Conga Sign Security

Conga Sign is a new, easy-to-use modern eSignature solution built for Salesforce.

All interactions between the Conga Sign service and your Salesforce account are managed exclusively by you through your Salesforce administration and security settings.

The Conga Sign service is hosted with Amazon Web Services (AWS) available in the continental United States, EMEA, and APAC which are mirrored across multiple geographically dispersed data centers for fault tolerance and business continuity purposes.

Conga Infrastructure

Conga controls access to the infrastructure that Conga utilizes to process customer data submitted to the Conga Sign service. Firewalls and other boundary devices are employed to enforce strict control of the system accessibility. Security patches and system updates are regularly performed on all servers and other infrastructure equipment. The underlying infrastructure of the Conga Service is maintained within the Virtual Private Cloud infrastructure of Amazon Web Services as a subservice organization.

Data flow

Documents begin within the customer's Salesforce Org. The processing between a Salesforce customer and a 3rd party is managed via a secured signing portal and email process.

User Encryption for External Connections:

TLS encryption technology is utilized for data transfer between all parties involved in the process. TLS connections are negotiated for at least 256-bit encryption or stronger. The private key used to generate the cipher key is at least 2048 bits. It is recommended that the latest available browsers approved by Salesforce, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to the Conga Service.

Network Access Control

All access to the AWS environments is through a segregated network connection, isolated from Conga's internal corporate network traffic and requires two-factor authentication. Industry accepted security processes designed to ensure that only approved operations and support engineers have access to the systems. Remote access to the environment is restricted to select operations staff and only available via two-factor authentication.

Network Bandwidth and Latency

Conga relies on the AWS network infrastructure to provide low latency network availability between Conga, Salesforce, and end users. The AWS Cloud infrastructure is built around Regions and Availability Zones ("AZs"). A Region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities. These Availability Zones offer you the ability to operate production applications and databases which are more highly available, fault-tolerant, and scalable than would be possible from a single data center. Conga monitors applicable networks and will work to address internal issues that may impact availability. Encryption Gateways and Associated Third Party Technologies that requires any re-direction of Conga-to-Salesforce connections are not currently compatible with the service.

Anti-Malware Controls

Conga leverages enterprise-class solutions employed on all servers to protect against virus and malware incidents. Signatures for anti-malware are updated in a near real-time process as soon as they are available from the applicable vendors.

Firewalls / Intrusion Prevention

Conga Services utilize firewalls to control access between the Internet and Conga Services by allowing only authorized traffic. Conga managed firewalls are deployed in a layered approach to perform packet inspection with security policies configured to filter packets based on protocol, port, source, and destination IP address, as appropriate, to identify authorized sources, destinations, and traffic types. In addition to perimeter firewalls at the Internet boundary, host-based Intrusion Prevention systems are employed at the server layer.

System Hardening / Monitoring

Conga employs standardized system hardening practices across Conga devices. This includes restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, and logging. Additionally, Conga employs an Enterprise Class vulnerability management program to monitor and alert on any non-authorized changes or security configurations.

System Access Control and Password Management

Authentication and authorization are managed via an OAuth flow utilizing a Salesforce, integration user. When the service is configured in a customer's Salesforce instance, the administrator will connect the application using this integration user which will provide API access for Conga Sign to fetch and update relevant data and documents using an OAuth token. This token prefaces a Conga service's interaction with Salesforce, and the service runs under the authority of that individual Salesforce user as defined by the customer's Salesforce administrator. The customer is responsible for all end-user administration within the program via salesforce.com. Conga does not manage the Customer's End-User accounts within Salesforce. Customer may configure additional built-in security features within Salesforce.

Data Management/Protection

Signed and unsigned documents are encrypted at rest utilizing a dedicated key via AWS KMS leveraging the 256-bit Advanced Encryption Standard (AES) algorithm in Galois/Counter Mode (GCM), known as AES-GCM. Conga maintains security incident management policies and procedures. Conga promptly notifies impacted customers of any actual or reasonably suspected unauthorized disclosure of their respective Customer Data by Conga or its agents of which Conga becomes aware to the extent permitted by law. All Conga systems used in the provision of the Conga Services, including AWS infrastructure components and operating systems, log information to their respective system log facility or a centralized Syslog server (for network systems) to enable security reviews and analysis.

Physical Security

AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff. Video surveillance, intrusion detection systems are in place at a minimum of all ingress and egress points. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Scalability

Conga Sign is designed to leverage the benefits of a "cloud architecture" which includes the capability to scale compute, memory and network resources to meet the demands of our customers. Conga uses AWS Auto Scaling to maintain application availability and scale our capacity up or down automatically according to demand. Auto Scaling allows Conga to increase the number of processing instances during demand spikes to maintain performance.

Conga Americas Global Headquarters
390 Interlocken Crescent
Suite 500
Broomfield, Colorado 80021
+1.303.465.1616

Conga EMEA London
3rd Floor
60-62 Margaret Street
London W1W8TF
+44 (0) 203 608 0165

Conga APAC Pty Ltd
Level 11
68 York Street
Sydney NSW 2000
+61 2 8417 2399

Emergency Management Standards

Conga leverages the AWS capabilities by balancing the architecture components between two Availability Zones to keep the system operational, even if one Availability Zone stops working. In the case of an Availability Zone failure, the DNS is configured to seamlessly exclude the unhealthy services from the pool of available services and redirect the traffic to the operational Availability Zone. To cover the increase of traffic in the new zone, the automatic scalability process will begin creating the extra resources needed to keep the service at an acceptable response level. When the original Availability Zone is back online, the Conga team follows a standard procedure to reverse this process so that the traffic will start flowing again into the original data center. This process is tested on an ongoing basis as a means to update systems and other maintenance activities and is seamless and transparent to end users.

Digital Signatures

The digital signatures are affixed using a key signed by a CA on the AATL (Adobe Approved Trust List) which provides a high level of trust. The signatures are timestamped by a TSA (Time Stamping Authority https://en.wikipedia.org/wiki/Trusted_timestamping) and LTV (Long Term Validation https://en.wikipedia.org/wiki/PAdES) enabled and thus are suitable for long-term archival.

Office Disruptions

Conga maintains a globally diverse operations staff in the event core offices have any significant disruption. Additionally, all Conga employees have laptops and a secure process to access necessary resources to support infrastructure and customers.

Audits and Certifications:

The following security and privacy-related audits and certifications apply:

Conga Sign complies with the Electronic Records and Signatures in Commerce Act (ESIGN 15 U.S.C. Chapter 96), eIDAS (910/2014/EC), and Uniform Electronic Transactions Act (UETA).

- EU/US and Swiss/US Privacy Shield: Customer Data submitted to the Conga Services from the EU to the US, is within the scope of the annual Privacy Shield Program administered by the U.S Department of Commerce. The current certification is available at https://www.privacyshield.gov/list.
- TRUSTe Privacy Seal: Conga has been awarded the TRUSTe Privacy Seal signifying that Conga's Web Site Privacy Statement and associated practices related to the Conga Services have been reviewed by TRUSTe for compliance with TRUSTe's program requirements including transparency, accountability, and choice regarding the collection and use of personal data. Additionally, the Conga Services undergo security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis and available under MSA or MNDA.

Conga Americas Global Headquarters
390 Interlocken Crescent
Suite 500
Broomfield, Colorado 80021
+1.303.465.1616

Conga EMEA London
3rd Floor
60-62 Margaret Street
London W1W8TF
+44 (0) 203 608 0165

Conga APAC Pty Ltd
Level 11
68 York Street
Sydney NSW 2000
+61 2 8417 2399