Flosum

Flosum Backup & Archive
User Guide

A Quick Start Guide to Implementing and Using Flosum Backup & Archive

Backup & Archive Version:	4.3.0
User Pool App Version:	1.5.3
User Guide Version:	4.3
Last Updated:	July 2025

Table of Contents

Flosum Backup & Archive User Guide

Version: 4.x | **Audience:** Admins, Architects, Compliance Officers

Overview

Flosum Backup & Archive (B&A) is an enterprise-grade data protection solution built specifically for Salesforce environments. It enables you to back up, restore, and archive your Salesforce data and metadata securely, efficiently, and on your terms.

Whether you're safeguarding against data loss, reducing Salesforce storage costs, or meeting compliance requirements, Backup & Archive provides flexible options to protect your most critical assets.

Built on Salesforce and AWS, it provides AES-256 encryption, customizable retention, and easy restore options—ensuring data protection, compliance, and business continuity.

This guide walks you through the installation and use of Flosum Backup & Archive.

Key Sections

Set Up Your Tenant - Register for Flosum Backup & Restore and add your Salesforce Org.

Backup Operations - Backup of your Salesforce Org with full or partial backups.

Archive Operations - Archive your Salesforce data to save space and remove old objects.

Restore Operations - Restore lost or corrupted Salesforce data.

Search Operations - Search for and purge backed-up and archived data.

Export Operations - Export your backed-up data.

Analytics - Review charts of your backup operations and visualize your Salesforce data.

Prerequisites and Planning for a Successful Backup & Archive Implementation

Before implementing Flosum Backup & Archive, it's essential to align your environment with a few key prerequisites. These steps help ensure your deployment is secure, compliant, and optimized for performance, whether you're running a trial or rolling out organization-wide.

We recommend collaborating with your internal Salesforce Admin and Security teams early in the process to streamline setup and ensure long-term success.

Salesforce User Configuration

To ensure smooth connectivity and access to all relevant data, Flosum Backup & Archive requires a dedicated generic user with the following settings:

- Use a **Salesforce Standard License** (not Community or Platform)
- Assign the **System Administrator profile** with permissions for:
  - API Enabled
  - Query All Files
  - Manage Flows
  - Query All Files
  - Set Audit Fields Upon Record Creation
  - View All Data / View All Files (if applicable)

> ⓘ Using a dedicated generic user ensures continuity—if a personal admin account is deactivated, backup jobs may fail. A separate generic user also improves auditability and access control. You can also add additional users to the Backup & Archive solution through the User Pool Service to assist with administering your backups.

Network Access and Allowlisting

To maintain secure and reliable connectivity between Salesforce and the Flosum platform, your organization should allowlist specific domains in your firewall, proxy (e.g., Zscaler), and email filtering tools.

Also, allowlist these email domains to ensure delivery of system notifications:
- @flosum.app
- @flosum.com
- @flosum.tech

> ⓘ Missing alerts or authentication traffic can delay the implementation and verification of backups.

Encryption Key Requirements (BYOK)

Flosum supports Bring Your Own Key (BYOK) for AES-256 encryption, giving you complete control over your data privacy posture. To enable BYOK, your team must:

- Provide a 32-byte Base64-encoded encryption key
- Use a secure internal key management system (Flosum never stores your key)

> ⓘ BYOK enables your security team to define and enforce key rotation and storage policies that align with internal governance and regulatory standards.

SSO and Identity Provider Integration

For secure, centralized access control, Flosum supports Single Sign-On (SSO) via standard OAuth providers.

Supported identity systems:

- Google
- AWS Cognito
- Azure Active Directory

SSO configuration and role assignment are managed through Flosum's User Pool. Detailed setup instructions are available in our deployment guides.

> ⓘ SSO simplifies user management, improves login security, and enables audit-ready access control—all essential for regulated or enterprise environments.

Generate AES-256 Encryption Key

Create an encryption key using your preferred method. Below are some options for generating encryption keys. Once you've created the key, store it securely (e.g., in a password manager). This key will be required during tenant registration and the Connect Org process.

> ⚠ Never share or email this key. If lost, encrypted data is unrecoverable.

Password Manager (Recommended)

Use a reputable password manager, such as Bitwarden, 1Password, or Dashlane. This is the easiest and safest option for most users.

- Length: 44 characters
- Character sets: A–Z, a–z, 0–9, +, /

- Base64 encoding: Enabled (if the option is available)

Command Line (For Technical Users)

Use OpenSSL to generate a secure key.

1. Open your terminal or PowerShell window.
2. Run the following command: `openssl rand -base64 32`
3. Copy the generated 32-byte key. Store it securely (e.g., password manager).

Python Script

Use Python to generate a secure key.

```python
import os
import base64
key = base64.b64encode(os.urandom(32)).decode('utf-8')
print(key)
```

- Copy the generated 32-byte key. Store it securely (e.g., password manager).

Set Up Your Tenant

This section walks you through setting up your tenant, establishing your login credentials, and connecting your Salesforce org. This tenant will act as a secure, dedicated storage container for all your backup data.

Self-Register Your Flosum Tenant
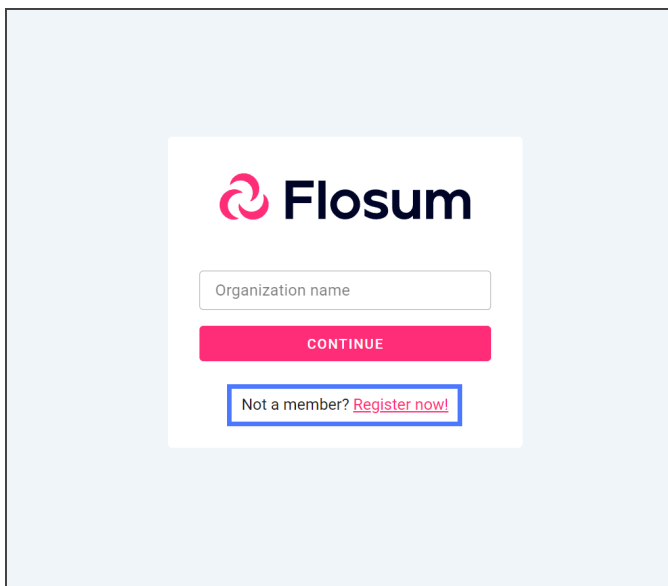
You can self-register to create a tenant on the Flosum regional instance, as well as your admin account on the Flosum User Pool, which you will use in the next step.

You will receive a confirmation email when your tenant is provisioned (typically within 30 minutes). Click the link that is provided to continue.

1. Go to the Flosum Backup & Archive Registration page. Choose the Instance URL for your desired region.

Region	Backup URL
US	backup-us-v3.flosum.app
Germany	backup-de.flosum.app
Japan	backup-jp.flosum.app

2. Click the **Register Now!** link.

3. Enter the following details to create your tenant:
   a. **Organization Name** (Save this name; it will be needed for future logins to the tenant.)
   b. **First Name**
   c. **Last Name**
   d. **Email Address**
   e. **Password** Use a strong password that is at least eight (8) characters long and includes one (1) letter, one (1) number, and one (1) special character.

4. Click **SIGN UP**.

Log In to the Flosum User Pool (Optional)

If you have Single Sign-On (SSO) or Multi-Factor Authentication (MFA) protocols in place, you may need to access the User Pool Application to configure them.
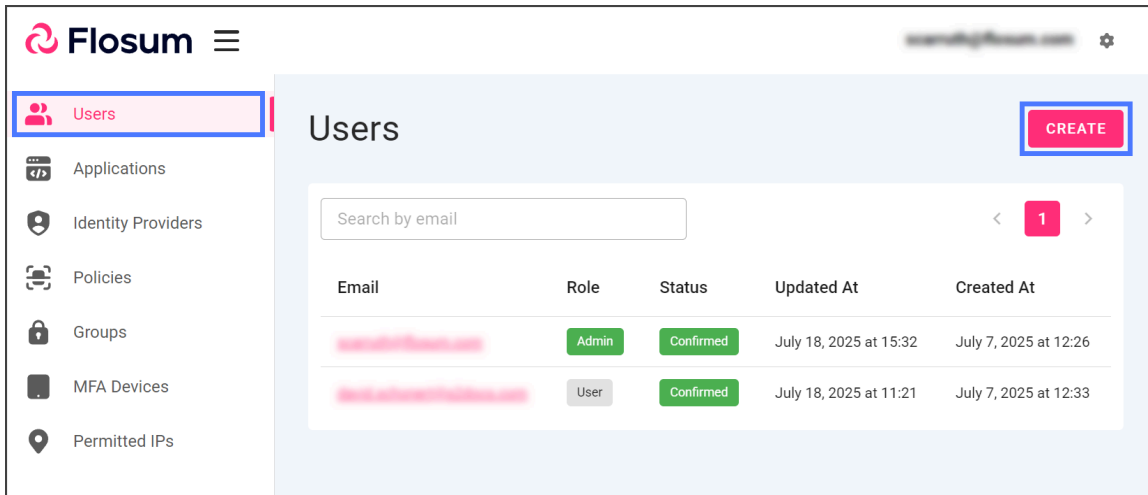
1. Navigate to the User Pool URL corresponding to the region you selected for your tenant creation.

Region	User Pool URL
US	`user-pool-us.flosum.app`
Germany	`user-pool-de.flosum.app`
Japan	`user-pool-jp.flosum.app`

2. Log in with your previously established admin account.

Add Users

1. Click **Users** from the sidebar menu.

2. Click **Create** to add additional users.

Add Single Sign-On (SSO)

The User Pool app supports integrating SSO providers using the OpenID Connect (OIDC) protocol, allowing users to authenticate using corporate credentials, providing a seamless and secure login experience. You can configure multiple identity providers if your organization uses separate providers for testing and production.

1. Click **Identity Providers** from the sidebar menu.

2. Click **Create** to add an SSO.
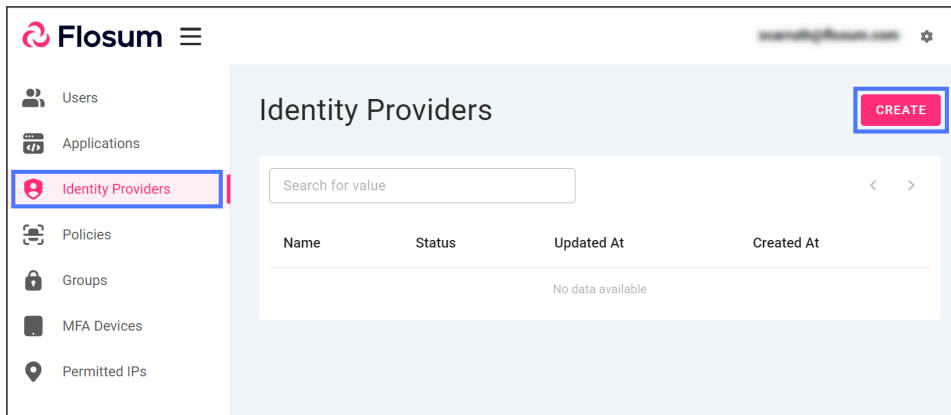
3. Refer to the [Flosum Knowledge Article - Configuring Identity Providers for SSO in the User Pool App](#) article for more detailed instructions to complete this.

4. After configuring SSO, the Flosum Backup & Archive Login Screen will display a **LOGIN WITH SSO** button at the bottom.
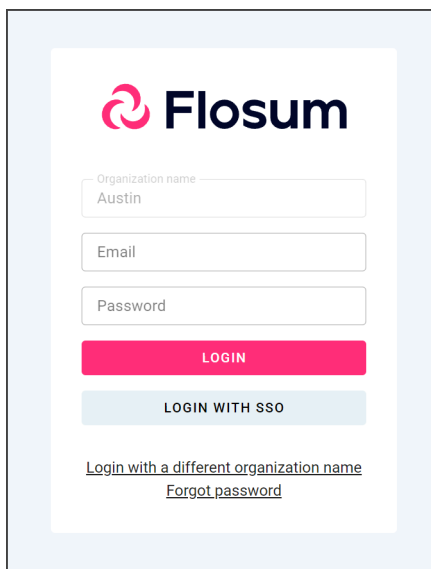
Add Multi-Factor Authentication (MFA)

MFA adds an extra layer of protection to your Flosum User Pool login. By requiring both a password and a time-based one-time passcode (TOTP), MFA significantly reduces the risk of unauthorized access and boosts your organization's overall security. Flosum Backup & Archive supports TOTP-based multi-factor authentication (MFA) using common mobile authenticator apps, such as Google Authenticator or Microsoft Authenticator.

1. Click **MFA Devices** from the sidebar menu.

2. Click **Add** to add an MFA device.
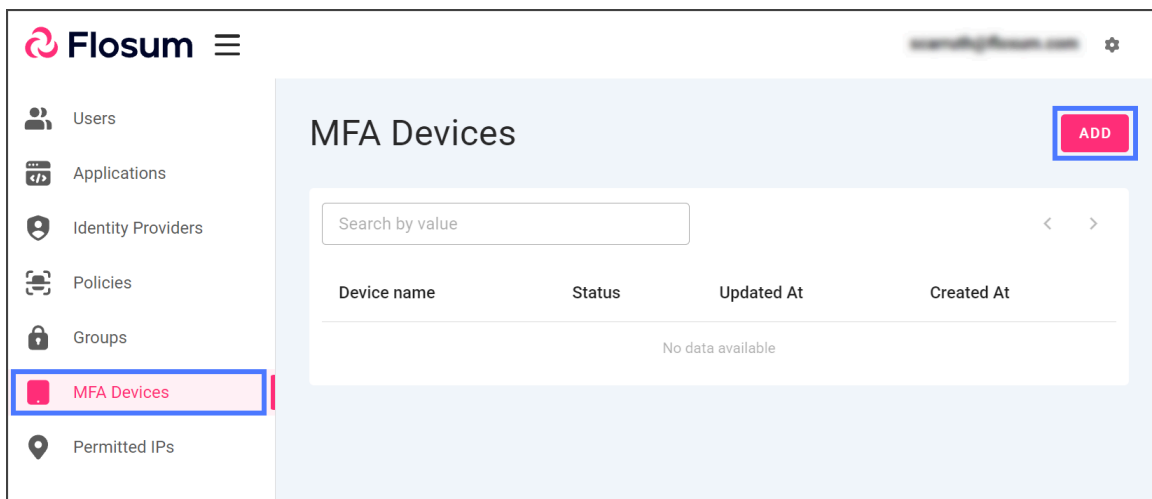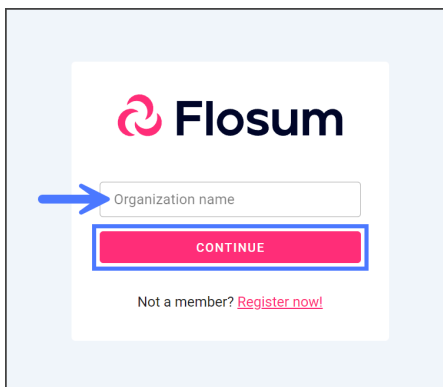
3. Refer to the [Flosum Knowledge Article - Setting up Multi-Factor Authentication in User Pool](#) article for more detailed instructions to complete this.

Log in to the Flosum Backup & Archive Application

Return to the Flosum Backup & Archive application via the URL previously used to create your tenant.
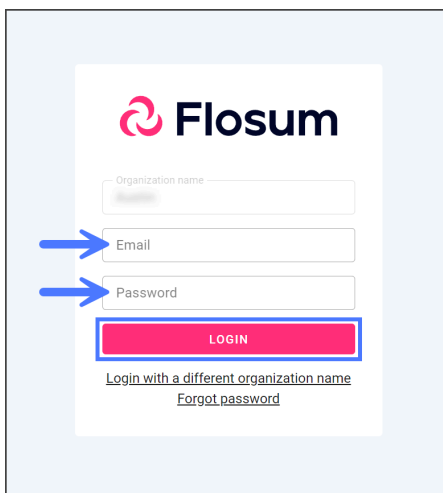
Region	Backup URL
US	backup-us-v3.flosum.app
Germany	backup-de.flosum.app
Japan	backup-jp.flosum.app

1. Provide the **Organization name** that you created earlier.

2. Click **Continue**.

3. Provide the **Email** and **Password** you provided earlier.

4. Click the **LOGIN** Button.
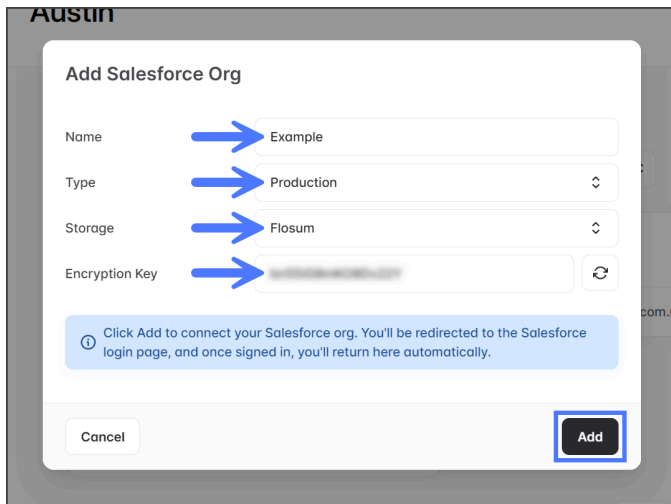
Connect Your Salesforce Org

1. In the **Flosum Backup & Archive** application, navigate to the **Home** page.

2. Click **Add Salesforce Org**.
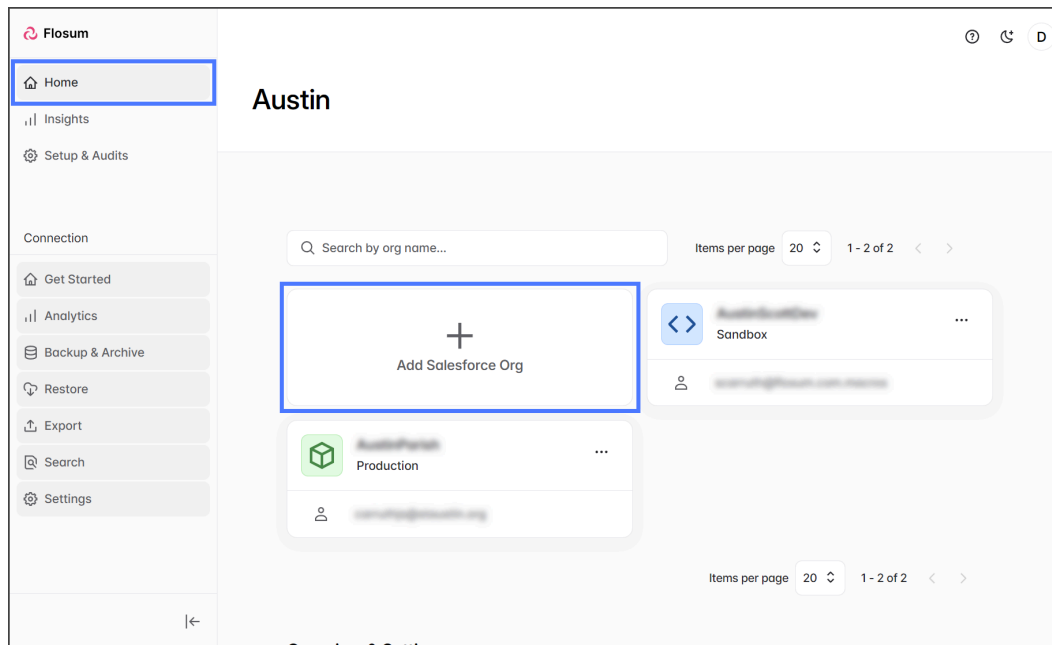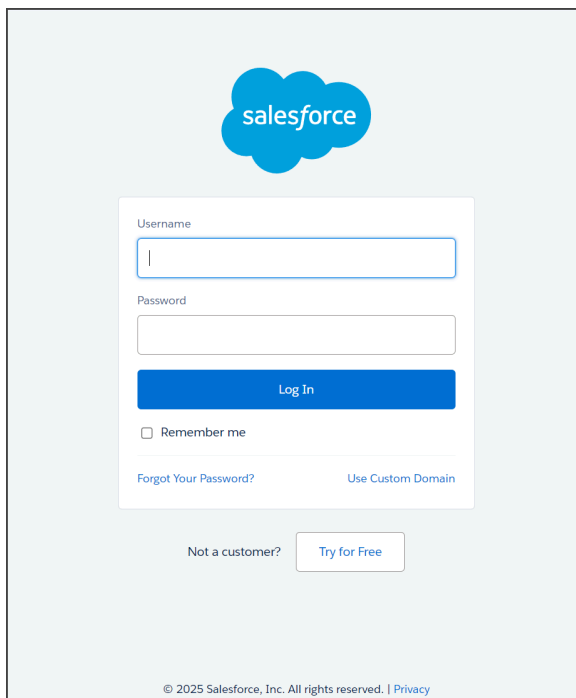
3. The **Add Salesforce Org** dialog will open.

4. Enter the **Name** of your Salesforce Organization that you will back up.

5. Select **Type** and choose either **Production** or **Sandbox.**

6. Select **Flosum** for Storage.

7. Enter the **Encryption Key** that you created earlier or use the one provided.

8. Click the **Add** button.

9. Authenticate via **Salesforce OAuth** (you'll be redirected to Salesforce).

10. Log in to Salesforce using an Admin account for your Org.

11. Grant access as requested.

Initial Encryption Service Load

When first connecting, the **encryption service** will be set up, which may take some time as the system establishes an initial connection to your Salesforce organization. If your login user has **System Administrator permissions** in Salesforce, this process will complete automatically.

If the service continues to load indefinitely:

- Ensure the user has full permissions.
- Contact Flosum Support if the issue persists.

Once loaded successfully, you'll be directed to the **Get Started** page for the Salesforce org you connected.
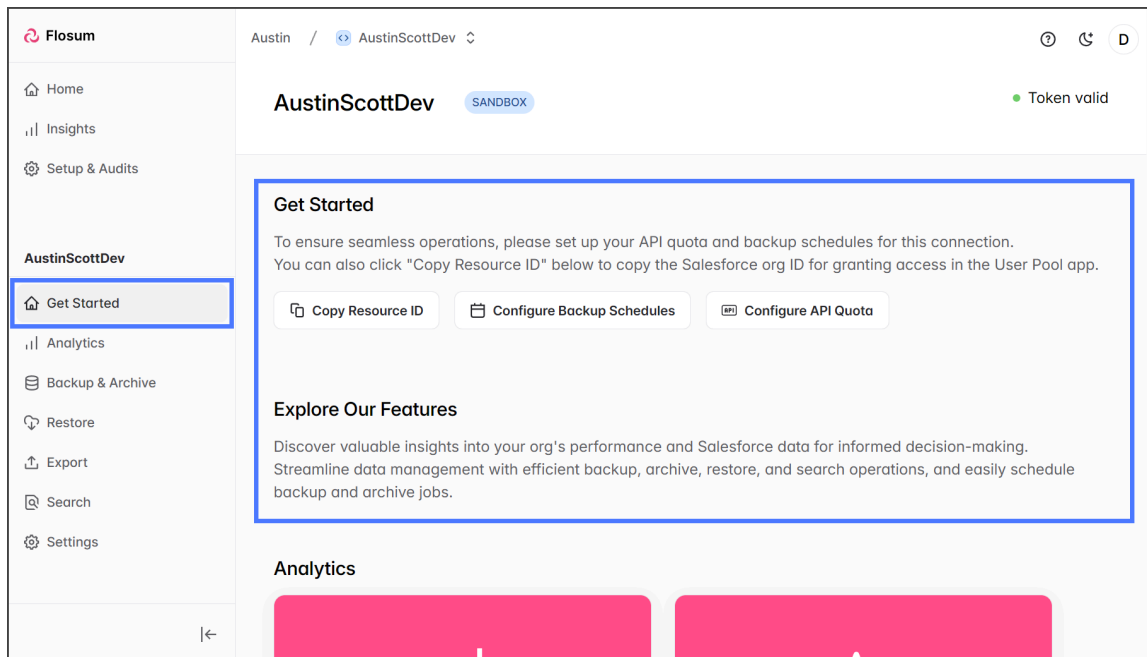
Backup Operations

Flosum offers two methods for performing Composite Backups: a full **Composite Backup** and a T**emplated Composite Backup**. The Composite Backup allows you to back up all your data in a single step. The Templated Composite Backup provides the flexibility to select specific objects, data, and files for inclusion. Both options can be executed immediately or scheduled for automatic runs at set intervals.

The Backup Operations section first explains System and User scheduled backups and how to edit and disable them. Next, it provides instructions for creating a Composite backup and a Templated backup.

System Scheduled

Each Salesforce org has two **system-scheduled** backup jobs: a **Default Composite Backup** and a **Default Composite & Sync Deleted Backup**. These jobs are managed by the system, and while they can't be deleted, you do have some control over when the jobs are scheduled to run. The section below explains how each default backup operates.

Default Composite Backup & Default Composite & Sync Deleted Backup

Flosum offers two backup methods: Composite Backup and Composite & Sync Backup. Each method plays a specific role in maintaining comprehensive, restorable snapshots of your org's data.

Default Composite Backup:

A Default Composite Backup is a lightweight process that tracks changes across your Salesforce org daily. After an initial full composite backup has been created, it saves any new, modified, or soft-deleted (Recycle Bin) records. By default, this system backup runs daily and can be used as an alternative to a user-defined composite backup.

- Tracks new and updated records.
- Flags records that are deleted and sent to the Recycle Bin.
- Optimized for daily execution.

Composite & Sync Backup:

A Default Composite & Sync Backup is a more intensive method that compares every record in your live Salesforce org to the ones stored in Flosum's backup repository. It detects even permanently deleted records, ensuring full fidelity. By default, this system backup runs monthly to detect purged records and ensure backup completeness. While a monthly backup schedule is recommended, you can change this backup to run on a weekly basis.

- Performs a full record comparison.
- Flags hard-deleted records that are no longer in Salesforce.
- Identifies discrepancies between the org and the backup.

Feature	Composite Backup	Composite & Sync Backup
Frequency	Daily	Monthly
Captures new/modified records	✅	✅
Captures soft-deleted (Recycle Bin) records	✅	✅
Captures hard-deleted records	❌	✅
Performs full record comparison	❌	✅
System performance impact	Low	High

Edit Default Backups
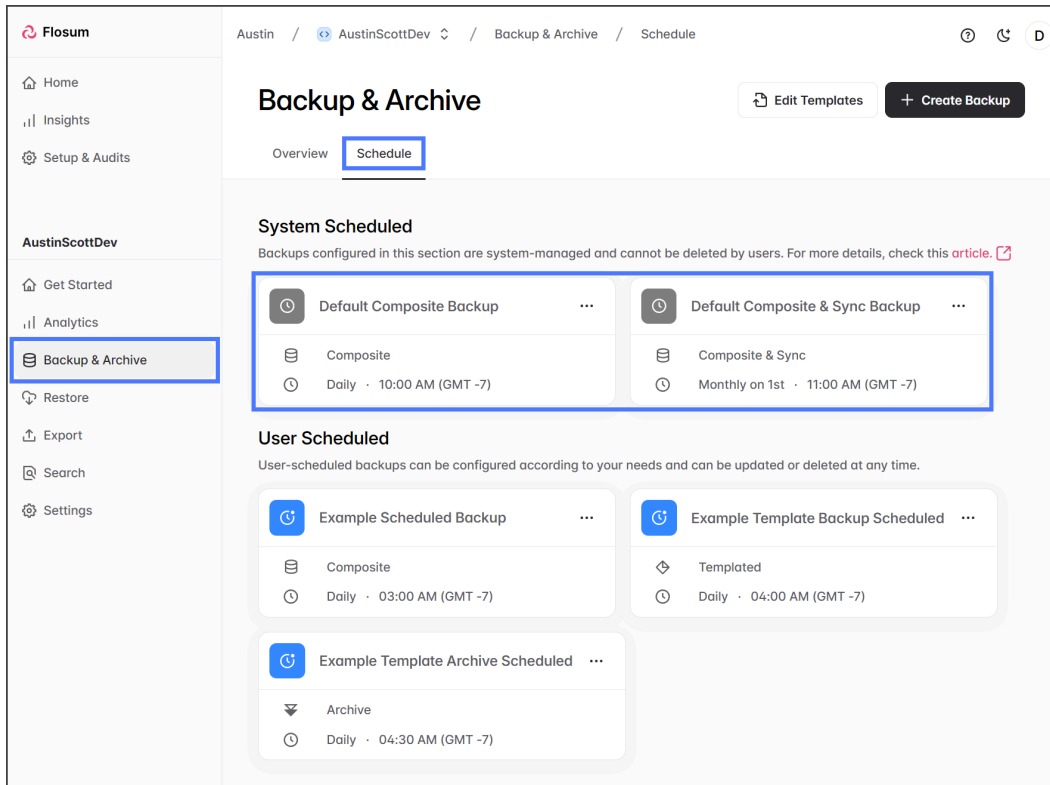
The schedules and job settings for the **Default Composite Backup** and **Default Composite & Sync Backup** can be changed.

1. From the **Home** page, select the **Org** to edit a default backup for.
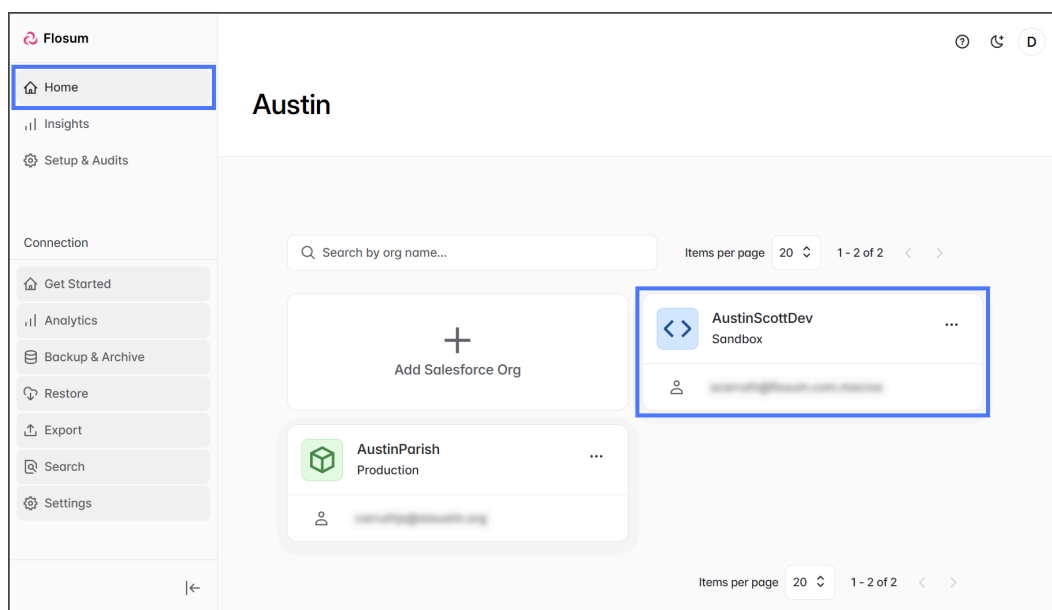
2. Click **Backup & Archive** from the sidebar menu.

3. Click the **Schedule** tab.
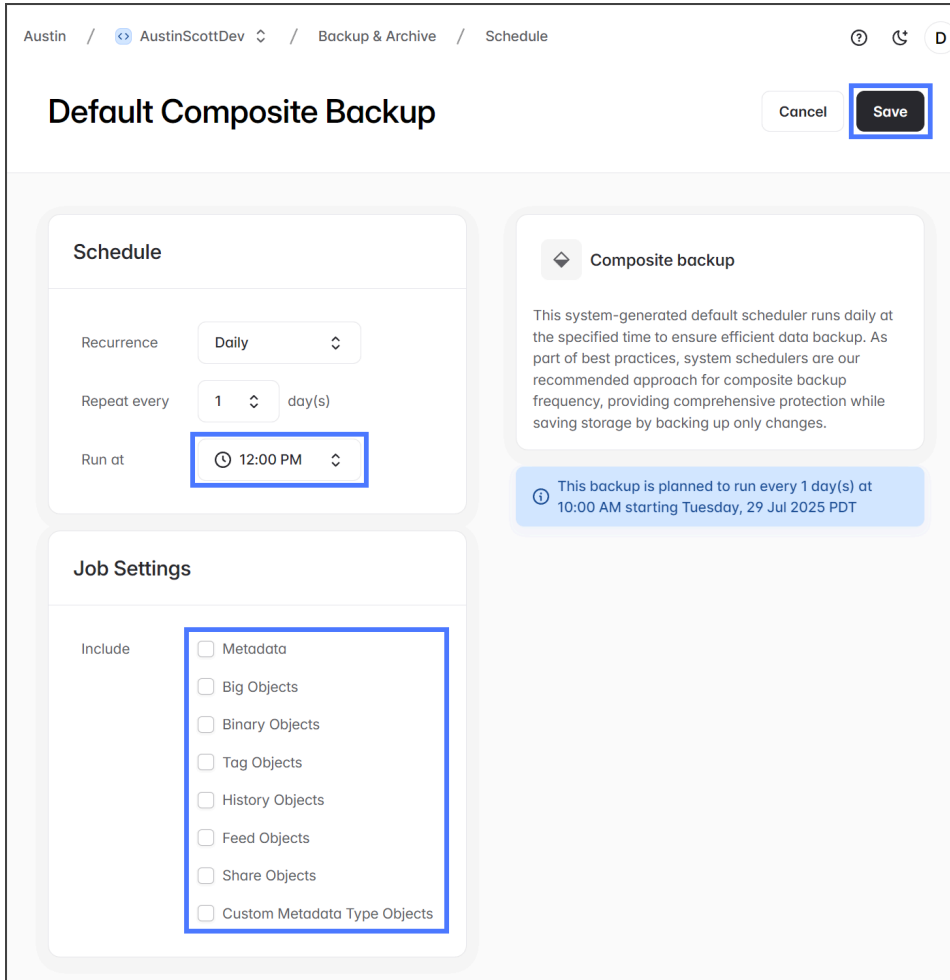
4. Click one of the **Default Backups**.

Default Composite Backup:

- The schedule for the **Default Composite Backup** is set to run daily, and only the **Run at** time can be changed.

- The **Job Settings** section allows you to check any of the object checkboxes to include or exclude from the backup.

- After making changes to the backup job, click **Save**.

Default Composite & Sync Backup:

- The schedule for the **Default Composite & Sync Backup** can be set to recur **Monthly** or **Weekly**. Click the **Recurrence** selector to switch between monthly and weekly options.

- For **Monthly** schedules, you can choose to set a fixed day each month or select the first or last occurrence of a specific day of the week. You can also set the time of day the backup runs.

- For **Weekly** schedules, you can select the number of weeks between runs (1-4) and the day of the week. You can also set the time of day when the backup runs.

- The **Job Settings** section allows you to check any of the object checkboxes to include or exclude from the backup.

- After making changes to the backup job, click **Save**.

User Scheduled Backups

The schedules and job settings for User Scheduled backups can be modified, or the job can be completely deleted. The options for adjusting a backup job's settings and schedule are the same as when creating a new one. Refer to the following sections for instructions to better understand the available options.

- [Composite Backup](#)

- [Templated Backup](#)
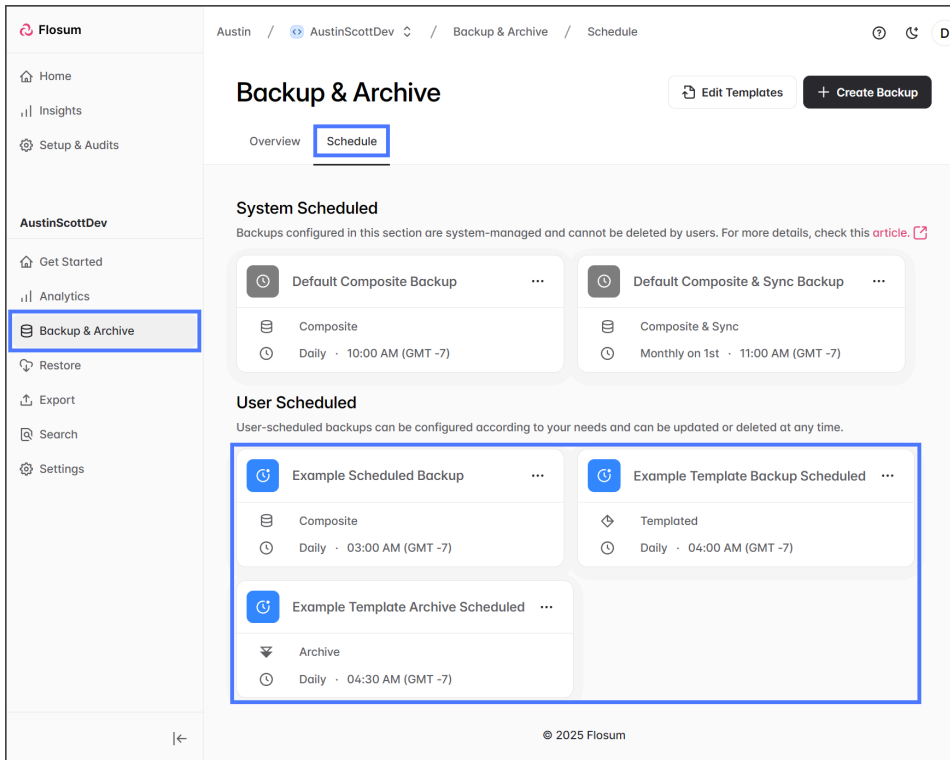
> ⓘ For a templated backup, while you can edit the template, you cannot change which template the backup job is using.

1. From the **Home** page, select the **Org** to edit a backup for.
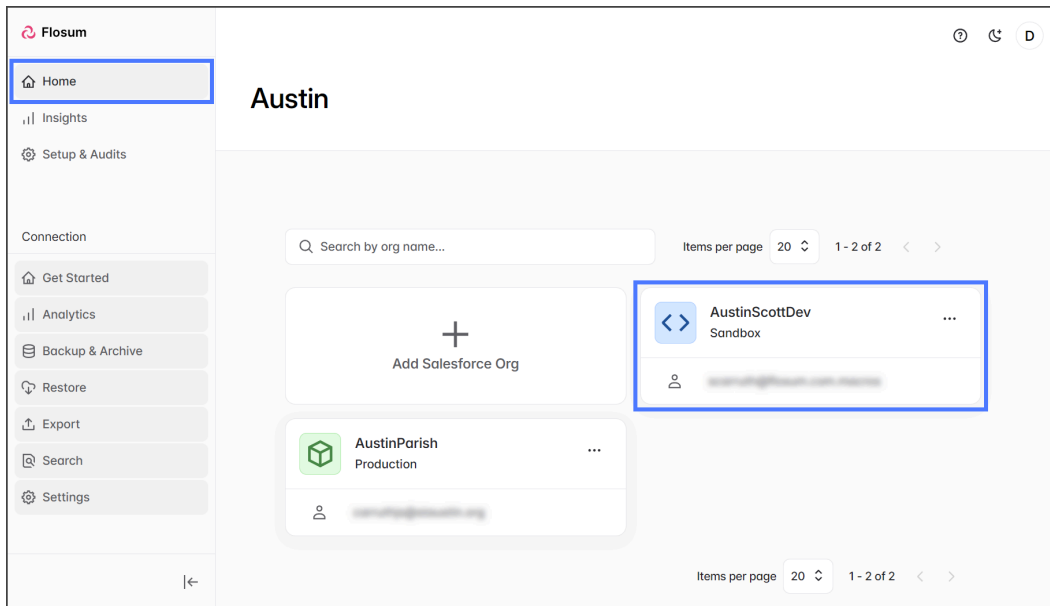
2. Click **Backup & Archive** from the sidebar menu.

3. Click the **Schedule** tab.

4. Click one of the **User Scheduled** backups.

Delete User Scheduled Backup

A User-Scheduled backup can be deleted permanently and will no longer be run.

1. Click the **User Scheduled** backup to delete.
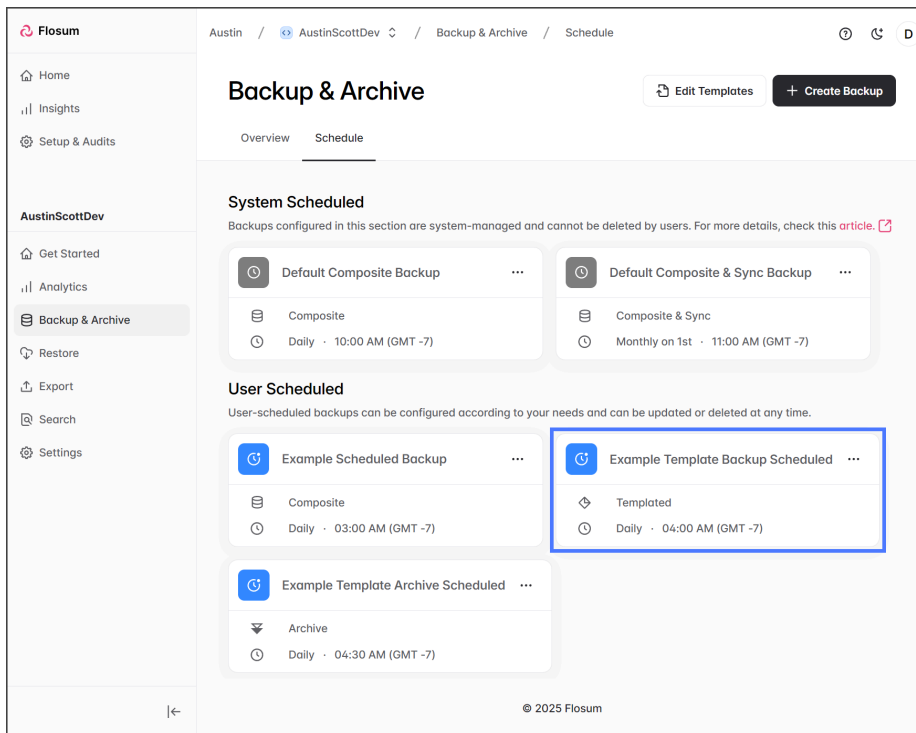
2. Click **Delete**. No confirmation dialog will be displayed.
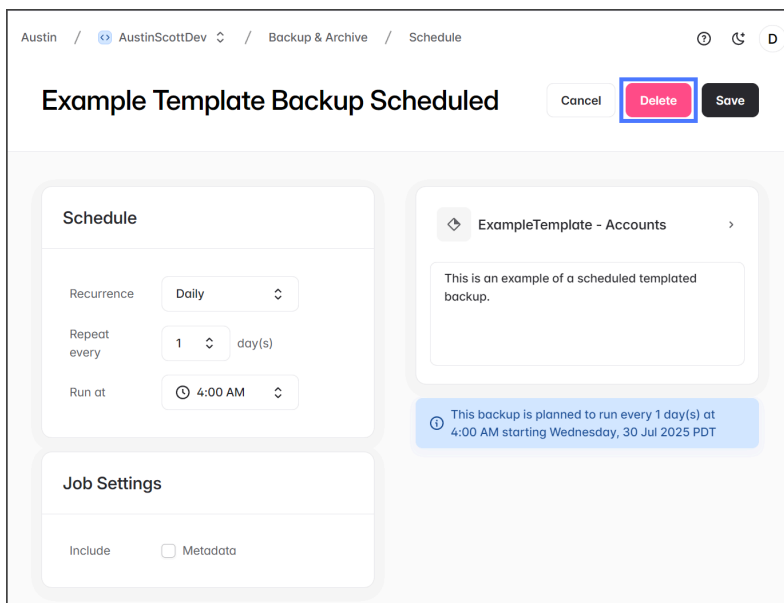
Disable Scheduled Backups

You can turn scheduled backups on or off for each organization. The default setting is **Enabled.** When scheduled backups are **disabled,** neither system nor user scheduled backups will run.

1. From the **Home** page, select the **Org** to edit a backup for.
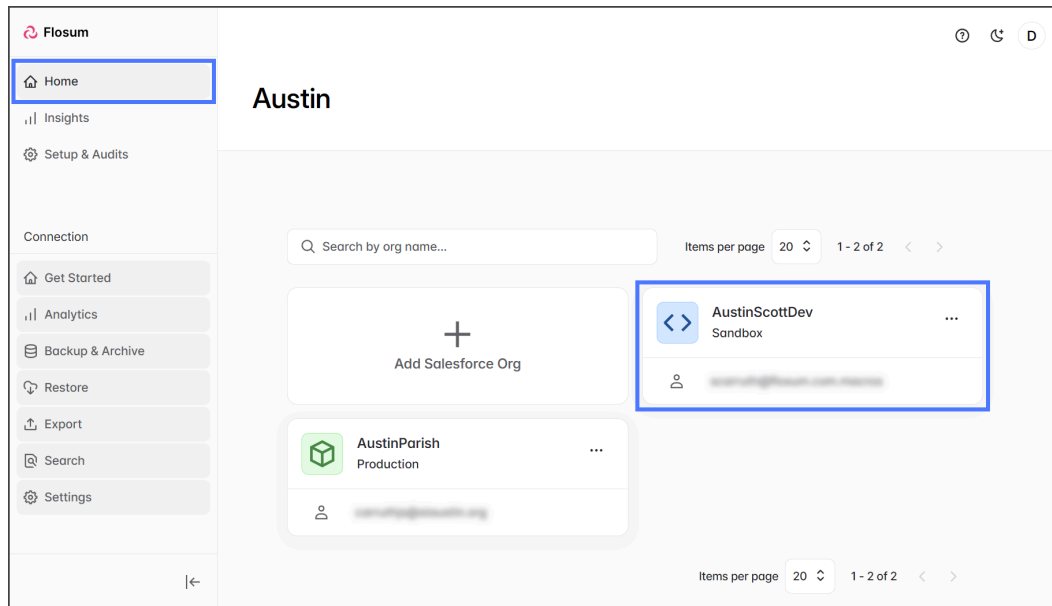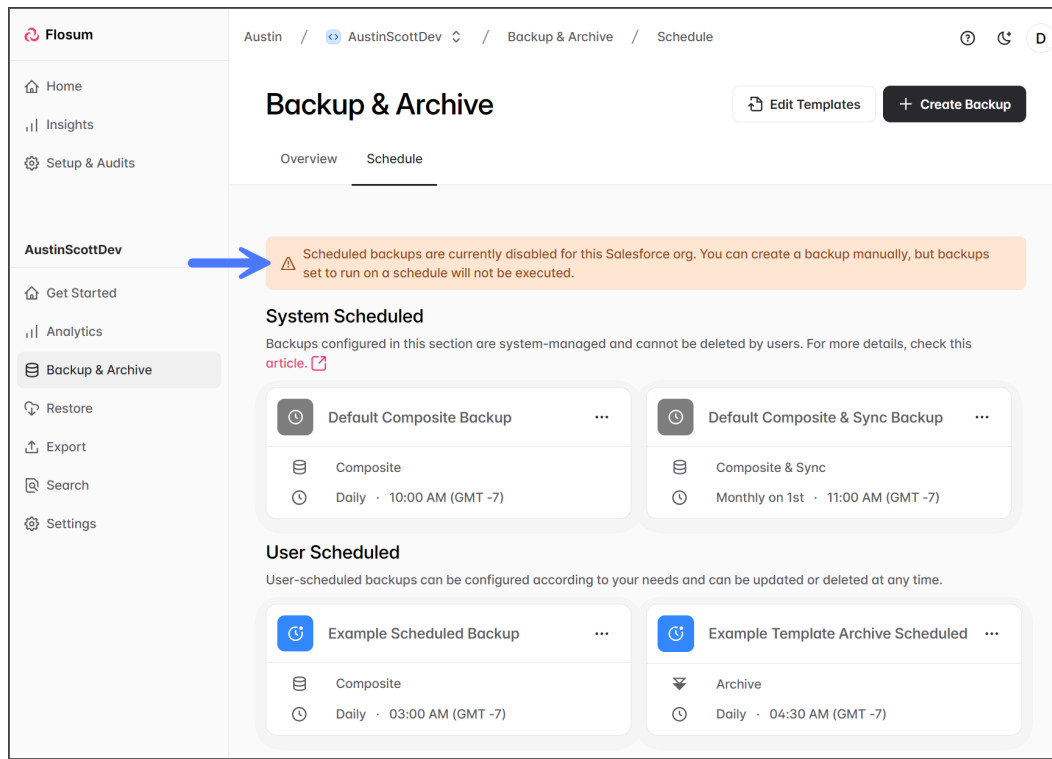
2. Click **Settings** from the sidebar menu.

3. On the **General** tab, scroll down to the **Manage Operations** section.

4. Click the **Scheduled backups** toggle to change from **Enabled** to **Disabled**. Both system and user scheduled backups will no longer run.
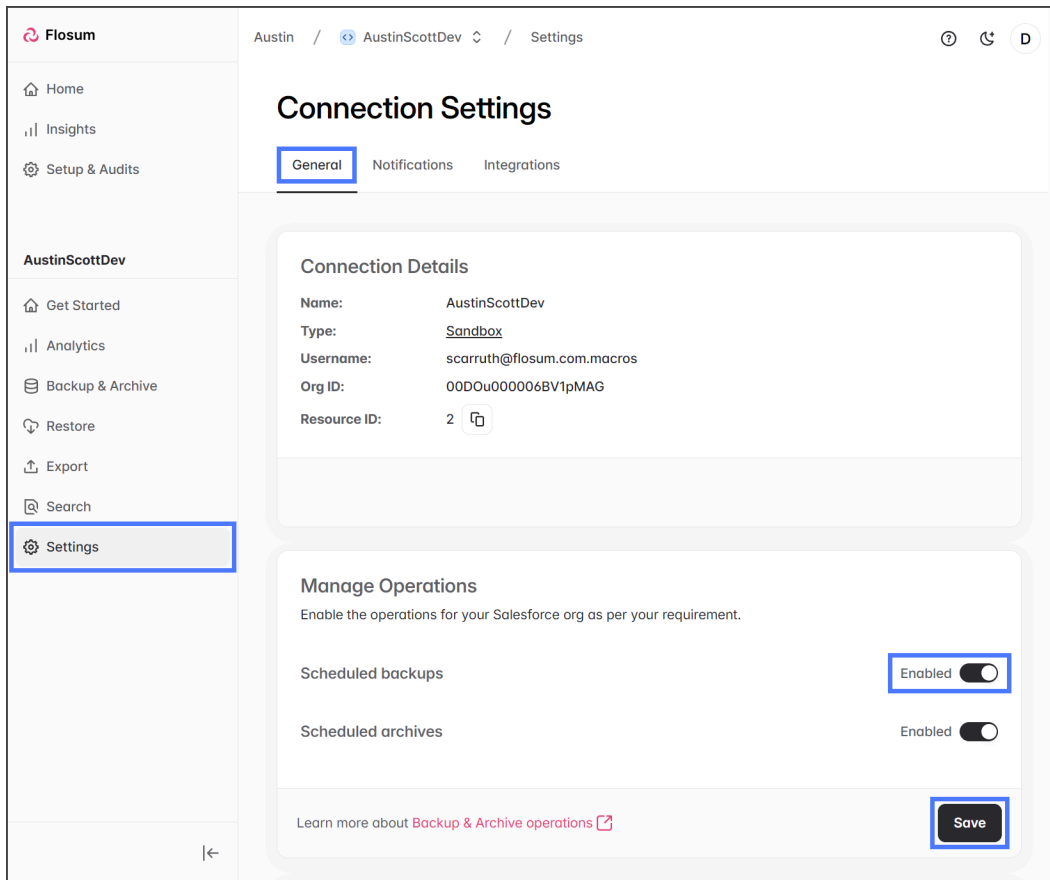
5. Click **Backup & Archive** from the sidebar menu.

6. Click the **Schedule** tab.

7. Confirm that the **Scheduled backups are currently disabled** warning is displayed.

Composite Backup

A Composite Backup backs up all objects, data, and files as selected in the Job Settings. The first time you run a Composite Backup, it takes a complete backup of your Salesforce organization. Subsequent backup jobs will then only backup the data and files that have changed. You can choose to run a backup immediately or schedule it to occur at a set interval.

Create a Composite Backup

1. From the **Home** page, select the **Org** to backup.

2. Click **Backup & Archive** from the sidebar menu.

---
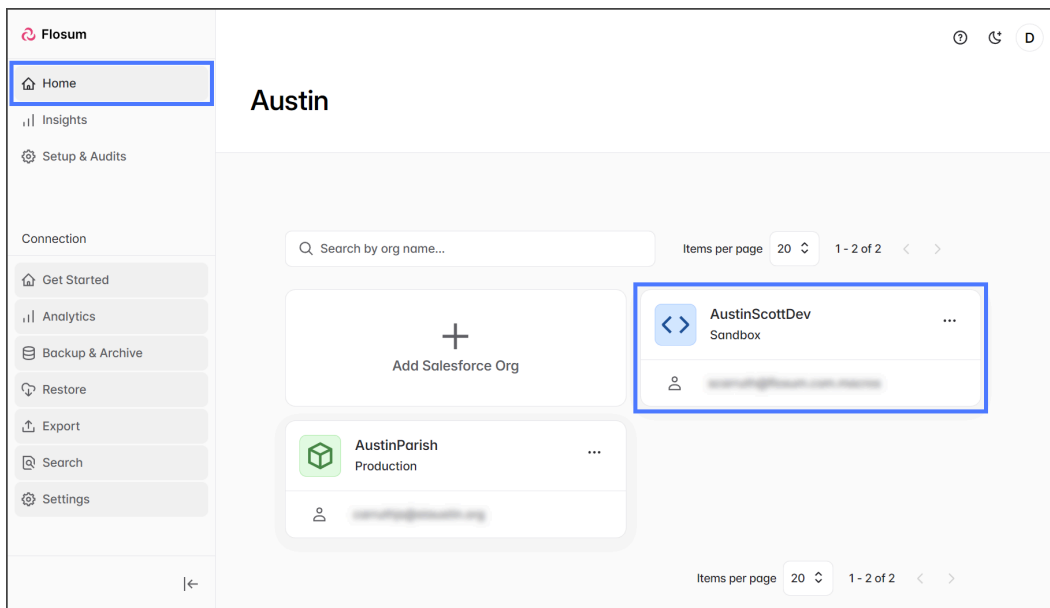
3. Click **Create Backup**.
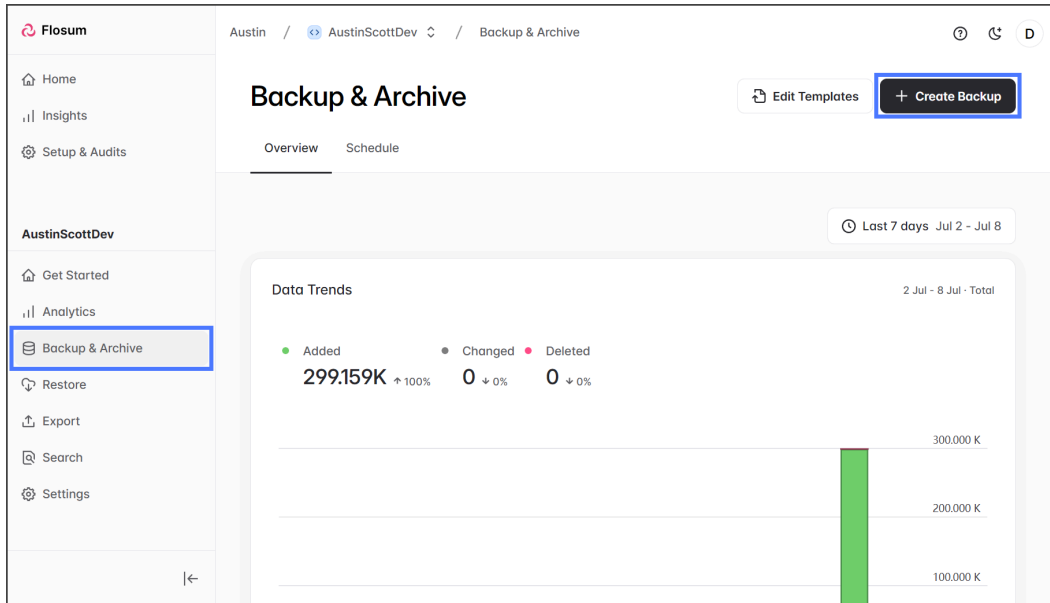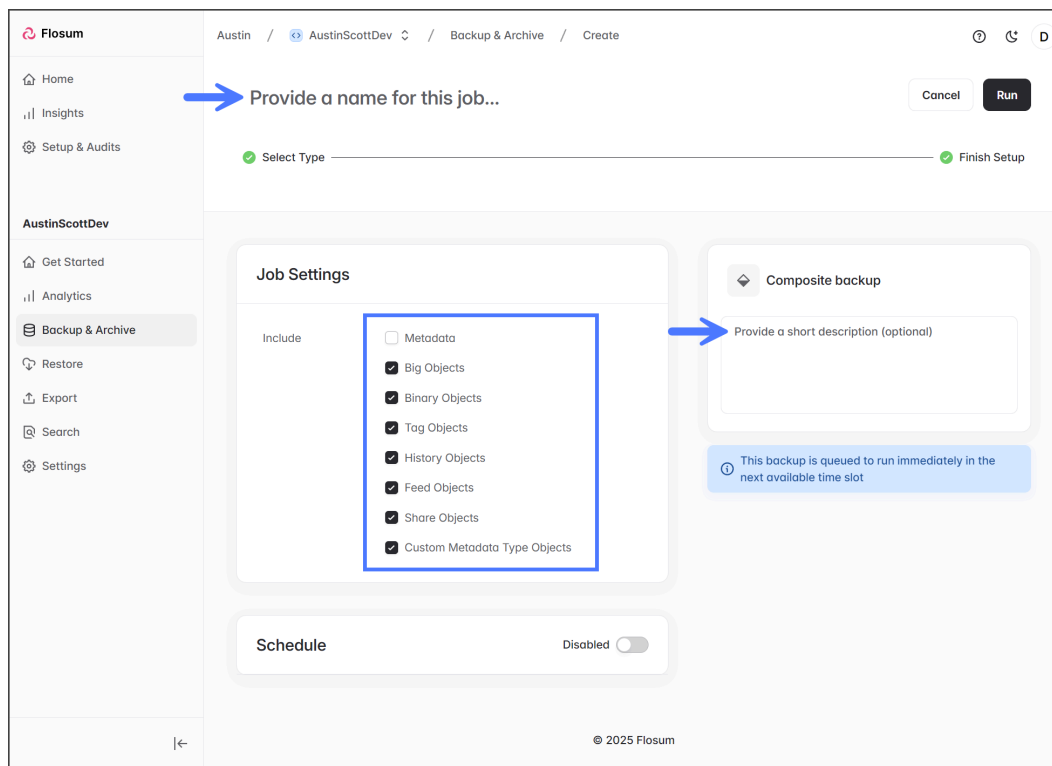
4. Click **Composite Backup**.
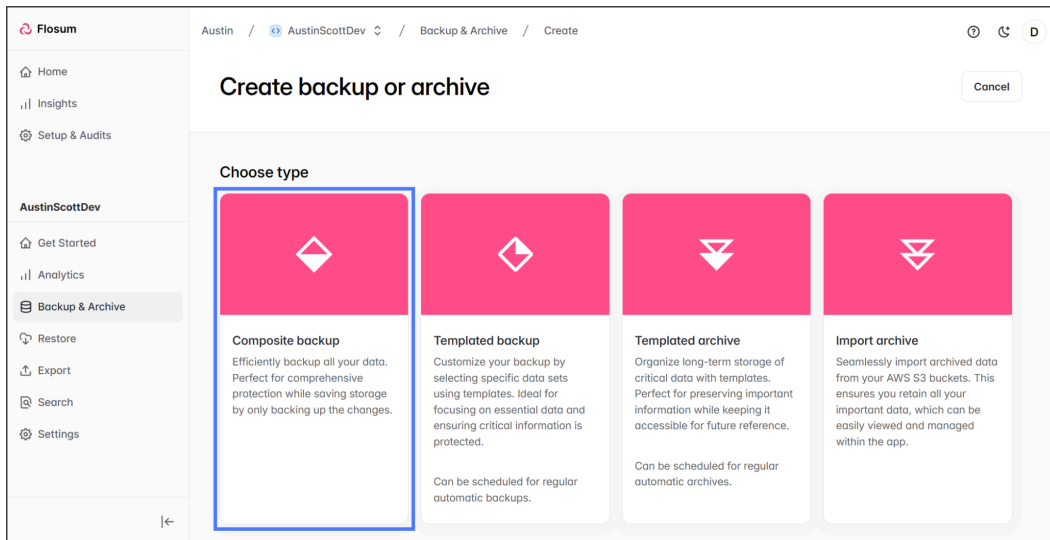
5. Enter a name for the backup job.

6. Select the **Job Settings** checkboxes for the objects to back up. You can leave the default options or choose a custom selection, including Metadata for the backup job.

7. (Optional) Enter a description of the backup in the **Composite Backup** textbox.
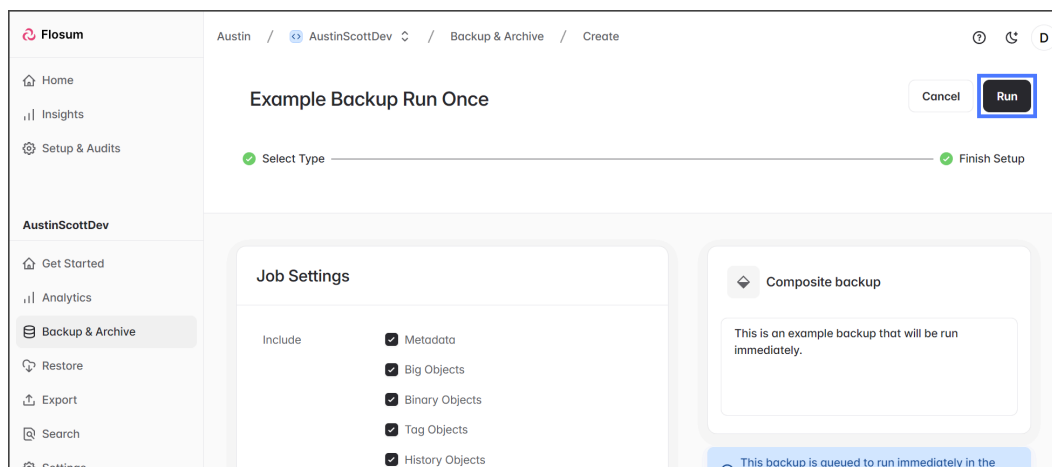
8. Click the **Run** button to start the Composite Backup.
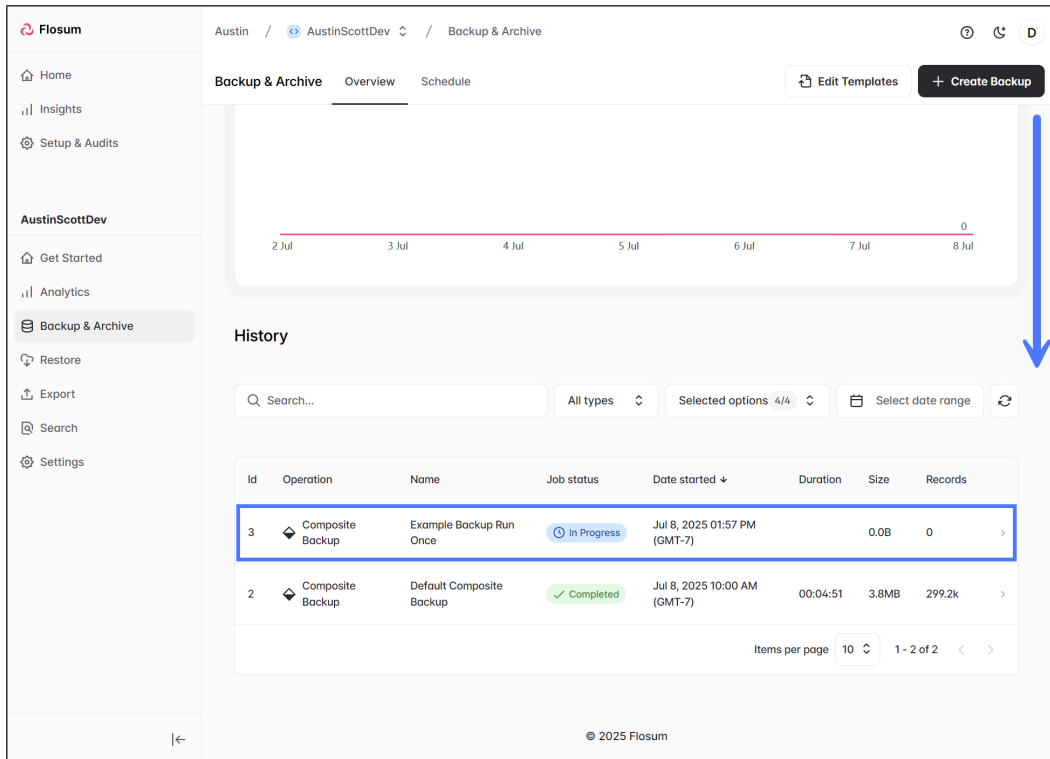
9. The Composite Backup job immediately.

10. Scroll down to the **History** table to view the status of the Composite Backup Job.

Schedule a Composite Backup

Alternatively, you can schedule your Composite Backup to run at a specific date and time interval. The process is similar to creating an immediate backup.

1. Complete the steps outlined in the [Create a Composite Backup](#) section above. Before clicking **Run**, enable the schedule option.

2. Switch the **Schedule** toggle to **Enabled**.

3. Select the **Recurrence** of the backup to run **Daily**, **Weekly**, or **Monthly**.

4. Configure the **Schedule** options. Daily, Weekly, and Monthly each have different options to set the time and date the backup is run.

5. Click the **Schedule** button to schedule your backup job.

6. Confirm the schedule is correct and click **Save**.

View Scheduled Backups

All scheduled backups for the selected Org will appear on the **Schedule** tab of the **Backup & Archive** section. Any scheduled backups you have created will be found in the **User Scheduled** section.

Templated Backup

A Templated Backup allows you to be more granular with what objects, data, and files are backed up. The first time you run a Templated Backup, it takes a complete backup of the selected data of your Salesforce organization. Subsequent backup jobs will then only backup the data that has changed. You can choose to run a backup immediately or schedule it to occur at a set interval.

Create a Templated Backup

1. From the **Home** page, select the **Org** to backup.
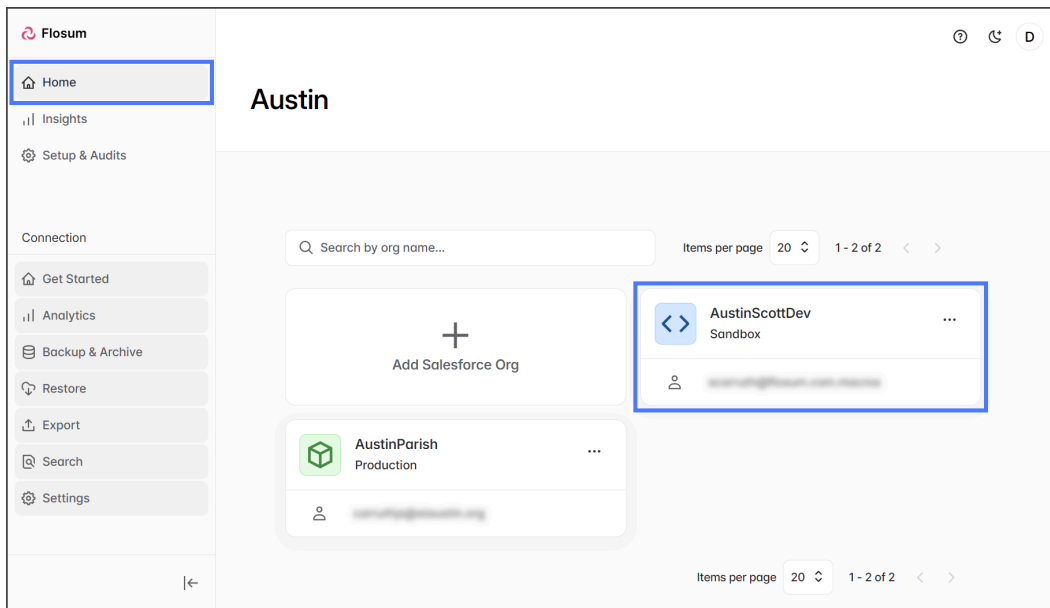
2. Click **Backup & Archive** from the sidebar menu.

3. Click **Create Backup**.
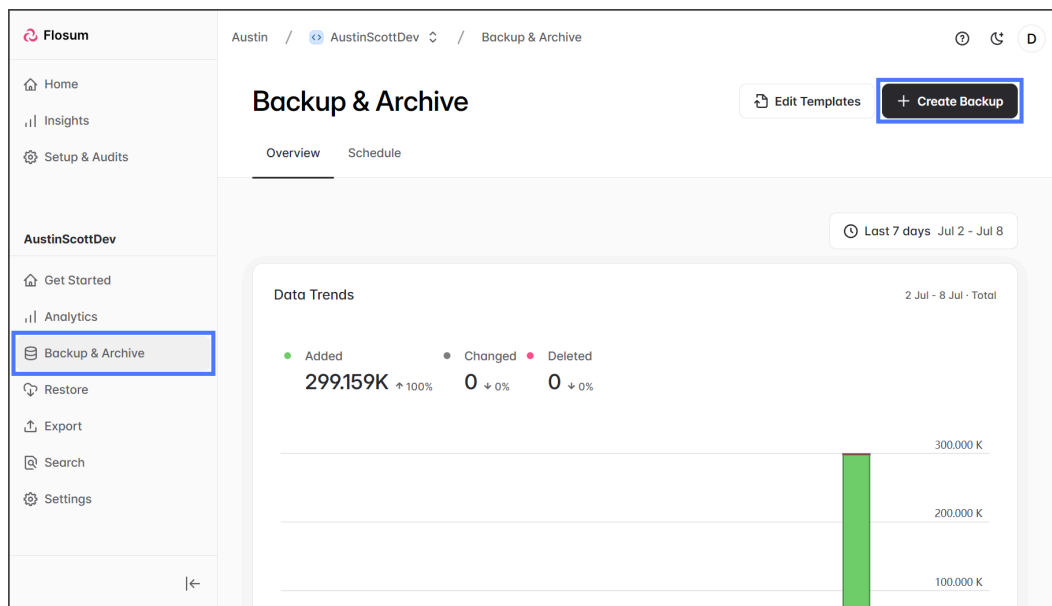
4. Click **Templated Backup**.
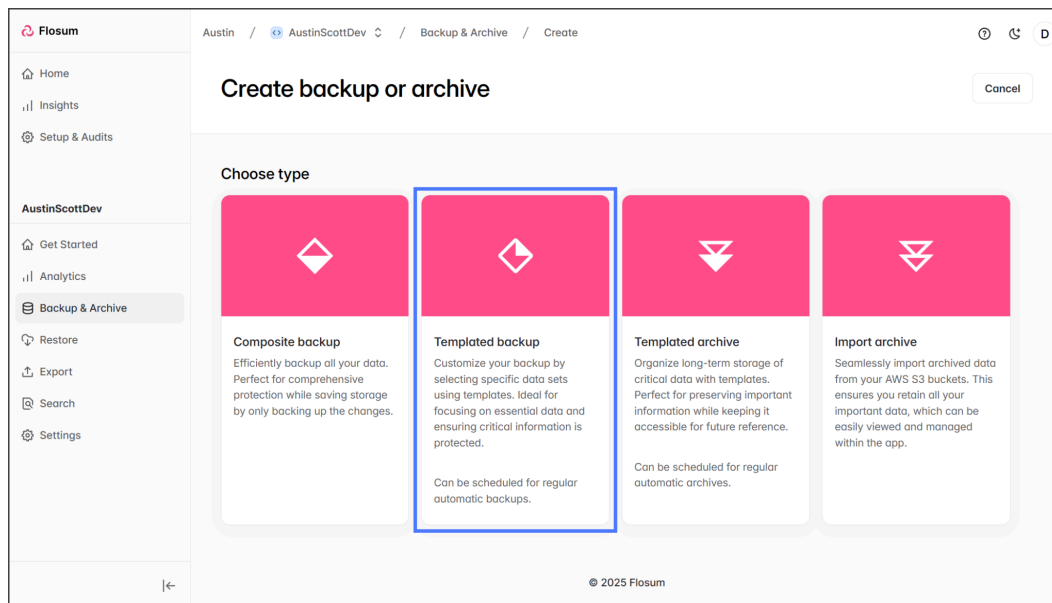
Create a Template

If there are no templates or you need to create a new one, follow the instructions below. Skip to [Finish Creating Templated Backup](#) if you don't need to create a template.

1. Click **Create Template** if there are no templates or if you need to create a new one.
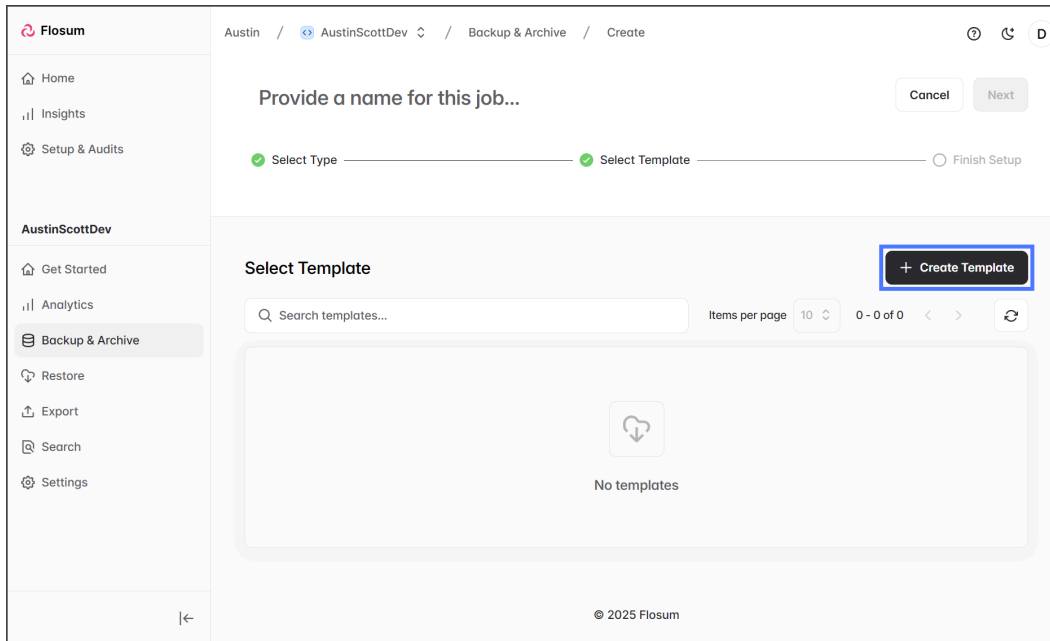
2. Enter a **Name** for the template.

3. Enter a helpful **Description** of the template's purpose in the optional **Backup Template** textbox.

4. Click the **Add object** menu button to select the Salesforce Objects to include in the template.
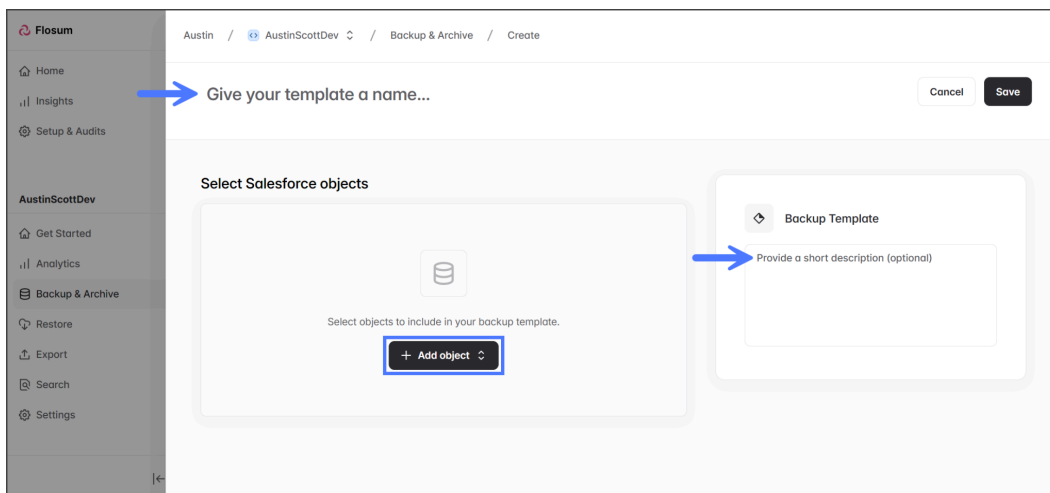
5. Search or browse for objects from the menu.

6. Check the objects you want to add.

7. Click **Add** to add all of the selected objects.
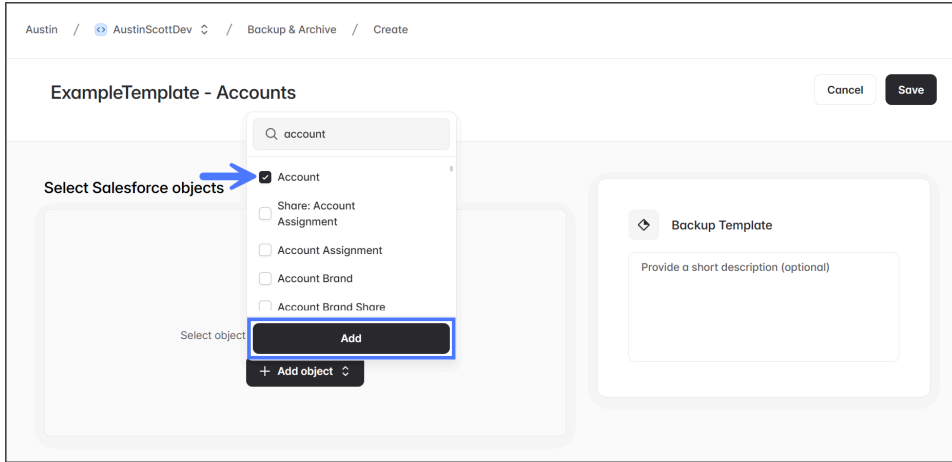
8. Once an object is added, you can add one or more child objects.

> ⓘ To the right of the object's name is a count of **Add/Available** child objects. In this example, the **Account** object has **123** child objects, and **0** of them have been added.
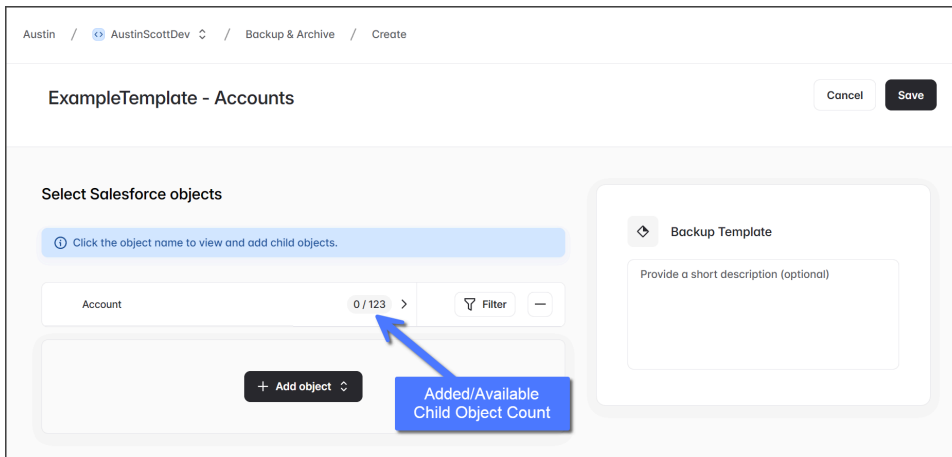
9. Click an object to open the **Add child objects** dialog.
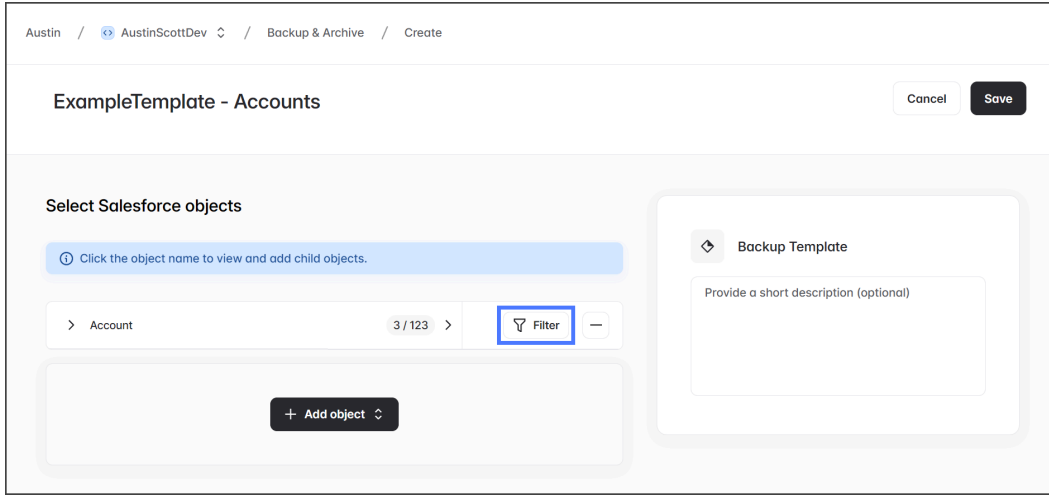
10. Click the **+ Add** button next to each of the child objects to add.
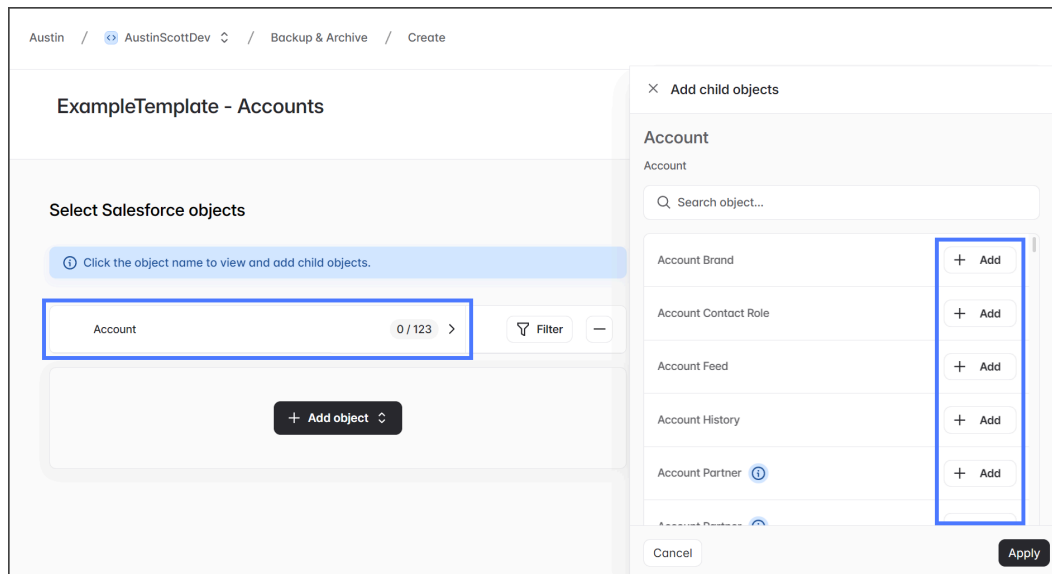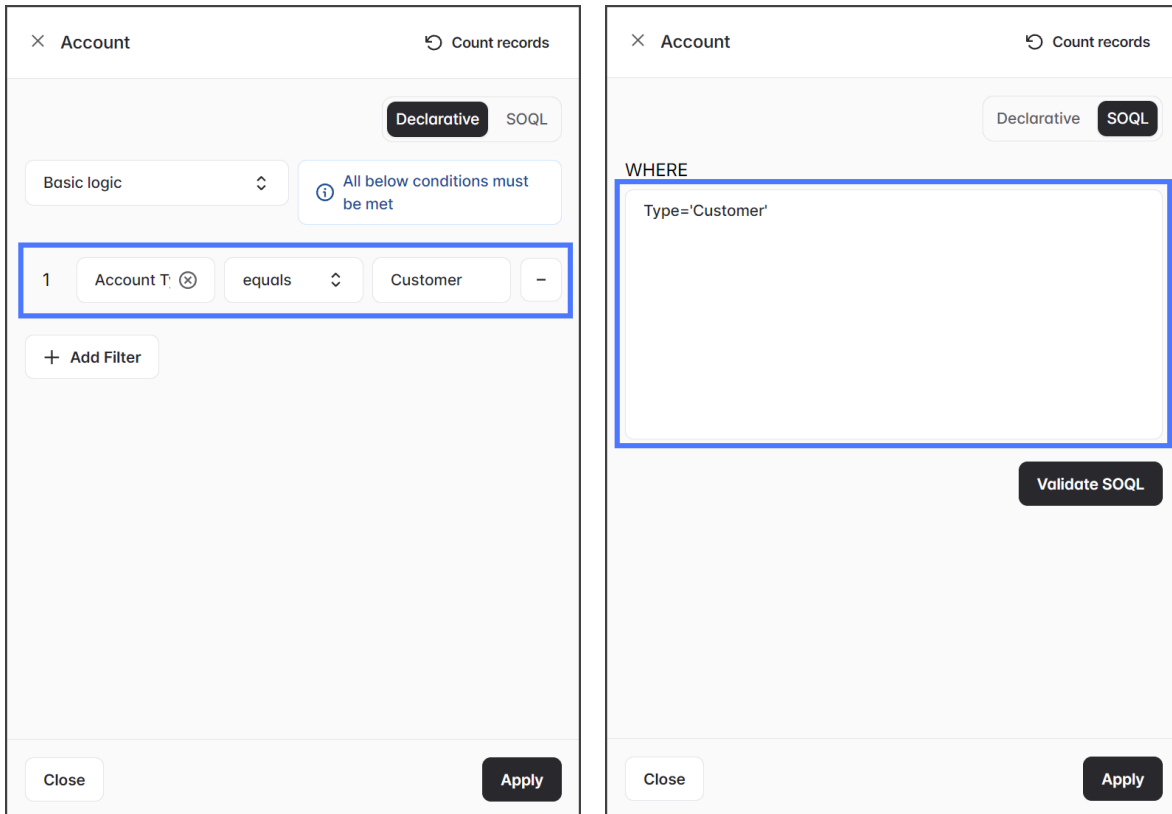
11. Once you have added all the objects, click **Apply** to save the changes.
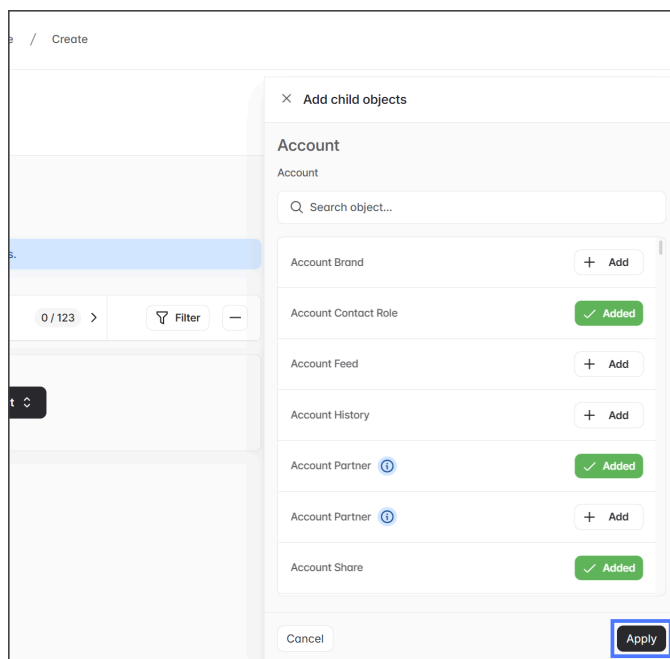
12. (Optional) Click **Filter** to add a filter to the object.

13. You can choose to filter using **Declarative** criteria, similar to Salesforce reporting, or through an **SOQL** query. An example of the same filter created each way is shown in the screenshots below.

14. (Optional) Click the **Count records** button to verify that the filter is retrieving the correct number of records.

15. Click **Apply** to save the filter.
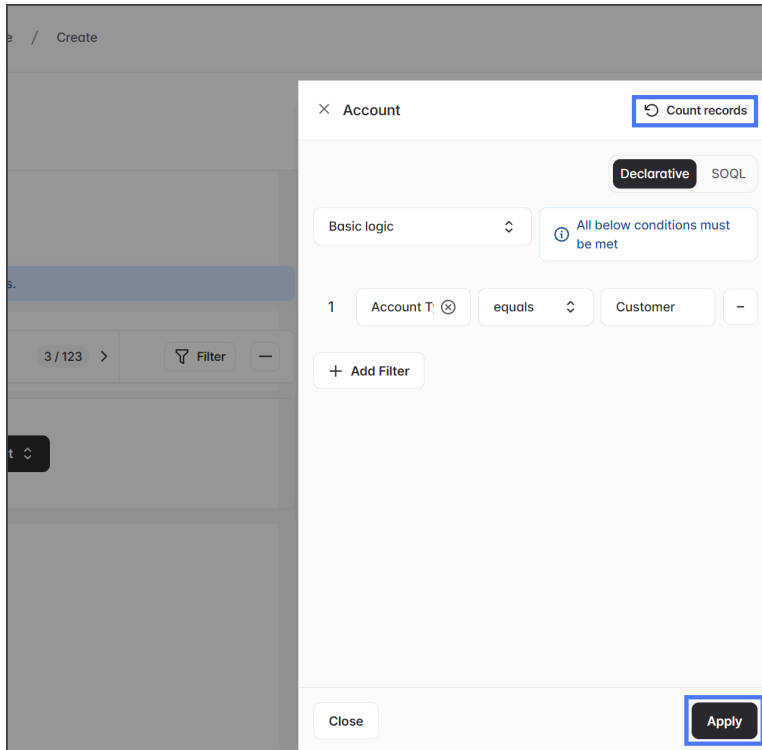
16. Click **Save** once you have configured all of the objects for this template.
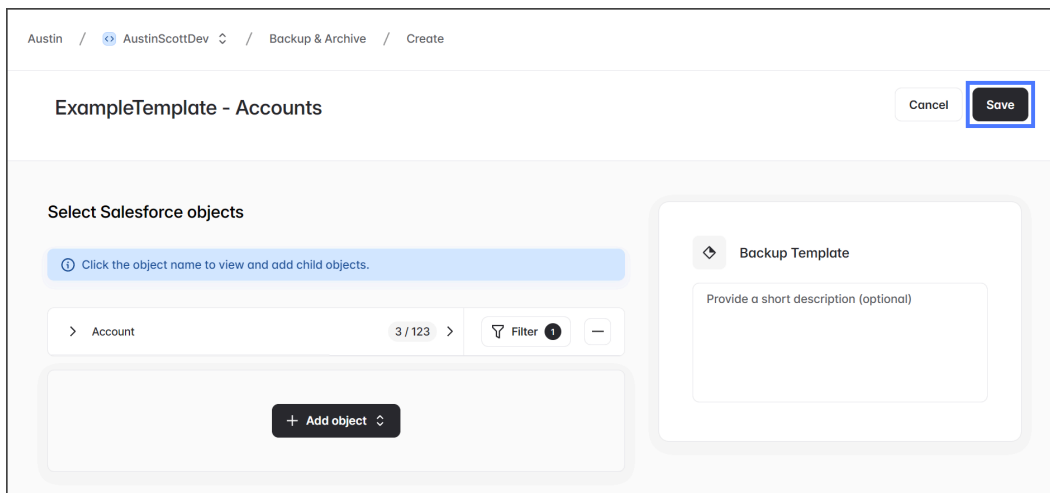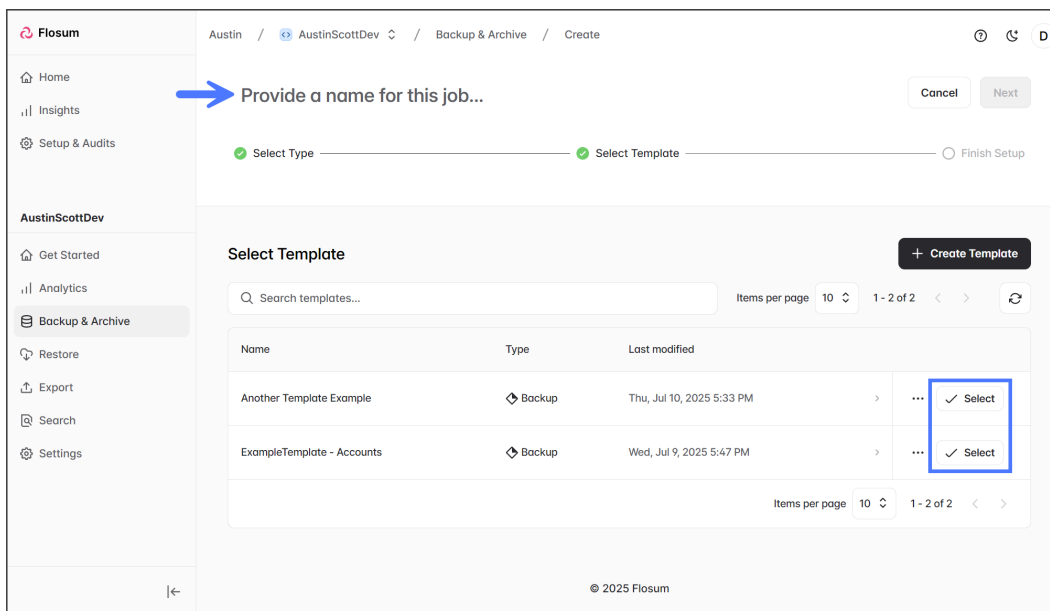
Finish Creating Templated Backup

Now that your backup template has been created, it's time to make a backup job to run the template.

1. Enter a name for the backup job.

2. Click the **Select** button of the template to use.

> (i) You can only select one template.

3. Click **Next**.

4. (Optional) Check the **Metadata** checkbox in the **Job Settings** section to include metadata in the backup.

5. (Optional) Enter a description of the backup in the textbox.

6. Click the **Run** button to start the Templated Backup.
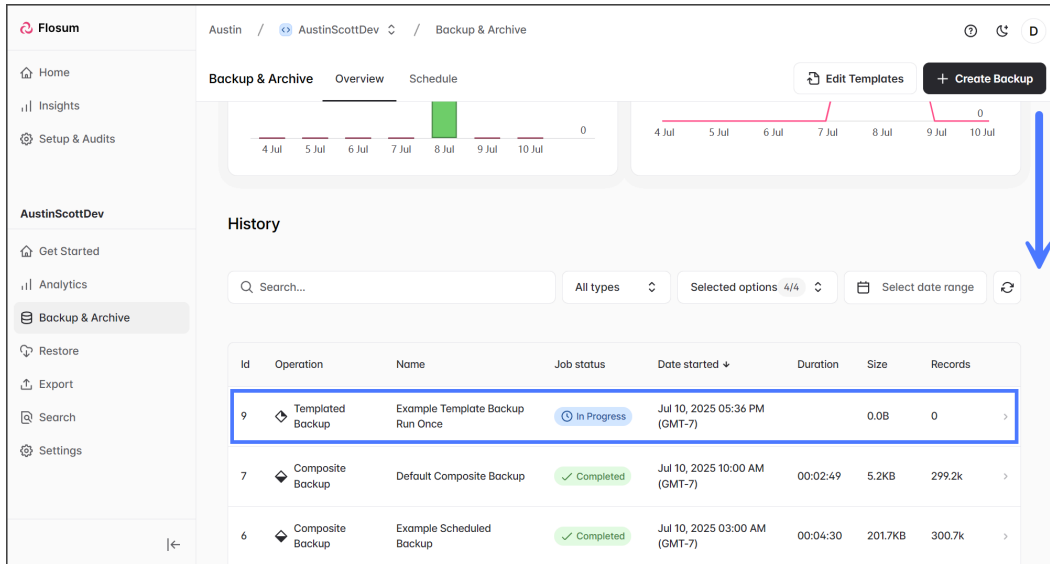
7. The Templated Backup job immediately.

8. Scroll down to the **History** table to view the status of the Backup Job.

Schedule a Templated Backup

Alternatively, you can schedule your Template Backup to run at a specific date and time interval. The process is similar to creating an immediate backup.

1. Complete the steps outlined in the [Create a Templated Backup](#) section above. Before clicking **Run**, enable the schedule option.

2. Switch the **Schedule** toggle to **Enabled**.

3. Select the **Recurrence** of the backup to run **Daily**, **Weekly**, or **Monthly**.

4. Configure the **Schedule** options. Daily, Weekly, and Monthly each have different options to set the time and date the backup is run.

5. Click the **Schedule** button to schedule your backup job.

6. Confirm the schedule is correct and click **Save**.

View your Scheduled Backup Jobs

All scheduled backups for the selected Org will appear on the **Schedule** tab of the **Backup & Archive** section. Any scheduled backups you have created will be found in the **User Scheduled** section.

View Job History

Once a backup job is completed, you can access detailed information about the job and the data that was backed up. The job details provide a comprehensive overview, including the data that was backed up, any selected metadata, the specific settings used, and the transaction logs. This feature allows you to gain valuable insights into the backup process and ensures that your data is secure.

1. From the **Home** page, select the **Org** to view the backup job for.
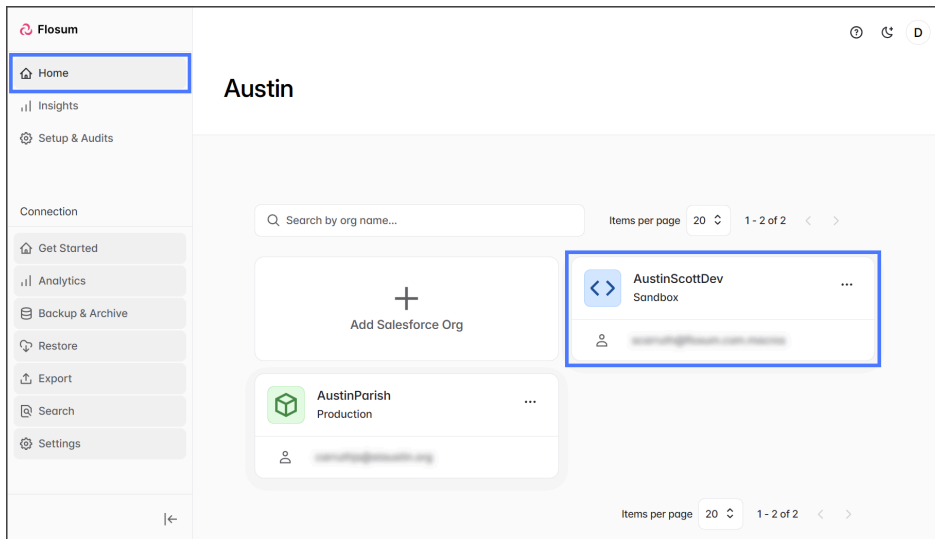
2. Click **Backup & Archive** from the sidebar menu.

3. Scroll down to the **History** table for the list of backup jobs.

4. Click a backup job to view its details.
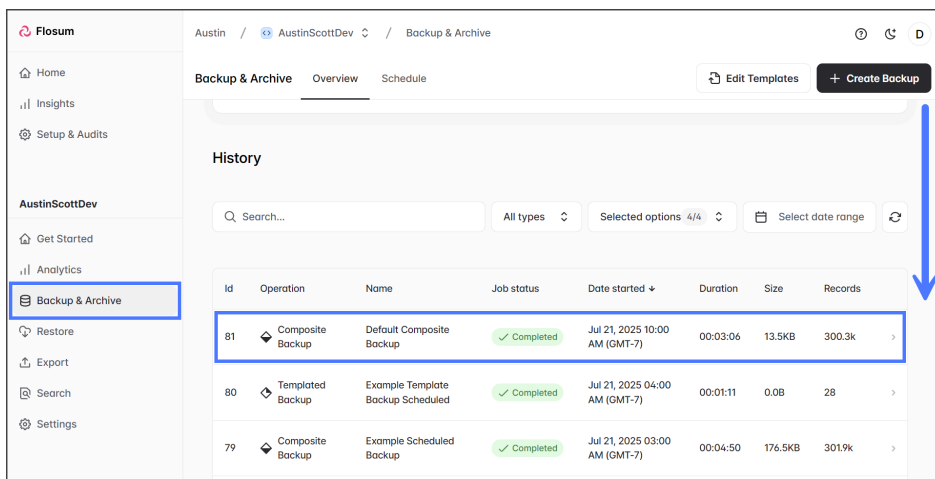
5. Each of the following sections explains a different tab of the job details.
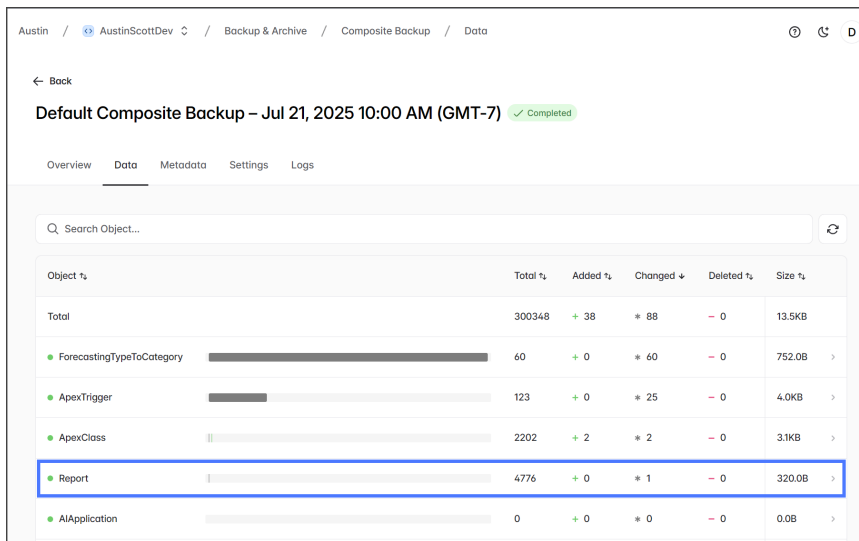
Overview Tab

- The Overview tab provided important information about the backup process. It included details such as the backup type, status, and run time.

- Statistics about the records backed up by this job include backup size, number of records included, and number of records added, modified, and deleted.
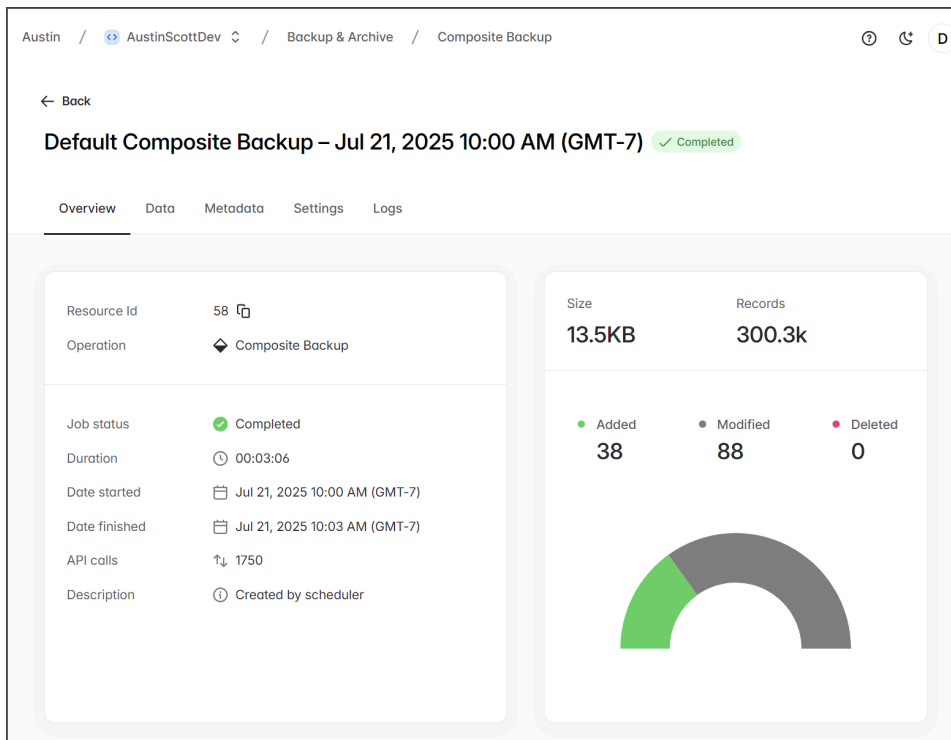
Data Tab

- The Data tab shows all objects in the backup. You can search for specific objects and sort the table by any of the columns.

- Clicking on an object opens backup details for the object and includes a table of the records contained in the backup. If no records for an object were added, changed, or deleted, no records will be listed here.

- Clicking on a record allows you to view the field **Details** for the record.

- The **History** tab allows you to compare the fields to previous versions.

- Use the **Select version** dropdown menu to pick a version to compare this version to.

- Click the **Show/Hide identical fields** button to toggle between showing all fields and showing only changed fields.

Metadata Tab

- The Metadata tab shows all metadata objects in the backup. You can search for specific objects and sort the table by any of the columns.

- Clicking on a metadata object opens a list of records for that object.

- Clicking on a record allows you to view the field values for the record.

Settings Tab

- The Settings tab displays the **Job Settings** chosen for this backup. The objects included in the backup are indicated with a grayed-out checkbox with a checkmark. In the example below, all objects are included.
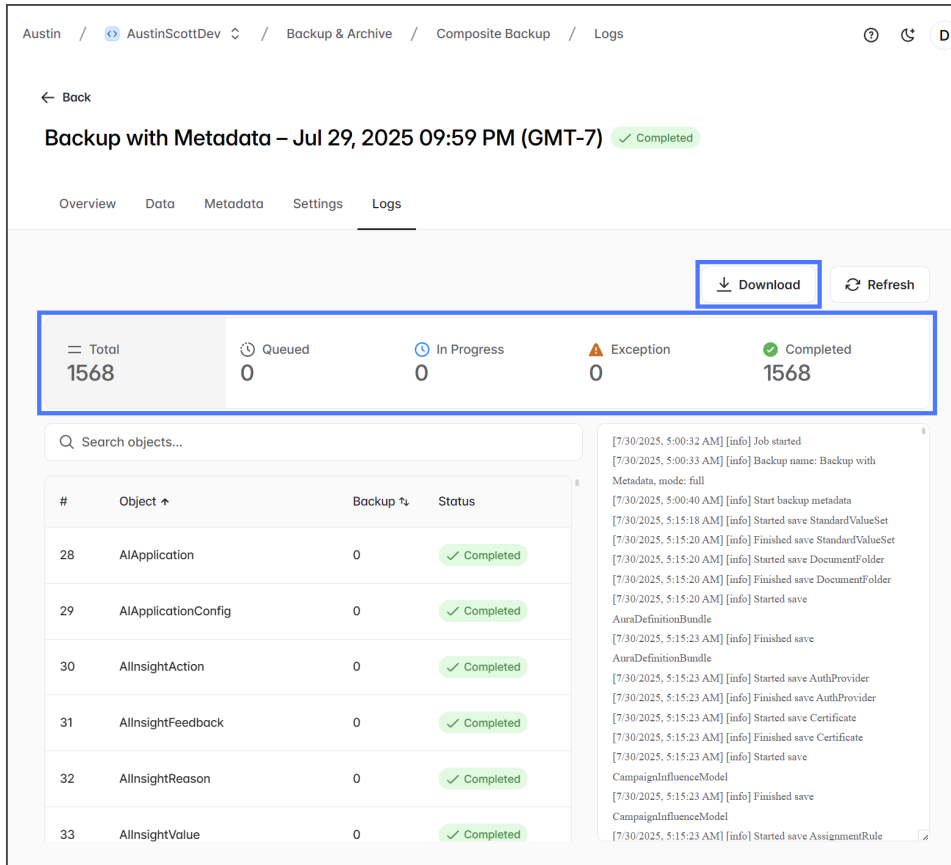
Logs Tab

- The Logs tab displays a list of all objects the job analyzed, along with the job log entries. The table of objects is searchable and can be filtered by column.

- You can filter the objects by their status by choosing **Total**, **Queued**, **In Progress**, **Exception**, or **Completed** from the status bar above the search bar.

- Clicking the **Download** button will save a CSV file of the backup job's logs.

Archive Operations

A **Templated Archive** in Flosum's Backup & Archive app lets you archive specific Salesforce data. Archives ensure efficient long-term storage while safeguarding critical business records. An Archive Job consists of two stages: first, the data is added to the archive in Flosum Backup & Archive, and then the data is deleted from Salesforce.

The **Retain This Object** feature enables users to archive child records while keeping parent records intact — perfect for archiving attachments while retaining Cases or Opportunities. Refer to the [Enable Retain This Object](#) section for more information about this feature.

Create a Templated Archive

1. From the **Home** page, select the **Org** to archive.
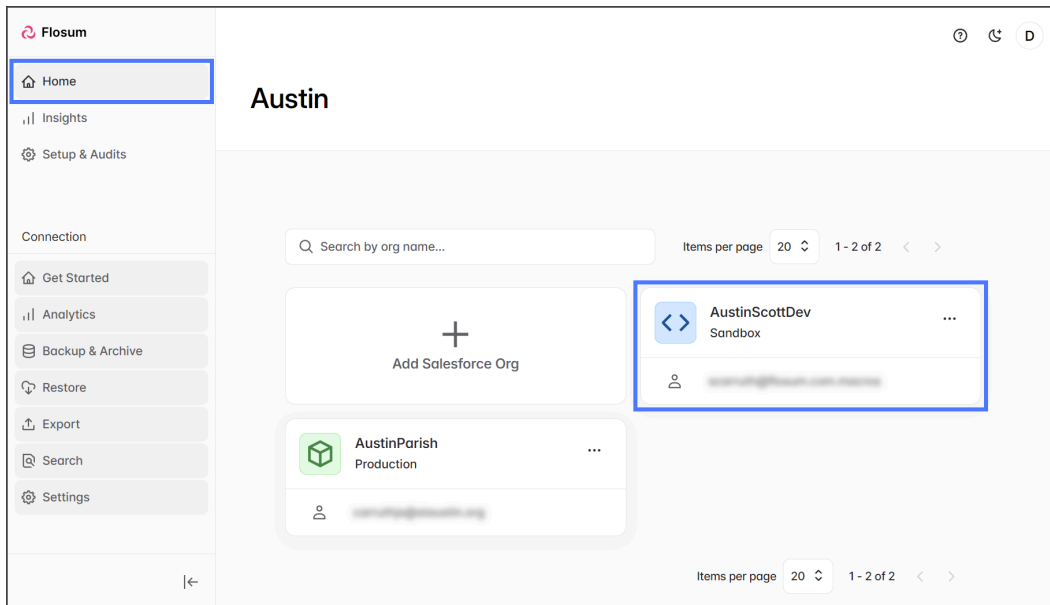
2. Click **Backup & Archive** from the sidebar menu.

3. Click **Create Backup**.
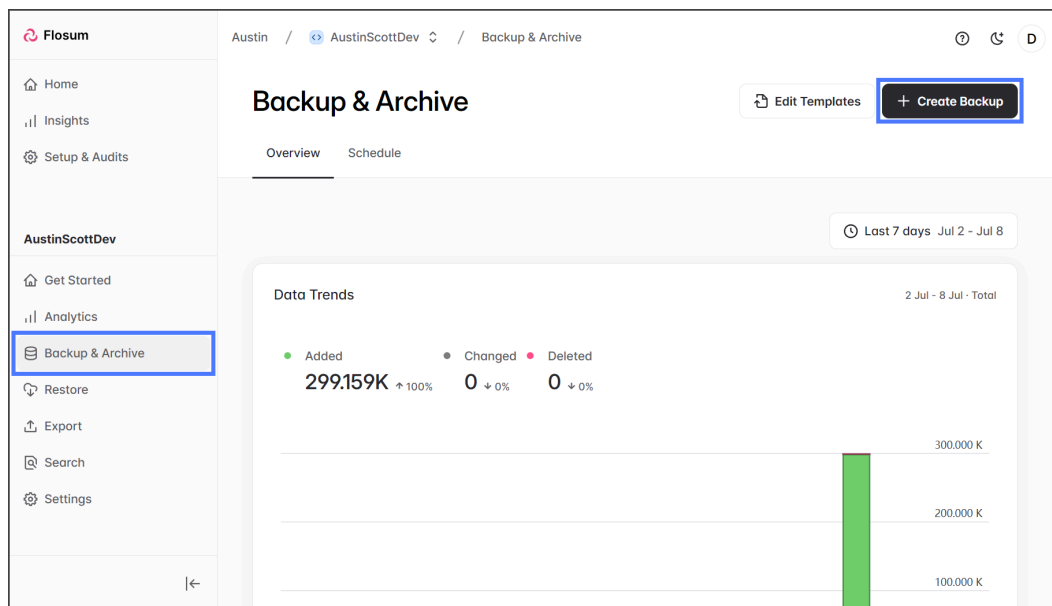
4. Click **Templated Archive**.
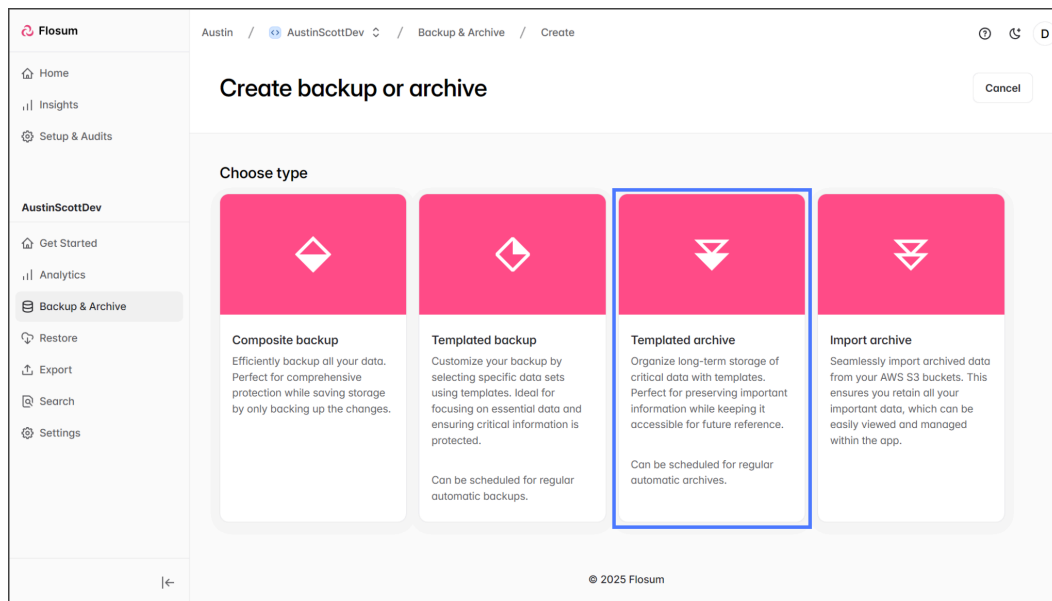
Create a Template

If there are no templates or you need to create a new one, follow the instructions below. Skip to [Finish Creating Templated Archive](#) if you don't need to create a template.

1. Click **Create Template** if there are no templates or if you need to create a new one.
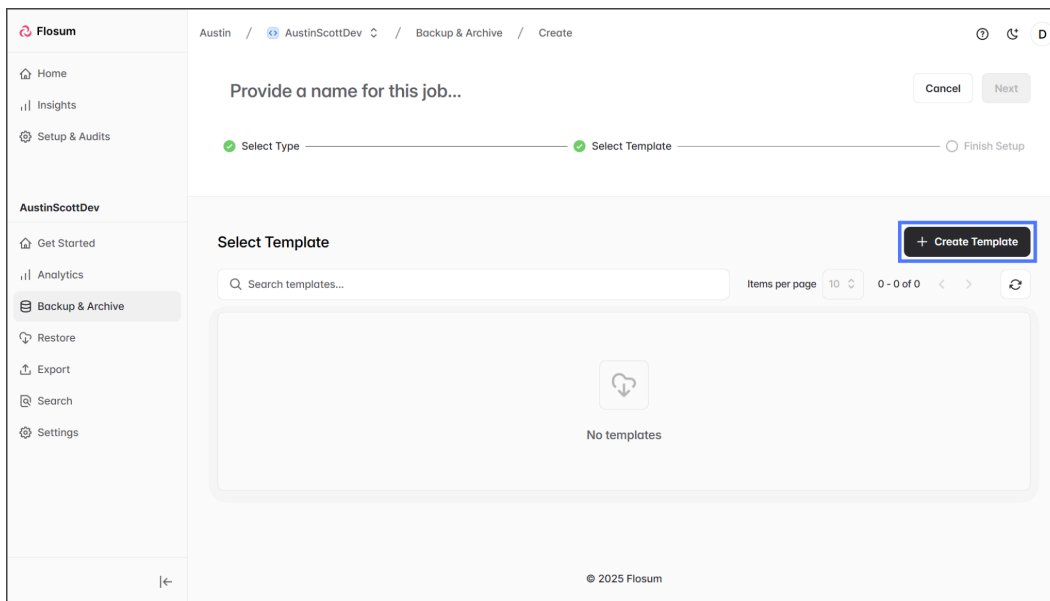
2. Enter a **Name** for the template.

3. Enter a helpful **Description** of the template's purpose in the optional **Archive Template** textbox.

4. Click the **Add object** menu button to select the Salesforce Objects to include in the template.
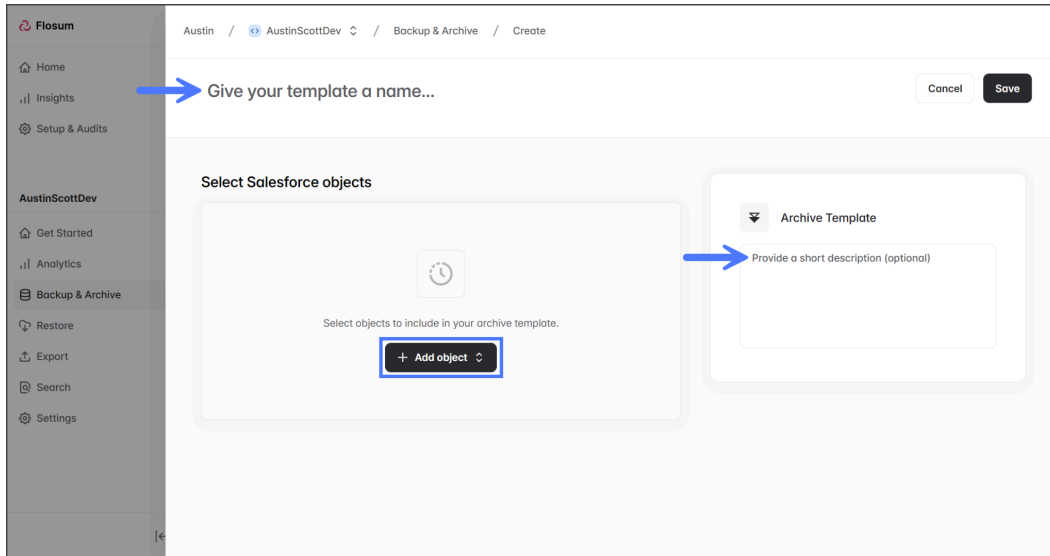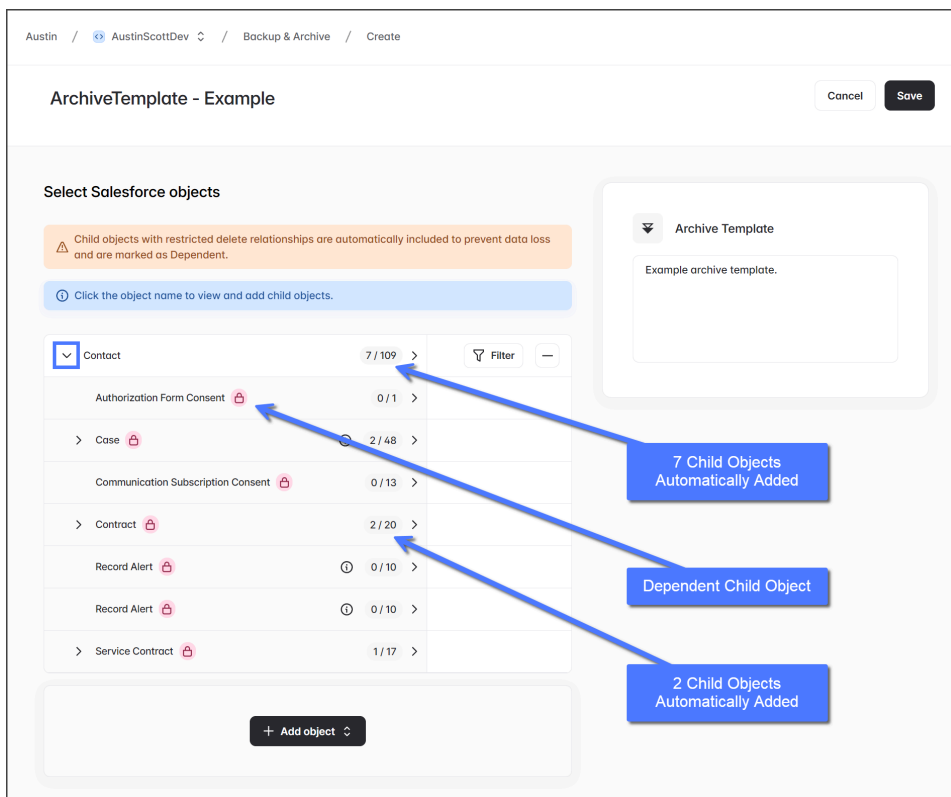
5. Search or browse for objects from the menu.

6. Check the objects you want to add.

7. Click **Add** to add all of the selected objects.
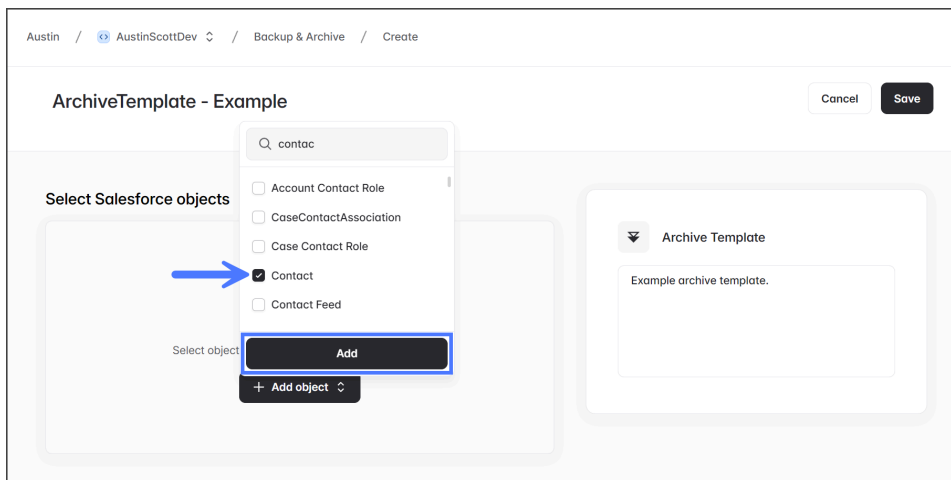
8. When an object is added to the archive, any child objects that are dependent on the parent object will automatically be added to the archive.

9. Click the **>** arrow to expand an object to see all of its child objects.

> ⓘ Every child object marked with a **Red Lock** icon is automatically added to the archive because it is dependent on its parent object. In the screenshot below, the **Contact** object has seven child objects that were automatically archived. Additionally, some of these child objects have their own dependent child objects, which were also included in the archive. This dependency results in a cascading delete; when the **Contact** object is archived, it will lead to the deletion of many child and grandchild objects from Salesforce. It is important to be aware of which object records will be removed from Salesforce when an archive job is run.

10. Click an object to open the **Add child objects** dialog.

11. See the Enable Retain This Object section below to learn how to use the **Retain this object** feature.

12. Click the **+ Add** button next to each of the child objects to add.
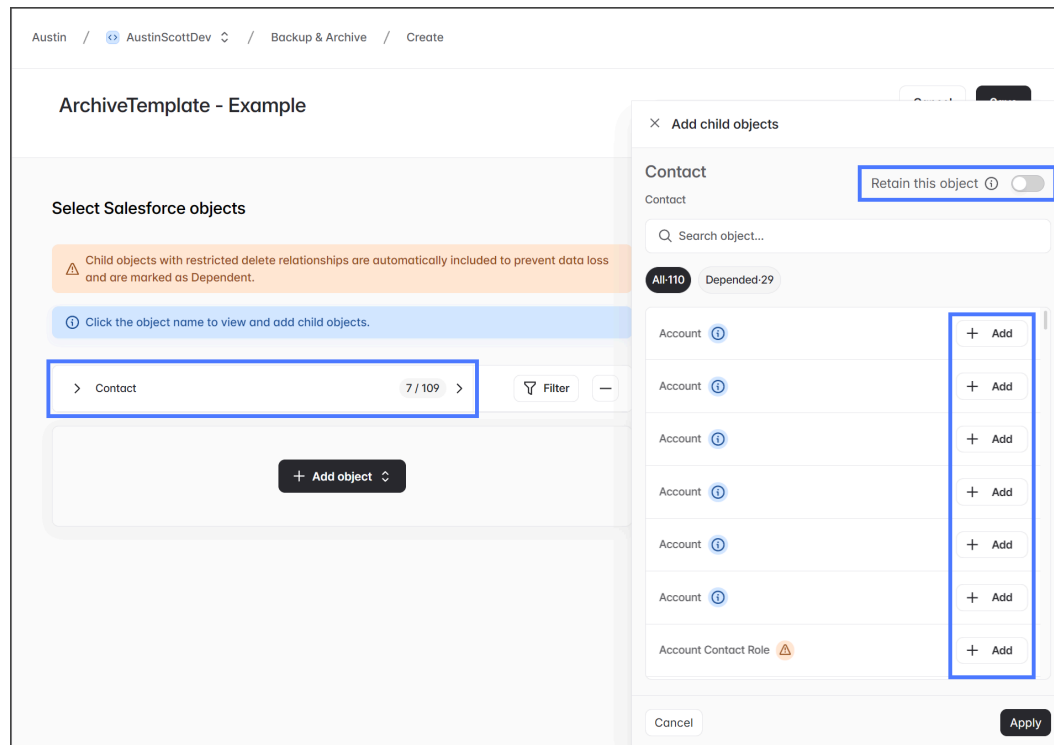
13. Once you have added all the objects, click **Apply** to save the changes.
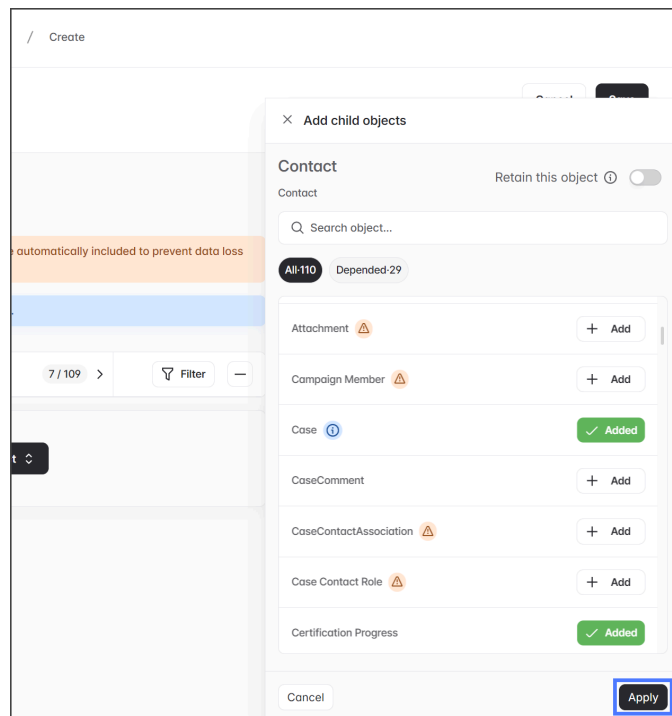
14. (Optional) Click **Filter** to add a filter to the object.
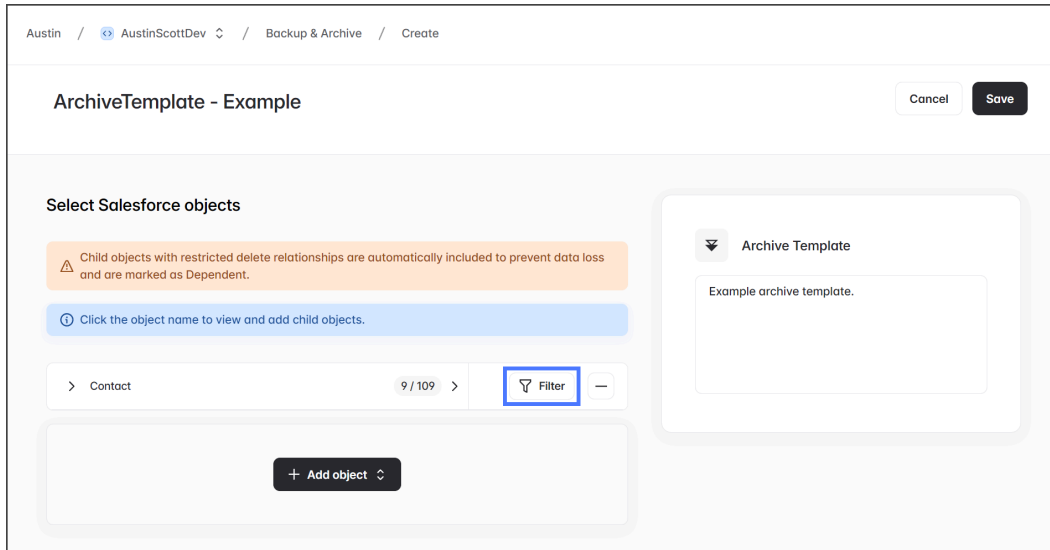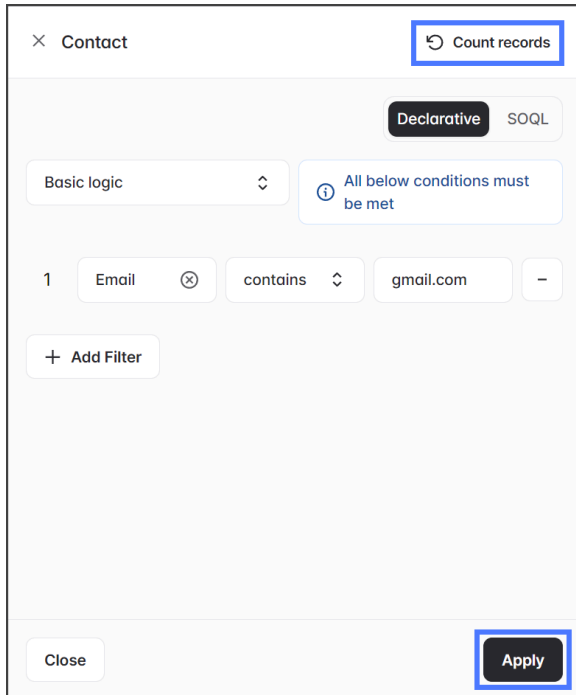
15. You can choose to filter using **Declarative** criteria, similar to Salesforce reporting, or through an **SOQL** query. An example of the same filter created each way is shown in the screenshots below.
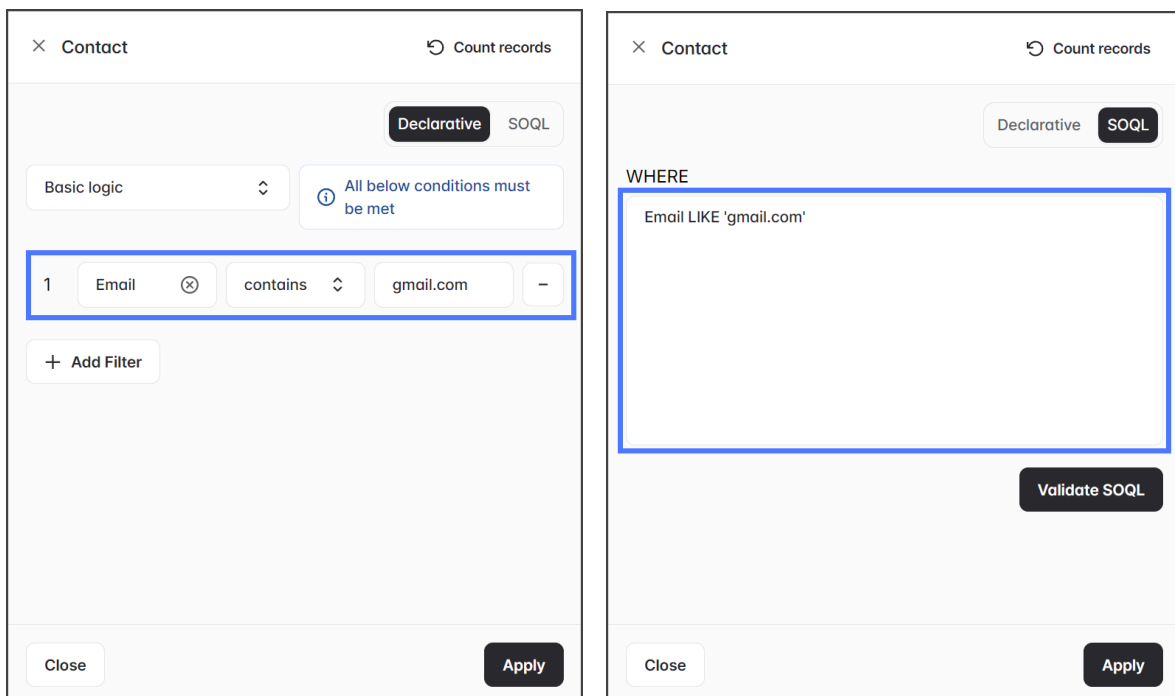
16. (Optional) Click the **Count records** button to verify that the filter is retrieving the correct number of records.

17. Click **Apply** to save the filter.
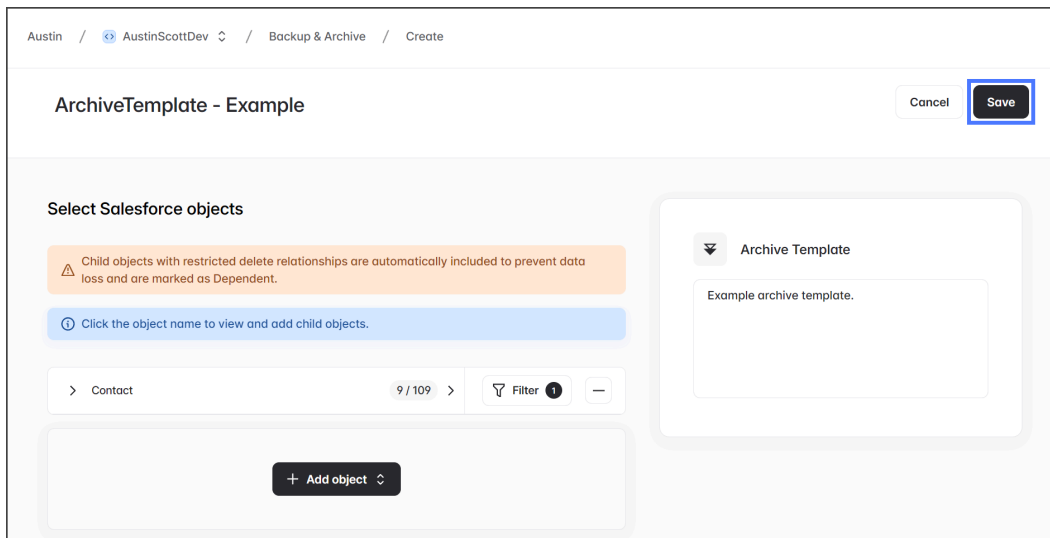
18. Click **Save** once you have configured all of the objects for this template.

Enable Retain This Object

The **Retain This Object** feature provides more control over what objects are deleted from Salesforce. With this feature, you can mark objects added to an archive as **Retained**, meaning that the object will be included in the archive but also remain in Salesforce. A child object that is not **retained** will still be deleted. The instructions below demonstrate how to use this feature and provide examples to illustrate the expected outcome.

> ⓘ By default, objects do not have **Retain This Object** enabled. Which means they will be deleted from Salesforce when archived.

1. Click an object to open the **Add child objects** dialog.

2. Click the **Retain this object** toggle to enable it.

3. Click **Apply** to save the changes.
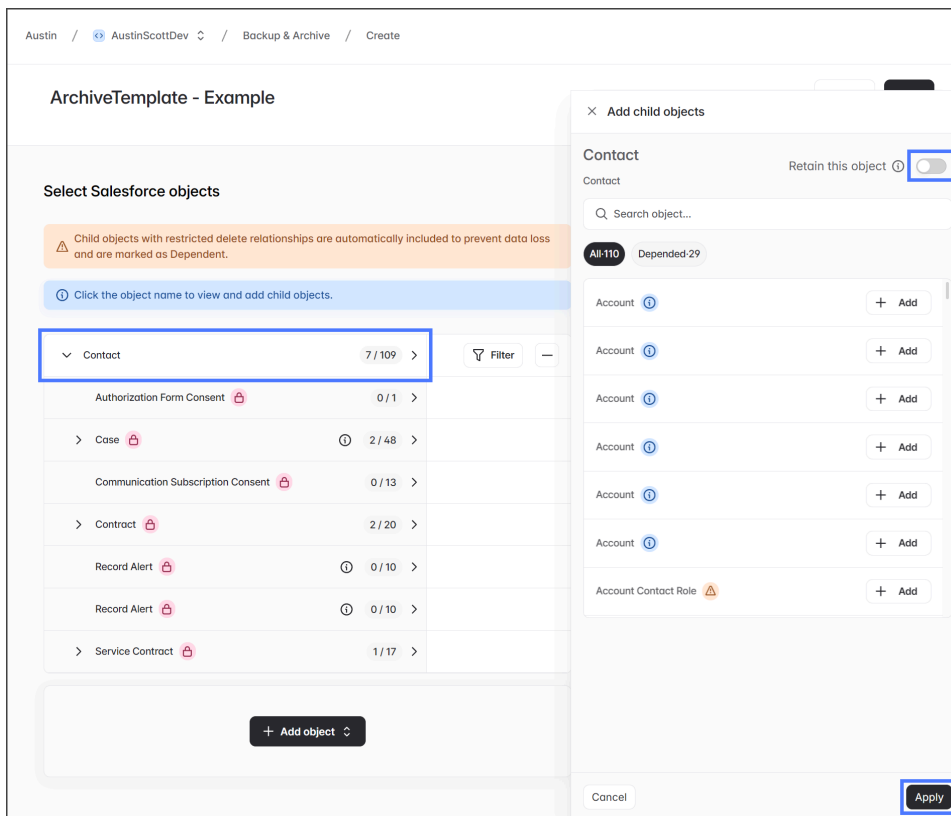
4. Once **Retain this object** is enabled, a **Green Shield** icon will appear next to the object.

Example 1:

In this example, the **Contact** and **Contact >> Contract** objects are both marked as **Retained**. The screenshot below indicates which objects will be deleted from Salesforce and which will be saved.

> ⓘ The **Case**, **Contract**, and **Service Contract** objects each have dependent child objects that will also be deleted. It's important to understand that a cascading delete can extend through multiple levels of objects. However, for simplicity, this example only lists the child objects that are directly dependent on the root parent object.

Example 2:

In this example, only the **Contact >> Contract** object is marked as **Retained**. However, because **Contact >> Contract** is dependent on its parent, it will still be deleted because **Contact** will be deleted, which will trigger a cascading delete of **Contact >> Contract**. The screenshot below indicates which objects will be deleted from Salesforce and which will be saved.

> ⓘ This example illustrates the importance of understanding how dependency works when using the **Retain This Object** feature. Objects marked as **Retained** will still be deleted if they are dependent on a parent that is deleted.

Example 3:

In this example, only the **Contact >> Client Answer** object is marked as **Retained**. Since **Contact >> Client Answer** is not dependent on its parent, it will be saved even after the **Contact** object is deleted. The screenshot below indicates which objects will be deleted from Salesforce and which will be saved.

Austin / ◇ AustinScottDev ⇕ / Backup & Archive / Create		

ArchiveTemplate - Example

Select Salesforce objects

⚠ Child objects with restricted delete relationships are automatically included to prevent data loss and are marked as Dependent.

ⓘ Click the object name to view and add child objects.

Delete ∨ Contact		8 / 109 >	▽ Filter —
Delete Authorization Form Consent 🔒		0 / 1 >	
Delete > Case 🔒	ⓘ	2 / 48 >	
Delete Communication Subscription Consent 🔒		0 / 13 >	
Delete > Contract 🔒		2 / 20 >	
Delete Record Alert 🔒	ⓘ	0 / 10 >	
Delete Record Alert 🔒	ⓘ	0 / 10 >	
Delete > Service Contract 🔒		1 / 17 >	
Save Client Answer ⊘		0 / 18 >	—

Example 4:

In this example, all objects are marked as **Retained** except for **Contact >> Content Document**. This is a practical example of archiving files attached to a contact while retaining the rest of the Contact record in Salesforce. The screenshot below indicates which objects will be deleted from Salesforce and which will be saved.

Austin / ⟨⟩ AustinScottDev ⌄ / Backup & Archive / Create

ArchiveTemplate - Example

Select Salesforce objects

⚠ Child objects with restricted delete relationships are automatically included to prevent data loss and are marked as Dependent.

ⓘ Click the object name to view and add child objects.
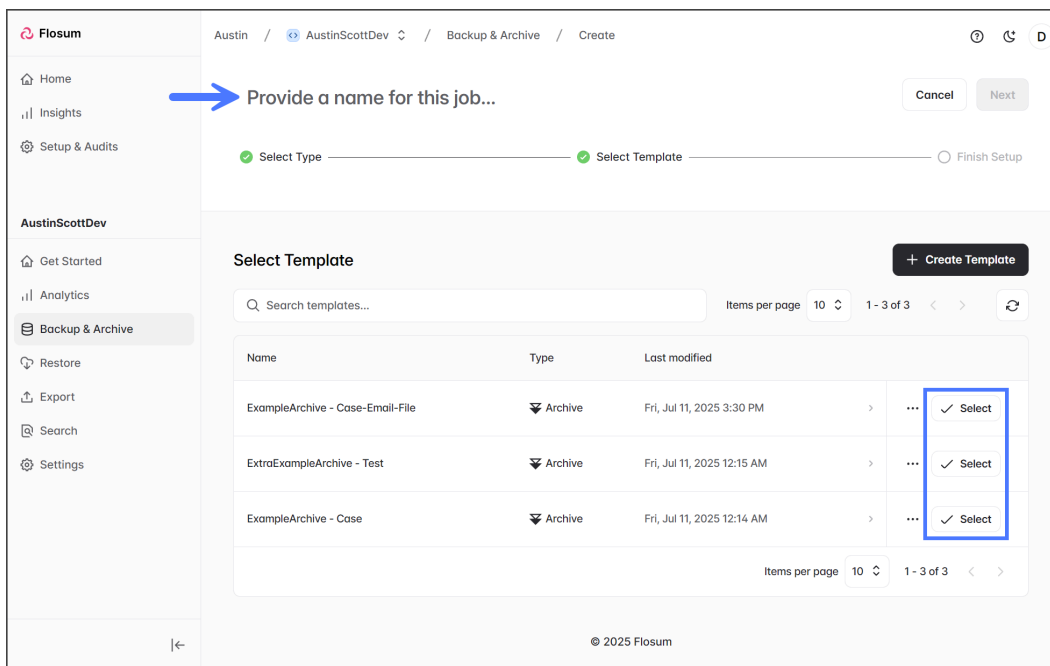
Save ⌄ Contact 🛡		8 / 109 ›	▽ Filter —
Save Authorization Form Consent 🔒 🛡		0 / 1 ›	
Save › Case 🔒 🛡	ⓘ	2 / 48 ›	
Save Communication Subscription Consent 🔒 🛡		0 / 13 ›	
Save › Contract 🔒 🛡		2 / 20 ›	
Save Record Alert 🔒 🛡	ⓘ	0 / 10 ›	
Save Record Alert 🔒 🛡	ⓘ	0 / 10 ›	
Save › Service Contract 🔒 🛡		1 / 17 ›	
Delete Content Document			—

Finish Creating Templated Archive

Now that your archive template has been created, it's time to make an archive job to run the template.

1. Enter a name for the archive job.

2. Click the **Select** button of the template to use.

> ⓘ You can only select one template.

3. Click **Next**.

4. (Optional) Enter a description of the archive in the textbox.

5. Click the **Run** button to start the Templated Archive.
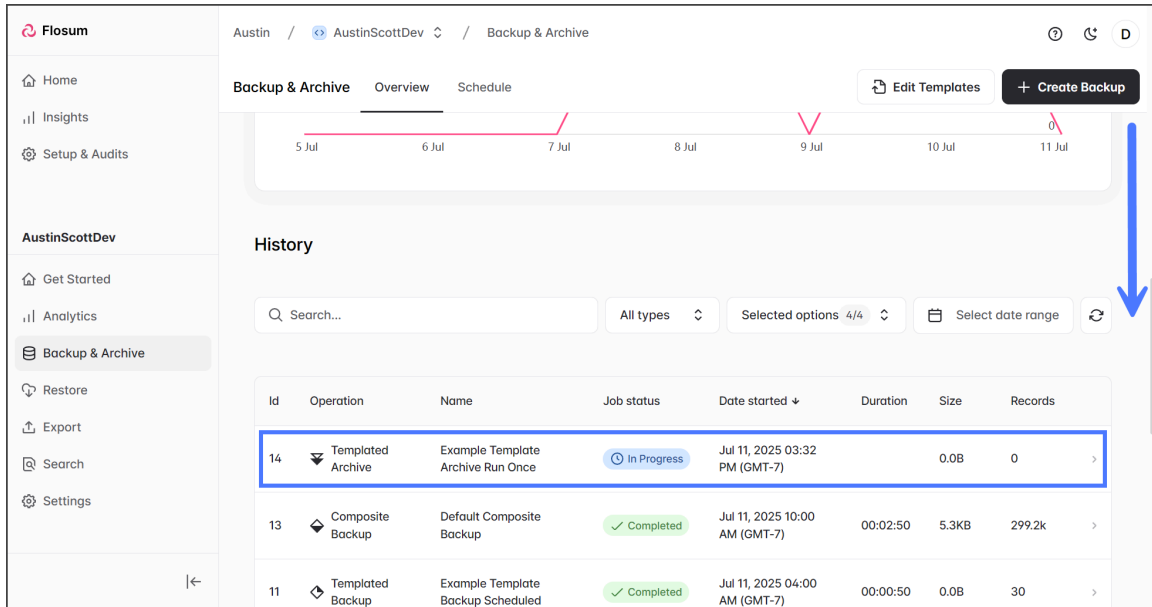
6. This will start your Templated Archive job immediately.

7. Scroll down to the **History** table to view the status of the Archive Job.

Schedule an Archive Job

Alternatively, you can schedule your Template Archive to run at a specific date and time interval. The process is similar to creating an immediate archive.

1. Complete the steps outlined in the [Create a Templated Archive](#) section above. Before clicking **Run**, enable the schedule option.

2. Switch the **Schedule** toggle to **Enabled**.
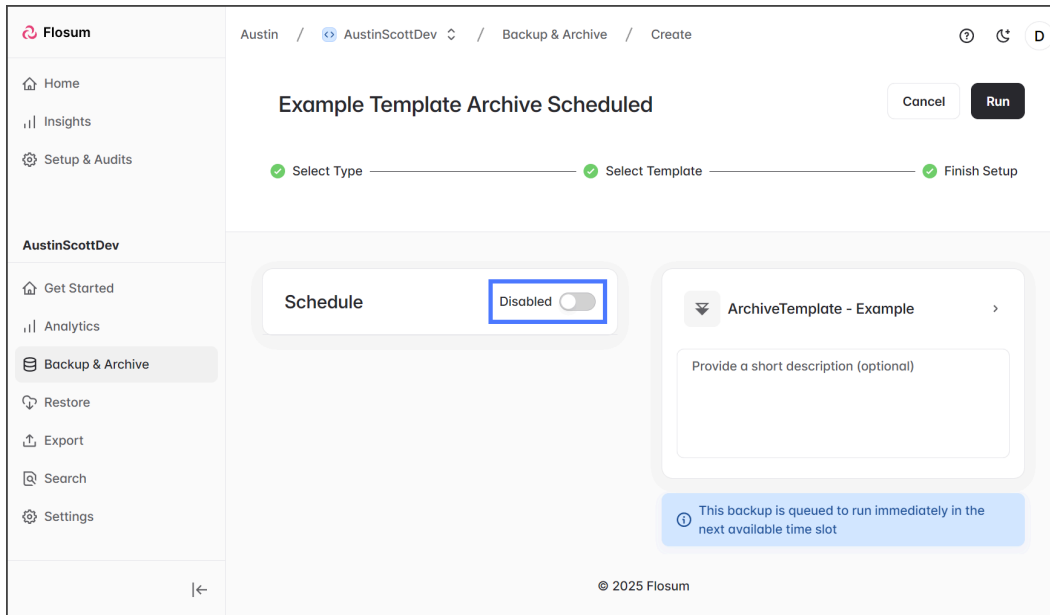
3. Select the **Recurrence** of the backup to run **Daily**, **Weekly**, or **Monthly**.

4. Configure the **Schedule** options. Daily, Weekly, and Monthly each have different options to set the time and date at which the archive is run.

5. Click the **Schedule** button to schedule your archive job.

6. Confirm the schedule is correct and click **Save**.

View your Scheduled Archive Jobs

All scheduled archives for the selected Org will appear on the **Schedule** tab of the **Backup & Archive** section. Any scheduled archives you have created will be found in the **User Scheduled** section.

Monitor Backup & Archive Jobs

You can view all active and finished backup and archive jobs for an organization. Clicking a finished job allows you to view details about the job, including the stored objects and records.

Job Status	Description
Success	The job was completed with no errors.
In Progress	The job is currently being processed or is pending processing.
Error	The job was completed with an error. See the logs to determine the cause.

1. From the **Home** page, select the **Org** to archive.

2. Click **Backup & Archive** from the sidebar menu.

3. Scroll down to the **History** section to view the jobs.

Restore Operations

Flosum restore operations allow you to retrieve data and files that have been deleted from your production environment.

Overview

Restoring data in Salesforce can be complex, but Flosum Backup & Archive simplifies the process with a highly accurate, flexible, and visual restore workflow. Whether you're recovering from data corruption, user error, or a security incident, Flosum lets you:

- Restore from backups, archives, or metadata snapshots

- Filter what to restore by object, record, and field

- Visually compare record versions before confirming the restore

- Speed up recovery by restoring only what has changed

This article provides a high-level overview of how the restore process works and how to get started with Flosum's two-step backup and restore workflow.

Its strong filtering and comparison features allow you to restore only what's necessary, down to the object, record, or field level—minimizing risk and reducing Recovery Time Objectives (RTO).
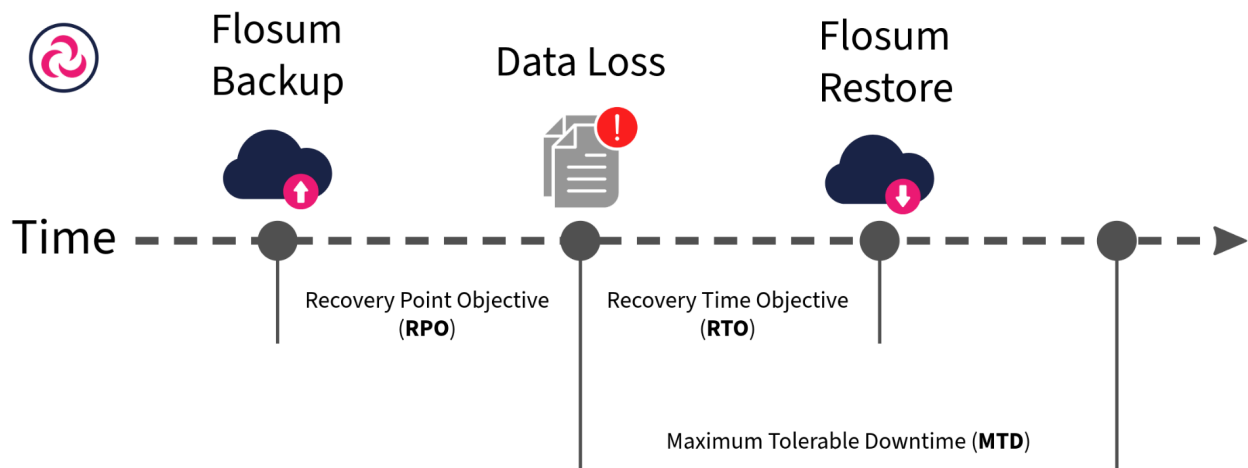
Restore operations are a two-part process. First, you create a restore request that selects the objects and fields to retrieve, including using filters to choose the records that matter. The second step is to actually retrieve the data once the records to be retrieved have been validated.

Create a Restore Job

Creating a restore job has several steps, as outlined below. A restore can be performed from several different data sources: **Backup**, **Archive**, and **Backup Metadata**. There are minor differences between each, but these instructions will focus on restoring from a **Backup**.

- [Select Restore Type](#)

- [Select Compromised and Correct Backups](#)

- [Select Objects to Restore](#)

- [Configure Object Settings](#)

- [Finish Restore Job Setup](#)

Select Restore Type

1. From the **Home** page, select the **Org** to archive.
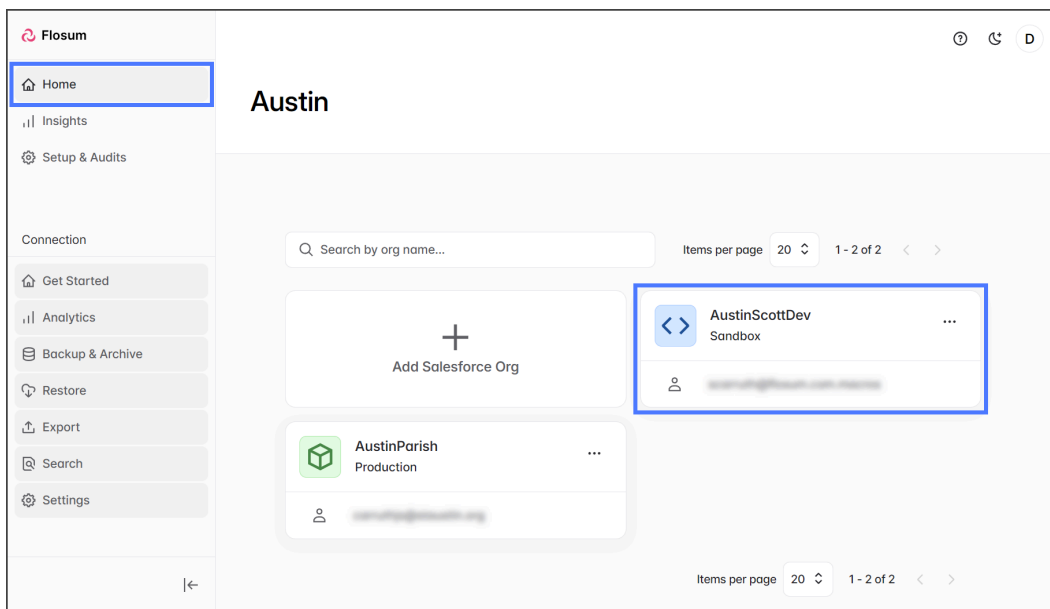
2. Click **Restore** from the sidebar menu.

3. Click **Create Restore**.
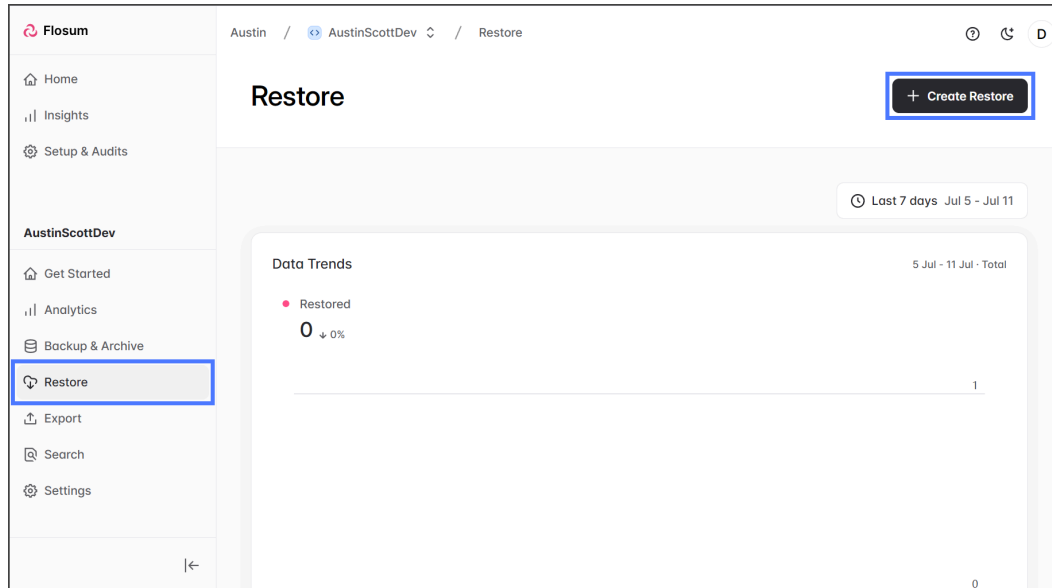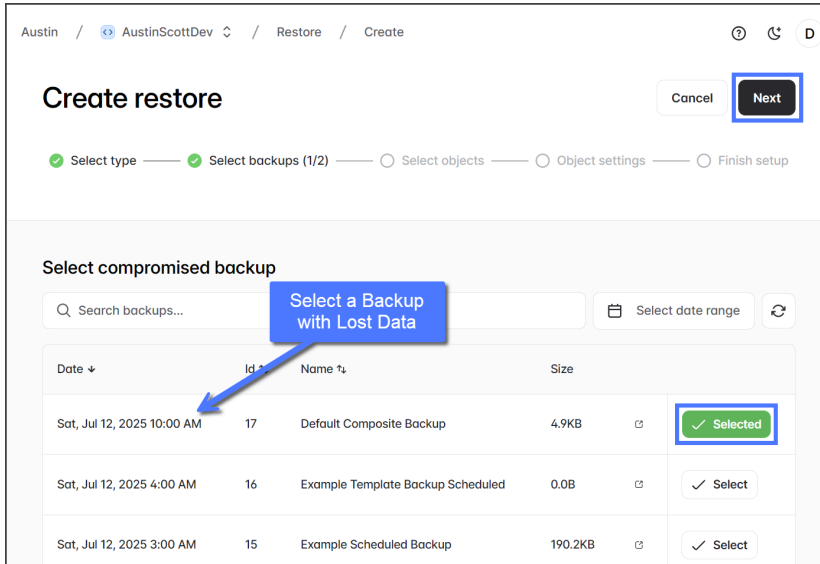
4. Click the restore **Type** for your purposes.

> (i) These instructions use the **Backup** type as an example. Although there are minor differences between each restore type, you can still follow these instructions for the other types of restores.
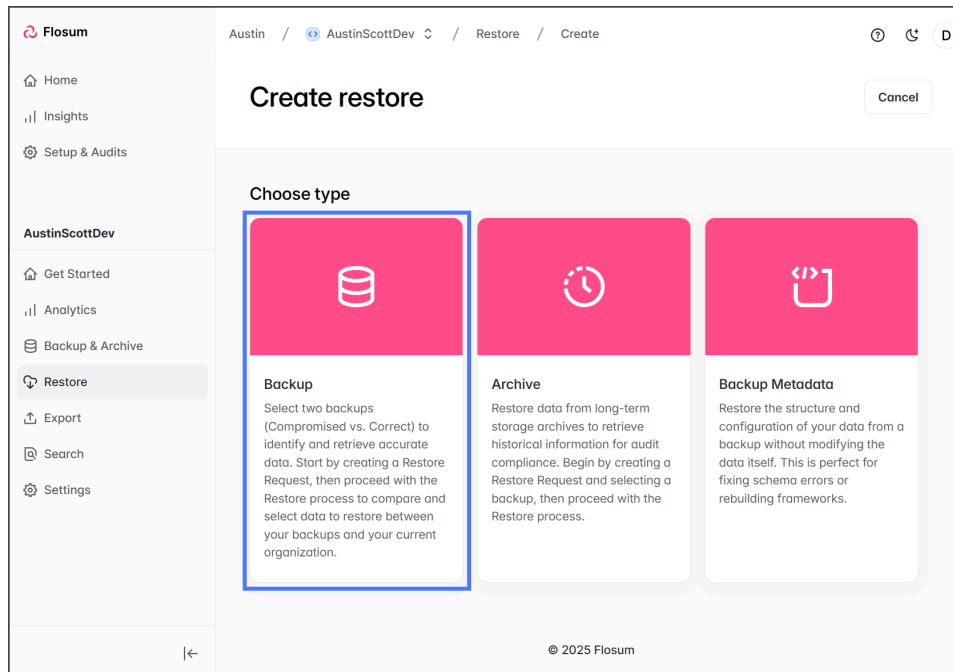
Select Compromised and Correct Backups

1. Click **Select** for the **Compromised Backup**. This is the backup from which data was lost; this is your Recovery Point Objective.
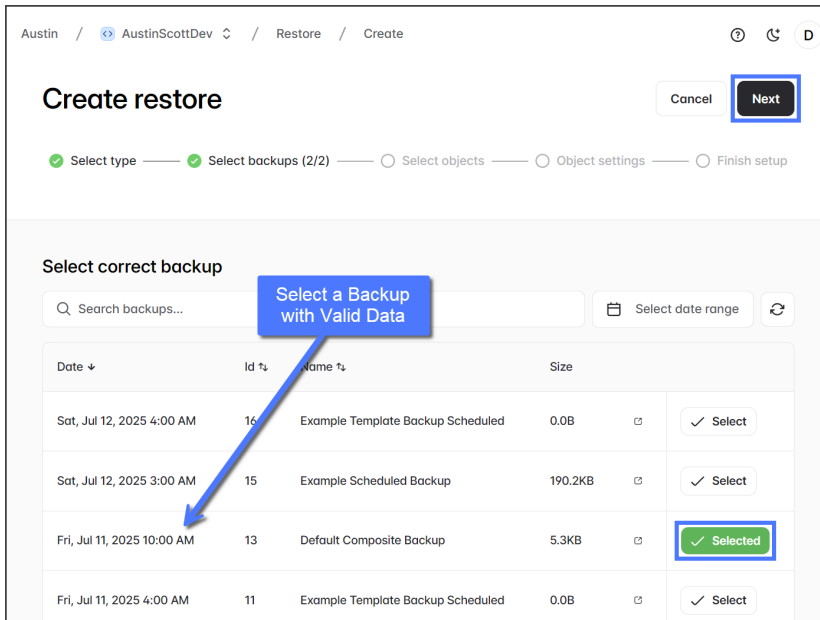
2. Click **Next**.

3. Click **Select** for the most recent successful **Correct Backup**. This is the backup with valid data before data loss (your Restoration Point).

4. Click **Next**.

Select Objects to Restore

In this section, you select the objects you want to restore, their related child objects, filter on what records you want to restore, and which fields you want to retrieve.

1. Click the **Add Object** menu to choose which Salesforce objects to restore.
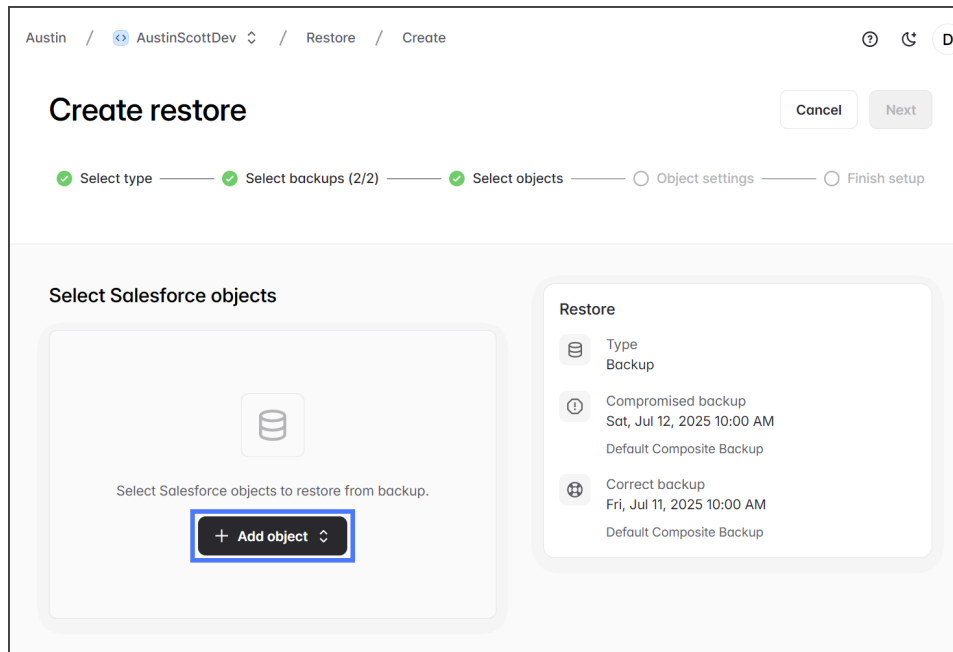
2. Search or browse for objects from the menu.

3. Check the objects you want to add.

4. Click **Add** to add all of the selected objects.
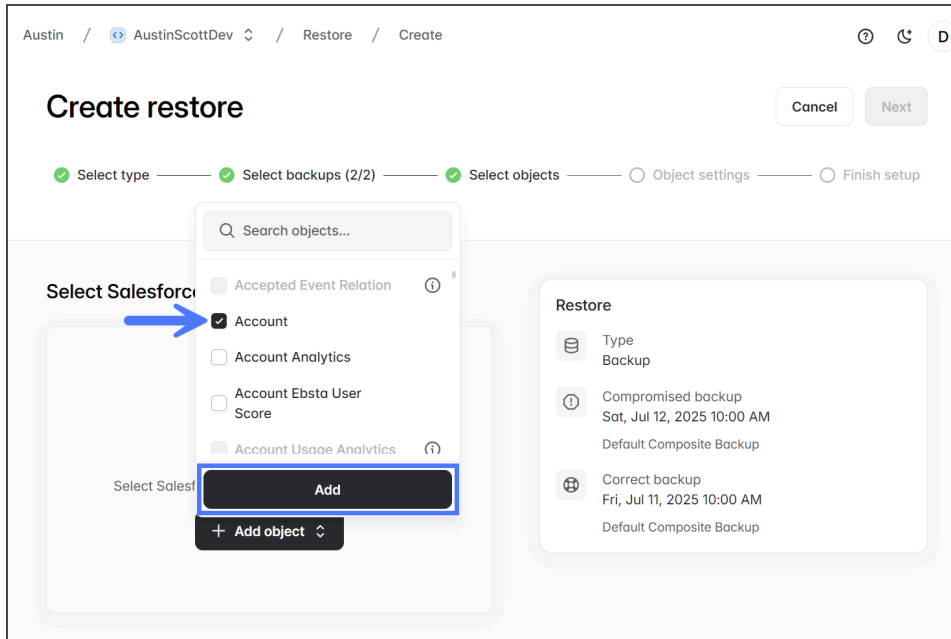
5. When an object is added, you will need to add at least one child object to restore.

> ⓘ To the right of the object's name is a count of **Added/Available** child objects. In the screenshot below, the **Account** object has **133** child objects, and **0** of them have been added.
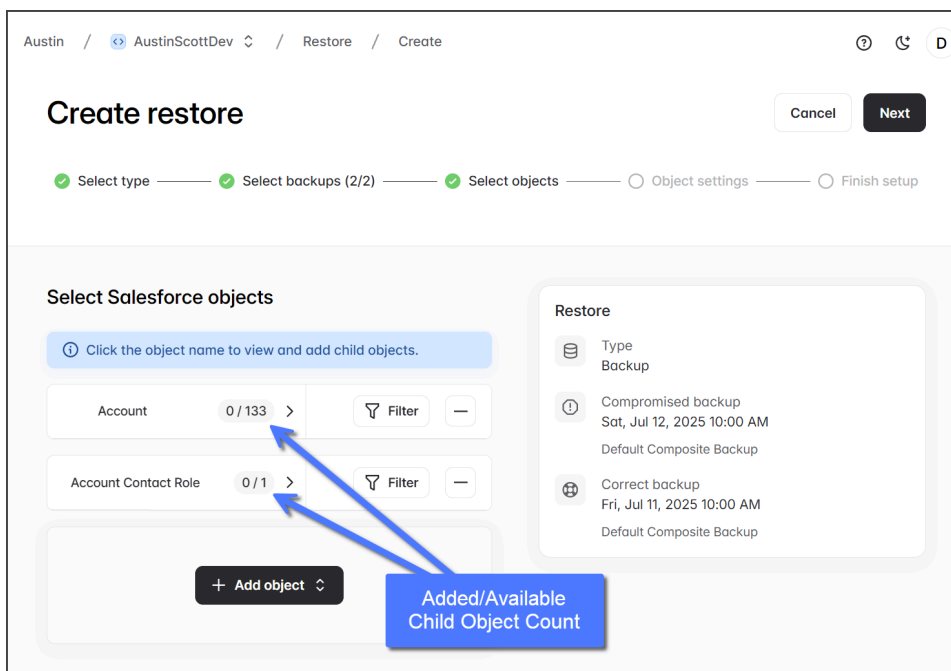
6. Click an object to open the **Add child objects** dialog.

7. Click the **+ Add** button next to each of the child objects to add.
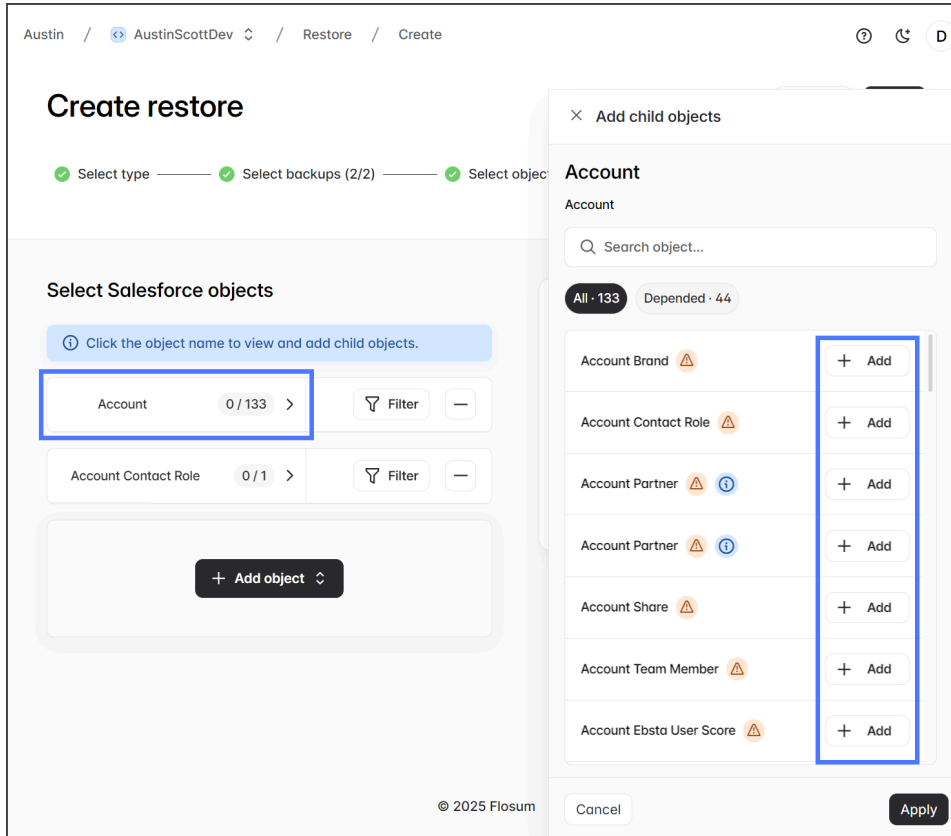
8. The **Caution** icon signifies that a child object is dependent on its parent object, and any child objects marked with this icon will lose data during a restore job if you do not add them to the job.

> ⓘ The following explanation will help you understand the process of a restore operation. During this operation, the records intended for restoration are first deleted from Salesforce. This deletion initiates a cascading delete, which removes any dependent child records associated with those parent records. After this step, the records to be restored are added back into Salesforce. To successfully restore the data in the dependent child records, you must select each child object you wish to restore.

9. Once you have added all the objects, click **Apply** to save the changes.
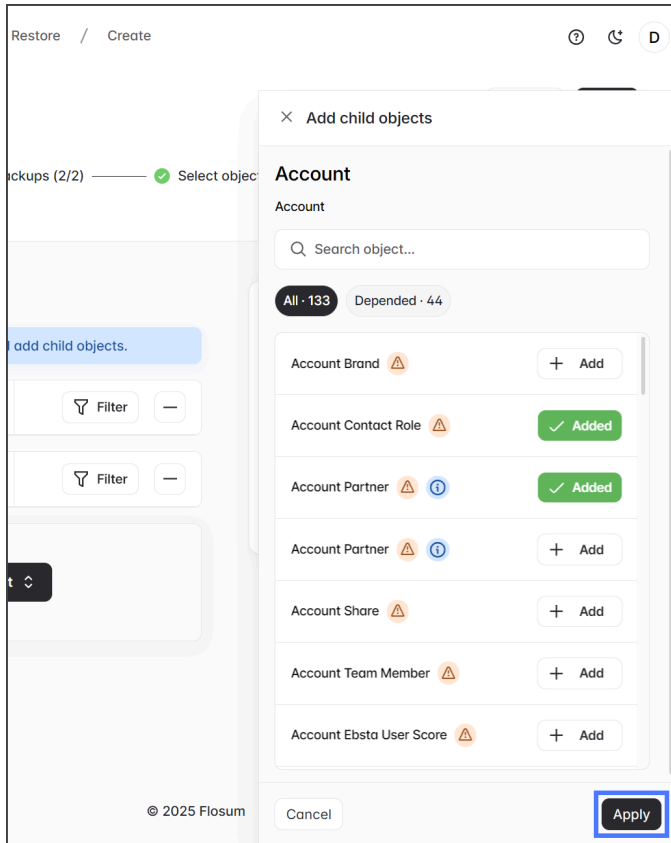
10. (Optional) Click **Filter** to add a filter to the object.
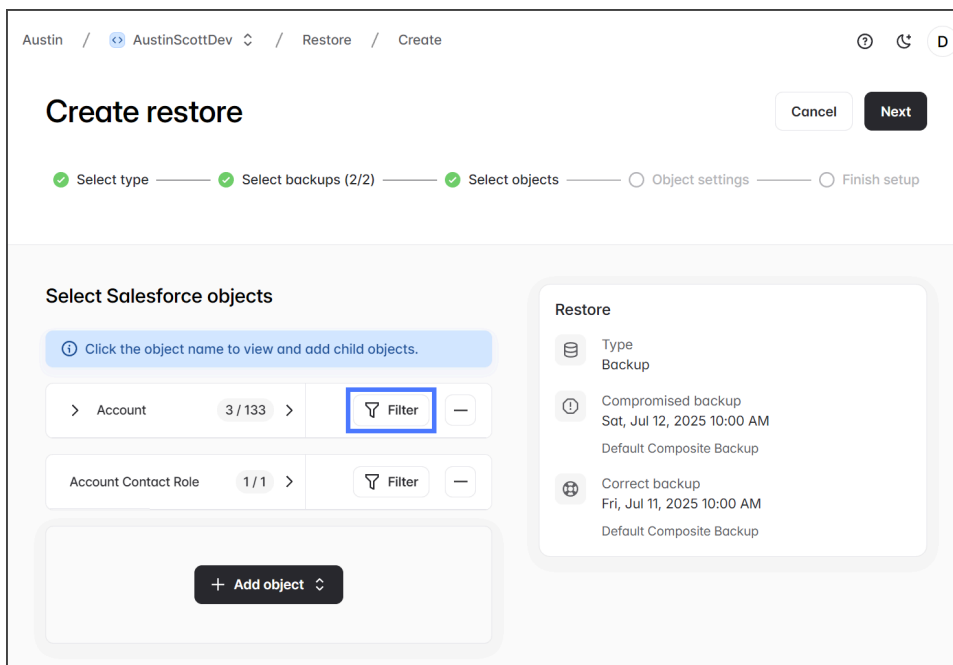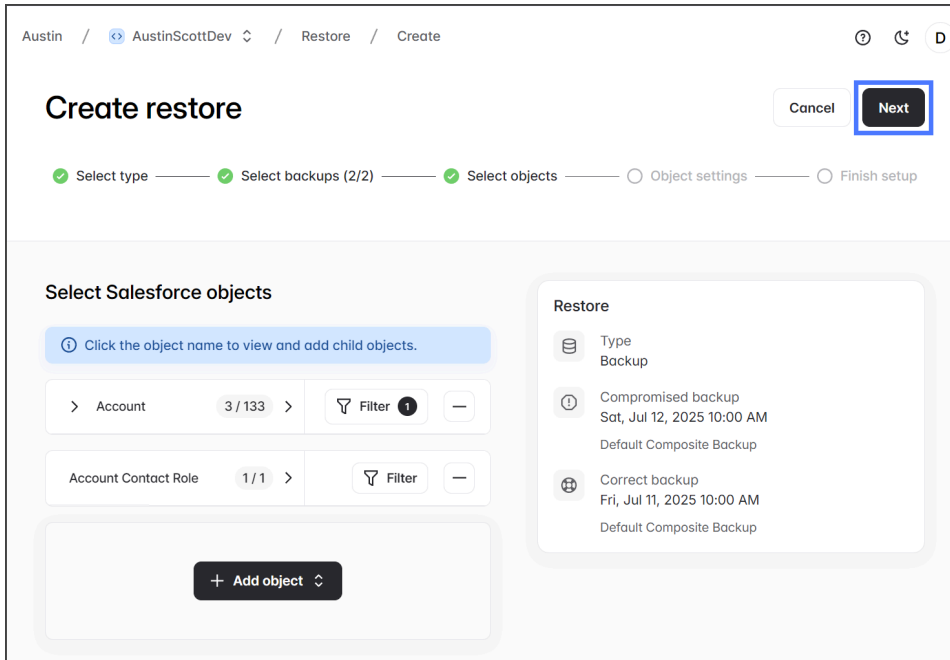
11. Click **Add Filter** in the filter dialog to add a filter criteria.

12. The screenshot below shows an example filter.

13. Click **Apply** to save the filter.
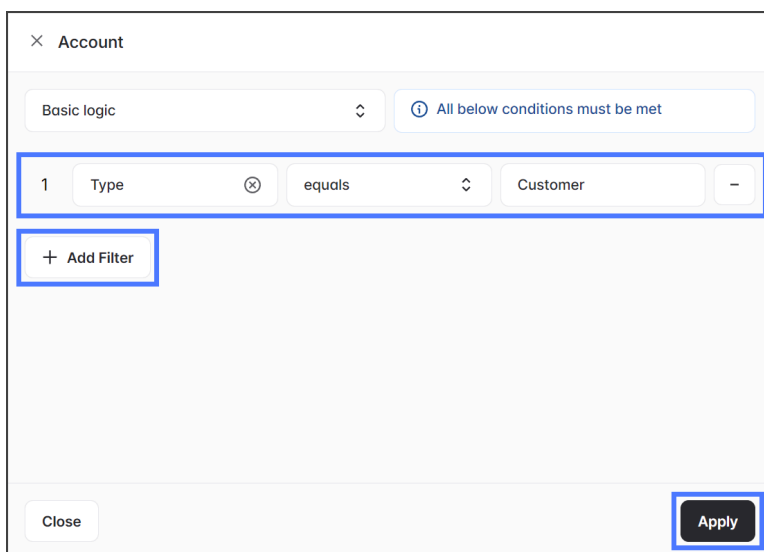
14. Once all the objects are selected and filtered, click **Next**.

Configure Object Settings

Object Settings allows you to select the **fields** to retrieve and the **automation processe**s to suspend during the restore process.

1. Click the **Fields** button for an object to select the fields that will be restored for that object. This will open the **Select fields for Object** dialog.
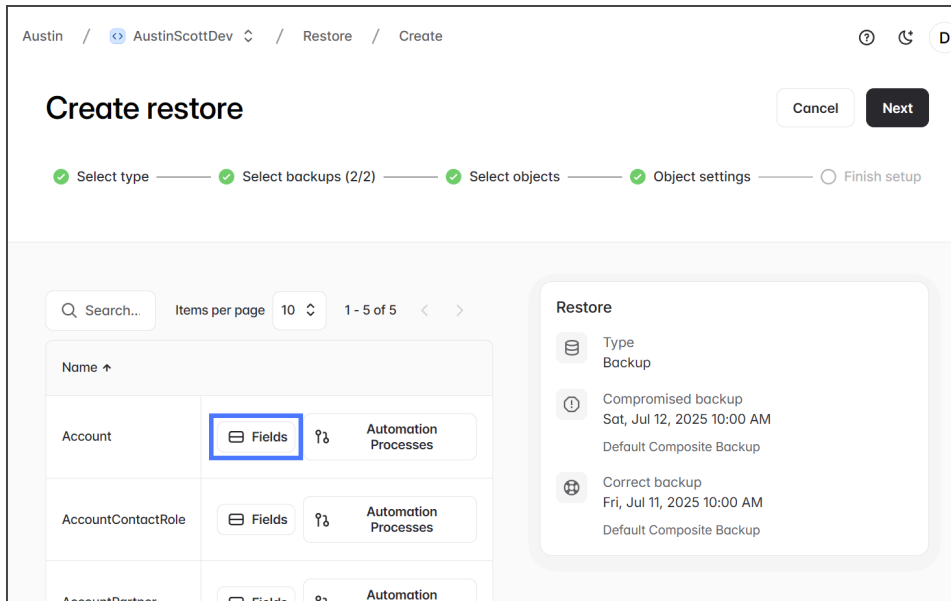
2. The **Select fields for Object** dialog contains two lists of fields. The right list shows all fields that are selected to be restored for the object, while the left list displays fields that are not selected. You can transfer fields between lists by selecting a field and clicking the arrows between them. Fields that are grey cannot be moved to the other list.

3. Click **Save** once you have selected the desired fields.
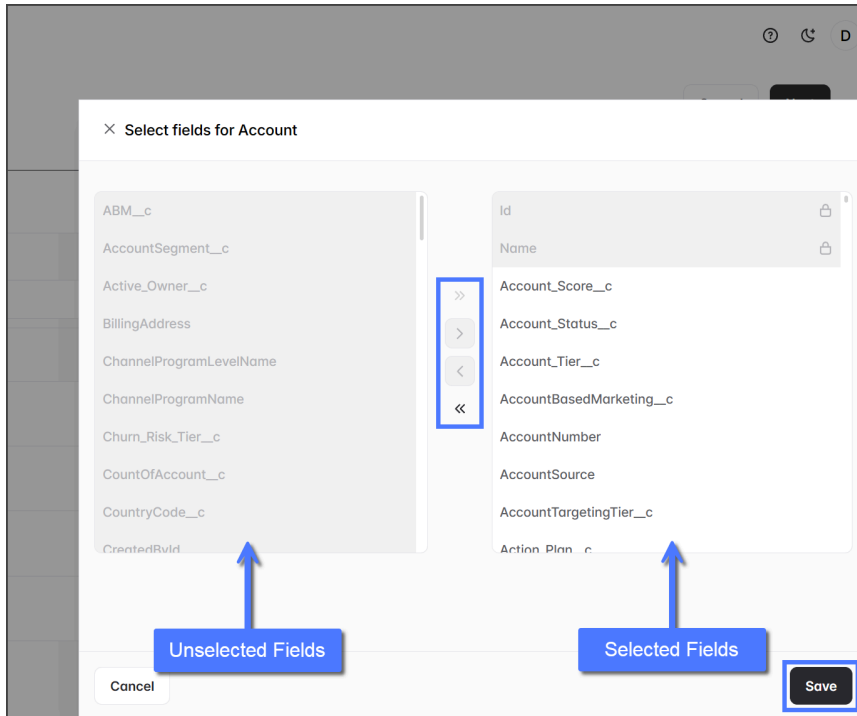
4. Click the **Automation Processes** button for an object to select the processes to suspend during the restore. This will open the **Disable automation processes for Object** dialog.
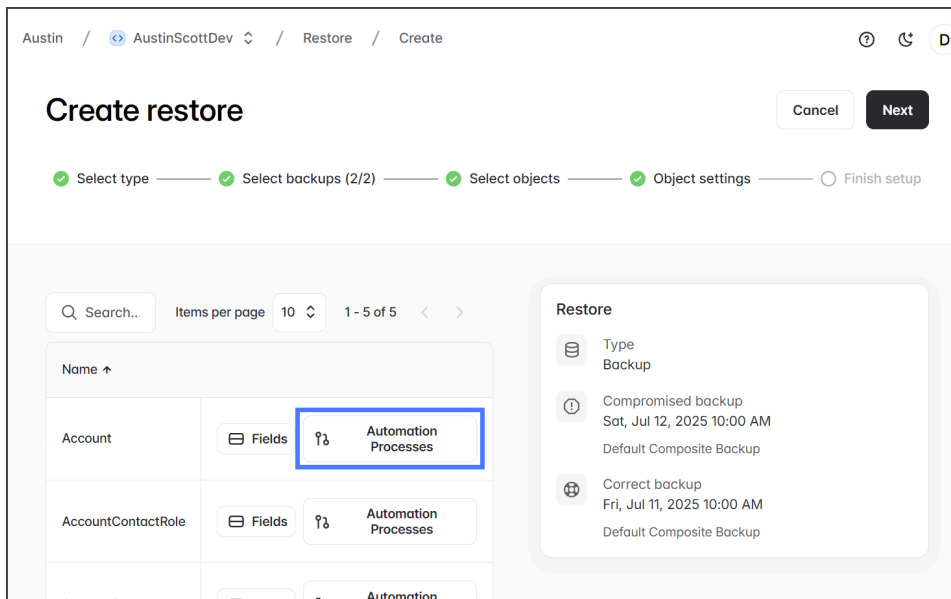
5. Check the checkboxes for any of the processes you want to suspend during the restore.

6. Click **Save**.
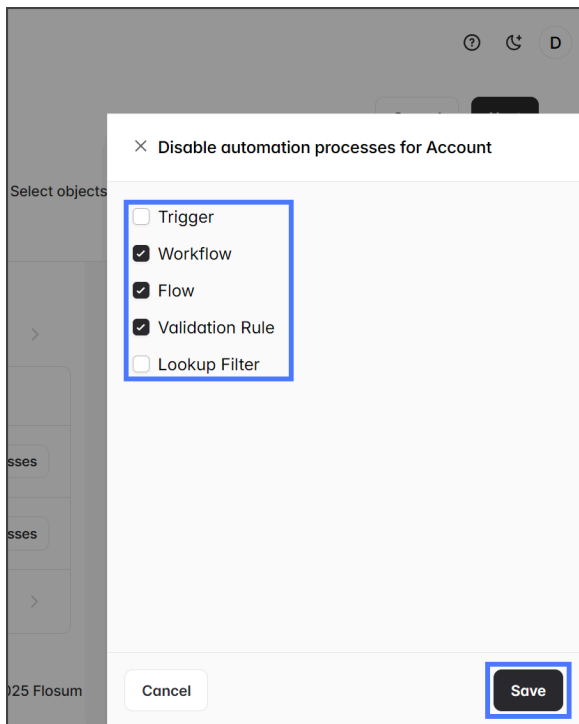
7. Once all the object settings are complete, click **Next**.
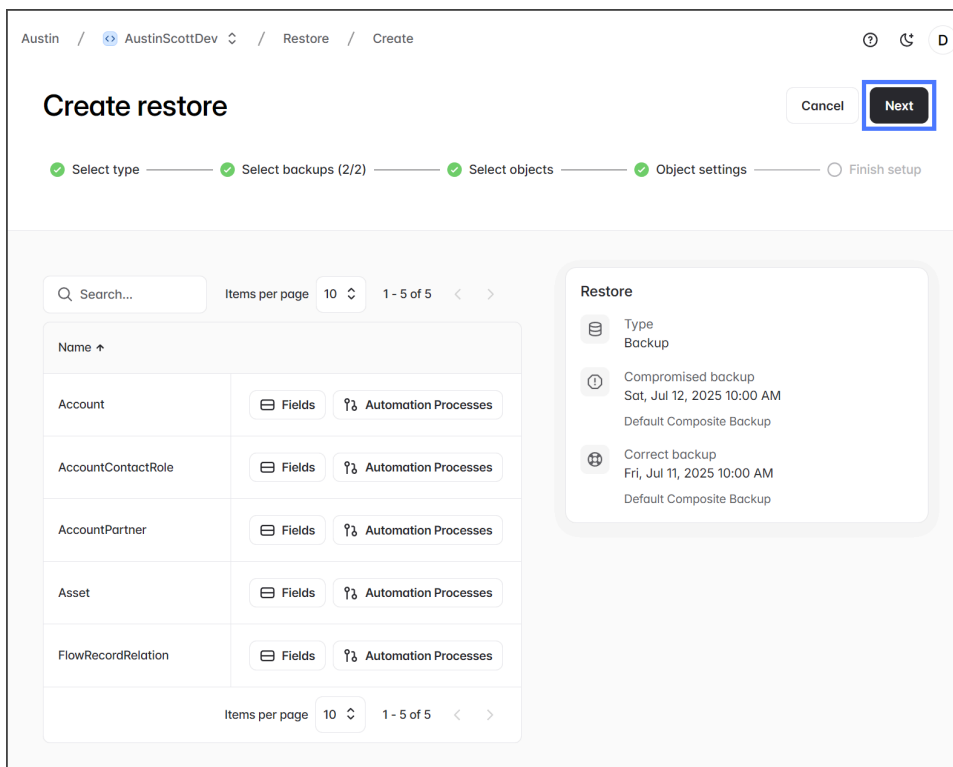
Finish Restore Job Setup

1. Review the restore request to verify that the correct backups for **Compromised** and **Correct** are selected and that the proper objects, filters, and fields are added.

2. Click **Create Request** to initiate the restore preparation job.

> ⓘ No data will be restored to Salesforce at this time. You must review the restored data and execute the restore job before the data is restored to Salesforce.

3. The restore request will begin processing.

4. Scroll down to the **History** table to view the status of the **Restore Request**.

Execute a Restore Job

The second part of the restore process involves reviewing the data retrieved from the Restore Request to ensure the correct data will be restored. If the Restore Request contains valid data, you can proceed to restore it to your selected Salesforce organization.

Select Restore Request

1. Scroll down to the **History** table on the **Restore** page to view all of the completed Restore Request jobs.

2. Click a **Restore Request** job that is marked as **Ready for restore**.

> ⓘ Only **Restore Requests** that have one or more **Records** will be marked as **Ready for restore**.
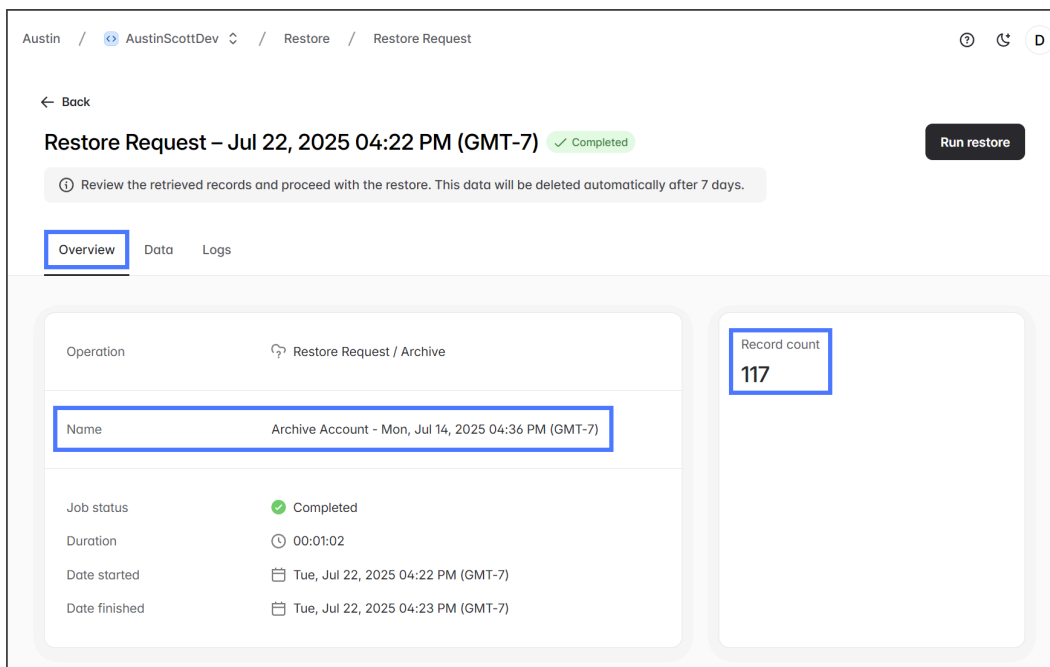
Review Restore Request

Before restoring data, it is recommended to review the request and the data to be restored.

1. Review the information on the **Overview** tab to verify that the data source and the number of records to restore are correct.

2. Click the **Data** tab to view the data to be restored.

3. Click an object to view the records for that object.

4. Click a record to view the fields for the record.

5. Review the field data to ensure the correct records are selected to restore.

6. Click the **Logs** tab to view the Objects and Log for this restore request.

Run Restore

Once you're satisfied with the data to restore, you can proceed to run the **Restore**.

1. Click **Run restore**.
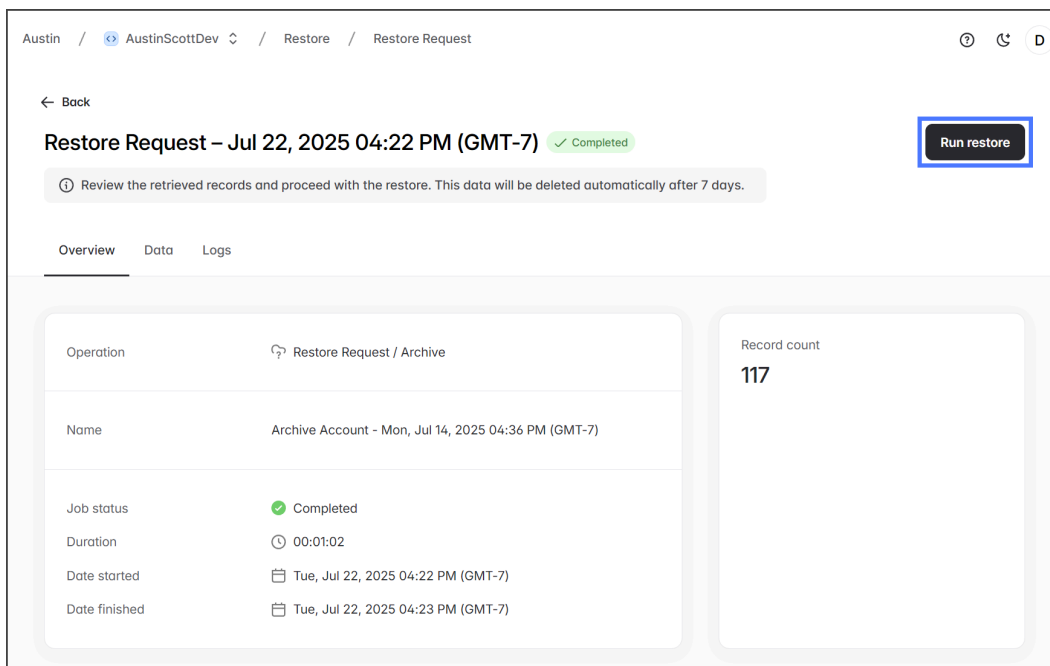
2. Click **Run restore** on the **Run restore** confirmation dialog box.

3. Scroll down to the **History** table to view the status of the Restore Job.

4. Once the **Restore** is complete, you can view the restored data in your Salesforce organization.

View, Compare, and Restore Data from within Salesforce

Prerequisites

Follow the instructions in the [Setting up Backup & Archive Salesforce Application](link) article to configure the **Flosum Backup & Archive** managed package in your Salesforce org.

View and Compare

Once you have added the **Time Machine** Lightning Web Component to your selected objects (i.e., Account, Case, etc.) on Lightning Web Pages, you can compare and restore previous versions of a record.

1. Open a Salesforce record (e.g., **Case**).

2. Click the **Time Machine** tab.

   > ℹ️ You need to add the **Flosum Time Machine** component to a record's page before using this feature. See the instructions above to add the component.

3. Click **Select Versions**.
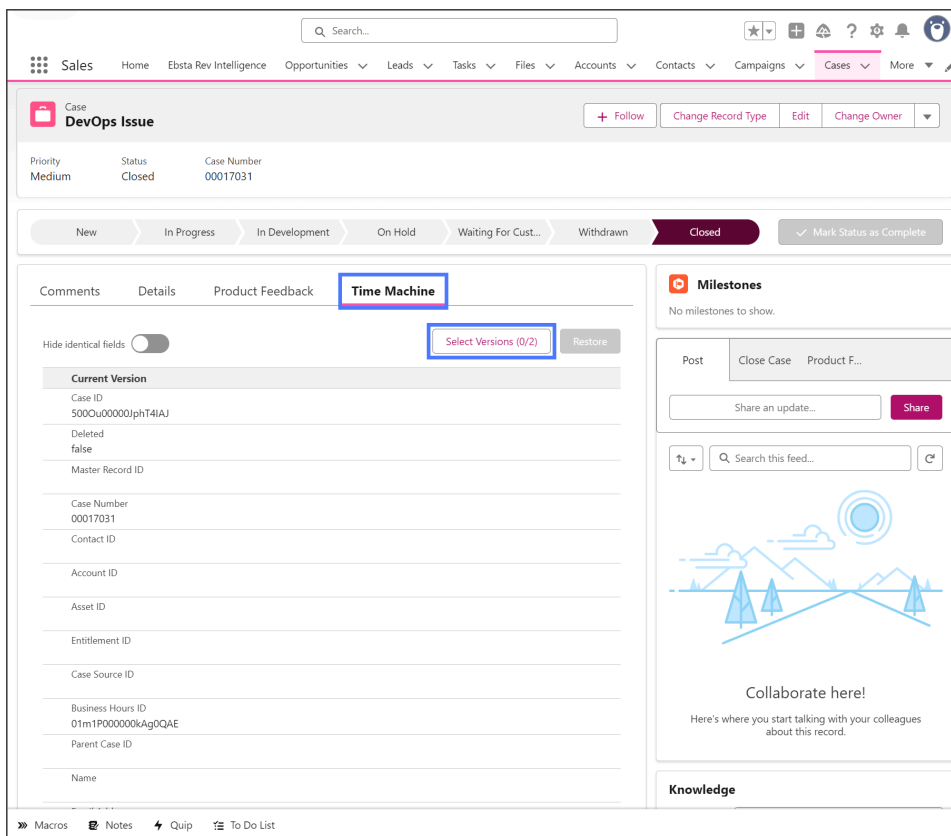
4. Add up to 4 versions from the **Available Versions** list to the **Selected Versions** list.

5. Click **Save**.
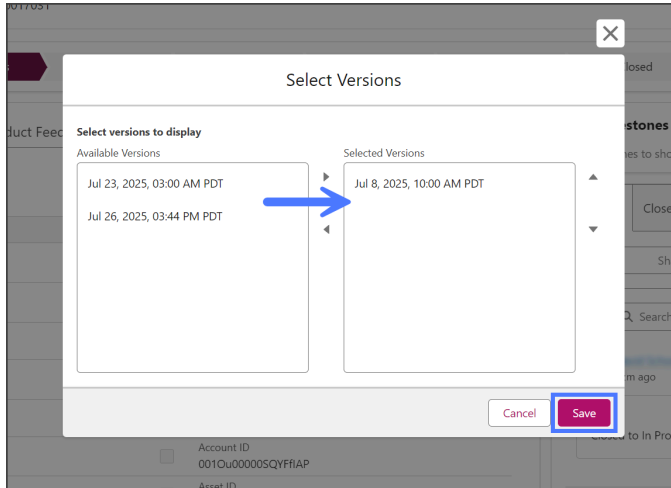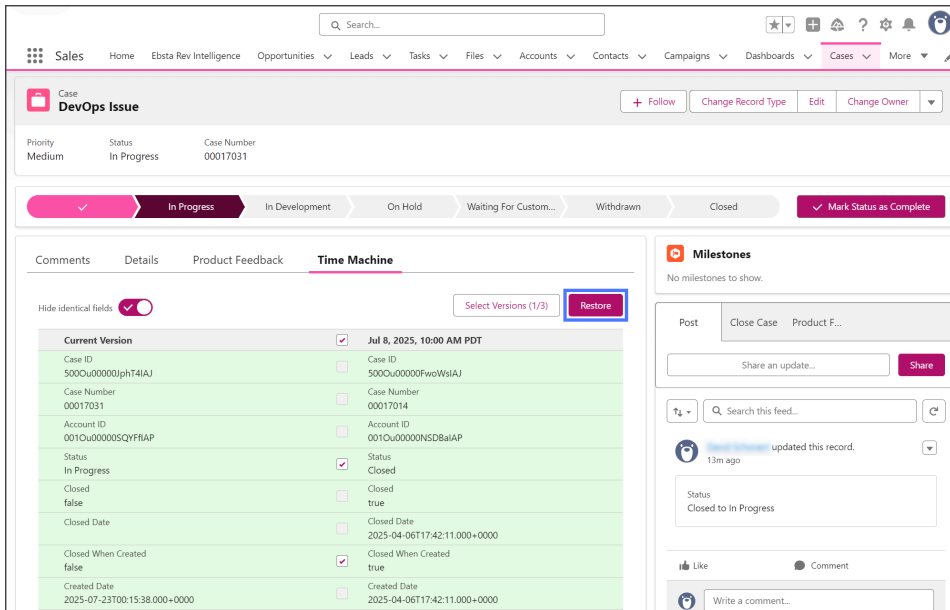
6. Compare the **Current Version** to all of the **Selected Versions**.

7. (Optional) Enable the **Hide identical fields** toggle to only show fields that have changed.

8. Select the fields to restore.

> (i) Only non-reference fields (not lookup fields) can be restored. The fields with the greyed-out checkbox are unavailable for restoration.

9. Click **Restore**.

10. After the fields have been restored, you will see a **Record restored successfully** message.

Export Operations

The Export to CSV feature in the Backup & Archive app enables you to export data from backups or archives into CSV files for external analysis or reporting purposes. You can export full or filtered datasets and download the results in a .zip file format.

Create Export

1. From the **Home** page, select the **Org** to export.
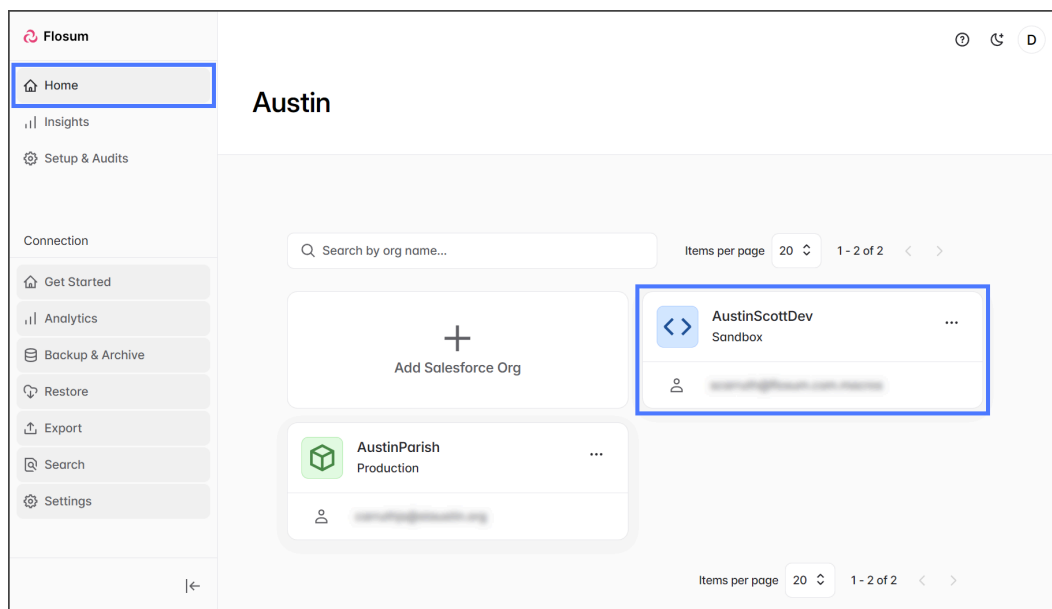
2. Click **Export** from the sidebar menu.

3. Click **Create Export**.
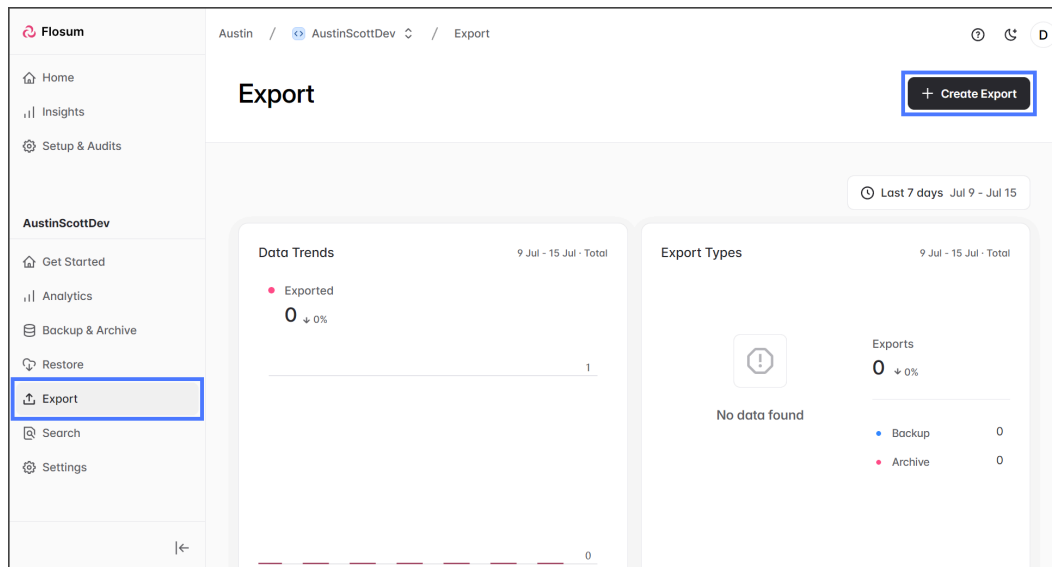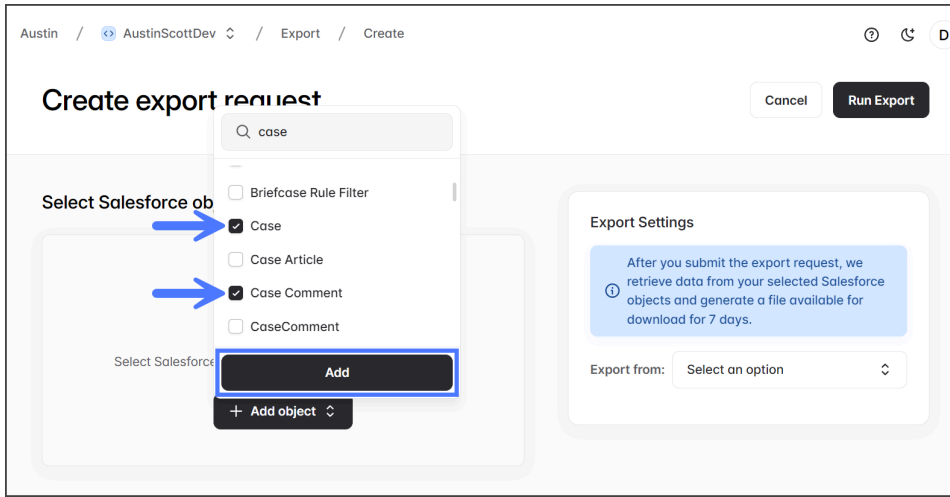
4. Click the **Add object** menu button to select the Salesforce Objects to include in the export.
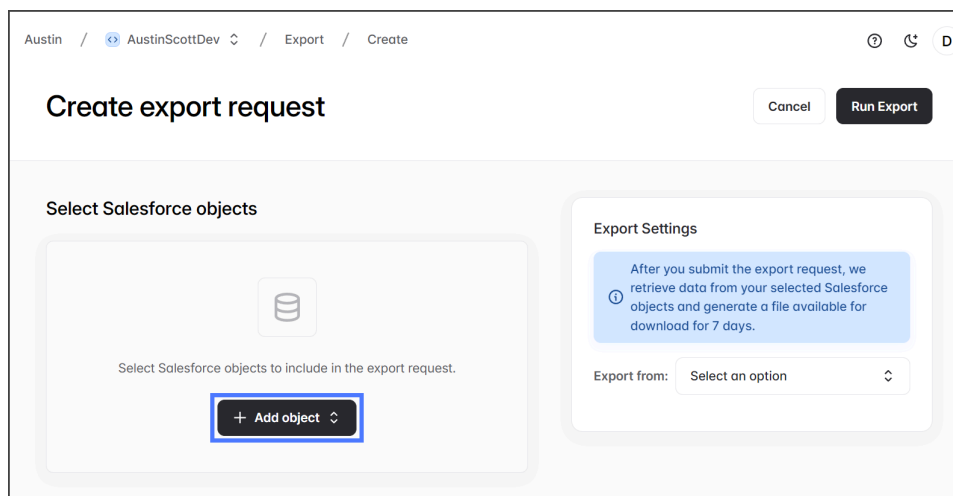
5. Search or browse for objects from the menu.
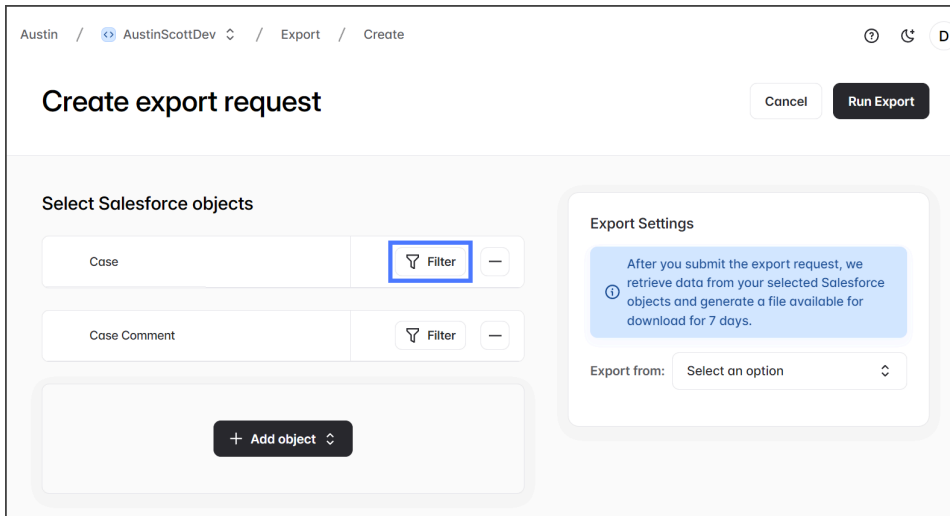
6. Check the objects you want to add.

7. Click **Add** to add all of the selected objects.

8. Click **Filter** to add a filter to the object.

> (i) Adding a filter is optional.

9. Click **Add Filter** to add a filter criteria. You can add more criteria by clicking **Add Filter**.

10. Click **Apply** to save the filter.
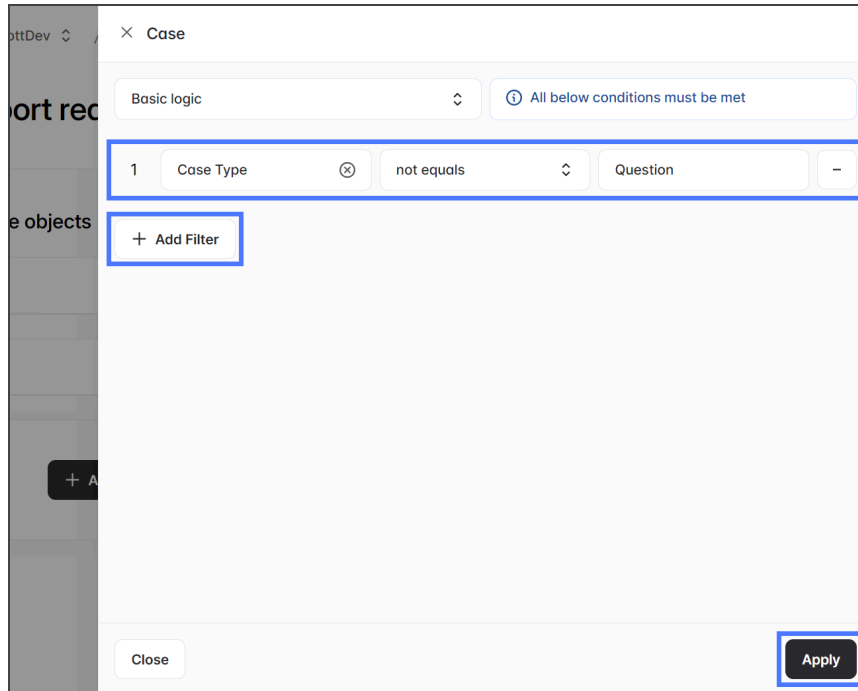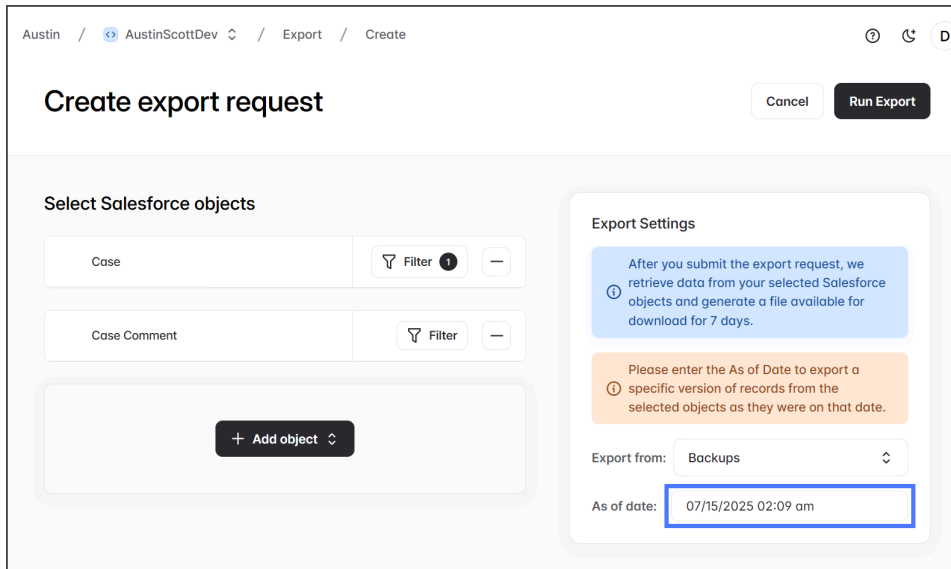
11. Click the **Export from** menu in the **Export Settings** section.

12. Select the source of the export: **Backups** or **Archives**. Configuring each is explained in the following two steps.
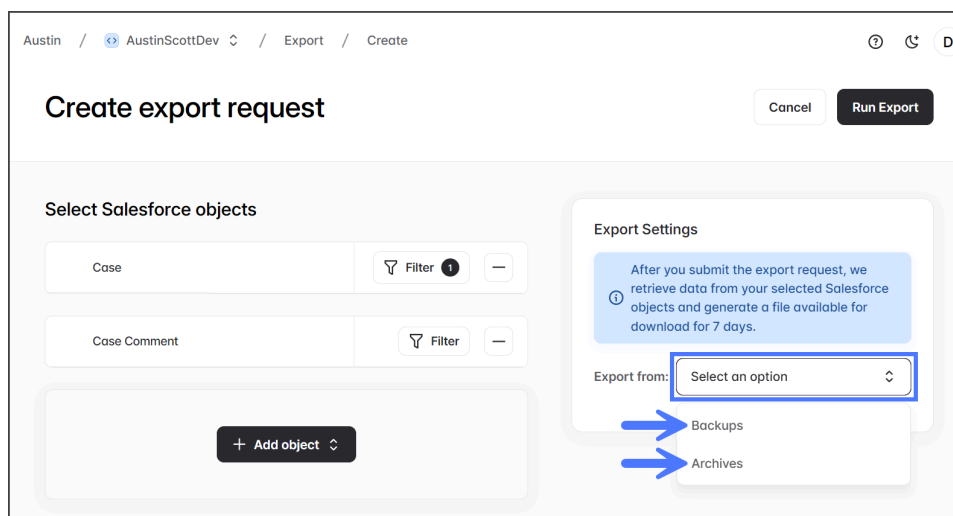
13. Backups: Select the **As of date**.

> (i) The **As of date** lets you choose which version of the records to export based on that date. The records will be exported from the backup that was created closest to, but before, the selected date. For instance, if you have a daily backup at 4 AM and you want to export data from the first of the month, select the first of the month as your date and pick a time that is after the 4 AM backup but before any other backups that day.
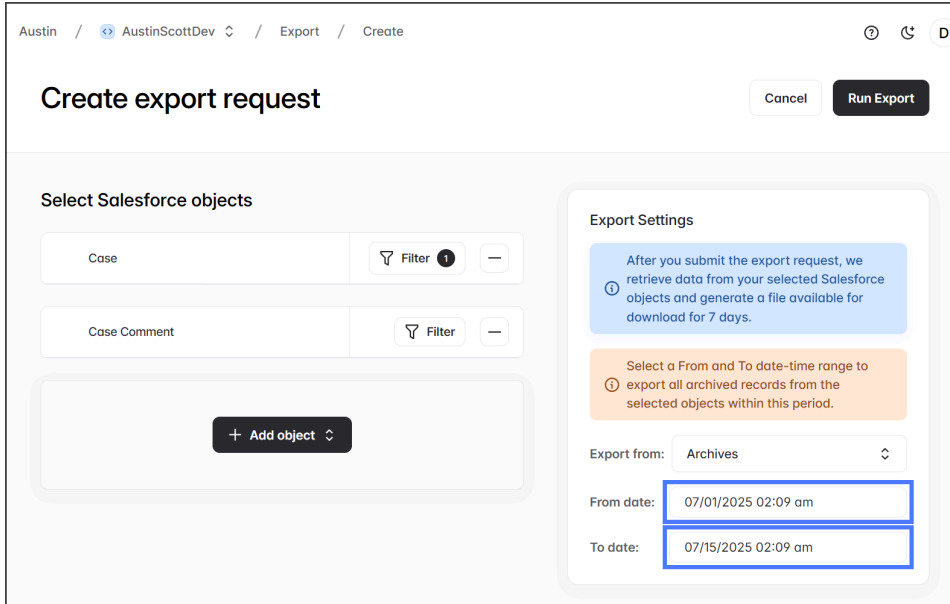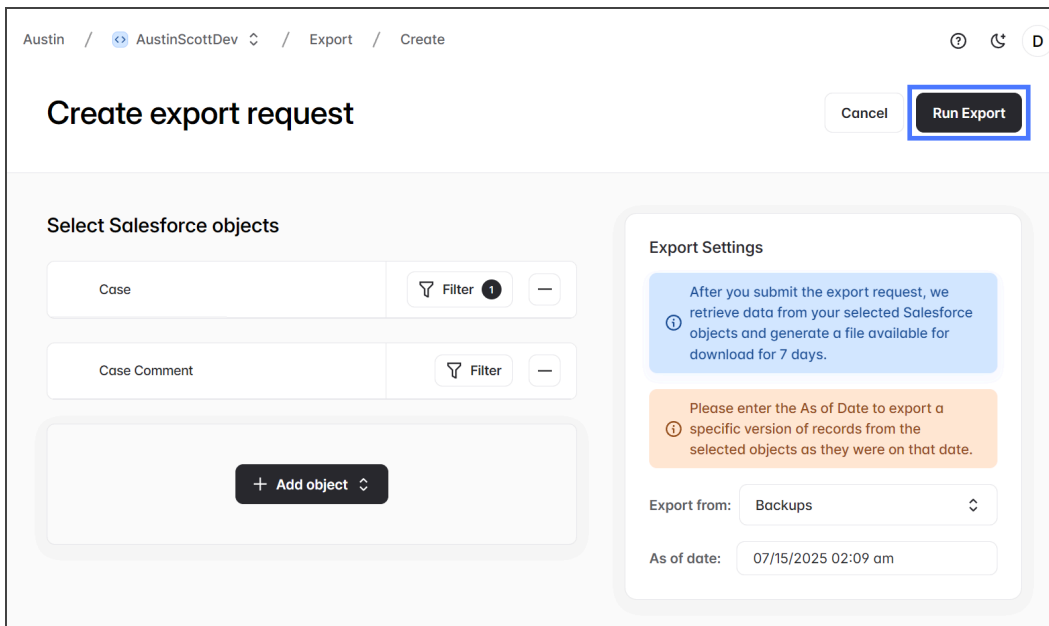
14. Archives: Select the **From date** and **To date**.

> ⓘ The **From date** and **To date** fields enable you to select a range of archived records for export. The records will be exported from the archives created between the selected dates. For example, if you select dates from July 1st to July 15th and there are three archives within this period, the records for the chosen objects will be exported from all three archives.

15. Click **Run Export**.

View and Download Exports

You can view the status of export jobs and download completed exports from the **History** section of the **Export** page.

View Exports

1. From the **Export** page, scroll down to the **History** section.

2. When an export is started, it will display **In Progress** until it is completed.

3. When an export is completed, it will be marked as **Ready for download** if there are any records to be exported.

4. Click an export to view more details and download records.

Download Exports

Export files are in a zip archive with the following file naming: **download-OrgName-DateTime.zip**
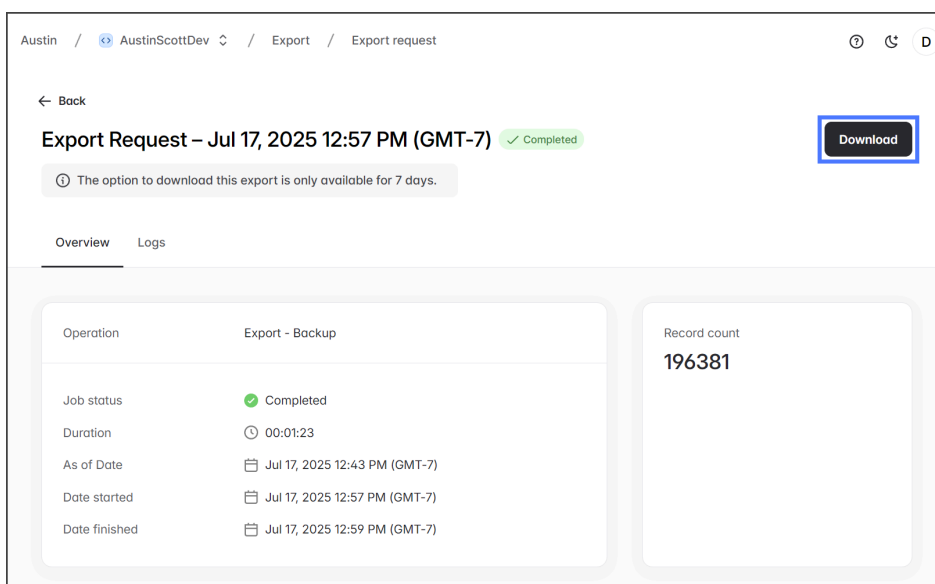
1. Click a **completed** export that is **Ready for download**.

2. Click **Download** to initiate the download process in your browser.
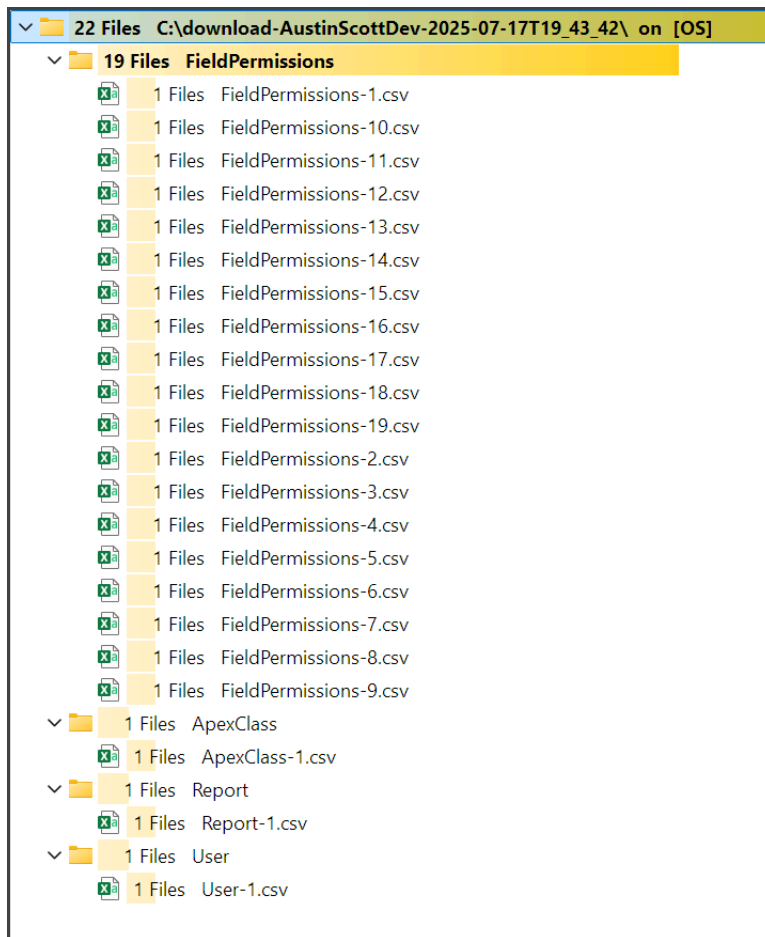
Export File Structures

The exported file will have different file structures based on the type of export.

Backup Export Structure

The .zip file contains a folder for each exported object, and each folder includes one or more CSV files with record data. Each CSV file contains up to 10,000 records. If there are more than 10,000 records, multiple files are created. In the screenshot below, the export includes the **FieldPermissions**, **ApexClass**, **Report**, and **User** objects. The FieldPermissions object has more than 10,000 records, so it is split into multiple files.

Archive Export Structure

The .zip file contains folders for each archive job named **Archive Job ID**. Each Archive Job folder contains subfolders for each object, and each subfolder includes one or more CSV files with record data. Each CSV file contains up to 10,000 records. If there are more than 10,000 records, multiple files are created. The screenshot below shows an export with two archives, each containing the Account object.
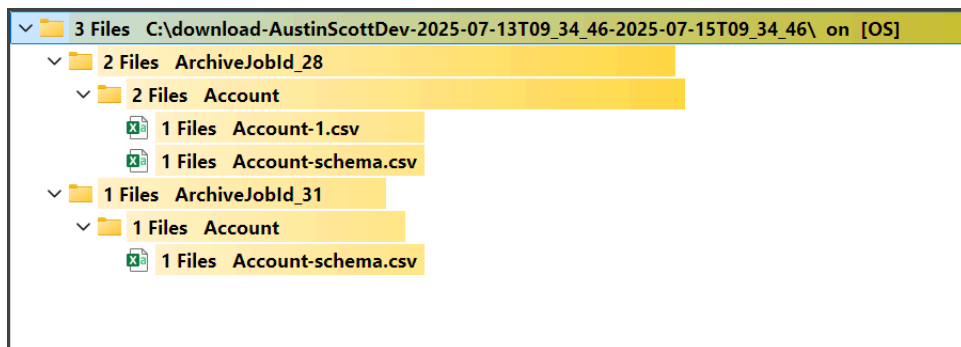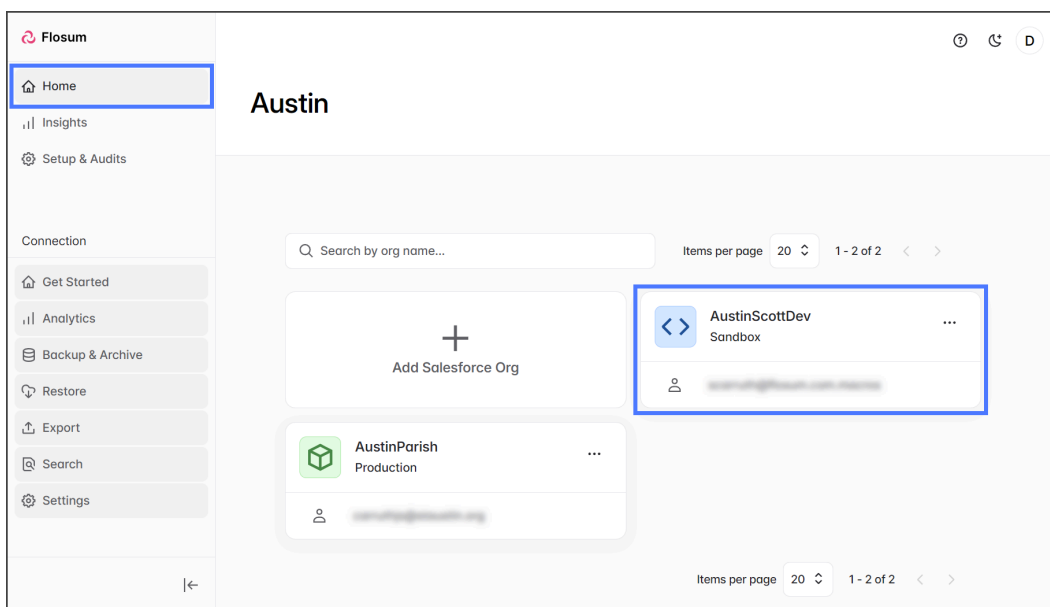
Search Operations

Use this feature to locate specific records across your backup and archive files in order to purge them. The search function retrieves records similar to how you restore them with a Search Job, followed by a Purge Job.
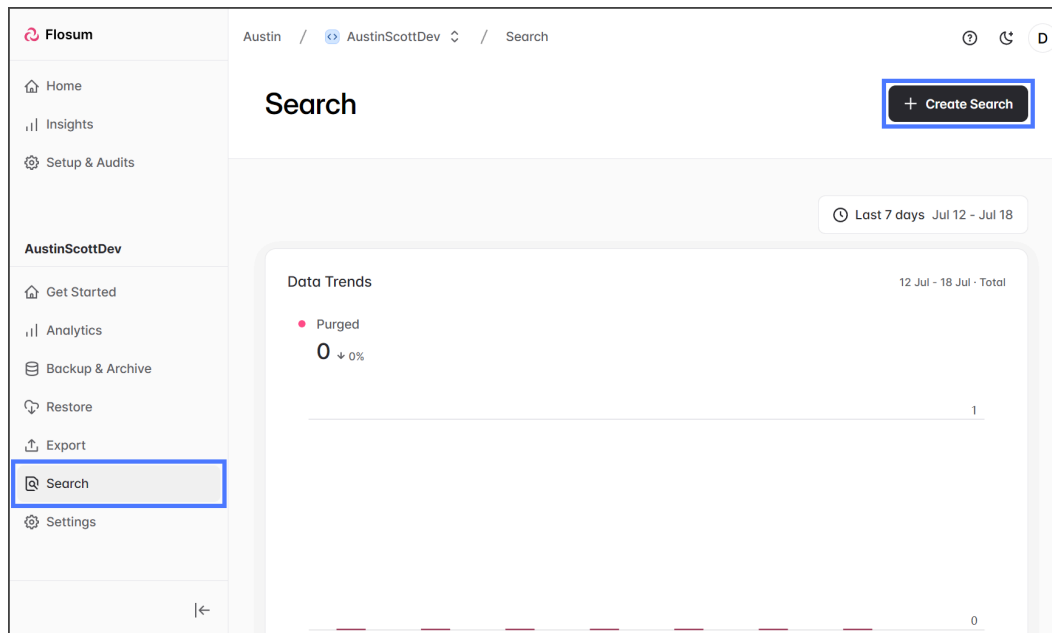
Create a Search Job

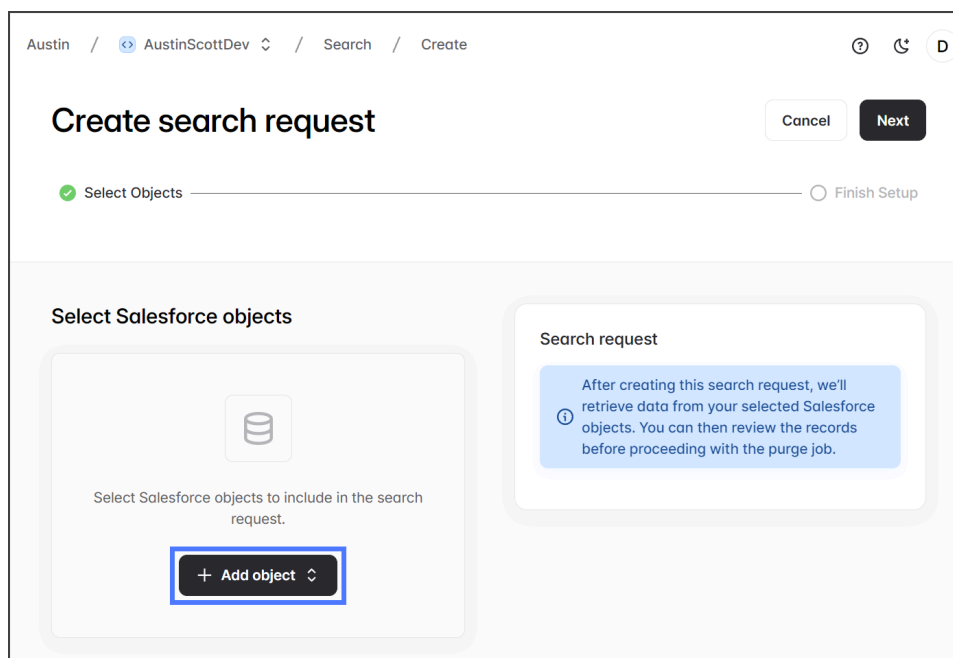1. From the **Home** page, select the **Org** to search.

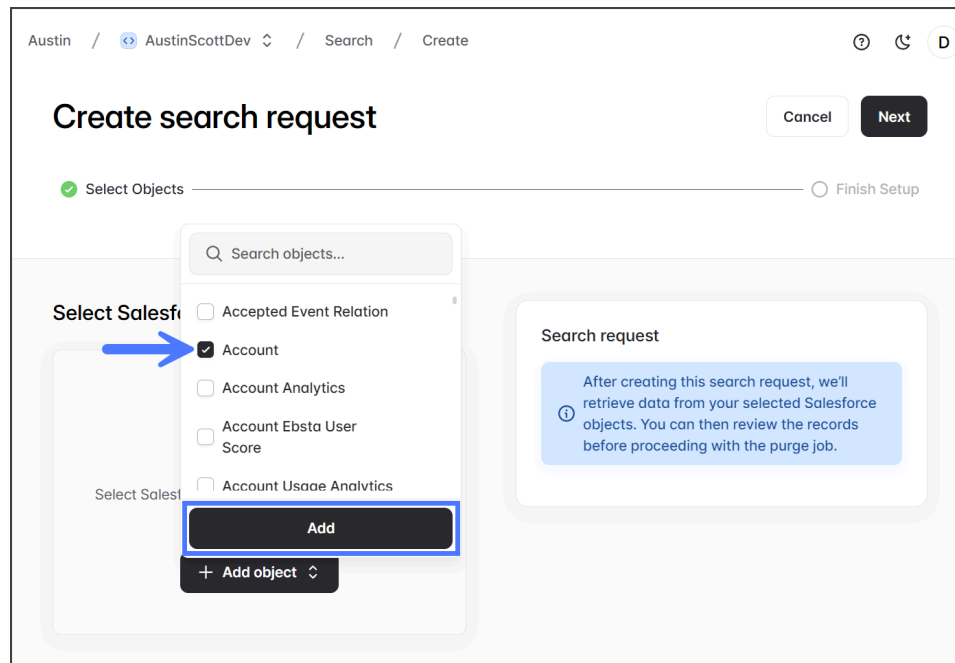2. Click **Search** from the sidebar menu.

3. Click **Create Search**.

4. Click the **Add object** menu button to select the Salesforce Objects to include in the search.

5. Search or browse for objects from the menu.
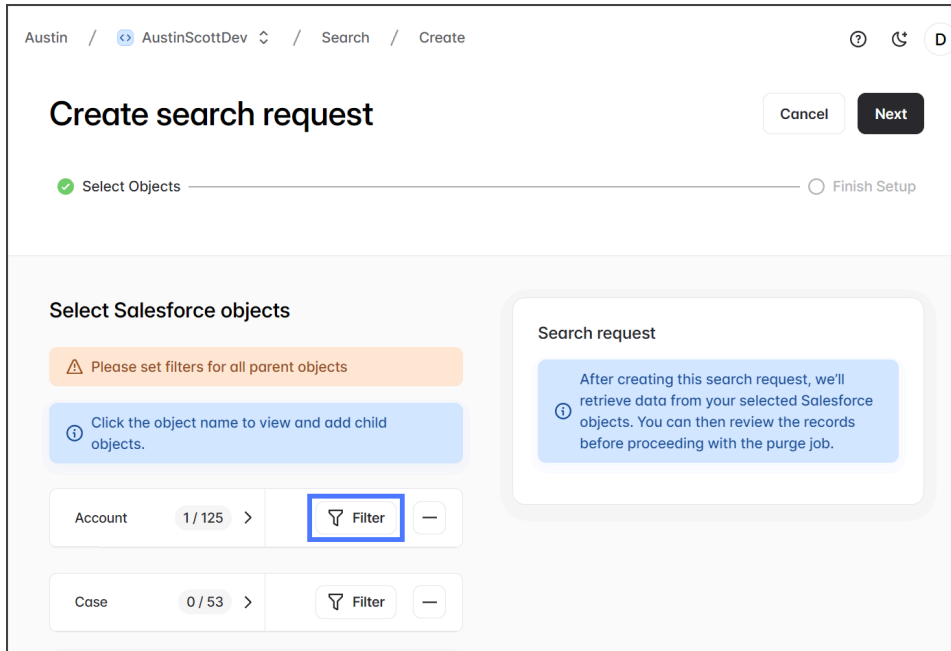
6. Check the objects you want to add.

7. Click **Add** to add all of the selected objects.

8. (Optional) Click an object to open the **Add child objects** dialog.

    a. Click the **+ Add** button next to each of the child objects to add.

    b. Once you have added all the objects, click **Apply** to save the changes.
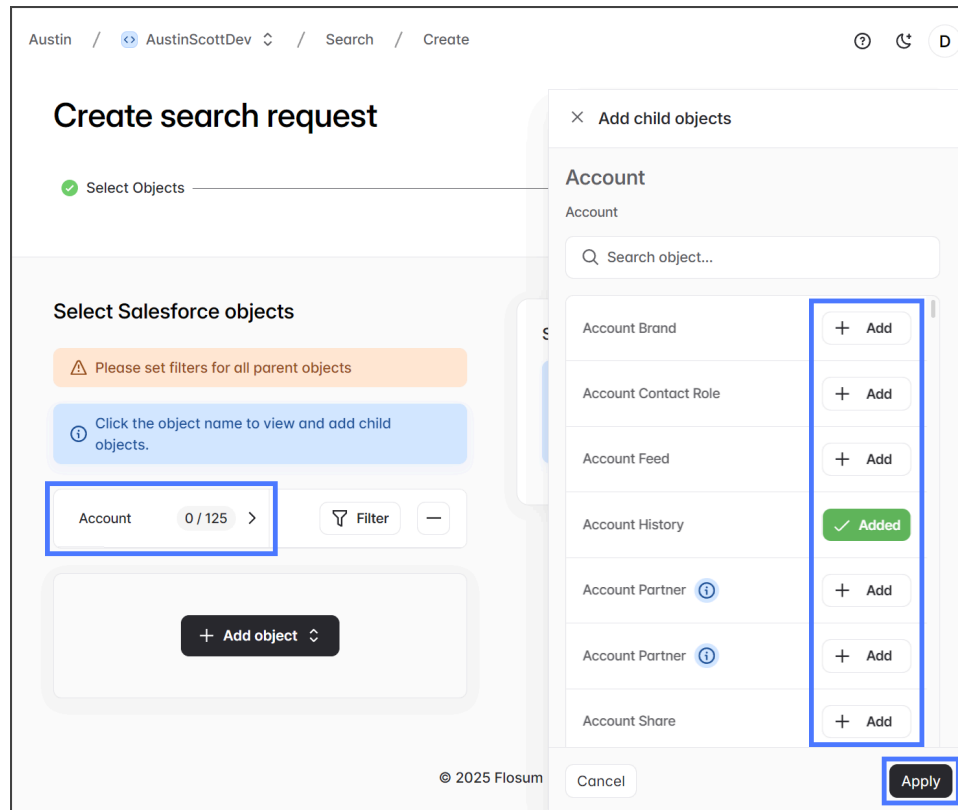
9. Click **Filter** to add a filter to the object. Filters are required for search operations.
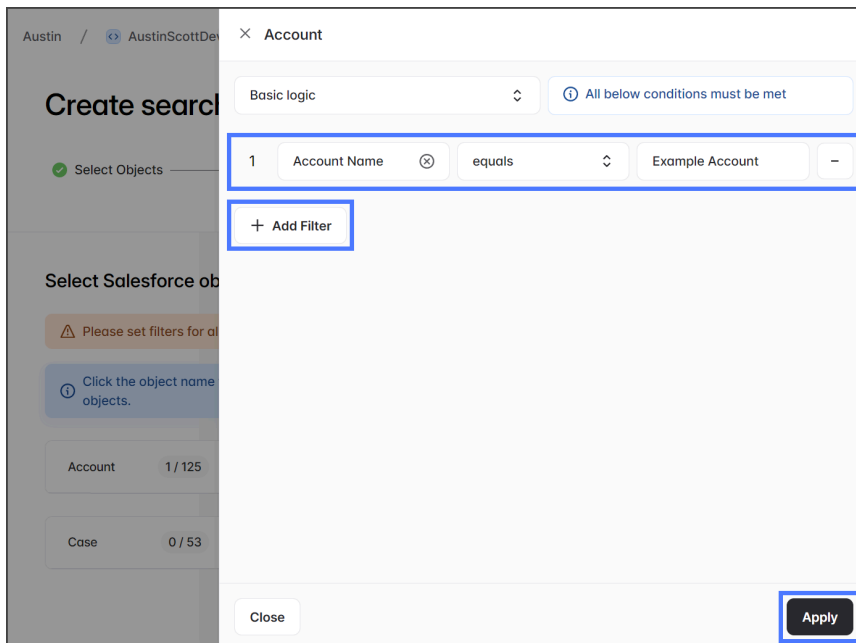
10. Click **Add Filter** in the filter dialog to add a filter criteria.

11. The screenshot below shows an example filter.

12. Click **Apply** to save the filter.
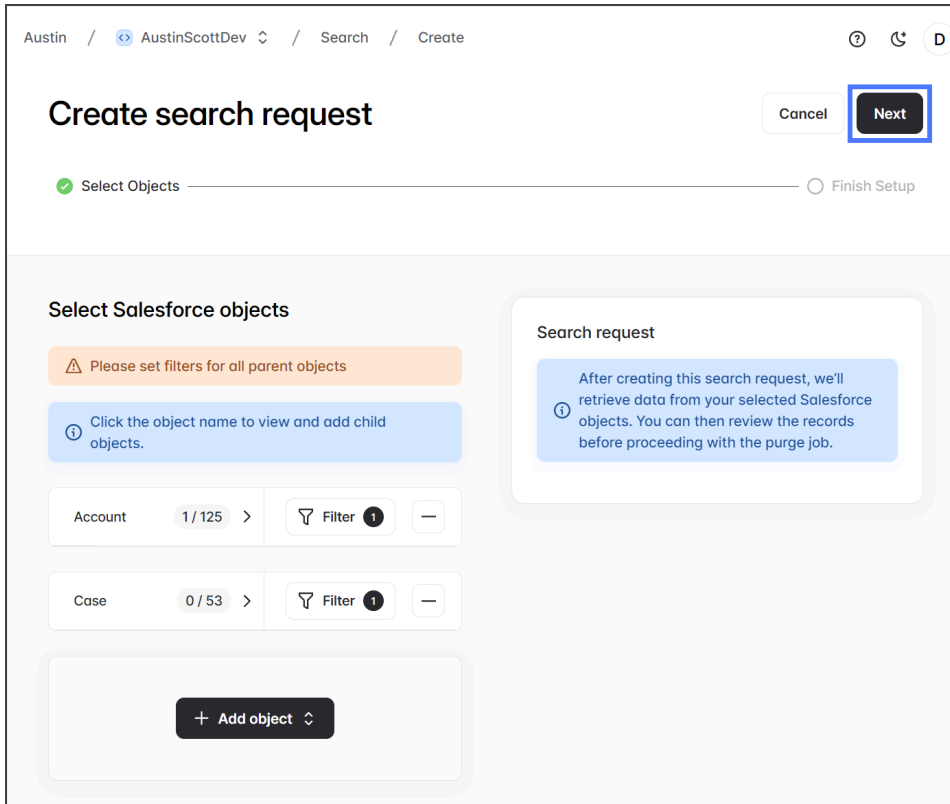
13. Click **Next**.

14. Review the selected objects and filters.

15. Click **Search** to start the search.
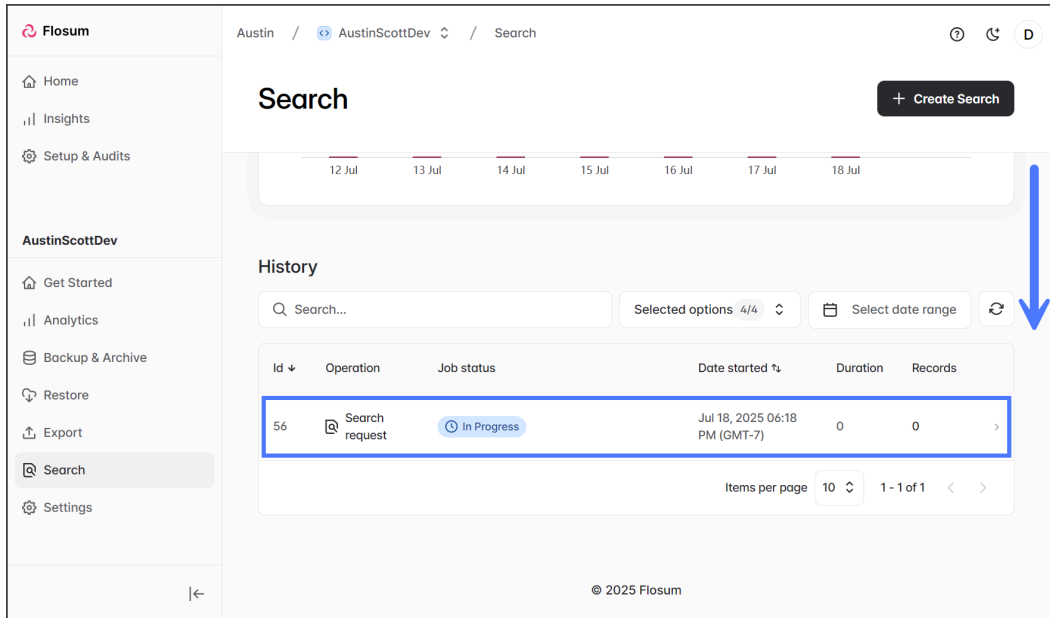
16. Scroll down to the **History** table to view the status of the Search Job.

Review a Search Request

Once your Search Request has completed, you can review its details and results. The data in a search request is organized as follows:

```
Search Request > Data > Object > Version > Record > Fields/Data
```

1. Scroll down to the **History** table on the **Search** page to view all of the completed search jobs.

2. Click a **Search Request** job to view the records that were found during the search.

> (i) The **Records** column indicates the number of records found in response to your search request. The **Ready for Purge** tag will only appear if the search job completes with one or more matching records. If the search job does not find any records that match the search criteria, no data will be available for viewing or purging.
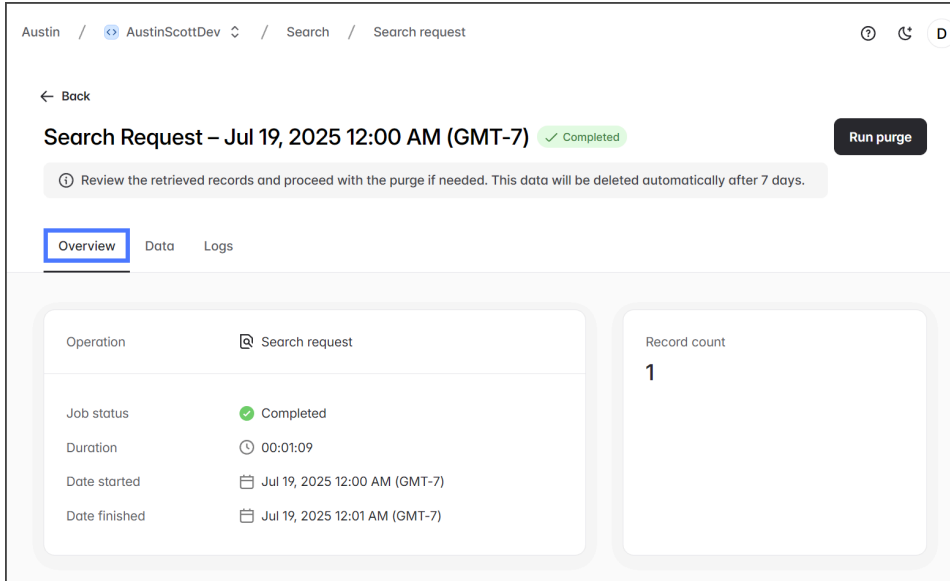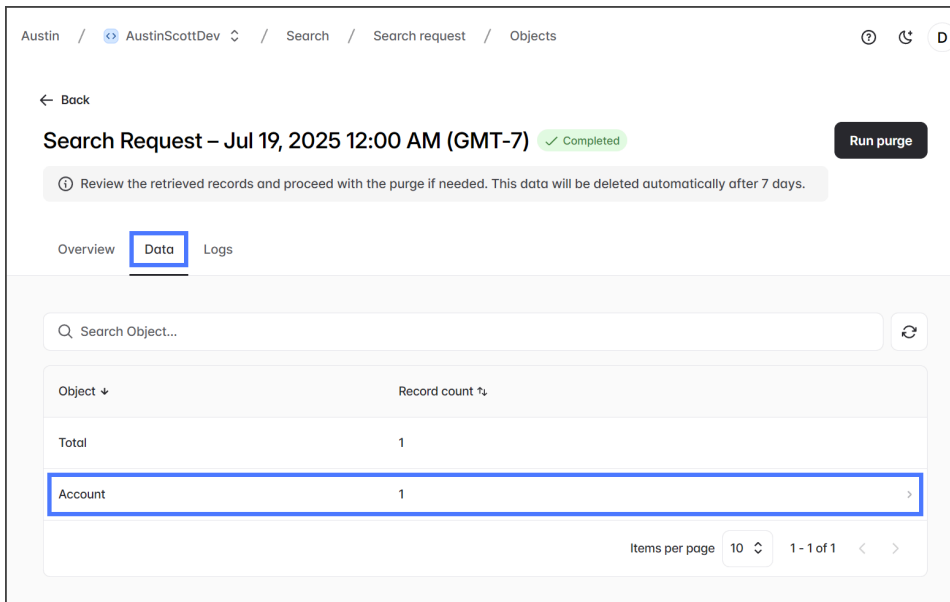
3. The **Overview** tab displays details about the search job.

4. Click the **Data** tab to view the data found by the search.

5. Click an object to view the records for that object.

6. Click a record to view the versions of that record.

7. Click a version to view the fields and data for that version of the record.

8. You can search or browse to view all of the data in the fields of this record.

Purge Data (Optional)

After reviewing the records identified by a search job, you can start a purge job. This process will remove all records found in the search job from every version listed. The purpose of purging data is to help you comply with GDPR requirements.

> ⚠ Purging Data will only delete records from the Flosoum **Backup & Restore** app. No data will be deleted from **Salesforce**.

1. Scroll down to the **History** table on the **Search** page to view all of the completed search jobs.

2. Click a **Search Request** job that is marked as **Ready for purge**.

> ⓘ Only **Search Requests** that have one or more **Records** and haven't been purged will be marked as **Ready for purge**.

3. Click **Run purge**.

> ⚠ Running a **Purge** will permanently remove the selected data from all backups and archives. Ensure you have confirmed that the correct data is chosen for deletion, as this process cannot be reversed.
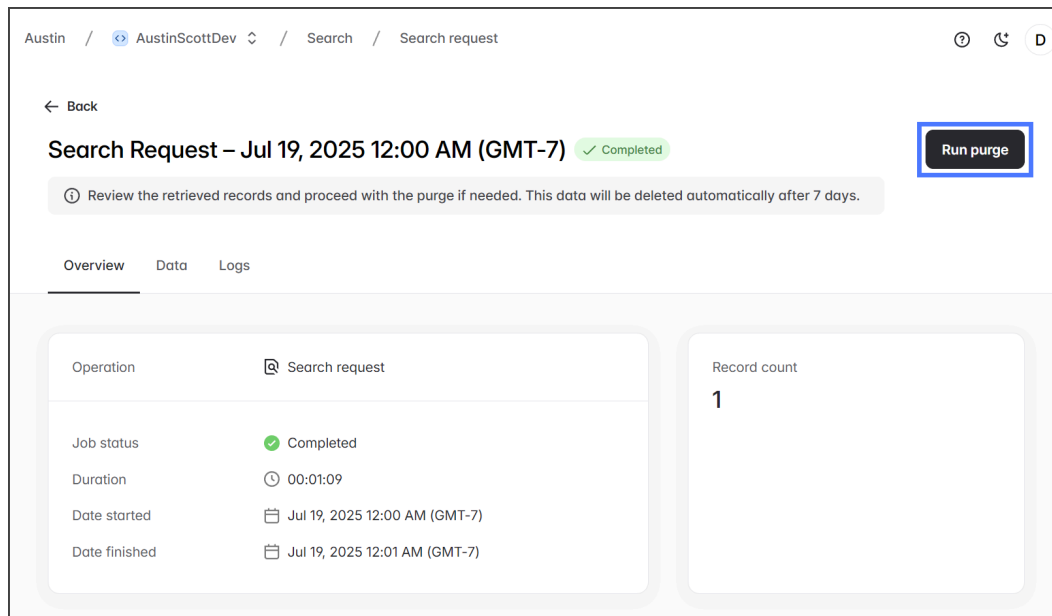
4. Click **Run purge** on the **Run purge** confirmation dialog box.
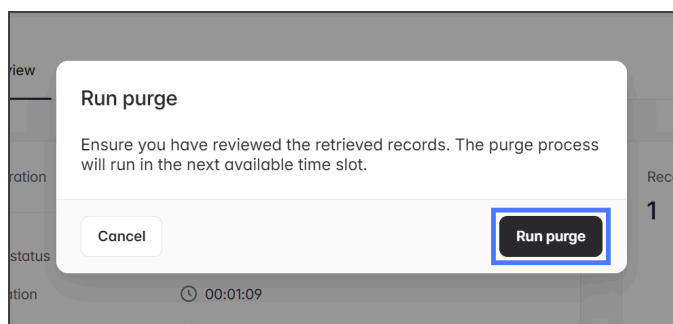
5. Scroll down to the **History** table to view the status of the Purge Job.

Settings

The **Settings** page item allows you to view general details about your tenant, set notifications, and configure integrations.

1. From the **Home** page, select the **Org** to view settings.
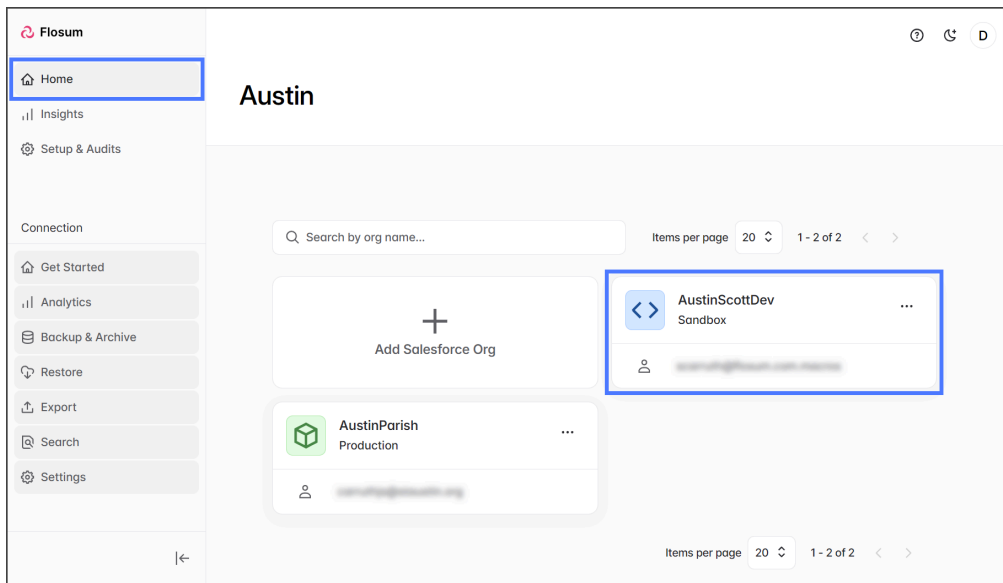
2. Click **Settings** from the sidebar menu.

3. Navigate to **General**, **Notifications**, and **Integrations** settings using the tabs.
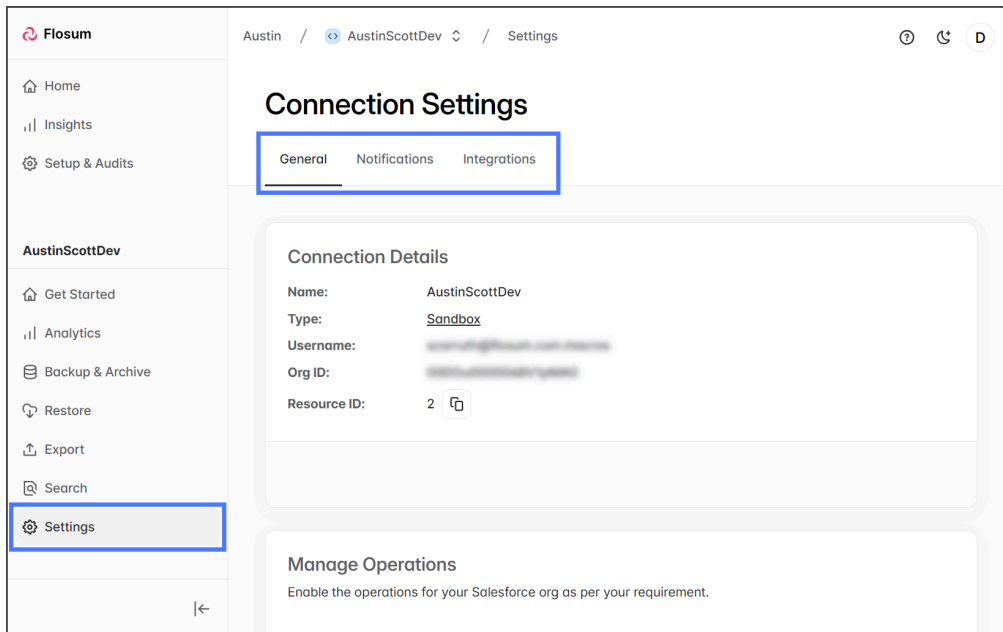
General Tab

The **General** Settings tab allows you to review the details of your tenant's connection to your Salesforce org, manage backup and archive operations, set API quotas, and delete the connection.
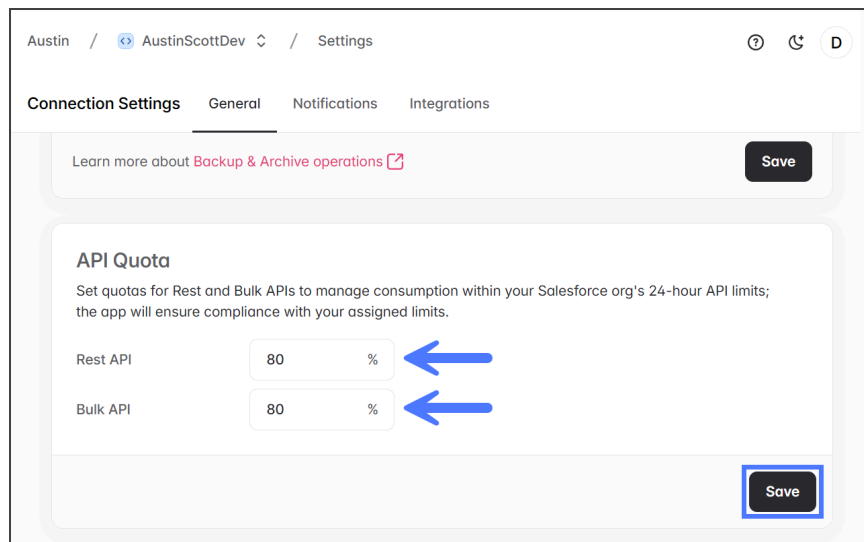
Manage Operations

By default, Flosum automatically enables scheduled backups and archives. This provides a restore point in case of data loss. If you turn off these settings, you cannot schedule backup or archive operations. If you make changes, click **Save** to apply them.
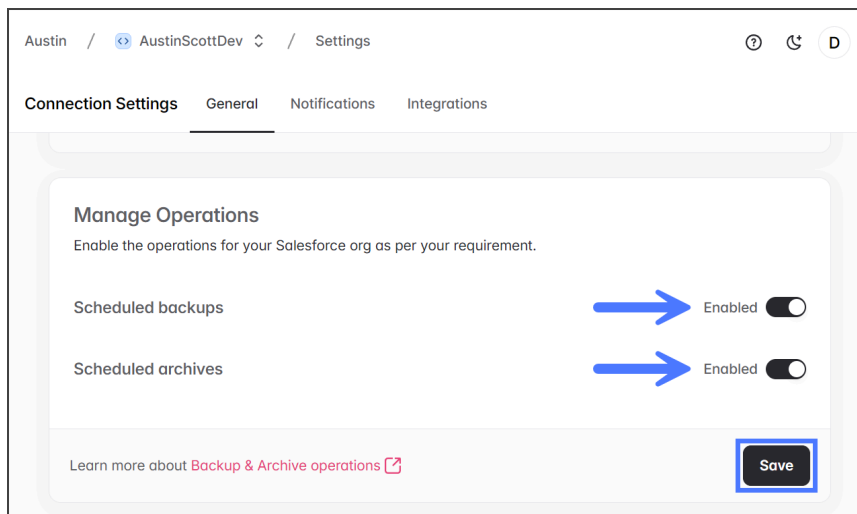
Configuration API Quota

Salesforce has governor limits on its API to prevent any single customer from overusing resources on its Points of Determination (PoDs). By default, Flosum caps Rest and Bulk API calls at 80%. This helps ensure that your backup and archive jobs stay within the governor limits while allowing other API operations to run. As a best practice, keep the limits at 80% to maintain capacity for other API calls and avoid job suspension if you exceed the 24-hour API limits. However, if necessary, you can change these limits. If you make changes, click **Save** to apply them.

Delete Connection

The Delete Connection section allows you to permanently remove the Salesforce Org connected to your tenant. Click **Delete** to perform this operation.

> ⚠️ Deleting an Org Connection will remove all backups, archives, and any other data related to this Org from Flosum Backup & Archive. This action is not reversible.
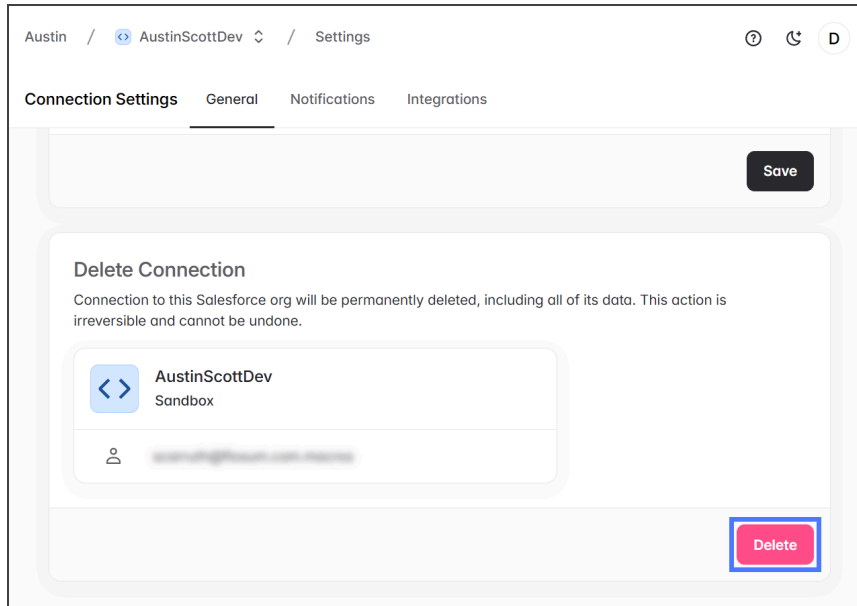
Notifications

The **Notifications** settings tab provides options for configuring notifications for your tenant. The notification settings are divided into three parts: **Recipients**, **Default Notifications**, and **Custom Notifications**.

Recipients
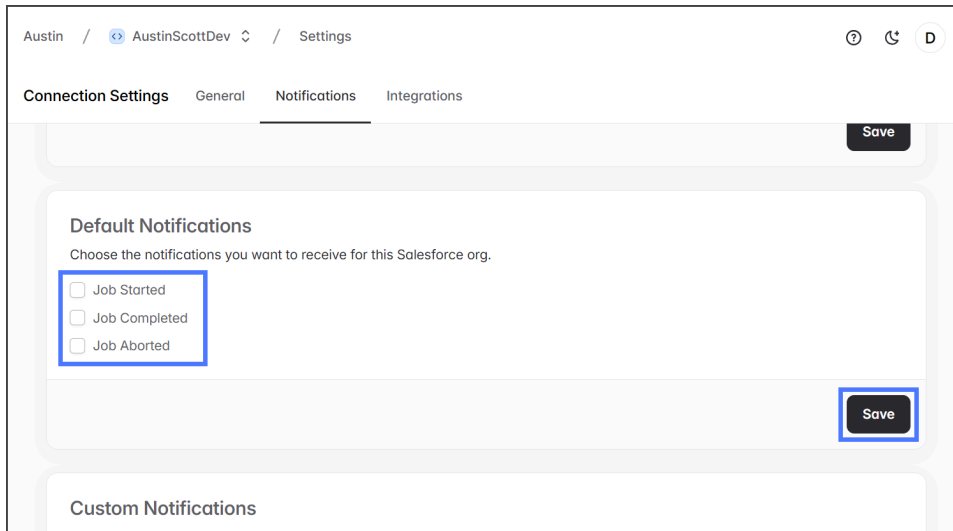
You can add, edit, and remove email addresses to the list of recipients to receive notifications.

1. Click **Add More** to add an email address.

2. Remove recipients from the list by clicking the **minus "-"** symbol next to their email address.

3. Click **Save** to apply any changes.
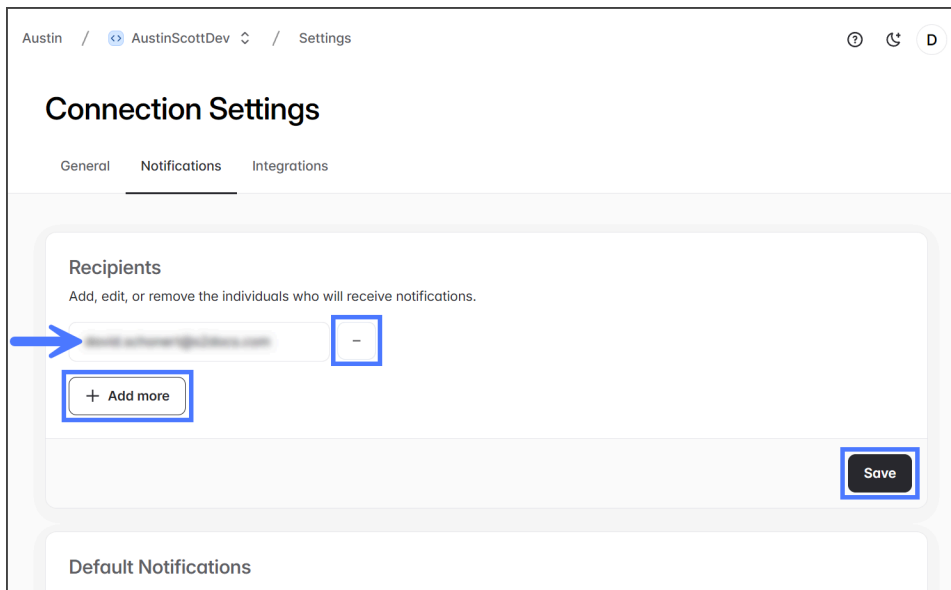
Default Notifications

Enable default notifications for job **Starts**, **Completions**, and **Aborts**. If you make changes, click **Save** to apply them.

Custom Notifications

Custom Notifications enable you to select specific objects and events for which you want to receive notifications. This is useful for monitoring particular object-level changes, such as spikes in new records, updates, or deletions. Each rule is evaluated after a backup has completed.

1. Click **Add More** to add a custom notification.

2. Configure the notification to meet your needs.

3. Remove notifications from the list by clicking the **minus "-"** symbol.

4. Click **Save** to apply any changes.

Integrations

With the latest version of Flosum Backup & Archive, Flosum offers a Lightning Web Component that you can install in your Salesforce organization to view your archived files. This component is installed through a managed package during the initial connection to your Salesforce org. Additionally, the Integrations tab allows you to update the integration as needed.
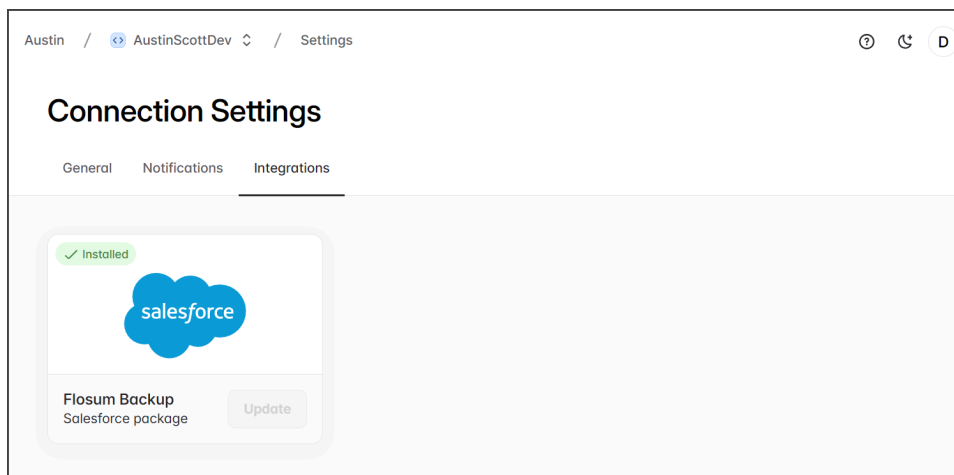
Analytics

The Flosum Analytics Dashboard provides detailed insights into your Salesforce environments, including usage trends, backup statistics, and storage metrics. This section guides you through the analytics and explains key visualizations.

1. From the **Home** page, select the **Org** to analyze.
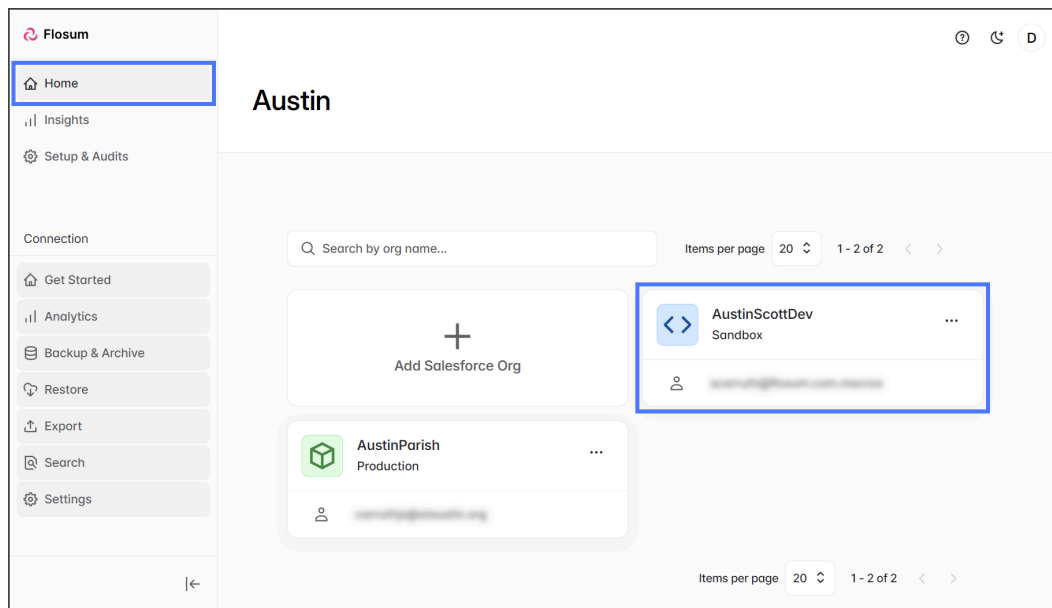
2. Click **Analytics** from the sidebar menu.
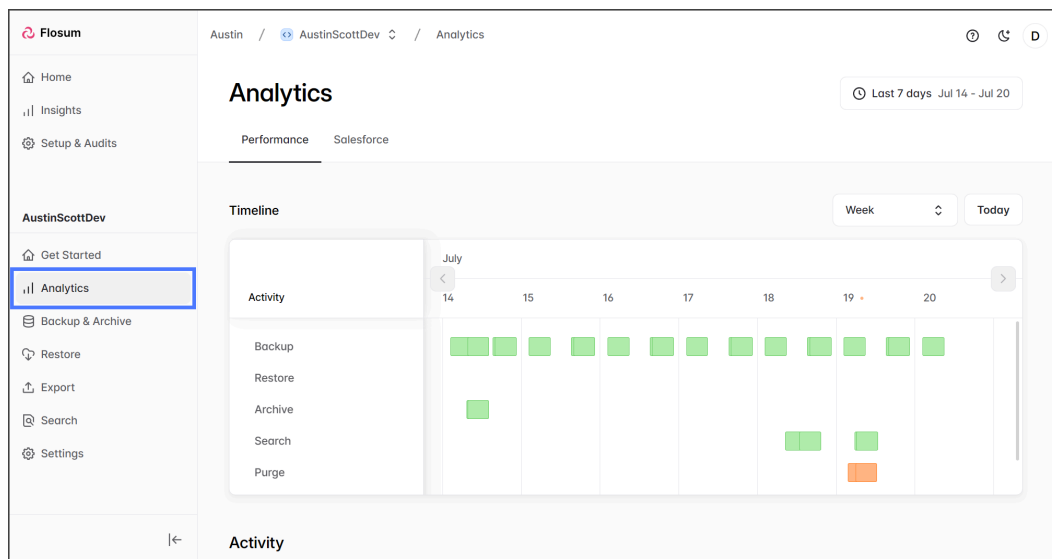
Set Date Range

The range of data displayed in the Analytics section can be adjusted using the **Date Range** box.

> (i) When switching tabs, the **Date Range** will be reset to the default of the **Last 7 days**. The max range is 12 months.

1. Click the **Date Range** box.

2. Use the calendar widget to select one of the predefined ranges or set a custom one.

3. Once selected, the range will automatically be applied.
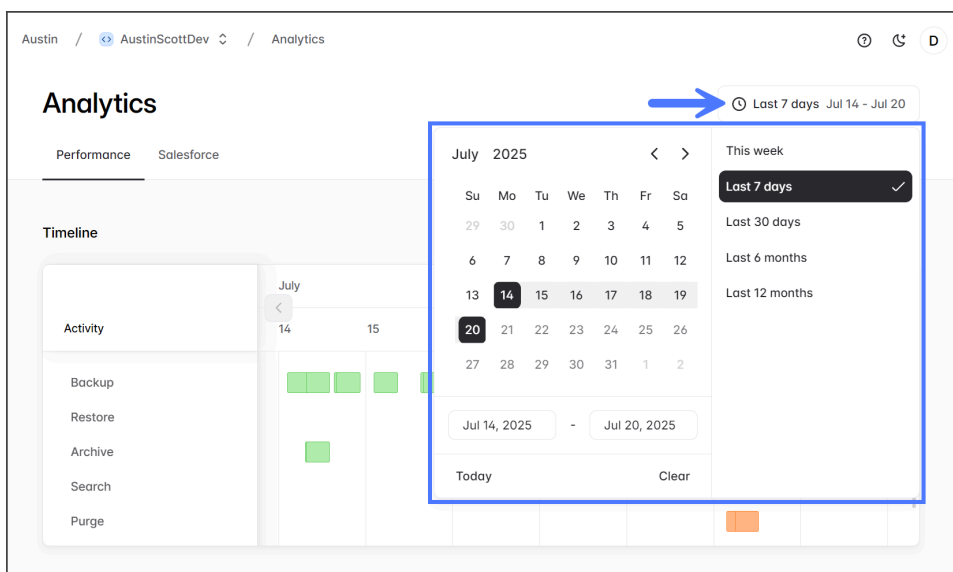
Performance Analytics

The Performance Analytics tab provides you with a timeline view of your Backup & Archive activity.

Timeline and Activity

In the **Timeline** chart, you can see when your Backup, Restore, Archive, Search, Purge, and Export actions took place. The timeline can be adjusted by Day or Week.

The **Activity** section displays the most recent Backup, Restore, Archive, and Export operations, along with relevant details.
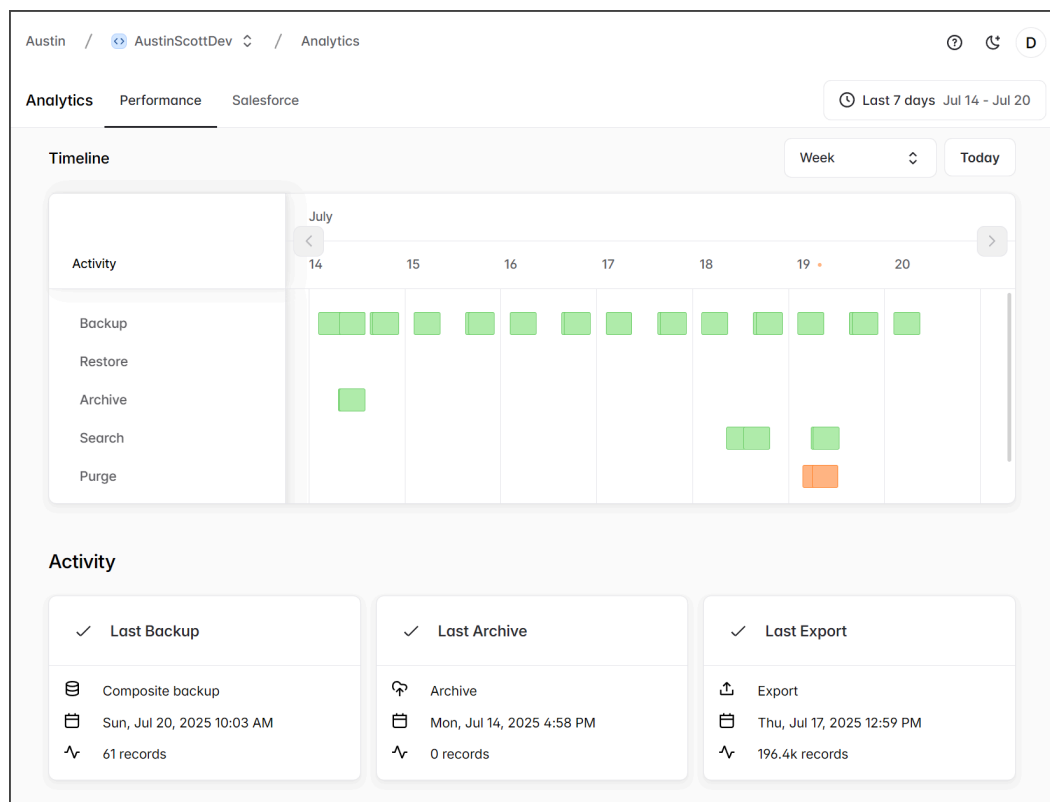
Summary

The summary graphic displays all operations and storage used within the specified date range.
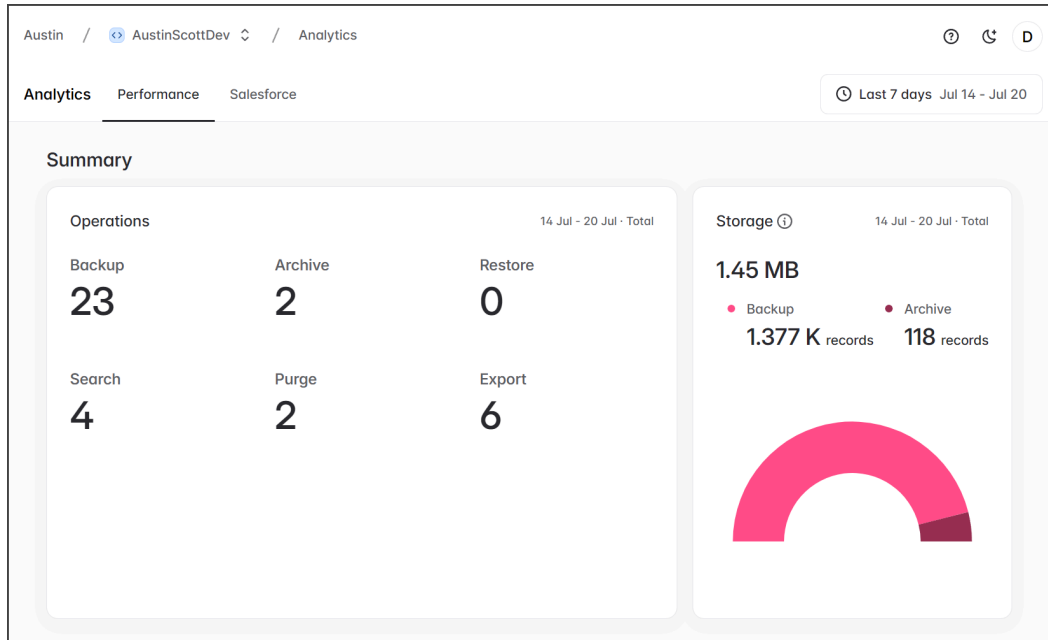
Monitoring

The monitoring charts display your **Salesforce API Usage Trend** and **Backup Duration Trends** over the selected date range. These charts help you identify whether you are exceeding your API limits and track the duration of your backups.
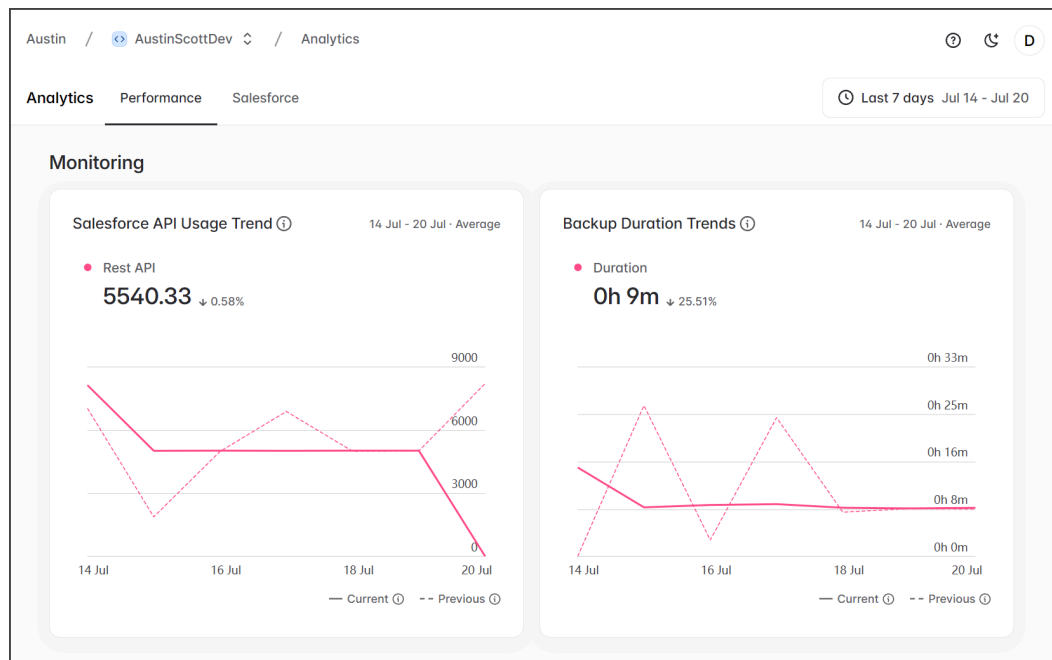
Salesforce

Analyze your Salesforce data changes using the **Salesforce** tab to track data growth trends and identify areas for improvement. This section includes charts that display how your data fluctuates over time, as well as the size and number of records stored in your backups.

Growth Trends

The **Growth Trends** chart displays the size of your backups over time. By default, the duration is set to the last 7 days. You can adjust the date range to show growth trends for different periods, up to the Last 12 months.
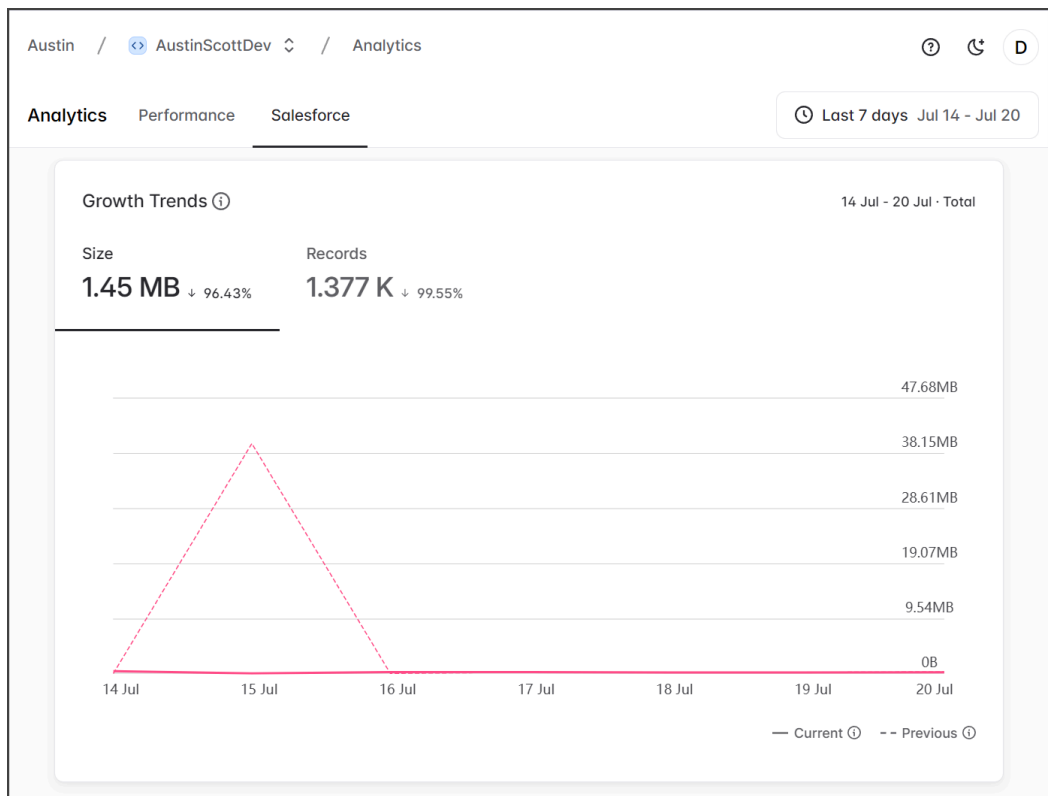
Data Lifecycle

The Data Lifecycle chart illustrates the flow of data from your Salesforce Org to your Flosum backup and its evolution over time. This chart allows you to visualize which objects have been created, updated, or deleted, along with the number of records involved, as they are backed up.

The chart can be rearranged by clicking and dragging a tag to any place on the chart.
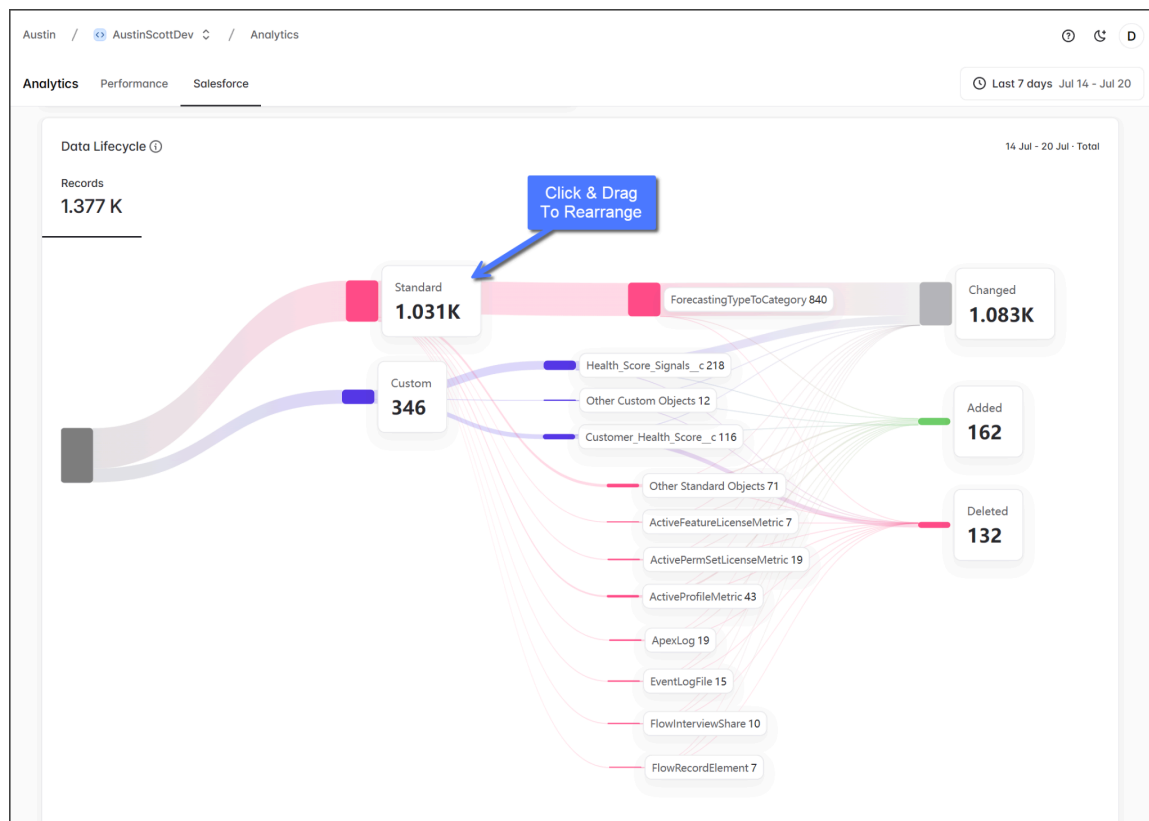
Storage

The **Storage** chart enables you to visualize the size and number of records in your data by using the **Size** and **Records** toggle. You can view the data in two types of charts: **Sunburst** and **Treemap**.
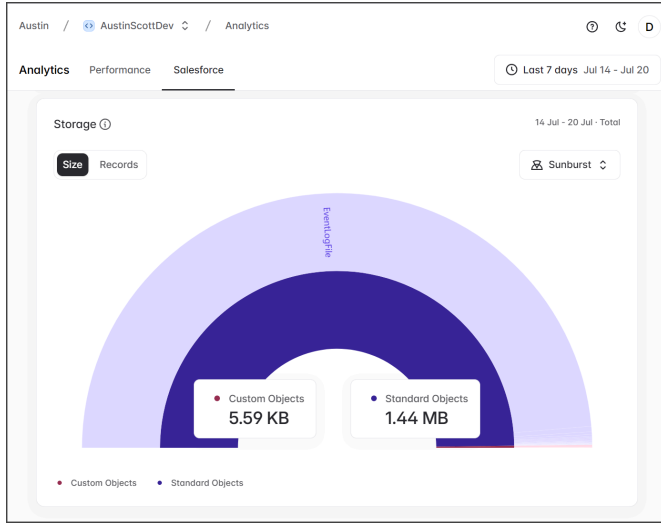
The **Sunburst** chart offers a hierarchical visualization of objects, while the **Treemap** presents a block-style distribution of those objects. The **Treemap** view is handy for identifying the most significant objects in your backup.

Sunburst - Size
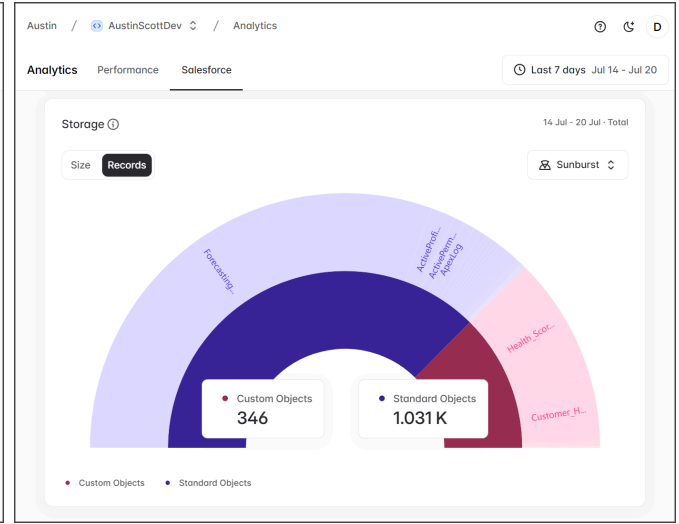
Sunburst - Records

Treemap - Size

Treemap - Records

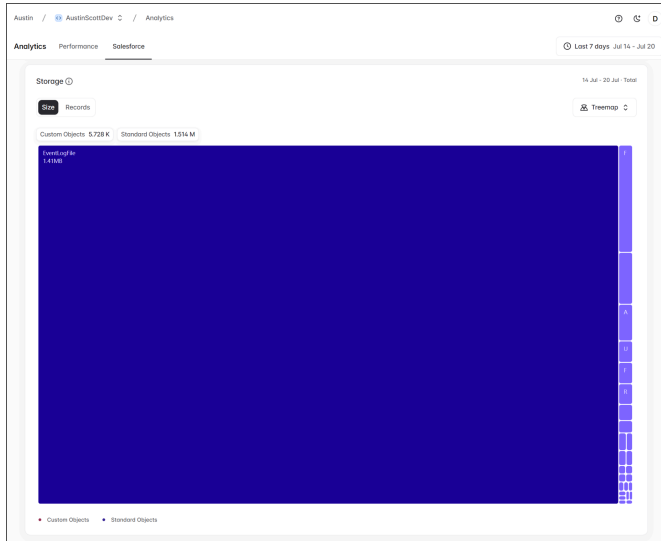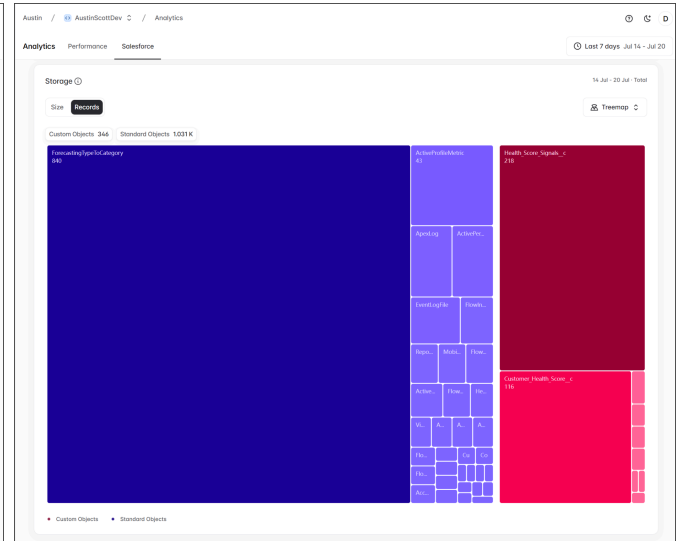## Security Notes

- Data is encrypted at rest with AES-256 using your key.
- Data in transit is protected by TLS 1.2 or higher.
- Encryption key management remains in your control.
- User authentication supports MFA and role-based access.

Summary of Best Practices

- Use Composite Sync Backup to see incremental backups in action.
- Test restores in a sandbox or with a limited data scope before a full restore.
- Enable job notifications for easier monitoring.
- Explore templated backups for efficiency.

References

- [Flosum Backup &Archive Overview](#)
- [Implementation Best Practices](#)
- [AES-256 Key Generation Guide](#)