Security, Privacy and Architecture of B2B Commerce

Published: May 7, 2021

Salesforce's Corporate Trust Commitment

Salesforce is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including protection of Customer Data as defined in Salesforce's Master Subscription Agreement.

Services Covered

This documentation describes the architecture of the security- and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to, Version 3.97 (Release 3.8) or higher of the services branded as B2B Commerce (the "B2B Commerce Services") (formerly branded as CloudCraze).

Architecture and Data Segregation

The B2B Commerce Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. The specific infrastructure used to host Customer Data is described in the "Infrastructure and Sub-processors" documentation available here.

Control of Processing

Salesforce has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Salesforce and its sub-processors. In particular, Salesforce and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by Salesforce and its sub-processors are subject to regular audits. The "Infrastructure and Sub-processors" documentation describes the sub-processors and certain other entities material to Salesforce's provision of the B2B Commerce Services.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to the B2B Commerce Services:

- **Payment Card Industry (PCI)**: For the B2B Commerce Services, Salesforce has obtained a signed Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry Data Security Standard (DSS), as formulated by The Payment Card Industry Security Standards Council ("PCI DSS"). A copy of Salesforce's AoC is available upon request from your organization's Salesforce account executive. B2B Commerce enables customers to accept credit card payments via a third party using an iframe. B2B Commerce does not store, process, or transmit cardholder data.
- **ISO 27001/27017/27018 certification**: Salesforce operates an information security management system (ISMS) for the Covered Services in accordance with the ISO 27001 international standard

and aligned to ISO 27017 and ISO 27018. The Salesforce ISO 27001/27017/27018 Certificate and Statement of Applicability are available upon request from your organization's Salesforce account executive.

- **System and Organization Controls (SOC) reports**: Salesforce's information security control environment applicable to the Covered Services undergoes an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402), SOC 2 and SOC 3 audits. Salesforce's most recent SOC 1 (SSAE 18 / ISAE 3402) and SOC 2 reports are available upon request from your organization's Salesforce Account Executive or the Salesforce Compliance Portal.
- **EU-U.S. and Swiss-U.S. Privacy Shield certification**: Customer Data submitted to the B2B Commerce Services is within the scope of an annual certification to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as administered by the U.S. Department of Commerce, as further described in our Privacy Shield Notice. The current certification is available at https://www.privacyshield.gov/list by searching under "Salesforce.
- **EU and UK Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the B2B Commerce Services is within the scope of the Salesforce EU and UK BCR for Processors. The most current versions of the Salesforce EU and UK BCR for Processors are available on Salesforce's website, currently located at https://www.salesforce.com/company/privacy/.
- **APEC Privacy Recognition for Processors (PRP)**: Customer Data submitted to the B2B Commerce Services is within the scope of Salesforce's PRP certification under the APEC Privacy Framework. The current certification is published in the PRP Compliance Directory at http://cbprs.org/compliance-directory/prp/.

B2B Commerce is hosted on the Salesforce Platform (also branded as Force.com). For information on security and privacy related audits and certifications received by the Salesforce Platform, including ISO 27001 and Service Organization Control (SOC) reports, please see the Salesforce Services Security, Privacy and Architecture Documentation.

Certain customers may have the option to subscribe to B2B Commerce Services hosted on the infrastructure of a public cloud provider ("Public Cloud Infrastructure"). This infrastructure is described in the "Infrastructure and Sub-processors" documentation. For customers who elect Public Cloud Infrastructure, this will mean the underlying physical infrastructure on which your Customer Data is stored will be with a public cloud provider for what is commonly referred to as Infrastructure as a Service, and the B2B Commerce Services will run on top of the public cloud provider. Unless otherwise noted in this documentation, customers who choose Public Cloud Infrastructure will receive the same services, software functionality and operational processes as described here.

Additionally, the B2B Commerce 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.

Security Policies and Procedures

The B2B Commerce Services are operated in accordance with the following policies and procedures to enhance security:

- Customer passwords are stored using a one-way salted hash.
- Passwords are not logged.
- Salesforce personnel will not set a defined password for a user. Passwords are reset to a random value (which must be changed on first use) and delivered automatically via email to the requesting user.

- User access log entries will be maintained, containing date, time, user ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address. Note that source IP address might not be available if NAT (Network Address Translation) or PAT (Port Address Translation) is used by Customer or its ISP.
- If there is suspicion of inappropriate access, Salesforce can provide customers log entry records and/or analysis of such records to assist in forensic analysis when available. This service will be provided to customers on a time and materials basis.
- Data center physical access logs, system infrastructure logs, and application logs will be kept for a minimum of 90 days. Logs will be kept in a secure area to prevent tampering.
- Certain administrative changes to the B2B Commerce Services (such as password changes and adding custom fields) are tracked in an area known as the “Setup Audit Trail” and are available for viewing by a customer’s system administrator. Customers may download and store this data locally.
- Multi-Factor Authentication and Single Sign-On for access to the B2B Commerce Services as set forth in the applicable Notices and License Information (NLI).

Intrusion Detection

Salesforce, or an authorized independent third party, will monitor the B2B Commerce Services for unauthorized intrusions using network-based and/or host-based intrusion detection mechanisms. Salesforce may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to prevent fraudulent authentications, and to ensure that the B2B Commerce Services function properly.

Security Logs

All systems used in the provision of the B2B Commerce Services, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

Incident Management

Salesforce maintains security incident management policies and procedures. Salesforce notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Salesforce or its agents of which Salesforce becomes aware, to the extent permitted by law.

Salesforce publishes system status information on the Salesforce Trust website. Salesforce typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Salesforce’s response.

User Authentication

Access to B2B Commerce Services requires authentication via one of the supported mechanisms as described in the Salesforce Security Guide, including user ID/password, SAML based Federation, OpenID Connect, Oauth, Social Login, or Delegated Authentication as determined and controlled by the customer. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

Physical Security

Production data centers used to provide the B2B Commerce Services have access control systems that permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, utilize redundant electrical and telecommunications systems, employ environmental systems that monitor temperature, humidity and other environmental conditions, and contain strategically placed heat, smoke and fire detection and suppression systems. Facilities are secured by around-the-clock guards, interior and exterior surveillance cameras, two-factor access screening and escort-controlled access. In the event of a power failure, uninterruptible power supply and continuous power supply solutions are used to provide power while transferring systems to on-site back-up generators.

Reliability and Backup

All networking components, network accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the B2B Commerce Services is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the B2B Commerce Services is stored on highly redundant carrier-class disk storage and multiple data paths to ensure reliability and performance. All Customer Data submitted to the B2B Commerce Services, up to the last committed transaction, is automatically replicated on a near real-time basis to the secondary site and is backed up on a regular basis. Any backups are verified for integrity and stored in the same data centers as their instance. The foregoing replication and backups may not be available to the extent the managed package is uninstalled by a Customer's administrator during the subscription term because doing so may delete Customer Data submitted to such services without any possibility of recovery.

Disaster Recovery

Production data centers are designed to mitigate the risk of single points of failure and provide a resilient environment to support service continuity and performance. The B2B Commerce Services utilize secondary facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event Salesforce production facilities at the primary data centers were to be rendered unavailable.

Salesforce has disaster recovery plans in place and tests them at least once per year. The scope of the disaster recovery exercise is to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing developed operational and disaster recovery procedures and documentation.

The B2B Commerce Services' disaster recovery plans currently have the following target recovery objectives: (a) restoration of the B2B Commerce Service (recovery time objective) within 12 hours after Salesforce's declaration of a disaster; and (b) maximum Customer Data loss (recovery point objective) of 4 hours. However, these targets exclude a disaster or multiple disasters causing the compromise of both data centers at the same time, and exclude development and test bed environments, such as the Sandbox service.

Viruses

The B2B Commerce Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the B2B Commerce Services by a customer. Uploaded attachments, however, are not executed in the B2B Commerce Services and therefore should not damage or compromise the B2B Commerce Services by virtue of containing a virus.

Data Encryption

The B2B Commerce Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the B2B Commerce Services, including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128-bit symmetric encryption keys at a minimum. Additionally, all data, including Customer Data, is transmitted between data centers for replication purposes across a dedicated, encrypted link utilizing AES-256 encryption.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the B2B Commerce Services (to the extent such data has not been deleted by Customer). During the contract term, customers may export a copy of any Customer Data that is made available for export through the Covered Services. Salesforce shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format. The foregoing return of Customer Data for B2B Commerce Services may not be available if the package was removed prior to contract termination.

Deletion of Customer Data

After termination of all subscriptions associated with an environment, Customer Data submitted to the B2B Commerce Services is retained in inactive status within the B2B Commerce Services for 120 days, after which it is securely overwritten or deleted from production within 90 days, and from backups within 180 days. Physical media on which Customer Data is stored during the contract term is not removed from the data centers that Salesforce uses to host Customer Data unless the media is at the end of its useful life or being deprovisioned, in which case the media is first sanitized before removal. This process is subject to applicable legal requirements.

Without limiting the ability for customers to request return of their Customer Data submitted to the B2B Commerce Services, Salesforce reserves the right to reduce the number of days it retains such data after contract termination. Salesforce will update this Salesforce Security, Privacy and Architecture Documentation in the event of such a change.

Day 0, subscription terminates	Day 0 - 30	Day 30 - 120	Day 121 - 211	Day 121 - 301
	Data available for return to customer	Data inactive and no longer available	Data deleted or overwritten from production	Data deleted or overwritten from backups

Sensitive Data

Important: B2B Commerce Services allow customers to accept credit cards through a third-party service using an iframe presented through a page hosted in the customer's Salesforce-hosted Customer Org. The cardholder data is collected by the third party that is configured and managed by the customer. For all other use cases customers must not submit payment cardholder data and authentication data, credit or debit card numbers, or any security codes or passwords to the B2B Commerce Services. Customers must not use the B2B Commerce Services to store credit card information.

For clarity, the foregoing restrictions do not apply to financial information provided to Salesforce for the purposes of checking the financial qualifications of, and collecting payments from, its customers, the processing of which is governed by Salesforce's Website Privacy Statement.

Additionally, for the B2B Commerce Services, the following types of sensitive personal data may not be submitted: personal health information, where Customer is a health care provider, health care clearinghouse, health plan, or an entity performing functions on behalf of such entities, except in limited circumstances where, subject to restrictions, Salesforce has expressly permitted such submission contractually.

If Customer does submit personal health information or other sensitive or regulated data to the B2B Commerce Services, then Customer is responsible for ensuring that its use of the B2B Commerce Services to process that information complies with all applicable laws and regulations.

Analytics

Salesforce may track and analyze the usage of the B2B Commerce Services for purposes of security and of helping Salesforce improve both the B2B Commerce Services and the user experience in using the B2B Commerce Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality.

Salesforce may share anonymous usage data with Salesforce's service providers for the purpose of helping Salesforce in such tracking, analysis and improvements. Additionally, Salesforce may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.

Interoperation with Other Services

The B2B Commerce Services may interoperate or integrate with other services provided by Salesforce or third parties. Security, Privacy and Architecture documentation for services provided by Salesforce is available in the Trust and Compliance Documentation. Salesforce also provides a variety of platforms and features that allow Salesforce users to learn about Salesforce products, participate in communities, connect third-party applications, and participate in pilots, testing and assessments, which are outside the scope of this documentation. Salesforce may communicate with users that participate in such platforms and features in a manner consistent with our Privacy Statement. Additionally, Salesforce may contact users to provide transactional information about the B2B Commerce Services; for instance, through the Adoption Manager program or through system-generated messages, such as Chatter notifications. Salesforce offers customers and users the ability to deactivate or opt out of receiving such messages.