Security Considerations at dScribe

Introduction

At dScribe, we understand that the integrity and confidentiality of your data are critical to your business operations. This document outlines the security measures that dScribe has implemented to make sure your data is secure.

This document aims to provide a detailed overview of the security features that make dScribe a trusted and secure partner for your data documentation needs. We are dedicated to full transparency and continuous improvement in our security practices, ensuring that our solutions not just meet but exceed expectations in safeguarding their critical information assets.

For any security-related inquiries or concerns, please contact Simon Temmerman, the Chief Technology Officer (CTO) of dScribe.

Simon Temmerman
Let's talk dScribe booking page
Mobile +32 472 11 48 05
Web www.dscribedata.com
Email simon.temmerman@dscribedata.com
Voskenslaan 95a, 9000 Ghent, Belgium

Data security

dScribe browser plugin

The dScribe browser plugin is available from the official Microsoft Edge and Google Chrome add-on stores. In both cases, the plugins – and each update released for it – is vetted by Microsoft and Google before being made generally available.

When working with the browser plugin to document your reports or any other web page, no direct connection is established between dScribe and your source systems. The plugin operates strictly within your browser application and only has access to metadata available via the browser, including the URL and the HTML code of the web page you are on.

Concerning the functionality of AI-generated documentation via the browser plugin, see also the section on LLMs.

Metadata integrations

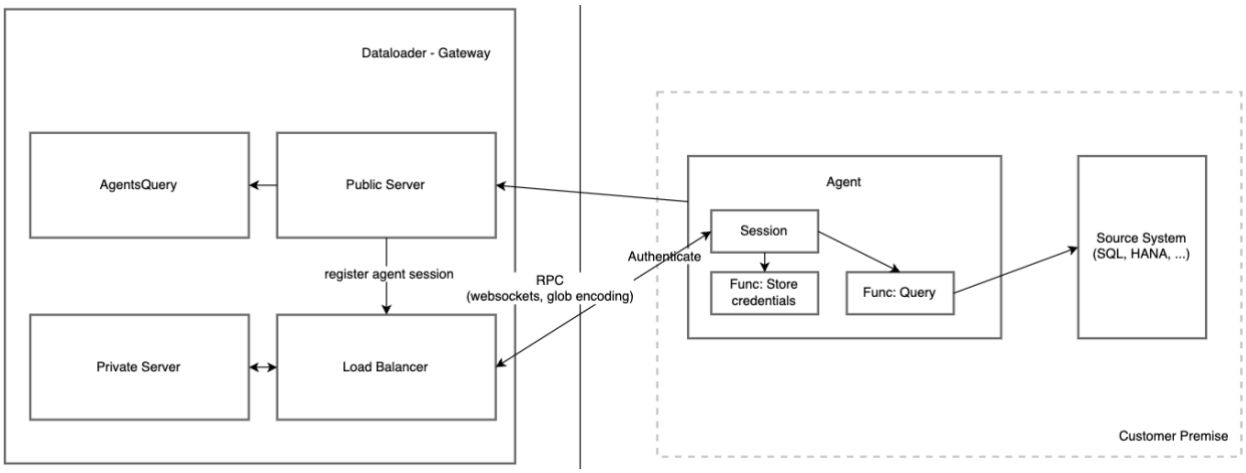
Cloud integrations

dScribe offers out-of-the-box integrations with many cloud sources. For a full list, including their setup details, see our documentation.

Private network integrations

The dScribe Agent can be installed when you want to set up metadata integrations between dScribe and sources protected within your organization's firewall.

The dScribe Agent is an important part of our data integration architecture, designed to operate securely within the customer's firewall. This piece of software, written in Go for its minimal dependency tree and better control over the running code, facilitates the operation of our data loader by crawling customer systems to collect metadata. To simplify deployment and minimize network configuration changes, the dScribe Agent is engineered to initiate outbound connections to our servers. This design makes sure the customer does not need to add firewall exceptions.



Other considerations

GDPR

Users have the right to access, amend, and request the deletion of their data from our systems at any time. To facilitate this, we provide a clear and accessible channel through which users can contact us to execute their data rights. Tickets can be logged via the application and questions can always be directed to support@dscribedata.com.

LLMs

We recognize the privacy concerns associated with using Large Language Models (LLMs) like OpenAI, especially regarding the handling of sensitive data. To address these concerns, we host our own LLM privately. This approach ensures that all data processing is confined within our controlled environment. Furthermore, all input data, such as screenshots used for generating documentation, are immediately removed from our systems after use, minimizing potential privacy risks.

Cypher injection

To prevent injection vulnerabilities, our approach is twofold: we avoid directly injecting values into cypher statements and ensure validation and sanitization of all input data. By implementing parameterized queries and prepared statements, we effectively segregate data from the code that manages it, thereby neutralizing the threat of injection.

Data Encryption

While the metadata we work with is not encrypted at rest, given its lower sensitivity, we ensure strong protection for more sensitive information. All critical data, including passwords, usernames, service principals, and keys used to set up integrations, are encrypted at rest.

Disaster recovery and backups

Our disaster recovery plan ensures resilience against the most common data incidents, including the main database going offline, secondary database failures, and accidental bulk data deletions. These protocols are designed to restore operations with minimal disruption, safeguarding your data integrity and availability. For a full overview of our disaster recovery strategies, please refer to our detailed Disaster Recovery Plan document.

Operational security

Operational security (OpSec) is the cornerstone of safeguarding our product and its underlying infrastructure from potential threats and vulnerabilities.

Dependency Management

To manage dependencies within our codebase effectively, we employ scanning protocols in our deployment pipelines to identify and mitigate vulnerabilities. Additionally, we maintain strict criteria for the use of open-source software, ensuring that only licenses with reputable standings are used in our system.

Infrastructure security

Azure infrastructure

dScribe Data utilizes Microsoft Azure to host our applications, leveraging Azure's well-established reputation for high security standards and compliance. Azure (and by some extent, dScribe as user of this platform) has achieved numerous certifications such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2.

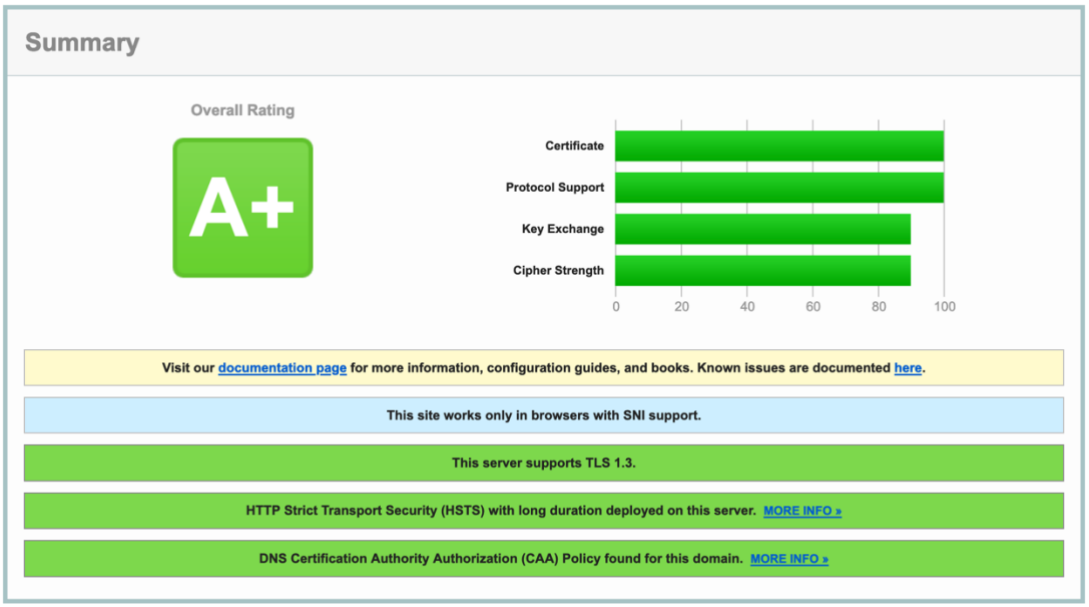
To bolster the security of sensitive information within our applications, dScribe employs tools that are made available to us on the Azure platform:

- Azure Key Vault. This tool ensures that critical data such as credentials and encryption keys are managed securely without being embedded in the application code or exposed to potential threats.
- Azure Private Link. This ensures that our network traffic is shielded from public internet exposure. Azure Private Link facilitates private access to Azure services, significantly reducing our exposure to threats by enabling direct, secure connections within Azure's private network.

DNS

HTTP Strict Transport Security (HSTS) is on the preload list. This ensures that all connections to our site are automatically upgraded to HTTPS, preventing any attackers from forcing connections over an insecure HTTP. Moreover, our HSTS policy extends to all subdomains, providing comprehensive protection across our entire domain structure.

In addition to these precautions, we have optimized our TLS cipher suites to ensure that they meet the highest security standards, consistently achieving an A+ rating from ssllabs.



Email

To ensure all emails sent in the name of dScribe are legitimate, we implement Domain-based Message Authentication, Reporting & Conformance (DMARC) with a quarantine policy. This protocol helps authenticate the emails sent from our domain, ensuring they have not been tampered with or spoofed. By setting DMARC to quarantine, we instruct receiving email servers to divert emails that fail DMARC checks to the spam or junk folder, rather than rejecting them outright.

Application security

Our application security strategy encompasses preventive measures, testing, and continuous monitoring to address vulnerabilities proactively and reactively.

XSS

Cross-Site Scripting (XSS) attacks pose a significant threat to web security, exploiting vulnerabilities that allow attackers to inject malicious scripts into web pages viewed by other users. We employ a Content Security Policy (CSP) to defend against these types of attacks. CSP is an effective security measure that helps detect and mitigate potential XSS vulnerabilities by specifying which dynamic resources are allowed to load, preventing the execution of unauthorized scripts.

Clickjacking

Clickjacking is a deceptive technique where an attacker tricks a user into clicking on something different from what the user perceives, potentially revealing confidential information or taking control of their computer. We mitigate this risk by implementing the X-Frame-Options HTTP

header across our web application. This security measure instructs browsers to not embed our pages within frames or iframes from other origins.

MIME confusion

MIME confusion attacks exploit discrepancies between declared and actual content types of transmitted data, allowing malicious content to be executed under misleading types. To combat this, dScribe Data implements the X-Content-Type-Options header with the "no sniff" directive across our web applications. This security measure prevents browsers from interpreting files based on their content if the content type does not match the declared MIME type.

User authentication and permissions

Enterprise Authentication (Single Sign-On)

By integrating OpenID, we provide you with a way to authenticate your users with their existing credentials from your company's Identity Provider (e.g. Azure Entra ID). This not only simplifies the login process but also centralizes access management for organizations. This approach allows users to access dScribe without the need to create and manage new passwords, thereby reducing the risk of password-related security breaches.

Direct user creation

Administrators can also invite new users directly on your dScribe environment. When using the direct login flow, a passwordless login flow is applied: users get a magic link sent to their inbox to authenticate themselves and log in, again reducing the risk of password-related security breaches.

Permissions management

dScribe allows for setting up very detailed access policies to give you full control over who can see or contribute to what knowledge entries stored in the knowledge hub. For more information on how to set this up, see our documentation.