STEELBRICK SERVICES SECURITY, PRIVACY, AND ARCHITECTURE

Last Updated: March 1, 2016

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 data submitted by customers to our services ("Customer Data").

Services Covered

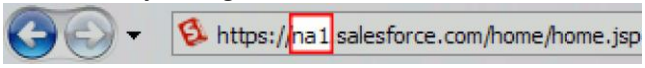
This documentation describes the architecture and the administrative, technical and physical controls applicable to the managed packages branded as SteelBrick (the "SteelBrick Services"). This documentation applies to the Steelbrick Services, in large part, by virtue of it being provisioned as managed packages and a component of the services provided by Salesforce branded as "Salesforce Services". The Security, Privacy and Architecture documentation for Salesforce Services is available in the Trust and Compliance Documentation section of help.salesforce.com.

Salesforce Infrastructure

Salesforce owns or controls access to the infrastructure that Salesforce uses to host Customer Data submitted to the SteelBrick Services except for the functions described in Third-Party Architecture below.

Each instance of the SteelBrick Services (for example, NA1 or CS2) contains many servers and other elements to make it run. Each instance in a primary data center has an exact copy in a secondary data center.

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



Alternatively, if your organization uses the My Domain feature, you may use the lookup form at https://trust.salesforce.com/trust/domainLookupLaunch/ to find the corresponding instance.

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

Instance Type	Primary Data Center Location	Secondary Data Center
APAC (e.g. AP0)	Japan	United States
EMEA (EU0, EU1, EU2, EU3)	United Kingdom	Germany

EMEA (EU5)	United Kingdom	United States
EMEA (EU4, EU6)	Germany	United Kingdom
North America (e.g. NA2)	United States	United States
Sandbox (CS5, CS6, CS31)	Japan	United States
Sandbox (CS80, CS81)	United Kingdom	United States
Sandbox (CS82, CS83)	Germany	United Kingdom
Sandbox (CS86, CS87)	United Kingdom	Germany
Sandbox (all other CS instance types)	United States	United States

.

Third-Party Infrastructure

The infrastructure used by Salesforce to temporarily process Customer Data submitted to the SteelBrick Services in order to facilitate SteelBrick's PDF generator and quote calculator functionality is provided by a third- party provider, Amazon Web Services, Inc. ("AWS") by virtue of using the Salesforce services branded as Heroku (the "Heroku Services") as a PaaS for such functionality. Any such data transmitted to AWS via the Heroku Services does not persist on AWS. Currently, the infrastructure hosted by AWS in the provisioning of the SteelBrick Services is located in the United States.

Audits and Certifications

As a managed package component of the services provided by Salesforce branded as "Salesforce Services", the SteelBrick 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.

See the Security, Privacy and Architecture documentation for Salesforce Services in the Trust and Compliance Documentation section of help.salesforce.com for further information about security and privacy-related audits and certifications that are applicable to Salesforce Services.

Information about security and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and Service Organization Control (SOC) reports, is available from the AWS Security Web site and AWS Compliance Web site.

Security Controls

The SteelBrick Services include a variety of configurable security controls that allow customers to tailor the security of the SteelBrick Services for their own use.

Security Procedures, Policies and Logging

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

- User passwords are stored using a one-way salted hash.
- 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 to assist in forensic analysis. This service will be provided to customers on a time and materials basis.
- Logs will be kept for a minimum of 90 days.
- Logs will be kept in a secure area to prevent tampering.
- Passwords are not logged under any circumstances.
- Certain administrative changes to the SteelBrick 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.
- 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.

Intrusion Detection

Salesforce, or an authorized third party, will monitor the SteelBrick Services for unauthorized intrusions using network-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 SteelBrick Services function properly.

Security Logs

All systems used in the provision of the SteelBrick Services, including firewalls, routers, network switches and operating systems, log information to their respective system's 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 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 SteelBrick Services requires authentication via one of the supported mechanisms as described in the Security Implementation Guide, including user ID/password, SAML based Federation, 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 SteelBrick 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 access screening, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure. Further information about physical security provided by AWS is available from the AWS Security Web site, including AWS's overview of security processes.

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 SteelBrick Services is stored on a primary database server with multiple active clusters for higher availability. All Customer Data submitted to the SteelBrick Services is stored on carrier-class disk storage using redundant devices and multiple data paths to ensure reliability and performance. All Customer Data submitted to the SteelBrick 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 and stored on backup media for an additional 90 days in production environments and 30 days in Sandbox environments after which it is securely overwritten or deleted from the SteelBrick Services. The foregoing replication and backups may not be available to the extent the Steelbrick Services managed package is uninstalled by a Customer's administrator during the subscription term. Any backups are verified for integrity and stored in Salesforce data centers.

Disaster Recovery

Salesforce has disaster recovery plans in place and tests them at least once per year. The SteelBrick Services utilize secondary facilities that are geographically remote 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.

The SteelBrick Services' disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Salesforce Service within 12 hours after Salesforce'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 SteelBrick Services do not scan for viruses that could be included in attachments or other Customer Data uploaded into the SteelBrick Services by a customer. Uploaded attachments, however, are not executed in the SteelBrick Services and therefore will not damage or compromise the SteelBrick Services by virtue of containing a virus.

Data Encryption

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

Return of Customer Data

If Customer's contract for SteelBrick Services has expired, and Customer's Salesforce Services Org is still active, customers may request temporary activation of appropriate SteelBrick Services licenses for a 30 day maximum period starting on the day the SteelBrick Services contract terminates by logging a case in the SteelBrick Customer Support Portal, provided the SteelBrick Services managed package has not been uninstalled. Within this period customers may export Customer Data using standard Salesforce Data Loader capabilities or Data APIs.

Deletion of Customer Data

After termination of the Salesforce Services contract, Customer Data submitted to the SteelBrick Services is retained in inactive status within the SteelBrick 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 SteelBrick Services (including Customer Data retained in inactive status) will be stored on backup media for an additional 90 days in production environments and 30 days in Sandbox environments after it is securely overwritten or deleted from the SteelBrick Services. 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. The foregoing backup and deletion process does not apply if the Steelbrick Services managed package is uninstalled by a Customer's administrator during the subscription term because doing so deletes Customer Data submitted to the Steelbrick Services without any possibility of recovery.

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

Tracking and Analytics

Salesforce may track and analyze use of the SteelBrick Services for purposes of security and helping Salesforce improve both the SteelBrick Services and the user experience in using the SteelBrick Services. Salesforce may also use this information and users' e-mail addresses to contact customers or their users to provide transactional information about the SteelBrick Services. Salesforce will offer customers and users the ability to opt out of receiving such emails. These communications may be sent using services provided by ExactTarget, Inc., an affiliate of salesforce.com, inc.

Without limiting the foregoing, Salesforce may share anonymous data about Salesforce's customers' or their users' use of the SteelBrick Services ("Usage Statistics") to Salesforce's service providers for the purpose of helping Salesforce in such tracking or analysis, including improving its users' experience with the SteelBrick Services, or as required by law. Additionally, Salesforce may share such anonymous data with other customers on an aggregate basis. Except when required by law, any such sharing of Usage Statistics will not include any identifying information about Salesforce's customers or customers' users.

Sensitive Personal Data

Important: The following types of sensitive personal data may not be submitted to the SteelBrick Services: government-issued identification numbers; payment cardholder data and authentication data, credit or debit card numbers, any related security codes or passwords, and bank account numbers); information related to an individual's physical or mental health; and information related to the provision or payment of health care.

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 the SteelBrick Web Site Privacy Statement.

Interoperation with Other Salesforce Services

The SteelBrick Services may interoperate with other services provided by Salesforce. The Security, Privacy and Architecture documentation for such services is available in the Trust and Compliance Documentation section of help.salesforce.com.