Analytics Platform Setup Guide

Salesforce, Winter '19

CONTENTS

ANALYTICS PLATFORM SETUP GUIDE

Set Up the Einstein Analytics Platform

Set up your organization to use the Salesforce Analytics platform by enabling Analytics and assigning basic permission sets or creating and assigning your own custom permission sets.

The information here describes how to set up your organization to use the Analytics platform and Analytics templated apps and Apps.

SEE ALSO:

> Set Up the Analytics Platform with Licenses Purchased Before October 20, 2015
>
> Migrating From Analytics Licenses Purchased Before 10/20/2015 to New Analytics Platform Licenses

Learn About Analytics Platform Licenses and Permission Sets

Introduce yourself to Analytics setup fundamentals, which apply to both basic and advanced setup procedures.

Each Analytics Platform license is a single-user license that provides access to the Salesforce Analytics Cloud. It provides access to Analytics Platform and Analytics templated apps and Apps features and functionality. The license limits your instance of the Analytics Cloud to 100 million rows of data. If you require more data, you can purchase Analytics Cloud - Additional Data Rows, which entitles you to an additional 100 million rows.

🛇 **Important:**

- Analytics license data storage limits are contractual, not technical. Licensee agrees to strictly monitor its total number of data rows.
- If you purchased an Analytics Platform license before October 20, 2015 with Analytics Cloud Builder or Analytics Cloud Explorer permission set licenses: Read Set up the Analytics Platform With Licenses Purchased Before October 20, 2015. If you're migrating users from Builder or Explorer licenses to the new Analytics Platform license: See Migrating From Analytics Licenses Purchased Before 10/20/2015 to New Analytics Platform Licenses before you start the setup process for those users.
- If you disable Analytics, user permissions are removed from each defined permission set. If you re-enable Analytics later, you must define the permission sets again.

Analytics Platform License Permission Sets

The Analytics Platform license includes two prebuilt permission sets:

- **Einstein Analytics Platform Admin** enables all permissions required to administer the Analytics platform, including permissions to enable creating Analytics templated apps and Apps.
- **Einstein Analytics Platform User** enables all permissions required to use the Analytics platform and Analytics templated apps and Apps

Basic setup involves choosing and assigning the prebuilt permission sets. To create your own custom Analytics permission sets use advanced setup.

When you assign any Analytics permission set to users in your org, Salesforce *auto-assigns* the Analytics Platform permission set license to that user.

> 📝 **Note:** For efficiency, you can assign a permission set to groups of users. You can also assign multiple permission sets to a user.

You can assign an Analytics permission set license along with any of the following Salesforce user licenses:

- Lightning Platform (app subscription)
- Lightning Platform (one app)
- Full CRM
- Salesforce Platform
- Salesforce Platform One

Basic Analytics Platform Setup

Follow these few steps to give users in your organization access to Analytics platform, templates, and apps quickly. Basic setup uses permission sets included with the Analytics Platform license, which cover the majority of most organizations' analytics needs.

Enable Analytics

1. Go to Salesforce Setup and enter *Analytics* in the **Quick Find / Search** field.
2. Select **Getting Started**.
3. Click **Enable Analytics**.

Select and Assign Permission Sets

1. In Salesforce Setup, select **Users**.
2. Select **Permission Sets**.
3. Select one of the two prebuilt permission sets.
   - **Einstein Analytics Platform Admin** enables all permissions required to administer the Analytics platform, including permissions to enable creating Analytics templated apps and Apps.
   - **Einstein Analytics Platform User** enables all permissions required to use the Analytics platform and Analytics templated apps and Apps

   That opens the page for the selected permission set.
4. Click **Manage Assignments**. The next page shows the users already assigned the selected permission set.
5. Click **Add Assignments** to see all the users in your org.
6. Select one or more users by checking the box next to their name in the left-hand column.
7. Click **Assign**.

You'll see a page that tells you if the permission set has been assigned. If permission set didn't succeed for one or more users, Salesforce tells you why. You can fix the problem and try again.

Advanced Analytics Platform Setup

Follow these steps to learn the details of Analytics permissions and to create and assign your own custom permission sets.

💡 **Tip:** For best results, follow the steps in the order shown.

Learn About Analytics Permission Set Licenses and User Permissions

When you create your own Analytics permission sets, you start by selecting the Analytics Platform permission set license instead of using the prebuilt permission sets. The permission set license includes the user permissions required to explore data with and manage the Salesforce Analytics platform.

- Each Analytics platform user needs an Analytics Platform permission set license to use the Analytics platform. Creating a permission set and assigning it to a user *auto-assigns* the Analytics platform permission set license to that user. You can also manually assign permission set licenses to users.
- Community users need an Analytics for Communities permission set license to view Analytics apps shared via dashboards embedded in Visualforce pages.

The Analytics Platform permission set license enables the following permissions.

User Permission	What It Enables
Use Analytics	Run Analytics apps to which you have access; view their datasets, lenses, and dashboards; and create and edit lenses.
Create and Edit Analytics Dashboards	Create, edit, and delete Analytics dashboards.
Create Analytics Apps	Create, edit, delete, and share Analytics applications.
Upload External Data to Analytics	Upload external data to Analytics to create a dataset. Monitor dataflow and system jobs in the data monitor.
Edit Analytics Dataflows	Edit, start, stop, and reschedule the dataflow to create datasets. Create, edit, and run dataset recipes to create datasets. Monitor dataflow and system jobs in the data monitor. Use discretion when assigning this user permission because it enables access to all Salesforce object data to which the Integration User has access. See Salesforce Data Access in Analytics.
Edit Dataset Recipes	Create, edit, and run dataset recipes to create datasets. Monitor dataflow and system jobs in the data monitor. Doesn't enable editing security predicates in existing recipes, or running and scheduling recipes based on datasets that have security predicates.
Manage Analytics	Access all Analytics features. Provides Analytics administrator-level capabilities.
Manage Analytics Templated Apps	Create and manage apps based on Analytics Templates. Edit Analytics dataflows. Edit dataset recipes. Monitor dataflow and system jobs in the data monitor. Some templates require extra permissions. See the help for each template.
Use Analytics Templated Apps	Use apps based on Analytics Templates. Can also create, edit, and delete Analytics dashboards. Some templates require extra permissions. See the help for each template.

Adoption Analytics Templates and Apps	Create and use apps based on the Adoption Analytics template.
Download Analytics Data	Download screenshots and data in tabular format through the Analytics user interface.
Add Analytics Remote Connections	Add connections to external data sources to enable replication in Analytics.
Trend Report Data in Analytics	Trend the data of a report with an Analytics dataflow.

You create your own permission sets based on these permissions.

📝 **Note:** When you create permission sets for Analytics users, selecting any Analytics permission automatically enables the "Use Analytics" permission as well. Also, the type of access granted on an app controls the actions that can be performed on its datasets, lenses, and dashboards. For example, if a user has the "Use Analytics" permission, the user must also have Viewer access on an app to view its datasets, lenses, and dashboards.

The Analytics for Communities permission set license enables the "View Analytics on Communities pages" permission. That permission enables external users to view Analytics dashboards embedded in their communities. See Enable Analytics for Communities on page 7.

Identify Analytics Platform User Types

Identifying types of Analytics platform users helps assure that custom permission sets meet your team's analytics needs.

The Analytics Platform license includes the permissions that enable users in your organization to import, work with, and explore data using the Analytics platform. The license also includes permissions that let administrators manage Analytics. To set up Analytics in the most useful way, think through the different ways people access Analytics features and categorize them into user types. Here are a few examples.

Most people on your team fall into two basic categories:

- Users, who view Analytics dashboards, lenses, and datasets and occasionally import data to Analytics.
- Administrators or managers, who access to the full range of Analytics functionality to create apps, dashboards, lenses, and datasets, edit data, and otherwise customize the Analytics experience.

Accordingly, when you set up the Analytics platform, creating two basic permission sets can meet the needs of most of your organization:

- A "view" permission set that contains the permissions needed by most basic-level users when they access Analytics.
- A "manage" permission set that's reserved for a select few administrators and managers and contains permissions to use all Analytics features

You can set up Analytics however you want, defining other user types and permissions sets based on the needs of users in your organization. For example, you can create a "superuser" permission set for users who create and share apps and dashboards. Or, a "data wizard" permission set would enable other users to work closely with datasets.

We focus on two main types of people on your team -- users and administrators -- in the example permission sets we describe in our detailed setup instructions.

Enable Analytics and Create Permission Sets

After identifying user types, be sure to enable Analytics in your org. Then select a permission set license and create your permission sets.

> **EDITIONS**
>
> Available in Salesforce Classic and Lightning Experience.
>
> Available for an extra cost in **Enterprise**, **Performance**, and **Unlimited** Editions. Also available in **Developer Edition**.

Enable the Analytics Platform

To use the Analytics platform, first enable it for your organization.

1. In the Salesforce Setup menu, under Administer, click **Analytics | Getting Started**.

2. Click **Enable Analytics**.

Create Permission Sets

The next step in the setup process is to create permission sets made up of Analytics user permissions. We show you how to create two permission sets:

- *Manage Analytics* permission set, for users who create and administer Analytics.
- *View Analytics* permission set, for users who explore app dashboards and datasets.

> 📝 Note:
>
> - Customers who purchased Analytics before October 20, 2015: See Set up the Analytics Platform With Licenses Purchased Before October 20, 2015 before following the instructions here.
>
> - The Manage Analytics permission set enables the equivalent functionality provided by the previous Analytics Builder license (purchased before October 20, 2015). If you have a Builder license or you're migrating to the current Analytics platform license, follow these steps to create a permission set with the same functionality.
>
> - The View Analytics permission set enables the equivalent functionality provided by the previous Analytics Explorer license (purchased before October 20, 2015). If you have an Explorer license or you're migrating to the current Analytics platform license, follow these steps to create a permission set with the same functionality.

1. In the Setup menu, under administer, click **Manage Users | Permission Sets** and then click **New**.

2. Enter `Manage Analytics` or `View Analytics` in the Label field, as appropriate. This automatically creates the API name as well. You can change it if you like, but it can't include spaces, end with an underscore, or have two consecutive underscores.

3. For License, select the license to associate with this permission set. In this case, select the Analytics Platform permission set license.

When you select a specific permission set license, any user assigned to the permission set is *auto-assigned* the permission set license. If you select --None--, you must *manually* assign the permission set license to users before you can add them to the new permission set.

4. Click **Save**. The Permission Set Overview page shows the new permission set. Now add user permissions to the set.

5. Click **System Permissions** to open the list of user permissions enabled by the Analytics Platform license. Then click **Edit**.

6. Do one of the following.

- If you're creating the Manage Analytics permission set, select "Manage Analytics" user permissions and click **Save**. You've successfully created a permission set that enables access to all Analytics features. You don't have to select any of the other individual permissions. Assign this permission set sparingly because it provides access to all Analytics features, many of which are inappropriate for most analytics users.

- If you're creating the View Analytics permission set, select "Use Analytics" and "Upload External Data to Analytics" user permissions and click **Save**. You've successfully created a permission set that enables a user to view the Analytics datasets, lenses, and dashboards that they have permission to view, and to upload data files from outside Salesforce.

7. You can now assign your new permission set to users, which is covered in Assign Permission Sets to Users.

Repeat these steps for every user in your organization who requires access to Analytics.

Assign Analytics Permission Sets to Users

Assign custom permission sets to one or more users—either one at a time, or in bulk—to give them access to Analytics functionality.

1. In the Setup menu, under administer, click **Manage Users | Permission Sets**.

2. Click the permission set you want to assign to users. If you've followed the instructions in Enable Analytics and Create Service Analytics Permission Sets on page 4, select either the Manage Analytics or View Analytics permission sets.

3. Click **Manage Assignments** and click **Add Assignments**.

4. Select the users who need access to Analytics, and click **Done**. When you assign the permission set to users, Salesforce *auto-assigns* the Analytics Cloud - Analytics Platform *permission set license* to those users.

Assign the Manage Analytics permission set sparingly, since it provides access to all Analytics features. Assign it only to users who administer or manage the Analytics platform.

USER PERMISSIONS
To assign a permission set to users: • Assign Permission Sets

Complete Setting up the Analytics Platform

After assigning permission sets with either basic or advanced setup, follow these optional procedures to enhance the Analytics experience and fine-tune Analytics access to Salesforce data.

Enable Preview Thumbnails for All Lenses and Dashboards

Make it easier for users to find their lenses and dashboards on the home page and on app pages. Replace the generic icons with preview thumbnails of the contents of all lenses and dashboards, including those assets that have row-level security restrictions.

If no security predicate is defined for a dataset, then preview thumbnails always appear. If a security predicate is defined, then preview thumbnails don't show unless this setting is enabled. With the setting enabled, preview thumbnails appear for all assets.

> ⊘ **Important:** Even if row-level security applies to the dataset used by a lens or dashboard, the preview thumbnail could expose data from restricted rows. Row-level security restrictions take effect only after you've clicked through to the lens or dashboard.

1. From Setup, enter `Analytics` in the `Quick Find` box, then select **Settings**.

2. Select `Show preview thumbnails for lenses and dashboards with row level-security enabled`.

3. Click **Save**.

Enable Analytics for Communities

Securely share Analytics apps with community partner and customer users.

> ✎ **Note:** Only users with a Customer Community Plus, Partner Community, or Lightning External Apps Plus license can use this feature. This feature is supported in communities but not in portals.

To enable Analytics for sharing with Communities, complete the following steps.

1. From Setup, enter `Analytics` in the `Quick Find` box, then select **Settings**. Select `Enable Analytics for Communities`.

2. Assign your community members the Analytics for Communities permission set license.

3. Create a permission set that includes the "View Analytics on Communities pages" permission and assign it to your community members.

4. Continue setting up Analytics for Communities with Step 2 in Share Analytics with Communities.

Enable Conversational Exploration

Quickly query and visualize data in guided, natural language conversations.

To set up Analytics to explore data using conversations, complete the following steps.

1. From Setup, enter `Analytics` in the `Quick Find` box, then select **Settings**.

2. Select `Enable Conversational Exploration`.

3. Click **Save**.

Enable the Analytics REST API

You can access Analytics datasets and lenses programmatically using the Analytics REST API. Selecting this option overrides the "APIEnabled" permission for individual users and gives all Analytics users (including Community users) access to the API.

1. From Setup, enter `Analytics` in the `Quick Find` box, then select **Settings**.

2. Select `Grant all users access to Wave API`.

3. Click **Save**.

Grant Users Access to the Dashboard Designer and Classic Designer

To grant users access to either dashboard designer, assign each of them the "Create and Edit Analytics Dashboards" user permission. For users to access the dashboard designer, the **Enable dashboard designer** setup option must also be enabled, which it is by default.

If dashboard designer is disabled, complete the following tasks to enable it.

1. From Setup, enter *Analytics* in the Quick Find box, then select **Settings**.

2. Select **Enable dashboard designer**, and then click **Save**.

3. For each user that builds dashboards, assign the "Create and Edit Analytics Dashboards" user permission to them.
   Each user has a choice whether to use the classic designer or dashboard designer for each dashboard.

EDITIONS

Available in Salesforce Classic and Lightning Experience.

Available for an extra cost in **Enterprise**, **Performance**, and **Unlimited** Editions. Also available in **Developer** Edition.

USER PERMISSIONS

To access the dashboard designer or classic designer:
- Create and Edit Analytics Dashboards

Enable Dashboard Views

Enable this feature to allow each Einstein Analytics user to create their own unique views of a dashboard. By default, this feature is enabled for your org. If the feature is disabled and you re-enable it, all previously created views are available.

1. From Setup, enter *Analytics* in the Quick Find box, then select **Settings**.

2. Select **Enable Wave dashboard saved views**, and then click **Save**.

EDITIONS

Available in Salesforce Classic and Lightning Experience.

Available for an extra cost in **Enterprise**, **Performance**, and **Unlimited** Editions. Also available in **Developer** Edition.

Enable Annotations on Dashboard Widgets

Annotate dashboard widgets with comments posted in the dashboard and in Chatter.

To enable annotations, complete the following steps.

1. From Setup, enter *Feed Tracking* in the Quick Find box, and then select **Feed Tracking** under Chatter.

2. Scroll down and select **Analytics Asset**.

3. Select Enable Feed Tracking.

4. Click **Save**.

   📝 Note: Annotations aren't supported in dashboards built with the classic designer.

Enable Downloading from Analytics

Enable users to download the results from lens explorations and dashboard widgets as images (.png), Microsoft® Excel® (.xls), or comma-separated values (.csv) files.

📝 Note: Complete dashboards can be downloaded only as images.

To set up users to download data from Analytics, complete the following steps.

1. From Setup, enter *Permission Sets* in the Quick Find box, and then select **Permission Sets** under Manage Users.

2. Select the Analytics Cloud Permission Set where you want to add the permission, and then select **System Permissions**.

3. Select Download Analytics Data.

4. Click **Save**.

Connected App for Analytics on Mobile

Install the Salesforce Analytics App Package to allow your mobile clients to easily connect to your org. This package contains the Connected App component that gives you control over who's logging in and how your mobile clients share images and links.

1. While logged in as an admin, navigate to:

   Production
   https://login.salesforce.com/packaging/installPackage.apexp?p0=04tB0000000cHCH

   Sandbox
   https://test.salesforce.com/packaging/installPackage.apexp?p0=04tB0000000cHCH

2. Select **Install for All Users**.

   If you install the Connected App only for certain roles, then only those clients are subject to your policies.

3. After clicking **Done**, click the Salesforce Analytics App Package and then **View Components**.

4. Select iOS or Android. To configure policies and other settings, click **Edit**. When you are finished, save your changes.

   For more information about Connected App settings, see Edit a Connected App.

5. If you want to disable sharing options for mobile users, click **New** in the Custom Attributes section.

   All sharing options are enabled by default. To disable an option, add its attribute key and enter "`false`" for the attribute value. See the table for the supported attribute keys.

Attribute Key	Mobile clients can share	Mobile Device
SHARE_IMAGE_AIRDROP	Images via AirDrop	iOS
SHARE_IMAGE_CAMERAROLL	Images to Camera Roll	iOS
SHARE_IMAGE_OPEN	Images to other apps and activities	iOS
SHARE_IMAGE_S1	Images to Salesforce	iOS
SHARE_IMAGE_EMAIL	Images via email	iOS
SHARE_LINK_NFC	Links via Near Field Communication (NFC)	Android
SHARE_LINK_BLUETOOTH	Links via Bluetooth	Android
SHARE_LINK_AIRDROP	Links via AirDrop	iOS
SHARE_LINK_CLIPBOARD	Links to Clipboard	iOS and Android
SHARE_LINK_S1	Links to Salesforce	iOS and Android
SHARE_LINK_EMAIL	Links via email	iOS and Android
SPOTLIGHT_SEARCH	Mobile clients can see Analytics assets in Spotlight search results	iOS

Note: To apply custom attributes to connected users, you can revoke them and ask them to reconnect.

EDITIONS

Available in Salesforce Classic and Lightning Experience.

Available for an extra cost in **Enterprise**, **Performance**, and **Unlimited** Editions. Also available in **Developer** Edition.

USER PERMISSIONS

To install and configure Connected App:
- Manage Analytics

6. To view and control how mobile clients connect to your Analytics-enabled org, from Setup, enter `Connected Apps` in the `Quick Find` box, then select **Connect Apps OAuth Usage**.

You can block user sessions, revoke individual users, and drill in to user details. For more information, see Monitoring Usage for a Connected App.

> 📝 **Note:** For certificate-based authentication, users must set their desktop browsers to allow cookies.

For additional security, use Mobile Device Management (MDM) with the option to show only authorized hosts. The "OnlyShowAuthorizedHosts" key allows you to hide the "Add New Account" plus sign in the mobile app. For more information, see Using MDM with Salesforce Mobile SDK Apps.

Analytics Security Implementation Guide

Analytics has different levels of security that your organization can implement to ensure that the right user has access to the right data.
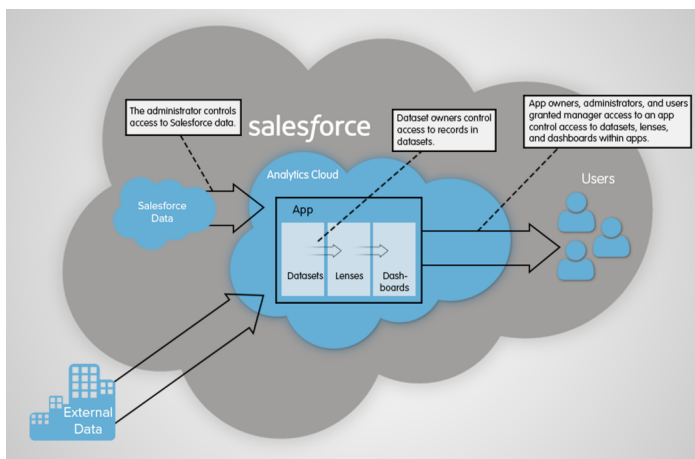
- The administrator can implement object-level and field-level security to control access to Salesforce data. For example, the administrator can restrict access to prevent the dataflow from loading sensitive Salesforce data into datasets. This document describes how Analytics uses object-level and field-level security on Salesforce data and how to configure permissions on Salesforce objects and fields.

- Dataset owners can implement row-level security on each dataset that they create to restrict access to it's records. If a dataset does not have row-level security, users who have access to the dataset can view all records. This document describes how to configure row-level security on datasets and provides some sample implementations based on datasets created from Salesforce data and external data.

- App owners, administrators, and users granted manager access to an app control access to datasets, lenses, and dashboards within apps. This document describes the different levels of access for apps and how to share datasets, lenses, dashboards in an app with other users.

  > 📝 **Note:** Analytics supports security predicates, a robust row-level security feature that enables you to model many different types of access controls on datasets. Also, Analytics supports sharing inheritance, to synchronize with sharing that's configured in Salesforce, subject to certain limitations. If you use sharing inheritance, you must also set a security predicate to take over in situations when sharing settings can't be honored.

For complete information about implementing Analytics security, see Analytics Security Implementation Guide.

Salesforce Data Access in Analytics

Analytics requires access to Salesforce data when extracting the data and also when the data is used as part of row-level security. Analytics gains access to Salesforce data based on permissions of two internal Analytics users: Integration User and Security User.

Analytics uses the permissions of the Integration User to extract data from Salesforce objects and fields when a dataflow job runs. Because the Integration User has View All Data access, consider restricting access to particular objects and fields that contain sensitive data. If the dataflow is configured to extract data from an object or field on which the Integration User does not have permission, the dataflow job fails.

When you query a dataset that has row-level security based on the User object, Analytics uses the permissions of the Security User to access the User object and its fields. The Security User must have at least read permission on each User object field included in a predicate. A predicate is a filter condition that defines row-level security for a dataset. By default, the Security User has read permission on all standard fields of the User object. If the predicate is based on a custom field, then grant the Security User read access on the field. If the Security User does not have read access on all User object fields included in a predicate expression, an error appears when you try to query the dataset using that predicate.

🛑 **Important:** Because Analytics requires the Integration User and Security User to access Salesforce data, do not delete either of these users.

Control Access to Salesforce Objects and Fields

Analytics requires access to Salesforce data when extracting the data and also when the data is used as part of row-level security. Configure the permissions of the Integration User on Salesforce objects and fields to control the dataflow's access to Salesforce data. Configure the permissions of the Security User to enable row-level security based on custom fields of the User object.

When configuring permissions for the Integration User or Security User, make changes to a cloned version of the user profile.

1. From Setup, enter `Profiles` in the `Quick Find` box, then select **Profiles**, and then select the user profile.

    For the Integration User, select the Analytics Cloud Integration User profile. For the Security User, select the Analytics Cloud Security User profile.

2. Click **Clone** to clone the user profile.

3. Name and save the cloned user profile.

4. Click **Object Settings**.

5. Click the name of the Salesforce object.

6. Click **Edit**.

    a. To enable permission on the object, select **Read** in the Object Permissions section.

    b. To enable permission on a field of the object, select **Read** for the field in the Field Permissions section.

    📝 **Note:** You can't change the permissions on standard fields of the User object.

7. Save the object settings.

8. Assign the cloned user profile to the Integration User or Security User.

    a. From Setup, enter `Users` in the `Quick Find` box, then select **Users**.

    b. Select the user to which you want to assign the user profile.

    c. Click **Edit**.

    d. In the Profile field, select the user profile.

    e. Click **Save**.

USER PERMISSIONS

To clone a user profile:
- Manage Profiles and Permission Sets

To edit object permissions:
- Manage Profiles and Permission Sets
  AND
  Customize Application

9. Verify that the Integration User or Security User has the right permissions on fields of the objects.

Set Up a Whitelist of Trusted Sites for Embedded Analytics Dashboards

Specify your trusted sites in the Analytics whitelist, you can include embedded Analytics dashboards in websites and apps outside of Salesforce servers.

To set up an Analytics whitelist, complete the following steps.

1. From Setup, enter `Whitelist` in the `Quick Find` box, then select **Whitelist** under Analytics.

2. On the Whitelist for Embedding Dashboards page, click **New**.

3. On the Whitelisted Site Edit page, enter the information for the site you want to add to the Analytics whitelist.

4. Click **Save**.

Einstein Analytics Encryption

The Einstein Analytics Encryption solution enhances security for Salesforce customers by extending encryption capabilities to the data at rest that is stored on the Salesforce file system.

If digital data is in transit, currently being processed, or stored in memory, that data is considered to be in use. By contrast, digital data is considered at rest if it is stored physically in persistent storage but is not currently in use. Einstein Analytics Encryption is for encrypting registered datasets in Einstein Analytics. To encrypt data at rest and preserve functionality, Einstein Analytics Encryption services are built natively into the Einstein Analytics platform. The solution applies strong, probabilistic encryption on data stored at rest. Platform encryption is based on the Advanced Encryption Standard (AES) with 256-bit keys using CTR mode for every write.

All operations, including sort and group-by, function the same as without encryption (except for key management functions, as noted in this topic).

How Einstein Analytics Encryption Works

As a prerequisite to Einstein Analytics Encryption, you must be approved by the Einstein Analytics Encryption Product Manager. Your org must have a Shield Platform Encryption tenant secret. (Einstein Analytics Encryption uses PE key management, so it's not necessary to encrypt objects and fields in core Salesforce.)

When using Einstein Analytics with your encryption-enabled instance, data read from and written to disk is automatically encrypted with the unique key for your account. For more information about the encryption technology, refer to the Shield Platform Encryption Architecture white paper. To verify that encryption is enabled, go to the Analytics Settings page in the Setup UI.
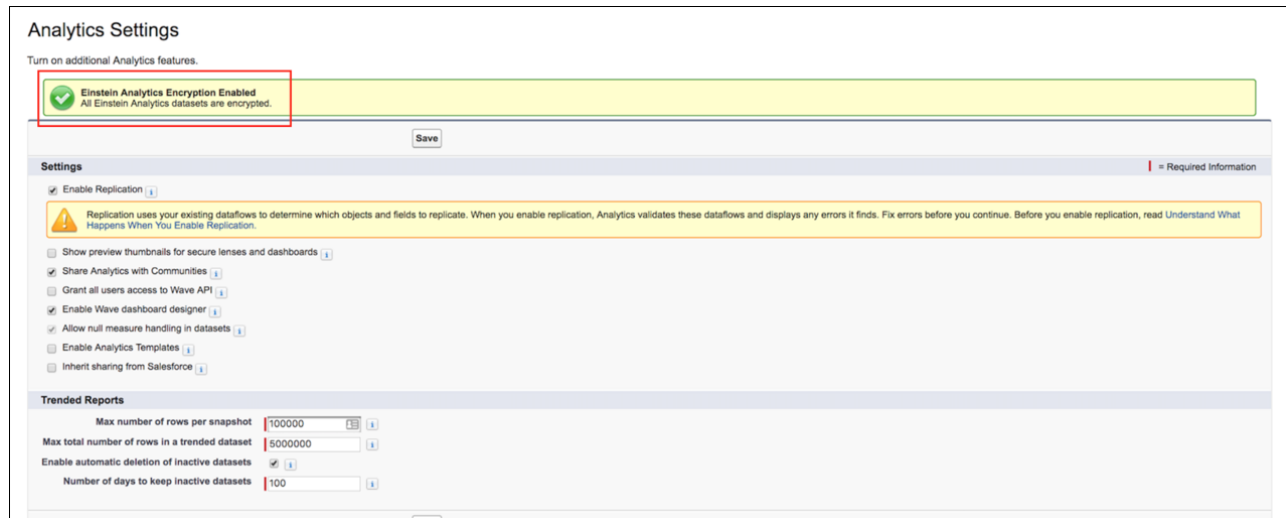
Features

Key export, Bring Your Own Key, key rotation, key revocation, and key import are available.

All Einstein Analytics features are supported, with the following exceptions:

- Pre-existing data is not encrypted.
- Data that was in Einstein Analytics before encryption was enabled is not encrypted.
- If pre-existing data is imported from Salesforce objects through the dataflow, the data becomes encrypted on the next dataflow run.
- Other pre-existing data (such as CSV data) must be reimported to become encrypted.
- Although pre-existing data is not encrypted, it is still accessible and fully functional in its unencrypted state when encryption is enabled.

Frequently Asked Questions

Is data encrypted in transit? Yes. However, encryption in transit is different from encryption at rest. This feature covers encryption at rest.

Can Einstein Analytics bring in data encrypted with Shield Platform Encryption? Yes. Einstein Analytics reads platform encrypted data in the same way that any user reads platform encrypted data. The data is then written and encrypted in Einstein Analytics. It is not required that data be encrypted with Shield Platform Encryption to be encrypted in Einstein Analytics. It is only required that a Tenant Secret exist for the org.

Can I mask my data? No. Masking data is not currently available and it does not fall under the Einstein Analytics scope.

Are the keys different for Shield Platform Encryption and Einstein Analytics Encryption? Yes, although Shield and Einstein Analytics use the same key management technology, they use different keys.

Do mobile dashboards still work with encryption? Yes. All Einstein Analytics functionality, including support for mobile devices, works with encryption enabled. All data stored on mobile (mainly JSON code and thumbnails) is AES 256 encrypted.

Is there any impact on application performance? The Einstein Analytics Encryption solution is designed to have at most a minimal performance impact on your Einstein Analytics application experience.

Set Up the Analytics Platform with Licenses Purchased Before October 20, 2015

If you purchased an Analytics Cloud Builder or Analytics Cloud Explorer license before October 20, 2015, you can continue to use your licenses to set up the Analytics plaform for users in your organization or you can migrate to the new single-user Analytics Platform license.

> 📝 **Note:** This information applies only to customers who purchased Analytics licenses before October 20, 2015, and continue to use the Analytics Cloud Builder or Analytics Cloud Explorer licenses after that without migrating to the new Analytics Platform license. If you purchased Analytics on or after October 20, 2015, go to Set Up the Einstein Analytics Platform.

> ⛔ **Important:** If you're migrating from the previous Analytics Cloud Builder or Analytics Cloud Explorer platform licenses to the single-user Sales Analytics Apps license, read Migrating From Analytics Licenses Purchased Before 10/20/2015 to New Analytics Platform Licenses.

The Analytics Platform License

An Analytics license purchased before October 20, 2015, enables you to turn on Analytics for your organization. Each previous Analytics Platform license is contractually limited to a maximum of 400 users. If you need more than 400 users, you can purchase additional Analytics licenses.

Each previous Analytics license enables you to:

- Store up to 250,000,000 rows in your final registered datasets.
- Run up to 50 concurrent queries in Analytics.

The Analytics Cloud Permission Set License

Each user needs one of two Analytics permission set licenses to use the product. The permission set license defines what user permissions can be assigned to the user. The administrator assigns permission set licenses to users.

For Analytics licenses sold before October 20, 2015, Salesforce provided the following permission set licenses:

- Analytics Cloud Builder permission set license enables users to access all Analytics features.
- Analytics Cloud Explorer permission set license enables users to upload external data to Analytics and explore data.

Here are Analytics user permissions included with each permission set license.

User Permission	Included in Explorer or Builder Permission Set License?	What It Enables
"Create and Edit Analytics Dashboards"	Builder only	Creating and editing Analytics dashboards.
"Create Analytics Apps"	Builder only	Creating and sharing Analytics applications.
"Edit Analytics Dataflows"	Builder only	Downloading, uploading, starting, stopping, and rescheduling the dataflow. Viewing dataflow and system jobs in the data monitor.
"Manage Analytics"	Builder only	Accessing all Analytics features. Provides Analytics administrator-level capabilities.

User Permission	Included in Explorer or Builder Permission Set License?	What It Enables
"Upload External Data to Analytics"	Builder and Explorer	Uploading external data to Analytics to create a dataset. Viewing dataflow and system jobs in the data monitor.
"Use Analytics"	Builder and Explorer	Using Analytics, and viewing the datasets, lenses, and dashboards that the user has permission to view. Automatically enabled when you select any other Analytics permission.

📝 **Note:** When you create permission sets for Analytics users, selecting any of the other Analytics permissions automatically enables the "Use Analytics" permission.

You can assign previous Analytics permission set licenses along with any of the following Salesforce user licenses:

- Lightning Platform (app subscription)
- Lightning Platform (one app)
- Full CRM
- Salesforce Platform
- Salesforce Platform One

SEE ALSO:

Migrating From Analytics Licenses Purchased Before 10/20/2015 to New Analytics Platform Licenses

To complete migration from previous Analytics Cloud Builder and Analytics Cloud Explorer licenses purchased before October 20, 2015, to the new Analytics Platform license, you may need to set up Analytics users in your organization with new permission sets.

When Salesforce provisions your organization with the new Analytics Platform license, you may have to set up some users with the new license.

- **Analytics Cloud Builder license users.** Users who access Analytics with the Analytics Cloud Builder license should be able to continue to use the Analytics platform without any additional setup. The Builder license is simply renamed *Analytics Platform*, and you'll see that permission set license in Salesforce Setup.
- **Analytics Cloud Explorer license users.** During the new license provisioning process, Salesforce may remove the Analytics Cloud Explorer license from your org. If that's the case, you'll see the new Analytics Platform license instead of the Explorer license and you have to set up users with that license. If the Explorer permission set license is still visible, you do not have to repeat the setup process for Explorer users.

EDITIONS

Available in Salesforce Classic and Lightning Experience.

Available for an extra cost in **Enterprise**, **Performance**, and **Unlimited** Editions. Also available in **Developer** Edition.

If users in your organization require you to set them up with the new Analytics Platform license—even if they used Analytics with a previous license—follow the steps in Analytics Platform Setup on page 1. You need to assign them the new permission set license, create one or more new permission sets, and assign the permission sets to users.

Einstein Analytics Limits

This section describes Analytics limits.

API Call Limits

These limits apply to all supported editions.

Limit	Value
Maximum concurrent Analytics API calls per org	100
Maximum Analytics API calls per user per hour	10,000

Dataset Storage Limits

These limits apply to all supported editions and are contractual, not technical. The licensee agrees to strictly monitor its total number of data rows. Use of a prebuilt Analytics app license, such as the Sales Analytics app license, does not increase the data limit for the Analytics Platform license.

Limit	Value
Maximum number of rows for all registered datasets combined	100 million with Einstein Analytics Growth or Einstein Analytics Plus
	25 million with Sales Analytics or Service Analytics
	50 million with Event Monitoring Analytics
	25 million with B2B Marketing Analytics
	25 million with Einstein Analytics for Financial Services Cloud
	25 million with Einstein Analytics for Health Cloud
	+100 million per Additional Data Rows license
	Whether the row limits are additive depends on the SKUs for your org. Examples:
	• The Einstein Analytics Growth and Einstein Analytics Plus SKUs include Sales Analytics and Service Analytics, so the total row limit is 100 million.
	• If your org has an Einstein Analytics Growth or an Einstein Analytics Plus SKU and then obtains an additional SKU for Sales Analytics or Services Analytics, the limit increases to 125 million.
	• If your org has an Einstein Analytics Growth or an Einstein Analytics Plus SKU and adds the Event Monitoring SKU, the total row limit becomes 150 million.
Maximum number of fields in a dataset	5,000 (including up to 1,000 date fields)

Limit	Value
Maximum value for each numeric field in a dataset	36,028,797,018,963,967
Minimum value for each numeric field in a dataset	-36,028,797,018,963,968

Dataflow Limits

Analytics uses the bulk API, but this does **not** count towards Salesforce bulk API limits. The dataflow submits a separate bulk API call to extract data from each Salesforce object. The dataflow uses a batch size of 100K to 250K, depending on whether the dataflow or the bulk API chunks the data. As a result, to extract 1 million rows from an object, the dataflow creates 4-10 batches.

Limit	Value
Maximum number of dataflows definitions (with data sync enabled)	35
Maximum number of dataflow runs in a rolling 24-hour period	50

> 📝 **Note:** Dataflow and recipe runs that take less than 2 minutes, and data sync, don't count toward the 24-hour dataflow run limit. However, you can't run any of these data jobs, regardless of size, if you've already reached the 24-hour run limit.

ELT Job Limits

ELT jobs include user dataflows, CSV uploads, dataset recipes, and data sync.

Limit	Value
Timeout for ELT jobs that have been scheduled but not executed	5 minutes

Data Sync Limits

If you are currently extracting more than 100 objects in your dataflows, contact Salesforce Customer Support before you enable data sync.

Limit	Value
Maximum number of objects that can be enabled for data sync	100

Trending Data Limits

Trended datasets count toward the overall Analytics platform limits, including total number of rows.

Limit	Value
Maximum number of trended datasets per user	5
Maximum number of rows per snapshot	100,000
Maximum number of rows for all monthly snapshots per org	40 million

Lens and Dashboard Creation Limits

These limits apply to the creation of lenses and dashboards.

Limit	Value
Character limit for description fields	1000
Default number of rows in a compare table	2000 (To set a different value, use the SAQL `limit` statement)
Default number of rows in a values table	100 (To set a different value, use the SAQL `limit` statement)
Maximum file size for geojson	10 MB
Maximum number of notifications per user	10

Story Creation Limit

This limit applies to the creation of stories in Einstein Analytics Plus.

Limit	Value
Story creation limit	500 with Einstein Analytics Plus (To purchase additional stories, purchase Einstein Analytics Plus - Additional Stories (1,000). Additional stories are purchased in blocks of 1,000.)
	100 per org per month with Einstein Predictions

Sales Analytics and Service Analytics App Limits

Sales Analytics and Service Analytics app limits custom object support to no more than 10 custom objects and one dataflow for each org that implements the app. These are contractual, not technical, limits.

External Data Limits

Limit	Value
Maximum file size per external data upload	40 GB
Maximum file size for all external data uploads in a rolling 24-hour period	50 GB
Maximum number of external data jobs per dataflow that can be run in a rolling 24-hour period	50
Maximum number of characters in a field	32,000
Maximum number of fields in a record	5,000 (including up to 1,000 date fields)
Maximum number of characters for all fields in a record	400,000

Query Limits

Trended datasets count toward the overall Analytics platform limits, including total number of rows.

Limit	Value
Maximum concurrent queries per organization	50 per platform
Maximum concurrent queries per user	10
Maximum number of rows returned per query 10,000 is the default value. To set a different value, use the SAQL `limit` statement	10,000*
Query timeout	2 minutes

*The maximum results returned by a query varies based on the step type that contains the query and whether the query is executed from a desktop or the mobile app.

Step Type	Applies to Dashboard Designer Dashboards?	Applies to Classic Designer Dashboards?	Desktop Default Limit	Mobile Default Limit
aggregate		✅	2,000	100 if the step contains a single grouping, 500 if it contains multiple groupings.
aggregateflex	✅		2,000	500
grain (for values tables only)	✅	✅	100	100
multi (for compare tables only)		✅	2,000	2,000
saql	✅		2,000	2,000
soql	✅		See *SOQL and SOSL Reference*.	See *SOQL and SOSL Reference*
static		✅	n/a	n/a
staticflex	✅		n/a	n/a

> 💡 **Tip:** To see the `limit` for a given step, click >_ in the explorer. If it's not set, Analytics returns up to 10,000 results. To change the limit, edit the SAQL or SOQL query. The higher you increase the limit, the longer the query might take. For more information about SAQL queries, see the *Analytics SAQL Reference*. For information about SOQL queries, see *Salesforce Object Query Reference*.

The limit only impacts the number of records returned for display. It doesn't impact calculations across all dataset records. For instance, a query groups by account name and the dataset contains one million account names. With a limit of 20, Analytics only returns 20 results for display, but the summary row adds up all one million records.

Analytics Developer Addition Limits

Analytics is built on the Lightning platform and is subject to the Lightning platform limits. For example, the SOQL query limit (20,000 characters) controls the number of fields from which the sfdcDigest transformation can extract data. If you exceed a Lightning Platform limit, an error occurs. See Lightning platform limits.

Limit	Value
Maximum number of data rows	250,000
Maximum number of concurrent queries	5

Einstein Analytics Limitations

Analytics differs from other Salesforce features in some ways.

General Limitations

This section describes Analytics limitations.

Update Schedule

All customers receive Analytics updates on the same schedule, regardless of instance.

Localization and Internationalization

Analytics has been localized with the following exceptions.

- We do not support right-to-left languages, such as Arabic and Hebrew.
- A subset of error messages is available only in English.
- The mobile iOS app includes only English versions of sample datasets and dashboards.

Analytics provides internationalization support with the following limitations.

- You must set both locale and language to see translated labels.
- Data within datasets is not modified for localization or internationalization.
- Each dataset can have a single locale specified in the metadata. The metadata locale is not overridden by individual user locale settings. All users see the same date, time, and number formats, and dimension names, regardless of their own locale and language settings.
- Search in filters is not case-sensitive.
- Multicurrency is not supported. When Analytics extracts your organization's default currency, it uses the currency for monetary values and doesn't convert to another currency.

SAQL Query Limitations

You can't filter, group, or sort based on the time fields generated for a date field, like <date_field>_Hour, <date_field>_Minute, and <date_field>_Second.

Sales Analytics Limitations

These limitations apply to Sales Analytics.

Sales Analytics Data Requirements

Sales Cloud data must meet the following requirements for Sales Analytics dashboards to function correctly:

- Use standard sales objects.
- Have at least one event and one task connected with an opportunity.
- Enable history tracking for Amount, Stage, and CloseDate fields on the Opportunities object.
- Cases must be connected to Accounts if you choose to import Cases data to Sales Analytics using the configuration wizard.
- There are two requirements if you choose to import Leads data to Sales Analytics using the configuration wizard.

  1. At least one lead must be converted to an opportunity.
  2. The lead must be connected to an account.

- There are two requirements if you choose to import Campaigns data to Sales Analytics using the configuration wizard.

  1. At least one opportunity must be connected to a campaign.
  2. At least one campaign member must be connected to a campaign.

- There are two requirements if you choose to import opportunity record types to Sales Analytics using the configuration wizard.

  1. At least one opportunity record type must be defined.
  2. The opportunity record type must be connected to at least one opportunity.

Sales Analytics Support for Salesforce Objects and Fields

Sales Analytics supports all Salesforce standard and custom objects and data. To add custom objects or additional fields not included when you first create the app, you need to update the Sales Analytics dataflow. For details see Create Datasets with the Dataflow.

When you first create the app it includes only a predefined set of objects and fields. Sales Analytics creates a dataflow that exposes selected fields from the following standard Salesforce objects:

- Accounts
- Users
- Roles
- Opportunities
- Products (Opportunities line item)
- Tasks
- Events

The fields provided are determined by the answers you provide when you create the app using the built-in configuration wizard.

Sales Analytics supports standard and custom fields on **standard Sales Cloud objects**. The fields provided are determined by the answers you provide when you create the app using the built-in configuration wizard.

Sales Analytics Support for Non-Salesforce Data

Sales Analytics does not support external data sources except a CSV file that contains quota data at the user level. Importing other external data requires an extra license. See your Salesforce representative for details.

To include data about quotas in Sales Analytics, you must upload a CSV file with the details. For more information, see Collaborative Forecasting and Quotas Data in Sales Analytics.

Other Contractual Sales Analytics Limitations

The Sales Analytics Apps license does not support use of Einstein Analytics platform bulk actions or Apex steps functionality. This limitation is contractual, not technical. Licensee agrees to strictly monitor its use of Analytics platform features.

Sales Analytics Limitations for Sales Cloud Einstein and Einstein Analytics Growth or Plus (Platform) Customers

Salesforce makes Sales Analytics available through three stock-keeping units (SKUs). Consult this chart to see limitations for each.

	Standalone	Sales Cloud Einstein	Einstein Analytics Growth or Plus
Data sources	Salesforce data and CSV file for quotas data (see Sales Analytics Support for Non-Salesforce Data, above)	Salesforce data	Salesforce and external data
Object support	Standard and custom objects	Standard objects	Standard and custom objects
Data volume	25 million rows	25 million rows	100 million rows to start
Can customize existing dashboards?	Yes	Yes	Yes
Can Create new dashboards?	Yes	No	Yes
Can customize existing datasets?	Yes	No	Yes
Can create new datasets?	Yes (using standard Salesforce objects and up to 10 custom objects)	No	Yes
Can create custom Analytics apps?	No	No	Yes
Supports Einstein Discovery and Community Cloud integration?	No	No	Yes
Supports bulk actions and APEX steps?	No	No	Yes
Supports Sales Cloud Einstein AI features?	No	Yes	No
Supports Salesforce Inbox?	No	Yes	No

Service Analytics Limitations

The following limitations apply to Service Analytics.

Service Analytics Data Requirements

Service Cloud data must include at least one each of the following for Service Analytics dashboards to function correctly: Events, tasks, closed cases, or published articles attached to a case or an opportunity. It also requires that your org have at least one contact ID associated with a case.

Custom formula fields on the Cases object must exist or be created for the SLA missed (text) and FCR (Boolean) fields.

Service Analytics Support for Salesforce Objects and Fields

Service Analytics supports all Salesforce standard and custom objects and data. When you first create the app by default it includes only a predefined set of objects and fields. The app creates a dataflow that exposes selected fields from the following Salesforce objects:

- Account
- Cases
- Contact
- User
- UserRole
- Task

Service Analytics also uses fields from the following options depending on the answers you select in the configuration wizard:

- Customer satisfaction (CSAT)
- Knowledge
- Business hours
- Case history
- Case record types
- Queues
- Opportunities
- Opportunity record types
- Events
- Telephony
- Live Agent
- Omni-Channel

Service Analytics supports standard and custom fields on standard Salesforce objects. The fields provided are determined by the answers you provide when you create the app using the built-in configuration wizard.

Service Analytics limits custom objects support to no more than 10 custom objects for each org that implements Service Analytics. This limitation is contractual, not technical.

To add custom objects or extra fields not included when you first create the app, you must update the Service Analytics dataflow. For details, see Create Datasets with a Dataflow. For details, see Create Datasets with the Dataflow.

More Service Analytics Limitations

Service Analytics does not support external data sources or registering new datasets from the app-generated dataflow.

Including CSAT score in dashboards/dataflow is optional. The app configuration wizard lets you associate CSAT from a custom case field or Custom Object associated to the Cases object.

You must manually add any security predicates or other dataset filters to the app dataflow.

The app does not support multi-hierarchy (team/manager) when you create it. You must manually add that functionality.

The Knowledge Usage dashboard currently reports on a single Article Type, which you select when you use the configuration wizard.

Adoption Analytics Limitations

These limitations apply to Adoption Analytics.

- Datasets created for the app count against row limits for your Analytics license.
- Includes only Analytics logs. For any Salesforce logs, use Event Monitoring.
- The first time you use Adoption Analytics, it may take 24 hours for data to collect in event logs before it can be registered in the app's datasets and dashboard.

Field-Level Security

Field-level security isn't available for external data that is uploaded via files. Field-level security that was implemented in the original database or Salesforce object isn't preserved when the data is loaded into an Analytics dataset. For more information, see the Analytics Security Implementation Guide.

Set Salesforce field-level security to enable the Analytics Integration User to see all fields used in your app—default fields and those selected in the configuration wizard. Integration users run the dataflow, and if they don't have proper field-level security permissions, the dataflow fails.

Analytics Templates

Limitations for Analytics templates are covered in the Help topic for each template.

Analytics on Mobile Devices

To view Analytics on a mobile device, use the Einstein Analytics mobile app for Android or iOS. Unlike the Salesforce app's Mobile Web option, Analytics isn't accessible from mobile browsers. However, Analytics dashboards embedded in web pages are available on mobile devices, with the limitations of embedded dashboards (for those limitations, see Embed Dashboards Everywhere).