

Venturelytic

Security Overview



Table of Contents

| | |
|----------------------------|----|
| 1. Platform Basics..... | 1 |
| 2. Storage & Location..... | 3 |
| 3. Manage Data Access..... | 4 |
| 4. Authentication..... | 8 |
| 5. Back-Up Solutions..... | 10 |
| 6. Health Check..... | 12 |
| 7. Security Add-Ons..... | 13 |
| 8. Best Practices..... | 14 |

1. Platform Basics

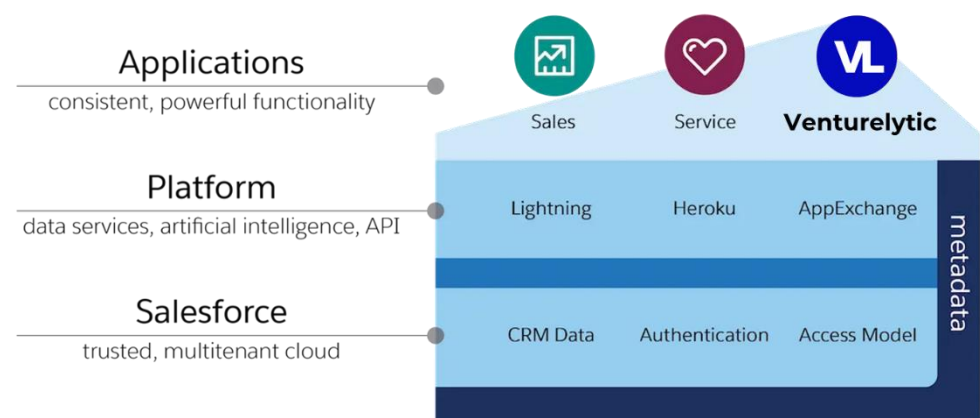
1.1 PLATFORM OVERVIEW

The Salesforce Platform is the preeminent example of a successful cloud computing platform and related ecosystem of applications. Since the turn of the millennium, the platform has been the enabling foundation for:

- Many popular business-purpose applications for common use cases such as sales and customer service
- Industry-specific applications for more specialized use cases such as finance and healthcare
- Millions of custom applications and application extensions for unique use cases

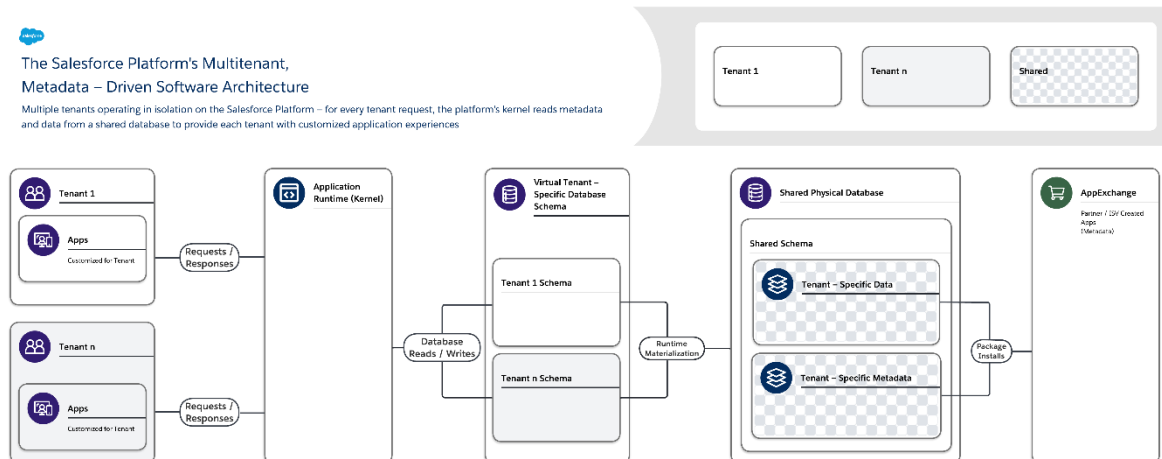
Ready-made solutions are available in AppExchange, the platform's expansive app marketplace. Built by a vast ecosystem of trusted partners and independent software vendors (ISVs), an AppExchange package is metadata from a third-party that describes free or paid-for application extensions and entire applications that you can use to meet specific business requirements.

Venturelytic is one of these Salesforce ISVs, providing investors with a dedicated investor data platform on top of Salesforce in the form of a so-called "managed package".



1.2 PLATFORM ARCHITECTURE

In large part, the Salesforce Platform is so successful and popular because its unique software architecture supports applications that are easy to build, use, customize, and extend with exceptional performance and reliability. The heart of the platform's software architecture is its multitenant, metadata-driven design.



The Salesforce Platform's software architecture is:

- Multitenant — It isolates and concurrently supports the varying requirements of many tenants (organizations, business units, and so on).
- Metadata-driven — It lets every tenant easily and quickly customize their apps and user experiences using metadata, data that describes elements such as the user interface (UI) and business logic.

When you create a new application object or write some code using the Salesforce Platform, the platform does not create an actual table in a database or compile any code. Instead, the platform simply stores some metadata that the it can then use at runtime to dynamically materialize virtual application components. The platform ensures that every tenant's metadata is private and easy to update without any locking or downtime required so that every tenant can build and customize apps in isolation. The Salesforce Platform uses the same metadata to provide custom APIs, RESTful and web services (SOAP-based) interfaces you can use to integrate your applications with other applications and automated processes.

To support this highly customizable and extensible architecture, a single instance of the Salesforce Platform uses:

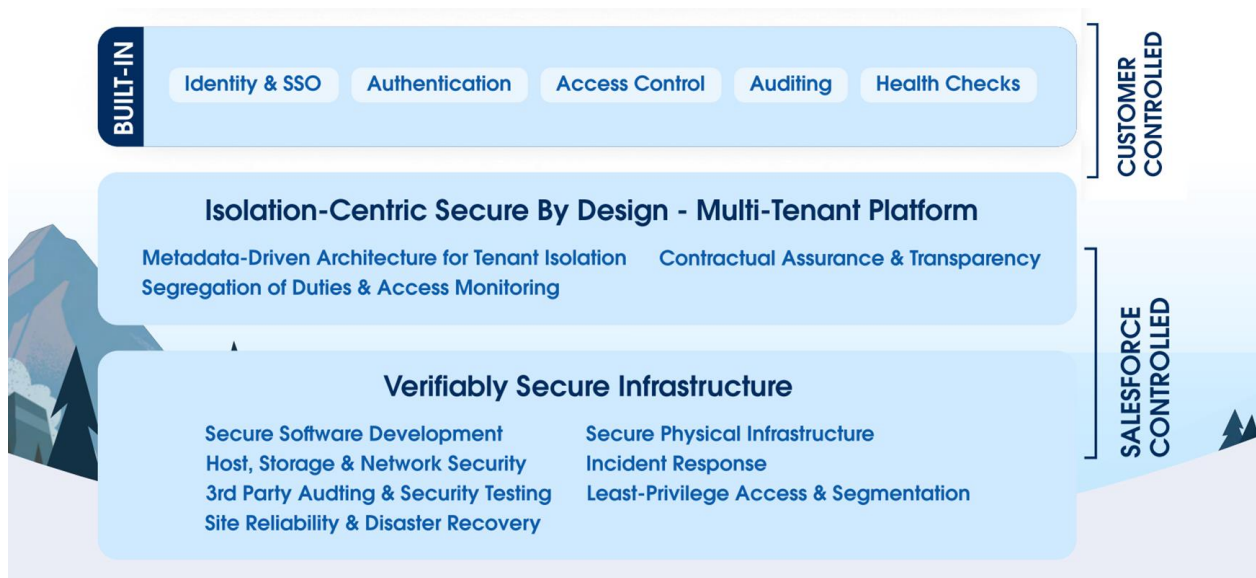
- A single shared multitenant database with a single schema that stores tenant-specific metadata and data.
- A multitenant kernel (application runtime) that reads metadata and data to dynamically provide tenant-specific applications, business logic, and APIs for each tenant's users at runtime.

This clear separation of the Salesforce-managed kernel from tenant-managed metadata makes it possible for Salesforce, tenants, and ISVs to independently evolve their portions of the system without interference.

For more information on the on the platform's multitenant architecture, please see: <https://architect.salesforce.com/fundamentals/platform-multitenant-architecture>

1.3 PLATFORM SECURITY

The figure below provides an overview of Salesforce's security infrastructure. The two blocks below outline both the measures taken by Salesforce to provide clients with a secure platform, as well as the design of the platform. Next to these Salesforce controlled measures, customers of Venturelytic and Salesforce are provided with a set of built-in tools to keep their environment secure. These tools are discussed in more detail in the other chapters.



2. Storage & Location

2.1 INFRASTRUCTURE BASIS

Every Salesforce environment relies on a common collection of data and metadata (code and configurations for customizing Salesforce) called your "Org" (short for "organization"). Each Org primarily belongs to a single instance, which is either on:

1. First-Party Infrastructure (owned and operated by Salesforce);
2. Public Cloud Infrastructure (hosted on Salesforce-managed AWS infrastructure that is not Hyperforce); or
3. Hyperforce Infrastructure (hosted on Salesforce-managed AWS Hyperforce Infrastructure)

Generally, a customer has only one Org to support all of the Services that rely on that Org. In other words, your Org can either be on Salesforce's First-Party Infrastructure, or on Salesforce's Public Cloud Infrastructure, or on Salesforce's Hyperforce Infrastructure, but it will only be on one of these.

2.2 SELECTION OF INSTANCE

At the moment client selects Venturelytic as its software provider by means of signing the SaaS Subscription Agreement, Venturelytic will create a Org for client with the preferred instance. This means, client has the option to select the instance it prefers its application to run on.

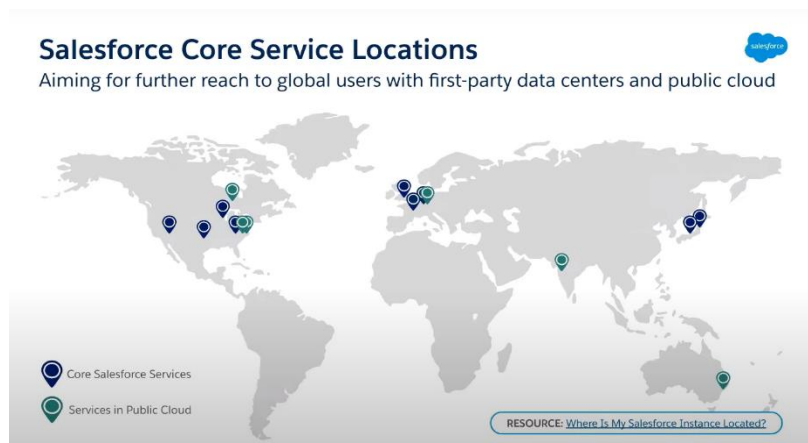
For an overview of the location of the instances, please check:

<https://help.salesforce.com/s/articleView?id=000382217&type=1>

2.3 LOCATION OF INSTANCES

Salesforce manages instances from multiple geographically diverse data centers to avoid single points of failure in their infrastructure. This design supports the continuous availability our customers.

At any given time, your Salesforce instance is actively served from one location with transactions replicated in near real-time across two or more availability zones in completely redundant, separate locations. Salesforce regularly site switches between the locations for maintenance, compliance, and disaster recovery purposes.



3. Manage Data Access

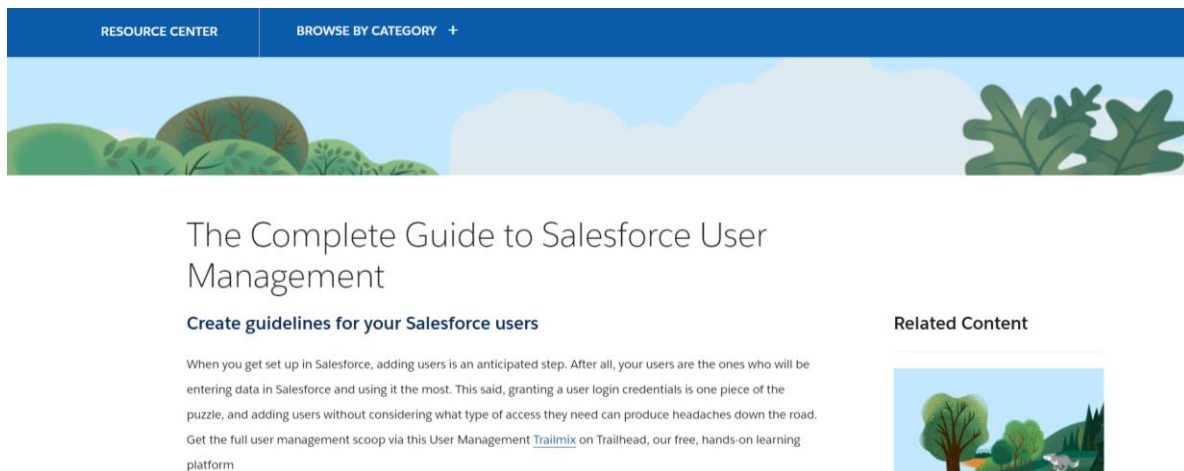
3.1 USER MANAGEMENT

Once an environment has been created by Venturelytic, your organization will be assigned one or multiple so-called administrators (admins) that are your in-house managers of the Venturelytic environment.

Your administrator(s) will be able to add new users to the environment, as well as assigning these users with the right profiles, roles, and data access.



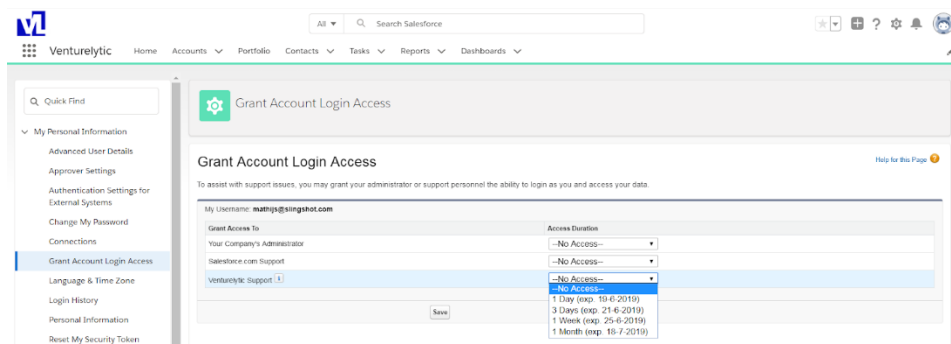
Salesforce created a comprehensive user management strategy that incorporates best practices and can be found here: <https://www.salesforce.com/resources/guides/salesforce-user-management-guide/>



For more info on the future of user management in Salesforce:
<https://admin.salesforce.com/blog/2022/the-future-of-user-management>

3.2 GRANT LOGIN ACCESS

Companies or people outside of your organization that are neither administrators nor users in your environment have no access to your application by default. This also holds for Venturelytic and Salesforce. In case you require our assistance, our support departments may ask you to "Grant Login Access" in order to assist you with a question, issue, or request.



Via the "Grant Login Access" functionality, our support departments can log in to the application using your login to troubleshoot and fix issues stemming from your inquiry. For security reasons, this functionality does not allow Venturelytic or Salesforce to make exports from your reports, thereby preventing support users from exporting valuable data into other sources outside of the Salesforce platform.

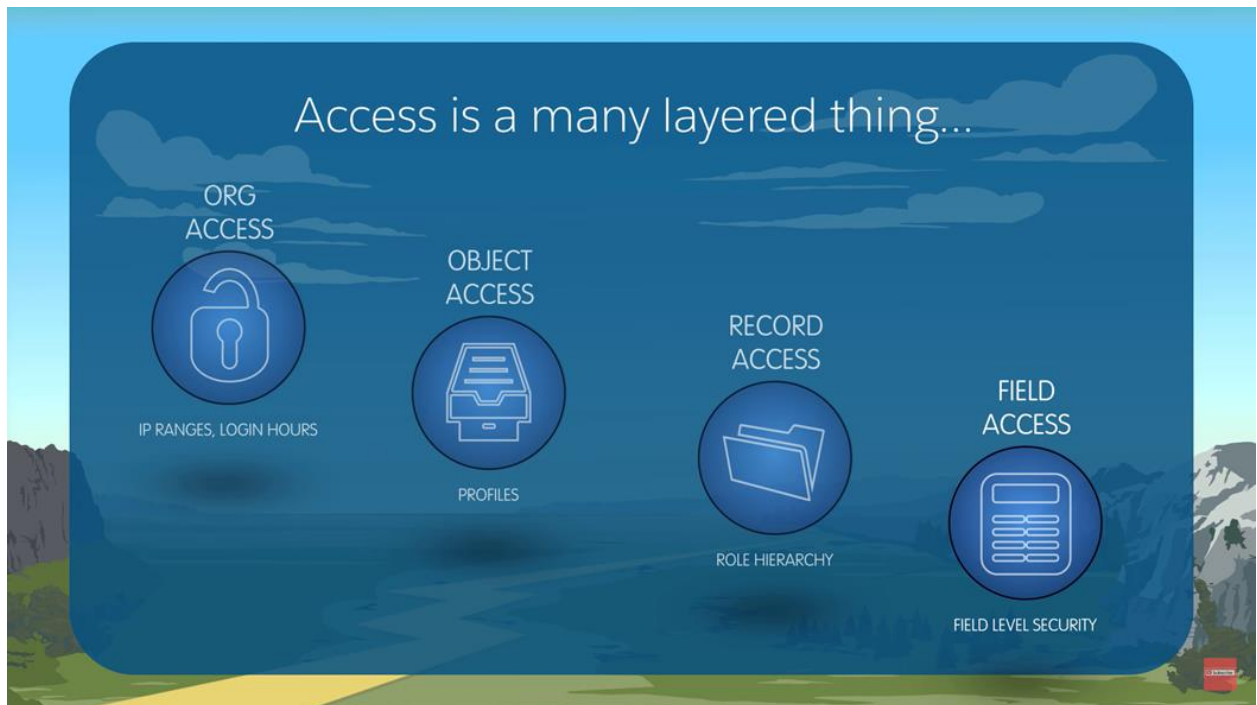
Last but not least, no one within Venturelytic or Salesforce support may log in to your org to resolve issues without this explicit permission and duration for the access.

3.3 LAYERS OF ACCESS

Salesforce provides a flexible, layered data sharing design that lets admins control user access to data. Managing data access enhances security by exposing only data that's relevant to users. Use permission sets, permission set groups, and profiles to control the objects and fields users can access. Use organization-wide sharing settings, user roles, and sharing rules to specify the individual records that users can view and edit.

Salesforce distinguishes the following layers of access:

- **Object-Level Security via Permission Sets and Profiles**
Object-level security—or object permissions—provide the bluntest way to control data access. You can prevent a user from seeing, creating, editing, or deleting any instance of a particular object type, such as a lead or opportunity, by using object permissions. You can hide tabs and objects from selected users, so that they don't even know that type of data exists. You can specify object permissions in permission sets and profiles.
- **Field-Level Security via Permission Sets and Profiles**
Sometimes you want users to have access to an object while limiting their access to individual fields in that object. Field-level security—or field permissions—control whether a user can see, edit, and delete the value for a particular field on an object. You can protect sensitive fields without hiding the entire object. You also can control field permissions in permission sets and profiles.
- **Record-Level Security via Role Hierarchy and Sharing Rules**
After setting object- and field-level access permissions, you can configure access settings for records. Record-level security lets you give users access to some object records, but not others. Every record is owned by a user or a queue. The owner has full access to the record. In a hierarchy, users higher in the hierarchy always have the same access to users below them in the hierarchy. This access applies to records owned by users and records shared with them. To specify record-level security, set your organization-wide sharing settings, define a hierarchy, and create sharing rules.



3.4 INSTRUMENTS TO MANAGE ACCESS

Find more information on the specific measures that can be taken below:

1. [User Permissions and Access](#)
User permissions and access settings are specified in profiles and permission sets. To use them effectively, understand the differences between profiles and permission sets.
2. [User Access Policies \(Beta\)](#)
With user access policies, you can declaratively define aggregated access for your users in a single operation. You can specify a set of users to grant or revoke access to permission set licenses, permission sets, and permission set groups, package licenses, queues, and groups. You can also create a policy to automatically assign access when creating or updating users.
3. [Profiles](#)
Profiles define how users access objects and data, and what they can do within the application. When you create users, you assign a profile to each one.
4. [Permission Sets](#)
A permission set is a collection of settings and permissions that give users access to various tools and functions. Permission sets extend users' functional access without changing their profiles.

5. [Sharing Settings](#)

In Salesforce, you can control access to data at many different levels. For example, you can control the access your users have to objects with object permissions. Within objects, you can control the access users have to fields using field-level security. To control access to data at the record level, use sharing settings and restriction rules.

6. [Restriction Rules](#)

Restriction rules let you enhance your security by allowing certain users to access only specified records. They prevent users from accessing records that can contain sensitive data or information that isn't essential to their work. Restriction rules filter the records that a user has access to so that they can access only the records that match the criteria you specify.

7. [Scoping Rules](#)

Scoping rules let you control the records that your users see based on criteria that you select. You can set up scoping rules for different users in your Salesforce org so that they can focus on the records that matter to them. Users can switch the set of records they're seeing as needed.

More information on managing data access can be found here:

https://help.salesforce.com/s/articleView?id=sf.security_data_access_mgmt.htm&type=5

4. Authentication

Authentication means preventing unauthorized access to your organization or its data by making sure each logged in user is who they say they are. The following authentication measures can be taken by Venturelytic's clients in collaboration with Venturelytic.

1. [Multi-Factor Authentication](#)

Multi-factor authentication (MFA) is a secure authentication method that requires users to prove their identity by supplying two or more pieces of evidence (or factors) when they log in. One factor is something the user knows, such as their username and password. Other factors include something the user has, such as an authenticator app or security key. By tying user access to multiple types of factors, MFA makes it much harder for common threats like phishing attacks and account takeovers to succeed.

2. [Single Sign-On](#)

Single sign-on (SSO) is an authentication method that enables users to access multiple applications with one login and one set of credentials. For example, after users log in to your org, they can automatically access all apps from the App Launcher. You can set up your Salesforce org to trust a third-party identity provider to authenticate users. Or you



can configure a third-party app to rely on your org for authentication.

3. [Custom Login Flows](#)

A login flow directs users through a login process before they access your Salesforce org or Experience Cloud site. You can use a login flow to control the business processes that your users follow when they log in to Salesforce. After Salesforce authenticates a user, the login flow directs the user through a process such as enforcing strong authentication or collecting user information. When users complete the login flow successfully, they're redirected to their Salesforce org or site. If unsuccessful, the flow can log out users immediately.

4. [Connected Apps](#)

A connected app is a framework that enables an external application to integrate with Salesforce using APIs and standard protocols, such as SAML, OAuth, and OpenID Connect. Connected apps use these protocols to authenticate, authorize, and provide single sign-on (SSO) for external apps. The external apps that are integrated with Salesforce can run on the customer success platform, other platforms, devices, or SaaS subscriptions. For example, when you log in to your Salesforce mobile app and see your data from your Salesforce org, you're using a connected app.

5. [Manage User Passwords](#)

Salesforce provides each of your users with a unique username and password that they enter at each login. As an admin, you can configure several settings to ensure that your users' passwords are strong and secure.

6. [Device Activation](#)

With device activation, Salesforce challenges users to verify their identity when they log in from an unrecognized browser or device or from an IP address outside of a trusted range. By adding extra verification to unfamiliar login attempts, device activation keeps your orgs and Experience Cloud sites secure.


7. [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.




5. Back-Up Solutions

Salesforce provides customers with multiple ways to back-up their data, and Venturelytic helps you selecting the best solution given the nature of your business.



Backup and Recovery Offerings

Native options and more

| Native | Platform-Aware | Third Party |
|---|---|---|
| <ul style="list-style-type: none"> • Data Export Services • Report Export • Data Loader • Data Import Wizard • Full Sandbox • Recycle Bin • Backup & Restore <p>Salesforce APIs:</p> <ul style="list-style-type: none"> • Metadata API • Bulk API • SOAP API | <ul style="list-style-type: none"> • Heroku Connect • Mulesoft <p>AppExchange Partners:</p> <ul style="list-style-type: none"> • Relational Junction • Spanning by EMC • Odaseva • OwnBackup | <p>Middleware:</p> <ul style="list-style-type: none"> • Informatica • Jitterbit • WebSphere Cast Iron • Boomi AtomSphere <div style="text-align: center; margin-top: 20px;">  </div> |

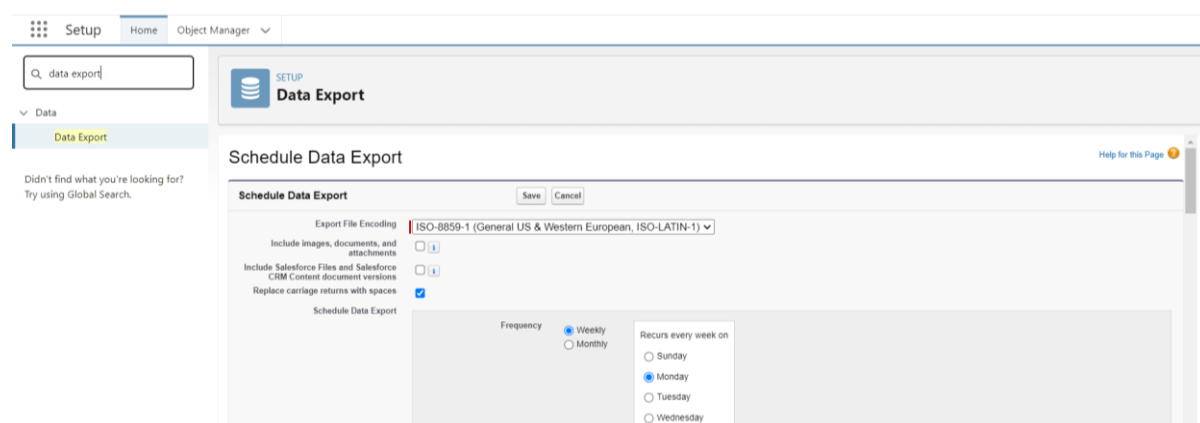
5.1 NATIVE SALESFORCE SOLUTIONS

5.1.1 BACKUP AND RESTORE

Salesforce's most comprehensive backup solution. Backup & Restore is a paid add-on, and will automatically backup, as well as restore your data in the event of data loss.

5.1.2 DATA EXPORT SERVICE

Allows you to perform a manual or scheduled backup of your data via the Salesforce UI. This will organize your data into a set of CSV files. This service can export your data on a weekly basis.



The screenshot shows the 'Setup Data Export' configuration page in Salesforce. The 'Schedule Data Export' section is active, showing settings for export file encoding (ISO-8859-1), including images, documents, and attachments, and including Salesforce CRM content document versions. The frequency is set to Weekly, recurring every week on Monday.

More information can be found here:

https://help.salesforce.com/s/articleView?id=sf.admin_exportdata.htm&type=5

5.1.3 DATA LOADER

This allows you to export data using the Data Loader. This option requires more manual steps but does give you more control over the data you are exporting.

5.1.4 REPORT EXPORT

A simple way to export data out of Salesforce using the reports interface.

The main differences between the out of the box data export feature and Salesforce paid Backup & Restore functionality is the possibility for clients to backup both data and metadata on a daily basis in the paid add-on.

More information on creating your back-up strategy can be found in this video:

https://www.youtube.com/watch?v=7Bv429T_odI

| Salesforce Tools Feature Comparison | | | |
|-------------------------------------|---|--|---|
| Backup methods you can trust | | | |
| | Features | Benefits | Limitations |
| Data Export | <ul style="list-style-type: none"> Generate backup files on a weekly or monthly basis Export all of your data into a set of comma-separated values (.csv) files | <ul style="list-style-type: none"> Good for backing up data on a regular basis Good for smaller orgs Export data on an ad hoc basis | <ul style="list-style-type: none"> Does not include metadata Heavy traffic may delay delivery |
| Backup & Restore | <ul style="list-style-type: none"> Backup org's data on a daily basis Restore data using criteria-based and time-based filters Leverages Bulk API | <ul style="list-style-type: none"> Managed package developed and updated by Salesforce Completes data backups more frequently than other native tools Backups do not count against org API limits | <ul style="list-style-type: none"> Metadata backup/restore on product roadmap |

5.2 THIRD PARTY SOLUTIONS

Salesforce AppExchange partners have been building their solutions long before Salesforce announced their Backup & Restore product at the end of 2021. This means that the third-party solutions below are arguably more comprehensive, and in most cases will back up data and metadata.

- OwnBackup: The market leader when it comes to Salesforce Backup. OwnBackup has over 4,000+ customers and provides comprehensive backup and recovery solutions.
- Spanning Backup: Established player in the Salesforce Backup space. They've been around since 2010, have a comprehensive platform, and also provide backup for GSuite & Microsoft 365.
- Gearset: one of the leading DevOps platforms for Salesforce. They also have a comprehensive platform for data and metadata backup.




Grow along with your investments

- AutoRABIT's: Salesforce DevOps platform includes a data protection tool called Vault that provides off-platform backup and recovery for Salesforce data and metadata structures.
- Odaseva: has a slightly different angle, selling themselves as an "Enterprise-proven Salesforce data management" solution. This includes data backup, as well as data privacy and compliance tools.
- Veeam: A global leader in backup is now available for Salesforce. Veeam Backup for Salesforce gives you the power to control where your data is stored. On-premises, in AWS, Azure, and more.

6. Health Check

Health Check is one of the additional built-in and customer controlled security measures provided by Salesforce. Health Check gives you visibility into all of your org's security settings and allows you to identify and fix vulnerabilities in your security settings, all from a single page. A score shows how "healthy" your org's security is, on a scale from 0-100 (100 being the most secure). The score is calculated by measuring how closely your org's security settings (the Your Value column) align with Salesforce's recommended settings (the Standard Value column).










Health Check

How well does your org meet Salesforce security standards? Reduce your security risk and limit data loss by optimizing the areas below.

Salesforce Baseline Standard ⌵ ⌵ Fix Risks

79% Good

of the standard met
[How did we calculate this score?](#)

| STATUS | SETTING | GROUP | YOUR VALUE | STANDARD VALUE | ACTIONS |
|-----------|--|--|---|---|--|
| Critical | Maximum invalid login attempts | Password Policies | No Limit | 3 | Edit  |
| Critical | Number of Objects with Default External Access Set to Public | Sharing Settings | 169 | 0 | Edit  |
| Compliant | Expired Certificate | Certificate and Key Management | 0 | 0 | Edit  |
| Compliant | Number of security risk file types with Hybrid behavior | File Upload And Download Security Settings | 0 security risk file types with Hybrid behavior | 0 security risk file types with Hybrid behavior | Edit  |
| Compliant | Lock sessions to the domain in which they were first used | Session Settings | Enabled | Enabled | Edit  |
| Compliant | Let users verify their identity by text (SMS) | Session Settings | Enabled | Enabled | Edit  |
| Compliant | Enable clickjack protection for Setup pages | Session Settings | Enabled | Enabled | Edit  |
| Compliant | Enable clickjack protection for non-Setup Salesforce pages | Session Settings | Enabled | Enabled | Edit  |

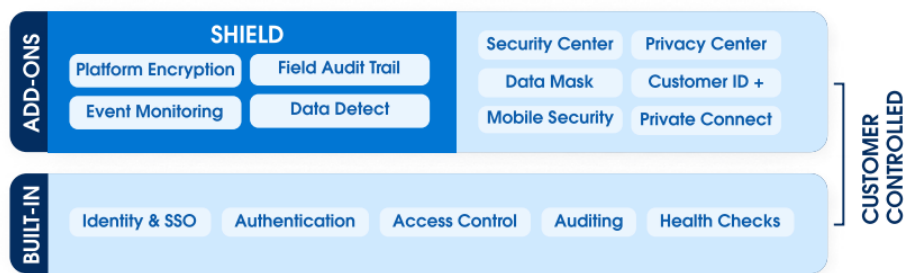


7. Security Add-Ons

7.1 SALESFORCE SHIELD

Shield is a suite of capabilities that provides an extra level of security and protection above and beyond what's already baked into Salesforce. With Salesforce Shield, you can ensure the sensitive data in your Salesforce environment is safe. Salesforce Shield Platform Encryption, Event Monitoring, and Field Audit Trail. For more information:

<https://www.salesforce.com/products/platform/products/shield/>



There is also a "classic encryption" feature that lets you protect only a special type of custom text field, which you create for that purpose.

https://help.salesforce.com/s/articleView?id=sf.security_pe_vs_classic_encryption.htm&type=5

7.2 EXTENSIONS FOR LARGER ORGANIZATIONS

Salesforce provides multiple additions to its core platform, with the two mentioned below being the most relevant for larger organizations.

7.2.1 SECURITY CENTER

The Salesforce Security Center is designed for clients managing multiple Orgs that require a simpler overview of all security configurations across all Salesforce environment. By connecting various Salesforce orgs (including Sandbox orgs) to a central org running Security Center, you'll have increased visibility into your security posture. Bringing key security metrics from all of your orgs into a single interface reduces the amount of time it takes to truly understand your overall security posture. For more information:

<https://www.salesforce.com/products/platform/products/security-center/>

7.2.2 PRIVACY CENTER

Privacy Center makes it easy to manage how your Salesforce org retains, deletes, anonymizes, and transfers customer data. Use customizable features to meet data privacy laws like GDPR, CCPA, and CPRA. See all privacy relevant data in one place – this includes your customers' opt-ins for emails and texts. Then, manage that data with a single click based on your customers' wishes or changes in regulation. This is mainly relevant for customers using one of Salesforce's marketing solutions, and less for dedicated Venturelytic users. For more information:

<https://www.salesforce.com/products/platform/products/privacy-center/>

8. Disaster Recovery

8.1 RISK MANAGEMENT TEAM

Venturelytic has appointed an internal risk management team that is mobilized when an incident or event occurs. These members are responsible for evaluating the situation and responding accordingly. The team receives an annual training and is updated when new practices have been established.

8.2 ANNUAL RISK ASSESSMENT

Venturelytic conducts an annual risk assessment to identify and evaluate key risks facing the company's operations. For every new client, the Venturelytic team internally registers relevant security considerations that serve as a resource during implementation, customer success and ad-hoc situations potentially posing a risk.

8.3 SHARED RESPONSIBILITY MODEL

Moving business processes and applications to the cloud creates a shared responsibility model between Venturelytic's customers, Venturelytic and Salesforce. This shared model maximizes efficiency and flexibility while maintaining a high level of security. Venturelytic manages and controls its applications and related services. This includes change management, incident management, product updates and patch management related to the Venturelytic applications. Salesforce operates, manages and controls the components from the API level down to the host operating system, underlying databases and physical security of data centers in which the services operate. For details on Salesforce security, see trust.salesforce.com and search "security" on help.salesforce.com.

Customers are responsible for user access and authorization, control and backup of data uploaded to the Venturelytic applications, as well as configuration of the underlying Salesforce platform in accordance with their requirements. Customers can also enhance the security of their Venturelytic implementation and address security and compliance requirements by leveraging security features of the Force.com platform that are extensively described in the other chapters of this guide.

8.4 SALESFORCE DISASTER RECOVERY PLANS

As client data resides on the client's instance of Salesforce, and Venturelytic provides client with the application on top of the Salesforce's infrastructure, Salesforce's disaster recovery plan is relevant to client. A summary of the plan can be found here: <https://compliance.salesforce.com/en/documents/a005A00000k4ayeQAA>. A broader set of compliance documents, can be found here: <https://compliance.salesforce.com/en>.



8.5 RECOVERY TIME AND POINT OBJECTIVE METRICS

Because Salesforce provides the infrastructure and all customer data entered into Venturelytic applications resides directly on the client's Salesforce instance, recovery time and point objective are passed down from Salesforce. The Salesforce Services' disaster recovery plans currently have the following target recovery objectives: (a) restoration of the Salesforce Service within 12 hours (RTO) after Salesforce's declaration of a disaster; and (b) maximum Customer Data loss of 4 hours (RPO); 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.

8.6 COMMUNICATION

All customers can review status for their environment on <https://status.salesforce.com>. Furthermore, administrators of potentially impacted Venturelytic's clients will be notified by Salesforce on the issue by email. A representative of the Venturelytic risk team will directly contact client's main contact person on the procedure that will be followed to minimize damages.



9. Best Practices

Other than the measures described in the chapters before, the following best practices could be followed by Venturelytic clients:

- Stay Informed About Certificate Rotations and Renewals
Salesforce does not recommend pinning leaf or intermediate SSL/TLS certificates, because they may create availability issues when intermediate certificates are rotated during routine operations. However, there may be certain use cases involving middleware integrations that may require certificates to be pinned. If you are pinning leaf/intermediate certificates, please consider only pinning the root certificate. To receive timely notifications on upcoming certificate rotations and renewals, join the Certificate Changes Trailhead Community and subscribe to the group email updates.

For more info: <https://trailhead.salesforce.com/trailblazer-community/groups/0F93000000001oAF?tab=discussion>

- Set Login IP Ranges
Login IP Ranges limit unauthorized access by requiring users to login to Salesforce from designated IP addresses — typically your corporate network or VPN. By using Login IP Ranges, admins can define a range of permitted IP addresses to control access to Salesforce. Those who try to login to Salesforce from outside the designated IP addresses will not be granted access.
 - If you are using Professional, Group, or Personal editions, you can configure Login IP Ranges under Security Controls > Session Settings.
 - If you are using Enterprise, Unlimited, Performance, or Developer editions, you can configure Login IP Ranges under Manage Users > Profiles.

For more information:

https://help.salesforce.com/apex/HTViewHelpDoc?id=login_ip_ranges.htm

- My Domain
My Domain allows you to add a custom domain to your Salesforce org URL. Having a custom domain lets you highlight your brand and makes your org more secure. Additionally, this allows you to follow our best practices of not specifying instance names in code and integrations (e.g. na1.salesforce.com). Following this best practice will provide you and your end-users a more seamless experience during any future maintenance.

Using My Domain, you define a custom domain that's part of your Salesforce domain. A custom domain is actually a subdomain of a primary domain. If we use an example of Universal Containers, their subdomain would be "universal-containers" in this My Domain example: <https://universal-containers.my.salesforce.com>.



A custom domain name helps you better manage login and authentication for your org in several key ways. You can:

- Block or redirect page requests that don't use the new domain name
- Set custom login policy to determine how users are authenticated
- Work in multiple Salesforce orgs at the same time
- Let users log in using a social account, like Google and Facebook, from the login page
- Allow users to log in once to access external services
- Highlight your business identity with your unique domain URL
- Brand your login screen and customize right-frame content

For more information:

https://help.salesforce.com/apex/HTViewHelpDoc?id=domain_name_overview.htm&language=en_US

- Decrease Session Timeout Thresholds

Users sometimes leave their computers unattended or they don't log off. You can protect your applications against unauthorized access by automatically closing sessions when there is no session activity for a period of time. The default timeout is 2 hours; you can set this value from between 30 minutes and 8 hours. To change the session timeout, click: Setup > Security Controls > Session Settings.

For more information: https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/security_overview_sessions.htm?search_text=session%20timeout

- Enable TLS 1.2 or higher

Transport Layer Security, or TLS, is the most widely deployed security protocol for web browsers and other applications that require data to be securely exchanged over a network. As of October 2019, Salesforce requires all secure org connections to use TLS 1.2 or higher to ensure the most secure environment and continued payment card industry compliance.

For more information: https://releasenotes.docs.salesforce.com/en-us/summer19/release-notes/rn_security_other_changes.htm#rn_security_tls_disable_cruc

- Password Policies

Strong password security is an important step in protecting your Salesforce accounts and Salesforce recommends these best practices:

- Password expiration – Salesforce recommends no more than 90 days to force users to reset their passwords
- Password length – Salesforce suggestions minimum password length of 8-10 characters



- Password complexity – Admins should require users to include a mix of alpha, numeric, and special characters in their Salesforce password

In addition, remind users to never reuse passwords on multiple accounts, or they risk compromise of more than one of their accounts. Last, users need to understand that they must never share passwords with anyone, either online or in person -- this includes their Salesforce password.

For more information:

https://help.salesforce.com/articleView?id=security_overview_passwords.htm&type=5

- Educate Users about Phishing

