MuleSoft 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 the security- and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to the services branded as MuleSoft or the Anypoint Platform or MuleSoft Composer ("MuleSoft Services") provided by salesforce.com, inc. and /or its affiliates (collectively, "Salesforce"). The MuleSoft Services consist of the MuleSoft Cloud Offerings and the MuleSoft Software as set forth in an Order Form, excluding the services branded as API Community Manager which are subject to the Community Cloud Documentation as applicable. Information on the Security, Privacy, and Architecture used by API Community Manager is available in the Community Cloud Trust and Compliance Documentation. For purposes of this Documentation, all terms applicable to the MuleSoft Cloud Offerings shall also apply to MuleSoft Composer. All capitalized terms used in this documentation are defined in Salesforce's Master Subscription Agreement, Data Processing Addendum, and/or the applicable ordering documents or Documentation.

Architecture and Data Segregation

The MuleSoft Cloud Offerings 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 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 only processed 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 the processing activities provided by them. 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 MuleSoft Cloud Offerings.

Audits and Certifications

The following security and privacy-related audits and certifications are applicable to MuleSoft's Cloud Offerings:

- **EU-U.S. and Swiss-U.S. Privacy Shield certification**: Customer Data submitted to the MuleSoft Cloud Offerings 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 MuleSoft Cloud Offerings 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/.
- **ISO 27001/27017/27018 certification**[1]: Salesforce operates an information security management system (ISMS) for the MuleSoft Cloud Offerings in accordance with the ISO 27001 international standard and aligned to ISO 27017 and ISO 27018. Salesforce has achieved ISO 27001/27017/27018 certification for its ISMS from an independent third party.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**[2]: Salesforce's information security control environment applicable to the MuleSoft Cloud Offerings undergoes an independent evaluation in the form of SOC 1 (SSAE 18 / ISAE 3402) and SOC 2 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.
- **Payment Card Industry (PCI)**[3]: For the MuleSoft Cloud Offerings, Salesforce has obtained a signed Attestation of Compliance ("AoC") demonstrating Level 1 compliance with the applicable Payment Card Industry Data Security Standard, as formulated by The Payment Card Industry Security Standards Council ("PCI DSS") as a data storage entity or third-party agent from a Qualified Security Assessor that is certified as such by The Payment Card Industry Security Standards Council. A copy of MuleSoft's AoC is available upon request from your organization's Salesforce account executive. Credit card information must be encrypted on MuleSoft Cloud Offerings in order to benefit from the MuleSoft AoC.
- **APEC Privacy Recognition for Processors (PRP)**[4]**:** Customer Data submitted to the MuleSoft Cloud Offerings 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/.

The MuleSoft Cloud Offerings 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 for the MuleSoft Cloud Offerings, the infrastructure used by Salesforce to host Customer Data submitted to the MuleSoft Cloud Offerings 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

[1] This section is not applicable to MuleSoft's Government Cloud Deployment.
[2] This section is not applicable to MuleSoft's Government Cloud Deployment.
[3] This section is not applicable to MuleSoft's Government Cloud Deployment.
[4] This section is not applicable to MuleSoft's Government Cloud Deployment.

and Service Organization Control (SOC) reports, is available from the AWS Security Website and the AWS Compliance Website.

Security Controls

The MuleSoft Cloud Offerings include a variety of configurable security controls that allow customers to tailor the security of the MuleSoft Cloud Offerings for their own use. These controls include:

- Customer applications deployed on the MuleSoft Cloud Offerings run within a single tenant environment, which the Customer has the ability to configure based on their internal security requirements.
- Multi-Factor Authentication and Single Sign-On for access to the MuleSoft Cloud Offerings as set forth in the applicable Notices and License Information (NLI).

Further information about security provided by AWS is available from the AWS Security Website, including AWS's overview of security processes.

Security Policies and Procedures

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

- Customer login passwords are stored using a one-way salted hash.
- User access log entries will be maintained, containing date, time, user ID, resource accessed, 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 a customer or its ISP.
- Salesforce personnel will not set a defined password for a user. If a user requests a password reset, Salesforce will deliver a temporarily valid, secret URL to the requesting user via email. A new password is set by visiting this URL.
- With respect to the MuleSoft Cloud Offerings only, if there is suspicion of inappropriate access to the MuleSoft Cloud Offerings, 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

Intrusion Detection

Salesforce, or an authorized independent third party, will monitor the MuleSoft Cloud Offerings for unauthorized intrusions. 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 prevent fraudulent authentications, and to ensure that the MuleSoft Cloud Offerings function properly.

Salesforce may conduct security scans and testing of customer code uploaded to the MuleSoft Cloud Offerings to detect abusive behavior or actions that violate terms for the MuleSoft Services.

Security Logs

All Salesforce systems used in the provision of the MuleSoft Cloud Offerings may log information to their respective system log facilities or a centralized logging service 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

Access to the MuleSoft Services requires a valid user ID and password combination, which are encrypted via SSL/TLS while in motion and login passwords are stored using a one-way salted hash. Alternatively, MuleSoft supports Single Sign On (SSO) utilizing SAML 2.0 which uses Public Key Cryptography and does not require MuleSoft to store a password. Following a successful authentication, a randomly-generated time-scoped credential is transmitted to the user's browser or command line interface (CLI). All subsequent requests are authenticated with that credential, as long as it is valid.

Physical Security

Production data centers used to provide the MuleSoft Cloud Offerings have access system controls in place. 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.

Reliability and Backup

Applications deployed on the MuleSoft Cloud Offerings are automatically replicated on a near real-time basis at the database layer and are backed up as part of the deployment process on secure, access controlled, and redundant storage.

Disaster Recovery

The MuleSoft Cloud Offerings utilize disaster recovery facilities that are geographically diverse from their primary data centers, along with required hardware, software, and Internet connectivity, in the event 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 or restore a MuleSoft service from a primary location to a secondary location utilizing developed operational and disaster recovery procedures and documentation.

Malicious Software

Salesforce implements practices and software to limit the risk of exposure to malicious software in the MuleSoft Cloud Offerings. However, the MuleSoft Cloud Offerings do not scan for viruses or malicious software that could be included in attachments or other data uploaded into the MuleSoft Cloud Offerings by or on behalf of Customers.

Data Encryption

Transport Layer Encryption (TLS) is required for all management MuleSoft Cloud Offerings and is available as an option for the MuleSoft Services in the runtime plane. MuleSoft Cloud Offerings in the runtime plane will default to encrypted services, however customers can control the protocol and encryption of many services and all runtime applications, as indicated in the Documentation.

Return of Customer Data

During the term of Customer's subscription to the MuleSoft Cloud Offerings, Customer may make copies of its Customer Data submitted to the MuleSoft Cloud Offerings as the Customer deems fit. Customers can request assistance from MuleSoft support up to 30 days after contract termination.

Deletion of Customer Data

After termination of Customer's subscription to all of the MuleSoft Services and expiration of the 30-day period described above, Customer Data submitted to the MuleSoft Cloud Offerings will be deleted. This process is subject to applicable legal requirements.

Transaction Processing Information is metadata related to transactions processed by MuleSoft Anypoint Partner Manager, including but not limited to dates, control numbers, transaction status (e.g., success or failure), message flow, and errors. For each MuleSoft Anypoint Partner Manager Customer using MuleSoft's cloud-based management plane, MuleSoft will retain Transaction Processing Information in MuleSoft's cloud-based management plane for 18 months from the date the transaction was processed by MuleSoft Anypoint Partner Manager. During this 18-month period, Customer may extract such Transaction Processing Information. MuleSoft may delete Transaction Processing Information older than 18 months.

Sensitive Data

Important: For the MuleSoft Cloud Offerings, 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, provided in no circumstances will Customer be permitted to submit any Protected Health Information, as defined under the U.S. Health Insurance Portability and Accountability Act, in any name fields (including but not limited to application names, flow names, load balancers, DNS records, URLs, configuration/properties etc.) or log such Protected Health Information via the Logger Component in Customer applications.

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

Analytics

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