Salesforce.com: Winter ‘14

Salesforce Security, Privacy and Architecture Documentation

Last updated: November 30, 2013

SALESFORCE

SFDC's Corporate Trust Commitment

Salesforce.com, inc. ("SFDC") 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 data submitted by customers to our services ("Customer Data").

Services Covered

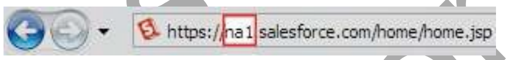
This documentation describes the architecture of, the security and privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to the services branded as Salesforce, Force.com, Sales Cloud, Service Cloud, and Chatter (the "Salesforce Services").

SFDC Infrastructure

SFDC owns or controls access to the systems used to provide the Salesforce Services except for the limited functions described below in "Third-Party Infrastructure."

Each instance of the Salesforce Services (for example, NA1 or CS2) contains many servers and other elements to make it run. We refer to each instance as a "pod." All of the elements of a pod are housed together in the same physical data center. Each pod in a primary data center has an exact copy in a data replication data center.

The instance your organization uses is indicated in the browser's address bar, shown highlighted below.



https://na1.salesforce.com/home/home.jsp

The following pods are currently located in data centers in the following geographies:

Instance Type	Primary Data Center Location	Data Replication Data Center
APAC (e.g. AP0)	Japan	United States
EMEA (e.g. EU1)	United States	United States
North America (e.g. NA2)	United States	United States
Sandbox (e.g. CS3)	United States, except for CS5 and CS6, which have their primary data center in Japan	United States

Third-Party Infrastructure

The Site.com Published Site product uses a third-party optimization service to improve performance and reliability. Customer Data processed by the Site.com Published product may be accessed by providers of optimization services necessary for the operation of the Site.com Published Site product.

The Activa Live Agent for Salesforce product is hosted by a third-party subcontractor.

Audits and Certifications

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

- **ISO 27001 certification:** SFDC is subject to an information security management system (ISMS) in accordance with the ISO 27001 international standard. SFDC has achieved ISO 27001 certification for its ISMS from an independent third party. The scope of SFDC's ISO 27001 certification is available here.
- **SSAE 16 Service Organization Control (SOC) reports:** SFDC's information security control environment applicable to the Salesforce Services undergoes an independent evaluation in the form of SSAE 16 Service Organization Control
- (SOC-1, SOC-2, or SOC-3) reports. **EU/US and Swiss/US Safe Harbor self-certifications**: Customer Data submitted to the Salesforce Services is within the scope of SFDC's annual self-certification to the EU/US and Swiss/US Safe Harbor frameworks as administered by the U.S. Department of Commerce. SFDC's current self-certification is available at http://export.gov/safeharbor by searching for "salesforce.com."
- **TRUSTe Privacy Seal:** SFDC has been awarded the TRUSTePrivacySeal signifying that SFDC's WebSitePrivacy Statement and associated practices related to the Salesforce Services have been reviewed by TRUSTe for compliance with TRUSTe'sprogramrequirements, including transparency, accountability, and choice regarding the collection and use of personal data.
- **PCI:** For the Salesforce Services, SFDC has obtained a signed Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the Payment Card Industry Data Security Standard version 2.0, as formulated by The Payment Card Industry Security Standards Council ("PCI DSS") as a data storage entity or third party agent from an Qualified Security Assessor that is certified as such by The Payment Card Industry Security Standards Council. SFDC's AoC is available here. Customers must use the Salesforce Services' "custom encrypted fields" technology to benefit from SFDC's PCI DSS AoC. Information about custom encrypted fields is available in the Security Implementation Guide.

Additionally, the Salesforce 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 Controls

The Salesforce Services include a variety of configurable security controls that allow customers to tailor the security of the Salesforce Services for their own use. These controls are set forth in the SecurityImplementationGuide.

Security Procedures, Policies and Logging

The Salesforce Services are operated in accordance with the following procedures to enhance security:

- User passwords are stored using a salted hash format for encryption.
- 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, SFDC can provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.
- Logging will be kept for a minimum of 90 days.

- Logging will be kept in a secure area to prevent tampering.
- Passwords are not logged under any circumstances.
- Certain administrative changes to the Salesforce Services (such as password changes and adding custom fields) are tracked in an area known as the "Setup Audit Log" and are available for viewing by a customer's system administrator. Customers may download and store this data locally.
- SFDC 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.

Intrusion Detection

SFDC, or an authorized third party, will monitor the Salesforce Services for unauthorized intrusions using network-based intrusion detection mechanisms.

Incident Management

SFDC maintains security incident management policies and procedures. SFDC promptly notifies impacted customers of any actual or reasonably suspected unauthorized disclosure of their respective Customer Data to the extent permitted by law.

User Authentication

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

Security Logs

All SFDC systems used in the provision of the Salesforce 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 the security audits referred to above.

Physical Security

Production data centers used to provide the Salesforce Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are secured by around-the-clock guards, two-factor card key & biometric access screening and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

Reliability and Backup

All networking components, SSL accelerators, load balancers, Web servers and application servers are configured in a redundant configuration. All Customer Data submitted to the Salesforce Services is stored on a primary database server with a multiple active clusters for redundancy. All Customer Data submitted to the Salesforce Services is stored on carrier-class disk storage using RAID disks and multiple data paths to ensure reliability and performance. All Customer Data submitted to the Salesforce Services, up to the last committed transaction, is automatically backed up on a regular basis and stored on backup media for an additional 90 days after which it is securely overwritten or deleted from the Salesforce Services. Any backups are verified for integrity and stored in SFDC data centers.

Disaster Recovery

SFDC has disaster recovery plans in place and tests them at least once per year. The Salesforce Services utilize disaster recovery facilities that are geographically remote from their primary data centers, along with required hardware, software, and Internet connectivity, in the event SFDC production facilities at the primary data centers were to be rendered unavailable.

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

Viruses

The Salesforce Services will not introduce any viruses to a customer's systems. However, the Salesforce Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the Salesforce Services by a customer. Any such uploaded attachments will not be executed in the Salesforce Services and therefore will not damage or compromise the Salesforce Services.

Data Encryption

The Salesforce Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Salesforce Services, including minimum 128-bit VeriSign SSL Certification and minimum 2048-bit RSA public keys. Additionally, Customer Data is encrypted during transmission between data centers for replication purposes.

Return of Customer Data

Within 30 days post contract termination, customers may request return of their respective Customer Data submitted to the Salesforce Services. SFDC shall provide such Customer Data via a downloadable file in comma separated value (.csv) format and attachments in their native format.

Deletion of Customer Data

After contract termination, Customer Data submitted to the Salesforce Services is retained in inactive status within the Salesforce Services for 180 days and a transition period of up to 30 days, after which it is securely overwritten or deleted. In accordance with the Reliability and Backup section above, Customer Data submitted to the Salesforce Services (including Customer Data retained in inactive status) will be stored on backup media for an additional 90 days after it is securely overwritten or deleted from the Salesforce Services. This process is subject to applicable legal requirements.

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

Anonymized and Aggregated Data

SFDC may track and analyze use of the Services for the purpose of helping the SFDC improve both the Salesforce Services and the user experience in using the Salesforce Services. Without limiting the foregoing, SFDC may share anonymous data about SFDC's customers' or their users' use of the Salesforce Services ("Usage Statistics") to SFDC's service providers for the purpose of helping SFDC in such tracking or analysis, including improving its users' experience with the Salesforce Services, or as required by law. Except when required by law, any such sharing of Usage Statistics to SFDC's service providers will not include any identifying information about SFDC's customers or customers' users.

Interoperation with Other SFDC Services

The Salesforce Services may interoperate with other services provided by SFDC. The Security, Privacy and Architecture documentation for such services is available at the following links:

- Data.comSecurity,PrivacyandArchitectureDocumentation
- Desk.com Security, Privacy and Architecture Documentation
- HerokuSecurity,PrivacyandArchitectureDocumentation
- MarketingCloudSecurity,PrivacyandArchitectureDocumentation
- Work.comSecurity,PrivacyandArchitectureDocumentation
- ExactTargetSecurity,PrivacyandArchitectureDocumentation
- PardotSecurity,PrivacyandArchitectureDocumentation