Fielo Platform Security

Security Control

fielo

FIELO PLATFORM SECURITY

CONTENTS

Objective

The purpose of this document is to present an overview of how Fielo's Engine tracks and guarantees the accuracy of its customers' sensitive information inside Force.com Platform.

Salesforce Security Basics

Authenticate Users

Authentication means preventing unauthorized access to the organization or its data by making sure each logged in user is who they say they are.

Salesforce provides a variety of ways to authenticate users.

Passwords
Salesforce provides each user with a unique username and password that must be entered each time a user logs in. An administrator can configure several settings to ensure that users' passwords are strong and secure.

Cookies
Salesforce issues a session cookie to record encrypted authentication information for the duration of a specific session.

My Domain
Using My Domain, you can define a Salesforce subdomain name to manage login and authentication for the org in several key ways.

Two-Factor Authentication
Salesforce admin can enhance org's security by requiring a second level of authentication for every user's login. Can also require two-factor authentication when a user meets certain criteria, such as attempting to view reports or access a connected app.

Network-Based Security
Network-based security limits where users can log in from, and when they can log in. This is different from user authentication, which only determines who can log in. Use networkbased security to limit the window of opportunity for an attacker and to make it more difficult for an attacker to use stolen credentials.

Captcha Security for Data Exports
By request, Salesforce can require users to pass a simple text-entry user verification test to export data from Salesforce. This type of network-based security helps prevent malicious users from accessing your organization's data, and can reduce the risk of automated attacks.

Session Security
After logging in, a user establishes a session with the platform. Use session security to limit exposure to your network when a user leaves the computer unattended while still logged in. Session security also limits the risk of internal attacks, such as when one employee tries to use another employee's session. Choose from several session settings to control session behavior.

Custom Login Flows
Use a login flow to introduce business processes during login, such as to prompt for a second factor of authentication, accept terms of services, or collect information from users. After users complete the login flow, they're logged in to Salesforce.

Single Sign-On
Single sign-on (SSO) lets users access authorized network resources with one login. You validate usernames and passwords against your corporate user database or other client app rather than Salesforce managing separate passwords for each resource.

Connected Apps
A connected app integrates an application with Salesforce using APIs. Connected apps use standard SAML and OAuth protocols to authenticate, provide single sign-on, and provide tokens for use with Salesforce APIs. In addition to standard OAuth capabilities, connected apps allow Salesforce admins to set various security policies and have explicit control over who can use the corresponding apps.

Desktop Client Access
Connect Offline and Connect for Office are desktop clients that integrate Salesforce with your PC. An administrator can control which desktop clients' users can access as well as whether users are automatically notified when updates are available.

Shield Platform Encryption

Shield Platform Encryption gives data a whole new layer of security while preserving critical platform functionality. It enables encrypt sensitive data at rest, and not just when transmitted over a network, so the company can confidently comply with privacy policies, regulatory requirements, and contractual obligations for handling private data.

Shield Platform Encryption builds on the data encryption options that Salesforce offers out of the box. Data stored in many standard and custom fields and in files and attachments is encrypted using an advanced HSM-based key derivation system, so it is protected even when other lines of defense have been compromised.

Data encryption key is never saved or shared across organizations. Instead, it is derived on demand from a master secret and your organization-specific tenant secret, and cached on an application server.

Encrypt Fields and Files
Specify the fields and files to encrypt. Remember that encryption is not the same thing as field-level security or object-level security. Those should already be in place before you implement your encryption strategy.

How Shield Platform Encryption Works
Shield Platform Encryption relies on a unique tenant secret that the company control and a master secret that is maintained by Salesforce. We combine these secrets to create unique data encryption key. That key is used to encrypt data that users put into Salesforce, and to decrypt data when authorized users need it.

Monitoring Organization's Security

Track login and field history, monitor setup changes, and take actions based on events. Review the following sections for instructions on monitoring the security of Salesforce organization.

Monitor Login History
Admins can monitor all login attempts for their org and enabled portals or communities. The login history page displays the most recent 20,000 attempts. To see more records, download the information to a CSV or GZIP file.

Field History Tracking
Select certain fields to track and display the field history in the History related list of an object. The field history data is retained for up to 18 months.

Monitor Setup Changes
Setup Audit Trail tracks the recent setup changes that you and other admins have made to your org. Audit history is especially useful in orgs with multiple admins.

Transaction Security Policies
Transaction Security is a framework that intercepts real-time Salesforce events and applies appropriate actions and notifications based on security policies you create. Transaction Security monitors events according to the policies that you set up. When a policy is triggered, you can receive a notification and have an optional action taken.

Salesforce Platform Data Security Model

Salesforce provides a security model that satisfies real-world business cases, a comprehensive and flexible data security model to secure data at different levels. Salesforce also provides sharing tools to open up and allow secure access to data based on business needs.

Overview

Salesforce provides three layers of security with lots of flexibility to accommodate virtually any business need. Profiles controls object-level and field-level access. Permission sets are used to provide access to additional objects. Field-level security controls provide access to individual fields within an object. Further, there are different types of record-level security: org-wide defaults, role hierarchy sharing, sharing rules and manual sharing.

Object-Level-Security

Before allowing a user access, Salesforce first verifies that the user has permissions to see objects of that type. Object-level access can be managed through two configurations, profiles and permission sets.

Profiles
In Salesforce, profiles control access to object-level and field-level security among other things like apps, tabs, and so on.

Permission Sets
Permission sets are used to provide additional (usually special) permissions to users who are already in a profile.

Record-Level-Security (Record Sharing Rules)

Salesforce provides some ways to share records with others and access others' records.

Organization-Wide Sharing Defaults
In Salesforce, records have a field called "OwnerId" that points to a real user. Owners of records are usually people who created the record and have full CRUD access to it. Salesforce provides other ways to automatically assign ownership to users and to transfer ownership from one user to another user.

Organization-wide defaults (OWD) control the default behaviour of how every record of a given object is accessed by users who do not own the record.

Role Hierarchies
Virtually all companies have an organization structure where groups of people report to their managers and their managers in turn report to their managers, forming a tree-like org chart. In order to simplify sharing, Salesforce provides an easy way to share records with managers. To use this sharing rule, an admin must first add the user to a role and grant access.

Sharing Rules
Hierarchy-based sharing only works for sharing upward and in a vertical direction. Sharing rules provides a way to share records laterally and in an ad-hoc fashion via public groups.

- Ownership-based sharing rules
  Ownership-based sharing rules let admins share records based on role, role-andsubordinate, and public group ownership.

- Criteria-based sharing rules
  Criteria-based sharing rules let users access records based on the value of a field in a record, irrespective of who owns the record.

Manual Sharing (Classic Only)
Record-level-security provides a mechanism to share individual records with others. This permission is accessed through the Sharing button on the record details page, and lets endusers share individual record with others.

Fielo Platform Data Access Security Model

Overview

Fielo helps create, manage and optimize highly scalable channel incentive programs to drive improved performance from partners, resellers and customers. Fielo engine security relies on Salesforce platform data security model. Objects designed to create the incentive programs have their access defined by the user Profile and Permission Sets.

Platform Main Objects

In order to secure different incentive and loyalty data inside the platform, Fielo distributes the information in some main objects.

Programs
Programs establish the general operations settings of your loyalty program. They allow you to manage and develop the Members community that you choose to incentivize. Fielo is multiprogram, which means that it can handle more than one Program at a time. This allows you to create different Programs for different states or countries, build different Fielo Sites for your different Programs and set different Incentives for your different Programs.

Members
Members are the people or entities registered in your Program. They are part of the community that you choose to incentivize. Members are the core of your Program as they interact with it by means of Transactions, Rewards and Redemptions. Fielo Membership model intuitively represents the community of most B2B programs, using Salesforce's Account and Contact structure as a basis.

Transactions
Transactions are actions that grant Points, Badges or Rewards to Members in exchange of performing specific activities. Transactions can be the result of processing a set of Actions or they even may start the processing itself. Access to this object may grant you some transactions general actions like Adjustment Transaction.

Points
Points are single units which can be granted to Members for performing specific activities. Points are configured in Programs and used in Rules or Transactions to redeem Rewards. Point Types comprise different kind of non-monetary Points. They enable to create exchange units based on distance, time, currency, etc. instead of regular numeral Points.

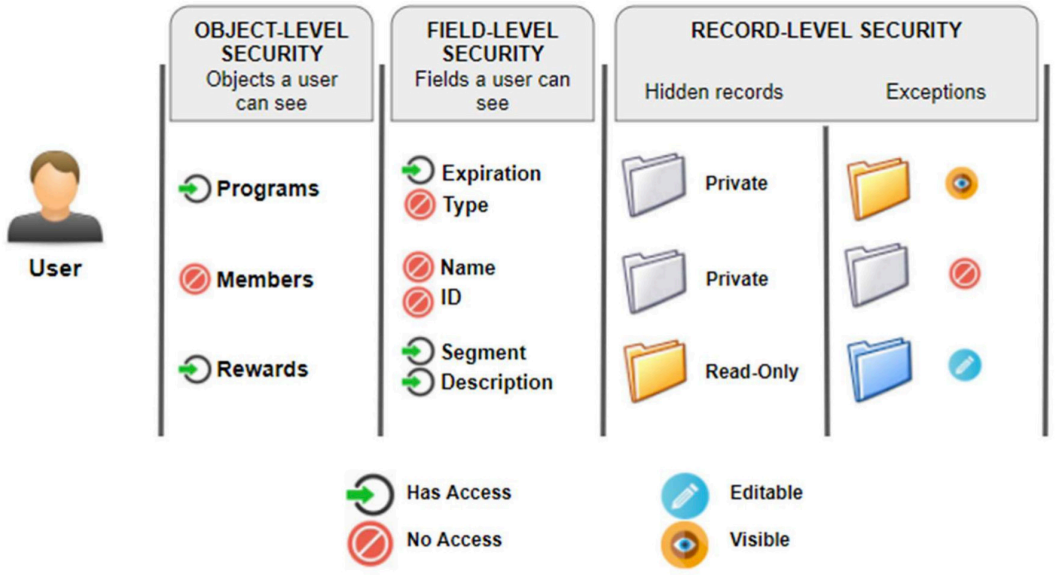
Rewards
Rewards are the prizes available to Members who are part of a Program. Fielo allows you to offer any kind of product or service to incentivize your community: electronic devices, household appliances, travel booking, retail, entertainment, experiences, etc. After completing the assigned Incentives, Members can redeem the Points they have obtained for Rewards.

Redemptions
Redemptions are the orders generated by Members when they redeem their available Points for Rewards. Redemptions may include as many Redemptions Items as Rewards redeemed as each Redemption Item represents a particular redeemed Reward.

Field-Level Security

After set the correct access to the Objects for each User and Member based on their business needs the System Administrator will be able to set the field-level security settings to restrict users' access to view and edit specific fields.

The fields that users see on detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always applies.



Salesforce Data Integration

In general, there are several different ways to integrate separate but related application systems at the data layer. For example, any number of apps can access a single shared database and efficiently manage data in real time. In contrast, when each app must maintain its own database, or when you want to import or export large amounts of data, mechanizing the transfer of data among pertinent systems helps preserve the consistency and quality of data across the entire organization.

Open APIs

At the core level, all Salesforce platforms have open APIs (based on industry-standards such as REST and SOAP) that you can use to integrate Salesforce endpoints (Force.com, Database.com, etc.) with external endpoints such as apps or enterprise integration hubs.

General purpose data integration APIs support applications that need to work with the core data managed by Force.com and Database.com.

- Data integrations via SOAP with the SOAP API
- Data integrations via REST with the REST API
- Data streaming with the Streaming API

Special purpose data integration APIs support applications that need to work with peripheral data models in Force.com and Database.com, or data managed by other Salesforce platforms such as Radian6, Do.com, and Desk.com.

- Social integration with the Chatter REST API
- Listen and engage on social media with the Radian6 API
- Work better with the Do API
- Support customers with the Desk API

Bulk Data Transfer API

The Bulk API provides programmatic access that lets you quickly load data into your Salesforce organization. It is a RESTful API that is optimal for loading or deleting large sets of data. You can use it to query, insert, update, upsert, or delete a large number of records asynchronously by submitting batches that Salesforce processes in the background.

Language-Specific Resources and Toolkits

When working with specific programming languages, several toolkits are available that abstract the core SOAP and REST APIs to support native development approaches and simplify integrations.

- Salesforce Mobile SDK (Android and iOS)
- JavaScript
- Ruby
- PHP
- Java

Cloud-to-Cloud Integration Toolkits

Several toolkits are available to help you integrate Salesforce Platform technologies such as Force.com (and Database.com) with other cloud-based services.

The following toolkits are available:

- Force.com for Amazon Web Services
- Force.com for Facebook
- Force.com for Google App Engine
- Force.com Toolkit for Google Data APIs
- Force.com Toolkit for Microsoft Azure
- PayPal X Toolkit for Force.com

Fielo Platform Integration

Fielo offers numerous incentivization options and can integrate with most third-party reward catalog providers, mobile apps, communities and external sites.

Fielo Platform Rest API

Fielo PLT REST API is a RESTful API that can be used to integrate Fielo Platform with any web or mobile app. Its references contain detailed descriptions about how to create new Members, Redemptions and Transactions, retrieve data from Members, Rewards, Redemptions and Transactions and manage a variety of other requests that an app or site might need to perform.

Authentication
Fielo PLT REST API uses a Salesforce's OAuth 2.0 protocol to allow users to securely access data without revealing user's credentials (username and password).

OAuth allows a client application restricted access to data at a resource server via tokens issued by an authorization server in response to an authorization.

There is a difference between Authentication and Authorization:

- Authentication: Proving correct identity.
- Authorization: Allowing a certain action.

An API might authenticate but not authorize to make a certain request.

The OAuth 2.0 RFC might authorize the client for a read-only access to some subset of data for a limited period of time, after which the authorization becomes invalid. It can even instruct the authorization server to revoke an access token if it decides that no longer wishes the client to have access and doesn't trust it to discontinue on its own.