ANACONDA.

Anaconda Platform Cloud:
Admin Onboarding Guide

ANACONDA.

Table of Contents

ANACONDA.

Introduction

This comprehensive onboarding guide provides **Business tier administrators** with essential knowledge to configure, manage, and secure your organization's **Anaconda Platform Cloud**. It covers key topics, such as enterprise single sign-on (ESSO), user access control, channel and token management, and package governance, to help you enable true “build once, run anywhere” functionality across environments, clouds, and devices.

What You’ll Learn

Through this guide, you’ll learn:

1. **User & Access Management**
    - Configure ESSO for centralized authentication
    - Manage user seats, roles, and permissions
    - Create and manage groups for controlled access
    - Handle user invitations and service accounts (API user onboarding)
2. **Repository & Channel Management**
    - Navigate Anaconda's Premium Repository and default channels
    - Create virtual, external, and private channels
    - Enable and configure the Community Channel (16,000+ open-source packages from conda-forge)
    - Control package access through channel permissions
3. **Security & Compliance**
    - Apply policy filters to enforce vulnerability thresholds [Common Vulnerabilities and Exposures (CVE)-based filtering]
    - Manage policies based on parameters such as license type, platform architecture, and CVE status
    - Track policy changes and receive automated alerts
    - Review package security through CVEs, Anaconda signature, and Software Bill of Materials (SBOMs)
4. **Token & Subscription Management**
    - Activate and manage individual access or site tokens
    - Monitor subscription details and seat utilization
    - Configure secure access to your organization's repository

ANACONDA.

Who This is For

This guide is designed for **system administrators** responsible for configuring and maintaining Anaconda Platform Cloud within their organization. Admin access to Anaconda Platform Cloud is required to follow along.

Notes:

1. Advice for individual Anaconda Platform Cloud users is *not* within the scope of this guide.
2. The contents of this guide are also available as a free self-paced course with **how-to videos**. To access this **Anaconda Platform Cloud: Admin Onboarding** course, log in to Anaconda Learning using your Anaconda credentials.

ANACONDA.

Enterprise Single Sign-on

Streamlining Access Management

Enterprise Single Sign-On (ESSO) integration, available to all our Business tier customers, allows your organization to authenticate users across Anaconda products using your existing internal identity platform. This enterprise-level authentication solution simplifies access management while enhancing security and compliance across your data science and AI development ecosystem.

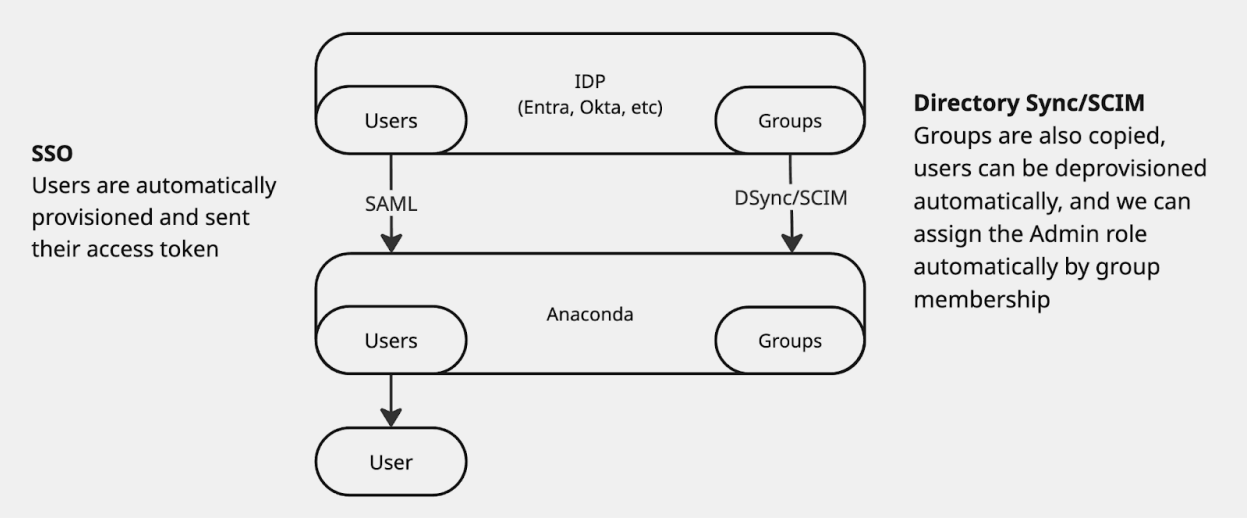
With ESSO, you can authenticate seamlessly across Anaconda endpoints through a single identity provider session, eliminating credential proliferation and reducing attack surface. If you're a system administrator, you gain centralized control over authentication events, ensuring consistent security policies while reducing administrative overhead through automated provisioning workflows.

ESSO helps you, the admin

- Centralize user management through an existing identity provider,
- Enforce IDP security policies including password requirements and MFA across Anaconda products,
- Quickly provision and deprovision user access across Anaconda products in minutes rather than days,
- Maintain detailed audit logs for compliance purposes, simplifying security audits and regulatory reporting, and
- Minimize security vulnerabilities from orphaned accounts with immediate access revocation.

ESSO helps your end users

- Access Anaconda products using their existing corporate credentials,
- Gain secure and consistent access wherever they work from, and
- Reduce context switching between applications, improving their productivity and workflow continuity.



SAML/OpenID Connect Integration

This integration establishes secure connections with major identity providers, allowing your organization to authenticate users through existing identity management systems using the OAuth 2.0 framework and JWT token-based authentication.

Automatic Account Linking

Through automatic account linking, you as the admin can identify and connect existing user accounts to your organization's SSO authentication system when users first authenticate through SSO, preserving account history, permissions, and customizations without requiring manual intervention from IT teams.

Automatic Provisioning

Automatic user provisioning streamlines the onboarding process by creating new user accounts with appropriate baseline permissions during a user's first SSO sign-in attempt, eliminating the traditional multi-step account creation process that typically requires your (i.e., the admin) involvement.

Access Token Generation

Automatically create and securely deliver user access tokens for premium repository channels via email upon successful authentication, giving your

developers immediate access to the resources they need without additional configuration steps.

Rollback Capability

A robust safety mechanism that allows you to quickly revert to standard authentication methods if needed, protecting business continuity by ensuring that authentication issues never block critical workflows.

Setting Up ESSO

Upon request, Anaconda will email a self-service setup link to you or your IT representative. Select either **Configure Single Sign-On** or **Configure Directory Sync**, then follow the prompts for your Identity Provider (IdP) to set up your Anaconda SSO configuration.

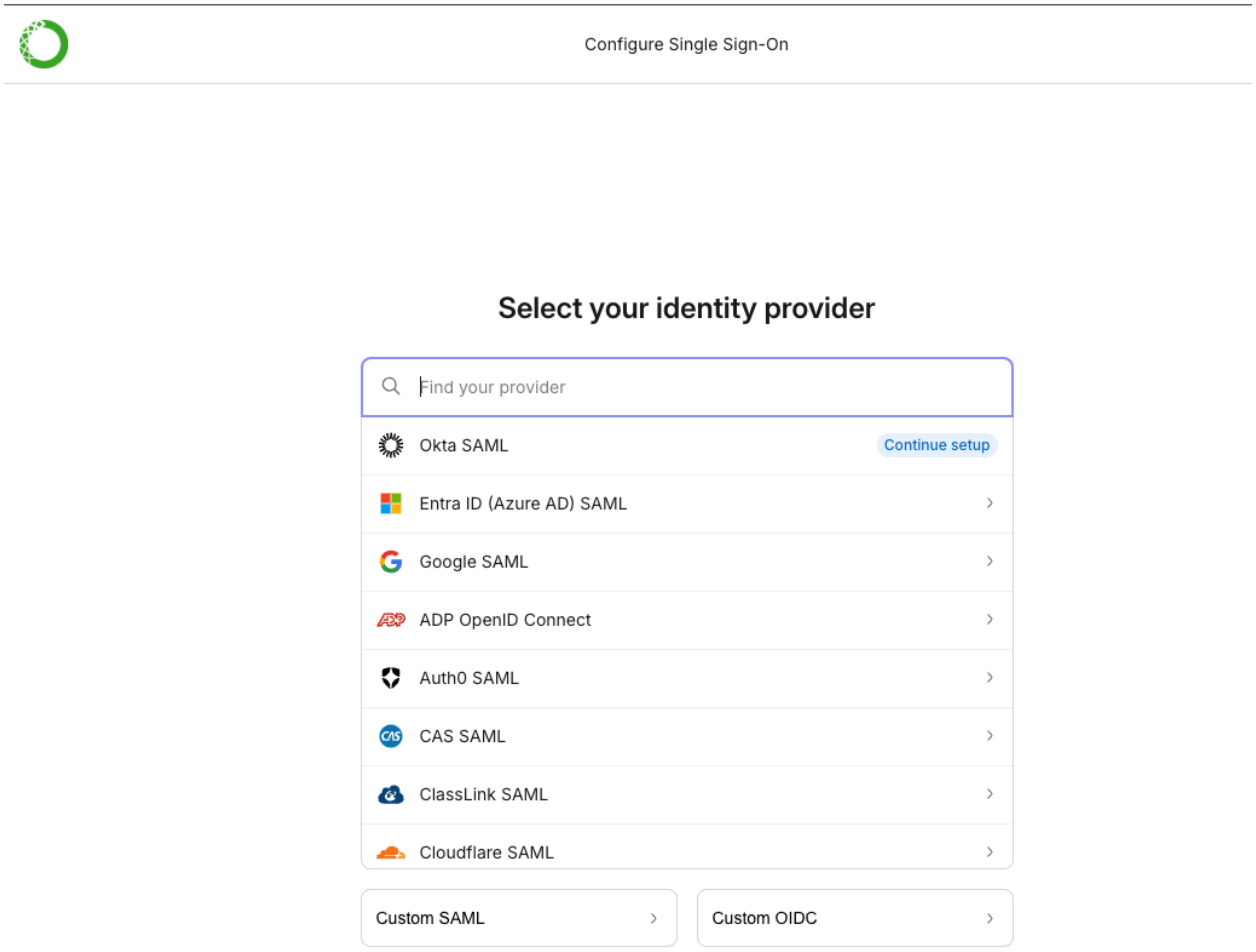
To request a self-service setup link, contact your dedicated Customer Service Manager (CSM) or open a Technical Request support ticket.

Configure Single Sign-on or Configure Directory Sync

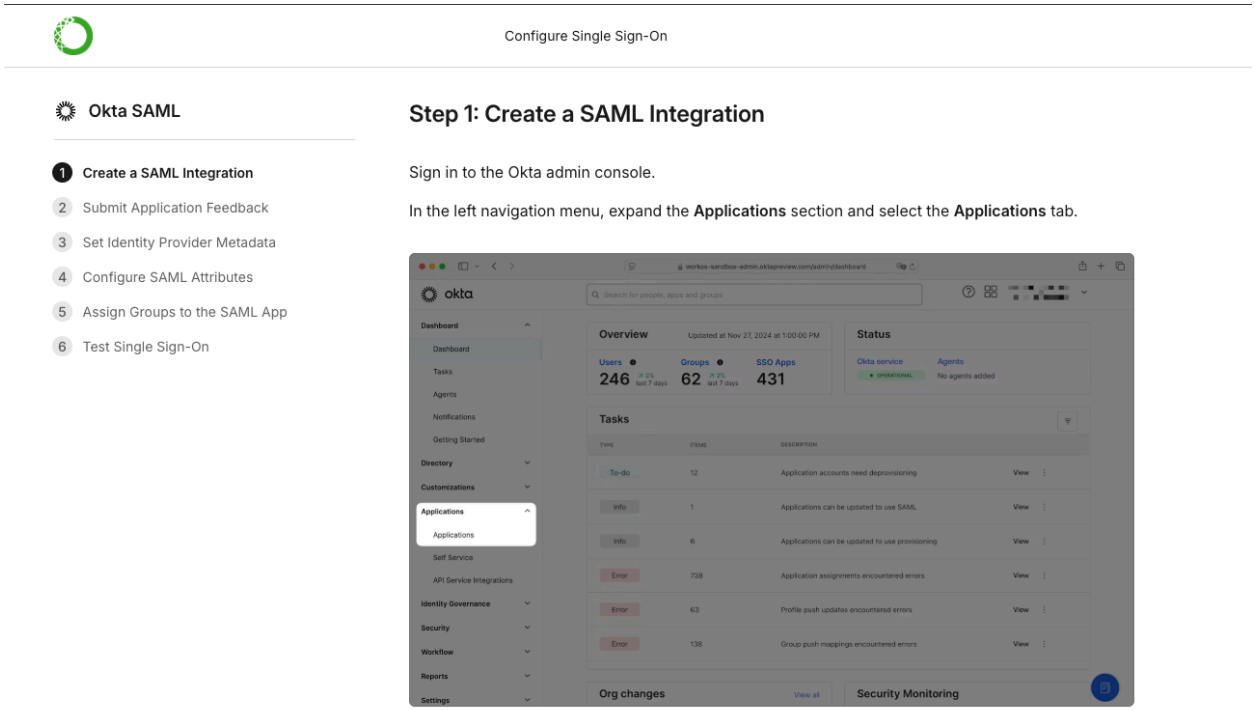
When you receive a self-service setup link from Anaconda, it will guide you through a step-by-step process to configure either SSO or Directory Sync.

After opening the link, you'll arrive at the Set up your Anaconda SSO/SCIM organization page, where you can select between two options: **Configure Single Sign-On** or **Configure Directory Sync**. Select the option that best suits your organization's needs.

Once you've made your selection, you'll be directed to the “Select your identity provider” page, where you can select your IdP. For this example, let’s select **Okta SAML**.



Selecting Okta SAML opens a step-by-step setup guide with detailed documentation and instructions specific to configuring Okta for your organization. The guide includes numbered steps such as "Create a SAML Integration," "Submit Application Feedback," "Set Identity Provider Metadata." Follow each step as instructed to successfully complete your SSO or Directory Sync configuration.



Next Steps

With SSO enabled, employees within your organization with matching domains will be prompted to authenticate via your IdP when signing in to Anaconda. When a user signs in with SSO for the first time, the system will:

- Create their Anaconda account,
- Add them to your organization with baseline permissions,
- Assign them a seat, and
- Send the organization access **token** to their email.

Direct your organization members to follow the instructions in the email to authenticate with Anaconda by setting up their organization access token. For additional details on access tokens, refer to Token Access.

Troubleshooting

If you encounter any issues with your ESSO setup, contact our Anaconda support team:

- support@anaconda.com
- support.anaconda.com
- Technical Support request ticket

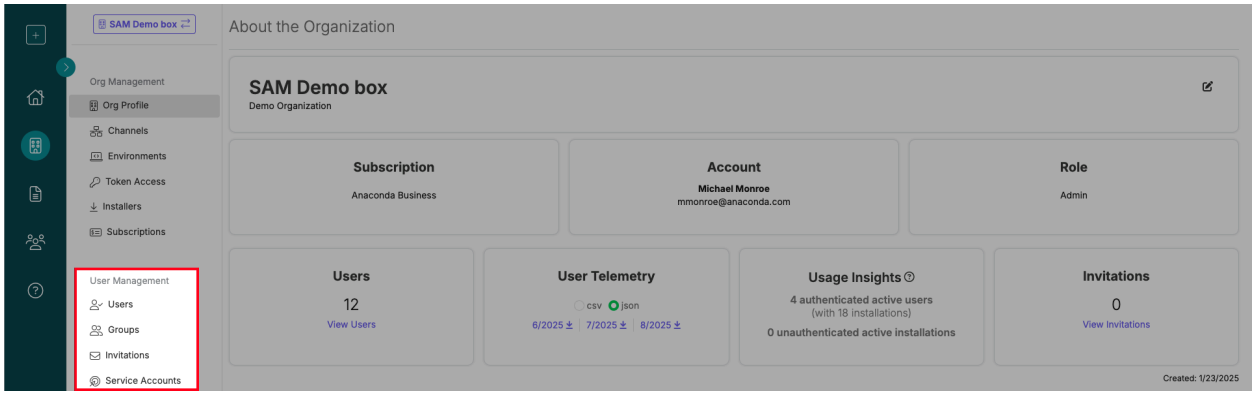
Supported SSO Providers

Provider	SSO Support	Directory Sync Support
ADP	Yes	—
Auth0	Yes	—
CAS	Yes	—
ClassLink	Yes	—
Cloudflare	Yes	—
CyberArk	Yes	Yes
Duo	Yes	—
Entra ID	Yes	Yes
Google Workspace	Yes	Yes
JumpCloud	Yes	Yes
Keycloak	Yes	—
LastPass	Yes	—
Microsoft AD	Yes	—
miniOrange	Yes	—
NetIQ	Yes	—
Okta	Yes	Yes

OneLogin	Yes	Yes
Oracle	Yes	—
PingFederate	Yes	Yes
PingOne	Yes	—
Rippling	Yes	Yes
Salesforce	Yes	—
Shibboleth	Yes	—
SimpleSAMLphp	Yes	—
VMWare	Yes	—
Custom SAML	Yes	—
Custom OIDC	Yes	—
Custom SCIM	—	Yes
Custom SFTP	—	Yes

User Management

As an admin, user management under Anaconda Organizations [to view "My Organizations", sign in to anaconda.com/app. You'll then see your organization(s) in the left panel] involves managing users (i.e., your team), their roles, permissions, and access:



Let's get familiar with the following pages under **User Management**:

- **Users**: Control user license and manage user access to the Anaconda Platform Cloud.
- **Groups**: Create and manage groups within the Anaconda Platform Cloud.
- **Invitations**: Send (and manage) invitations to your users so they can join the Anaconda Platform Cloud.
- **Service Accounts**: API programmatic access through service accounts.

Users Page

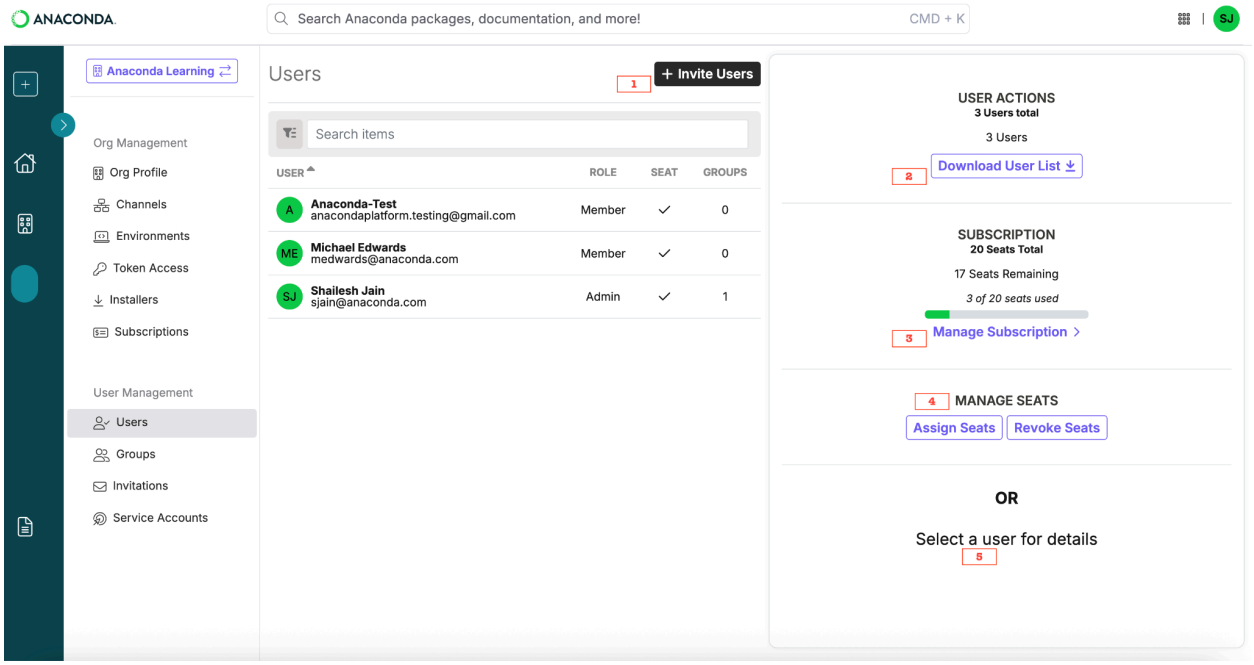
Through the **Users** page, you can manage users (i.e., your team members) and their roles, assign seats*, and control access to the Anaconda Platform Cloud. You can also assign users to groups from this page.

Requirements and Access:

- You must be an admin to access this feature and invite/manage users.
- Access the Users page by navigating to **Org Profile > User Management > Users**

Users Page Capabilities:

1. Invite users (process for inviting users is explained under the Invitations Page section)
2. Download user list
3. Manage subscription (shows details about your subscription, renewal date, and seats)
4. Manage seats (assign or revoke)
5. Manage individual users



*Understanding Seats:

- Each seat represents a license for a user in your organization.
- As evident in the above image, there are a total of 3 users (organization name: Anaconda Learning), including the admin. Of 20 seats, the admin has assigned a seat to 2 users, with 17 seats remaining available for others.
- When you assign a seat to a user, they gain access to the Anaconda Platform Cloud and receive authentication tokens to access your organization's Anaconda Premium Repository.
- Note that users without an assigned seat won't be able to access the Anaconda Platform Cloud.

Download User List

To download a list of all users in your organization

1. Navigate to **Org Profile** > **User Management** > **Users**. On the Users page, select **Download User List.**
2. A CSV file will subsequently get downloaded containing the following information for each user:
    - User's first and last name
    - Email address
    - User type (i.e., their assigned role: Member, Admin, or Billing Manager)
    - Subscriptions (indicates if they have been assigned a seat)

You may use this exported CSV file for record-keeping, auditing, or managing users outside of the platform.

Example User List

User name	Email	User type	Subscriptions
		admin	security_subscription
		admin	security_subscription
		admin	security_subscription
		member	security_subscription
		member	
		admin	
		admin	security_subscription
		admin	security_subscription
		admin	security_subscription
		admin	security_subscription
Test1 Test1	ztest1001@yopmail.com	member	

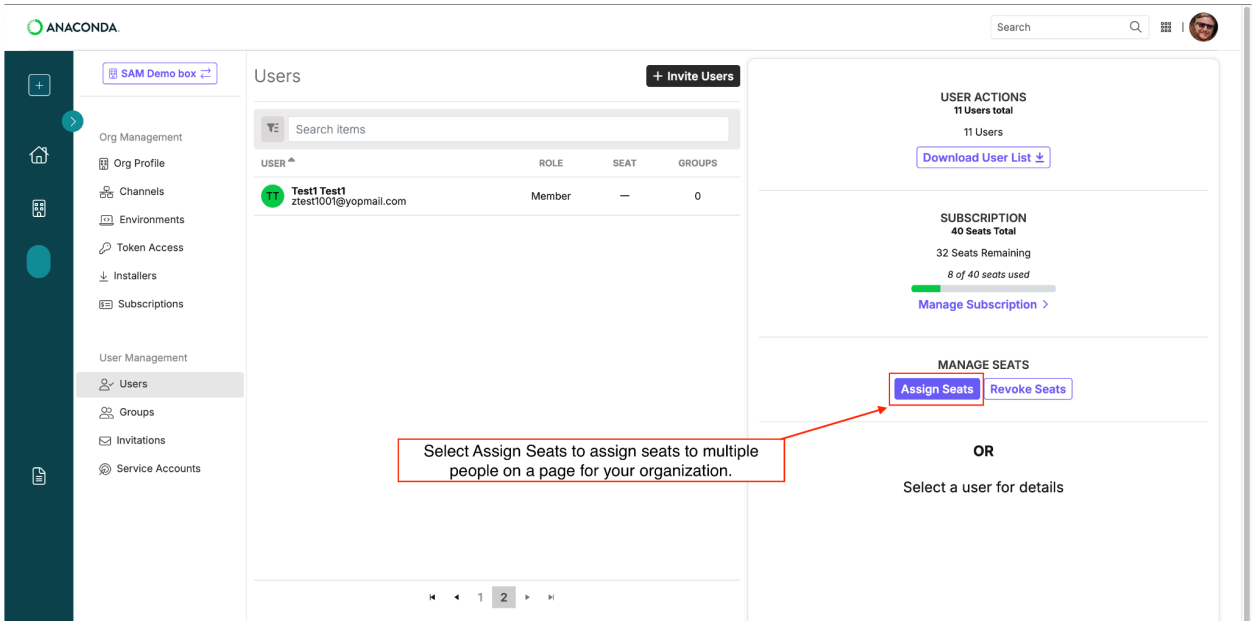
Manage Seats: Assign or Revoke

Lets learn how to assign or revoke seats for multiple users simultaneously.

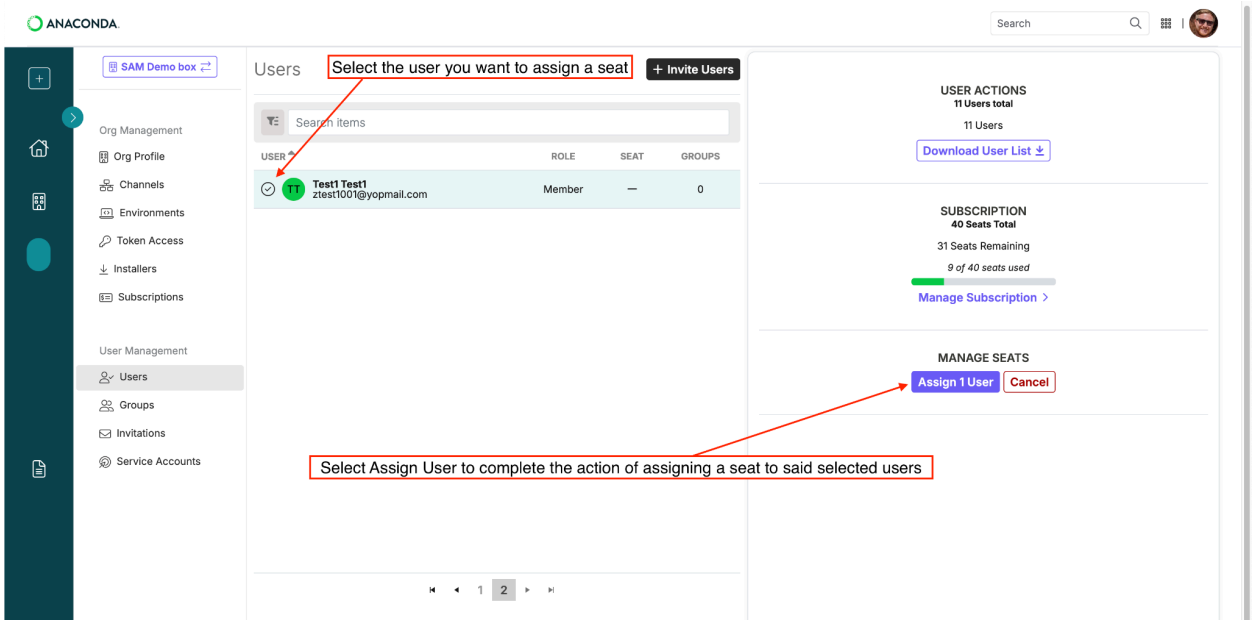
Assign Seats

On the Users page

1. Under **Manage Seats**, select **Assign Seats**.



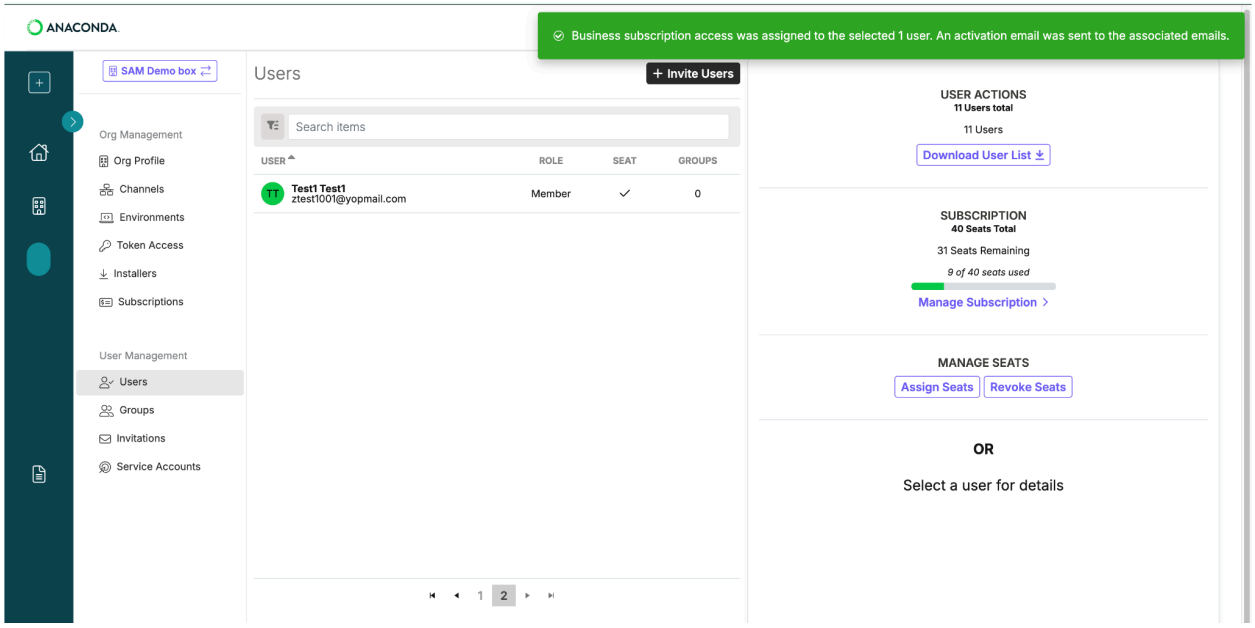
2. Now select the users you want to assign a seat to.
3. Select **Assign X User(s)** (X represents the number of users you are assigning seats to).



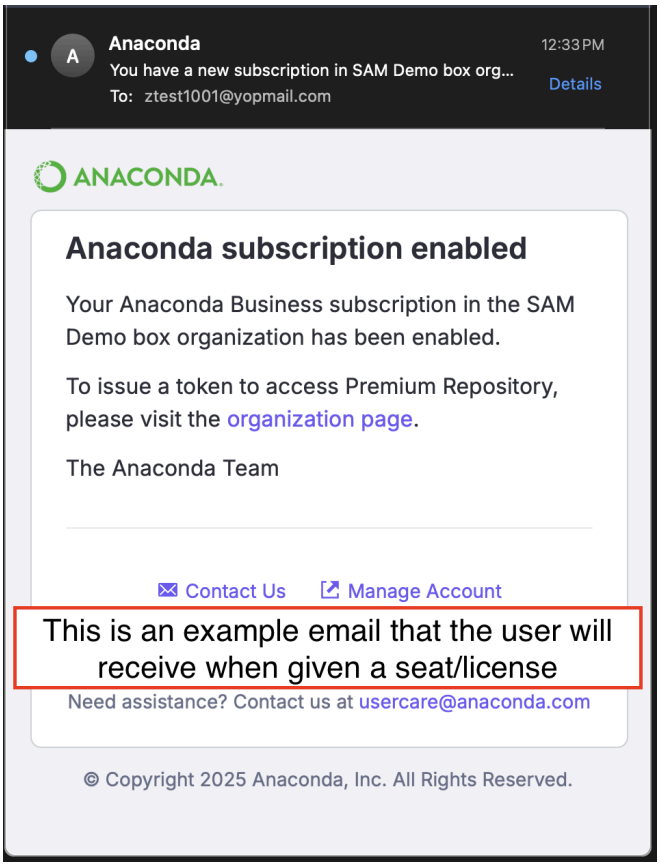
4. Confirm your action by selecting **Assign** in the “Assign Users?” pop-up.

What happens next:

- A confirmation banner appears in the top right corner.



- A check mark appears in the Seat column for each assigned user.
- Each user receives an email notification about their subscription change.



Revoke Seats

On the Users page

1. Under **Manage Seats**, select **Revoke Seats**.
2. Next, select the users whose seats/licenses you wish to revoke.
3. Select **Revoke X User(s)** (X represents the number of users whose seats are being revoked).
4. Confirm your action by selecting **Revoke** in the “Revoke Users?” pop-up.

What happens next:

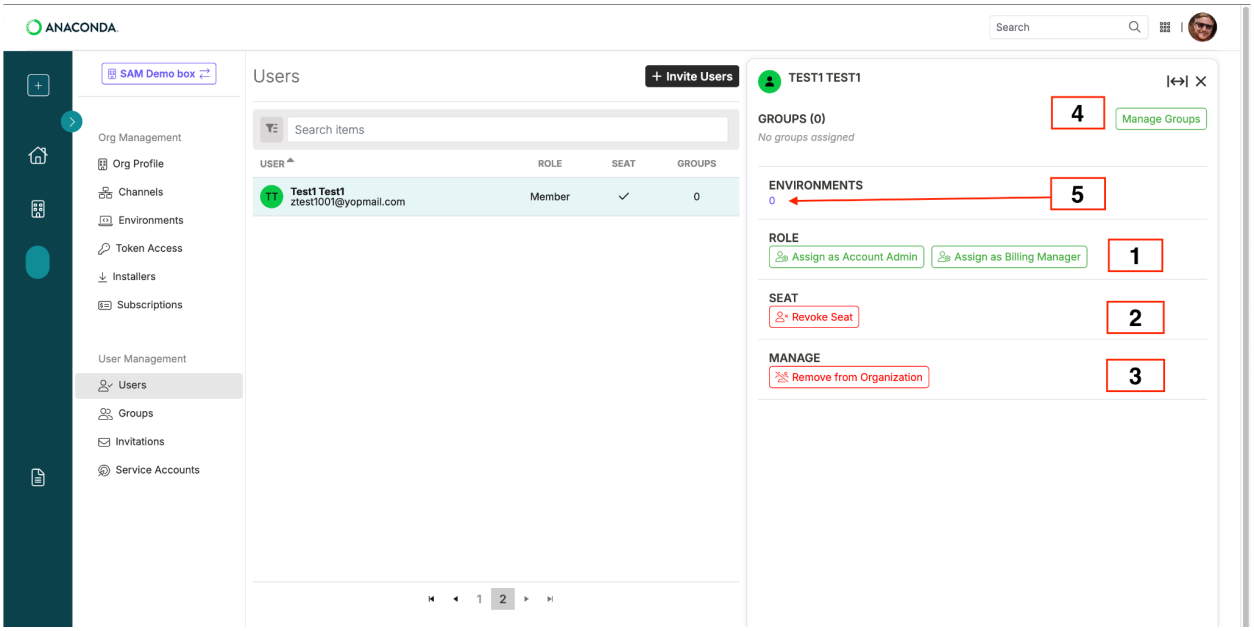
- A confirmation banner appears in the top right corner.
- The check mark appearing on seat assignment now disappears.

Manage Individual Users

On the Users page, you can manage individual users to modify their roles, assign or revoke seats, assign them to groups, check their logged environments, or remove them from the organization altogether.

To manage individual users, select a user to access the management panel with the following options:

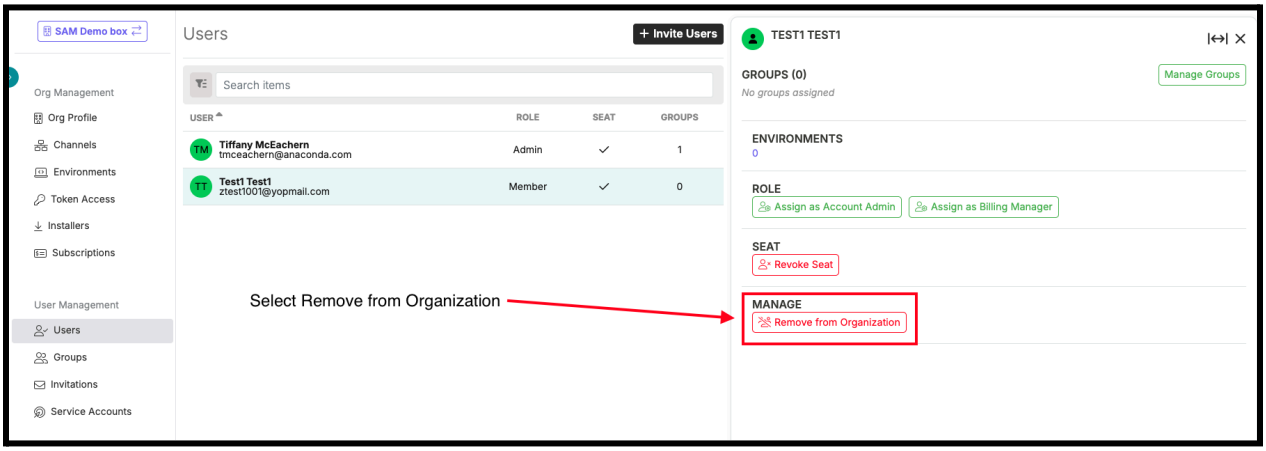
1. **Role**: Assign roles to users in your organization. You can assign one of three roles:
    - **Member** is the default role assigned to a user. Members have the least privileges and access.
    - **Admins** have the highest access control, with access to User Management and Channels. Admins can also apply policies to channels and assign seats/licenses to users. This role has access to all the same resources as a Member and Billing Manager.
    - **Billing Manager** can update billing and subscription information. They can also view the user count under User Management, but they cannot change user information.
2. **Seat**: Revoke or assign a seat to an individual user.
3. **Manage**: Remove a user from your organization. This will revoke the user's seat and permanently remove them.
4. **Manage Groups**: If you have created a group, you can assign users to a group and manage them. You can also view the groups assigned to an individual user.
5. **Environments**: The total number of environments the user has logged into is shown here. Selecting the number under Environments will take you to the Environments page, where you'll see a list of that user's environments.



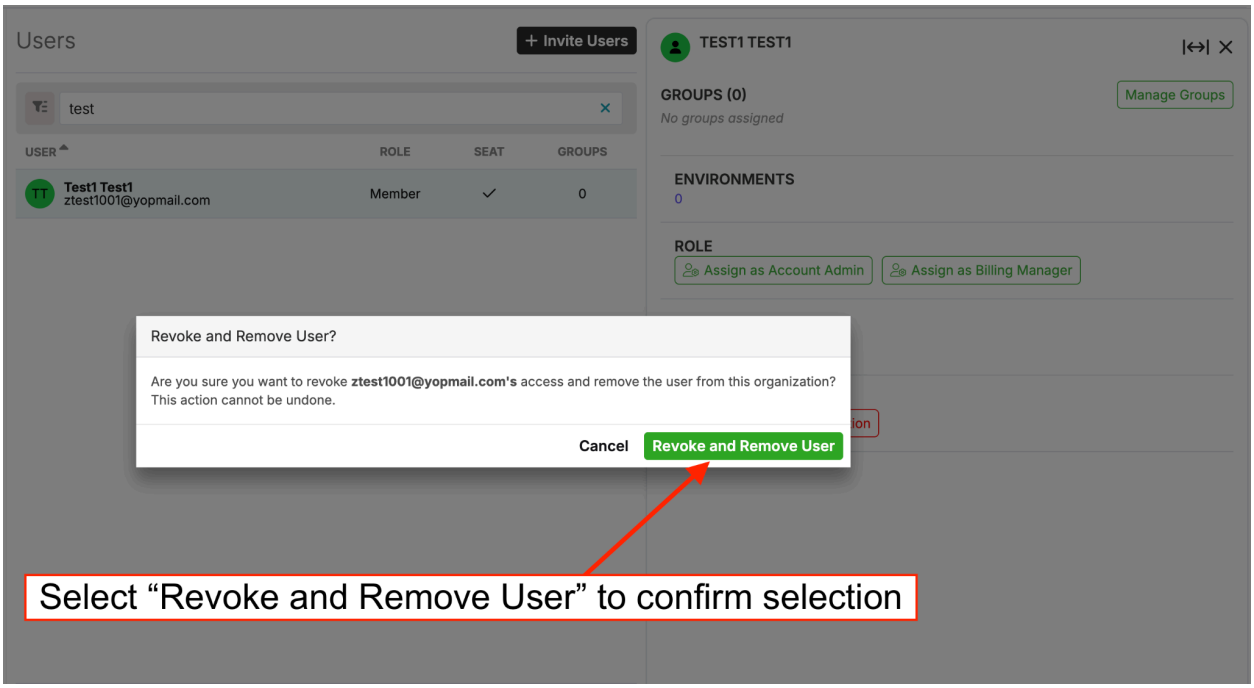
Remove a User

To remove a user for your organization

1. Navigate to **Org Profile** > **User Management** > **Users**. On the Users page, select the user you wish to remove.
2. In the user-specific management panel on the right, under Manage, select **Remove from Organization**.



3. In the Revoke and Remove User? pop-up, select **Revoke and Remove User** to confirm your action.



Note that this action will permanently remove the user from your organization and revoke their seat/license.

Groups Page

Groups are **access management** tools that control which organization members can view specific channels. For example, when you create a private channel and assign a group to it, only users within that group can access the private content.

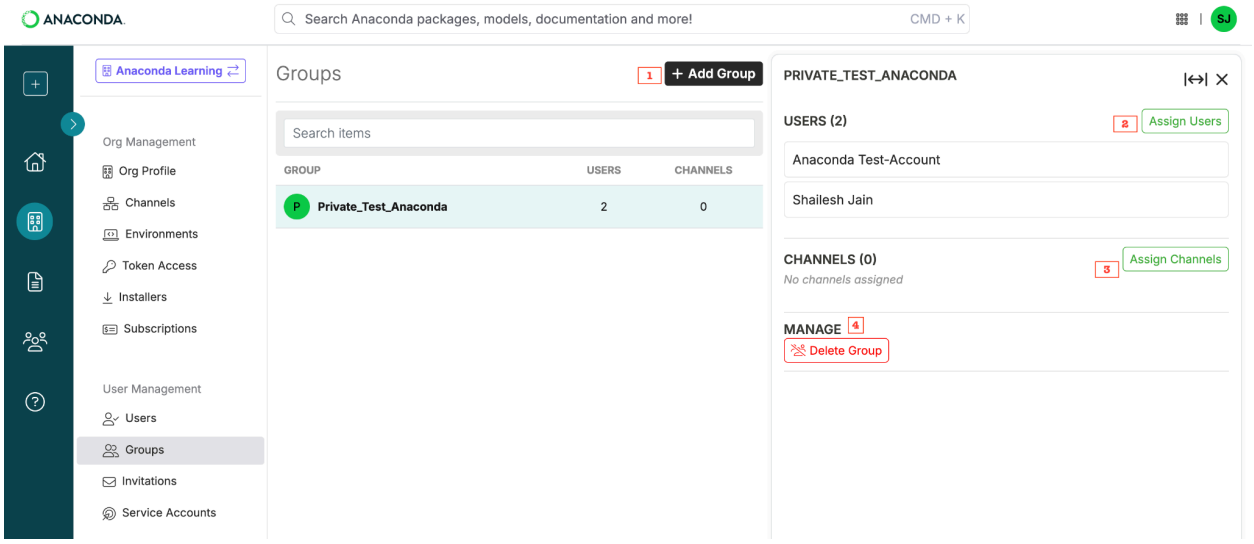
Requirements and Access:

- You must be an admin to access the Groups feature.
- Access the Groups page by navigating to **Org Profile** > **User Management** > **Groups**.

Groups Page Capabilities:

1. Add a group
2. Assign (or remove) users from the selected group and view current group members
3. Assign (or remove) private channels from the selected group

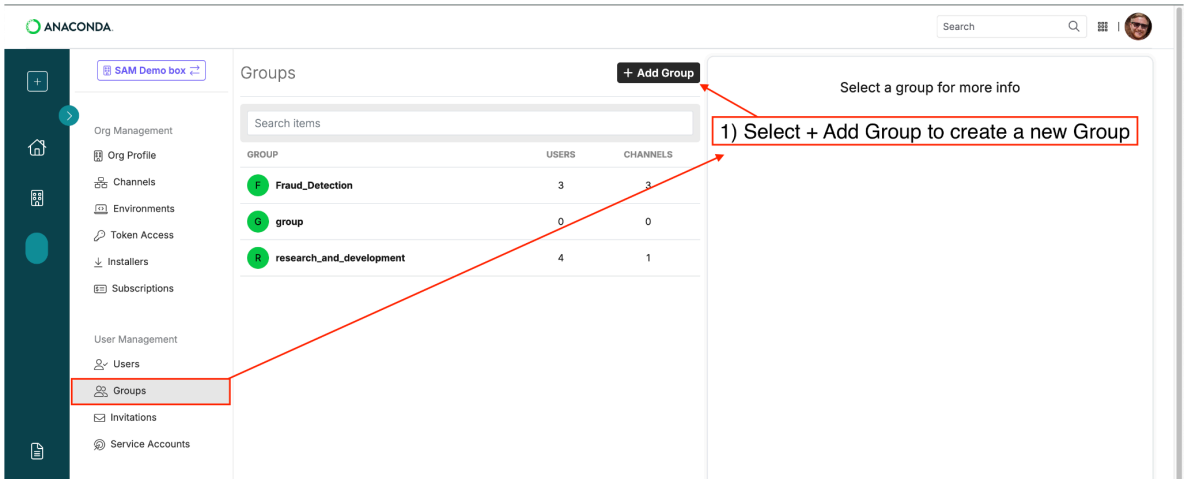
4. Delete groups



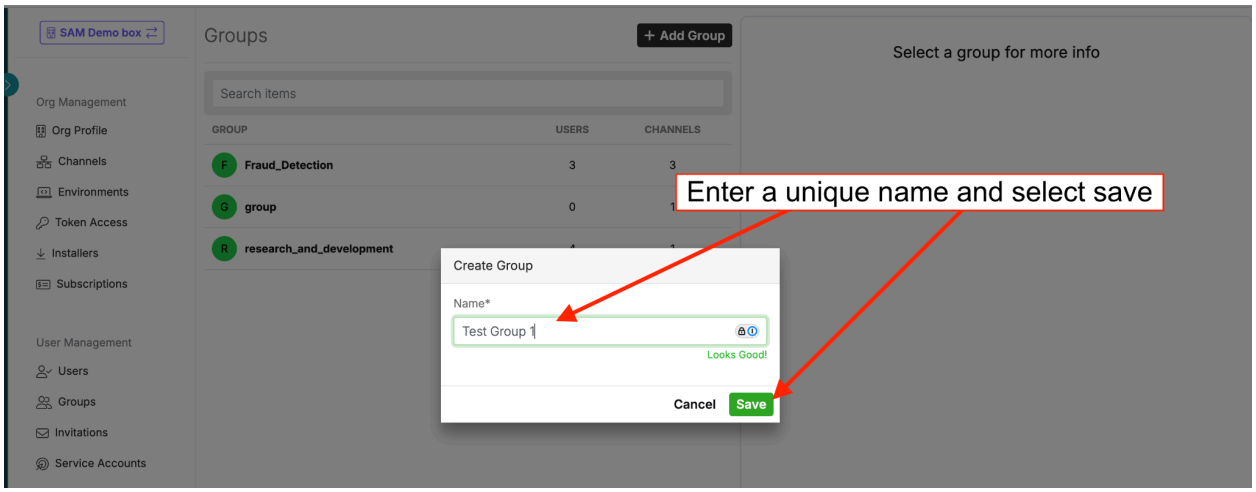
Add a Group

To add a new group

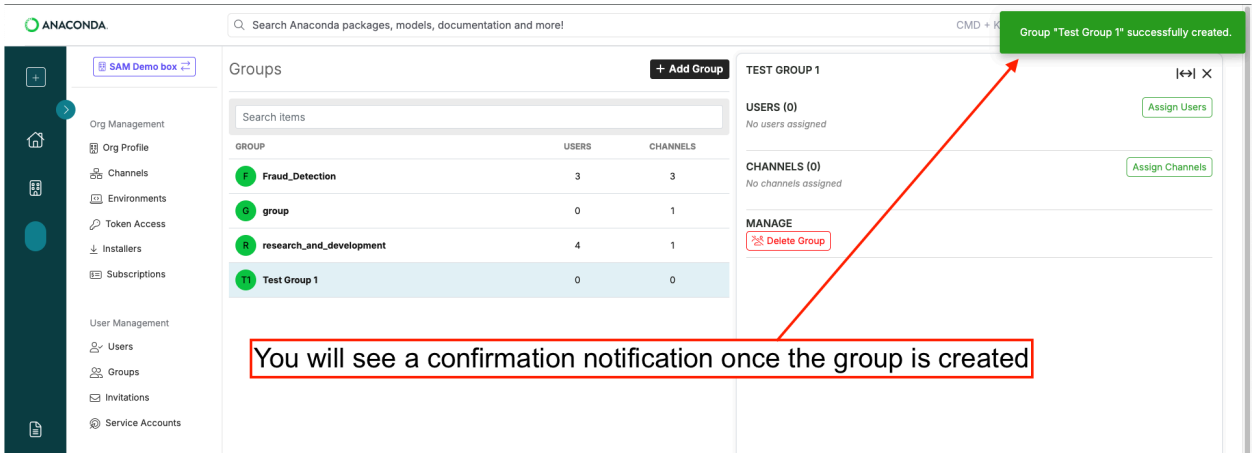
1. Navigate to **Org Profile** > **User Management** > **Groups**. On the **Groups** page, select **+ Add Group**.



2. Enter a unique name for your group and select **Save**.



3. A notification will appear to confirm that your group was successfully created. The new group will appear in the **Group** list, along with the number of users and channels it contains.

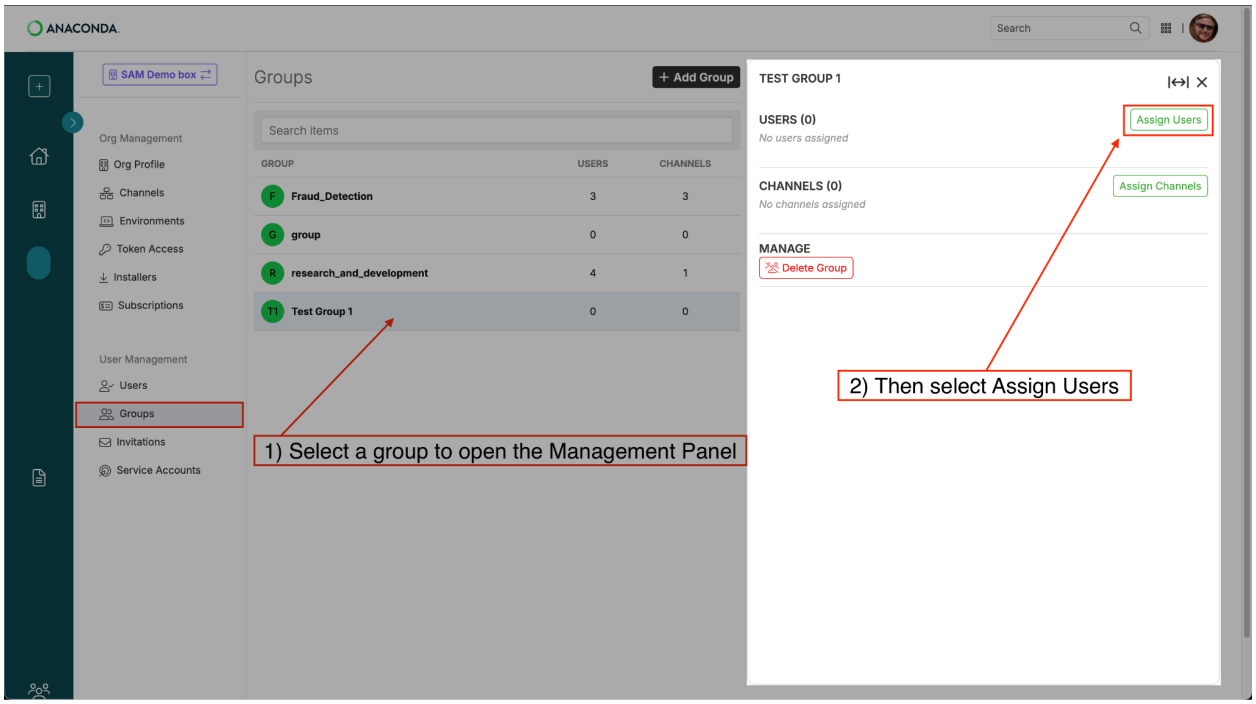


Assign Users To Groups

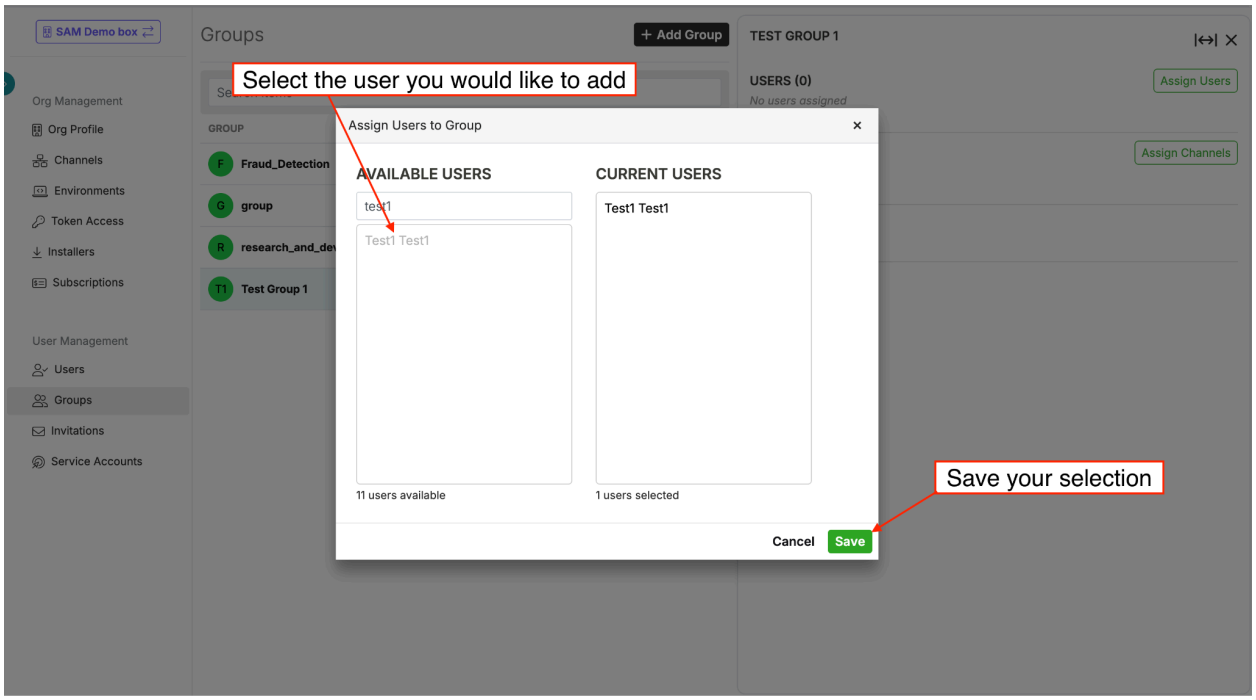
There are two ways in which you can assign users to groups:

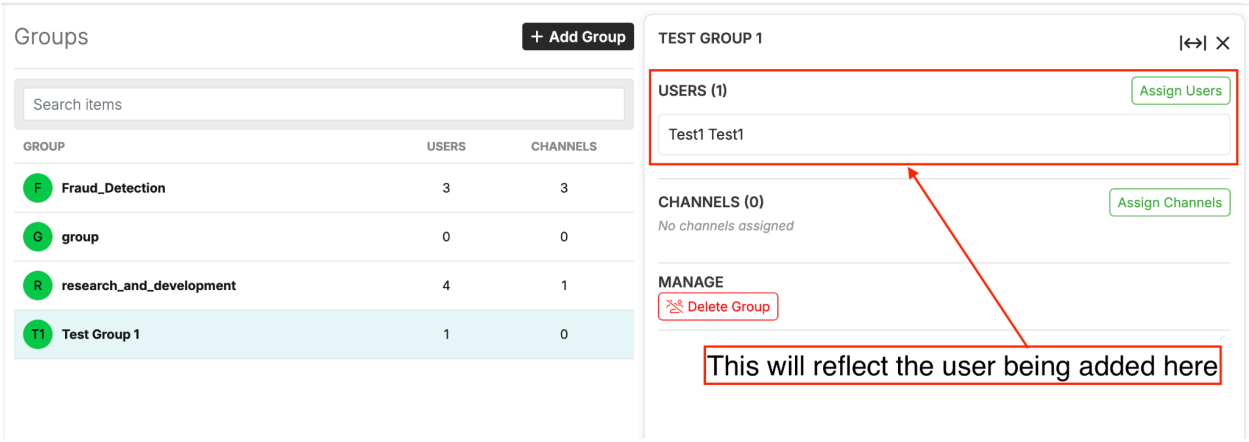
Method 1: From the Groups Page

1. On the Groups page, select a group to open its management panel.
2. In this panel, select **Assign Users**.



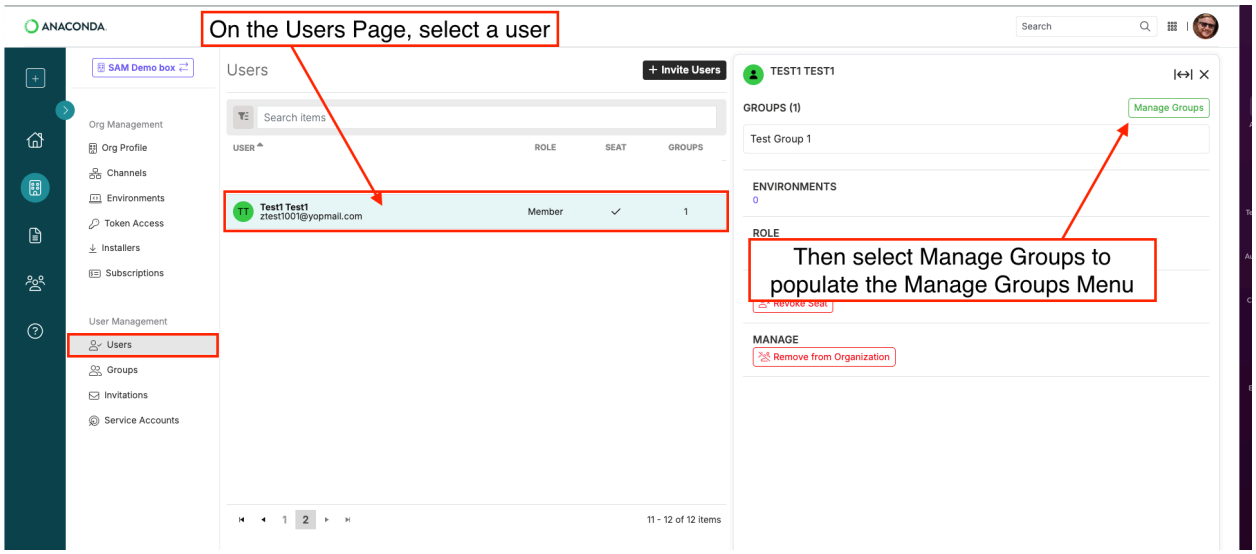
3. A pop-up called **Assign Users to Group** will appear.
4. Select the user(s) you wish to add to this group and then select **Save**. This will add the user(s) to the group, and they'll receive a notification email from Anaconda.



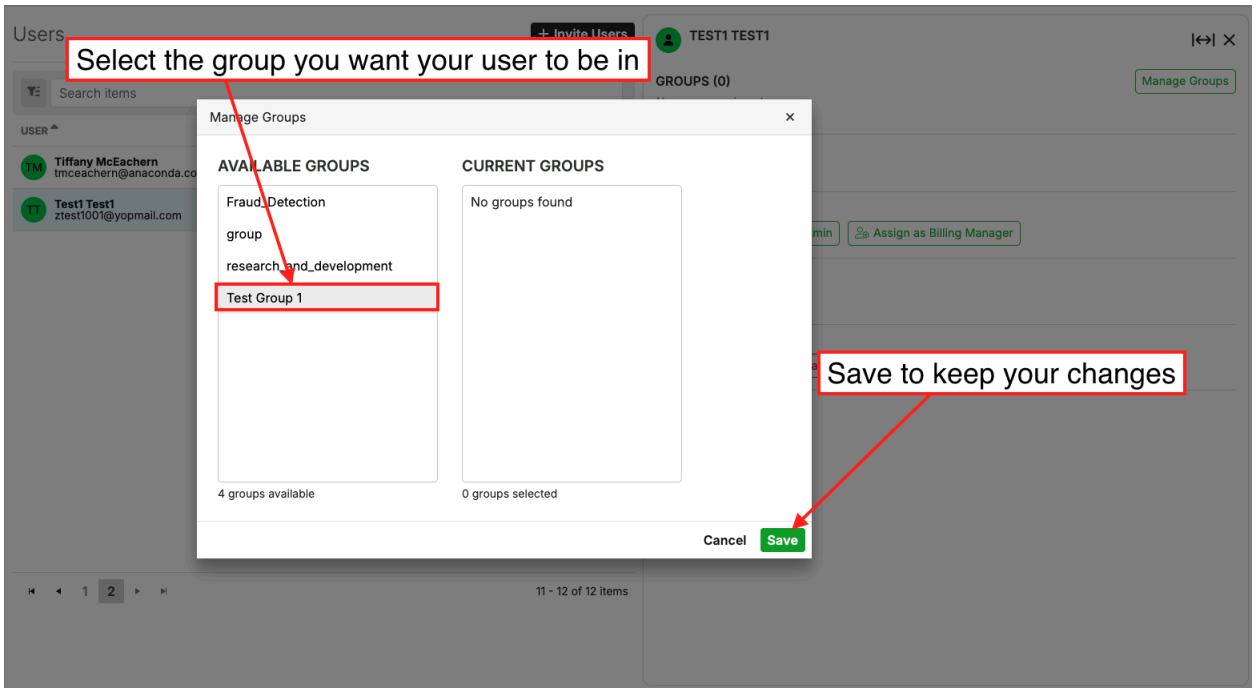


Method 2: From the Users Page

1. On the Users page, select a user you would like to manage.
2. In this user-specific management panel on the right, select **Manage Groups**.



3. A pop-up called **Manage Groups** will appear. Use this pop-up to add this particular user to one or more groups.
4. Select a group from **Available Groups** to assign this user to the selected group, and then select **Save**. This will add the user to the group(s), and they'll receive a notification email from Anaconda.

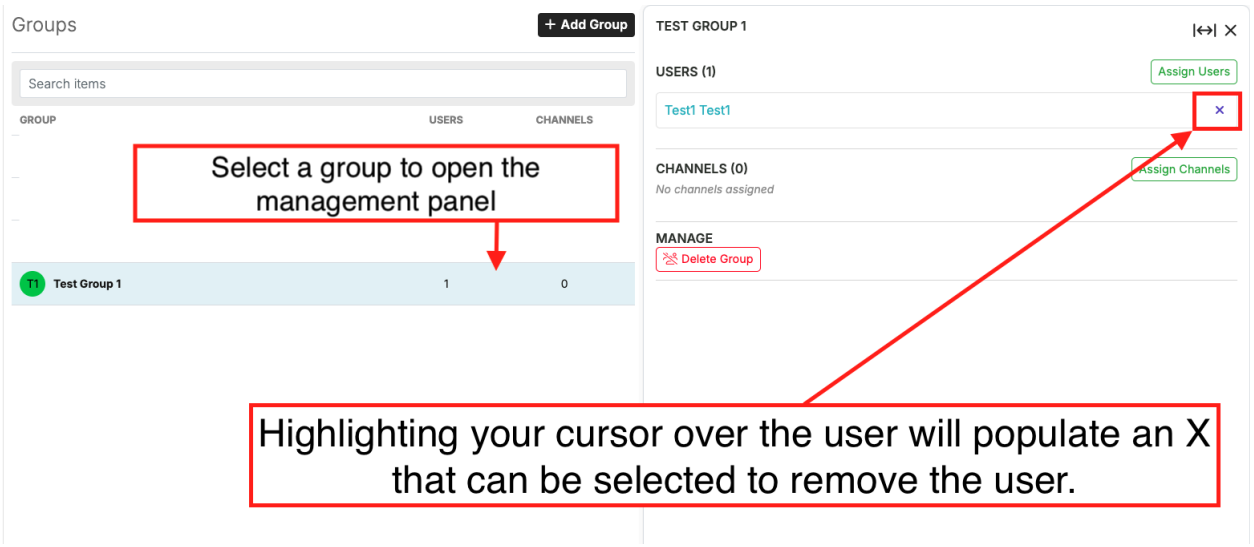


Remove Users from Groups

You can remove users from groups using one of the following three methods:

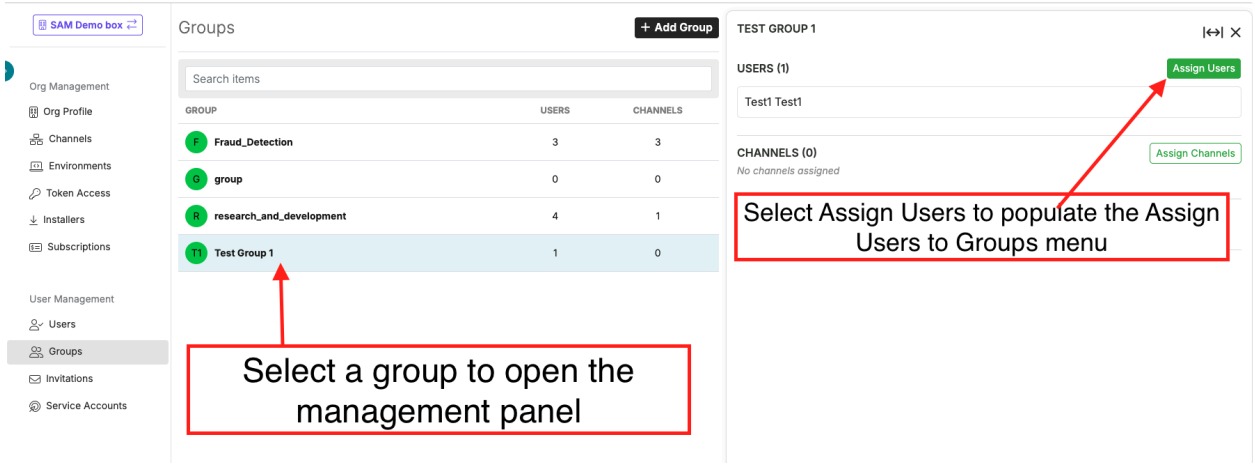
Method 1: Direct Removal from the Groups Page

1. On the Groups page, select a group to open the management panel.
2. Hover over the user and see an **X** icon appear.
3. Select this icon to remove the user from the group.



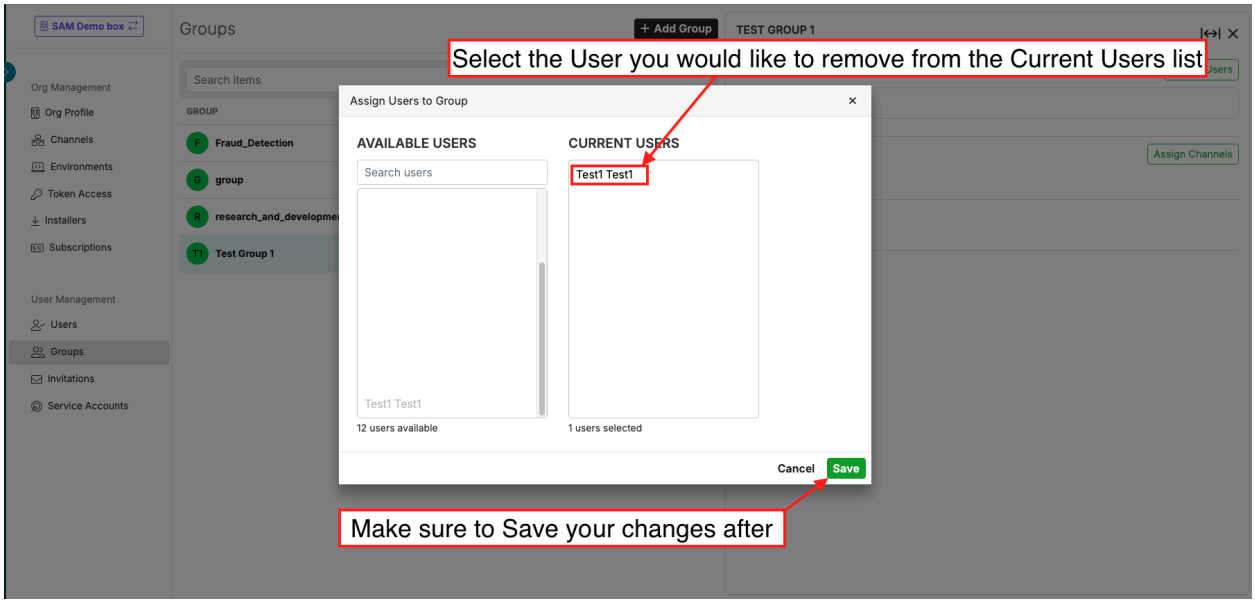
Method 2: "Assign Users" from the Groups Page

1. On the Groups page, select the group to open the management panel.
2. Select **Assign Users**.



3. The **Assign Users to Group** pop-up will appear.

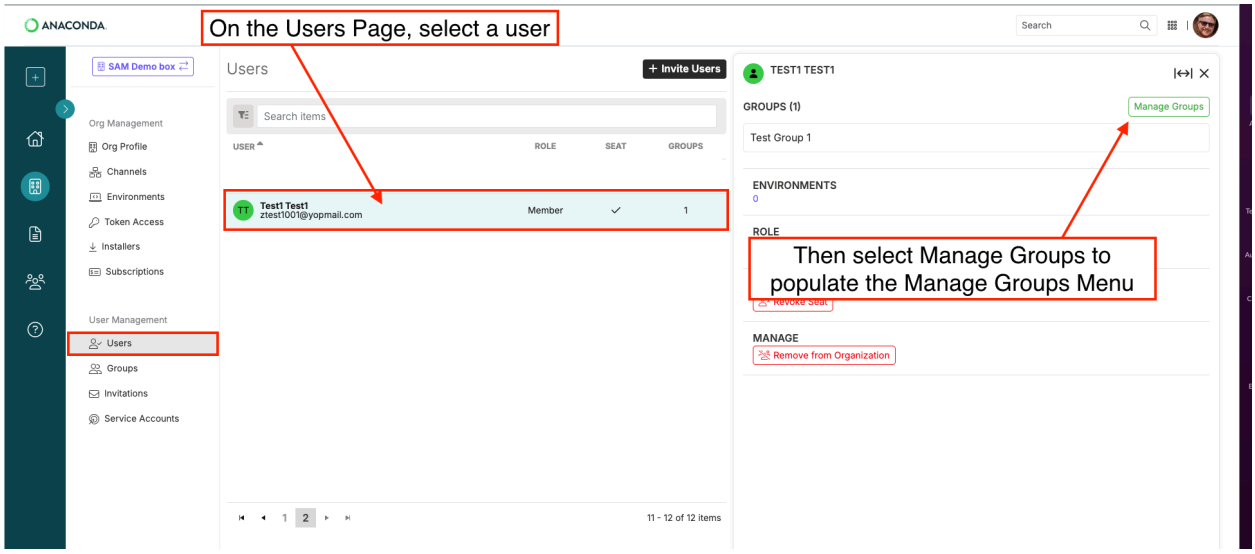
4. Deselect users from the **Current Users** list to unassign them.



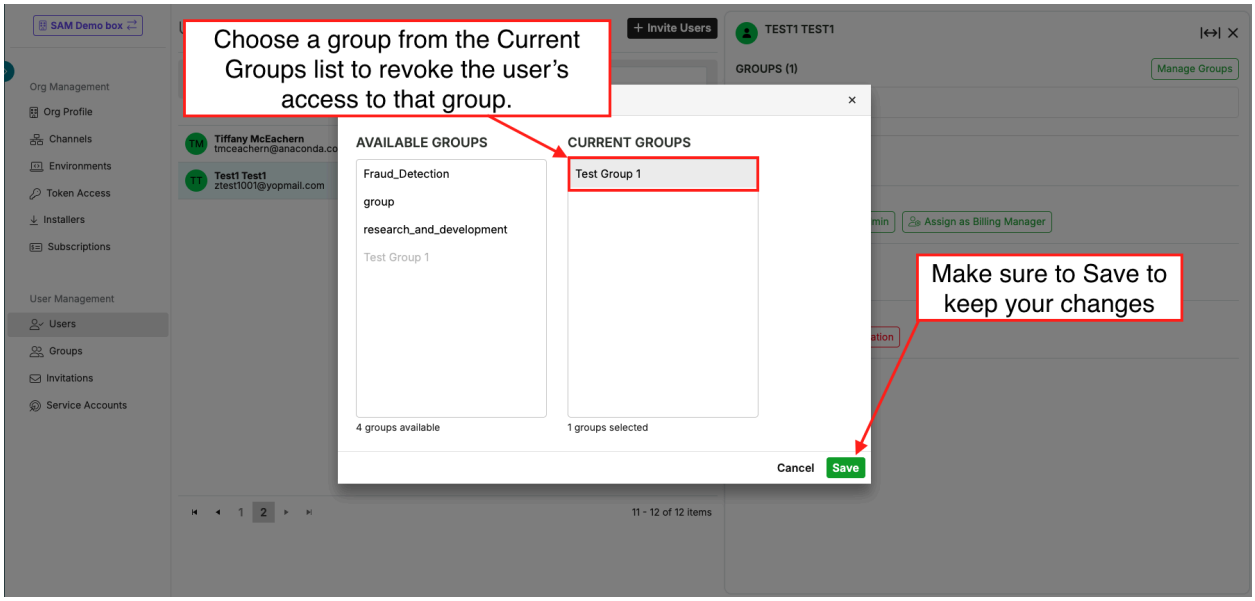
5. Select **Save** to confirm your changes.

Method 3: "Manage Groups" from the Users Page

1. On the Users page, select the user you wish to manage.
2. Select **Manage Groups** to open the Manage Groups pop-up.



3. In this pop-up, deselect groups from the **Current Groups** list to remove the user from those groups.



4. Select **Save**.

On removing users from groups, they will receive a notification email from Anaconda, informing them of this change.

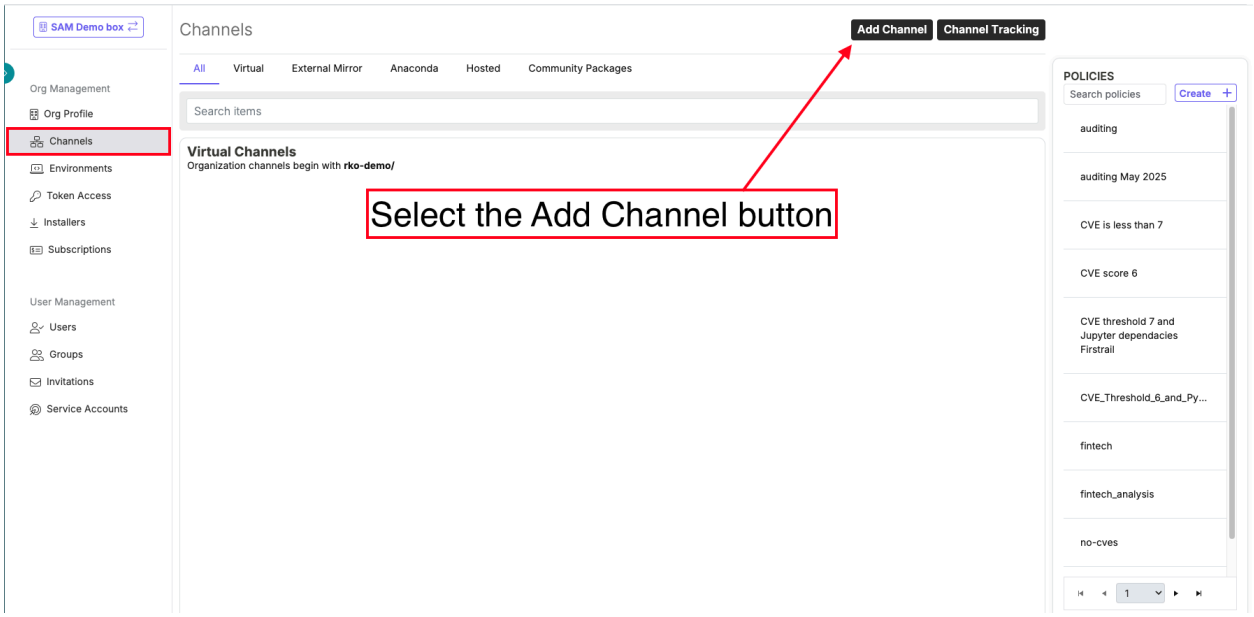
Assign a Private Channel to a Group

Private channels restrict content to users who belong to the assigned group(s). Multiple groups can be assigned to a single private channel. We'll learn more about private channels later in this course.

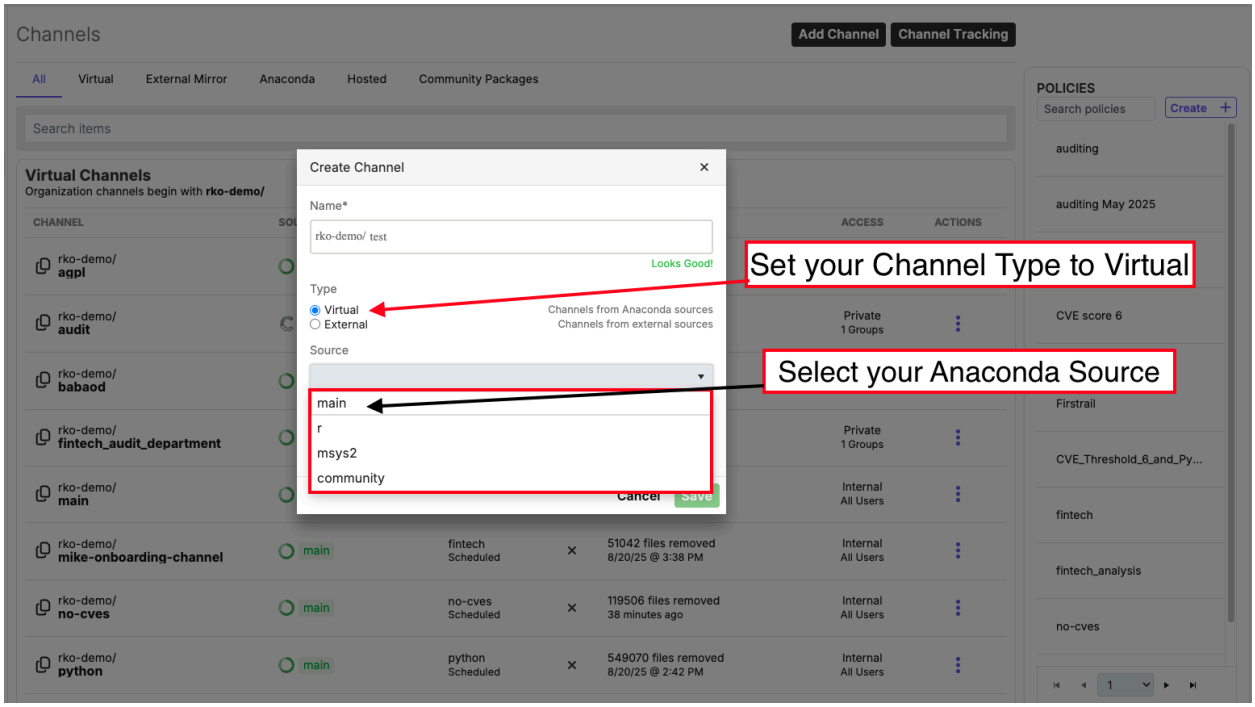
Create a New Private Channel and Assign a Group

1. Navigate to the **Channels** page.

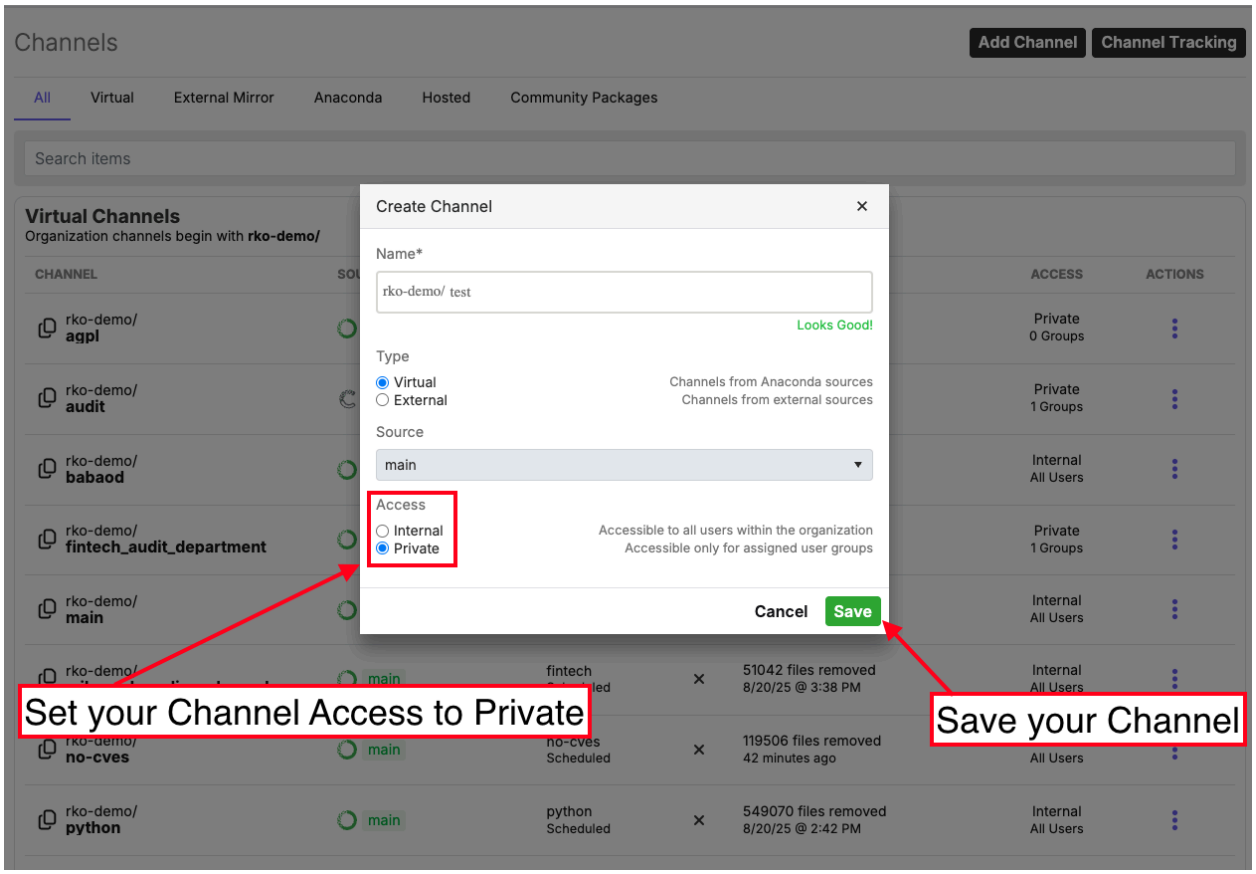
2. Select **Add Channel** to open the Create Channel pop-up.



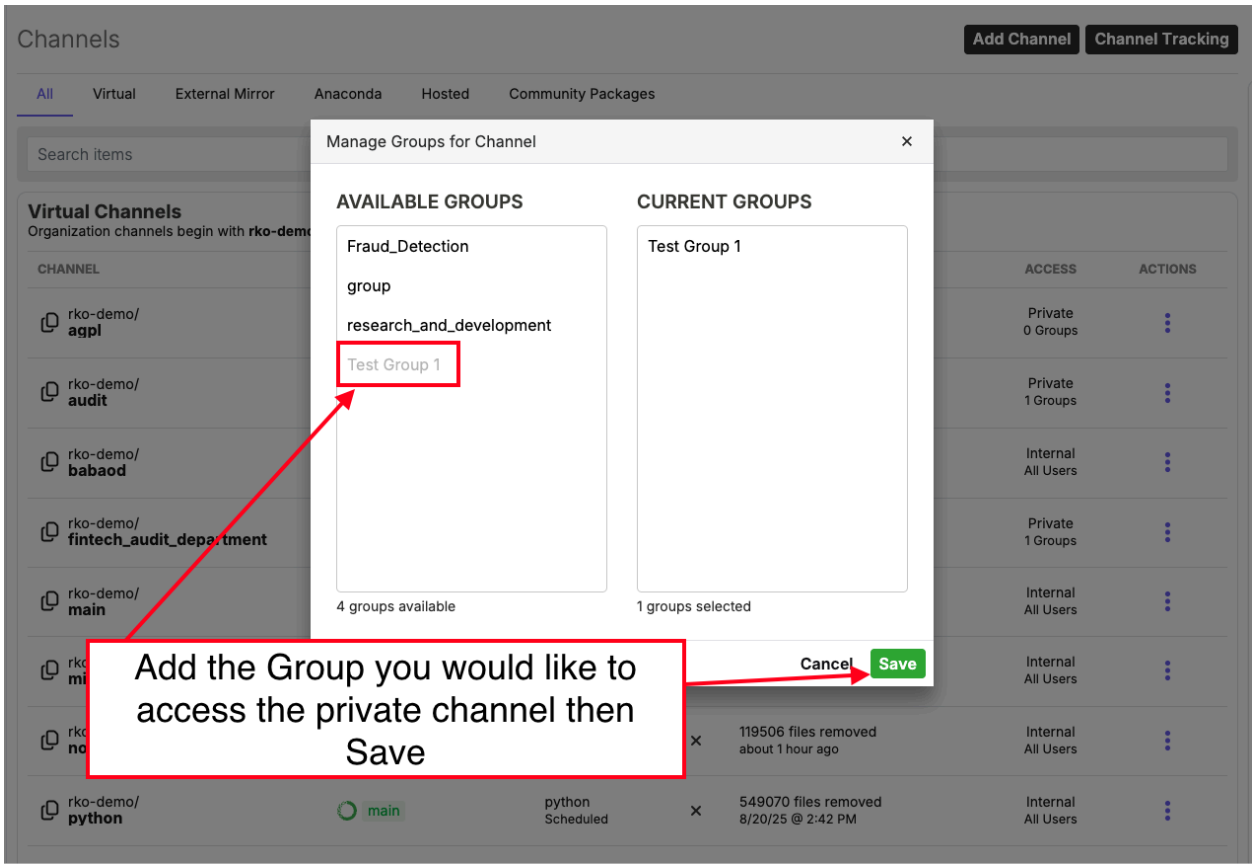
3. Enter a unique name.
4. Select **Virtual** as your channel type to mirror from Anaconda sources (main, r, msys2, community).
5. Select the **Source** dropdown menu.



6. Set **Access** to **Private** to make the channel private.



7. Select **Save** to create this virtual private channel.
8. A **Manage Groups for Channel** pop-up will appear.
9. Select a group from the **Available Groups** list that you would like to assign to the private channel.



10. Select **Save** to confirm your action.

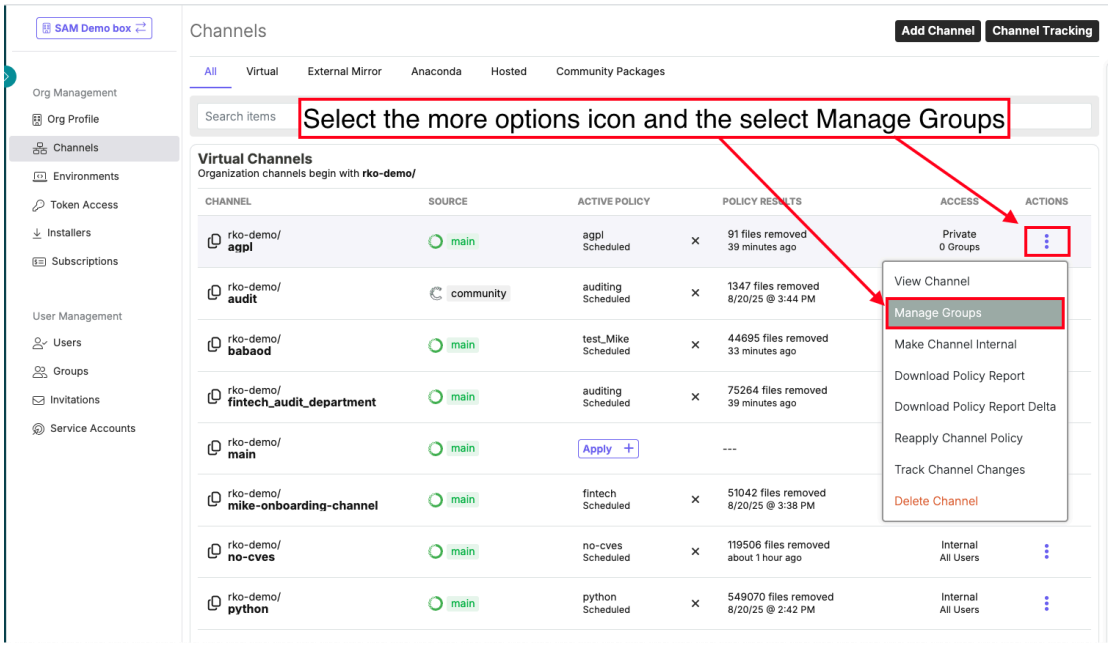
Manage Groups for Existing Private Channels

If you have a private channel already created and need to manage the groups for the channel, you can do this from either the **Channels** page or **Groups** page.

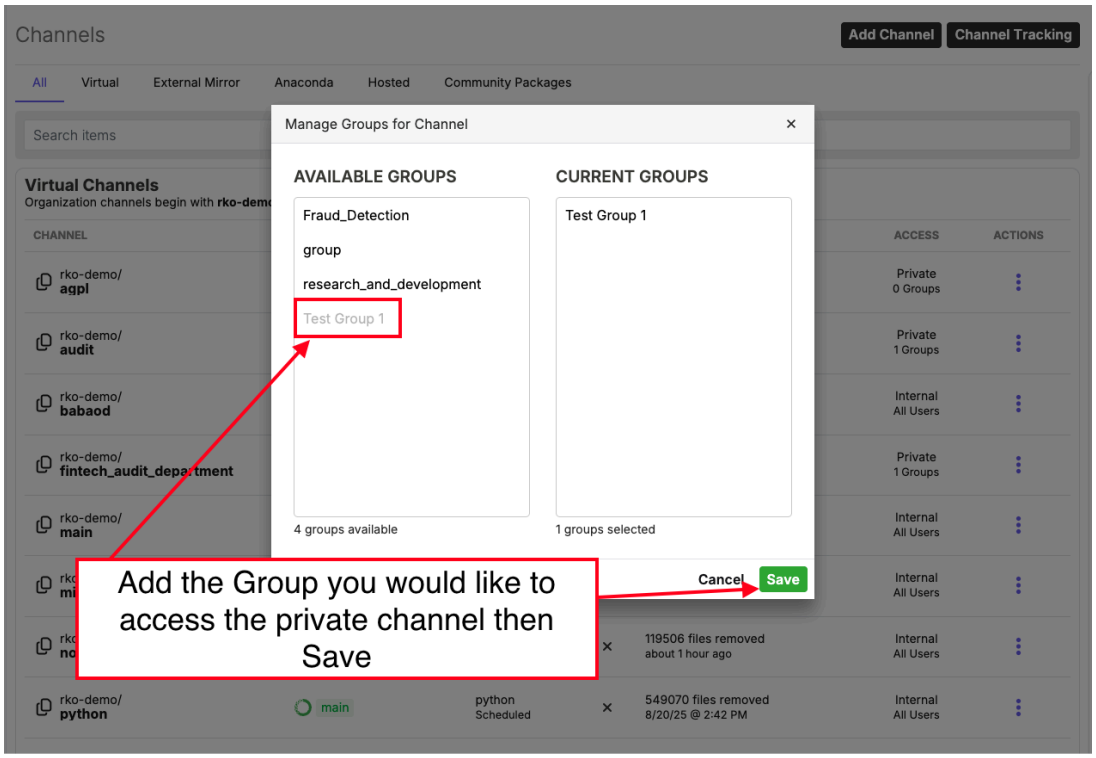
Method 1: From the Channels Page

1. Select the more options icon (⋮) under the Actions column for the channel.

2. A dropdown menu will appear. Select **Manage Groups**.



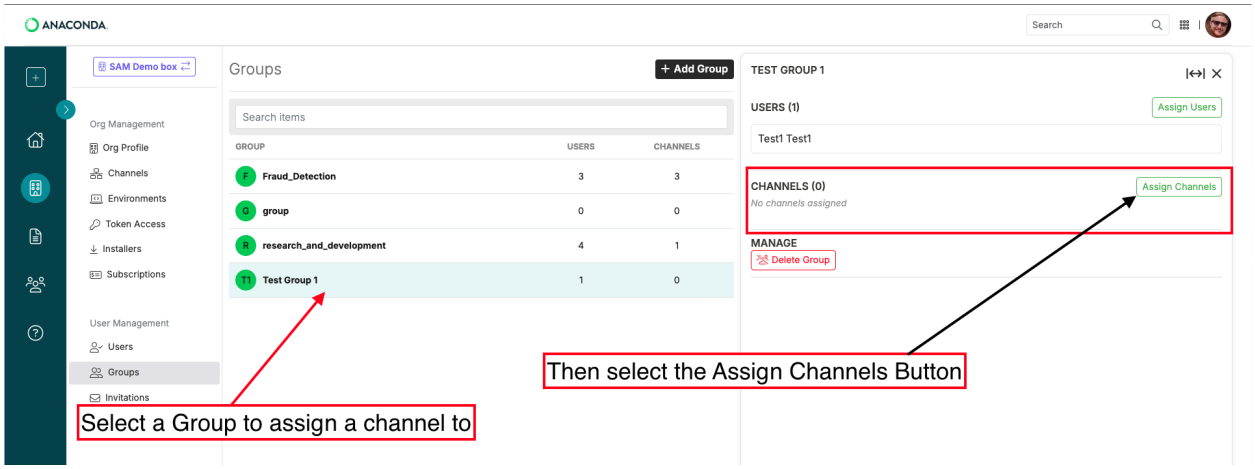
3. Select the groups you wish to add or remove to this private channel.



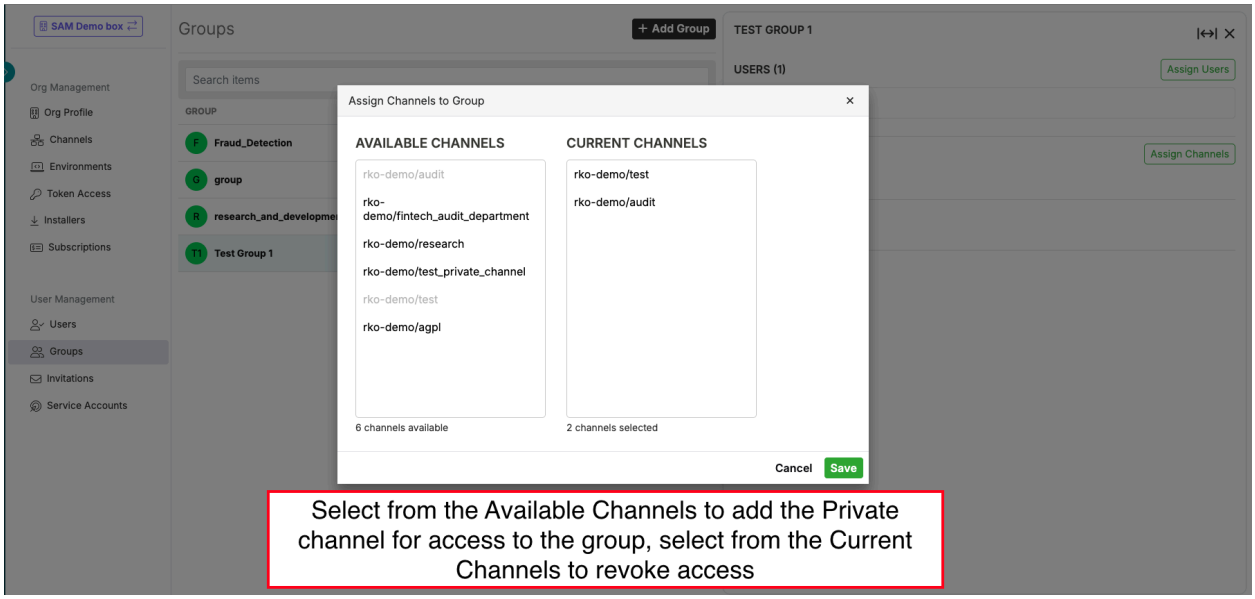
4. Select **Save**.

Method 2: From the Groups Page

1. Select a group to edit its channel access.
2. Select **Assign Channels**.



3. Select your private channel(s) from the **Available Channels** list to add to the group, or deselect channels from the **Current Channels** list to remove them.



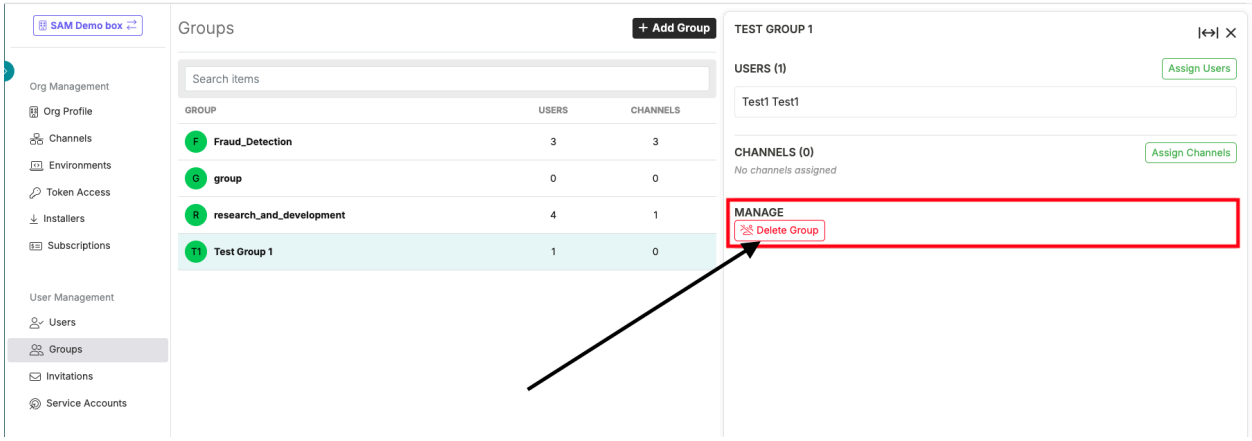
4. Select **Save**.

Delete Groups

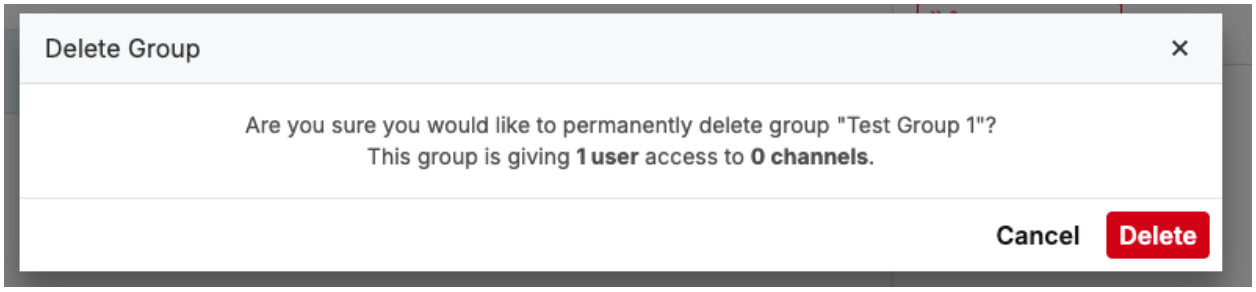
To delete groups

1. On the Groups page, select the group you wish to delete.

2. Under Manage, select **Delete Group**.



3. A confirmation pop-up will appear. Select **Delete** to permanently delete the group from your organization.



4. As the admin, you'll receive an email notification on deleting a group.

Invitations Page

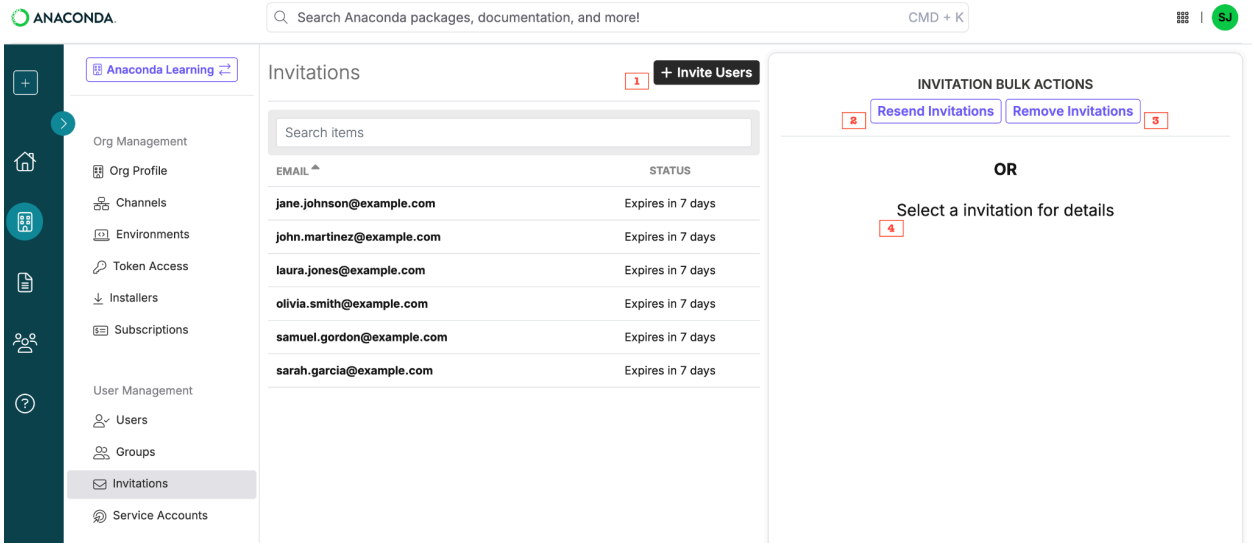
You can invite users (i.e., your team members) to your organization from either the Users or the Invitations page. This is necessary so that your team can seamlessly access the Anaconda Platform Cloud.

Requirements and Access:

- You must be an admin to invite/manage users.
- Access the Invitations page by navigating to **Org Profile > User Management > Invitations**

Invitations Page Capabilities:

1. Invite Users
2. Resend Invitations
3. Remove Invitations
4. Manage invitations

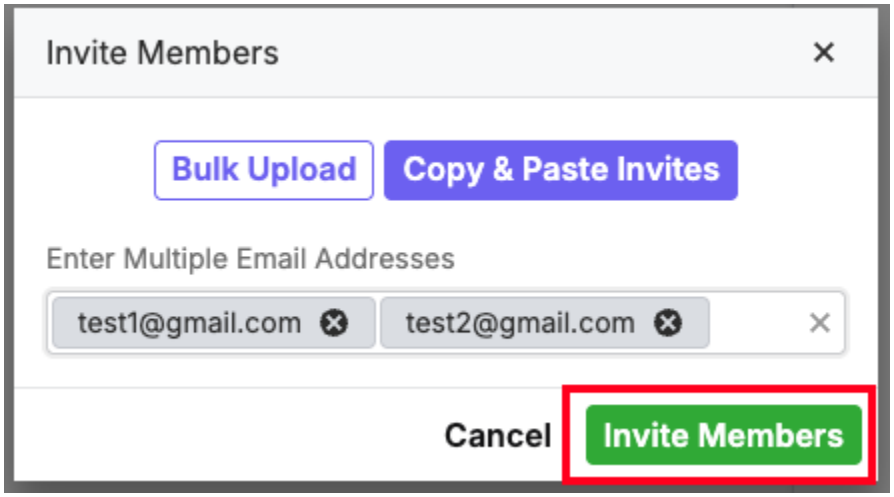


Invite an Individual User

To invite an individual user

1. Navigate to **Org Profile** > **User Management** > **Invitations**. On the Invitations page, select **+ Invite Users.**
2. In the **Invite Members** pop-up, under **Enter Multiple Email Addresses**, enter the user's email address, and press Enter or Return. Repeat this step to add more users.

3. Once done, select **Invite Members**.



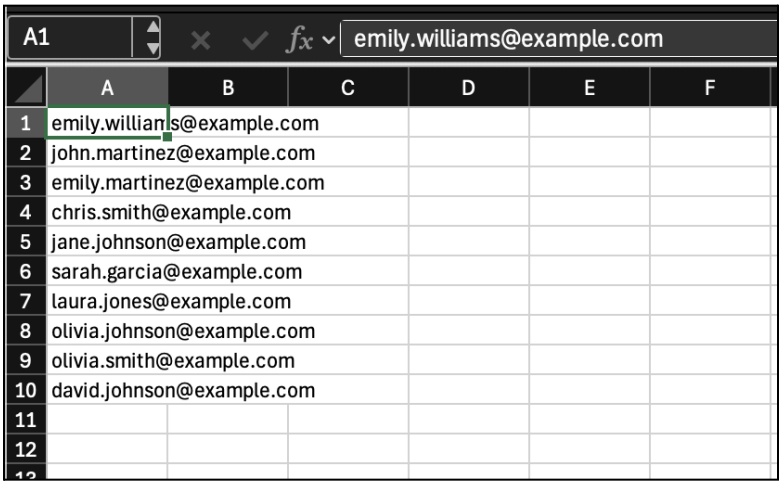
4. All invited users will then receive an email from Anaconda asking them to accept the invitation (they need to select **Join Organization**).

Once the invited user has accepted the invite, you, as the admin, will also receive an email to notify you that this user has joined the organization.

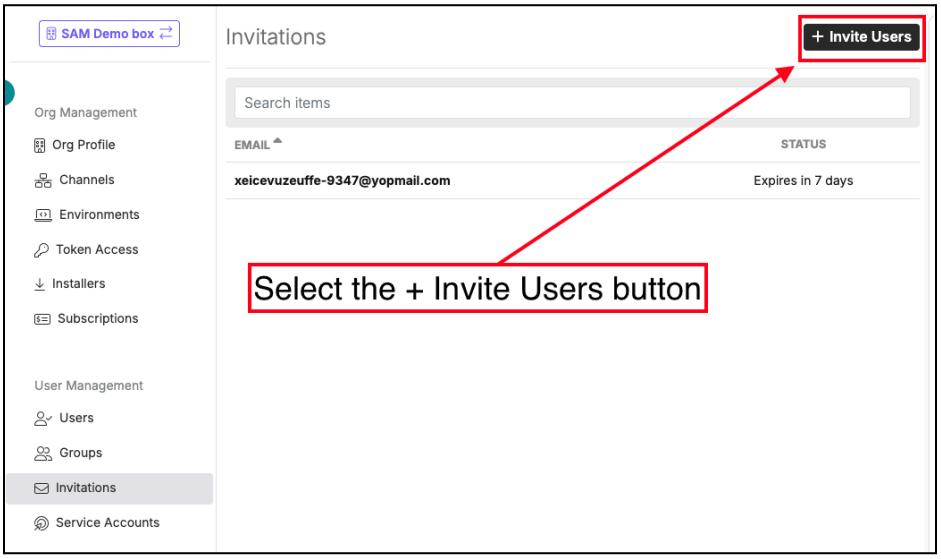
Invite Multiple Users

To invite multiple users simultaneously

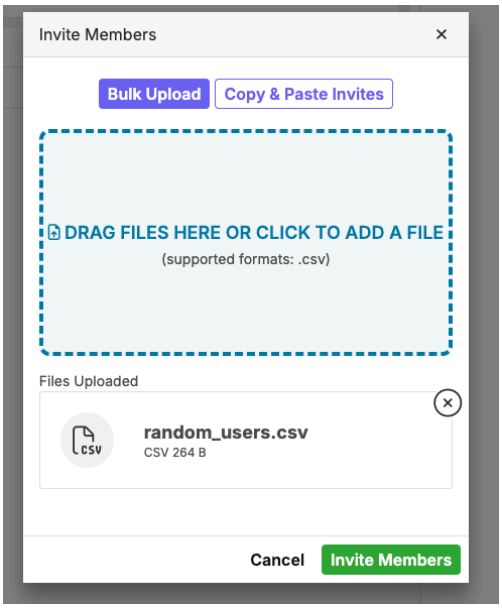
1. First, in a CSV file, enter all email addresses that you wish to invite. Include email addresses in the first column; no other details are needed (the column should not have a header/title). Save this file on your local system.



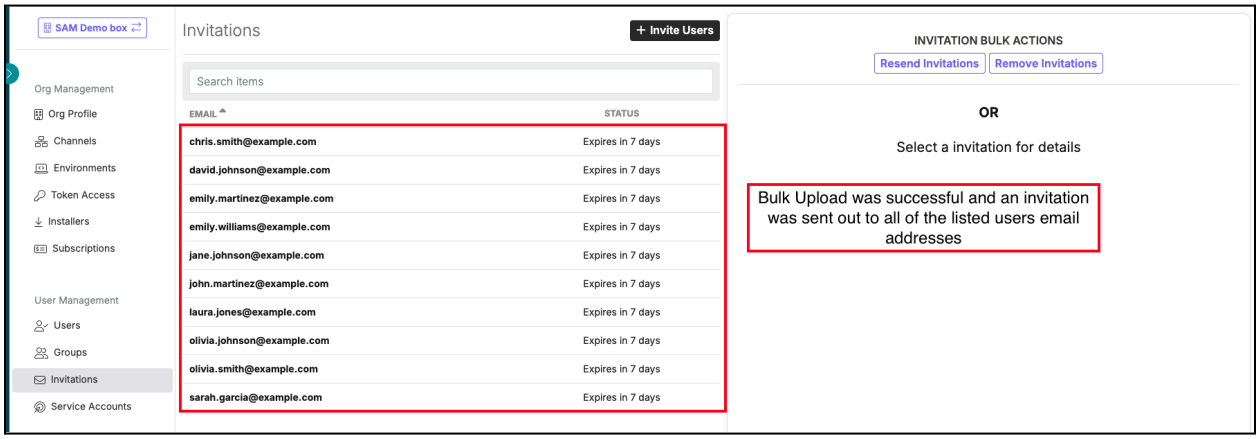
2. Now navigate to **Org Profile** > **User Management** > **Invitations**. On the Invitations page, select **+ Invite Users.**



3. In the **Invite Members** pop-up, select **Bulk Upload.** Drag and drop the CSV file from your local system, and select **Invite Members**.



4. All invited users will then receive an email from Anaconda asking them to accept the invitation (they need to select **Join Organization**).



Once the invited users have accepted the invite, you, as the admin, will also receive an email to notify you that users have joined the organization.

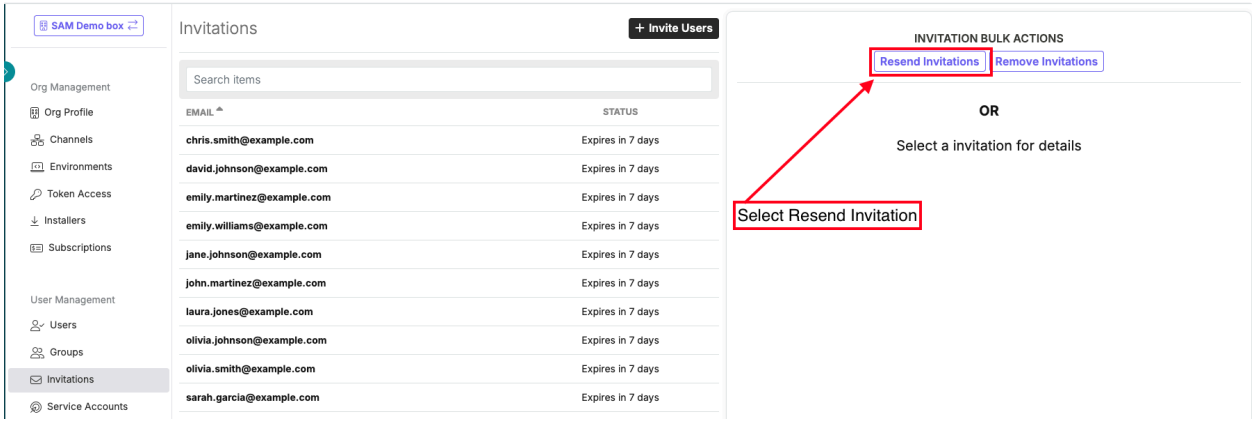
Note: Invitations are valid for only **7 days**. You can track invitation status on the **Invitations** page. If an invite expires, you'll need to send a new invitation.

Resend Invitations

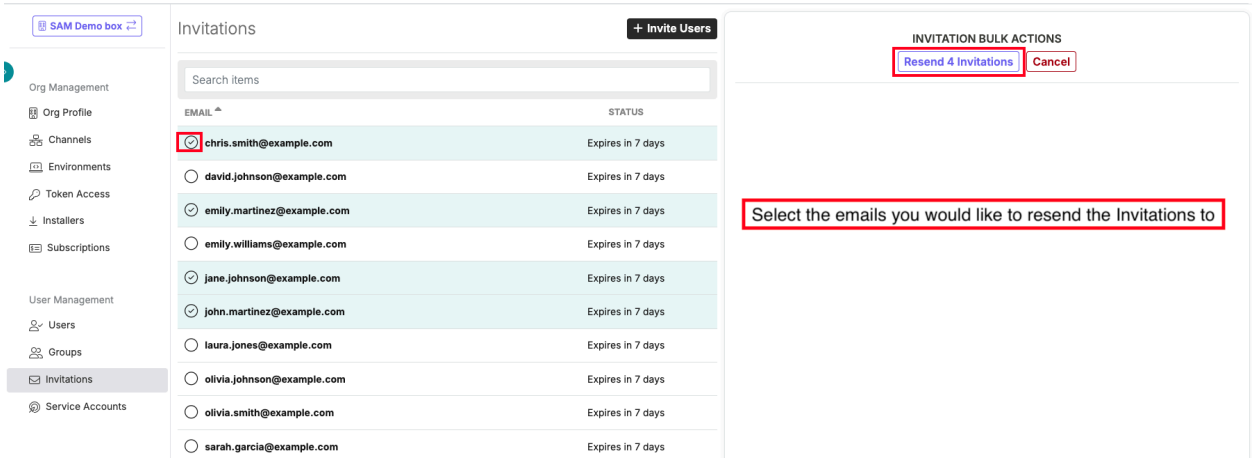
User invitations to the Anaconda Platform Cloud expire 7 days after being sent. If a user's invitation has expired or is about to expire, you can resend it.

To resend an invitation

1. Navigate to **Org Profile** > **User Management** > **Invitations**.
2. On the Invitations page, select **Resend Invitation.**



3. Select the email addresses to which you want to resend invitations.



4. Select **Resend X Invitations** (X represents the number of users being reinvited), and then confirm your action.

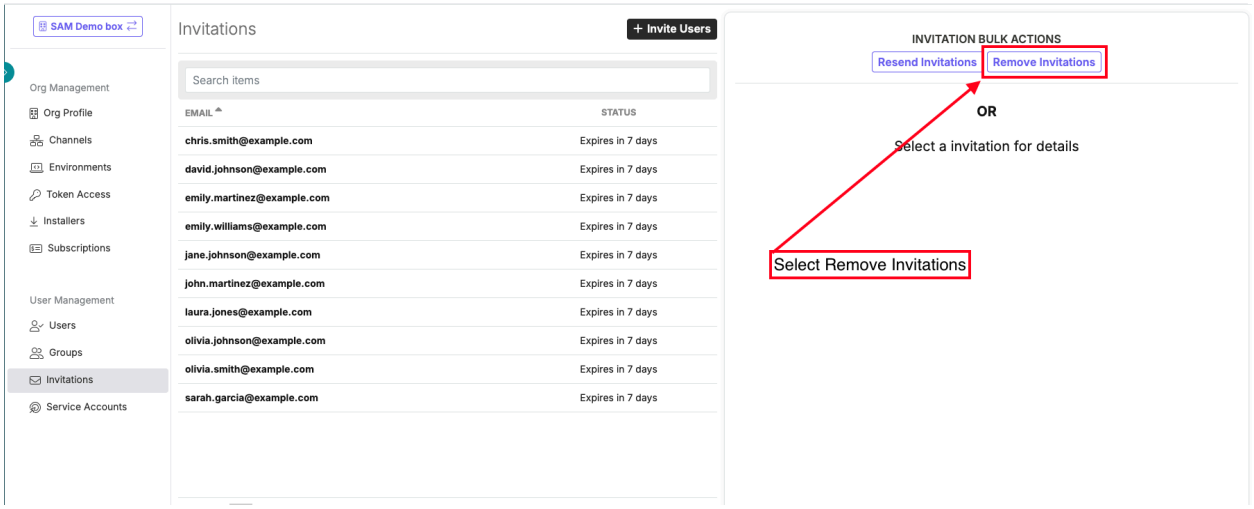
Remove Invitations

Invitations can be removed, which revokes an invite that you have sent out to a user within your organization.

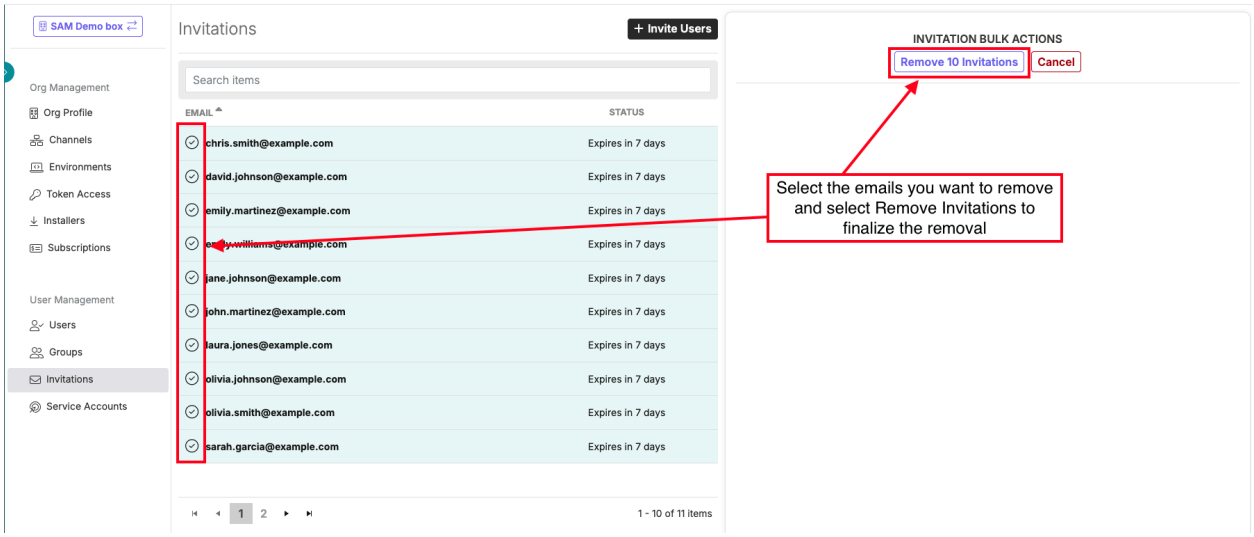
To remove an invitation

1. Navigate to **Org Profile** > **User Management** > **Invitations**.

2. On the Invitations page, select **Remove Invitations**.



3. Select the email address(es) that you would like to remove from your invitation list.
4. Selecting **Remove X Invitations** (X represents the number of invitations being removed), and then confirm your action.



Service Accounts Page (API User Onboarding)

A service account consists of authentication credentials—a client ID and client secret—that enable programmatic management of your organization through the anaconda.com organization management API. **Only admins can create service accounts.**

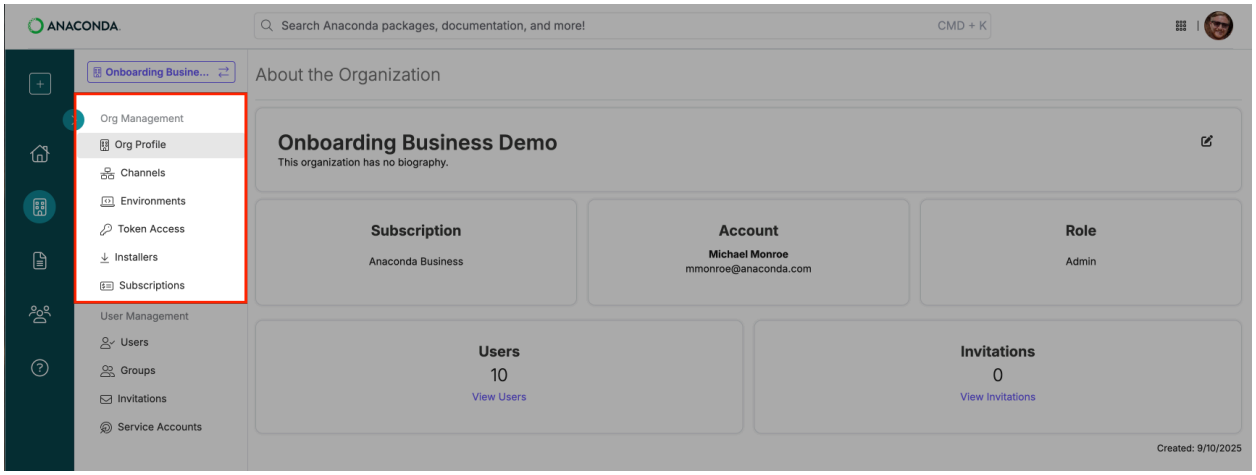
While you can create multiple service accounts for your organization, we recommend creating only as many as needed for your operations. Limiting the number of service accounts improves your organization's overall security posture.

For more information about service accounts and anaconda.com organization management API, refer to the following resources:

- Service account management
- Managing your organization using the API

Org Management

As an admin, **Org Management** under Anaconda Organizations [to view "My Organizations", sign in to anaconda.com/app. You'll then see your organization(s) in the left panel] includes the following:



- **Org Profile**: View an overview of your organization and edit organizational settings.
- **Channels**: Manage your Anaconda Repository and configure channel settings.
    - **Policies**: Establish organizational policies and manage channel/package access controls aligned with your security and compliance standards.
    - **Packages**: Access package-related information, including package structures, SBOMs, CVE identification, and Anaconda's curation practices.
- **Token Access**: Create and manage authentication tokens for repository access.
- **Subscriptions**: Review your plan details and manage billing information.

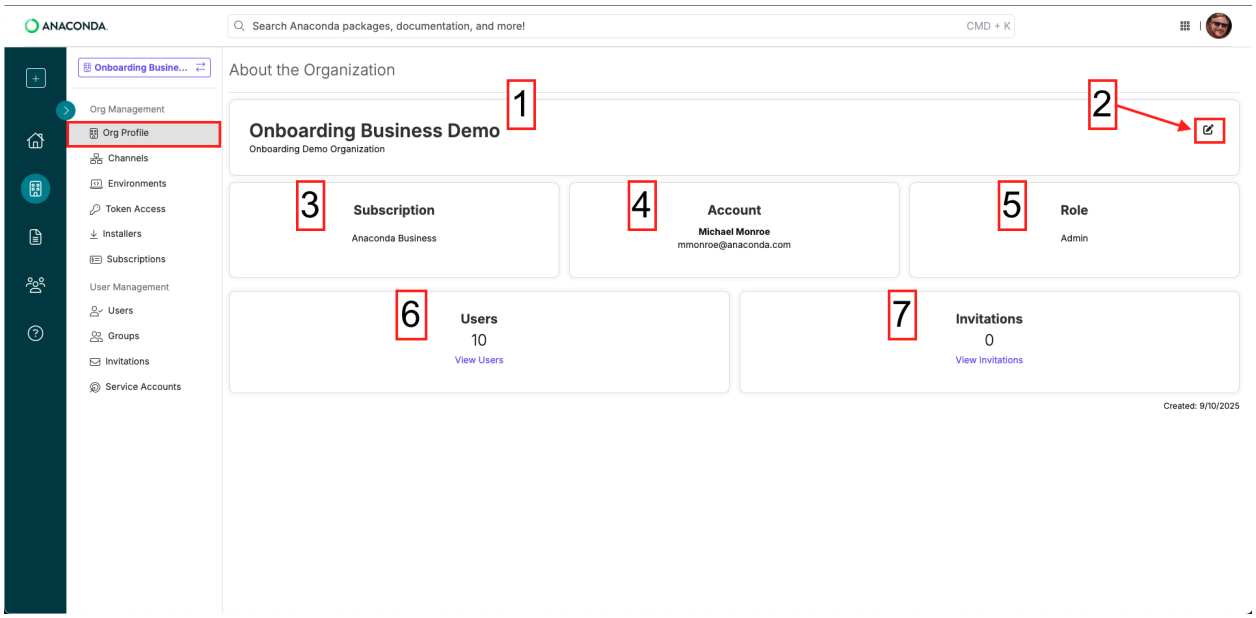
Org Profile Page

The **Org Profile** page displays an overview of your organization and allows you to configure your organization's settings for various features.

Org Profile Page Overview

The main Org Profile page displays the following information:

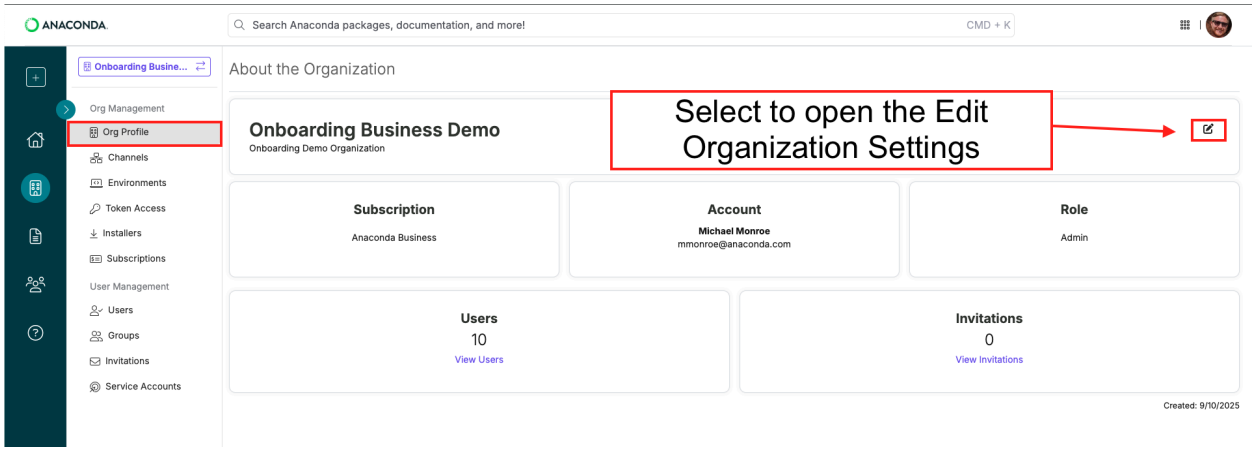
1. **Organization Name and Biography**: Your organization's name and description
2. **Edit Organization Settings** Button: Opens the settings dialog to modify your organization's settings
3. **Subscription** Status: Displays your current plan (e.g., Anaconda Business)
4. **Account**: Shows which account is currently logged in
5. **Role**: Displays your role within your organization's Anaconda Platform Cloud
6. **Users**: Shows the total number of users (i.e., admins, billing managers, and members) in your organization
7. **Invitations**: Displays the number of users with pending invites



Edit Organization Settings

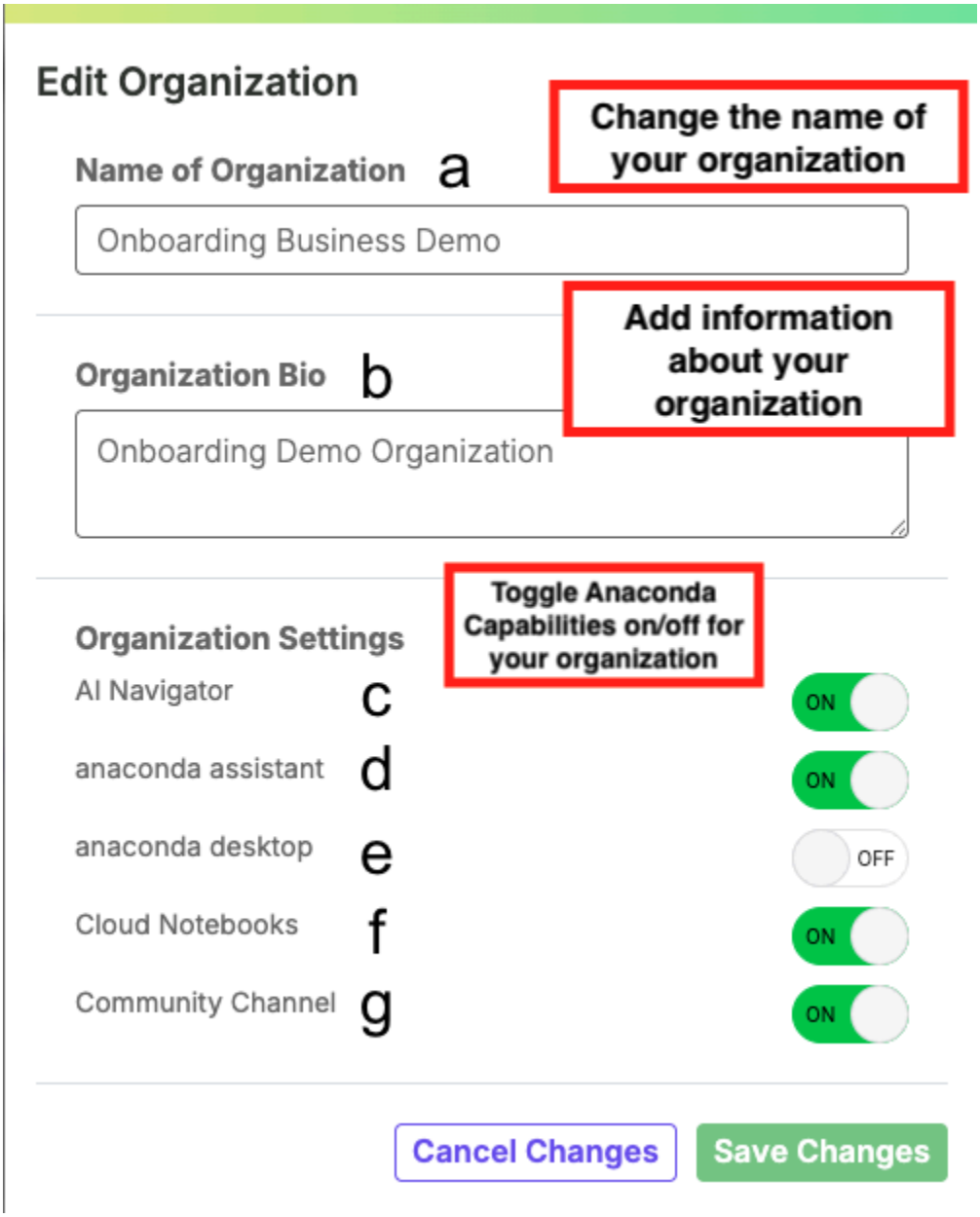
To edit your organization settings

1. Navigate to **Org Profile** under **Org Management**.
2. On the Org Profile page, select Edit Organization Settings (pen and paper icon) on the right:



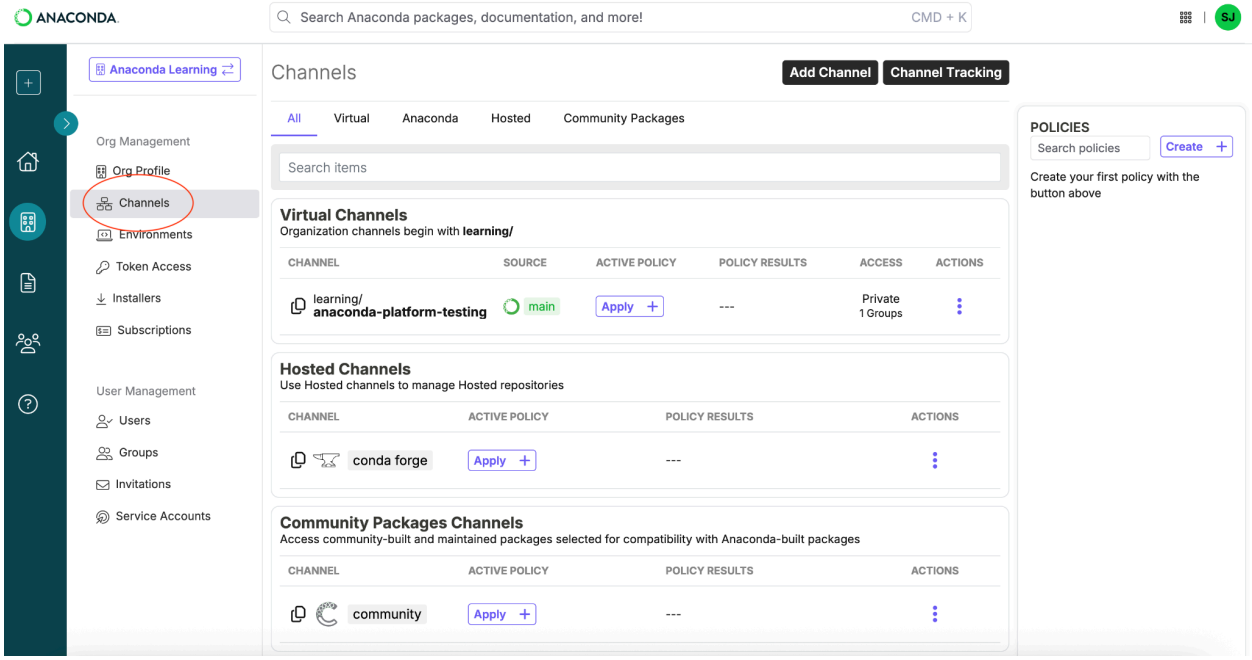
3. In the **Edit Organization** pop-up window, you can modify the following settings and toggle Anaconda capabilities on or off for your organization:
    a. **Name of Organization:** Use this to change your organization name on the Anaconda Platform Cloud.
    b. **Organization Bio:** Use this to include a brief description of your organization.
    c. **AI Navigator:** For downloading and running large language models (LLMs) locally on your system.
    d. **Anaconda Assistant:** An AI-powered digital pair programmer built into Anaconda Cloud Notebooks and Anaconda Toolbox.
    e. **Anaconda Desktop:** Anaconda Distribution installer (soon to be released)
    f. **Anaconda Cloud Notebooks:** A browser-based platform that allows you to instantly launch Jupyter notebooks with pre-configured packages, computing power, and storage.
    g. **Community Channel:** Provides secure access to 16,000+ open-source packages from conda-forge, integrated into Anaconda's secure pipeline and fully compatible with Anaconda Distribution.

Note: Product access controls for **c to f** can be toggled on or off for your organization from this pop-up window.



Channels Page

A channel is a location where conda can search for **packages** to install in **environments** on your system. Conda finds these channels via URL, name, or file path, depending on your setup.



The **Channels** page is where you, as the admin, can curate specific sets of packages and control which users can access them. Users can access their channels via this page.

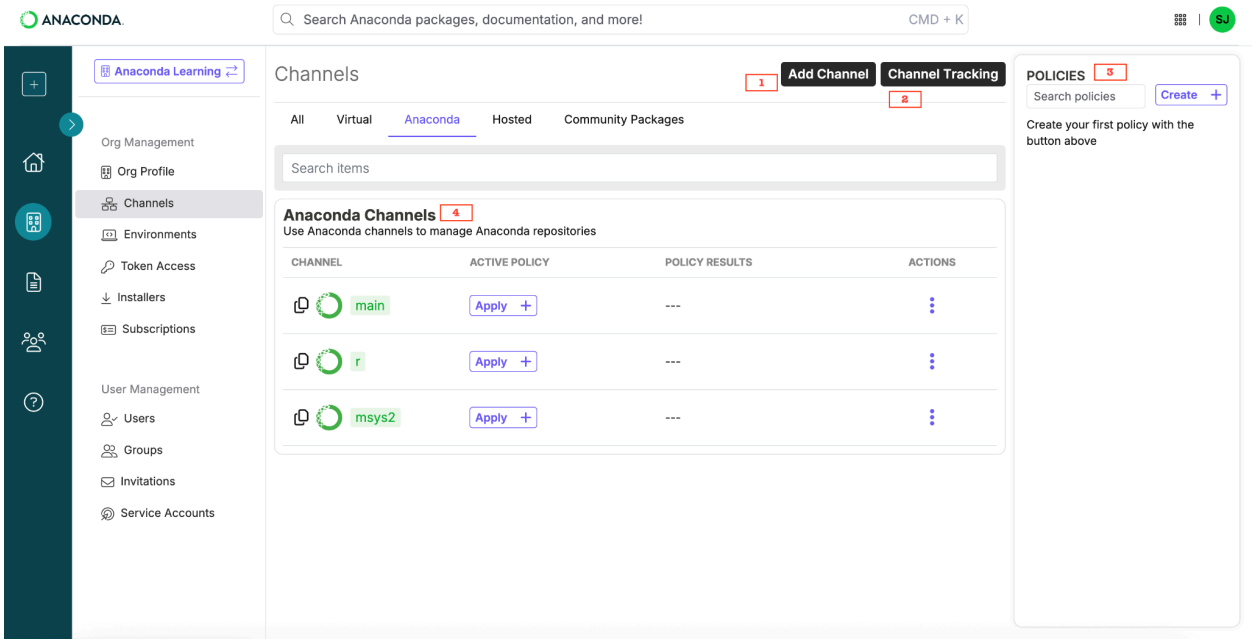
Requirements and Access:

- You must be an admin to create channels and manage access.
- Access the Channels page by navigating to **Org Profile** > **Org Management** > **Channels**

Channels Page Capabilities:

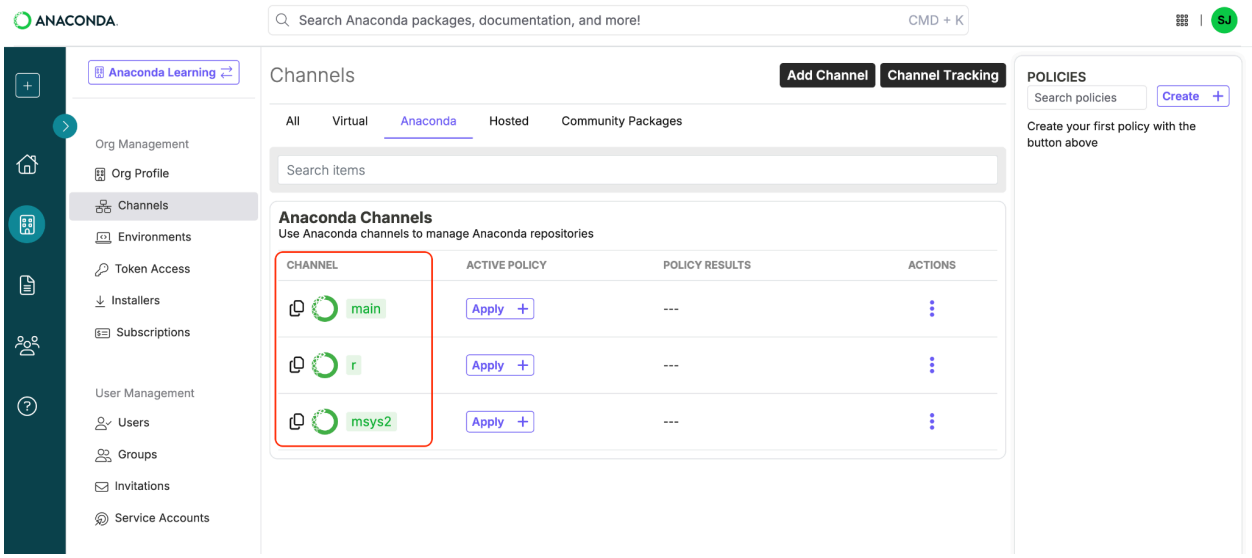
1. **Add Channels**: You can create External, Virtual, Internal, and/or Private channels in addition to the three default Anaconda channels.

   a. [Virtual channels](#) are copies of Anaconda sources (main, r, and msys2).
   b. [External channels](#) are mirrored channels pointing to external repositories. Note that at present, only anaconda.org channels can be created as external channels.
   c. **Internal channels** are channels visible to all members of your organization.
   d. **Private channels** are restricted to users who are part of a group that is assigned to the private channel. Only members of this group can access this private channel that is assigned to them. For more information, refer to Assign a Private Channel to a Group.
2. **Channel Tracking** allows you to track channels with attached policies.
3. [Policies](#): Creating a policy allows you to apply filters to any channel, except external channels.
4. **Anaconda Channels:** These are our default channels. For more information, refer to Anaconda (Default) Channels.



Anaconda (Default) Channels

Anaconda, Inc. maintains the **defaults** channels: repo.anaconda.com/pkgs/**main**, repo.anaconda.com/pkgs/**r**, and repo.anaconda.com/pkgs/**msys2**. These channels are specified in an order that ensures dependencies resolve correctly.



- **main**
  - Contains packages built by Anaconda, Inc. with the new compiler stack.
  - Most new Anaconda, Inc. package builds are hosted here.
- **r**
  - Contains Microsoft R Open conda packages and Anaconda, Inc.'s R conda packages.
  - MRO is the default R implementation when creating new environments.
  - **Important:** Changes to Anaconda's R Channel Support.
- **msys2**
  - Windows-only packages necessary for Anaconda, Inc.'s R conda packages and some others in pkgs/main and pkgs/free.
  - Provides a bash shell, Autotools, revision control systems, and tools for building native Windows applications using MinGW-w64 toolchains.

These channels are automatically configured in your .condarc file when you install Anaconda Distribution or Miniconda. Note that these channels come with **Terms of Service**. While largely free for individual users, students, and small companies, there are scenarios where a license might be required.

Anaconda Free Repository

repo.anaconda.com is our repository that is publicly accessible and hosts main, r, and msys2 packages for individual non-commercial users and students. Accessing this repository without a license may violate our Terms of Service if you do not fall within these categories.

URL paths:

- repo.anaconda.com/pkgs/main
- repo.anaconda.com/pkgs/r
- repo.anaconda.com/pkgs/msys2

Anaconda Premium Repository

If you need access to Anaconda Premium Repository, you must have an active seat assignment in your organization. Access is granted through Token Access, enabling you to authenticate and pull packages from repo.anaconda.cloud. **Licensed users should configure their environment to use repo.anaconda.cloud instead of the free public repository (repo.anaconda.com) to access curated, secure packages with CVE visibility and Software Bill of Materials (SBOMs)**

Anaconda Premium Repository hosts our main, r, and msys2 packages.

URL paths:

- repo.anaconda.cloud/repo/main
- repo.anaconda.cloud/repo/r
- repo.anaconda.cloud/repo/msys2

Anaconda Premium Repository includes our curated packages that have:

- Visibility into Common Vulnerabilities and Exposures (CVEs)
- Signatures that ensure the integrity and authenticity of our packages
- SBOMs

Virtual Channels

Virtual channels are copies of their source channel (main, r, msys2, or community). For example, a virtual channel created from the Anaconda main

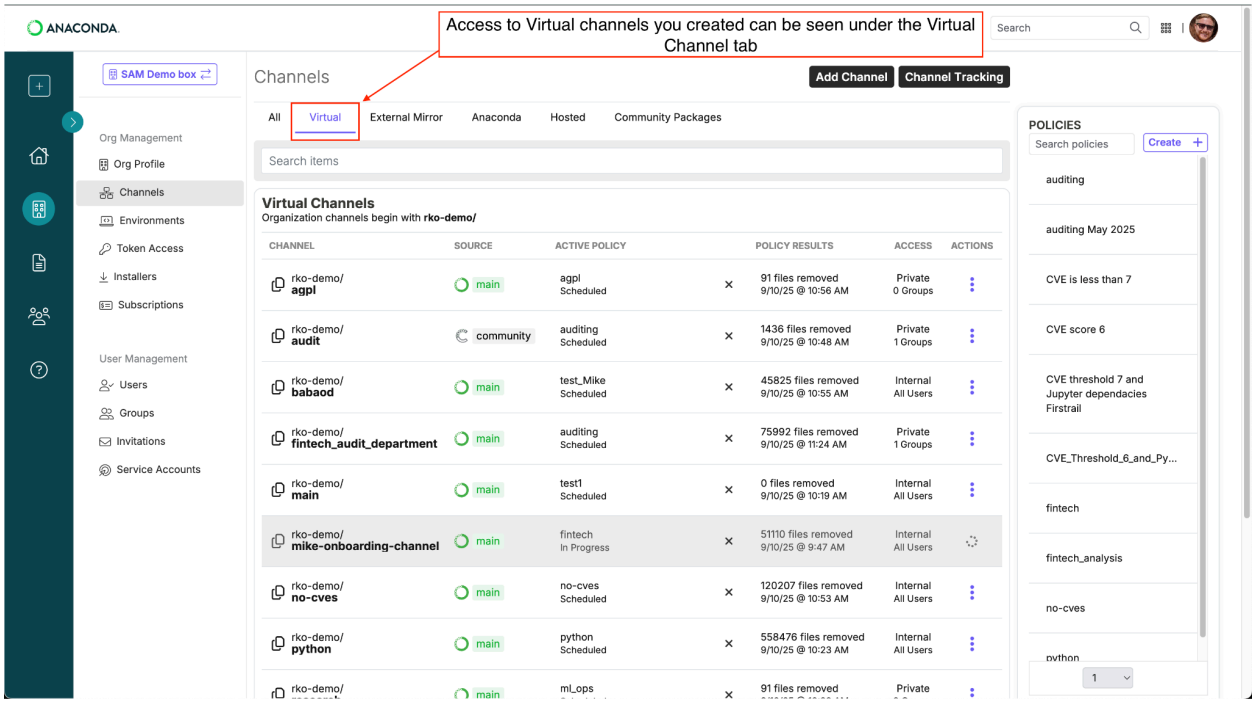
channel contains the same packages as main. This allows you to create new channels with different policy filters than the original channel.

You can create virtual channels with two access levels:

1. **Internal channels** are visible to all members of your organization with an assigned seat.
2. **Private channels** are only accessible to members of the group that the private channel is assigned to.

This functionality enables you to grant specific groups access to particular packages using policy filters, which are discussed in detail later.

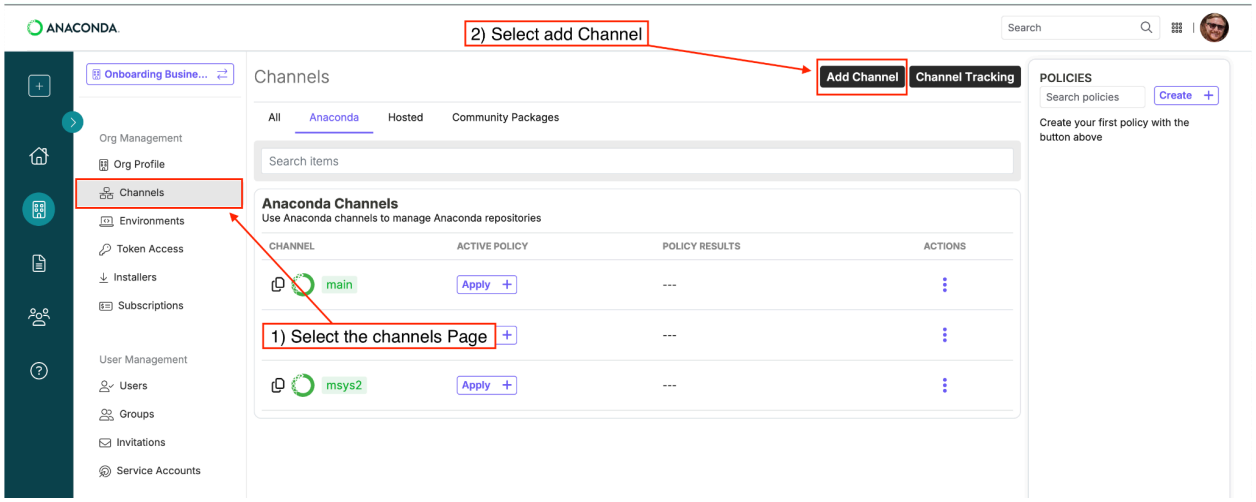
To view and manage virtual channels, navigate to **Org Profile** > **Org Management** > **Channels** > **Virtual**:



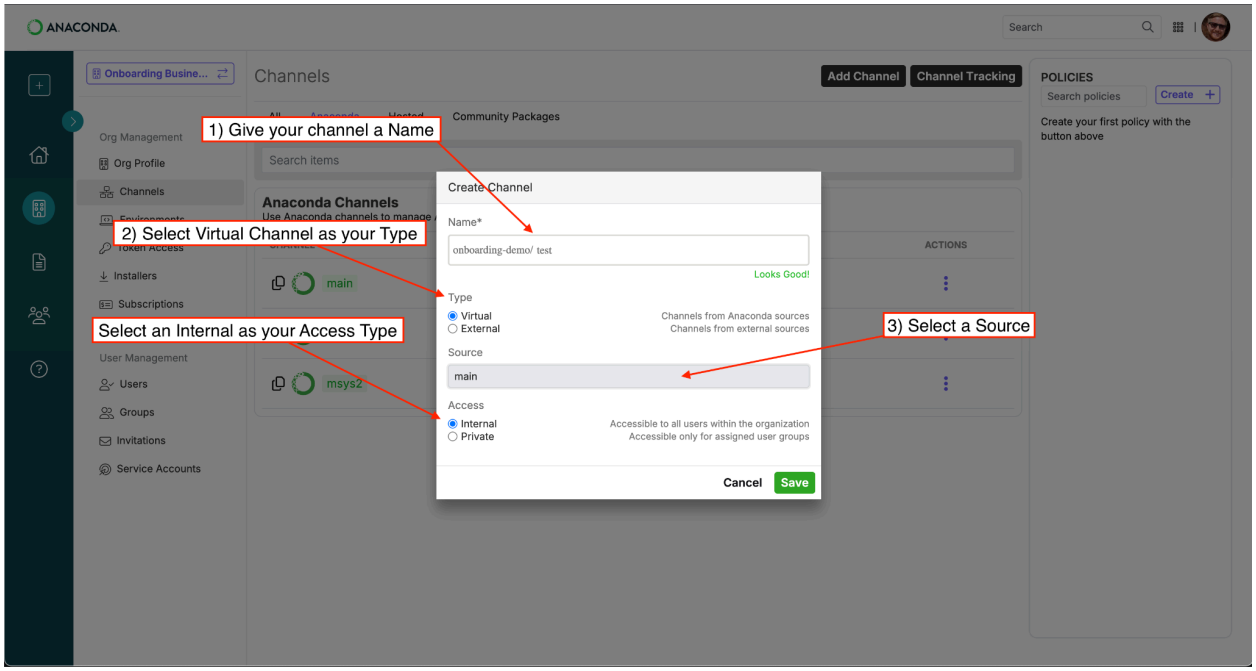
Create a Virtual Channel with Internal Access

To create a virtual internal channel

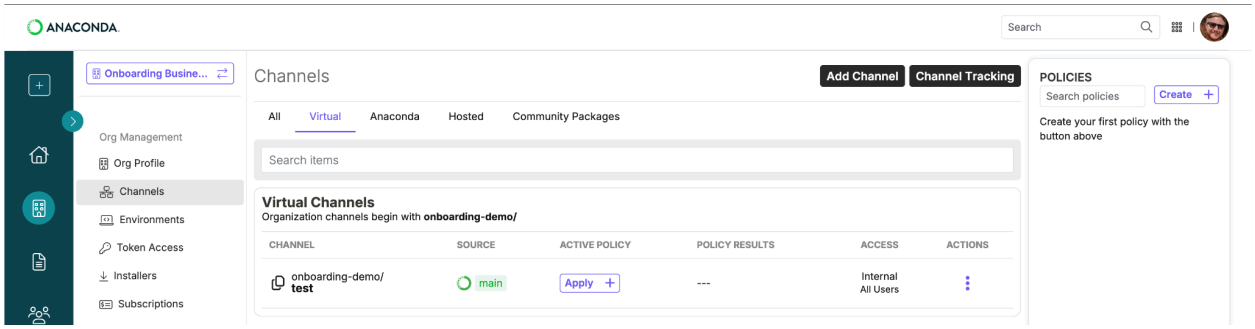
1. Navigate to **Org Profile** > **Org Management** > **Channels** > **Virtual**.
2. Select **Add Channel**.



3. In the **Create Channel** pop-up:
    - Enter a Name for your channel
    - Select **Virtual** under (channel) Type
    - Select Source: main, r, msys2, or community
    - Set Access to **Internal**
4. Select **Save**.



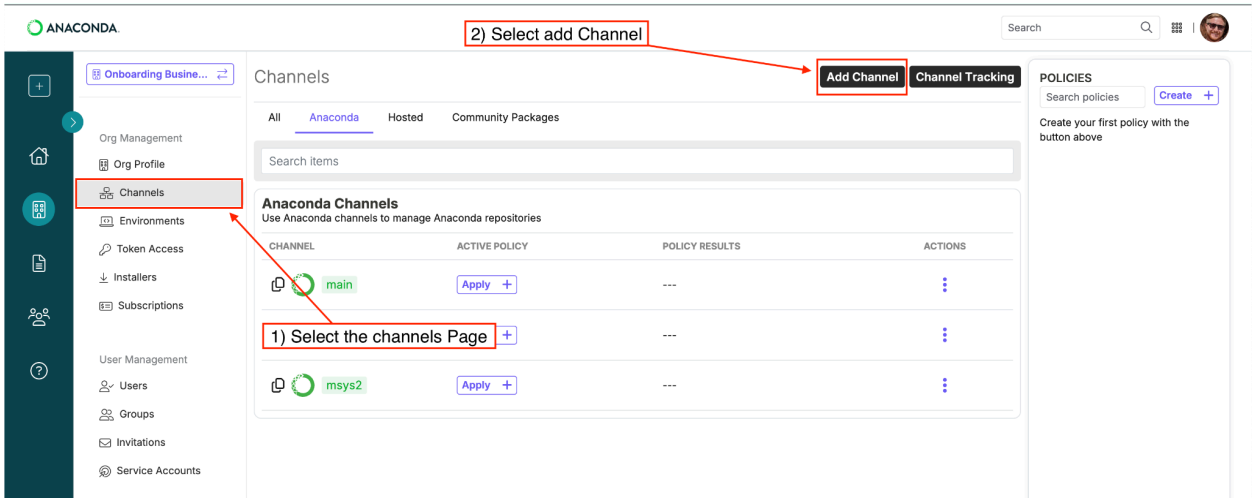
All your organization users will now be able to view and use this virtual internal channel.



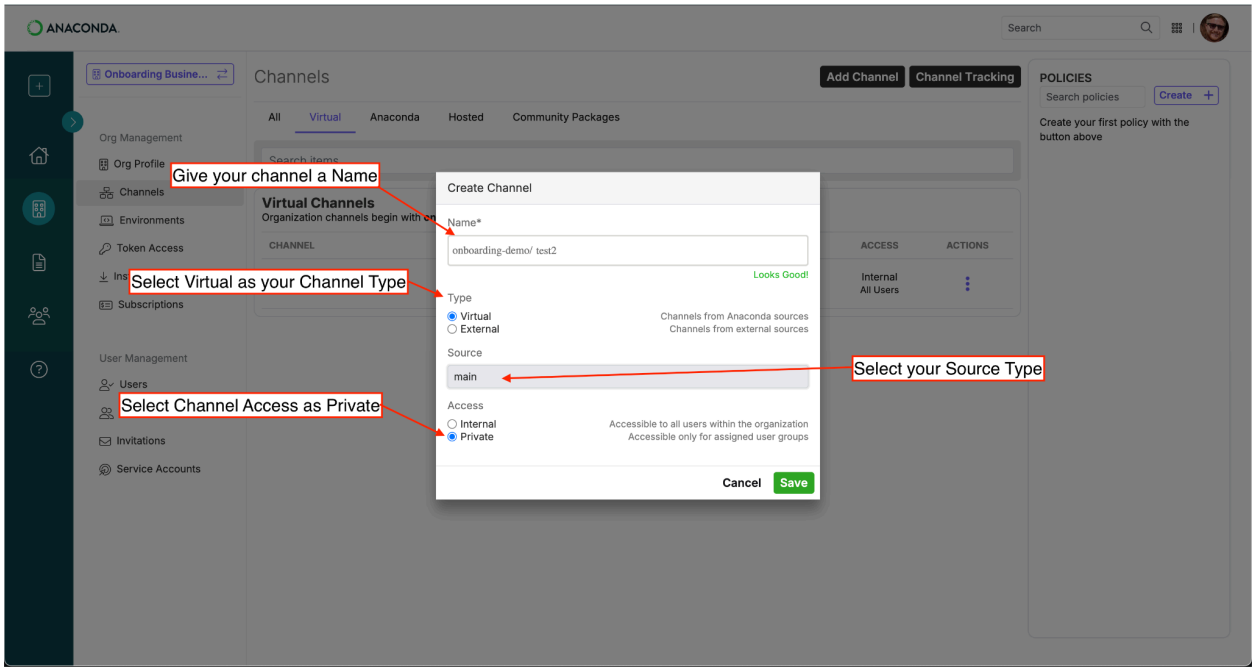
Create a Virtual Channel with Private Access

To create a virtual private channel

1. Navigate to **Org Profile** > **Org Management** > **Channels** > **Virtual.**
2. Select **Add Channel**.

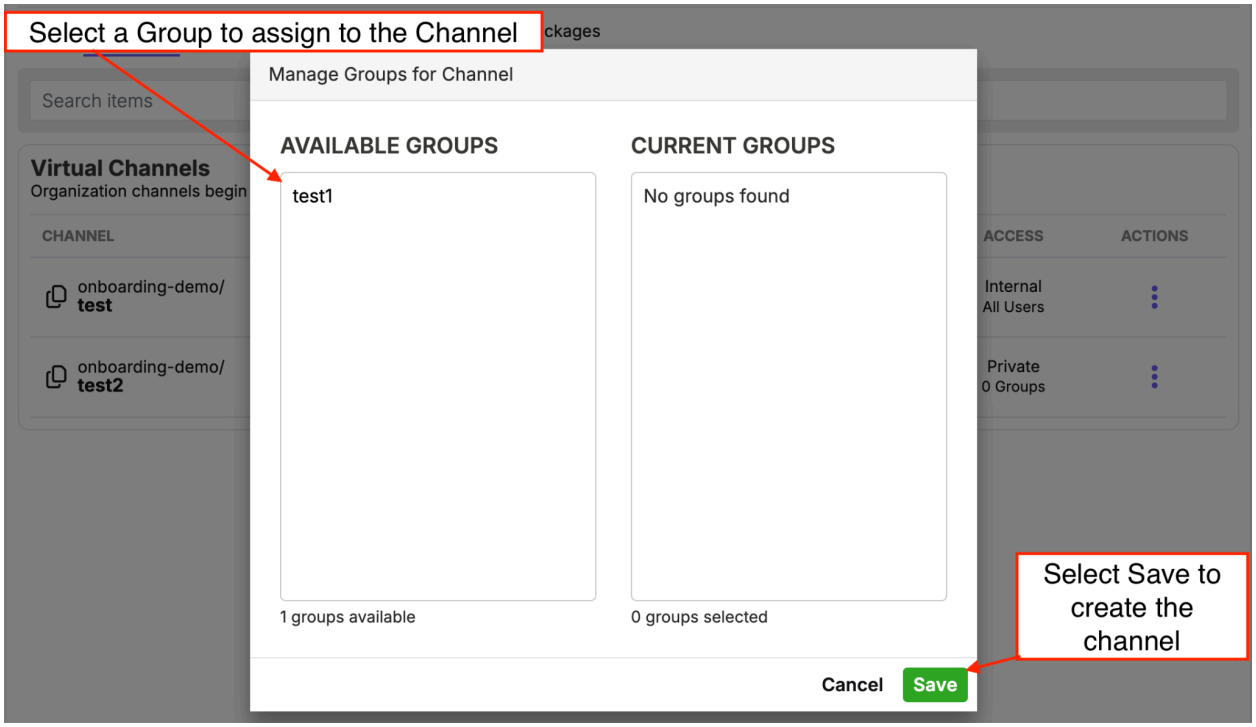


3. In the **Create Channel** pop-up:
    - Enter a Name for your channel
    - Select **Virtual** under (channel) Type
    - Select Source: main, r, msys2, or community
    - Set Access to **Private**
    - Select **Save**

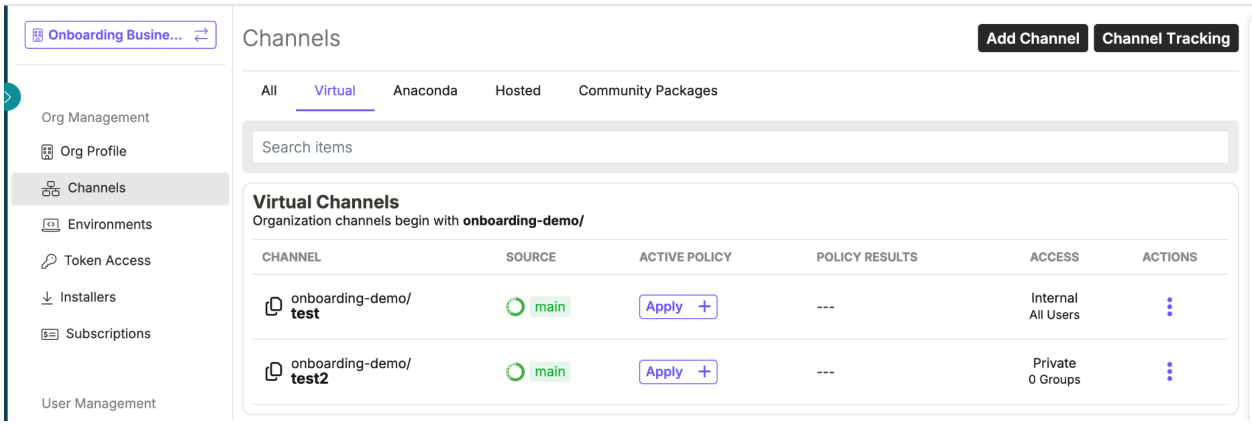


5. Select an **Available Group** to assign to this private channel:

    - If no groups exist as yet, you can create this channel without a group and assign one later (refer to Assigning a Private Channel to a Group).



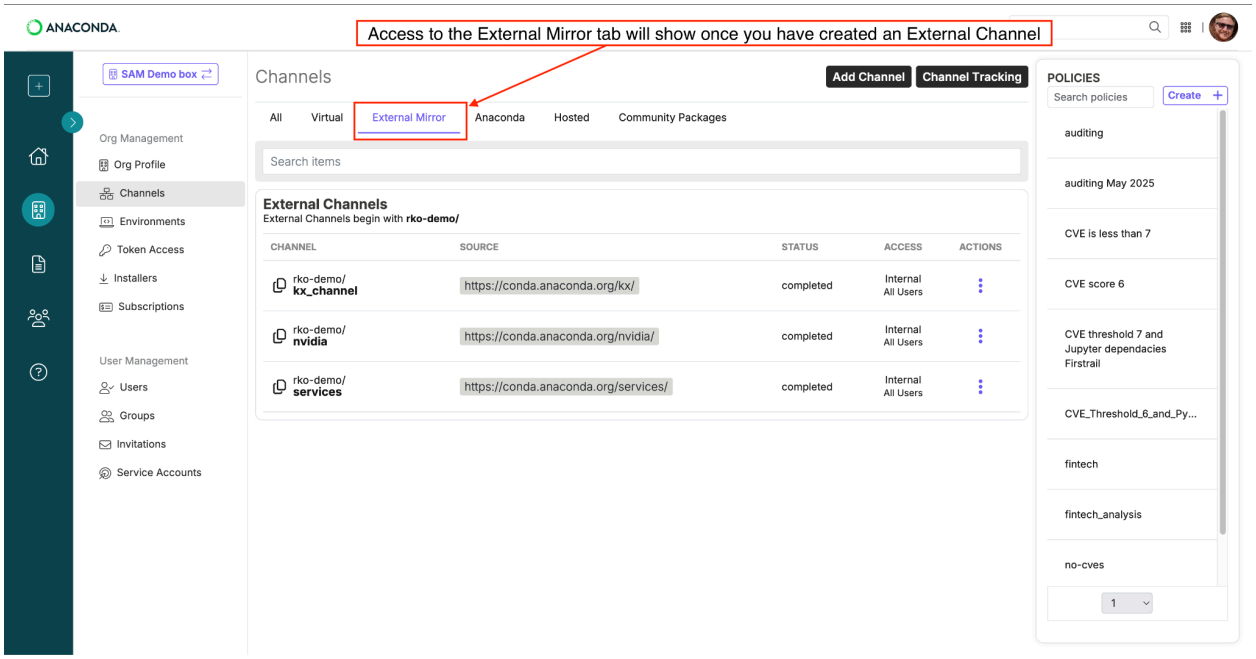
6. Select **Save** to create your virtual private channel.



External Channels

External channels are mirrored channels that point to external packages. At present, only anaconda.org channels can be mirrored as external channels. Use external channels to import packages from anaconda.org that your organization uses.

To view and manage external channels, navigate to **Org Profile** > **Org Management** > **Channels** > **External Mirror** (**note**: External Mirror tab will appear only once you've created an external channel):



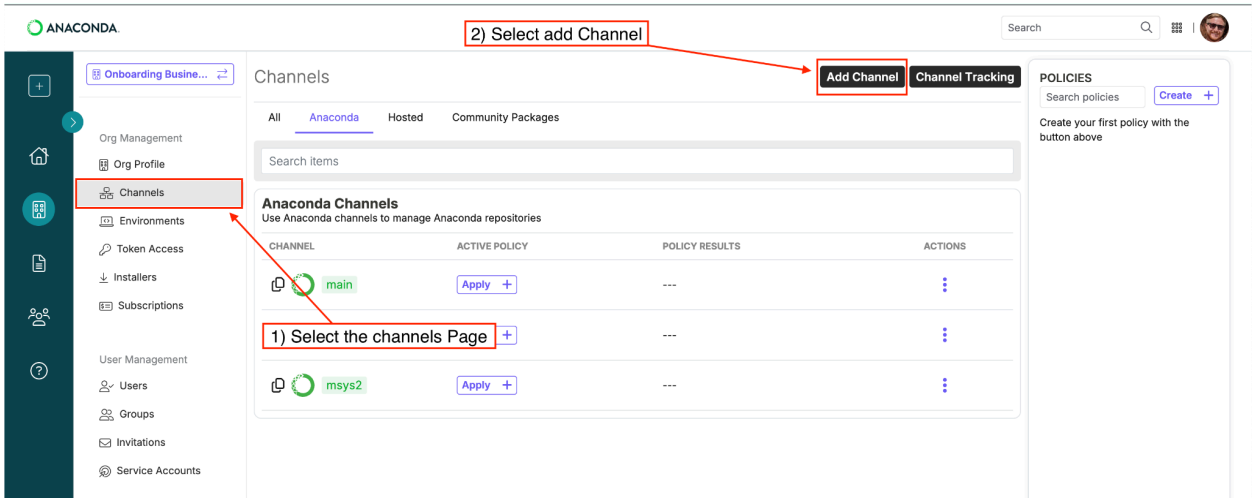
Important notes:

- Access to external channels can be either **Internal** (accessible to all) or **Private** (accessible to specific groups only).
- **Policy filters** cannot be applied to external channels. If you mirror a channel on anaconda.org, all packages from the source will be imported.
- The **conda-forge** channel cannot be mirrored. It is available as a **Hosted** channel. If you need assistance, reach out to your Customer Success Manager (CSM) via cs@anaconda.com or support at support.anaconda.com.

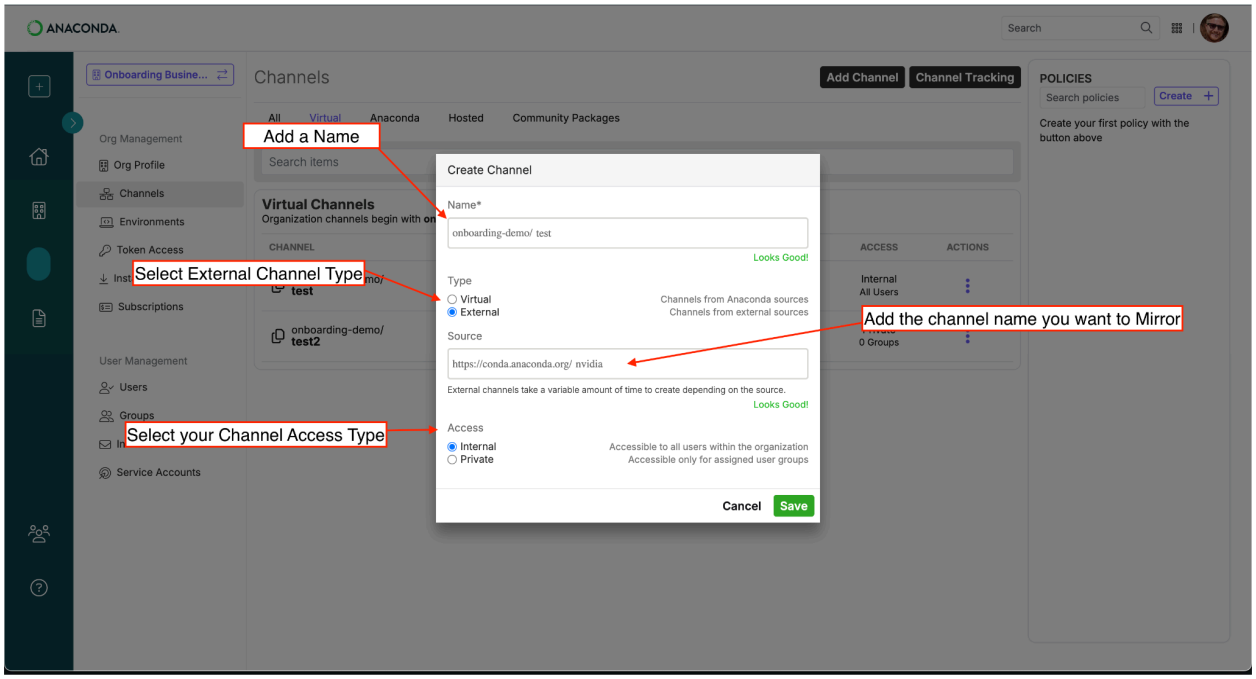
Create an External Channel

To create an external channel

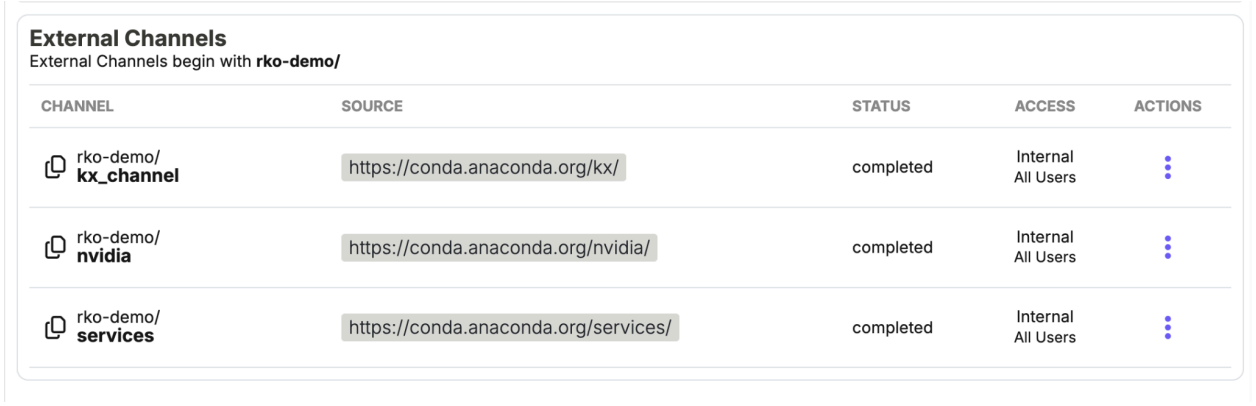
1. Navigate to **Org Profile** > **Org Management** > **Channels**.
2. Select **Add Channel**.



3. In the **Create Channel** pop-up:
    - Enter a Name for your channel
    - Select **External** under (channel) Type
    - Enter the channel to mirror (refer to **Finding Channels to Mirror** below) using this format: http://conda.anaconda.org/<channel_name> (**note**: channel names are case sensitive, so use “nvidia” not “NVIDIA”)
    - Set Access to **Internal** or **Private** (assign a group if selecting Private)
4. Select **Save**.



Allow time for the mirroring to complete. Once finished, you'll have access to the external mirrored channel.



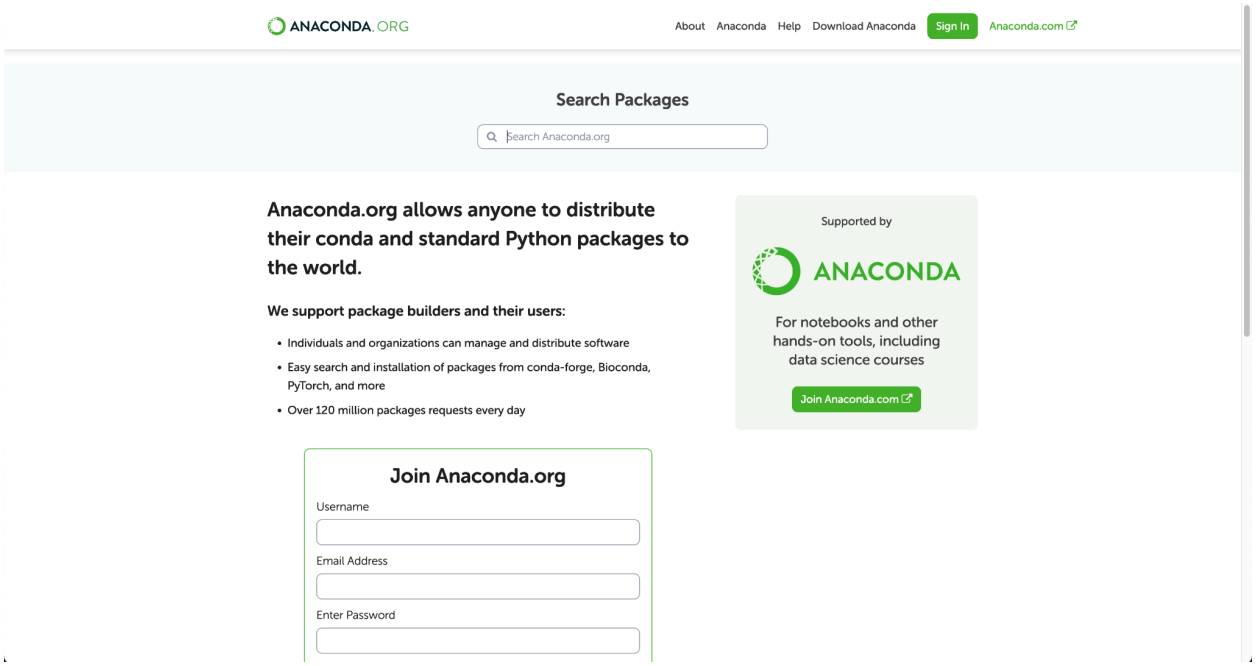
External Channels

External Channels begin with **rko-demo/**

CHANNEL	SOURCE	STATUS	ACCESS	ACTIONS
rko-demo/ **kx_channel**	https://conda.anaconda.org/kx/	completed	Internal All Users	
rko-demo/ **nvidia**	https://conda.anaconda.org/nvidia/	completed	Internal All Users	
rko-demo/ **services**	https://conda.anaconda.org/services/	completed	Internal All Users	

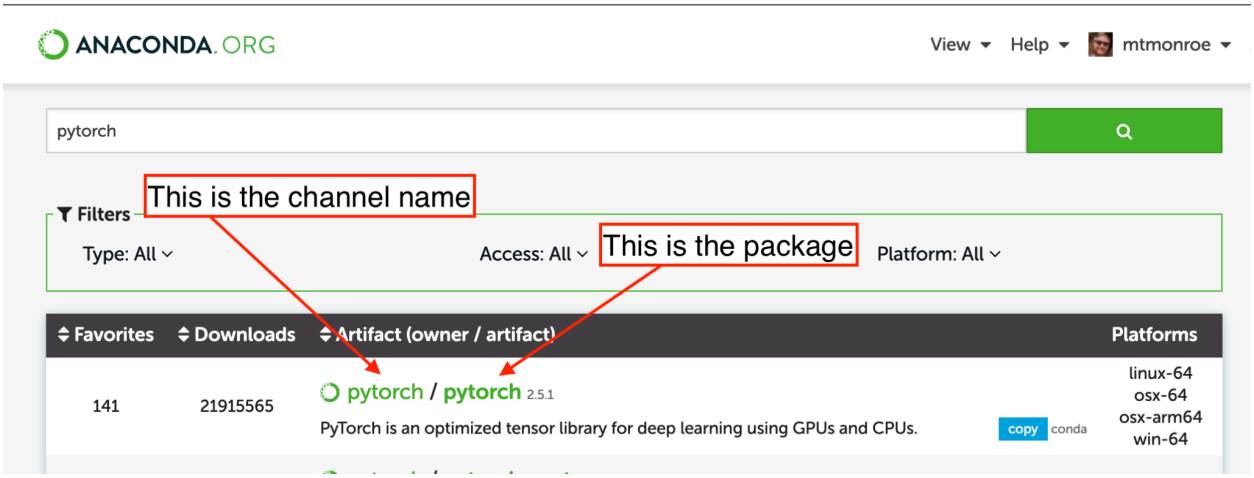
Finding Channels to Mirror

At present, external mirroring only works for channels on anaconda.org. Use the search feature to find public channels that contain packages uploaded by the community.

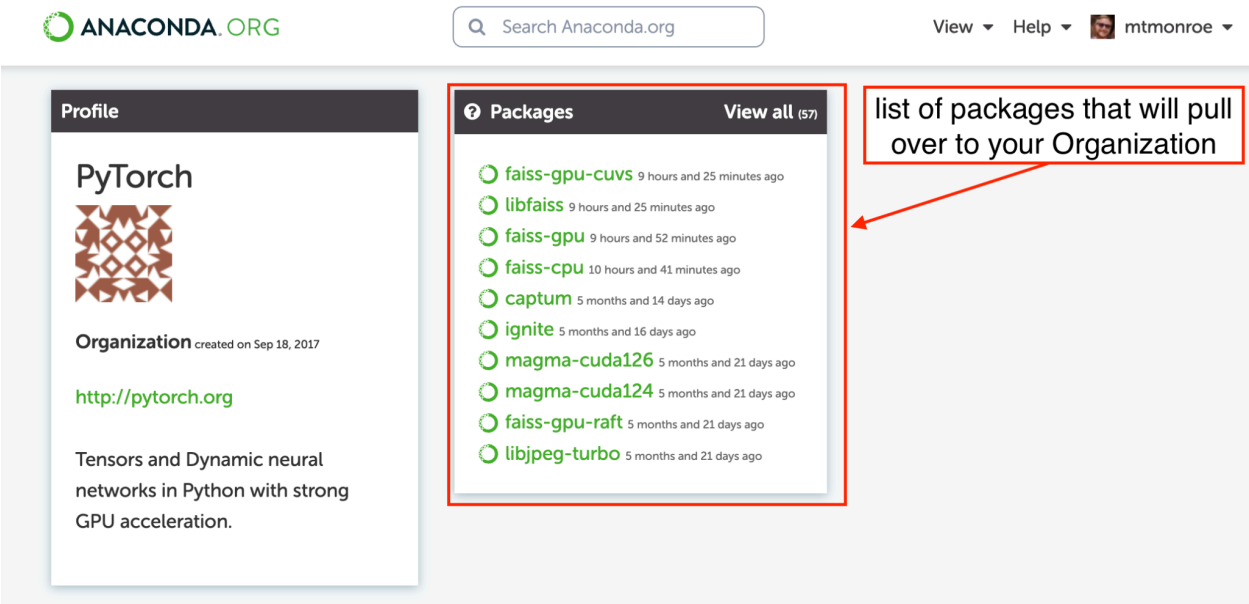


Example: Mirroring the PyTorch Channel

1. Search for “pytorch” on anaconda.org to find the PyTorch channel and related packages.



2. Select the PyTorch channel to view its complete package list.



3. When you mirror this channel to Anaconda Platform Cloud, you'll import all the 57 associated packages.

Hundreds of channels and thousands of packages are available on anaconda.org, but note that these community-owned packages are not vetted or curated by Anaconda.

Important notes:

- No anaconda.org sign-in is required to search packages.
- Private packages require you to sign-in but are a legacy offering no longer supported by Anaconda.
- anaconda.org accounts are separate from Anaconda Platform Cloud accounts.
- The conda-forge channel cannot be mirrored. See **Hosted Channels** for details.

Hosted Channels

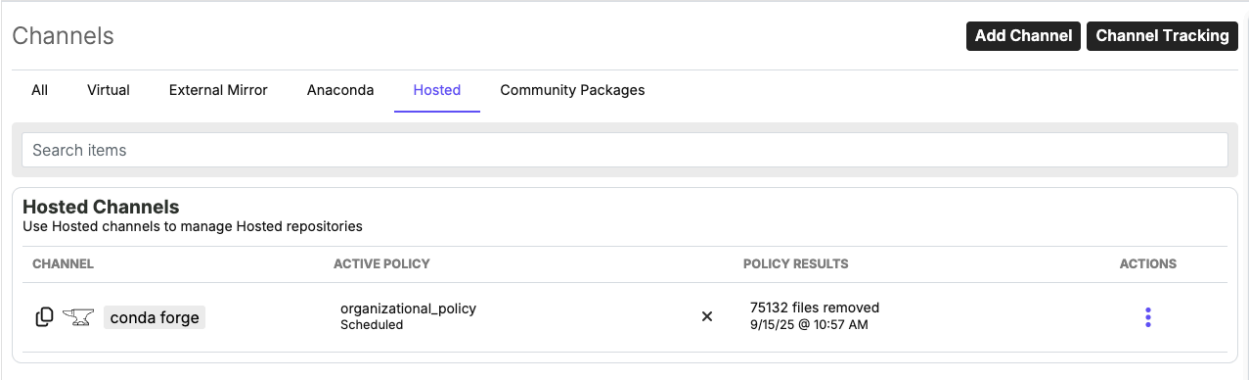
Hosted channels are external channels that mirror large repositories using a redirect method. This approach prevents Anaconda from storing channel data locally, which could slow down the Anaconda Platform Cloud, while allowing URLs to function as if channels originate from our premium repositories. Here's an example: https://repo.anaconda.cloud/repo/conda-forge.

This configuration enables your security teams to block direct network access to anaconda.org while still providing your users access to hosted channels, such as conda-forge, resulting in a unified platform experience.

Requesting Access:

To access the **conda-forge hosted channel**:

1. Contact your Customer Success Manager (CSM) via cs@anaconda.com or support at support.anaconda.com.
2. Access will be provisioned to your individual Anaconda Platform Cloud organization.
3. Once granted, conda-forge will appear under the **Hosted** tab on the Channels page.



Community Channel

The Community Channel expands your organization's package ecosystem by providing secure access to 16,000+ additional open-source packages from conda-forge. These volunteer-maintained packages are integrated into Anaconda's secure pipeline and fully compatible with Anaconda Distribution.

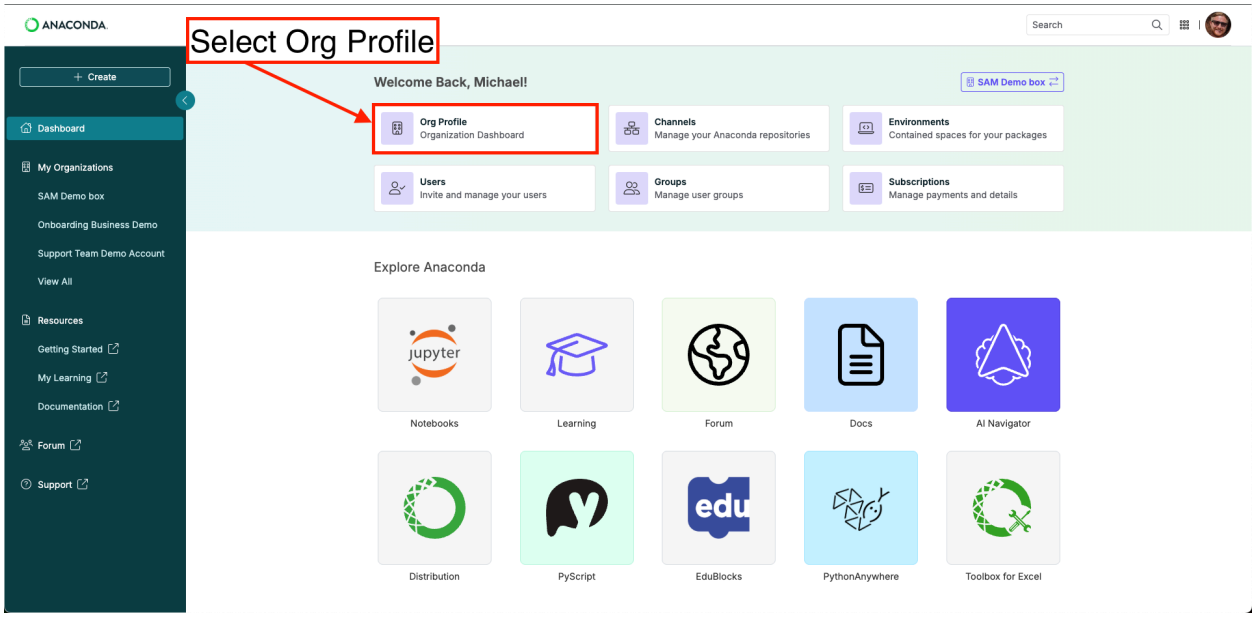
Key Benefits:

- **Maintain Security Standards**: Apply your existing policy filters and organizational security practices across the expanded package ecosystem.
- **Unified Platform Experience**: Access thousands of packages through a single, centralized platform to accelerate AI application development.
- **Eliminate Fragmentation**: Source all packages from one repository instead of managing multiple tools and sources.
- **Controlled Open Source Access**: Transform open source from potential liability into strategic advantage while preserving governance controls.

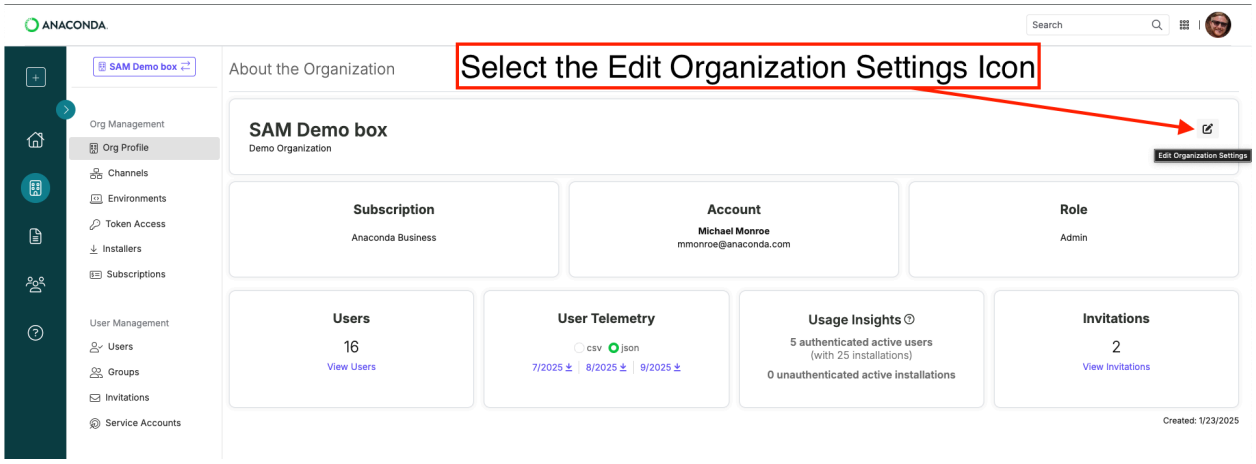
This approach gives your teams significantly broader package access without compromising the governance or secure standards required by your organization.

Enable the Community Channel

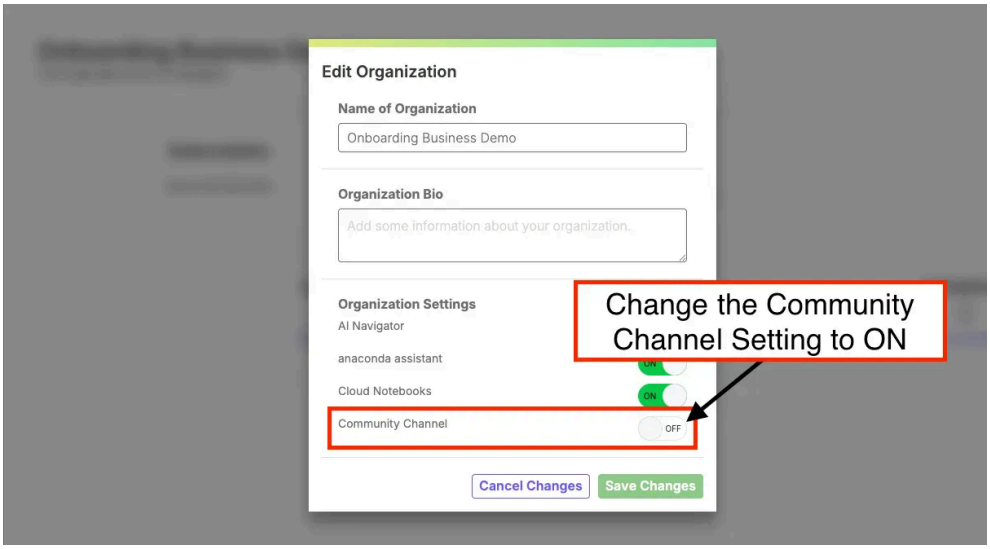
1. Navigate to **Org Profile**.



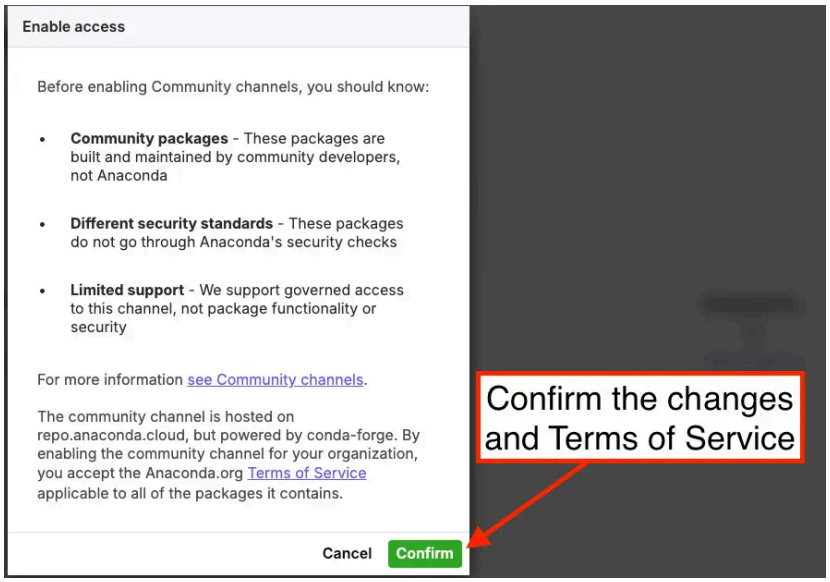
2. Select **Edit Organization Settings** (pen and paper icon) in the top right corner.



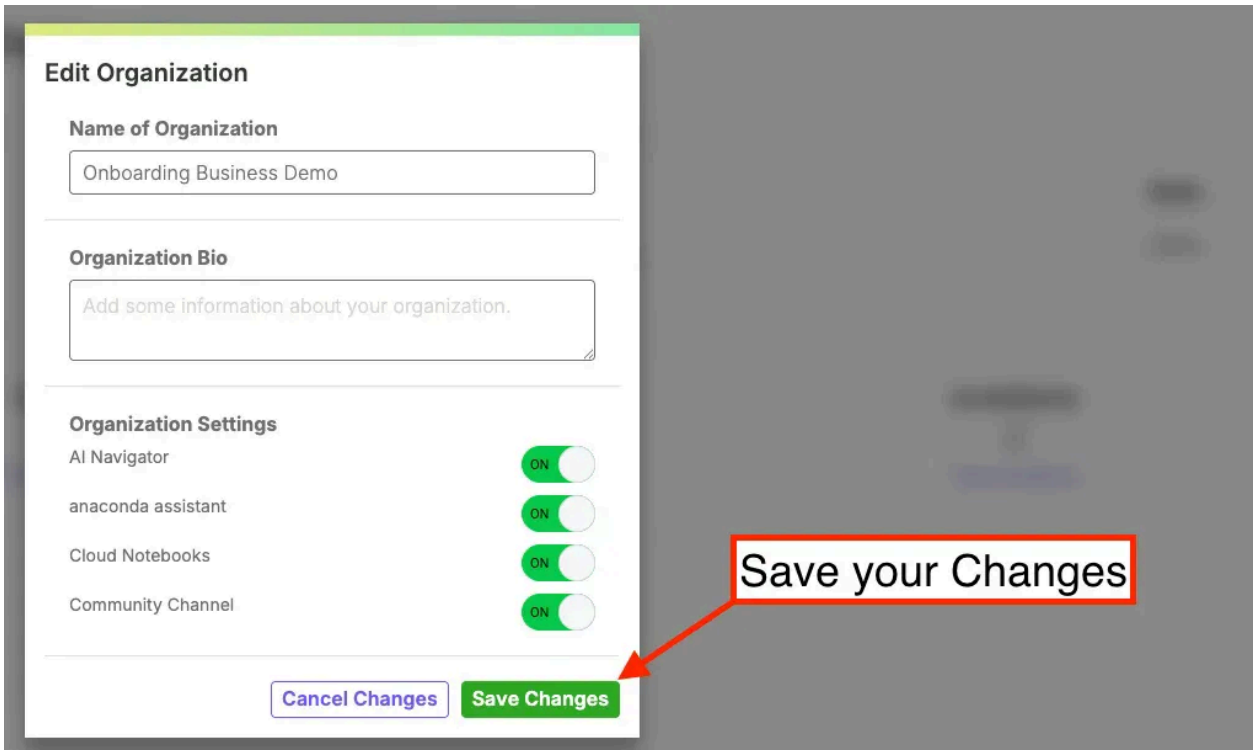
3. In the **Edit Organization** pop-up, scroll to **Organization Settings** and find the **Community Channel** toggle switch (initially set to OFF).



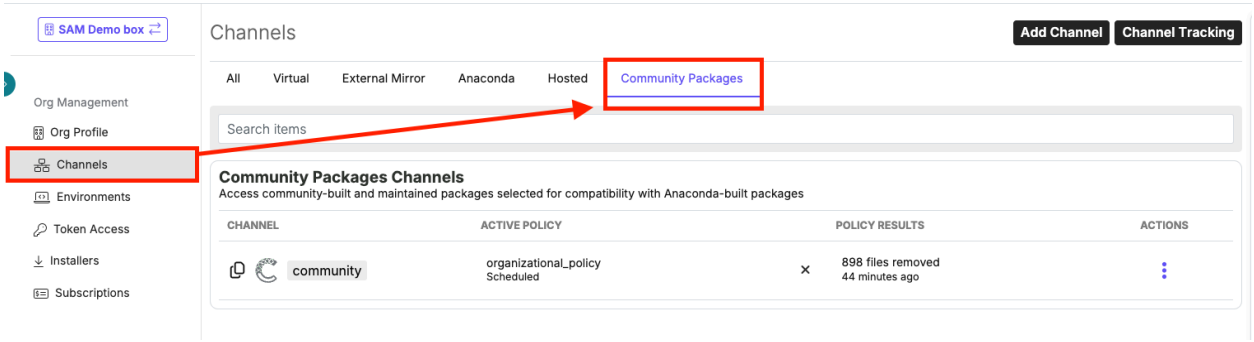
4. Select the toggle switch to turn it from OFF to **ON**.
5. An **Enable Access** pop-up will appear with Community Channel details. Review all information about Community packages, security standards, limited support, and Terms of Service.
6. Select **Confirm** to accept the terms and enable Community Channel access.



7. On selecting Confirm, you'll return to the Edit Organization pop-up where the Community Channel toggle is now set to ON. Click **Save Changes**. The setting will be saved and become active for your organization.



Once enabled, the Community Channel tab will appear on your Channels page.

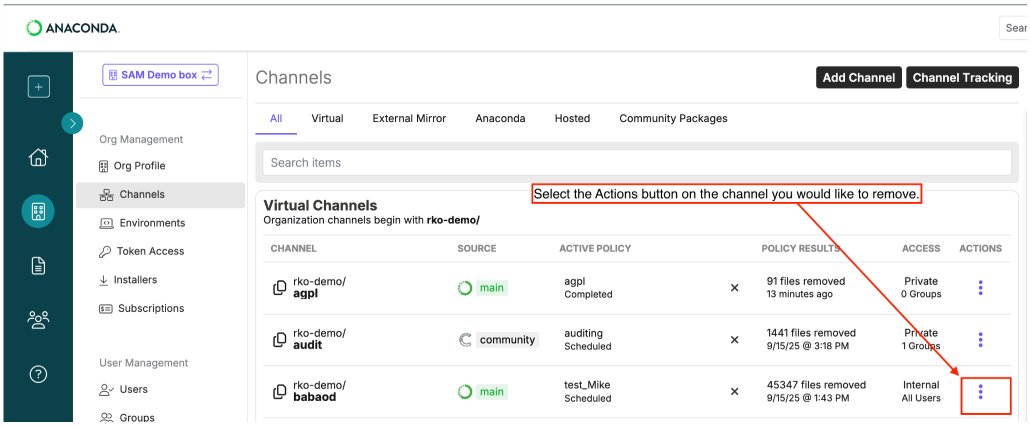


Delete a Channel

You can easily delete Virtual and External channels that you've created using the Actions button (⋮).

To delete a channel

1. Navigate to **Org Profile** > **Org Management** > **Channels**.
2. Locate the channel you want to delete. Select the Actions button (⋮) next to the channel.



3. From the dropdown, select **Delete Channel**.

ANACONDA.

Policies

Policy Filters

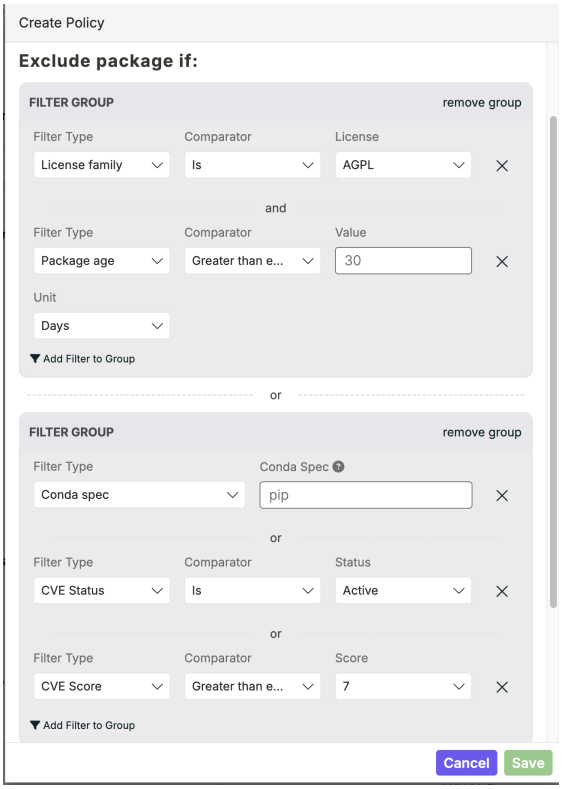
Policy filters provide an additional layer of security and compliance by acting as automated controls that restrict which packages can be accessed from a channel. When configured, they automatically limit package availability to only those meeting your organization's security criteria and compliance requirements, including filtering out specific license types that some organizations must restrict. This eliminates the need for manual admin review when new CVEs are discovered and/or License Family type changes occur on a package.

Anaconda's policy filters can **exclude packages** and **override exclusions and include packages.** Policy filters run every 4 hours, removing or adding any packages in a channel depending on your configured rules.

Policy Filter Parameters

Exclude Package If

Parameters provided by Anaconda for excluding packages include License Family, CVE Score, CVE Status, Conda Spec, Package Age, and Platform:



1. **License Family**
   - Excludes packages with the specified license.
   - Conditions available: “is” and “is not”
   - License families:
     - AGPL
     - APACHE
     - BSD
     - CC
     - GPL
     - GPL2
     - GPL3
     - LGPL
     - MIT
     - MOZILLA
     - None
     - OTHER
     - PSF
     - Public-Domain
2. **CVE Score**
   - Excludes packages with a specified CVE score.
     - Score range: 1-10
     - Conditions available: “Greater than” and “Greater Than or Equal to”
3. **CVE Status**

- Excludes packages associated with a CVE that has the specified status.
- Conditions available: “is” and “is not”
- CVE statuses:
  - Active
  - Reported
  - Mitigated
  - Cleared
  - Disputed

4. **Conda Spec**
   - Uses a rule to exclude a specific package or package version.
     - For example, typing `pip` would remove every version of `pip`. Similarly, typing `python=3.12.8` would remove the Python package version 3.12.8.
   - Refer to this table for further information on the different types of conda spec configurations:

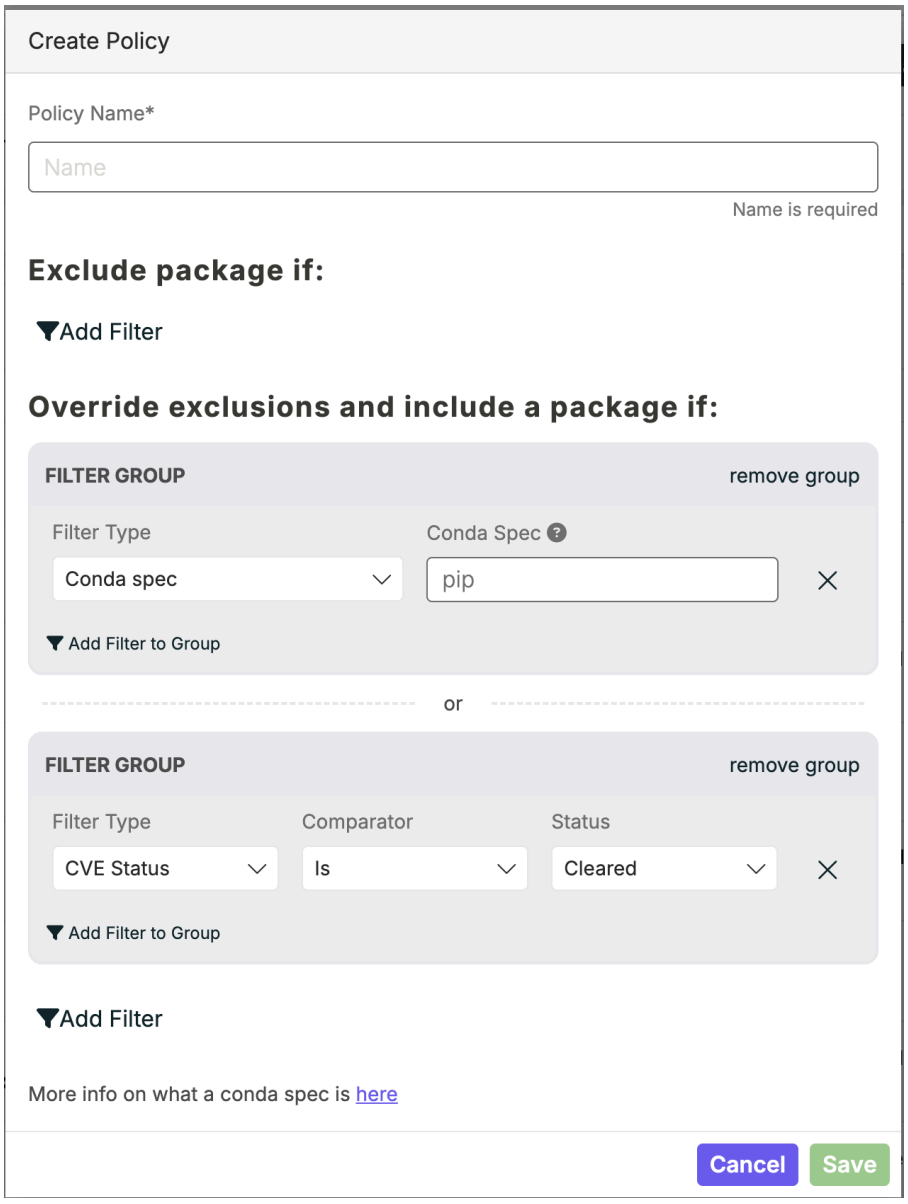
Symbol	Explanation	Example
<, >, <=, >=	Relational operators on versions, compared using PEP-440	<=1.0 matches 0.9, 0.9.1, and 1.0, but not 1.0.1.
==, !=	Relational operators on versions, compared using PEP-440	<=1.0 matches 0.9, 0.9.1, and 1.0, but not 1.0.1.
~=	Yes	~=0.5.3 is equivalent to >=0.5.3, <0.6.0a.
|	OR	1.0|1.2 matches version 1.0 or 1.2.
*	Matches 0 or more characters in the version string (equivalent to regex r'.*')	1.0|1.4* matches 1.0, 1.4, and 1.4.1b2, but not 1.2.

,	AND	>=2,<3 matches all packages in the 2 series. 2.0, 2.1, and 2.9 all match, but 3.0 and 1.0 do not.

5. **Package Age**
    - Excludes packages based on a specified age.
        - Age units: days, months, or years.
        - Conditions available: “Greater than” and “Greater Than or Equal to”
6. **Platform:**
    - Excludes packages from a specified platform.
        - Platforms: Linux, NoArch, Windows, or MacOS
        - Conditions available: “is” and “is not”

Override Exclusions and Include a Package If

Parameters provided by Anaconda for overriding exclusions and including a package comprise Conda Spec and CVE Status:



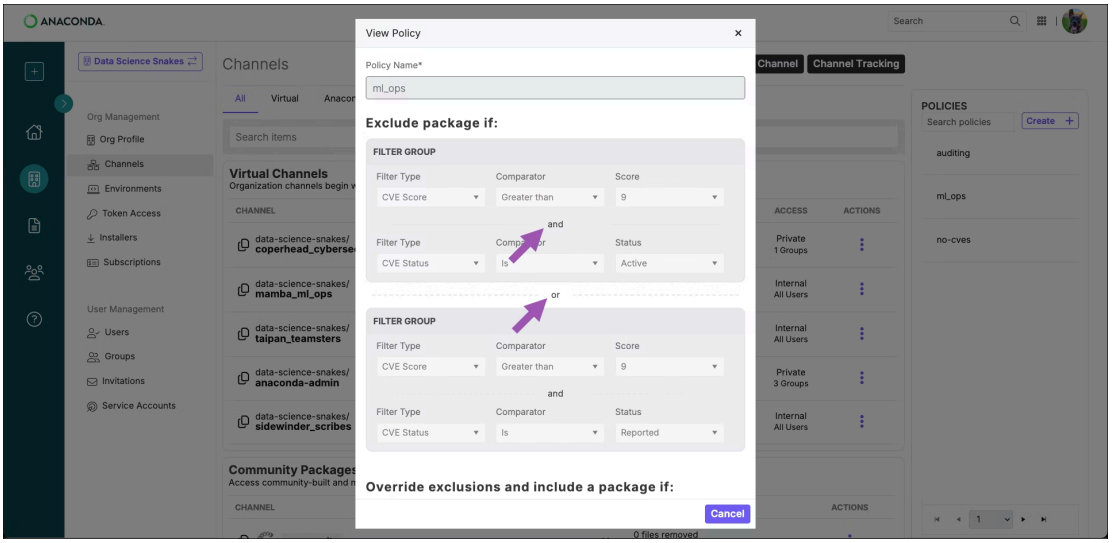
1. **Conda Spec**
    - Uses a rule to override exclusions and include a specific package or package version.
        - For example, typing `pip` would override the exclude filtering process to retain the `pip` package in your channel.
2. **CVE Status**
    - Includes and overrides the exclusion filter for packages associated with a CVE that has the specified status.
    - Conditions available: “is” and “is not”

- CVE statuses:
  - Active
  - Reported
  - Mitigated
  - Cleared
  - Disputed

Understanding Filter Logic

AND/OR Operators

Policy filters can be applied using either **and** or **or**. Click the operator to toggle between AND and OR. This operator significantly impacts which packages are excluded:



How Operators Work

AND Operator

When using **and** between filter conditions, a package must meet **all filter parameters** to be excluded.

Example:
A filter that excludes packages with:

- CVE Score **greater than 9** `and`
- CVE Status **is Active**

This **only excludes** packages that meet **both the conditions, i.e.,** they must have a CVE score of >9 AND have an active CVE status.

`OR` Operator

When using **or** between filter conditions, a package must meet **at least one filter parameter** to be excluded.

Example:
A filter that excludes packages with:

- CVE Score **greater than 9** `or`
- CVE Status **is Reported**

This excludes:

- All packages with a CVE score of >9 (regardless of CVE status)
- All packages with a reported CVE status (regardless of CVE score)

Examples

Example 1: A filter set to exclude packages with a CVE score greater than 7 **and** linux-64 platform excludes only linux-64 packages with a CVE score of >7.

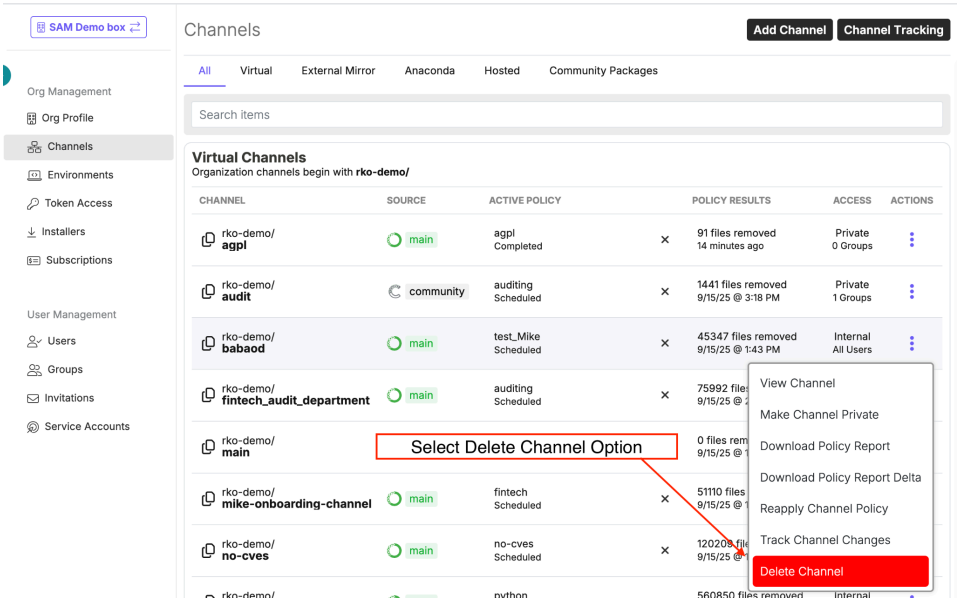
Example 2: A filter that excludes packages with a CVE score greater than 7 **or** linux-64 platform excludes:

- All packages with a CVE score of >7 (regardless of platform)
- All linux-64 packages (regardless of CVE score)

Scenario	AND Logic	OR Logic
CVE Score > 7 and/or **Platform = linux-64**	Excludes only linux-64 packages with CVE score > 7	Excludes ALL packages with CVE score > 7 AND ALL linux-64 packages
Impact	More restrictive (fewer exclusions)	More permissive (more exclusions)

Best Practices

- Use **and** when you want to target packages that meet multiple specific criteria.
- Use **or** when you want to cast a wider net and exclude packages meeting any of several criteria.
- Always test your policy logic to ensure it excludes the intended packages.



4. Confirm to delete the channel permanently.

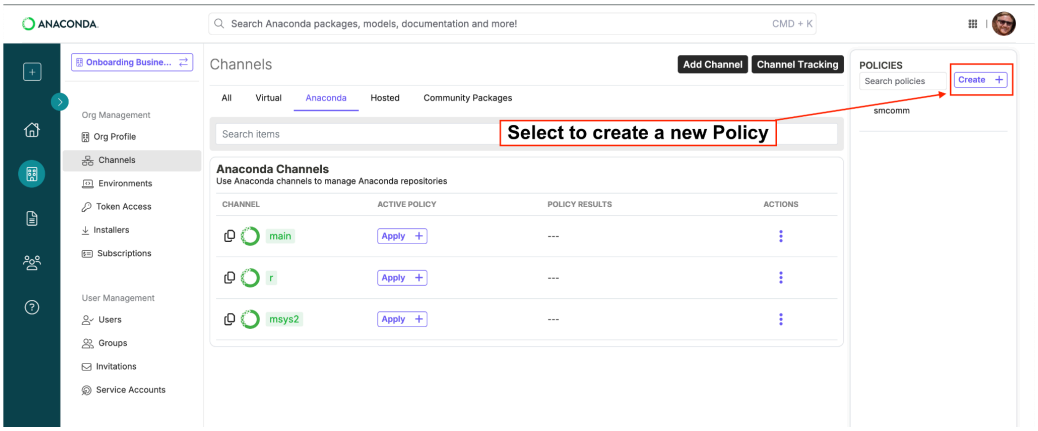
Note: This action permanently deletes the channel and cannot be undone.

Create a Policy

Policies are created using filter groups with AND/OR operators, enabling you to configure your specific criteria.

To create a new policy

1. Navigate to **Org Profile** > **Org Management** > **Channels**.
2. Locate **Policies** on the right:



3. Select **Create +** to start policy creation and define filters.
4. In the **Create Policy** pop-up, configure your policy to decide how you would like to govern your channels:
    - Enter a unique policy name.
    - Define exclusion criteria.
    - Define override exclusion and inclusion criteria.
    - Select **Save**.

All saved policies will appear as a list under Policies on the right.

Note: By creating policies and specific filters, you can define security and governance rules that will automatically filter packages from your channels based on package vulnerability, license compliance, platform, and/or package age. For more information on filter parameters, refer to Policy Filter Parameters.

Example 1: Vulnerability-Based Package Filtering (CVEs)

1. As evident from Image 1, *organizational_policy* excludes packages that meet either of these conditions:
    - Filter Group 1: CVE Score > 9 **AND** CVE Status = Active **OR**
    - Filter Group 2: CVE Score > 9 **AND** CVE Status = Reported
    - Select **Save**.

This configuration means any package with a critical vulnerability (CVE score > 9) that is either actively being exploited or has been reported will be automatically excluded.

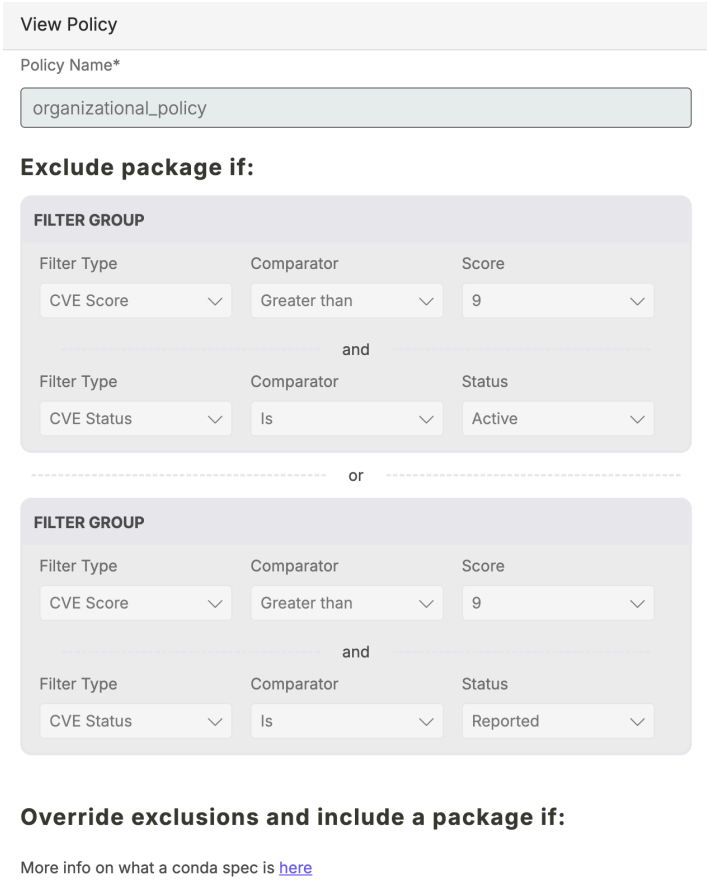


Image 1

2. Once the policy has been saved and applied to a channel (see Apply a Policy to learn how to apply a policy), it runs and updates every 4 hours (Image 2). As a result of the filters defined above:
    - **Hosted Channels** (e.g., conda-forge): 75,320 files removed
    - **Community Packages Channels** (e.g., community): 912 files removed
    - **Anaconda Channels** (e.g., main): 26,466 files removed

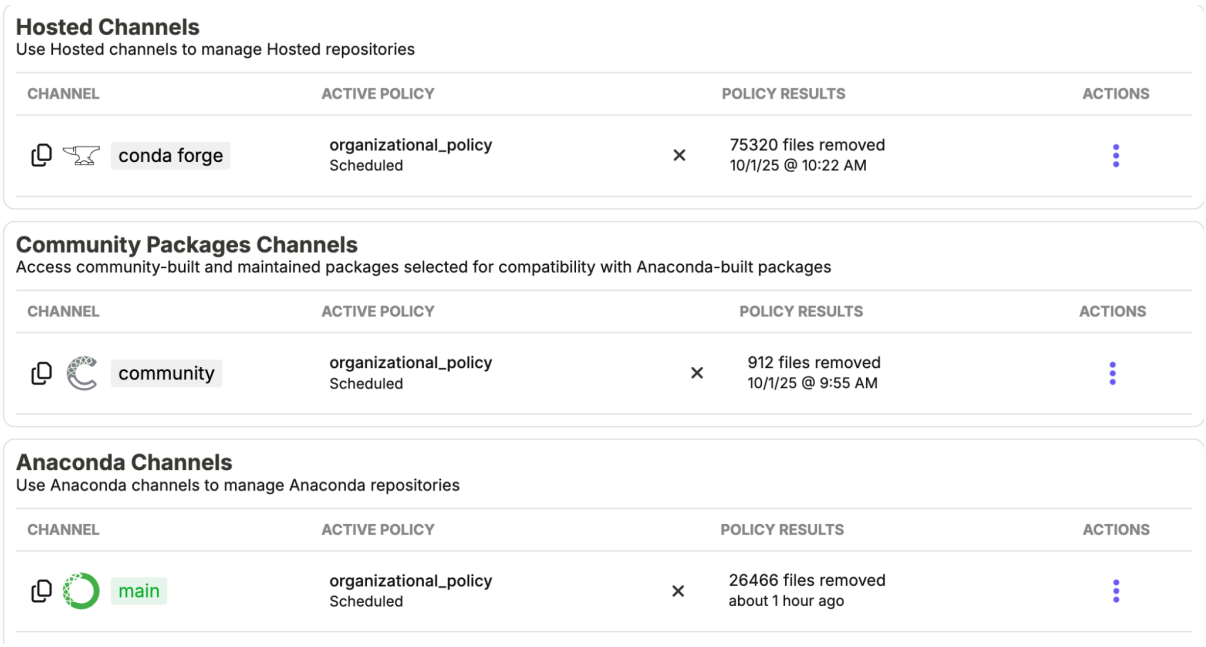


Image 2

3. The **Policy Results** column displays the impact of your governance rules, showing how many files were removed and when the policy last ran, giving you visibility into your organization's security posture.

Example 2: License-Based Package Filtering

In addition to security-based filtering, you can create policies that enforce license compliance requirements for your organization.

1. As evident from Image 3, *agpl* is configured with a simple exclusion criteria:
    - Under Exclude packages if, select **License family** is **AGPL**.
    - Select **Save**.

This configuration will automatically exclude all packages with AGPL licensing, which is commonly restricted in enterprise environments due to its viral copyleft requirements that can impact proprietary code.

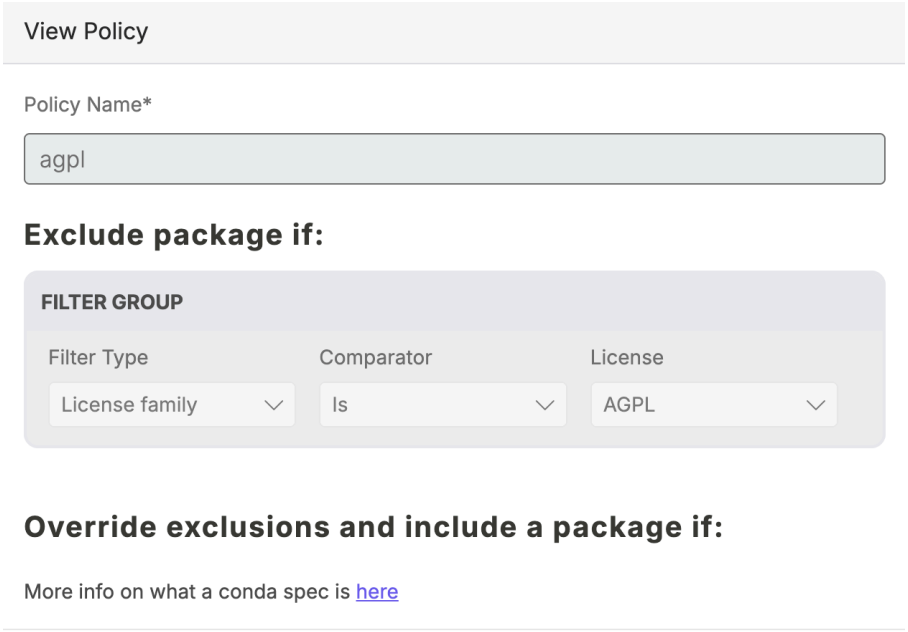


Image 3

2. **Optional: Override exclusions and include a package if** allows you to create exceptions to your exclusion criteria.
3. As evident from Image 4, on applying the *agpl* policy to the rko-demo/agpl virtual channel, 91 files were removed (i.e., packages with AGPL license).

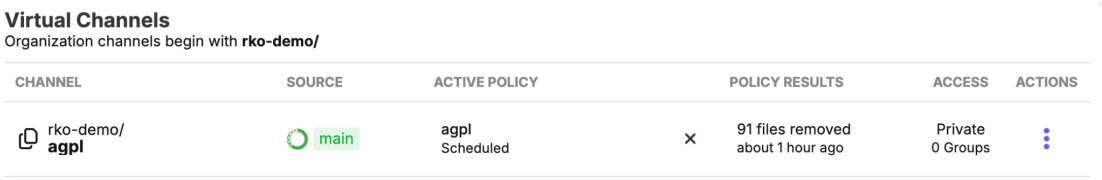


Image 4

This ensures your organization maintains license compliance by preventing developers from accidentally introducing packages with incompatible licensing terms into your environment.

Example 3: Platform-Based Package Filtering

You can also create policies that enforce platform architecture requirements for your organization.

1. As evident from Image 5, *windows64only* is configured to exclude packages that do not meet the below criteria:
    - Filter Group 1: Platform type is not win-64 (Windows 64) **OR**
    - Filter Group 2: Platform type is not NoArch
    - Select **Save**.

This configuration will automatically exclude all packages that aren't a "win-64" or "noarch" package from your channels.

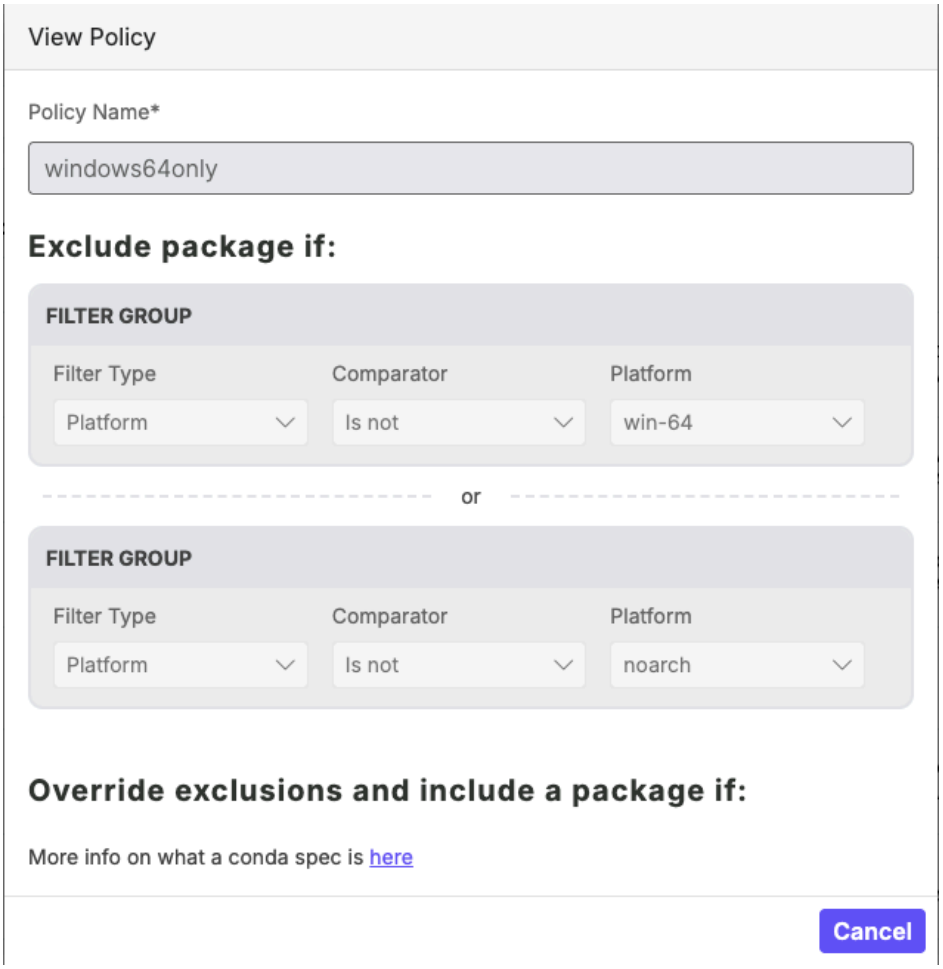


Image 5

2. As evident from Image 6, on applying this policy to the data-science channel, 571793 packages were removed.

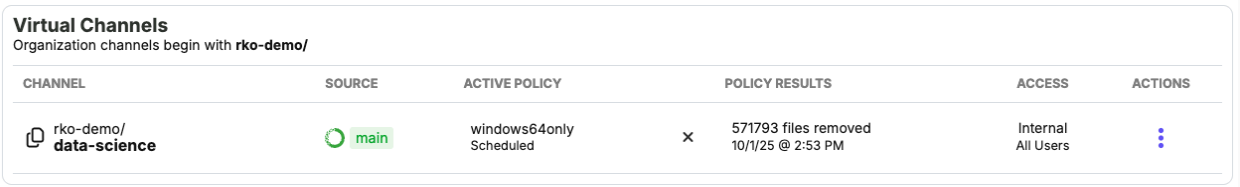


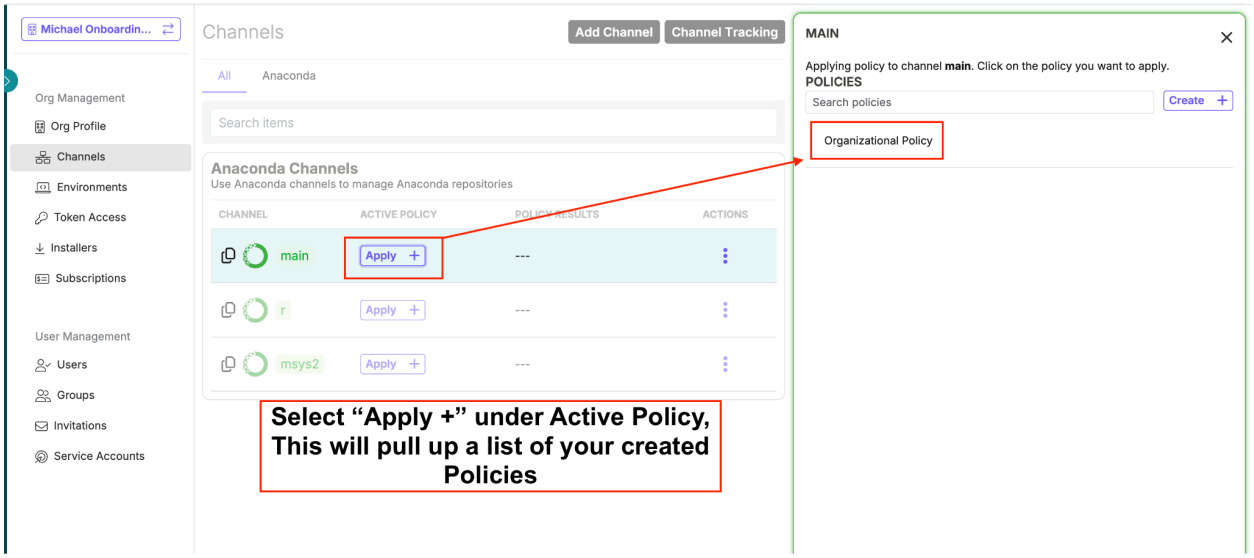
Image 6

Apply a Policy

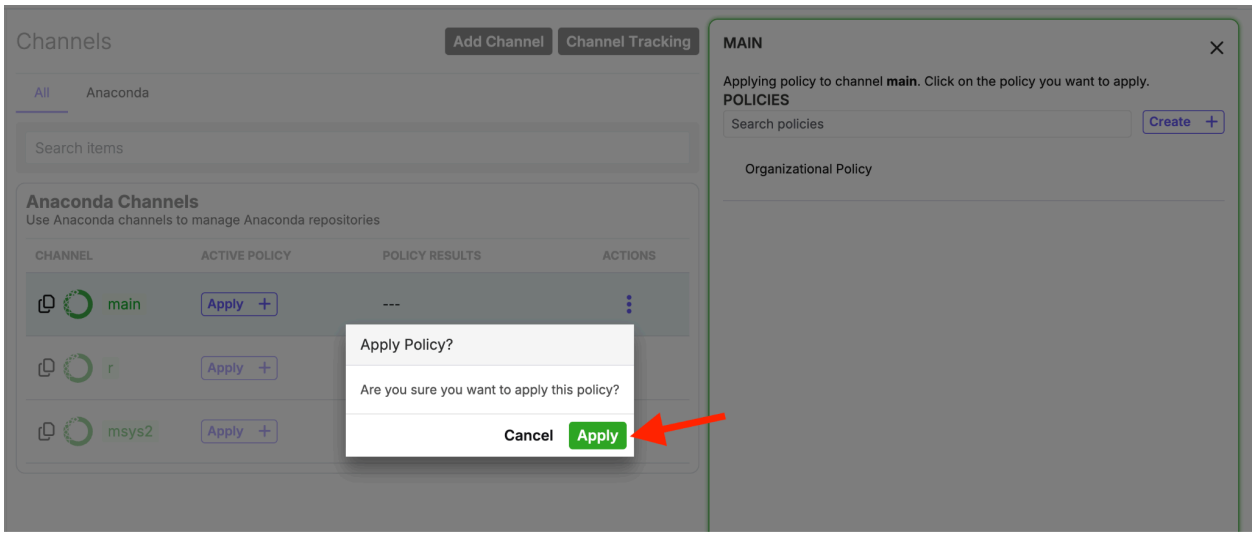
Once you've created a policy, you're ready to apply it to channels.

To apply a policy

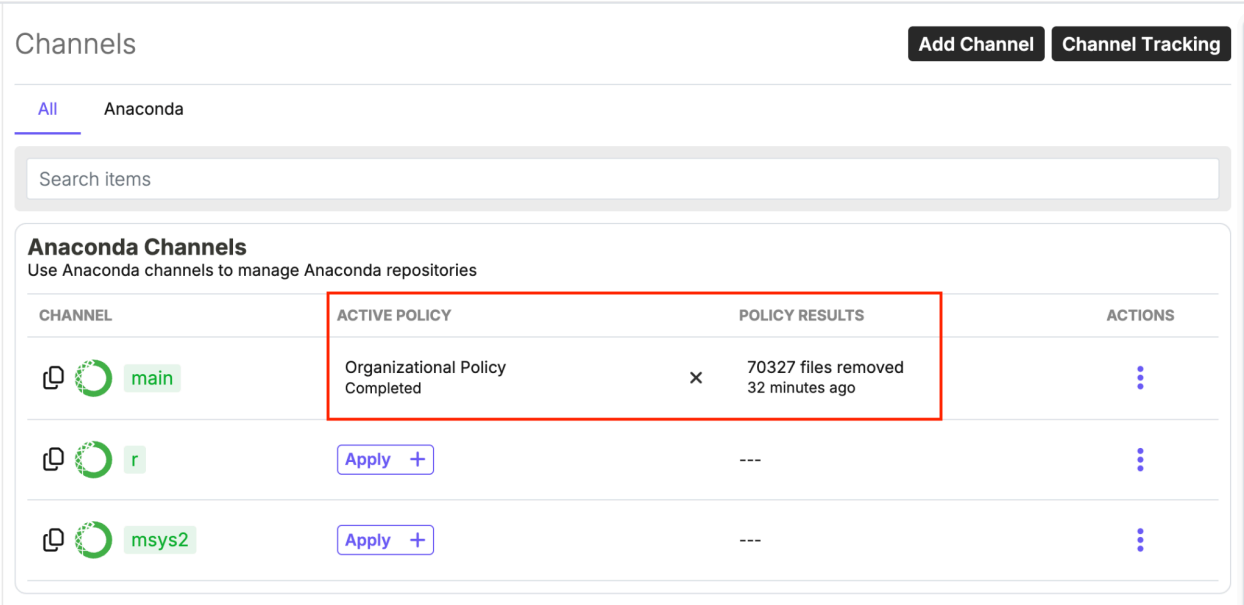
1. Navigate to **Org Profile** > **Org Management** > **Channels**.
2. Locate **Policies** on the right. Under Policies, you'll see a list of policies you've created and saved.
3. As an example, let's apply *Organizational Policy* (filters: exclude packages with CVE score greater than or equal to 7 and CVE status = Active **OR** CVE score greater than or equal to 7 and CVE status = Reported) to Anaconda's **main** channel. Select **Apply +** under the **Active Policy** column:



4. In the **Apply Policy** pop-up, select **Apply**.



5. Allow the policy to run. This may take some time depending on the filtering criteria.
6. Once the policy has been applied, you'll see the results under the **Policy Results** column. As evident below, on applying *Organizational Policy*, 70327 files were removed.



Notes:

1. Policy filters run every 4 hours, removing and adding packages based on your configurations.

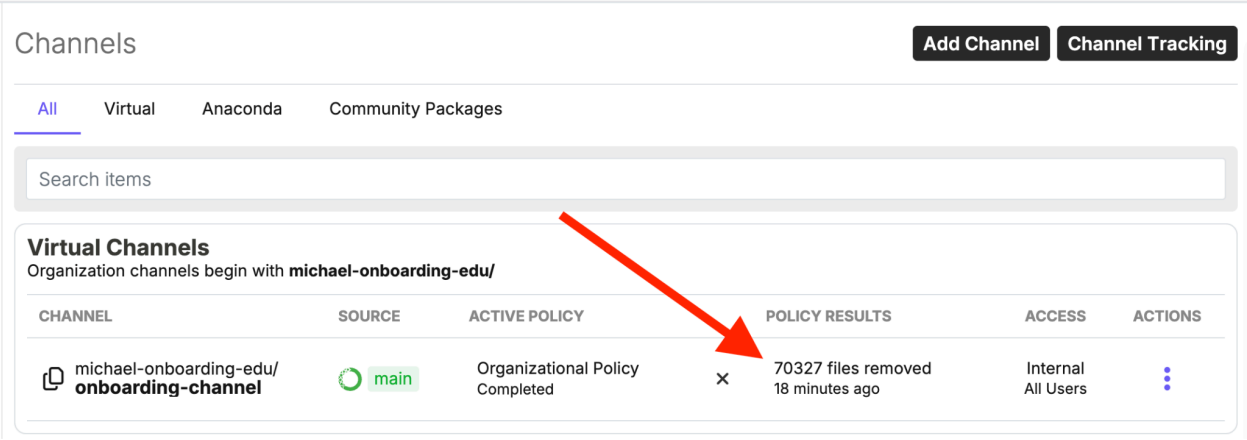
2. You *cannot* edit or delete a policy that has already been applied to a channel. If you need to modify a policy, first remove it from all the channels you've applied it to, and then edit or delete the policy. Alternatively, you can create a new policy and apply it to your channel(s).

Policy Results

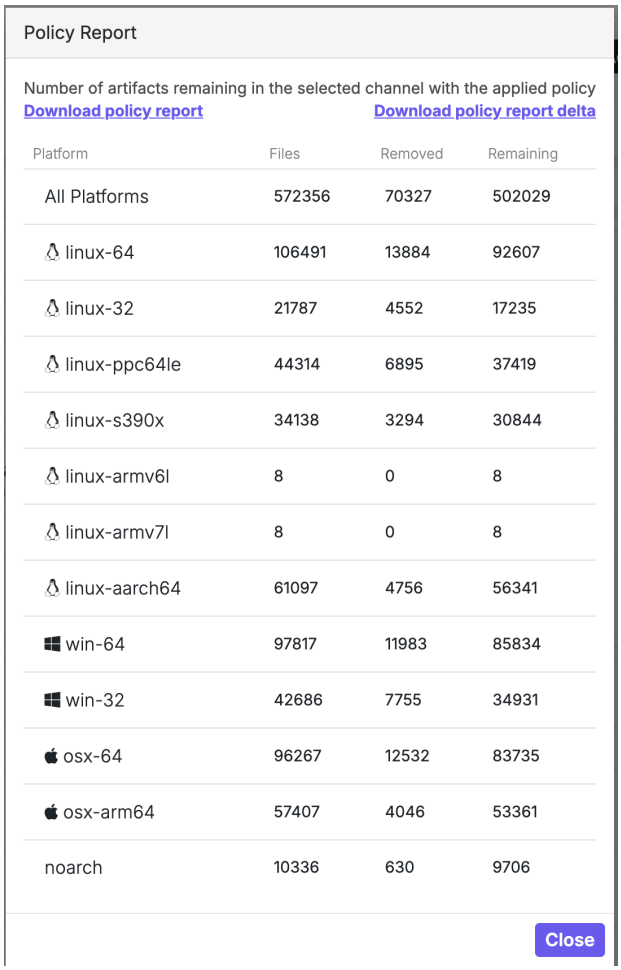
Now that you know how to create and apply a policy, let's learn how to examine policy filtering results.

View Policy Results

1. Navigate to **Org Profile** > **Org Management** > **Channels**.
2. Under Channels, start by selecting the number of files removed under **Policy Results** for a channel.



3. You'll see **Policy Report**, which shows the results for the files removed and the different platforms these files were removed from.

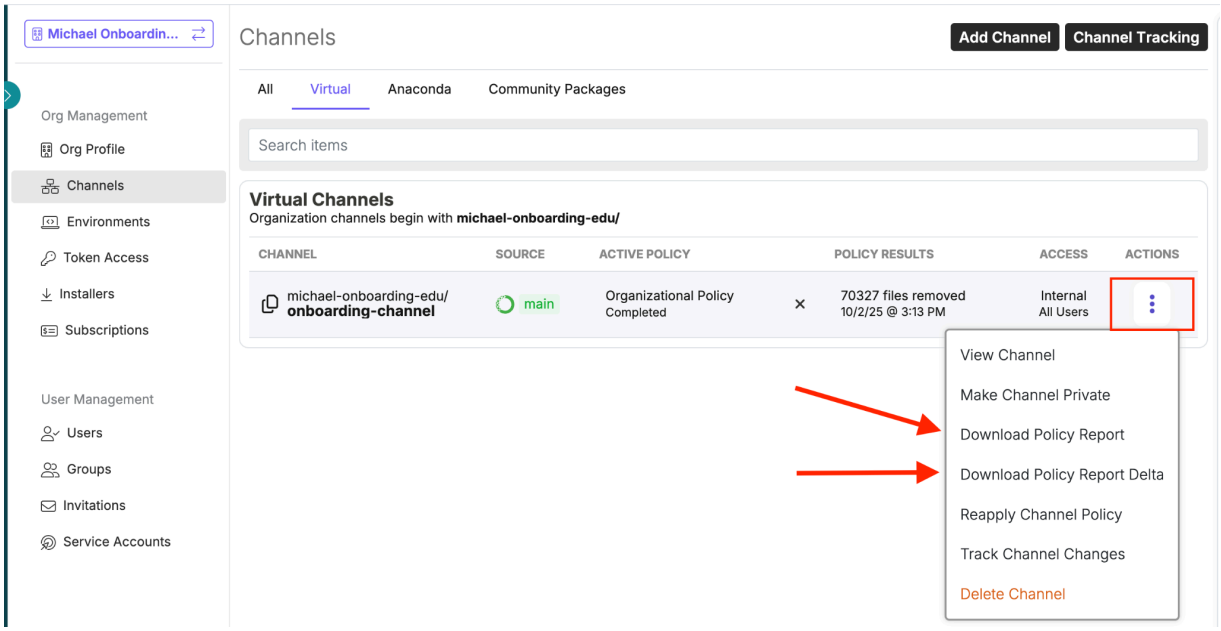


Policy Report

Policy Report helps you see a breakdown of all the packages removed from your channel due to the policy you have enforced.

To download the policy report

1. Select the ⋮ icon under the **Actions** column for a particular channel.
2. From the dropdown menu, select **Download Policy Report**.



3. This downloads a CSV file containing the policy name, the last execution date and time, the next scheduled execution date and time, and details related to the removed packages.

policy_name	last_executed	next_scheduled_at	removed_package	file_removed_reason
Organizational Policy	2025-10-02 20:03:36.960856+00:00	2025-10-03 00:13:23.991330+00:00	pillow-5.1.0-py35h3deb7b8_0.tar.bz2	CVE score of 7.5 is greater than or equal to 7 and CVE status is 'active'
Organizational Policy	2025-10-02 20:03:36.960856+00:00	2025-10-03 00:13:23.991330+00:00	tensorflow-base-1.11.0-eigen_py27h4dcebc2_0.tar.bz2	CVE score of 7.5 is greater than or equal to 7 and CVE status is 'active'
Organizational Policy	2025-10-02 20:03:36.960856+00:00	2025-10-03 00:13:23.991330+00:00	pillow-8.0.0-py38h9a89aac_0.tar.bz2	CVE score of 8.8 is greater than or equal to 7 and CVE status is 'active'
Organizational Policy	2025-10-02 20:03:36.960856+00:00	2025-10-03 00:13:23.991330+00:00	tensorflow-base-1.6.0-py27hdbcaa40_1.tar.bz2	CVE score of 7.5 is greater than or equal to 7 and CVE status is 'active'
Organizational Policy	2025-10-02 20:03:36.960856+00:00	2025-10-03 00:13:23.991330+00:00	libcurl-7.65.2-h20c2e04_0.tar.bz2	CVE score of 9.8 is greater than or equal to 7 and CVE status is 'active'
Organizational Policy	2025-10-02 20:03:36.960856+00:00	2025-10-03 00:13:23.991330+00:00	tensorflow-base-1.9.0-gpu_py35h9f529ab_1.tar.bz2	CVE score of 7.8 is greater than or equal to 7 and CVE status is 'active'

Policy Report Delta

Once a policy is applied to a channel, it automatically runs every 4 hours. During these scheduled runs, your channel's contents may change due to newly reported licensing changes, CVEs, or updates to existing CVE scores or statuses.

You can track such changes using two methods:

Method 1: Via the Main Channels Page

Note: Policy Deltas can be viewed only when a policy has run more than once and if the results between these runs differ.

1. On the **Channels** page, select the ⋮ icon under the **Actions** column for a particular channel.

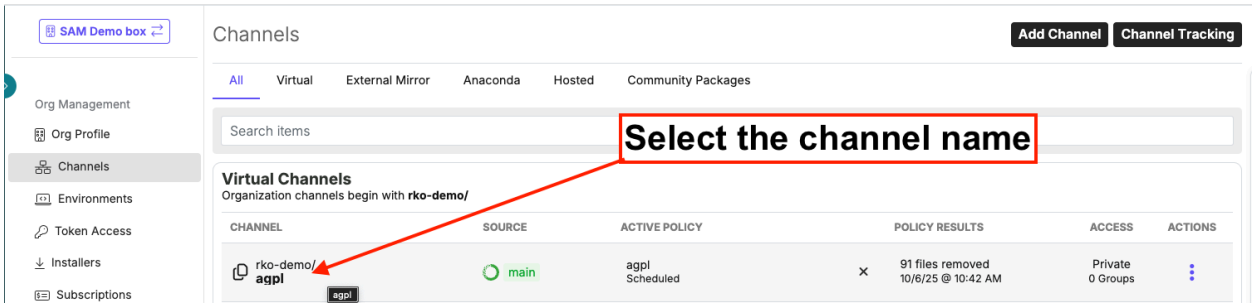
2. From the dropdown menu, select **Download Policy Report Delta** to download a CSV file.

rko-demo_agpl-policy-report delta

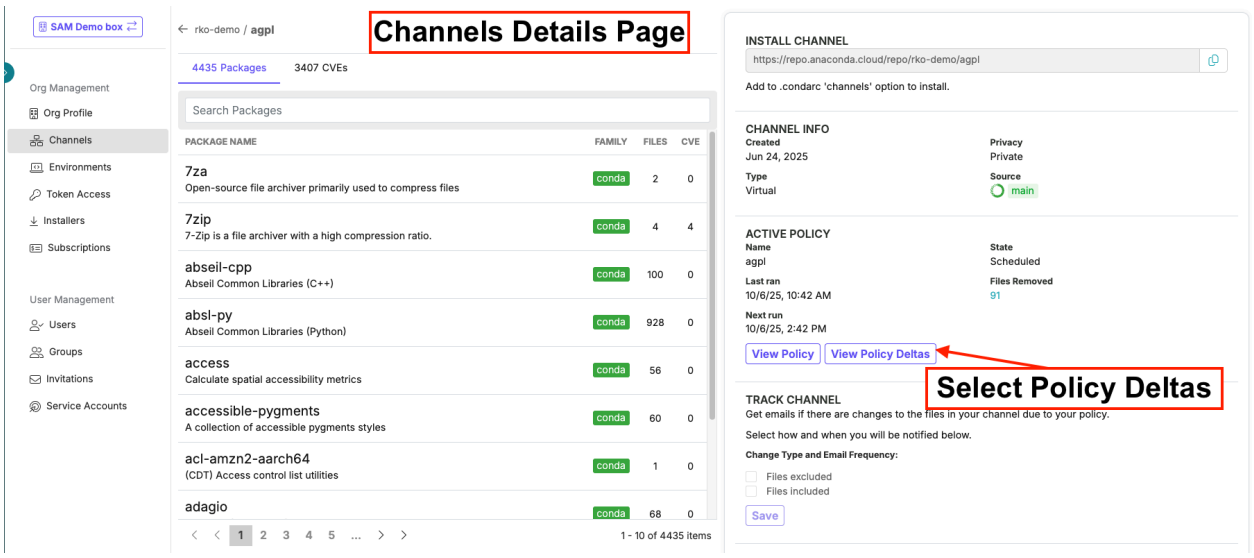
type	platform	artifact_name	why
added	osx-64	pdoc3-0.11.6-py312hecd8cb5_0.tar.bz2	License family 'AGPL' is 'AGPL'
added	osx-64	pdoc3-0.11.6-py311hecd8cb5_0.tar.bz2	License family 'AGPL' is 'AGPL'
added	osx-64	pdoc3-0.11.6-py313hecd8cb5_0.conda	License family 'AGPL' is 'AGPL'
added	osx-64	pdoc3-0.11.6-py311hecd8cb5_0.conda	License family 'AGPL' is 'AGPL'

Method 2: Via Channel Details

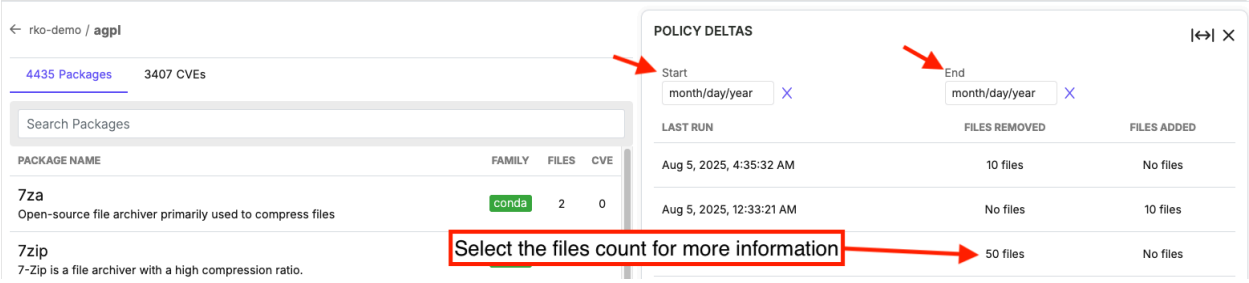
1. On the **Channels** page, select a channel of choice to view additional information and the list of packages in that channel.



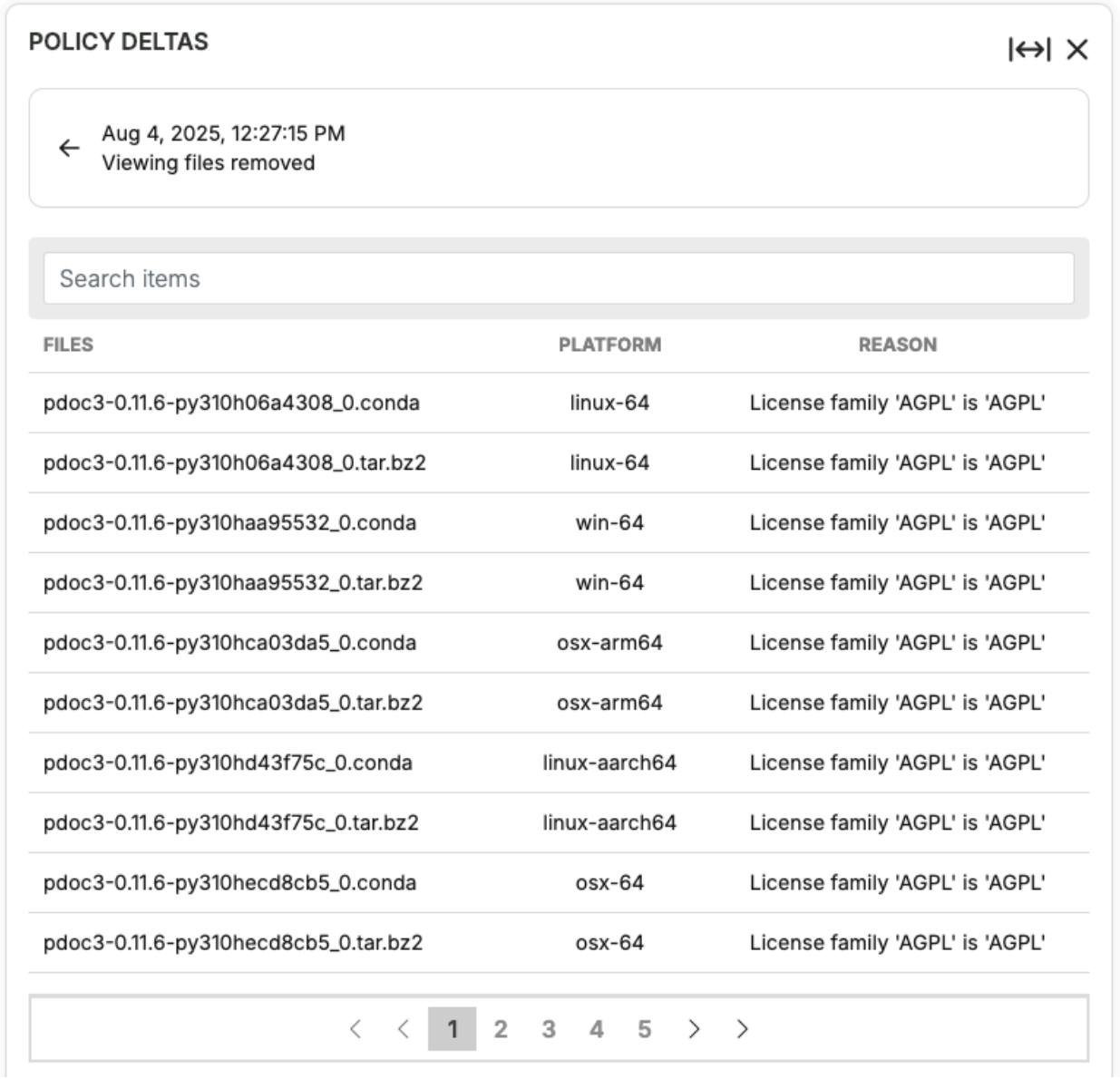
2. On the details page for that channel, select **View Policy Deltas**.



3. You'll now see details regarding the past runs, along with the number of files removed and added. Policy Delta History begins from when you first apply a policy to a channel. Note that once a policy is removed or edited, the history is erased.



4. Use **Start** and **End** date filters under **Policy Deltas** to adjust your search duration to view a specific delta report.
5. When viewing Policy Deltas, you can select the number of files under **Files Removed** or **Files Added** to see more details.



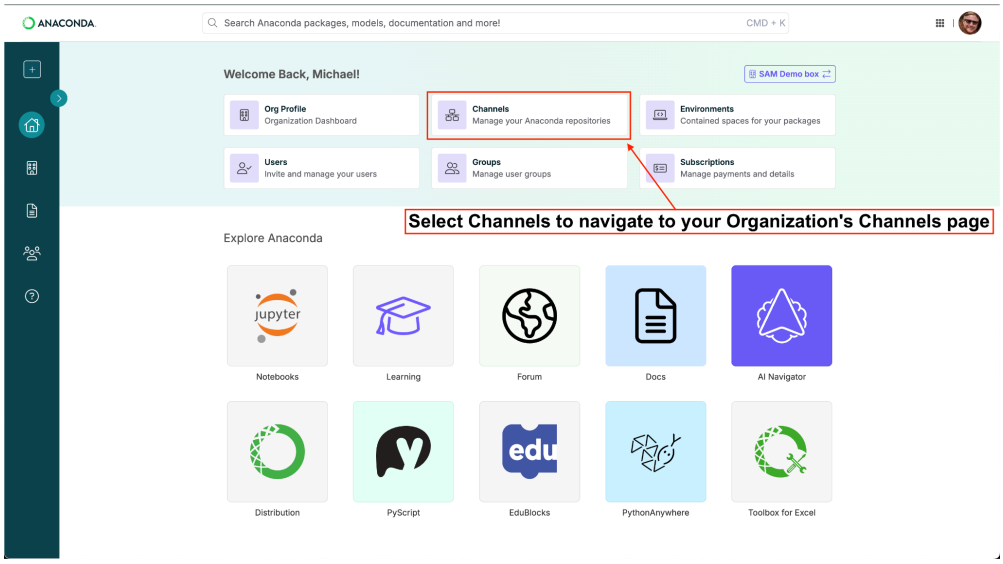
Channel Tracking

Through Channel Tracking, you can receive email notifications whenever channels with active policy filters are updated. You'll receive alerts when your policy filter settings add or remove packages from a tracked channel.

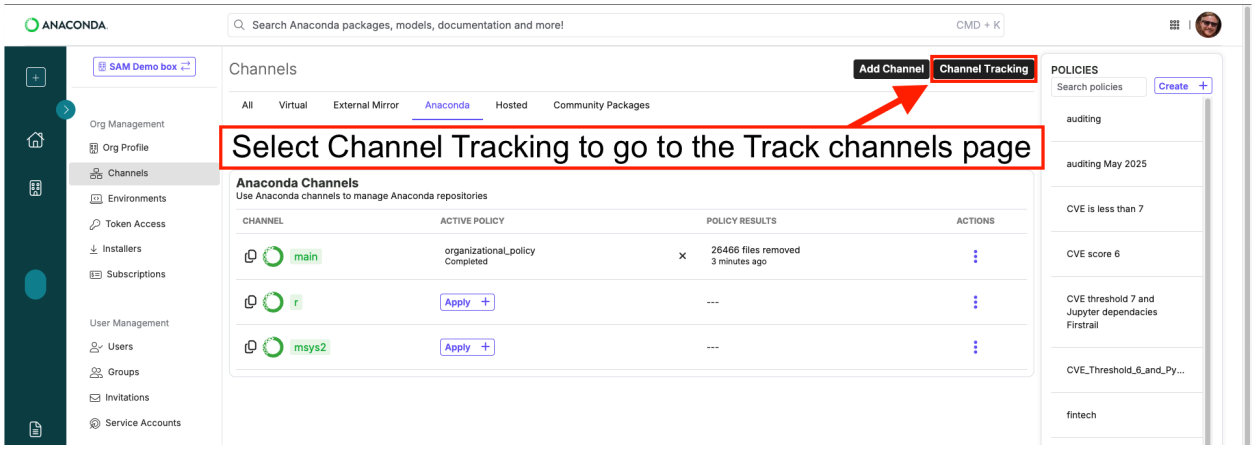
Note: You must have an active policy filter on a channel before you can enable Channel Tracking.

Enable Channel Tracking

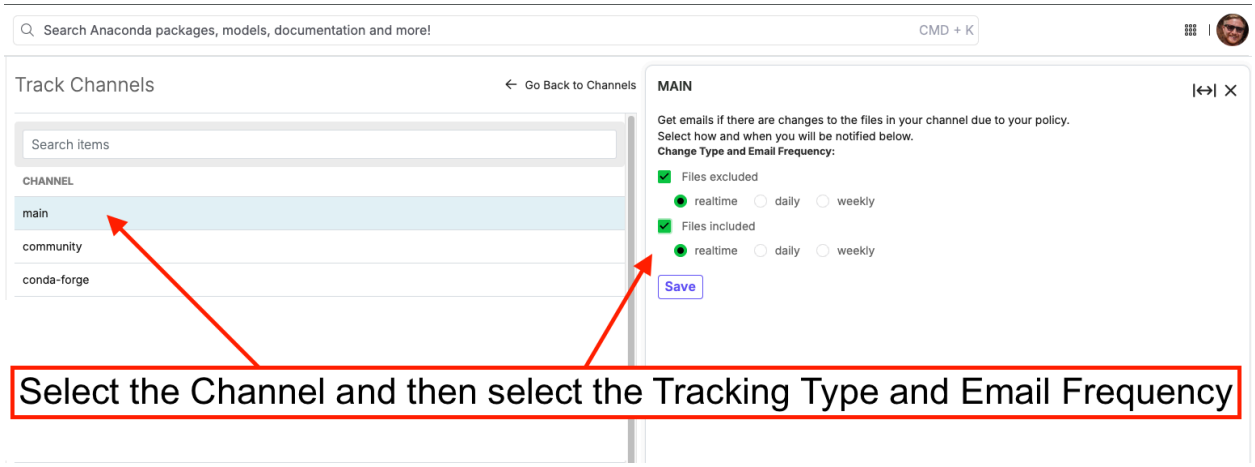
1. Navigate to **Org Profile** > **Org Management** > **Channels**. Alternatively, select Channels on your dashboard to directly go to the Channels page.



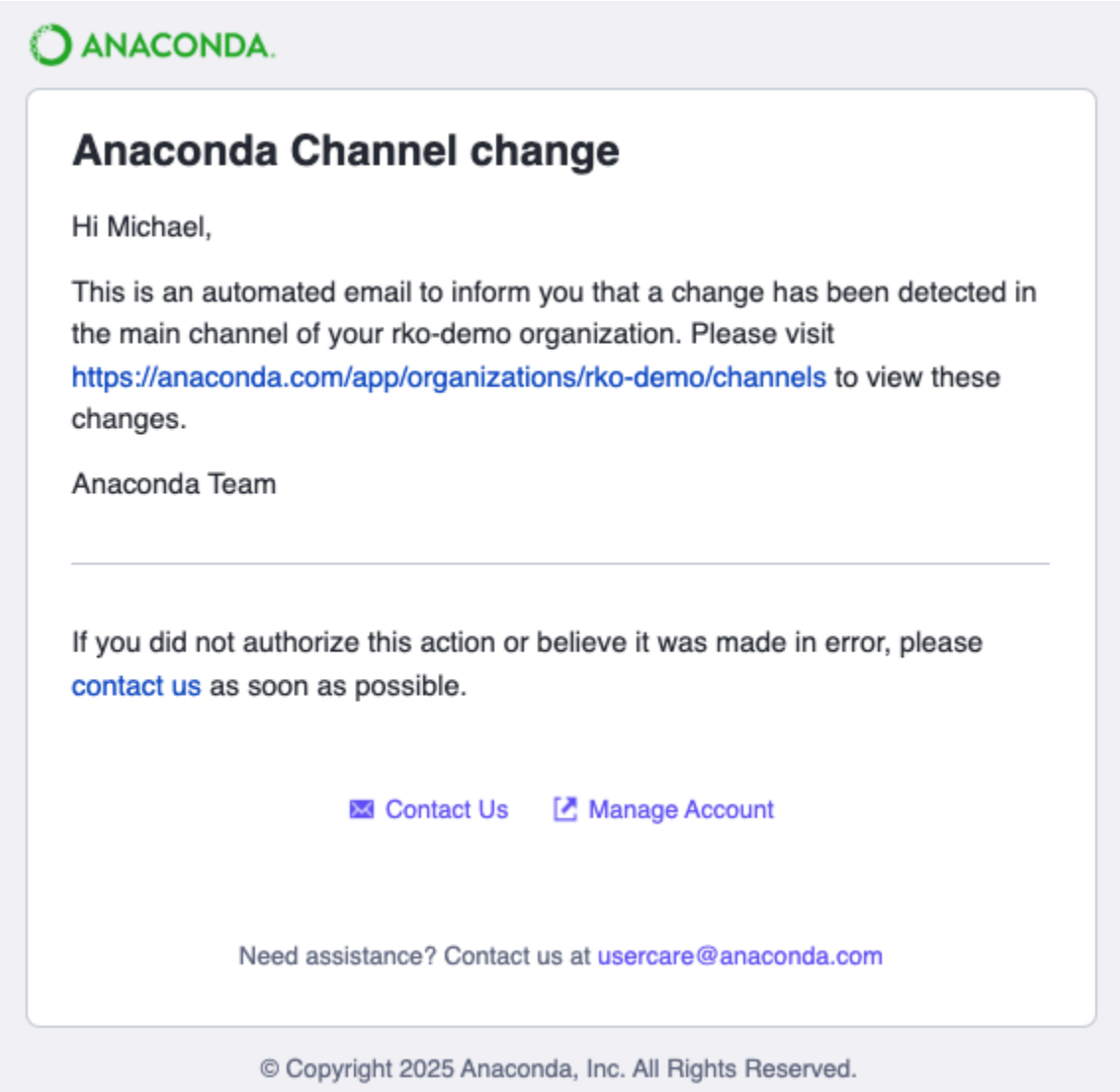
2. Now select **Channel Tracking** in the top right corner to open the **Track Channels** page. This page shows you a list of all channels with an active policy filter. In other words, these are the channels available for tracking.



3. Select a channel from the list, choose which email notifications you'd like to receive (files excluded and/or files included in your channel based on your policy filters), and set how frequently you want them delivered (real-time, daily, or weekly).
    - **Notes:**
        i. You'll receive emails only when changes actually occur due to your policy filters.
        ii. **Real-time** sends you an email immediately after a change is detected. Considering that policy filters run every 4 hours, you'll receive at most 1 email every 4 hours.
        iii. **Daily** sends an email once per day when a change is detected.
        iv. **Weekly** sends an email every Friday when a change is detected.



4. After selecting your preferences, select **Save**.
5. Here's what an email notification looks like:



ANACONDA.

Anaconda Channel change

Hi Michael,

This is an automated email to inform you that a change has been detected in the main channel of your rko-demo organization. Please visit https://anaconda.com/app/organizations/rko-demo/channels to view these changes.

Anaconda Team

If you did not authorize this action or believe it was made in error, please contact us as soon as possible.

Contact Us Manage Account

Need assistance? Contact us at usercare@anaconda.com

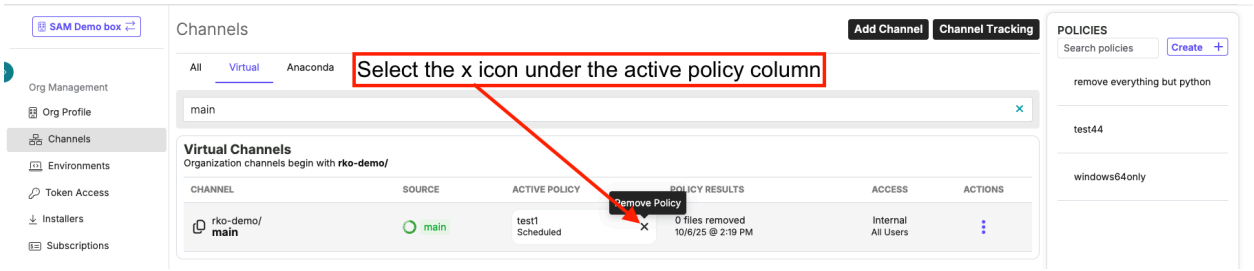
- Selecting the link in this notification email will take you to your organization's Channels page. From there, you can access the channel mentioned in the notification email (“main” channel in this example) and Download Policy Report Delta for detailed information about which packages were added or removed based on your policy filters.

Delete a Policy

Prerequisite: To delete a policy, you must first remove it from all channels you've applied it to.

Remove a Policy from Channels

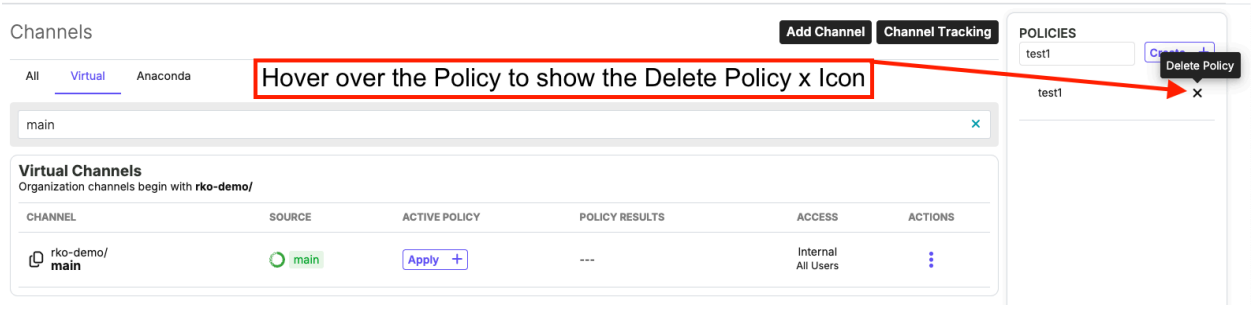
1. Navigate to the **Channels** page.
2. Locate the channels you've applied the policy to.
3. To remove the policy from a channel, select the **X** icon to the right of the policy name.



4. In the **Remove Policy** pop-up, select **Remove**.
5. Repeat this step, if needed, for all channels using the policy.

Delete the Policy

1. Once the policy is no longer applied to any channels, navigate to **Policies** on the right side of the **Channels** page.
2. Hover over the policy you want to delete—an **X** icon will appear.
    - **Note:** The **X** icon only appears if the policy is not currently applied to any channels (refresh the page in case you cannot see this icon).
3. Select the **X** icon to permanently delete the policy.



Note: This action cannot be undone. Once deleted, the policy and all its configuration settings will be permanently removed.

Packages

Anaconda Packages: Overview

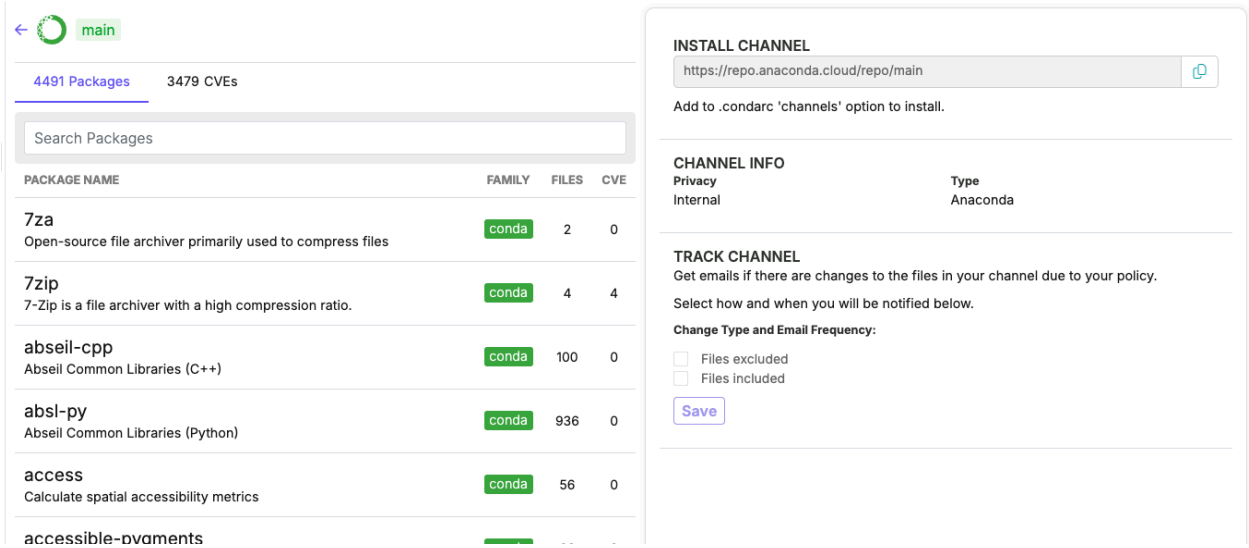
Anaconda Packages are pre-built software libraries and tools distributed through Anaconda's package repository. They contain popular data science, machine learning, and scientific computing libraries, such as NumPy, pandas, and TensorFlow, that have been compiled, tested, and optimized to work seamlessly together.

Unlike building software from source code, Anaconda Packages are ready to install and use immediately with **conda**, i.e., Anaconda's package manager. Each package includes the library itself as well as all its dependencies, ensuring compatibility across operating systems (Windows, macOS, and Linux). This eliminates the common "it works on my machine" problem and simplifies environment reproducibility across teams.

Anaconda Packages are curated and maintained to deliver reliable, stable versions of essential tools, enabling data scientists, analysts, and developers to focus on their work rather than troubleshooting installation issues.

Channel and Package Details

The **Channel Details** page on the Anaconda Platform Cloud (to view this page, navigate to **Org Management**, then **Channels**, and then select a channel of choice) provides comprehensive information related to packages, including CVEs, Anaconda curation reviews, SBOMs, licensing details, package dependencies and dependants, and file-level metadata.



Channel Overview

This page displays

- Total number of packages in a channel,
- Total number of CVEs across all packages,
- Installation instructions with the channel URL and configuration guidance for adding the channel to your `.condarc` file,
- Channel metadata, such as privacy settings and channel type, and
- Channel tracking options to receive email notifications when files are excluded or included due to policy changes.

Package Details

You can access the following details for each package in a channel:

- **File Metadata:** Signature (green check mark), architecture type, version number, and upload date
- **Security information:** CVEs associated with the package, supplemented by Anaconda's curation reviews that offer additional vulnerability context and analysis
- **Licensing details:** Complete licensing information to verify compliance with your organization's policies and requirements
- **Dependencies:** Packages required for the selected package to operate properly

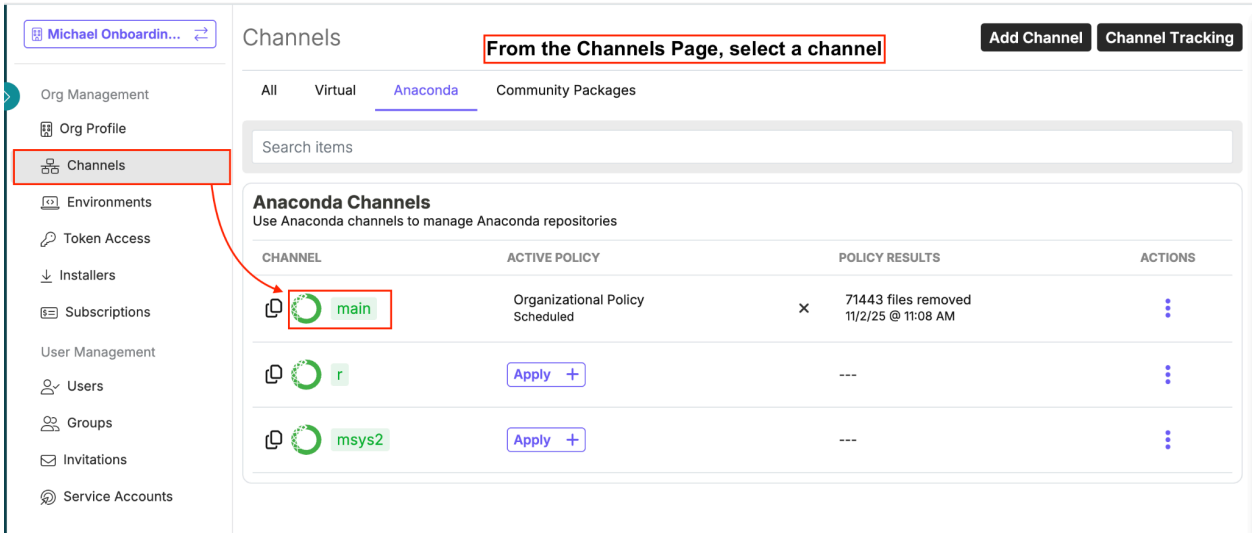
- **Dependants:** Packages that rely on the selected package for functionality
- **File-level data:** Detailed information of individual files within the package, including file metadata, file-specific CVE information, and SBOMs, providing a comprehensive inventory of all package components

This centralized system enables you and your team(s) to make informed decisions about package usage, security posture, and compliance requirements.

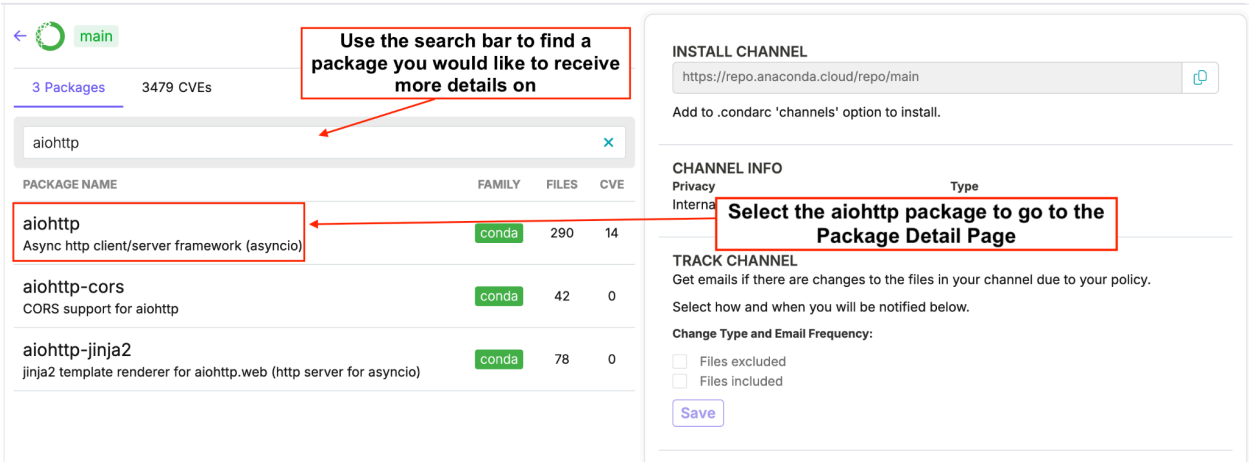
Viewing Package Details

To view package details

1. Navigate to **Org Management** > **Channels.**
2. On the Channels page, select a channel of your choice. For example, let's select the Anaconda channel `main`.



3. Select the channel name to view Channel Details.



4. Use the search bar to find packages within the `main` channel. For example, let's search for **aiohttp** to view all packages containing aiohttp in their name.
5. On selecting **aiohttp**, you'll see the following information:
    a. **Files:** The Files tab displays all files associated with this package, providing detailed information for each file including:
        - **Package version:** Specific package version available
        - **Python version compatibility:** Python version supported by Anaconda for each aiohttp package file
        - **Platform:** Target operating system and architecture (e.g., win-64, osx-arm64, linux-64)
        - **File size:** Size of each file
        - **Uploaded:** Date when the file was uploaded to the channel

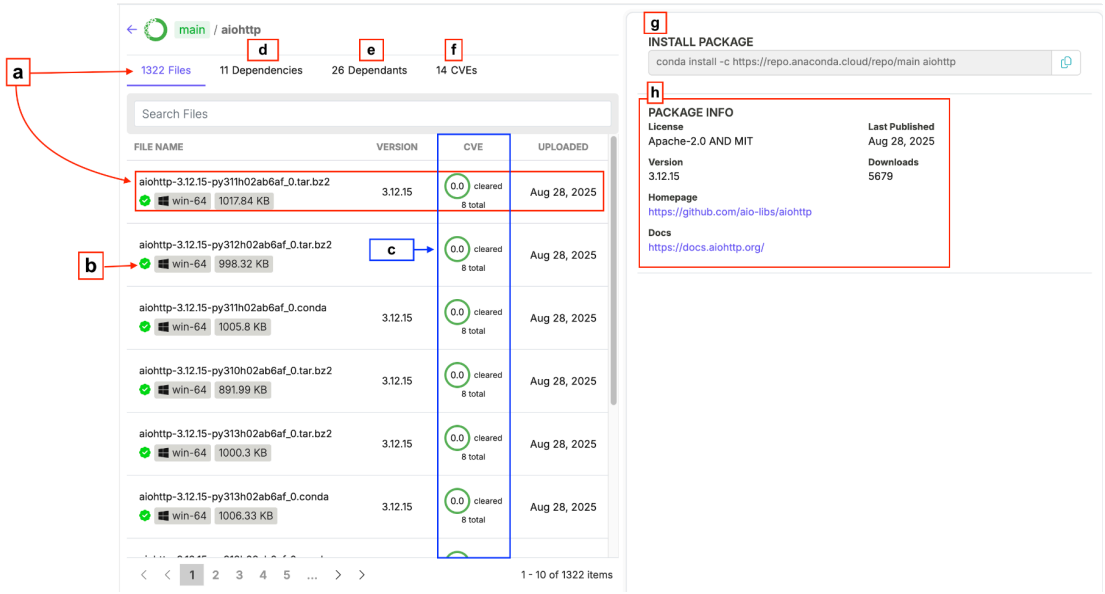
        This information enables you to identify which package version is compatible with your specific Python version and platform requirements.

    b. The green check mark next to each file indicates **Anaconda Signature status.****
    c. **CVE:** The CVE column displays the total number of CVEs associated with each package file, the CVE status, and the highest CVE score, enabling rapid security risk assessment for each file.
    d. **Dependencies:** This tab lists all packages that aiohttp requires to function correctly. In other words, these are the prerequisite or dependent packages that must be installed alongside aiohttp.

e. **Dependants**: This tab lists all packages that rely on aiohttp as a dependency for their functionality. In other words, these packages require aiohttp to be installed to operate correctly.
f. **CVEs:** This tab displays all CVEs identified within the package and its associated files.
g. **Install Package:** This section, on the right, provides the command-line syntax needed to install the package via conda, along with the channel URL (e.g., `conda install -c https://repo.anaconda.cloud/repo/main aiohttp`). You can copy this command directly to install the package from the specified channel.
h. **Package Info:** Under this section, you'll find
    - **License:** Licensing terms for the package (e.g., Apache-2.0 AND MIT)
    - **Version:** Current version number of the package (e.g., 3.12.15)
    - **Last Published:** Date when the package was last published (e.g., Aug 28, 2025)
    - **Downloads:** Total number of times the package has been downloaded (e.g., 5679)
    - **Homepage:** Link to the package's official website
    - **Docs:** Link to the package's documentation

****Note:**

Package Signatures: Packages in Anaconda's Premium Repository include a security signature. This unique cryptographic key value verifies the package's integrity and confirms it has not been modified or tampered with after completing Anaconda's curation process. Files with a valid signature have a green check mark next to their name. You can view the complete signature value in the metadata file at the bottom of the package details.



Let's explore the Files, Dependencies, Dependants, and CVEs tabs in more detail.

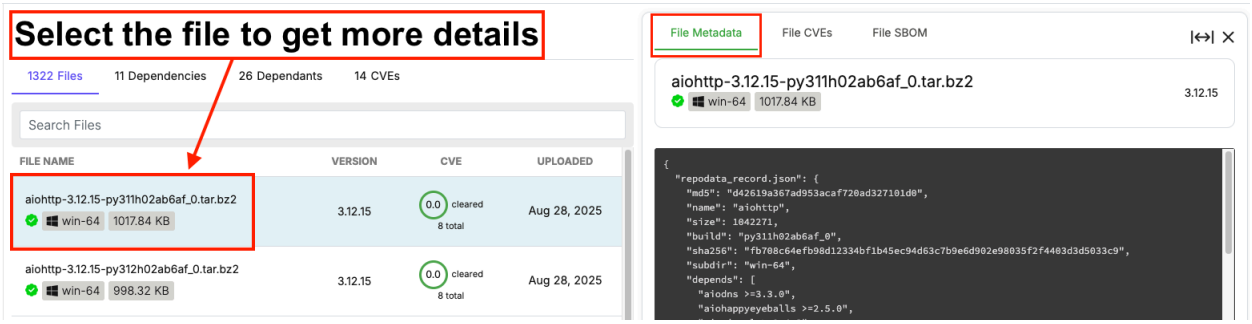
Files Tab

Package files under the Files tab serve as a comprehensive security and dependency manifest, providing all necessary information to verify package integrity, understand dependencies, and assess security risks for, for example, the aiohttp package in Anaconda's repository.

Select a package file to view the following details:

1. **File Metadata**

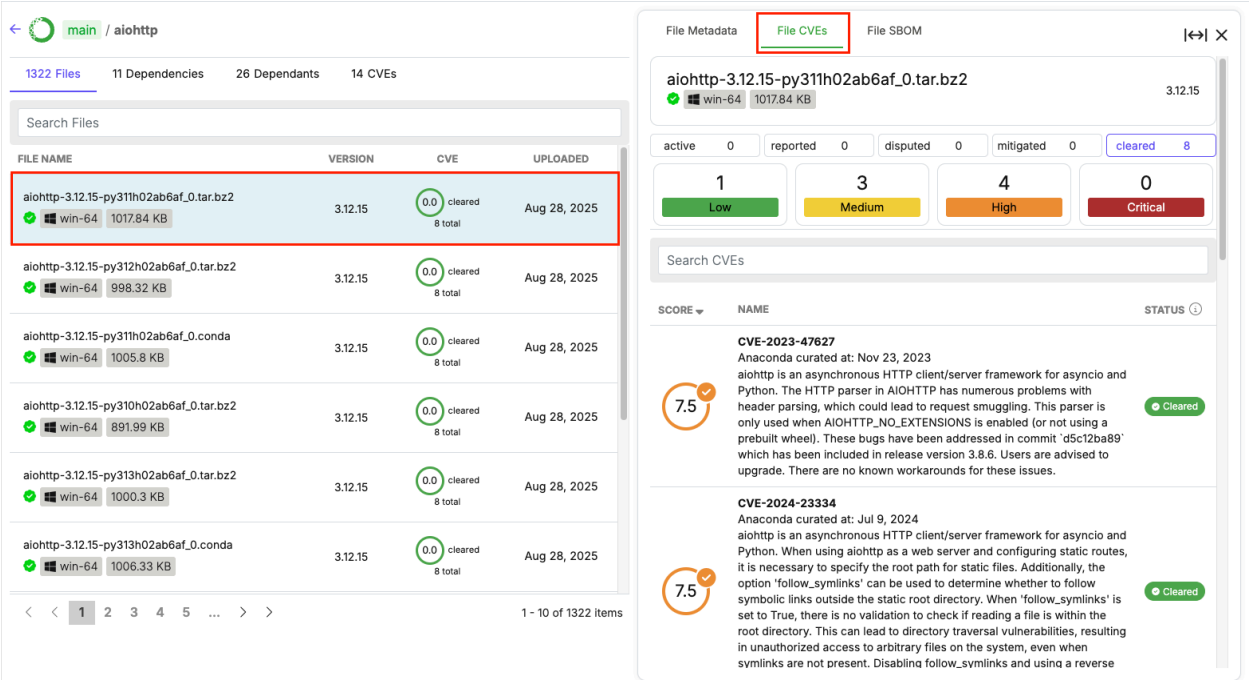
This JSON file provides comprehensive technical details and security information for the selected package file (version 3.12.15, Windows 64-bit platform). It contains the following information:



- **Package Info (repodata_record.json):** Contains core technical details, including package identity (aiohttp 3.12.15 for Python 3.11 on win-64), file size and sha256 checksums, dependencies, license (dual in this case: Apache-2.0 AND MIT), and key dates.
- **CVEs:** Shows 8 cleared CVEs, with severity scores ranging from 1.7 to 7.5. Note that all 8 have been marked as "cleared" by Anaconda's security team. For each CVE, you can view a detailed description, including Anaconda curated date and affected versions.
- **Signatures (Integrity Verification):** Provides cryptographic proof of authenticity through sha256 hash keys and digital signatures, confirming the package hasn't been tampered with since completion of Anaconda's curation process.

2. File CVEs

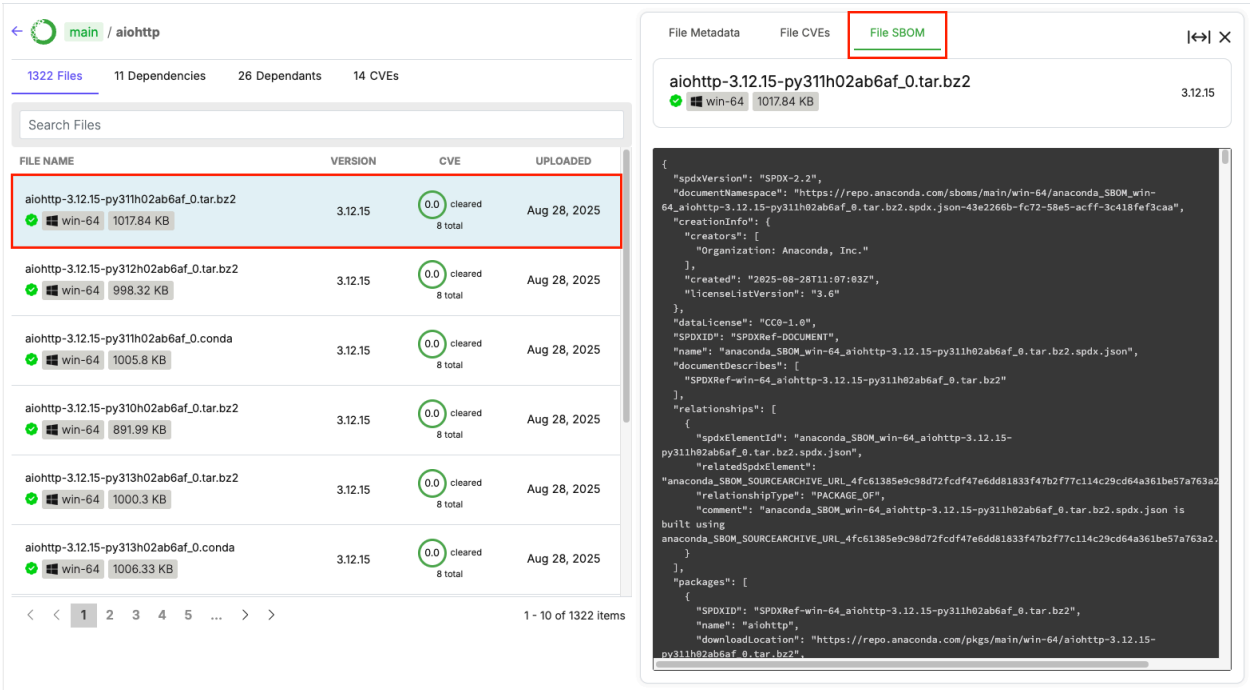
Under this tab, you can view the security risk of a specific package file. Here you'll find all existing vulnerabilities, their severity level, and status (e.g., cleared, indicating that Anaconda's security team has cleared a CVE).



3. File SBOM

This tab provides transparency about every component in, for example, the aiohttp package, enabling you (and your organization) to:

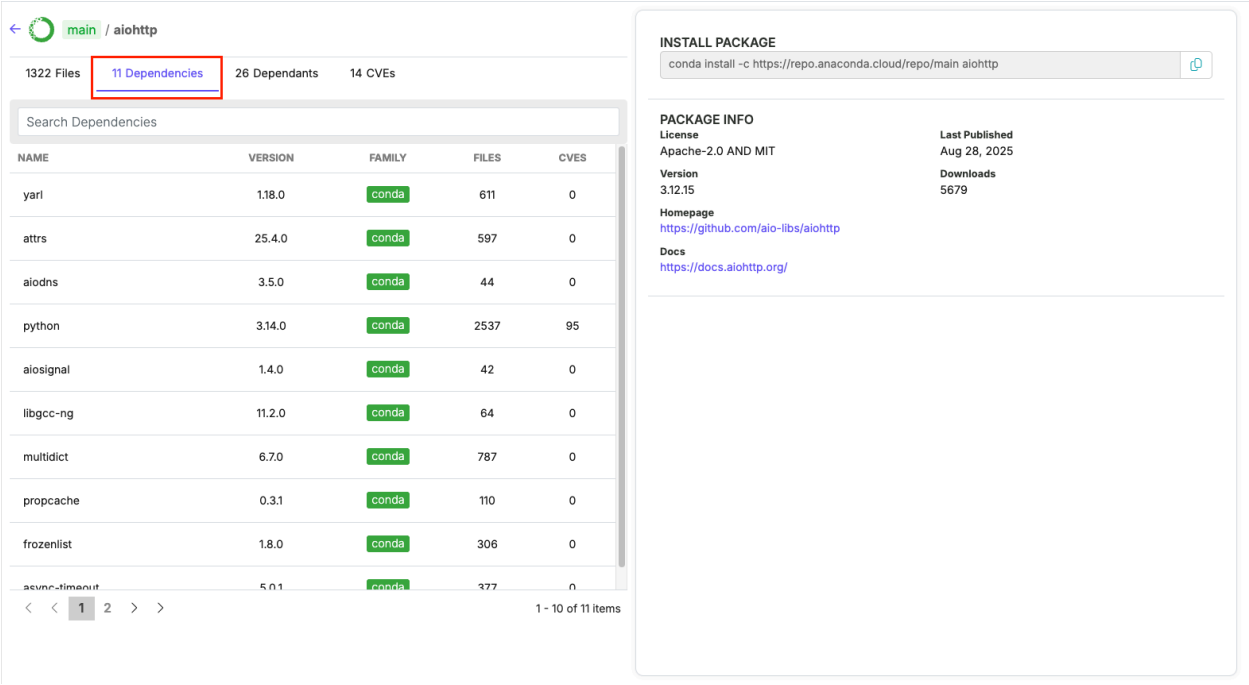
- Scan for security vulnerabilities in all package components,
- Verify license compliance across all files,
- Validate supply chain integrity with cryptographic checksums, and
- Track package provenance from source to distribution



Dependencies Tab

Continuing with our example, note that aiohttp (version 3.12.15) is an asynchronous HTTP client/server framework for Python, containing 1,322 files and licensed under Apache-2.0 AND MIT.

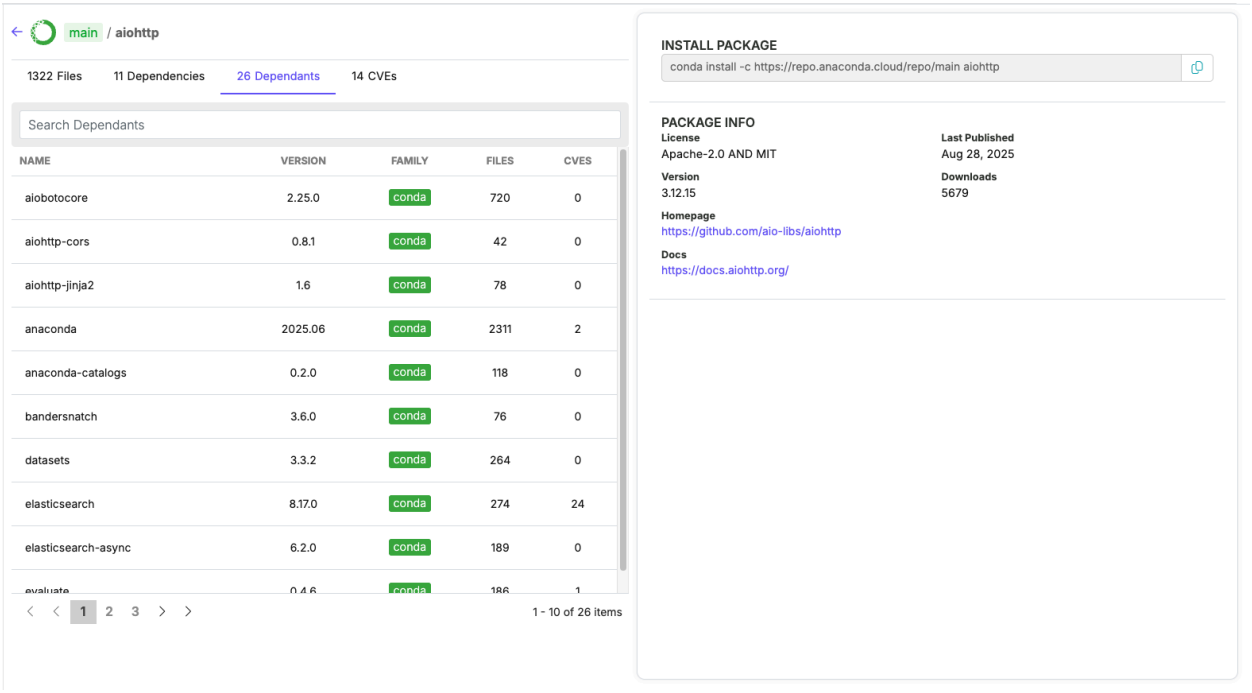
Dependencies (11 packages for aiohttp) are the packages that aiohttp ***requires*** to function properly. These must be thus installed alongside aiohttp.



Dependants Tab

Dependants (26 packages) are packages that ***rely on*** aiohttp as a dependency. These packages would be affected if aiohttp has issues or breaking changes.

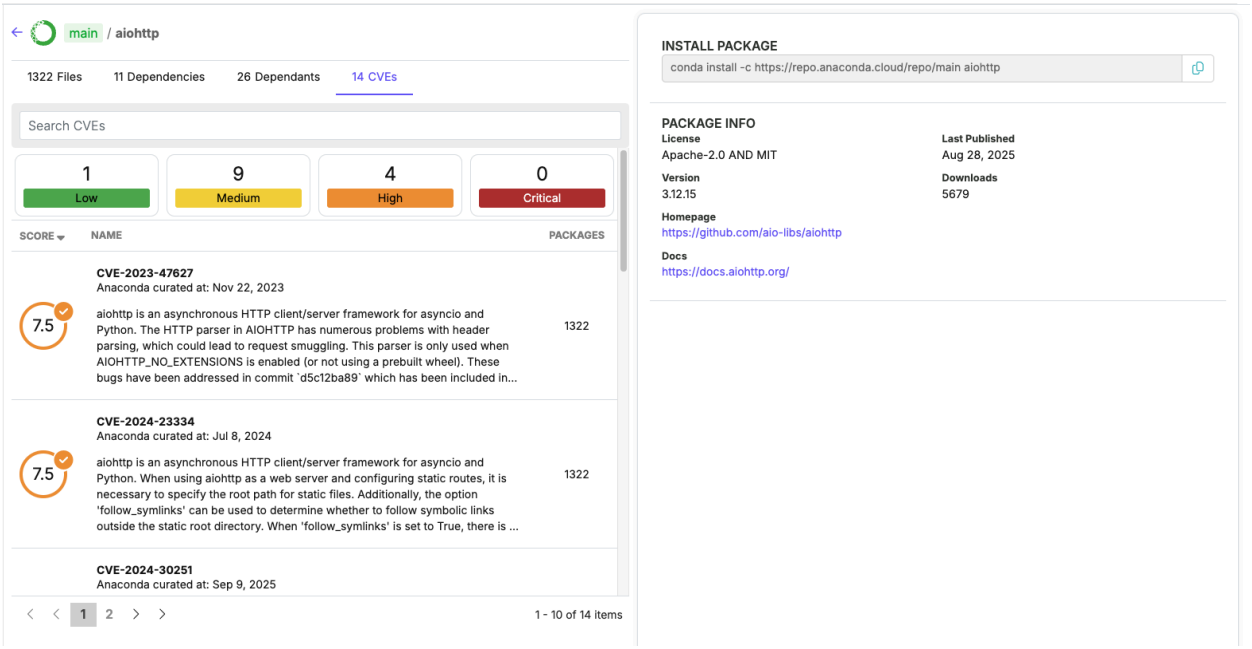
In our example, the presence of 26 dependants demonstrates that aiohttp is a widely used foundational package in the Python async ecosystem.



CVEs Tab

The number of **CVEs** indicates that aiohttp has 14 identified vulnerabilities, of which 8 are marked as "cleared," meaning that they have been reviewed and resolved by Anaconda's curation process.

Security Summary: While aiohttp has 14 CVEs, all reviewed vulnerabilities have been cleared. Organizations are recommended to monitor both direct vulnerabilities in aiohttp and security risks in its dependency chain and dependent packages.



Token Access Page

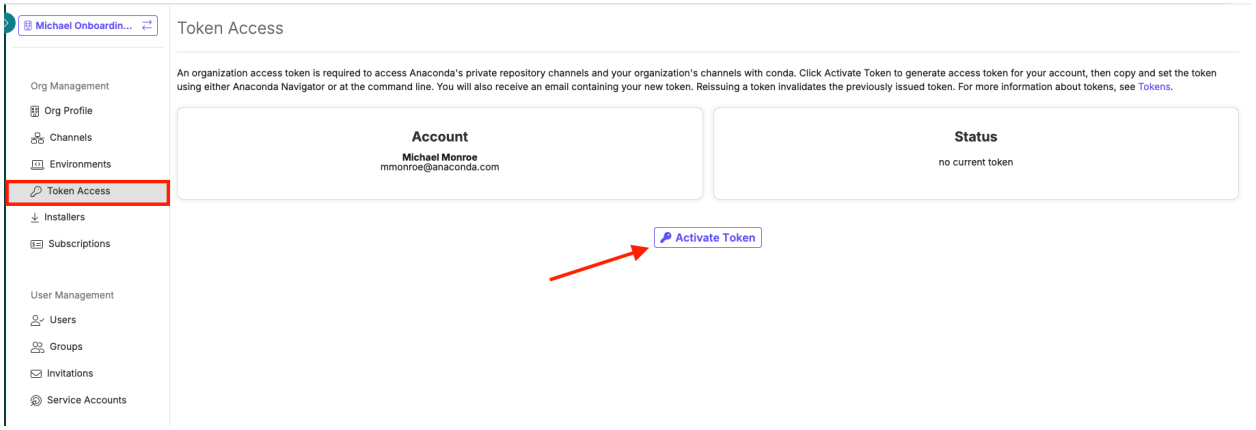
Anaconda tokens are authentication credentials that allow you and your users to securely access your organization's Anaconda Premium Repository (repo.anaconda.cloud) and the channels available on your Anaconda Platform Cloud.

Token Types

Your organization can use two types of access tokens:

1. **Individual Access Tokens:** Token credentials that you activate individually to access your organization's Anaconda Premium Repository.
2. **Site Token:** A shared access token for the entire organization. Unlike individual access tokens, this single site token can be used by any organization member to authenticate to the organization's channels.

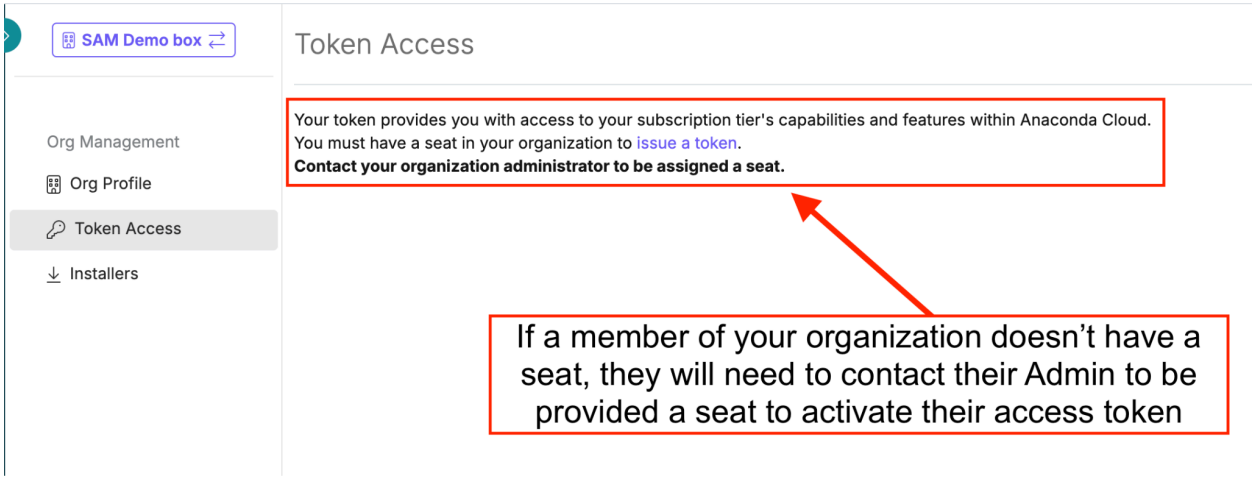
Anaconda tokens are activated and accessible through the **Token Access** page when you or your users are assigned a seat:



Individual Access Tokens

Individual access tokens provide access to your organization's packages for building local environments. Each user, including you as the admin, receives a unique token on seat assignment (to learn how to manage seats, refer to User Management), unless your organization uses a site token.

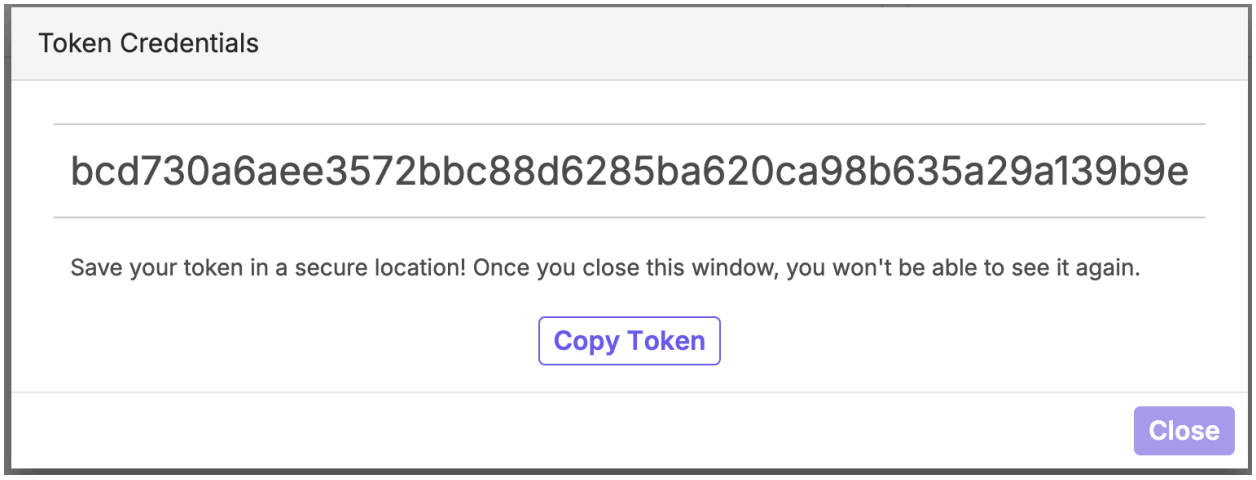
When a seat is not assigned to a user, they will see a message on the **Token Access** page instructing them to contact you, as the admin, for seat assignment:



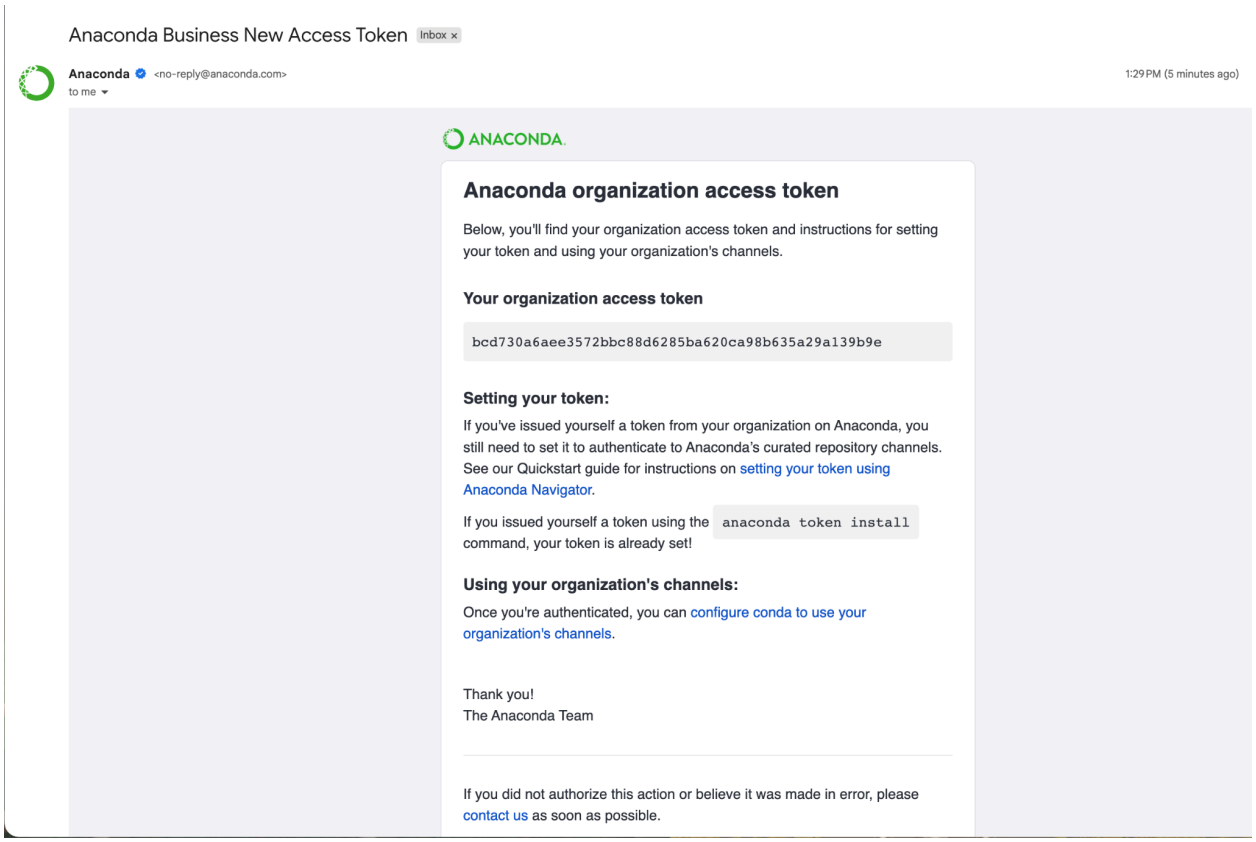
Activate Individual Access Tokens

To activate your token

1. Navigate to the **Token Access** page under **Org Management**.
2. For a user with an assigned seat, the **Token Access** page will display **Activate Token**. Select Activate Token.
3. Your **Token Credentials** will appear in a pop-up window. Select **Copy Token** and then save it securely, similar to how a password is handled. You may then close this pop-up window.

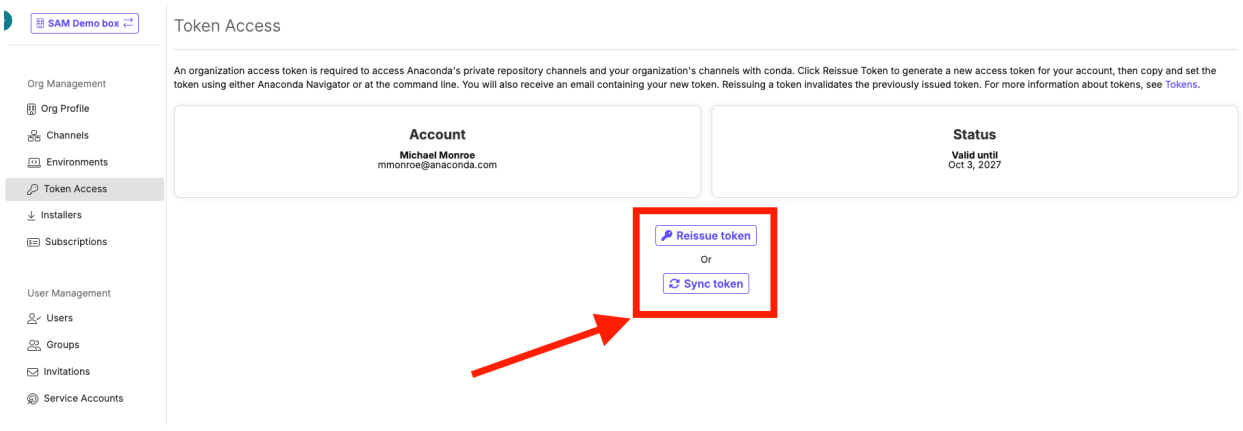


4. On token activation, you'll also receive a notification email, containing your token access credentials and setup instructions.



Reissue and Sync Tokens

On token activation, **Activate Token** on the Token Access page is replaced by **Reissue Token** and **Sync Token**.



Reissue Token allows you to generate new token access credentials. To do so

1. Select **Reissue token** on the **Token Access** Page.

2. In the pop-up window, select **Reissue Token**.
3. You'll now see your new **Token Credentials**. Select **Copy Token** and then save it securely.

Notes:

- Reissuing a token automatically invalidates your previous credentials.
- Use this option only if your token access credentials are lost or compromised.

Sync Token allows you to synchronize your token access with your organization's current subscription. To sync your token

1. Select **Sync token** on the **Token Access** Page.
2. The **Valid until** date under **Status** *may* change once syncing is complete.

Notes:

- Synchronizing extends your token's lifespan to match your organization's subscription validity.
- Use **Sync Token** after your organization renews its subscription to avoid needing to reissue a token to yourself, as subscription renewals don't automatically extend your token validity (validity date is visible under **Status** on the Token Access page).
- Note that token syncing may take a few minutes to complete.

Site Token

A site token is an access token used by your entire organization. This single token authenticates all members to your organization's Anaconda Premium Repository. Site tokens are provided to users by you, i.e., organization administrators.

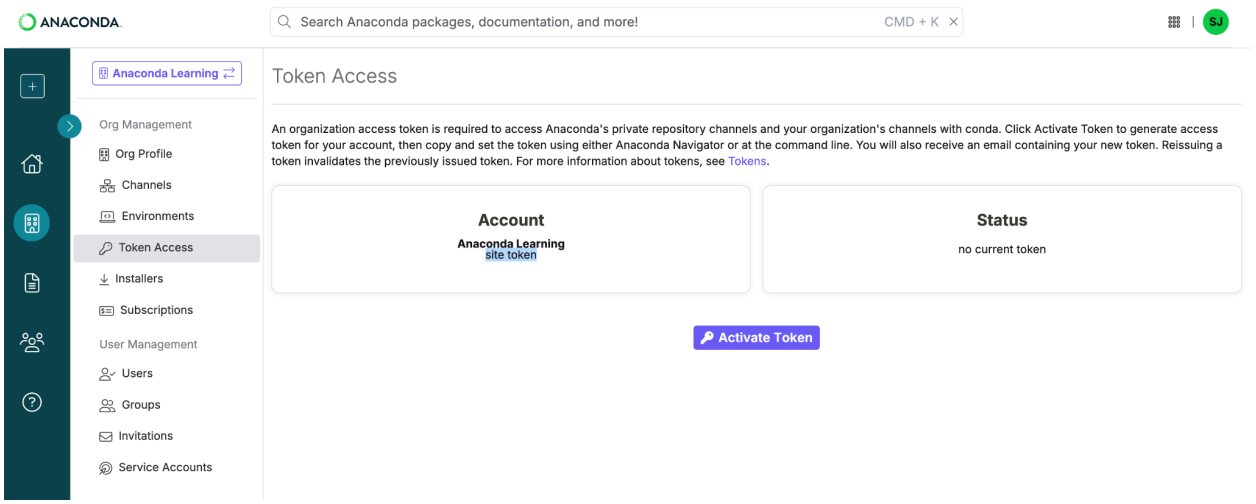
Important: You do not need to assign seats to users if your organization is using a site token.

Site tokens are activated, reissued, and synced similarly to individual access tokens, with two key differences:

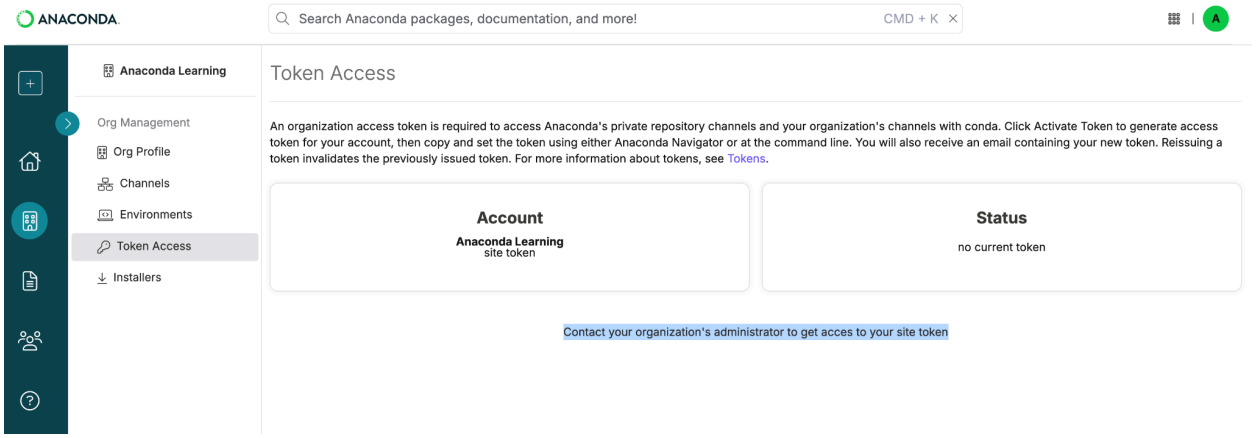
1. Only organization administrators can perform these actions, and
2. The token is displayed only in the browser. No email notifications are sent.

If you need to purchase a site token, reach out to sales@anaconda.com.

Here's what the **Token Access** page with a site token looks like **for admins**:



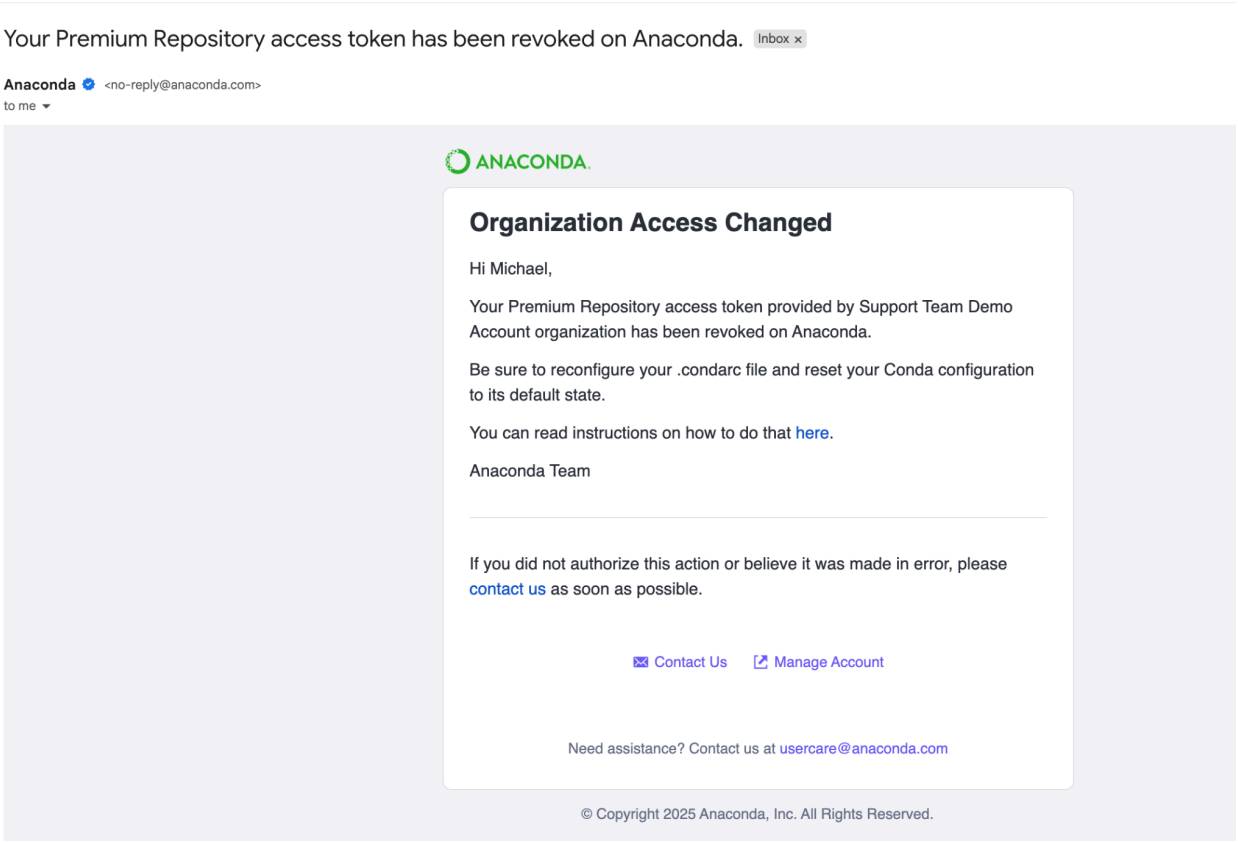
Here's what the **Token Access** Page with a site token looks like **for those who aren't an admin**:



Revoke User Seat and Token Access

If for some reason, you revoke a user's seat, they'll lose their token access. In this case, they'll see a message on the **Token Access** page instructing them to contact you, the admin, for seat assignment.

When a user's seat is revoked and they lose their activated token, they'll receive a notification email. For those who haven't activated their token, no notification email is sent.

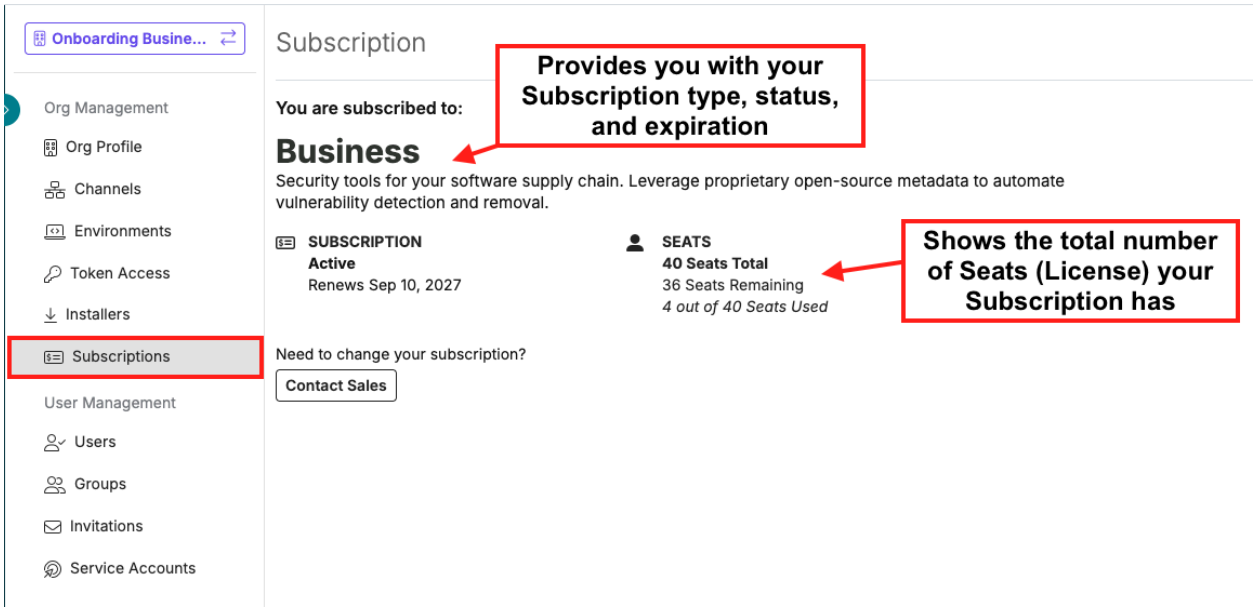


Subscriptions Page

To view subscription-related information

1. Navigate to the **Subscriptions** page under **Org Management**.
2. Here, you can review
    a. Subscription Type: Your current plan level
    b. Status: Whether your subscription is active or inactive
    c. Validity: When your current subscription renews
    d. Seats (Licenses): Total number of used and remaining seats (or licenses)

3. You can also contact our Sales team via this page. Select Contact Sales to raise a form. Alternatively, you can contact your Customer Success Manager (CSM) via cs@anaconda.com.



ANACONDA.

Conclusion and Next Steps

Summary

Through this guide, you've learned the essential skills to administer your organization's Anaconda Platform Cloud. You've learned how to configure ESSO, manage users and groups, create custom channels with security policies, and maintain compliance through CVE monitoring and license filtering. As you implement these capabilities, we recommend you to regularly review policy results, track channel changes, and adjust filters as your organization's security requirements evolve. Leverage the Token Access system to provide secure repository access to your teams, and use the comprehensive package details (including CVEs, SBOMs, and dependencies) to make informed decisions about your data science and AI infrastructure.

Finally, note that the contents of this guide are also available as a free self-paced course with **how-to videos**. To access this **Anaconda Platform Cloud: Admin Onboarding** course, log in to Anaconda Learning using your Anaconda credentials.

ANACONDA.

Need Help?

If you have questions or need any help setting up Anaconda Platform Cloud, reach out to your Customer Success Manager (CSM) via cs@anaconda.com. We're here to help you succeed!

Appendices

Common Vulnerabilities and Exposures (CVEs)

Understanding CVEs

CVEs are security flaws in software that attackers exploit to gain unauthorized access to sensitive data (e.g., credit card details or social security numbers). In today's world, as software becomes increasingly sophisticated with multiple layers, interconnected dependencies, varied data sources, and external libraries, security vulnerabilities naturally develop over time. Understanding which components in your codebase are susceptible to security threats can enable you to proactively reduce risk. Anaconda provides comprehensive tools and resources to maintain a secure development pipeline.

Anaconda's CVE Management

To reduce vulnerability risks in our applications and webpages, we at Anaconda routinely synchronize CVE databases from the National Vulnerability Database (NVD) and the US National Institute of Standards and Technology (NIST). Our curation process involves

- Assessing CVE impact on Anaconda-built packages,
- Determining affected versions in our repository, and
- Implementing appropriate mitigations.

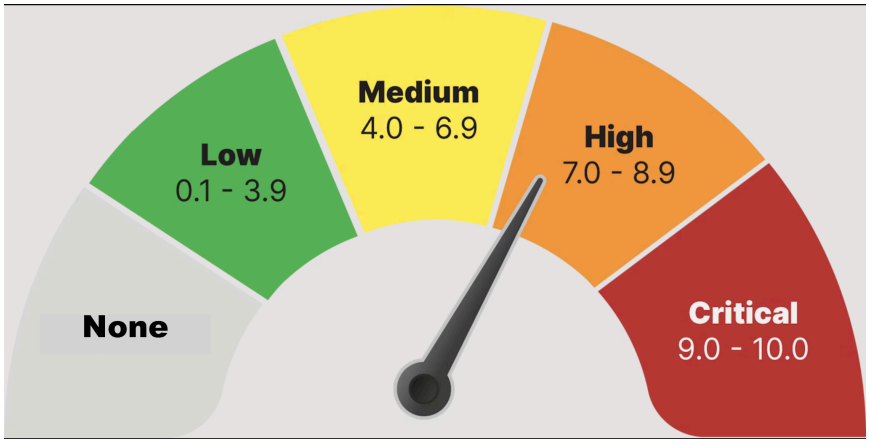
Common Vulnerability Scoring System (CVSS)

The criteria for assessing CVE severity have significantly evolved over the years. CVSS emerged in 1999 as a quantitative framework for evaluating vulnerability characteristics. CVSS v2 was introduced in 2007, followed by CVSS v3 in 2015, which provided enhanced scoring methodology designed to better represent actual vulnerability impact in real-world environments. To learn more, refer to Common Vulnerability Scoring System SIG.

CVE Scores and Severity Ratings

Software developers use CVE databases and scores to minimize the risk of using vulnerable components (packages and binaries) in their applications or webpages. CVE scores and ratings fall into five categories:

Severity	Description	Score
None	No impact	**0.0**
Low	Minimal risk, difficult to exploit	**0.1 - 3.9**
Medium	Moderate impact, requires some skill to exploit	**4.0 - 6.9**
High	Serious impact, relatively easy to exploit	**7.0 - 8.9**
Critical	Severe impact, highly exploitable	**9.0 - 10.0**



CVE Status Categories

Through Anaconda's curation process, CVEs are assigned a status category:

Status Category	Description
Active	The vulnerabilities identified in this package are active and potentially exploitable.
Reported	The vulnerabilities identified in this package have been reported by NIST but not reviewed by the Anaconda team.
Mitigated	The vulnerabilities identified in this package have been proactively mitigated through a code patch in this build.
Disputed	The vulnerabilities' legitimacy is disputed by upstream package maintainers or other community members.
Cleared	The vulnerabilities identified in this package have been analyzed and determined to be not applicable.

License Families

License families are groupings of software licenses that share similar characteristics, permissions, and restrictions. Understanding license families can help you, and your organization, classify packages based on their legal obligations and usage rights, making it easier to maintain compliance with corporate policies and legal requirements.

License Family Types

1) **Affero General Public License (AGPL):** A strong copyleft license that requires sharing source code for any modifications, including software accessed over a network. This makes it particularly restrictive for SaaS and cloud deployments.
2) **Apache License (APACHE):** A permissive open-source license that allows use, modification, and distribution. It includes an explicit patent grant to users.

3) **Berkeley Software Distribution (BSD):** Permissive, minimal-restriction licenses that allow nearly unrestricted use, modification, and redistribution, typically requiring only attribution.
4) **Creative Commons (CC):** Primarily used for content and data. They offer a range of permissions and restrictions, including attribution, non-commercial, and share-alike clauses.
5) **GNU General Public License (GPL):** A strong copyleft license requiring that derivative works and redistributions remain under the same license and that source code be made available.
6) **GPL version 2 (GPL2):** A widely used copyleft license that requires source code disclosure and same-license distribution for derivatives, but it lacks some of the patent and compatibility provisions found in GPL3.
7) **GPL version 3 (GPL3):** Also a strong copyleft license, but it adds explicit patent protection, anti-tivoization provisions, and improved compatibility with other licenses.
8) **Lesser General Public License (LGPL):** A weak copyleft license that allows linking to proprietary software. However, modifications to the LGPL-covered components themselves must be open-sourced.
9) **MIT License (MIT):** A highly permissive license allowing reuse, modification, and redistribution with minimal requirements, typically just attribution.
10) **Mozilla Public License (MOZILLA):** A weak copyleft license requiring that modifications to MPL-licensed files be shared, but allows combining with proprietary code in larger works.
11) **None:** Indicates that no license information is provided, meaning the legal status is unclear and use may not be permitted.
12) **OTHER:** A catch-all category for licenses that do not fit standard classifications. This may include custom, niche, or less common open-source or proprietary licenses.
13) **Python Software Foundation License (PSF):** A permissive license used for Python and related projects, allowing broad use, modification, and redistribution.
14) **Public-Domain:** Indicates that work is not protected by copyright and can be freely used, modified, and redistributed by anyone for any purpose.
