SCRIBE ONLINE SECURITY

This document provides an overview of Scribe Online's Security.

SCRIBE ONLINE

Scribe Online is an Integration Platform as a service, allowing you to quickly and easily integrate any cloud or premise application you need. It includes a visual design studio to build integration flows between multiple endpoints, a management console to tend to the care and feeding of your integrations over their lifetime, and a set of developer toolkits which allow you to extend the platform to fit your needs.

Integration flows are executed by Scribe Online agents, which are either hosted in our Scribe Cloud or on a local machine inside your or your customer's network. This allows multiple options for Scribe customers to securely transfer data using the Scribe Integration Platform.

SCRIBE SOFTWARE SECURITY STATEMENT

Scribe is committed to our customer's data security and privacy. Our service employs secure agent technology which can be directly installed on the customer's hardware behind the customer's firewall. This agent is compiled code which prevents hacking or code injection. The secure agent communicates with Scribe Online via HTTPS to receive instructions or to send job status information. The customer does not need to open additional ports on the firewall.

Our connectors use the secure authentication method provided by the application vendor. Scribe Online customers use whichever authentication method and credentials to connect to these applications as supported by the application API. Generally speaking, the connections we make through the agent are as secure as the connection by a user to that application through the vendor's web client or other vendor provided interface.

Our agents communicate and transfer data directly between your business applications. That data transfer is encrypted. We do not send, store, or cache your business data in Scribe Online en route. The only data we store in Scribe Online are a) your organization and contact information that you provide to create an account in Scribe Online; b) integration process definitions and instructions; and c) job status and error messages. Further security features are discussed in a later section.

Our Online service is designed with security in mind and we employ operational best practices to monitor and secure our infrastructure. Our service runs on highly secure infrastructure platforms provided by Microsoft Azure and Amazon EC2. We employ an outside security firm to audit our service and infrastructure on a regular basis. Due to the sensitive nature of our security practices, we cannot share specifics of our audit reports or details of our security operations in our service or infrastructure.

SCRIBE ONLINE SECURITY FEATURES

Scribe Online User Model – Scribe Online employs a unique model to user security. The model requires a Scribe Online Admin user for a specific organization to invite other Scribe Online users into that one organization. Without that invitation, there can be no access to the organization details, both from the UI or from the API even by a Scribe employee.

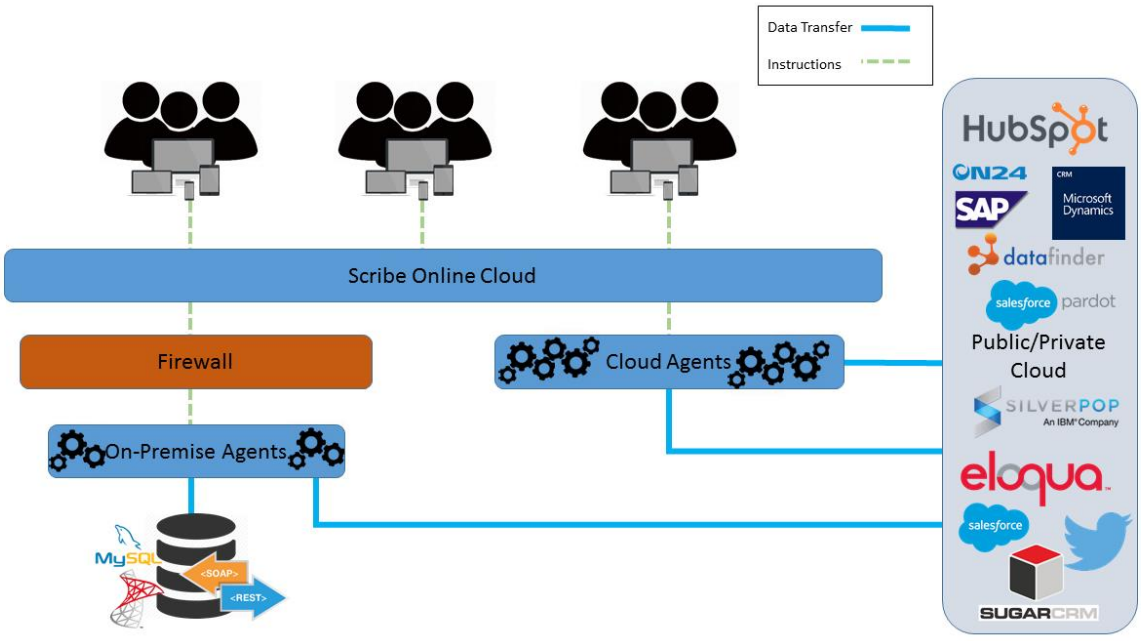
Scribe Online Data Retention - Scribe Online will store any and all error information for 45 days, after which that data is purged from the system. That data will include the error code and message, as well as a copy of the source data tied to that error for re-processing. If you would not like this stored in the Scribe Online, you can disable this feature by going to your security settings within the Scribe Online organization.

Scribe Online Agents – Scribe Online Agents, both on premise and cloud, are the mechanism by which integrations are run. They store a local instance of the integration mapping as compiled code. The credentials needed are also stored as an encrypted value in these Agents. When an Agent runs an integration, that data is processed only through that agent, never by the Scribe Online cloud. You can connect multiple cloud applications with a premise agent, and all that data will flow from the cloud app, down to your local agent, and out to the other cloud apps involved.

Scribe also allows for you to define your own security rules, where you can restrict access to your particular tenants' endpoint (for both Event Based Integration as well as API access) to a defined IP range. You are in control of this from within the Scribe Online UI, and can have separate approved zones for both the API and Event endpoints.

Scribe Online Endpoints – Scribe provides REST Endpoints which allow for integration flows to be triggered from other systems. These are hosted by Scribe, and provide a secure relay for communication with Scribe Agents. These Endpoints adhere to the same security rules as described above.

SCRIBE ONLINE DIAGRAM



FAQ

ENCRYPTION

Is your solution's client authentication communication encrypted? If so, what type of encryption does it use?

Yes. Scribe Online uses a standard web browser as a client, and authentication communications are encrypted with the HTTPS (SSL) protocol.

Are the data transferred between the client and the application encrypted (please describe the algorithms used)?

Yes. All communication between the web browser client and the Scribe Online servers in the cloud are encrypted using HTTPS.

Are the data encrypted when stored (please describe the algorithms used)?

Passwords are stored in encrypted form, primarily using Microsoft's AES Managed symmetric algorithm. We have additional layers of encryption using other algorithms that vary depending on the storage location which we could discuss if needed. Other data such as map definitions and execution history is not encrypted when stored.

What security compliances do you adhere to?

The Scribe Online cloud runs in Microsoft Azure, which provides our access to the design and management studio of the product. The way the Scribe Online agent architecture is built, if security is a concern you can run the data via a local agent, in which case none of your data is processed via the Scribe cloud. If you do decide to use a cloud agent, they are hosted in Amazon AWS on Scribe run and managed virtual machines. Because we run on both Azure and Amazon, we can pass through those security compliance protocols to our customers, and both can be seen using the following links: Azure | Amazon

AUTHENTICATION

What type(s) of authentication method(s) does your solution use to authenticate users?

Scribe Online authenticates its users using Microsoft's ASP.NET Membership provider. We use the option to store passwords only as hash codes. Additionally our application provides access to third-party applications that use a wide assortment of authentication methods. We would be happy to discuss further if needed.

What type of user access control is supported?

Scribe Online supports individual user access control, and each user account can be associated with one or more organizations. There are two permission levels, administrator and user, and an account can have different permissions in different organizations.

MISCELLANEOUS

Does the solution or application require that it be hosted on-premises or off-premises?

Scribe Online provides a cloud-based environment for managing connections, defining integration maps, scheduling jobs and monitoring results. It uses an agent to perform the actual integration work which is either deployed in Scribe's cloud or on premise.

Where is the scribe data center?

Our cloud is hosted on Microsoft Azure. Our cloud agents are hosted on Amazon EC2. On-premise agents are installed at customer sites at the customer's discretion.

When using an online agent syncing data between two online applications, where will that data reside?

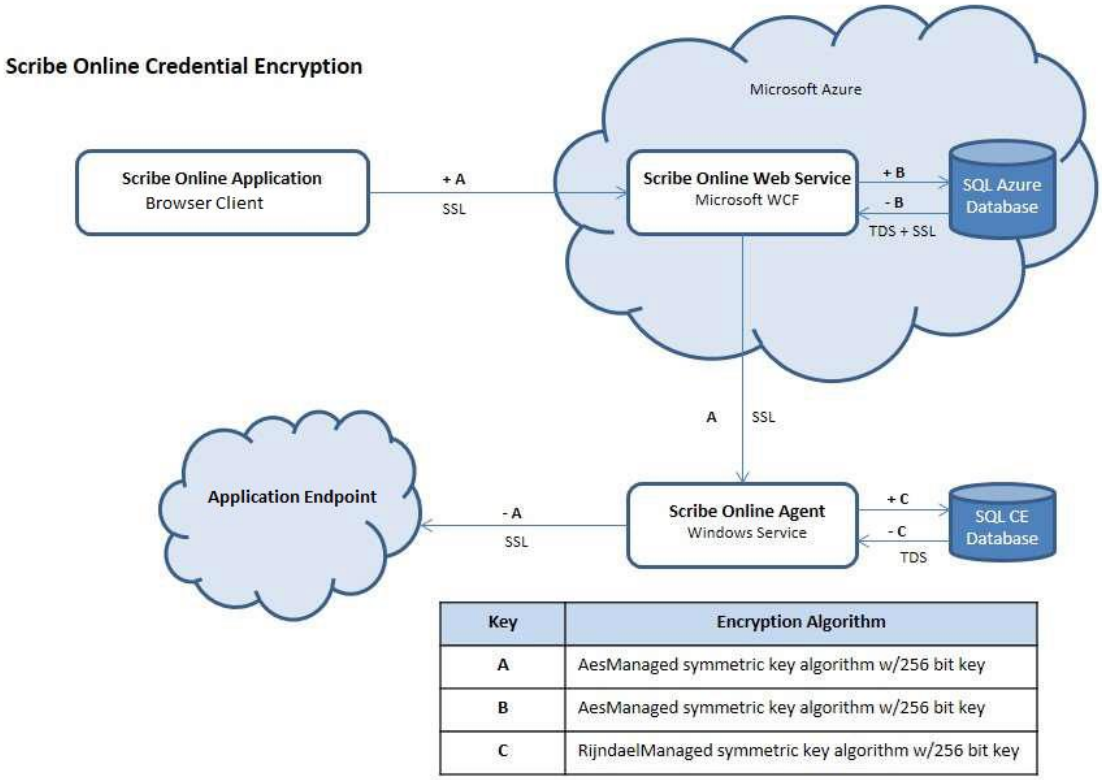
When a Scribe Online agent is processing data, that data is not persisted to the agent nor to our cloud database with one exception. If in trying to write data to the target connection the data fails to process, for example due to violation of some constraint in the target system, that row of data from the source is optionally persisted to our cloud database in an encrypted failed rows table.

How are credentials stored securely?

Connection credentials are used in three circumstances: A) when testing a connection, B) when saving connections to our cloud database, and C) when processing data when an agent is running a solution instance.

- When a user tests a connection, the credentials are passed to the agent using SSL encryption and those credentials are not persisted. (See A in diagram.) We also add a basic level of encryption to the password so that even in test and development environments passwords are never transmitted as plain text.
- When a user saves a connection, credentials are persisted in our cloud database using an AES algorithm and a 256 bit key. The implementation of the AES algorithm uses standard .NET code and follows the best practices for this type of encryption. The key is generated using a .NET library method, again following standard .NET code best practices. (See B in diagram.)
- When a user has completed their integration configuration in our UI, they save what we call a solution instance. Before the credentials in the solution instance can be used they must be decrypted, transmitted, and then encrypted and stored in the local database used by the Scribe Online agent. This encryption is done using an AES algorithm (different then when saving connections to our cloud database) and a 256 bit key which is never persisted on the agent. The agent requests the encryption key via an SSL-encrypted

web service call whenever it needs to perform encryption or decryption. (See C in diagram.)



Key	Encryption Algorithm
A	AesManaged symmetric key algorithm w/256 bit key
B	AesManaged symmetric key algorithm w/256 bit key
C	RijndaelManaged symmetric key algorithm w/256 bit key

What Ports need to be open on our firewall for an OnPemise Agent to work properly?

Scribe Online makes use of the Azure Service Bus. So a firewall need to be configured to allow the following:

- Outgoing TCP communication on TCP ports 9350 to 9355
- Outbound HTTPS connection to Port 443
- HTTP connection to Port 80, are required to allow a connection

Additional information about this topic can be found in the following page the help file.

How do your Cloud Agents communicate?

Scribe Online's Cloud Agents are hosted in Amazon AWS. They communicate over two IP addresses, so you only need to whitelist those two (52.6.65.166, 52.21.2.156) in order to allow secure communication from our Cloud Agents to your systems.

What are the System Requirements for OnPremise Agents?

The requirements can be found in our Online Help file topic On-Premise Agent Requirements