SECURITY DATA SHEET

Conga Quote Generation for Salesforce CPQ & Conga Invoice Generation for Salesforce Billing

Security, privacy, and architecture

Services overview

Conga Quote Generation for Salesforce CPQ and Conga Invoice Generation for Salesforce Billing supplement native Salesforce CPQ and Billing to improve quote template authoring and generation. They feature: easier administration, improved support for larger documents, the ability to store documents as files, and a robust API.

You maintain exclusive control over all access and interactions between your Salesforce account, your Salesforce CPQ and/or Billing users, and the Conga service through your Salesforce administration and security settings.

Conga infrastructure

The services are regionally hosted with Amazon Web Services (AWS), available in the continental United States, within Europe, or Australia. Each region is mirrored across multiple, geographically dispersed data centers for fault tolerance and business continuity within the region the service is set to use. Customers may select specific regional processing locations upon implementation or by submitting a support ticket at support.getconga.com/Reference/Contact_Support.

Encryption for external connections

Customer access to the Conga service takes place via the Internet, and only after the authorized end user is properly authenticated. Conga service access requires TLS encryption technology. 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.com be utilized for connecting to the Conga service, as they are compatible with higher cipher strengths and have improved security.

Network access control

A limited number of Conga operations team members are granted access to customer environments, and then only after the completion of a successful background check, awareness and acknowledgment of privacy and confidentiality agreements, and security training. Access occurs through a multi-factor VPN or Private Proxy connection. Additional authentication, authorization, and accounting are implemented through standard security mechanisms. These measures are 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. 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, and 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 addresses internal issues that may impact availability.

Anti-virus and anti-malware controls

Conga leverages best in class tools in order to monitor and block virus and malware behavior. This includes protection against emerging threats beyond traditional, signature based solutions.

Firewalls and intrusion prevention

Conga utilizes firewalls as one component of a layered approach to application infrastructure security. To control access and allow only authorized traffic to Conga infrastructure, managed firewalls are used. In addition, Conga employs security policies to manage ingress and egress of data based upon protocol, port, source and destination within the environment. Any traffic not adhering to these strict access controls is discarded at the Internet boundary. Internally host-based intrusion prevention and monitoring systems are deployed at the server and network layers, respectively.

System hardening and monitoring

Conga employs standardized system hardening practices across Conga-managed 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.

Services undergo 3rd party penetration tests on an annual basis or prior to release of a material change.

Account provisioning and access control

When a Salesforce user launches a Conga routine, the user's Salesforce OAuth token is passed to the specified Conga service in a TLS-encrypted connection, together with other query string parameters for data, template(s) and output behavior. The OAuth token is a temporary token that identifies the user who generated it (via their login to Salesforce) and grants access to Salesforce under that user's authority. 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 via salesforce.com. Conga does not manage the customer's end user accounts within salesforce.com.

Conga employee access to the service is limited to what is required for support and maintenance purposes. Employee access is contingent on a successful background check, confidentiality agreements, and documented authorization by an engineering VP or above. Access for approved employees is strictly controlled via VPN and other authentication mechanisms.

Data management and protection

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.

Conga services do not maintain customer data post-processing except for templates. All templates will be disposed of upon termination of services or at customer's request. Data will be disposed of in a manner designed to ensure that they cannot reasonably be accessed or read. The only exception is if there is a legal obligation imposed on Conga which prevents it from deleting all or part of the environments or data.

The information customers provide during their use of Conga services that pertains to other individuals and entities is not collected or used by Conga, and remains under the ownership of Conga's customers. Conga processes customer data under the direction of its customers and has no direct control or ownership of the personal data it processes. Customers are responsible for complying with any regulations or laws that require providing notice, disclosure, and/or obtaining consent prior to transferring the data to Conga for processing purposes.

Incident response

Conga has a rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of systems or data. If an incident occurs, the security team logs and prioritizes it according to its severity. Events that directly impact customers are assigned the highest priority. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. Key staff are trained in forensics and handling evidence in preparation for an event, including the use of third-party and proprietary tools. To help ensure the

swift resolution of security incidents, the Conga security team is available 24/7 to all employees. If an incident involves customer data, Conga will inform the customer and support investigative efforts via our security team.

Physical security

Processing occurs within AWS data centers that are housed in nondescript facilities. Professional security staff strictly control physical access both at the perimeter and at building ingress points.

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, are signed in, and are continually escorted by authorized staff.

Scalability

Conga services are designed to leverage the benefits of a cloud architecture. This ensures 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 to scale our capacity up or down automatically, according to demand. With Auto Scaling, Conga can increase the number of processing instances during demand spikes to maintain performance.

Availability and disaster recovery

Conga maintains geographically diverse data centers and leverages the near seamless failover technologies from AWS. The people, processes, and technology necessary to conduct our business are distributed among these sites, with critical business operations conducted at multiple globally diverse locations. If activity at any one of these sites is disrupted, our systems are designed to continue operating at the other locations without serious interruption for customers.

Available data centers are built in clusters in various regions. All data centers are online and serving customers. No data center is "cold." In the case of failure, automated processes move customer data traffic away from the affected area. Each availability zone is designed as an independent failure zone.

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.

Conga audits and certifications

Conga is committed to achieving and maintaining the trust and confidence of our customers. Integral to this mission is Conga's dedicated, in-house security and privacy team. This team is tasked with enabling Conga customers to meet a multitude of compliance, data protection, and regulatory obligations from around the globe. Conga's trust and assurance activities include:

- Conga certifies to the U.S. Department of Commerce that it adheres to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. Conga's current certification is available at privacyshield.gov/list.
- Data Processing Addendums or Agreements including the Standard Contractual Clauses as approved by the European Commission and incorporating stringent requirements of Article 28 of the EU General Data Protection Regulation 2016/679.
- Service Organization Control (SOC) reports: Conga's information security control environment undergoes an independent evaluation annually. Conga's most recent SOC 2, Type II report covering security, availability, and confidentiality is available upon request.
- Penetration testing conducted by industry-recognized 3rd party on material environment changes or annually.
- Conga only utilizes infrastructure partners demonstrating the ability to meet rigorous standards (ISO 27001, SOC 2).
- Conga is ISO 27001 and ISO 27701 certified.

For More Information
Email info@conga.com or call your local Conga office to talk to a Conga advisor.

Corporate Headquarters
13699 Via Varra
Broomfield, CO 80020
+1 303.465.1616
conga.com

Global Offices
APAC: +61 2 8417 2399
EMEA: +44 (0) 203 608 0165