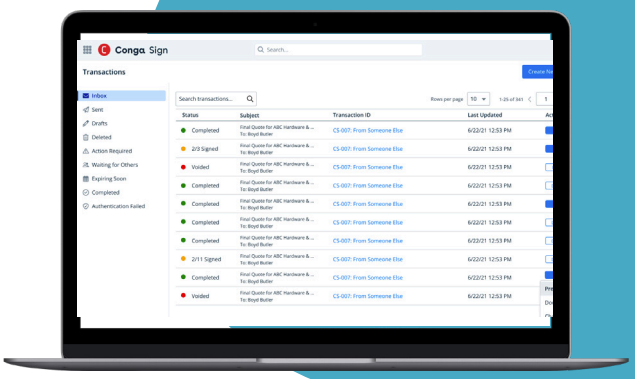
SECURITY SHEET



Conga Sign

Security, privacy, and architecture

Services overview

Conga Sign is a modern eSignature application built to efficiently execute your digital documents. With Conga Sign, you can securely and easily add eSignature capability to your existing revenue management solutions.

Conga infrastructure

The Conga Sign service is regionally hosted with high availability using Amazon Web Services (AWS), with data processing centers in North America. Conga's services run in logical groups of servers called site groups. Each Conga site group contains multiple, geographically dispersed data centers for fault tolerance and business continuity within the site group or, an appropriate disaster recovery plan with active service status monitoring. Customers that wish to run in a dedicated site group can submit a support ticket at our Conga Support page.

Encryption for external connections

TLS encryption technology is utilized for data transfer between all parties involved in the eSignature 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's recommended to use the latest browser versions approved by Conga for connecting to Conga services as they are compatible with higher cipher strengths and have improved security.

Network access control

A limited number of Conga's operations team members are granted access to customer environments, - only after the completion of a successful background check, awareness and acknowledgment of privacy and confidentiality agreements, and security training. Select vendor operations team members are granted access to customer environments in a comparable manner and are subject to Conga's operating standards when assisting in support of Conga services. Access to any customer environment infrastructure requires a multi-factor, SSO session. 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.

This access is revoked when no longer needed, and the approved access list is reviewed quarterly. 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, any subprocessor services, and our end users. The AWS Cloud infrastructure is built around regions, site groups, and availability zones. A site group is a logical group of data processing centers, typically distributed across multiple regions. 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 are housed in separate facilities. These availability zones offer you the ability to operate in production applications and databases that are more highly available, more fault tolerant, and more 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. Managed firewalls are used to control access and allow only authorized traffic to Conga infrastructure. 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. Internal 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 send alerts 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

The customer is responsible for end-user administration within the Conga Admin portal, and within any integrated applications or platforms that are connected to the Conga platform. Conga does not manage the customer's end-user accounts within integrated applications or platforms.

Authentication and authorization for Conga Sign services are managed by a secure, Conga-issued JSON Web Token (JWT). All requests made to Conga Sign are authenticated and validated using this JWT system. Web based requests are protected by a best-in-class web application firewall and other standard protections.

Conga employees' 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 a multi-factor SSO authentication mechanism. Select vendor operations team members are granted access to

customer environments in a comparable manner and are subject to Conga's operating standards when assisting in support of Conga services. This access is revoked when no longer needed, and the approved access list is reviewed quarterly.

Data management and protection

All Conga systems used in providing Conga services, including cloud infrastructure components and applications, log information to their respective system log facility and/or to a centralized Conga logging facility to enable security reviews, analysis, and support.

Post termination, data will be disposed of in a manner designed to ensure that it cannot reasonably be accessed or read. The only exception is if there is a legal obligation imposed on Conga which prevents deleting all or part of the environments or data.

The information customers provide during their use of Conga Sign services that pertain to other individuals and entities may be collected by Conga and is only used by Conga for support purposes. This data remains under the ownership of Conga's customers and can be deleted upon request. Conga processes customer data under the direction of its customers and has no direct 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. This data is encrypted in transit leveraging Transport Layer Security (TLS) protocols. This data is encrypted at rest leveraging AWS S3 encryption keys using the 256-bit Advanced Encryption Standard (AES) algorithm in Galois/ Counter Mode (GCM), known as AES-GCM.

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, it's logged and prioritized according to its severity by the security team. 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 of an event, including the use of 3rd 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 or Microsoft Azure data centers where physical security is strictly enforced through a variety of means.

- AWS data center physical security policies
- Microsoft Azure data center physical security policies

Scalability

Conga services are designed to leverage the benefits of cloud architecture. This includes the capability to scale Conga's compute, memory, and network resources to meet the demands of our customers. Conga uses auto scaling technology to maintain application availability and 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 lowest-latency active/active architecture and near seamless failover technologies from our cloud hosting providers. 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 to customers.

Available data centers are built in clusters in various regions and site groups. All data centers are online and serve customers. In the case of failure, automated processes move customer data traffic away from the affected area.

Office disruptions

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

Digital signatures

Digital signatures are affixed to documents using a key signed by a Certificate Authority on the Adobe Approved Trust List (AATL) which provides a high level of trust. The signatures are time stamped by a Time Stamping Authority (TSA) and are enabled for Long Term Validation (LTV), and thus are suitable for long-term archival.

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 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 Sign complies with the Electronic Records and Signatures in Commerce Act (ESIGN 15 U.S.C. Chapter 96), eIDAS (910/2014/EC), and the Uniform Electronic Transactions Act (UETA).
- 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 is ISO 27001 certified.
- HIPAA: Conga Sign Business Associate Agreements (BAAs) for Sign.