



Cirrus Insight

Earning Your Trust



We built Cirrus Insight to respect and protect your data. We utilize OAuth 2.0 authentication with Salesforce, Microsoft Office 365, and Google for Work. We use SSL for secure transmission of data between platforms. And we do regular third-party security audits by Bishop Fox. We also participate in the EU–U.S. Privacy Shield Framework.

Authentication

- Our product uses OAuth for user authentication. We never have access to Salesforce, Google, Microsoft, Apple, or Android passwords.
- Cirrus Insight for iPhone and iPad encrypts the mail login credentials in the keychain just like the native Apple Mail app.
- Cirrus Insight supports Single Sign On (SSO) and SAML (Security Assertion Markup Language).
- Support for Salesforce Sandbox
- OAuth support for Community, Partner Portal, and Chatter licenses
- HTTP Strict Transport Security which declares that complying web browsers are to interact with Cirrus Insight using only secure HTTPS connections.

Granting Permission

- If you're installing Cirrus Insight for Gmail in a Chrome web browser, you'll see a notice about granting Cirrus Insight permission to run on two specific domains: mail.google.com and secure3.cirrusinsight.com which enables Cirrus Insight to run securely inside Gmail.
- Without your explicit authorization, Cirrus Insight cannot access your Salesforce data. After installing Cirrus Insight you'll be asked to sign in via Salesforce and to approve our request for access. This is called the "OAuth handshake." We tell Salesforce what level of access we need to provide the Service which is called the "scope."

The levels of access that we request are:

- "id" so we can identify you.
- "api" so we can search Salesforce and create leads and contacts and other records when you want.
- "refresh_token" so we can get a new session with Salesforce on your behalf and run background jobs for you like email sync and calendar sync.
- "web" so we can take you to a specific record in Salesforce without forcing you to sign in every time.

Please note:

- We can't do anything you can't do. For example, if you don't have access to edit Contacts in Salesforce, you won't be able to edit a Contract record in Cirrus Insight.
- We can do almost everything you can do. If you can see every Account in Salesforce, our API access gives us the ability to search every Account on your behalf.
- You can revoke our access at any time from your Salesforce user record. More information.

Encryption

- Data in transit is encrypted via SSL (Secure Socket Layer).
- Sensitive data stored is encrypted using an AES 256 cipher.

Data We Collect

- User profile information (name, email address, etc.)
- OAuth refresh tokens (encrypted)
- Salesforce configuration information including time zone, language preference, and profile and permission set.
- As you use Cirrus Insight, we collect data about the features in use. We use this data to populate your Cirrus Insight Dashboard, assist with customer support, and plan for future features.
- We use the payment processor Stripe for credit card payments. When you enter your credit card information on our site, the information is sent directly to Stripe. Your credit card number is never sent to Cirrus Insight servers.

Access to Systems

- All interaction between Cirrus Insight and third-party platforms (e.g. Salesforce, Google, Microsoft) occurs over a secure HTTPS connection.
- We host our systems on industry-leading cloud infrastructure services including Amazon Web Services.

Incident Response and Remediation

- We monitor our systems 24/7/365 with several performance measurement and error-checking tools such as New Relic.
- If an incident causes downtime, we post the update to the Cirrus Insight status page. We also monitor the health dashboards for Salesforce and Google and Amazon from the status page.
- Should a security incident occur, we will notify affected users of the nature and extent of the breach, and take steps to minimize any damage. There have been no security incidents to date.

Data Confidentiality

- Cirrus Insight does not rent, sell, trade or disclose your Personal Information to third parties without your consent.
- Access to customer data by Cirrus Insight employees is limited based on the need to access such data (e.g. to resolve a customer support ticket).
- When requested, we will destroy a user's account, removing all customer data associated with that account.
- Cirrus Insight adheres to the permissions assigned to user profiles in the customer Salesforce org.

Vulnerability Management

- We perform regular internal vulnerability scans of our applications using accredited industry standard tools including the BURP scan.

Third-Party Security Reviews

- We passed the Salesforce Security Review starting in December 2011, and we are listed on the Salesforce AppExchange. We have 1,300+ reviews on the AppExchange, making Cirrus Insight the third most reviewed application of all time behind DocuSign and EchoSign.
- We are Google for Work Premier Partner and we are listed on the Chrome Web Store.
- We are a member of the Microsoft Partner Network and we are listed on the Office Store.
- We are an Apple Partner and we are listed on the iTunes App Store.
- We are a Google Partner and we are listed on the Google Play Store.
- We are self-certified in the U.S.-EU Safe Harbor program managed by the US Department of Commerce.
- We commission third-party application and network security audits by a leading security firm.

Mobile

- Salesforce OAuth 2.0 authentication
- Supports Salesforce 2-factor authentication
- Supports SSO
- Email sign in token is stored encrypted in the device keychain (same as native email applications)
- Supports offline access. Salesforce actions will be transmitted when connectivity is re-established.

Cookies

A cookie is a small amount of data, which often includes an anonymous unique identifier, that is sent to your browser from a web site's computers and stored on your computer's hard drive.

Cookies are required to use the Cirrus Insight service.

Disclosure

- We may disclose personally identifiable information under special circumstances, such as to comply with subpoenas or if your actions violate the Terms of Service.

Email Tracking and Link Tracking

- Cirrus Insight optionally includes Email Tracking and Link Tracking features. Cirrus Insight customers may enable or disable email tracking and link tracking in the Cirrus Insight administrator dashboard.
- The usage of tracking functionality is consistent with industry standards. If a Cirrus Insight customer enables Email Tracking, Cirrus Insight embeds a small transparent image pixel in the out going email. If the email is opened, Cirrus Insight may be able to inform the user about who opened the email, when it was opened, and where it was opened. If Link Tracking is enabled, Cirrus Insight re-writes the link URL so that it is trackable. If the link is clicked by the recipient, Cirrus Insight may be able to inform the user about who clicked on the link, when it was clicked, and the general location of the visitor when they clicked the link.
- Email recipients may block email open tracking via the settings on their email client or by using a pixel-blocking extension.

Email Search

- When you open or compose an email message, we search for the sender's or recipient's email address in Salesforce and return information about the Lead or Contact. All communication between your browser and our servers is protected by the same level of SSL encryption that banks use for online banking services.
- When we search Salesforce for information about a specific email address, we return information about related Activities, Account, Opportunities, Cases, and other relevant records. Each new query typically takes 2-3 API calls so we cache the data in RAM (data is not written to disk) for a period of 5-10 minutes. As a result, any searches for an email address in the cache will be returned from the cache making for a much faster response for the user and many fewer API calls for the organization. When the cache expires, the data is permanently deleted.

Email Sync

- When you save/sync an email to Salesforce, the email is encrypted and sent to our servers where we search Salesforce for matching Contact(s) and then save it into Salesforce related to the right Contact(s). We do not store the email.

Email Attachments

- If you enable our attachments feature, you can save attachments from Gmail, Outlook, and/or mobile to Salesforce. We never save file attachments to our server.
- Additionally, we also support saving Google Drive attachments with an email to Salesforce.

- Saving Google Drive attachments does not require any additional permission. A link to the file in Google Drive can be saved into the email Activity or into Chatter in Salesforce.

Calendar Sync

- Calendar Sync app keeps your Google, Outlook, and/or Mobile calendars in sync with Salesforce. In order to keep everything straight, we store the event IDs for each calendar and a list of the attendee emails for each event so that we can sync attendees. All information about the events is deleted from our database when the events are outside our sync window (e.g. 2 weeks in the past for default calendar sync service).

3rd Party Services

- To provide the best experience and level of service, we utilize a number of third party services to monitor systems and track application usage such as New Relic and Zuora.
- We may also partner with other cloud software providers to bring additional features to users of Cirrus Insight. Currently, we partner with RingLead to provide a service that allows Cirrus Insight to extract contact information from the email signature when a user wants to create a new Lead or Contact. RingLead does not store any transmitted data. Additionally, the feature may be enabled or disabled by the organization administrator and/or on an individual user basis.

Our Continuing Commitment

We are continuously improving Cirrus Insight to take advantage of new technologies as well as new capabilities of the Salesforce, Google, and Microsoft platforms.