Medallia Experience Cloud End-to-End Data Protection

Answers to your most pressing information security questions

Medallia

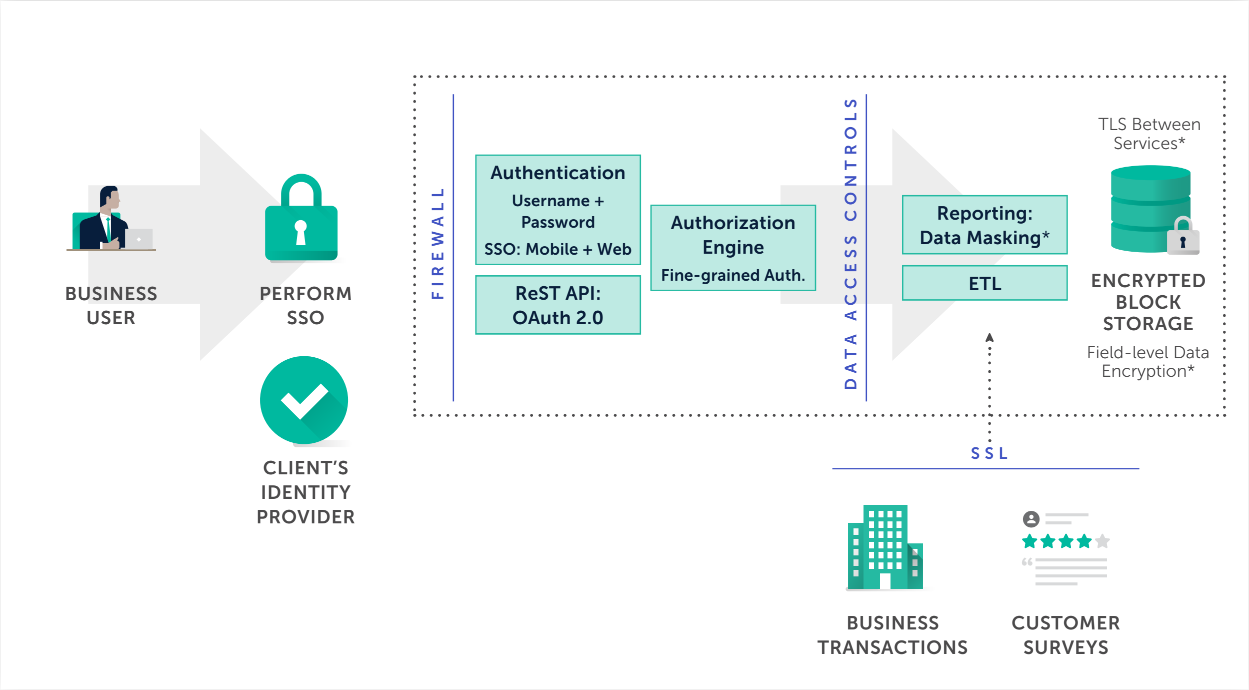
Introduction

Businesses around the world rely on the Medallia Experience Cloud to interact with their customers, analyze feedback and take action to improve the customer experience.

Customer data is at the heart of our platform, and we know how important protection of that data is to our clients' daily operations, as well as their reputation and trust with their customers. Data protection is a top priority for Medallia. We build our platform using the following core principles:

- We treat all customer data as private and sensitive.
- We do NOT sell data to third parties.
- Our customers are in control of their data. We have standard, industry compliant policies for deletion and retention of data that our customers can use, but they can opt for stronger requirements.
- We've architected our platform with security and compliance in mind, using privacy by design principles.

Medallia Experience Cloud Security



*Add-on data security capabilities

- Medallia provides industry-leading data protection, with enterprise-grade controls to govern data access and the security of data across the Medallia platform.

Data Access Controls

One of the most important benefits of the Medallia Experience Cloud is its ability to distribute customer experience data throughout a client's organization, allowing for each employee to be closely aligned to the voice of the customer. However, this benefit also requires sophisticated authentication and control of what information each employee is authorized to access.

Single Sign-On

To control login access, Medallia supports Single Sign-On (SSO). This improves security by countering password fatigue, while at the same time improving the user authentication experience. Medallia has implemented SSO using the SAML 2.0 industry standard, supporting all major SSO technologies, such as Microsoft Active Directory and Azure Active Directory, Okta, Ping, Centrify, OneLogin, Oracle Enterprise Single Sign-On, Google Identity Platform, CA Single Sign-On, and many more.

Medallia also supports configuration of multiple SSO providers at the same time. A possible use case would be if a company had separate identity stores for employees in different geographies or different business groups; Medallia can segregate user identities by distinguishing between stores — the identity store selection can either be automatic using predefined rules or can be user selectable.

To manage users of the Medallia Mobile application, secured access can be controlled through any Enterprise Mobility Management platform that supports the AppConfig Community standards.

Two-Factor Authentication

Two-Factor Authentication (2FA) is the process by which a user provides two separate login credentials before getting access to the system. Medallia uses Time-based One-Time Password (TOTP) as the second authentication factor, after the user has provided their credentials. The platform performs step-up authentication using the second factor when the user attempts to perform sensitive actions on the system. Users can enroll in 2FA in a self-service mode with mobile apps like Google Authenticator or Duo.

Data Access Controls

Authorization - Admin and Data Permissions

Authorization determines what a user can and cannot do after login to the system. The Medallia Experience Cloud supports a fine-grained authorization model, allowing an administrator to grant access based on user groups / roles, organizational hierarchy and data permissions.

The company's identity store dictates role membership and account validity, and Medallia executes the authorization decision at run-time, based on Attribute-based Access Control (ABAC) and Role-based Access Control (RBAC). Medallia provides both data and user controls following the least access principle.

The platform provides a layered authorization mechanism that permits an administrator to expose different data sets to different users. An administrator can define permission profiles and role-level shared permissions to allow users access to individual or groups of data records.

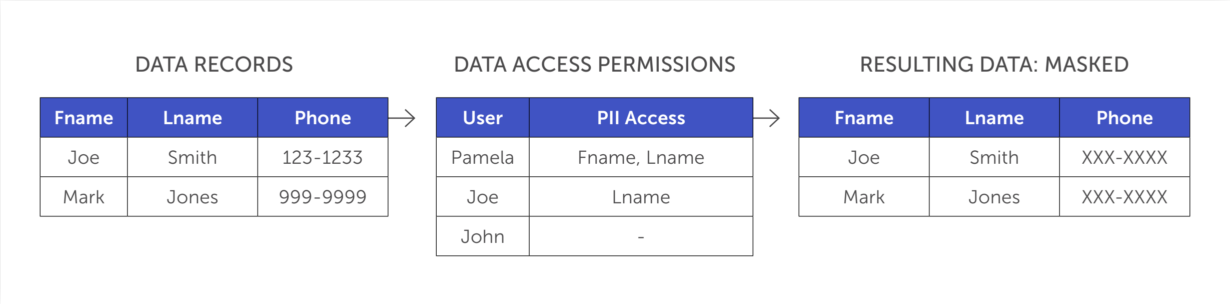
Additionally, user controls dictate what functions a user can perform in the system. Actions include: View/Edit Reports, View/Edit Surveys, and Edit Security Setup. Hence a combination of these controls are used to yield the desired level of data access and system functionality for each user.

Data Masking

For personal data or other sensitive data, Medallia offers the ability for specified data fields to be masked from the view of users without authorized access rights, safeguarding end customers' privacy by obscuring those fields from users who don't need access to it.

The platform provides predefined roles, which can be assigned to a user, automatically masking personal or other sensitive data.

This capability enables compliance with regulations which require that data access is provided on a need-to-know basis, such as the General Data Protection Regulation in the EU and HIPAA in the US (for more on how Medallia supports these and other regulations, go to the **Regulatory Compliance** section of this document).



DATA RECORDS

Fname	Lname	Phone
Joe	Smith	123-1233
Mark	Jones	999-9999

DATA ACCESS PERMISSIONS

User	PII Access
Pamela	Fname, Lname
Joe	Lname
John	-

RESULTING DATA: MASKED

Fname	Lname	Phone
Joe	Smith	XXX-XXXX
Mark	Jones	XXX-XXXX

» Medallia's data masking capabilities allow for obscuring Personally Identifiable Information (PII) except for designated users.

Data Security Controls

Protecting our clients' data requires a robust architecture that secures customer data across the entire platform architecture. Medallia provides best-in-class data security from our cloud infrastructure to the application layer.

Data Centers

Medallia has implemented extensive security processes for protecting access to our data center infrastructure, all of which is Tier III, SOC 2 and/or ISO 27001 certified.

All Medallia data centers have common security practices, including closed-circuit video monitoring and 24/7-manned guards, and each requires the use of biometric access controls to our locked cages.

Data Transfer

Medallia provides both Secure FTP and REST-based API's sent via Secure Sockets Layer (SSL) for the transfer of data to and from the Medallia Experience Cloud. Medallia uses the standards-based OAuth 2.0 authorization framework and OpenID Connect (an identity layer on top of OAuth) to ensure that only authorized third-parties (e.g., clients and partners) can interact with the Medallia Experience Cloud via API.

Network Monitoring

Medallia uses both internal and external services to perform continuous scanning and monitoring of our network and platform.

We also conduct regular vulnerability scans, risk assessments and penetration tests to ensure secure systems.

Data Encryption

Medallia provides encryption for data rest residing in the Medallia Experience Cloud, as well as various types of data in motion.

The following page provides additional details on Medallia's data encryption capabilities.

Data Encryption Details

Medallia offers multiple levels of encryption for protecting unauthorized access of data in the Medallia Experience Cloud.

Encryption on Storage

Medallia uses encryption at three levels for stored customer data. Customer instances are hosted in containers and a database is used as a data store.

Level 1: Encryption at the Compute O/S layer BEFORE sending to the storage server. There is a unique encryption key for each program instance. This protects against unauthorized access to the Storage infrastructure. For example, if anyone were to gain unauthorized access at the compute O/S layer itself, then they would still not have any access to unencrypted data on storage.

Level 2: Encryption at the Storage O/S layer BEFORE sending to media.

Level 3: Encryption at the Media level. This protects against hardware loss or theft.

Field-level Personal Data Encryption

Survey data in Medallia Experience Cloud is retained in a database and is only accessible to our Database Administrators for maintenance purposes. But, the specific fields that contain personally identifiable information, also known as PII (such as first name, last name, email address, phone number, etc.), in the database are not encrypted. This allows a DBA or anyone with authorized access to the database to view the information through a SQL client (e.g. psql).

Medallia offers an add-on option enabling field-level encryption of a default set of PII fields in the database, with the ability to encrypt additional selected fields. Field are encrypted with a tenant-specific encryption key stored in a Secrets vault. This option ensures that these fields are only accessible to users through an authorized application request which includes the tenant key.

Encryption on the Wire

Medallia Experience Cloud encrypts data from the end users browser to Medallia Experience Cloud services.

TLS v1.2 (Transport Layer Security) is a data protection protocol specification with two layers: the TLS record protocol provides connection security, and the TLS handshake protocol enables the sender and receiver to authenticate each other and to negotiate security keys before any data is transmitted. Also, Medallia has public APIs that customer applications invoke. Those API endpoints are also secured with TLS v1.2

In addition, encryption on the wire, within the Cloud between Medallia Services is supported as as add-on option, adding TLS encryption for any data transfers between different Medallia Experience Cloud components that are used by the customer program (for example, data passing between the reporting engine and the org sync service).

Encryption for File transfer

Customers can import from or export data to Medallia Experience Cloud services. The data is transferred via various file formats of customer's choice and those files are encrypted using PGP. Medallia keys are stored in a Secrets vault and with unique keys per tenant.

Regulatory Compliance

The Medallia Experience Cloud is used by companies and organizations around the world, which are bound by a variety of industry-based and regional data protection regulations.

Our processes and controls are regularly audited by internal and external parties. We have third party certifications for SOC 2 and ISO27001 frameworks, and are compliant with ISAE3000 and HIPAA.

Medallia has data center infrastructure located in multiple geographies to comply with various data residency requirements. In addition, Medallia's GovCloud infrastructure has been certified as FedRamp Ready for US Federal Government agencies.

Additionally, Medallia provides our clients compliance with the following data privacy and protection regulations.

Privacy Shield

Medallia complies with the Privacy Shield principles for data it receives of European and Swiss individuals in its SaaS platforms, and is certified under these frameworks. For more information on Privacy Shield compliance, see our listing on the Privacy Shield website.

Data Protection and Privacy Regulations

Medallia's platform is prewired to comply with the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). This means that Medallia provides tools that allow our clients to permanently delete, export, or correct information associated with an individual survey taker or employee based on that individual's request, as well as to verify and create reports on the deletion of information.

Medallia also offers a data processing agreement that includes the controller-to-processor Standard Contractual Clauses approved by the European Commission, with updates to specifically address the requirements of GDPR.

Opt-Out Regulations

In order to ensure compliance with various regulations concerning digital communications, Medallia provides opt-out functionality via opt-out links in its email survey invitations, and we honor SMS requests to stop future communications. These prevent Medallia from sending out additional survey requests to our clients' customers who do not wish further communications from that company.

Summary

At Medallia, we have built an enterprise-grade customer experience management platform, protecting our clients' customer data at every layer and interaction point.

Additional details regarding Medallia's data controls and policies can be found at medallia.com/privacy-policy.

About Medallia

Medallia is the pioneer and market leader in Experience Management. Medallia's award-winning SaaS platform, the Medallia Experience Cloud, leads the market in the understanding and management of experience for customers, employees and citizens. Medallia captures experience signals created on daily journeys in person, digital and IoT interactions and applies proprietary AI technology to reveal personalized and predictive insights that can drive action with tremendous business results. Using Medallia Experience Cloud, customers can reduce churn, turn detractors into promoters and buyers, and create in-the-moment cross-sell and up-sell opportunities, providing clear and potent returns on investment. Medallia has offices worldwide, including Silicon Valley, Buenos Aires, London, New York, Tel Aviv and McLean, Virginia. Learn more at www.medallia.com.

Follow us: in medallia-inc blog.medallia.com @Medallia

Medallia