NGC User Guide

Application Note
# Table of Contents

Chapter 1. What is NVIDIA NGC? ...................................................................................................... 1

Chapter 2. Why NGC Software........................................................................................................... 2

Chapter 3. NGC Organizations and Teams.................................................................................... 3
  3.1. NGC Teams................................................................................................................................. 4
  3.2. NGC Org Owner and Other Org Users...................................................................................... 6
    3.2.1. Securing the Owner Account with Multi-Factor Authentication................................ 12
    3.2.2. Contacting your Org Owner............................................................................................... 13
  3.3. User Accepting an NGC Org Invitation.................................................................................. 16

Chapter 4. Accessing NGC Org........................................................................................................ 18
  4.1. Accessing NGC as an Account Owner..................................................................................... 18
    4.1.1. Signing Up for an NVIDIA Cloud Account and Activating an Individual NGC Org...18
      4.1.1.1. Setting up your NCA Account .................................................................................. 27
      4.1.1.2. Setting Up NCA Recovery Email ............................................................................ 29
    4.1.2. Accessing an NGC Subscription from an NGC Welcome Email................................... 32
      4.1.2.1. NGC Subscription - New User ................................................................................ 33
      4.1.2.2. NGC Subscription - Existing NGC User ................................................................. 37
    4.1.3. Accessing NGC from an NCA Invitation Email............................................................. 40

Chapter 5. NGC Org Authentication Using an External SSO Provider......................... 48
  5.1. NGC IdP Membership Rules.................................................................................................... 49

Chapter 6. Activating Your Subscription (Offer Dependent)............................................. 59

Chapter 7. Switching Orgs or Team After Logging into NGC........................................... 63

Chapter 8. NGC API Keys............................................................................................................. 64
  8.1. Generating a Personal API Key............................................................................................... 65
  8.2. Generating a Service API Key............................................................................................... 70
  8.3. Generating NGC API Keys.................................................................................................... 75

Chapter 9. Notification Services.................................................................................................... 77
Chapter 1. What is NVIDIA NGC?

Important: NGC is now accessed using NVIDIA Cloud Accounts (NCA). NCA provides a convenient and scalable way to set up and manage access to NVIDIA cloud services and run applications for different users in your company. To learn more about NCA, refer to NVIDIA Cloud Accounts User Guide.

NVIDIA NGC™ is a cloud platform providing fully managed services, including NVIDIA AI Enterprise, DGX Cloud, and Riva Studio for Natural Language Understanding (NLU) and speech AI solutions. AI practitioners can leverage NVIDIA DGX Cloud for model training, NVIDIA AI Enterprise to obtain the latest NIM models, and the NGC Private Registry for securely sharing proprietary AI software. NGC also hosts a catalog of GPU-optimized AI software, SDKs, and Jupyter Notebooks to accelerate AI workflows and offers support through NVIDIA AI Enterprise.

Enterprises access their AI cloud services via a dedicated virtual NVIDIA Cloud Account (NCA) linked to the NGC organization where their services are enabled.
Chapter 2. Why NGC Software

NGC provides software to meet the needs of data scientists, developers, and researchers across various levels of AI expertise.

All software hosted on NGC undergoes thorough scans for common vulnerabilities and exposures (CVEs), crypto, and private keys.

In addition to security scanning, NGC software is tested against a wide range of GPU-enabled platforms, including public cloud instances, workstations, and OEM servers designed for data center or edge deployments. Supported GPUs include H100, V100, A100, T4, Jetson, and the RTX Quadro.

NGC software is tested and assured to scale across multiple GPUs and, in some cases, across multiple nodes, ensuring users can fully utilize their GPU-powered servers out of the box.

For select containers, NVIDIA offers NGC Support Services for running software on DGX platforms or certified OEM servers. The service gives enterprise IT direct access to NVIDIA subject matter experts to quickly address software issues and minimize system downtime.
Chapter 3. NGC Organizations and Teams

An NGC organization (org) is linked to an NVIDIA Cloud Account and shares the same account number. The dedicated account instance is used to enable and manage NVIDIA cloud services.

Users can access an NGC org in the following ways:

1) A user can sign up for a free NGC org through the NGC sign-in portal and create a new NVIDIA cloud account.

2) An NVIDIA representative onboards a user through a purchase order, early trial program, or other commercially related offers. The customer provides the users’ contact information to an NVIDIA representative. An NVIDIA NGC org gets created on behalf of the user, and an org owner welcome email is sent to the user’s email address. The user is requested to create an NVIDIA cloud account and access NGC via an invite URL embedded in the email.

3) The account owner can onboard a user to an NGC org. The account owner will invite the user through an NCA invitation email or add the user using a corporate AD group membership rule mapped to the NGC org. Note that only ‘enterprise’ type orgs support the ability for account owners to manage additional users.

Users who sign up for an NGC org through the NGC sign-in portal get assigned an NCA account linked to an individual org that is automatically enabled with the NGC Catalog service and grants authenticated access to the catalog. An individual org is only accessible by a single user, the org owner. The NCA account linked to the org supports additional users, but these users cannot be assigned NGC access permissions.

An NVIDIA premium cloud service subscription, such as NVAIE or DGX Cloud, will be granted through purchase, an early access program, or the NGC Activate Subscription portal. Subscriptions get enabled on enterprise NGC orgs created by NVIDIA. Alternatively, an individual org is converted to an enterprise org when a user activates their subscription through the NGC activate subscription portal. An NGC enterprise org is linked to an NCA account and supports additional users, teams, and role-based access rules.
3.1. NGC Teams

An NGC team is a virtual sub-unit within an org, each with its own registry space. Only members of the same team have access to that team’s registry space. Creating teams allows users to share images within their team while keeping them hidden from other teams in the same organization. Only the org owner or a user with the user admin role can create teams. A user admin assigned at the org level (without specifying teams), can manage users across all teams within the organization. If assigned to a specific team, the user admin can only access and manage users exclusively within that team.

To create a team, follow these steps:

1. Log on to the NGC application.
2. Select Organization from the user account menu.
3. On the dashboard or in the left navigation, select Teams.

4. On the Teams page, click Create Team on the upper right corner.
5. Enter a team name and description. Note that names must be all lowercase.
6. Click Create Team to finish.

3.2. NGC Org Owner and Other Org Users

When an NGC org is created, an NVIDIA Cloud Account (NCA) is required to access the org. The NCA account is automatically generated and the user simply needs to name the NCA account. The user is assigned the owner role in NCA and NGC - as the initial user.

Refer to NVIDIA Cloud Accounts for more information.

As mentioned above, an individual org is only accessible by the org owner. Additional users are not supported. To verify the type of org you manage, sign in to NGC to access your org. Under the user account menu, select Organization. In the left navigation, select Organization Profile.

The org owner possesses the highest admin privileges in an NGC org. The org owner of an enterprise org can add and remove NGC teams and users, and assign NGC permissions to each added user by managing the assignment of teams and roles. When a new user gets added, the org owner invites the user to join the NVIDIA Cloud
Account, then assigns access to the entire org or limits the user’s access to a team or a set of teams created within the org. Then, the org owner controls the user’s access by assigning the permissions (roles) necessary to perform their functions within the org or team.

An org supports up to three org owners, and only an org owner can add or invite additional org owners to share in the NGC org management responsibilities. In NCA, only one owner is supported, therefore to support the additional NGC org owners the account owner must assign the NCA “Admin” role when creating the add user invitation. For details, see the steps to add org additional org owners. To prevent accidentally adding an outside user as an org owner, the email address domain between all org owners’ users must match.

For example, if the users' email addresses are john@intelligence.ai, jane@intelligence.ai, and peter@intelligence.ai, then all three can be added as org owners because their email address domains match. In contrast, if Peter’s email address was peter@artificial.ai, then Peter cannot be added as an org owner.

Note: If the org has not linked to an external IdP, an org owner can invite a user with a different email domain as an org user and assign the required roles to that user.

Follow the steps below to add a new org owner or additional users with different access permissions.

1. Sign in to NGC. Make sure to select the correct NCA account linked to the NGC org you want to manage, and click Continue.
2. Select Organization from the user account menu. On the dashboard or in the left navigation, select Users.
3. Click Add User at the top-right corner.

Important: If your org is linked to an external IdP/SSO service, it is recommended to manage user membership using IdP groups. If your IdP doesn’t support groups, you can use the NGC add user service.

4. In Step 1, invite the user to be an "admin" in your NCA account.
   - Enter the user email address, making sure the domain matches your email domain.
   - Assign the NVIDIA Cloud Account Role "Admin".
- Customize the invitation email to inform the user what this is for (optional).
- Set an expiry for the invitation link (default: 6 hours).
- Click Add User and Send Invitation before proceeding to Step 2.

After completing Step 1, you will see a successful invitation pop-up and Step 2 configuration buttons become active. To assign the 'org owner' role to a user:

- Select Organization for role assignment.
- Under the Organization roles, select Owner.
- Click Add Role to finish.
5. To assign controlled permissions to a user
   - Click the Organization or Team radio button
   - Assign a "role" under each NGC application, depending on the level of access to grant the user

   **Note:** If the user being added will not manage users or NGC teams, assign the "member" role in NCA and don't assign the Owner or User Admin role in NGC.
In this example, the user added is assigned the 'viewer' role under NVAIE and the 'user' role under the private registry. These permissions limit the user to viewing and pulling artifacts from the NVIDIA Catalog and pushing and pulling artifacts to the org’s private registry.

To learn more about NGC cloud services user roles, refer to the links below.

- Base Command roles
- Fleet Command roles
- Private Registry roles
- NVAIE viewer role

Note that assigning the user at the team level allows the new user to perform commands within the assigned team. If the new user needs access to the entire org, the user must be assigned at the "Organization" level.

6. The user added will receive an NCA invitation email message that includes the NCA URL to accept the invite and access the NGC org.

In the case of org owners, after all three org owners are added, any org owner can initiate the replacement of another org owner when needed. An org owner can remove another org owner by going to the 'users' list and selecting Remove User.

When an org owner is deleted, an email message is sent to the remaining active owners, notifying them of the deletion event. A replacement owner can be invited using the same steps above.

3.2.1. Securing the Owner Account with Multi-Factor Authentication

When you create your owner account, you receive an NVIDIA identity account that is protected by a password you set at the time of owner account creation. You can further secure access to your owner account by setting up multi-factor authentication using the directions below:

1. Go to NVIDIA and click the sign-in icon.

2. Sign in with the credentials you set up during the org owner account setup.
3. From your NVIDIA user profile page, navigate to the bottom of the page, click on Security settings, and click Update.

4. You will be prompted to enter your password again to access security settings.

6. You can now configure your identity account for two-factor authentication. Go to the NVIDIA N-factor help page for details on how to set it up.

### 3.2.2. Contacting your Org Owner

As a user within an NGC organization, you may need to contact the organization owner to request a new service subscription or add a new user. NGC simplifies this communication with the Contact Admin option in your user account menu.

1. First, sign into the NGC application with your organization. Then click on your user ID in the top right corner to access the user account menu.
2. Select Contact Admin to open the email editor dialog.
Within this editor, you can choose from the following email templates:

- **Product Request**: Use this template when requesting a specific product for your `<org-name>` organization. For example, "I’d like to request the [product name] product for the `<org-name>` organization."
- **Team Access Request**: Select this template if you need to request access to the org or a particular team, such as “[team-name],” within your `<org-name>` organization.

Both templates come with pre-populated message content, but you can edit or delete portions of the message to create a customized message to send to your organization owner.

3. Once you are ready to send the message, click Send.

   The organization owner will receive the email from `noreply-ngc@nvidia.com` and will include your email address. The following is a sample email message:

   ```
   I'd like to request access to [team-name] in demo org.
   ```
By following these steps and using the Contact Admin option, you can easily initiate communication with your organization owner.

### 3.3. User Accepting an NGC Org Invitation

A user added will receive an NCA invite email requesting the user to join the NCA account to access NGC.
After clicking the Login link in the email message, the user is automatically redirected to their appropriate sign-in method. Suppose this is the user's first time signing into NVIDIA Cloud Accounts. In that case, they will be automatically prompted to create a new NVIDIA identity account using their email address or can select More Signup Options in the NVIDIA identity account creation portal to sign in using an existing social platform user account (e.g., Google, Facebook, Apple, or Discord).

Users who have an existing NVIDIA identity account are automatically prompted for their password to sign in and access NVIDIA NCA. Users ready to accept an invitation to access their NGC org go here. Users whose company has federated their NGC org to an external SSO identity provider are automatically redirected to their SSO portal to provide authentication credentials to sign in. To learn more about bringing your own SSO/IdP provider, see NGC Org Authentication Using an External SSO Provider.

Important: For a successful user onboarding experience, customers should add the following NVIDIA email addresses to their allow-list in their firewall rules: 'noreply-ngc@nvidia.com', 'account@tmail.nvidia.com', noreply-cloud-accounts@nvidia.com, and 'account@nvidia.com'.

NGC User Guide
Chapter 4. Accessing NGC Org

The following are ways to access an NGC org.

**NCA/NGC owner**
A user must create a new NVIDIA identity account, cloud account, and register a new NGC individual org against it. Alternatively, the user receives an NCA welcome email and is invited to accept and sign in as the org owner of a new enterprise org.

**Org user**
The org owner, or an org user admin, adds a new user to the org (or team) and sends an NGC welcome email inviting the user to sign in.

**Subscription**
To access subscription-based software, users must provide Business Address details and a token (serial number, activation code, and so on.). Note that this category also requires Authenticated Access.

### 4.1. Accessing NGC as an Account Owner

Instructions for accessing NGC org as the account owner.

#### 4.1.1. Signing Up for an NVIDIA Cloud Account and Activating an Individual NGC Org

This section describes the steps to sign up for an NCA account and activate an individual NGC org.

1. Go to the [NGC sign-in page](#) from your browser, enter your email address, and then click Continue.
2. In this step you will create your NVIDIA sign-in identity using NVIDIA's default IdP. At the Create your Account screen, create a password, make sure to review the NVIDIA Account Terms of Use and Privacy Policy, and click Create Account to accept and proceed with account creation. You will receive an email to verify your email address.
Create Your Account

Email
[Input field]

Password
Enter your password

Confirm password
Enter your password

[Checkbox] Stay logged in
[Button] Log In With Security Device

By proceeding, I agree to the NVIDIA Account Terms Of Use and Privacy Policy

[Button] Create Account
[Button] More Signup Options

A verification email is sent to your email address.
3. Open the NVIDIA account creation email and click Verify Email Address.
Hello,

We are almost done creating your NVIDIA account. Click the link below to verify this email address.

Verify Email Address

If you did not register for an NVIDIA Account, someone may have registered with your information by mistake. Contact NVIDIA customer care for further assistance.

You are automatically directed to nvidia.com and see an email verified successfully page. This window will close automatically.
4. At the Almost done! dialog, set your communications preferences, and then click Submit.

5. Enter the password you just created to continue setting up your NVIDIA Cloud Account. (This is a required security measure).
6. Give your NVIDIA Cloud Account (NCA) a name that will help you identify it easily the next time you sign-in.
Create a NVIDIA Cloud Account

You need a cloud account to use NVIDIA Services. Provide your cloud account name to start the setting up process.

Provide a Cloud Account Name

Choose a distinctive name for your cloud account to easily identify it in the future.

Account Name *

Enter Cloud Account Name

Create NVIDIA Cloud Account

Learn more about NVIDIA Cloud Accounts

7. Complete your user profile at the Set Your Profile screen, agree to the NVIDIA GPU Cloud Terms of Use, and then click Submit.
Your NVIDIA account is created, and you are automatically redirected to your individual NGC org.
Your access to NVIDIA NGC org is completed, you can choose to complete the setup of your NVIDIA Cloud Account now, or at a later time.

4.1.1.1. Setting up your NCA Account

To finish setting up your NVIDIA Cloud Account, find your NCA invitation email message in your inbox and click Log In Now.

1. Your NVIDIA Cloud Account (NCA) provides the services to set up a recovery email address in case your existing one becomes unavailable, manage access for additional users (subscription required), and set up billing information to purchase consumption-based NVIDIA cloud products.

2. Enter your email address to Login and click Continue.
3. Enter the credentials you created for your NVIDIA identity account.
4. On the NCA landing page you can find the details of your account. Here you can setup a recovery email address that can be used to regain access if the email address you used to create your account becomes unavailable. Go to Setting Up NCA Recovery Email for steps on how to setup your recovery email.

4.1.1.2. Setting Up NCA Recovery Email

To set up your NVIDIA Cloud Account (NCA) recovery email, follow these steps.

1. Click Edit on the Account Details pane under the Account Management > Details page.
2. On the Edit - Details dialog, enter the email address that you want to use for account recovery. This email address must be different from the address used to create the account. You can optionally set a description of this account, click Save.

3. Check to see that the recovery email status on the Account Details pane changed to Pending.
4. Go to your recovery email inbox, search for the NVIDIA message with the title "NVIDIA Cloud Account, Verify Your Recovery Email", and click Verify.

**NVIDIA Cloud Account, Verify Your Recovery Email**

noreply-cloud-accounts@nvidia.com

To: [Your Email Address]

NVIDIA Cloud Account

Verify your recovery email for your NVIDIA Cloud Account.

To verify your email address please click on the link below

[VERIFY]

You should see that your email has been verified.
5. Go back to your NCA console and check the recovery email status has updated with the address you assigned.

4.1.2. Accessing an NGC Subscription from an NGC Welcome Email

When you are approved for an "early access" program for NVIDIA AI software delivered on NGC, you will receive a welcome email where you start your onboarding journey to access the software. To access NGC, you will need an ‘NVIDIA Cloud Account’ to manage access to NGC for you and additional users. Below are the steps to use your welcome email.

Go to your email inbox you used to apply for the early access program to find the email "Welcome to NVIDIA NGC". Click the Accept invitation and sign-in button.
If you are an existing NVIDIA user, go directly to NGC Subscription - Existing NGC User.

4.1.2.1. NGC Subscription - New User

This section describes signing in if you are new to NVIDIA. New users are automatically prompted to create a new NVIDIA account.

1. If you are new to NVIDIA, follow the steps below to create your NVIDIA sign-in identity account, make sure to review the NVIDIA account Terms of Use and Privacy Policy, and click Create Account to accept and proceed with your identity account creation.
A verification email is sent to your email address.
2. Open the email and click Verify Email Address.
You are automatically directed to nvidia.com and see an Email verified successfully page.
3. In the Almost done! dialog, select your communication preferences, and then click Submit.

4.1.2.2. NGC Subscription - Existing NGC User

This section describes signing in if you already have an NVIDIA account.

After successfully signing into your NVIDIA identity account, you will need to choose an existing NCA account to claim the new software subscription or create a new NCA account that will generate a separate NGC org linked to the new account to claim the subscription.
Select your NVIDIA Cloud Account

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyNCA-VDR (0474895331875198)</td>
<td>Owner</td>
</tr>
<tr>
<td>ExternalIDP (0462258828931128)</td>
<td></td>
</tr>
<tr>
<td>nvaie-stage (0436885730436677)</td>
<td></td>
</tr>
<tr>
<td>kdtwnxodlOqi (0278214794327184)</td>
<td>Owner</td>
</tr>
<tr>
<td>i1dyqpfbrhvo (0278149351511184)</td>
<td></td>
</tr>
<tr>
<td>xvy2tenvwbmgl</td>
<td></td>
</tr>
</tbody>
</table>

Create New NVIDIA Cloud Account

Owner indicates that you are the owner of the account.

Note: You must be an ‘owner’ of an existing account to activate a new subscription against it.

If this is your first NCA account or you chose to create a new account for your subscription, you are prompted to name your account with a meaningful name that will help you identify it easily the next time you sign-in.
Create your NVIDIA Cloud Account

Start by giving your cloud account a unique name. This name will help you identify your account in the future.

Name *

My2ndNCA

Create NVIDIA Cloud Account

Accept the "Terms of Use" and "Privacy Policy."

Terms of Use

Please review and accept the following Terms of Use

☐ I agree to the NVIDIA Privacy Policy
☐ I agree to the NVIDIA GPU Cloud Terms of Use
Your NVIDIA Cloud Account is created, and you are automatically redirected to your enterprise NGC org.

Your access to NVIDIA NGC org is now complete. You can choose to complete the setup of your NVIDIA Cloud Account now, or at a later time.

Follow the steps in Setting up your NCA Account to finish setting up your NCA account. You will need to access your NCA account to add users to your enterprise NGC org.

4.1.3. Accessing NGC from an NCA Invitation Email

Follow these steps to accept an invitation to join an NVIDIA Cloud Account and access NGC.

1. Check your email inbox for a message titled "You’ve been invited to an NVIDIA Cloud Account." Open the email and click Login to proceed.
2. If you are new to NVIDIA, you are prompted to create an NVIDIA identity account. Create a password that is at least 9 characters long and uses a mix of uppercase and lowercase letters, numbers, and special characters. If you already have an NVIDIA identity account, enter your password to continue. You can skip to Step 6 below.
Create Your Account

Email

Display name

Enter your display name

Date of birth

YYYY-MM-DD

Password

Enter your password

Confirm password

Enter your password

Log In With Security Device >

By proceeding, I agree to the NVIDIA Account Terms Of Use and Privacy Policy

Create Account

More Signup Options

You will be asked to verify your email address in a confirmation email.
3. Check your email inbox for a message titled "NVIDIA Accounts". Open the email and click Verify Email Address.

Hello,

We are almost done creating your NVIDIA account. You can use this account to log in to GeForce NOW, GeForce Experience, NVIDIA Games, NVIDIA Indie Spotlight, NVIDIA Omniverse, NVIDIA Game Developer Portal, GTC, NVIDIA Application Hub, and NVIDIA AI.

Click the link below to verify this email address.

Verify Email Address

If you did not register for an NVIDIA Account, someone may have registered with your information by mistake. Contact NVIDIA customer care for further assistance.

The email confirmation message will display in your browser.
4. NVIDIA would like permission to send you the latest news related to our software and products, as well as learn more about how you use our websites to make sure we send you information relevant to you. Select your options and click Submit.

5. You are prompted by NVIDIA Cloud Accounts to accept the invitation to join your company's account. Click Accept Invitation to continue joining.
6. Enter your password (required for security).
7. Accept the terms of use and privacy policy to access your software subscription.
You can now access the NGC org.
Chapter 5. NGC Org Authentication Using an External SSO Provider

An enterprise org can be federated to an external SSO/IdP identity service to centrally manage a company’s rules for user authentication to cloud services.

The setup process to federate an NGC org to an external SSO identity provider requires manual steps between the customer and an NVIDIA representative. To learn more on how to bring your own SSO/IdP service to NGC, contact your NVIDIA sales representative or submit a support case with NVIDIA Enterprise Support. If you don’t have an NVIDIA sales rep or an active support contract, email ngc-sso@nvidia.com with your request.

The setup process to federate an NGC org to an external SSO identity provider requires manual steps between the customer and an NVIDIA representative. To learn more on how to bring your own SSO/IdP service to NGC, email ngc-sso@nvidia.com with your request.

After an NGC org is federated against an enterprise SSO/IdP identity service, the users signing into NGC will automatically be prompted to authenticate against their enterprise SSO/IdP service and redirected back to NGC after a successful sign-in. To add new users to an org federated to an external SSO/IdP provider, the org owner follows the same steps described in #unique_22. Alternatively, suppose the external IdP provider supports OIDC claims to identify the user’s membership to a group or set of groups. In that case, NGC can be configured to map these OIDC claims to NGC org, teams, and role assignments. See the section NGC IdP Membership Rules for more details.

Note the org owner role is created as the break-glass/recovery account and must always authenticate through an NVIDIA account. This provides access to the org in case the external SSO/IdP service is unavailable. See the section #unique_23 to learn how to sign in to your org owner account.

NVIDIA recommends org owners add themselves to their enterprise org as new users and assign access rules set at the org level with admin roles across all org services. Using the same org owner email address to add themselves as new admin users is supported. The users’ new service admin accounts will be authenticated using the external SSO/IdP authentication service and inherit the same role privileges as their org owner account.

Important:
For NVIDIA to automatically detect the deletion or deactivation of a user managed by the external IdP, the customer must also integrate their IdP user management service to our NVIDIA identity federation system using "SCIM" or "Security Event Tokens" and allow the user update events to flow to NVIDIA. NVIDIA will use these events to ensure deleted user accounts from the enterprise side are reflected across all NVIDIA services. Any credential assets (e.g., API keys) owned by the removed user are immediately revoked upon receiving the deletion or deactivation event.

During the federation process, NVIDIA will share our IdP federation "Synchronization of users and group changes" document, and we will need to record a written acknowledgment (email is okay) of receipt of this information, and a decision on whether or not you (customer) will implement the security event integration.

Some NVIDIA products (like NGC) provide a UI option for customers to manually disable/deactivate/dis-enroll users manually within the NVIDIA application and trigger the revocation of credential assets by deleting the user. For example, NGC supports removing a user from an NGC org, and this event automatically triggers the revocation of user-owned NGC API keys. However, such application-specific admin functions do not remove users from other NVIDIA applications. The risk with this process is that if the user were part of other NVIDIA services that grant credential assets, these assets would remain as active dangling assets against those services because the user account remains "active" in our central identity service. The user’s API keys are thus not revoked. The only way to guarantee NVIDIA-wide user account removal is to integrate user event sharing with the NVIDIA IdP federation service, and the customer must be guided to execute the NVIDIA recommended de-provisioning operations in the NVIDIA IdP federation service.

5.1. NGC IdP Membership Rules

An enterprise org can be federated to an external SSO/IdP identity service to centrally manage a company’s rules for user authentication to cloud services.

When the NGC org is linked to an external IdP, the org owner will see the ability to start creating membership rules under the Organization > External IdP configuration page.

Important: Only the org owner role is permitted to create membership IdP Rules.

If the NGC org is not linked to an enterprise-owned SSO IdP provider, the ‘External IdP’ web prompt is disabled with a message stating the org is not linked to an IdP. You can request to link your org to an enterprise-owned SSO IdP by emailing ngc-sso@nvidia.com.
The membership rules feature uses Open ID Connect (OIDD) claims containing the user's membership attributes, either included in the ID token or retrieved from the OIDD user-info endpoint. Here is an example of an OIDD claim that carries membership attributes.
The ID-token contains several claims that carry attributes associated with the user. Specifically, we are interested in the "groups" claims values that map users to specific membership groups in their Active Directory (AD) service.

It's important to note that the external IdP uses the name "groups" to carry membership attribute values in the example above. However, other IdP providers may use a different name for their membership attribute claim. If your IdP provider uses a different claim name, check that NGC supports it by emailing ngc-sso@nvidia.com.

An org owner will create membership rules by mapping the name (alias) value of the IdP 'groups' claim to NGC org roles and permissions. Within the enterprise AD service, users assigned to these groups will receive the roles and permissions assigned to the group name in the NGC IdP rules.

Example

In this example, we are using Okta as the enterprise-owned SSO IdP provider. It is assumed the same person managing Okta also has NGC org owner permissions.

Okta Settings
First, the NGC org gets linked as a client application to the Okta IdP service.

On Okta, managed users get assigned to the NGC client application, enabling them to sign in to NGC using their Okta SSO account.

At this point, users *have not* been assigned to a 'group'.
On Okta, secure AD groups are created, and users can be assigned to a group or a set of groups.
In this example, Adam and Amy are assigned to the NGC_AIE_PR_Admin group. Note that this is being done manually using the Okta user management feature, but this is typically managed automatically by using an enterprise active directory integrated into the IdP provider.
At this point, Adam and Amy can sign into NGC, but there isn’t an IdP rule that assigns them NGC org roles and permissions. The next section covers creating the NGC IdP membership rules that will grant Adam and Amy their roles.

Configuring NGC

After the IdP groups are created and users are assigned to secure AD groups on the Okta IdP side, the administrator (org owner) is ready to configure NGC IdP membership rules.

NGC

In the NGC web application, go to NGC External IdP settings and click Create Rule.

Type in a Rule Name that describes the purpose of the rule.

Then, under the If group equals field, enter the name of the IdP ‘group’ claim that will map to this rule. Note that the name must match exactly and is case-sensitive.

Finally, assign the NGC team or org-level access, and assign cloud service roles to grant to users that are assigned to the group. Click Save.
### Rule Name

NVAIE and Private Registry admin

### If group equals

NGC_AIE_PR_Admin

⚠️ This field is case sensitive. Please ensure the group name entered matches the one in your IdP.

### then assign to

TB2-org (no team)

### as

**Base Command Platform**

<table>
<thead>
<tr>
<th></th>
<th>Admin</th>
<th>User</th>
<th>Viewer</th>
</tr>
</thead>
</table>

**Fleet Command**

<table>
<thead>
<tr>
<th></th>
<th>Admin</th>
<th>Operator</th>
<th>Viewer</th>
</tr>
</thead>
</table>

**NVIDIA AI Enterprise**

- Viewer

**Omniverse Cloud**

<table>
<thead>
<tr>
<th></th>
<th>Admin</th>
<th>User</th>
<th>Read</th>
</tr>
</thead>
</table>

**Private Registry**

- Admin

**Organization**

<table>
<thead>
<tr>
<th></th>
<th>User Admin</th>
</tr>
</thead>
</table>
Once the rule is saved, the org owner must activate the rules to apply the membership roles to Adam and Amy when they sign in.

This completes the creation of an NGC IdP membership rule.
The org owner can create multiple rules to support multiple group claim values from the IdP. An example of multiple IdP membership rules created can be seen below.

Important: The NGC IdP membership rules do not go into effect until they are "activated". Users’ accounts that were added using the manual method will continue to use NGC role permissions assigned through 'Users' invite user membership configurations.

When the Activate Rules button is clicked, the org owner is prompted to confirm activation of the IdP rules. When the rules are activated, the NGC IdP rule system reviews user memberships previously added to the org using the "user invitation" method. The NGC IdP rule system will check if the user account maps to a new IdP membership rule. If one does, the previous account membership is deleted, and a new user account membership using the same email address and IdP association will be created. The permissions and roles that get assigned to the new account membership are based on the IdP 'groups' claim attribute.

Note: Previous user accounts that are determined not to have an associated IdP rule remain as active user accounts under "Users" account memberships. An org owner or user admin can remove these users if the org should only be accessible by members mapped to IdP rules.
Chapter 6. Activating Your Subscription (Offer Dependent)

This section describes activating a subscription and linking it to your NGC Account.

Note: These steps are only required for customers who have been given an activation code as part of the purchase of a GPU or DPU.

1. Access the activation page directly via Activate Subscription.
2. Sign in to NGC with your email address and password if prompted. If you have not created an NGC account, create one now.
3. On the Activate Subscription page, enter your Business Information using your company's headquarters address and the serial number or activation code described by the specific offer.
   If entering multiple serial numbers or activation codes, use a comma to separate each.
4. Click Activate Subscription.
5. Once the system validates the serial numbers, review the information displayed and click Request Activation.
6. The Subscriptions page will display for your organization with the active NVIDIA AI Enterprise subscription.
7. Use the left navigation and click Enterprise Catalog to access the NVIDIA AI Enterprise software suite.
NVIDIA AI Enterprise

NVIDIA AI Enterprise, an enterprise-grade AI software platform, accelerates and streamlines development and deployment of production-ready generative AI, computer vision, speech AI, data science, and more. With enterprise-grade security, stability, manageability, and support, NVIDIA AI Enterprise speeds time to value while mitigating the potential risks of open-source software, ensuring business continuity and a reliable platform for running mission-critical AI applications.

Learn More
Chapter 7. Switching Orgs or Team After Logging into NGC

This section describes switching to a different org or team after logging in.

In the top menu bar, click your user account icon. Then, select your org menu to expand the view to other available orgs. If you manage many orgs, you can use the search field to find the specific org you want to select. Select the desired org by clicking it once.

Depending on the org or team you select, your current page may also refresh.
Chapter 8. NGC API Keys

NVIDIA NGC API keys are required to authenticate to NGC services using NCG CLI, Docker CLI, or API communication. NVIDIA NGC supports three types of API keys.

**API Key (Original)**
This is the original type of API key available in NGC since its inception. This type allows you to create only one "API key" at a time. Generating a new key automatically revokes the previous one, as they cannot be rotated. The active key immediately becomes invalid when you create a new key.

Note: NVIDIA will continue to support this key type for services that have not transitioned to the next-generation API keys. However, we encourage customers to migrate to our next-generation API keys when possible.

NVIDIA NGC introduces two new types of API keys supporting Role-Based Access Control (RBAC) configuration and the ability to manage the state of each key.

**Personal API Key**
Any user who is a member of an NGC org can generate Personal API Keys. These keys are tied to the user's lifecycle within the NGC org and can access up to the permissions and services assigned to the user. During the key generation steps, users can configure which NGC services are accessible by the API key and the time-to-live from one hour to 'never expires'.

**Service API Key**
Service API keys are not associated with individual user accounts; instead, they are linked to an NVIDIA cloud account and manage their lifecycle within the NGC org where they are created. The org owner and members assigned the user_admin role can create and manage Service API keys. The user_admin role must be assigned along with the specific application role for which the user will generate and manage service keys.

Note: Service keys do not currently support listing artifacts in NGC CLI or Docker CLI. This functionality will be added in the future. In the meantime, use a Personal API key to list artifacts.

As NVIDIA rolls out support for "Personal" and "Service" API keys, the original NGC API keys will continue to be supported. We highly recommend generating new API keys using the latest "Personal" or "Service" type API keys. These key types deliver the ability to
configure an expiration date, revoke or delete the key using an action button, and rotate the key as needed.

The NVIDIA NGC applications/services that support Personal and Service Keys are listed below:

<table>
<thead>
<tr>
<th>NGC Application/Services</th>
<th>Service API Keys</th>
<th>Personal API Keys</th>
<th>NGC API Keys (Original)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVIDIA NGC Catalog</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NVIDIA NGC Private Registry (Helm charts are not yet supported).</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NVIDIA NIM™</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>NVIDIA Fleet Command</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NVIDIA Base Command Platform</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

If your NGC service isn’t listed under Personal or Service Keys, continue using the original NGC API key. We’ll update this list by adding support for other NGC services into our next-generation key types.

8.1. Generating a Personal API Key

1. Sign in to the NGC website.
   - From a browser, go to https://ngc.nvidia.com/signin and then enter your email and password.
2. Click your user account icon in the top right corner and select Setup.
3. Click Generate Personal Key from the available options. Personal Keys allow access to a set of NGC service APIs.

4. On the Setup > Personal Keys page, click + Generate Personal Key, on the menu or the pane.
5. In the Generate Personal Key dialog, fill in the required information for your key.

- **Key Name**: Enter a unique name for your key.
- **Expiration**: Choose the expiration date for the key.
6. Click Generate Personal Key when finished.
   Your API key appears in the following dialog.
7. NGC does not save your key, so store it securely. You can copy your API Key to the clipboard by selecting Copy Personal Key or using the copy icon to the right of the API key.
You can generate up to eight personal keys and manage them from the Setup > Personal Keys dashboard. To activate or deactivate a key, click the Active toggle. The Actions (ellipsis) menu allows you to rotate or delete a personal key.
8.2. Generating a Service API Key

1. Sign in to the NGC website.
   From a browser, go to [https://ngc.nvidia.com/signin](https://ngc.nvidia.com/signin) and then enter your email and password.
2. Select Organization from the user account menu on the upper right.

Select Service Keys on the organization dashboard.
3. On the Organization > Service Keys page, click + Create Service Key button to create a key.

![Create Service Key](image1.png)

4. In the Create Service Key dialog, fill in the required configuration. Service keys currently support services such as NVIDIA NIM, NGC Catalog, and Private Registry. Assign scopes and resource permissions to the key.

![Create Service Key](image2.png)

In the Entity Type field, select from the available options to grant to the API key.

Note: If you choose ‘All Entity,’ the organization will be set to ‘nvidian’ and cannot be changed. To select other organizations, please consider different entity types such as ‘All Containers,’ ‘All Models,’ etc.”
In the Scope field, choose from the available options.

5. Click Next Step to review your key configuration.
6. Once you verified the configuration, click Confirm to generate your service key. Your service key appears in the next dialog.

7. NGC does not save your key, so store it securely. You can copy your API Key to the clipboard by clicking the copy icon to the right of the API key or the Copy Service Key button.
Make sure to copy the key value before leaving this page. Once you navigate away, the key value cannot be retrieved, and replacing it will require generating a new key.

NGC supports multiple Service API keys, which are managed from the Organization > Service Keys dashboard.

To activate or deactivate a key, click the Active toggle. The Actions (ellipsis) menu allows you to rotate or delete a service key.

Note: When managing containers, ensure the scopes Get Container and Get Container list are assigned to your service key. For other types of artifacts, add the Get Artifact and Get Artifact list scopes. These scopes are the minimum required to discover the artifacts that need to be managed. Refer to the NGC Catalog User Guide and Private Registry User Guide for more information.
8.3. Generating NGC API Keys

This section describes obtaining an API key to access locked container images from the NGC Registry.

1. Sign in to the NGC website.
   From a browser, go to https://ngc.nvidia.com/signin and then enter your email and password.
2. Click your user account icon in the top right corner and select Setup.
3. Click Generate API Key to open the API Key page.
   The API Key is the mechanism that authenticates your access to the NGC container registry.
4. On the API Key page, click + Generate API Key to generate your API key.
   A warning message shows that your old API key will become invalid if you create a
   new one.
5. Click Confirm to generate the key.
   Your API key appears.
   You only need to generate an API Key once. NGC does not save your key, so store it
   securely.

   Tip: You can copy your API Key to the clipboard by clicking the copy icon to the right of
   the API key.

   You can generate a new one from the NGC website if you lose your API Key. When you
   generate a new API Key, the old one is invalidated.
Chapter 9. Notification Services

The NGC Notification Services feature enables NGC users to subscribe to email notifications to receive service change events. By subscribing to notifications, users can stay updated with the latest changes and developments in the NGC cloud platform and its services.

NGC customers can be informed of the following types of changes:

▶ Customer-impacting service enhancements (release notes)
▶ Security vulnerabilities (CVEs) and scanning reports
▶ Software end-of-life announcements
▶ Scheduled web portal maintenance to an NGC property

NGC customers can subscribe to notifications in the following ways:

▶ During their first sign-in, the NGC portal will pop up a modal allowing users to set their notifications preferences.
The following sample toast notification confirms the user’s email preference settings:

Email preferences has been updated for 3 services:
- Private Registry
- Organization
- NVIDIA AI Enterprise Essentials

▲ After their initial sign-in, users can edit their notification preferences under their NGC user account settings page.
Notification preferences are organized based on the subscriptions enabled within the organization. Access to these preferences will be gated by the service roles assigned to each user.