IoT Cloud Security, Privacy and Architecture

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, privacy-related certification received for, and the administrative, technical and physical controls applicable to, the services branded as IoT Cloud (the "IoT Cloud Services"). The IoT Cloud Services do not include the service branded as IoT Explorer (including IoT Plus), which is addressed in the Salesforce Services documentation available in the Trust and Compliance Documentation.

Architecture and Data Segregation

The IoT Cloud Services are operated in a segregated tenant architecture that physically separates Customer Data, restricts access based on user privileges, and provides separate environments for different functions. 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 IoT Cloud Services.

Audits and Certifications

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

- **EU and UK Binding Corporate Rules (BCR) for Processors:** Customer Data submitted to the IoT Cloud 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/.
- **EU-U.S. and Swiss-U.S. Privacy Shield certification:** Customer Data submitted to the IoT Cloud 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".
- **APEC Privacy Recognition for Processors (PRP):** Customer Data submitted to the IoT Cloud 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/.

- **TRUSTe Certification:** Salesforce's Website Privacy Statement and privacy practices related to IoT Cloud Services are assessed by TRUSTe annually, for compliance with TRUSTe's Certification and Verification Assessment Criteria. For more information on the status of Salesforce's certification/verification status, click here.

The IoT Cloud 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.

As further described in the "Infrastructure and Sub-processors" documentation, the infrastructure used by Salesforce to host Customer Data submitted to the IoT Cloud Services is provided by a third party, Amazon Web Services, Inc. ("AWS"). Information about security- and privacy-related audits and certifications received by AWS, including information on ISO 27001 certification and System and Organization Controls (SOC) reports, is available from the AWS Security Website and the AWS Compliance Website.

Security Policies and Procedures

The IoT Cloud Services are operated in accordance with the following policies and 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.
- Certain administrative changes to the IoT Cloud Services (such as password changes) 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.
- Multi-Factor Authentication and Single Sign-On for access to the IoT Cloud Services as set forth in the applicable Notices and License Information (NLI).

Intrusion Detection

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 IoT Cloud Services function properly.

Security Logs

All Salesforce systems used in the provision of the IoT Cloud Services 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.

User Authentication

The IoT Cloud Services are accessible only through an authenticated connection from an instance of the "Salesforce Services," which are described in the Trust and Compliance Documentation. Access to the IoT Cloud Services requires authentication via one of the supported mechanisms for the Salesforce platform 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 IoT Cloud Services have access control systems. 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.

Viruses

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

Data Encryption

The IoT Cloud Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the IoT Cloud Services, including 256-bit TLS Certificates and 2048-bit RSA public keys at a minimum.

Return of Customer Data

Within 30 days post contract termination, customers may request Salesforce to provide access to their respective Customer Data if it is still retained and stored within an AWS S3 bucket at the time of the request in order to export such data. Customers are solely responsible for downloading such data.

Deletion of Customer Data

Salesforce may delete Customer Data 180 days or more after its submission to the IoT Cloud Services as per its internal retention and data storage policies. After termination of the IoT Cloud Services, to request deletion of Customer Data submitted to the IoT Cloud Services, please contact your account representative. This process is subject to applicable legal requirements.

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

Analytics

Salesforce may track and analyze the usage of the IoT Cloud Services for purposes of security and helping Salesforce improve both the IoT Cloud Services and the user experience in using the IoT Cloud 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.

Sensitive Data

Important: The following types of sensitive personal data may not be submitted to the IoT Cloud Services: government-issued identification numbers; and financial information (such as credit or debit card numbers, any related security codes or passwords, and bank account numbers).

Additionally, for the IoT Cloud 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 IoT Cloud Services, then Customer is responsible for ensuring that its use of the IoT Cloud Services to process that information complies with all applicable laws and regulations.

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 Salesforce Website Privacy Statement.

Interoperation with Other Services

The IoT Cloud 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 IoT Cloud 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.