

Data sheet G: Security Overview (Snap Hosted solution)

Information Sent From the Snap Client to the Snap Platform

- **Content-control data:** In order for the Snap Platform to determine whether new or updated content should be distributed to the user, the Snap Client transmits some basic control data that indicates to the Snap Platform what items of content have already been downloaded. This data uses a series of hash codes to represent this information.
- **Content-view results:** The Snap Client collects information about which items of content have been viewed by the user and at what time this occurred. Collectively, this information is known as "results", and is transmitted to the Snap Platform where it is used in aggregate form to create reports visible within the Snap Content Manager.
- **Basic diagnostic information:** Snap Client reports to the Snap Platform some basic information including: Snap Client version number, Windows operating system version number
- **Identity data:** Each instance of a user running the Snap Client has a unique identifier which identifies them to the Snap Platform. The unique identifier is randomly generated and assigned by the Snap Platform on first use, and is used in subsequent communications to identify the instance of the user.
- **Machine name:** The machine name is collected and is used by the Snap Platform to track multiple instances of users if users log on to more than one machine in the network. It is also for reporting purposes to determine the number of unique machines that have Snap Client installed. This information is not visible within the Snap Content Manager.
- **User & group information:** Information about the user of the Snap Client is obtained from Active Directory and sent to the Snap Platform where it is used for targeting purposes. The user's name is collected as well as the list of group names of all of the groups that the user belongs to.

Communications Security

All connections between the Snap Client and the Snap Platform are initiated by the Snap Client. All data is sent over a secure connection using HTTPS. The use of SSL ensures that all data/information sent between the Snap Client and the Snap Server is kept secure whilst in transit. Briefly, the use of SSL provides the following benefits:

- **Confidentiality:** because the communication is encrypted, it is not readable or otherwise intelligible to persons intercepting the traffic on the network
- **Integrity:** because the communication is encrypted, it is not possible for persons to intercept and modify the contents of the communication
- **Server Authentication:** the SSL certificate provides proof of the server's identity thus ensuring that communication only occurs if the server's domain name matches the name on the certificate.

Snap Platform Security

- All data is stored on server machines within SQL databases.
- Administrator-level access to the SQL databases and access to administrator-level accounts on the server machines is restricted to authorized Snap personnel only.
- The data on the server machines is protected by access-controls at the file-system level that restricts access to authorized Snap system administrators only.
- Access to Snap system administrator user accounts is controlled through the use of strong passwords that are changed regularly.
- Portions of the data held within the databases can be viewed and/or modified by users of the Snap Content Manager. Access to the Snap Content Manager is controlled through the use of a login requiring a user name and password.
- The server machines are located within a secure tier 1 internet data centre, with physical access restricted to authorized personnel only.

The server machines are located behind a firewall which restricts incoming and outgoing traffic to essential services only.