissioner's Office there were 176 recorded data breaches in the public sector in 2009. Within the government sector, the pressures on data security are more high profile, placing a greater burden on government agencies to ensure data security and protection.

The Government Connect Secure Extranet (GCSx) is a private Wide-Area Network (WAN) framework that has enabled secure interactions between connected Local Authorities and other governmental organisations. GCSx is part of the wider Government Secure Intranet (GSI) connecting to nearly all central departments:

- ▶ Government Secure Extranet (GSX)
- ▶ Government Secure Intranet (GSI)
- ▶ National Health Service (NHS)
- ▶ Criminal Justice Extranet (CJX)
- ▶ Police National Network (PNN)

Local authorities who connect through the infrastructure must adhere to information security controls defined by Code of Connection (CoCo) for the Government Secure Intranet (GSI) and GCSx (Memorandum Number 22).

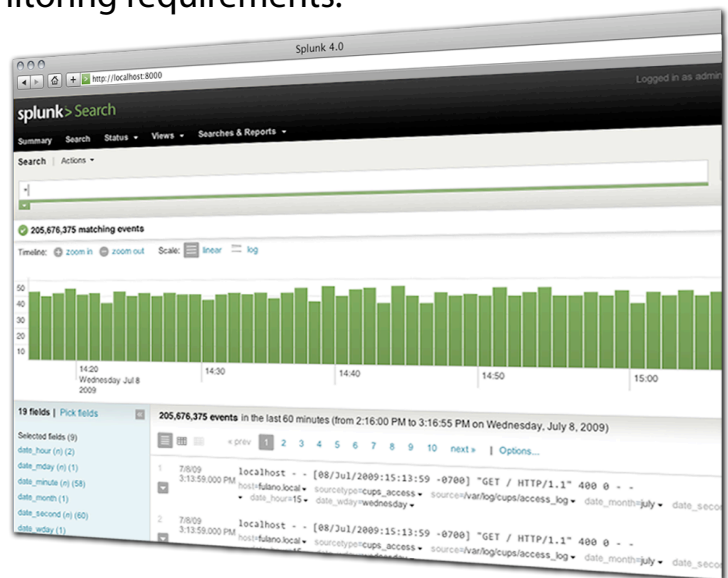
Local authorities failing to comply with CoCo will be unable to access the GCSx, hence, will be cut off from central information resources that are key to the delivery of effective public services.

## The Challenge of CoCo.

To gain the benefits of GCSx local authorities need to sign-up to the Code of Connection (CoCo) that stipulates the standards and processes an authority must comply with before being able to connect to GCSx. CoCo mandates require that organisations monitor, alert and report on their log and IT data.

There are many challenges with this. Logs and IT data is scattered across IT and is very difficult to access, manage and analyse. Manual methods are simply too slow and labour intensive to effectively comply, and the traditional technologies available are too complex: requiring custom connectivity, slow back-end databases and proprietary consoles to meet the specific requirements of CoCo.

With strict deadlines and stringent requirements for compliance, Local Authorities need highly scalable, simple-to-deploy and cost effective solutions to meet these requirements.



## Why Splunk?

The concept behind Splunk is simple, if Google can make it possible for users to search billions of pages of Web content, why not do that for the datacenter? Splunk is a search engine for IT data. The result of thinking differently, Splunk is software that lets you search and analyse all the data your IT infrastructure generates from a single location in real time. We call this IT Search.

No need for databases, connectors, custom parsers or proprietary consoles. With Splunk you can troubleshoot IT problems and investigate security incidents in minutes, not hours or days. Monitor all your applications, servers and network devices from one place. Report on all your compliance controls in a fraction of the time.

By making it possible for humans to interact with terabytes of IT data, Splunk fundamentally changes how organisations manage, secure and audit increasingly complex computing environments. Splunk arms network engineers, sys admins, security and compliance analysts, developers, help desk with an up-to-the-moment understanding of what's happening in their IT infrastructures.

## Customers Using Splunk for GCSx



## Requirements.

Splunk IT Search is the cost effective and flexible way to meet your CoCo compliance requirements from audit trail collection and reporting, to file integrity monitoring.

Featuring a single software solution, Splunk will let you monitor activity, alert on unauthorized or inadvertent change, and provide auditors with the reports they need to satisfy the mandates. In addition, the flexibility of Splunk IT Search will satisfy any ad-hoc reporting requests.

Splunk enables you to automate monitoring and reporting to meet the following CoCo Requirements.

Record the following user activity occurring on your network:

- ▶ Unauthorised application access
- ▶ File access attempts to protectively marked information
- ▶ Unsuccessful login / logout
- ▶ Successful login / logout
- ▶ Privileged system changes
- ▶ 6 month log retention
- ▶ General Requirement 21 - Log File Integrity
- ▶ General Requirement 22 - Log Retention
- ▶ General Requirement 23 - Audit Frequency
- ▶ General Requirement 24 - Vulnerability Assessment
- ▶ General Requirement 25 - Protective measures against threats
- ▶ Security Requirement (SR1) - Clock Synchronisation
- ▶ Security Requirement (SR2) - Unique Identification
- ▶ Security Requirement (SR3) - Reveal the Event Date/Time
- ▶ Security Requirement (SR4) - Identify Physical & Logical Address
- ▶ Security Requirement (SR5) - Identify Source & Destination
- ▶ Security Requirement (SR6) - Reveal the Type of Service
- ▶ Security Requirement (SR7) - Identify Privileged Command
- ▶ Execution & Security Requirement (SR8) - Identify Unauthorised
- ▶ Applications & Security Requirement (SR15) - Reveal Changes to any Executables or Configuration Files
- ▶ Security Requirement (SR13) - Reveal Untypical Gaps in Accounting Logs
- ▶ Subscription Process
- ▶ 4.5 Supply User Details
- ▶ 6.2 Re-Submit (annually) CoCo Statement of Compliance

## CoCo Requirements and Beyond ...

Most local authorities are aware of the need to secure and protect their critical systems and network from unauthorized access but there remains a large number of other systems, applications, and devices that are often unprotected or trail behind in security priority. Some of these fall outside of the direct realm of CoCo, with universal access to all IT data, Splunk can help fill these gaps.

Securing and compliance reporting on the IT infrastructure are only a part of the IT picture. Managing and monitoring performance, troubleshooting errors, delivering on service levels and doing more with less are now part of every IT organisations charter. Splunk delivers on these with the ability to detect anomalies before they result in downtime and track and trace errors to the root cause.

Splunk is also proactive, alerts can be set based on pre-determined thresholds triggering email alerts, RSS notifications, or scripts to open trouble tickets, or restart a server.

Splunk has capabilities well beyond CoCo compliance and the same instance of Splunk can be used across all of IT for a variety of use cases. Many of the Splunk CoCo customers are using Splunk in other areas such as:

- ▶ Digital Forensics
- ▶ Incident Investigations
- ▶ Application Troubleshooting
- ▶ Transaction Tracing
- ▶ Network Management
- ▶ Server Management
- ▶ Virtualisation Management
- ▶ Change Management
- ▶ PCI Compliance
- ▶ Business Intelligence

Evaluate Splunk for free today. You will be up and running in minutes and delivering value almost immediately.

### Free 60-day Enterprise Trial

Download and run Splunk with a free 60-day Enterprise Trial license. At 60 days upgrade to a full license or download a limited-use free license. <http://www.splunk.com/download>

### Get Started Today!

- Download Splunk today: [www.splunk.com/download](http://www.splunk.com/download)
- UK Office: **01628 509031**
- Email: [emea\\_sales@splunk.com](mailto:emea_sales@splunk.com)