# Admin Console Documentation

SIEMENS

## About Siemens Digital Industries Software

Siemens Digital Industries Software is a global leader in the growing field of product lifecycle management (PLM), manufacturing operations management (MOM), and electronic design automation (EDA) software, hardware, and services. Siemens works with more than 100,000 customers, leading the digitalization of their planning and manufacturing processes. At Siemens Digital Industries Software, we blur the boundaries between industry domains by integrating the virtual and physical, hardware and software, design and manufacturing worlds. With the rapid pace of innovation, digitalization is no longer tomorrow’s idea. We take what the future promises tomorrow and make it real for our customers today. Where today meets tomorrow. Our culture encourages creativity, welcomes fresh thinking and focuses on growth, so our people, our business, and our customers can achieve their full potential.

Support Center: **https://support.sw.siemens.com**

Send Feedback on Documentation: **https://support.sw.siemens.com/doc_feedback_form**

# Table of Contents

# 1. Getting Started with the Admin Console

## Introduction

The Siemens Xcelerator Admin Console is a centralized management tool that enables customer administrators to efficiently manage their Siemens Xcelerator product subscriptions. It provides a unified approach to subscription management across the entire Siemens Xcelerator portfolio, streamlining the administration process regardless of the product being managed. With the Siemens Xcelerator Admin Console, portfolio administrators can onboard users once and efficiently assign access to multiple products.

> **Note**
>
> Each Enterprise Customer Account(ECA) is associated with at least one ECA administrator, who manages account through the Siemens Xcelerator Admin Console.

### Core Capabilities

The Siemens Xcelerator Admin Console currently provides the following capabilities:

**Manage Product Subscriptions**:

- View product and license-based addon subscriptions
- Manage user assignments for products and addons
- Manage server users and their credentials
- Bulk import of users

**Audit and Reporting**:

- Track token consumption
- Generate audit log reports

**Authentication**:

- Add a custom identity provider
- Configure Multi-Factor Authentication(MFA)
- Enable Domain Validation

# Getting Started with the Siemens Xcelerator Admin Console

This section explains how to get started with the Siemens Xcelerator Admin Console. Contact your Siemens Xcelerator subscription purchaser for administrator access to Enterprise Cloud Accounts (ECA).

## Access the Siemens Xcelerator Admin Console

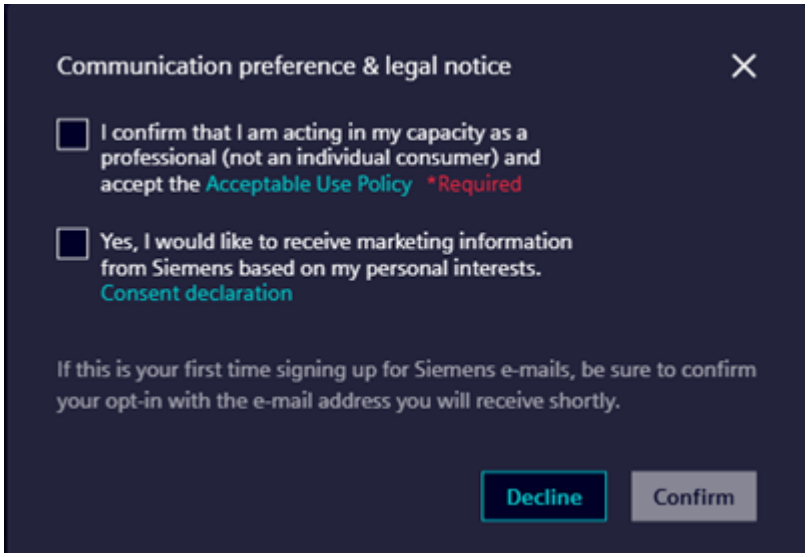
If you are an Enterprise Cloud Account (ECA) administrator, you should receive an email notification confirming your access along with a link to access the Siemens Xcelerator Admin Console. To access, click **https://cloud.sws.siemens.com/admin/**

**Note**

- First-time users must create a Siemens ID account before proceeding.
- Use the same email address to create the Siemens ID account that received the notification.

## Setting your Enterprise Cloud Account Name

During the initial sign-in, configure your communication preferences and review the Acceptable Use Policy. Select your consent preferences and click **Confirm**.




Your account identifier is a number that uniquely identifies your ECA. However, you have the option to add a memorable account name for easy recognition, especially if your organization has multiple ECAs.

**Note**

You can update the account name at anytime using the "Edit Account" option. For more information, refer to **Account Details**.

## Adding ECA Administrators

You can enhance by adding additional ECA administrators. The **Account details and settings** page shows the current list of administrators. Current administrators can add or remove other administrators. For more information, refer to **Manage Additional Administrators**.

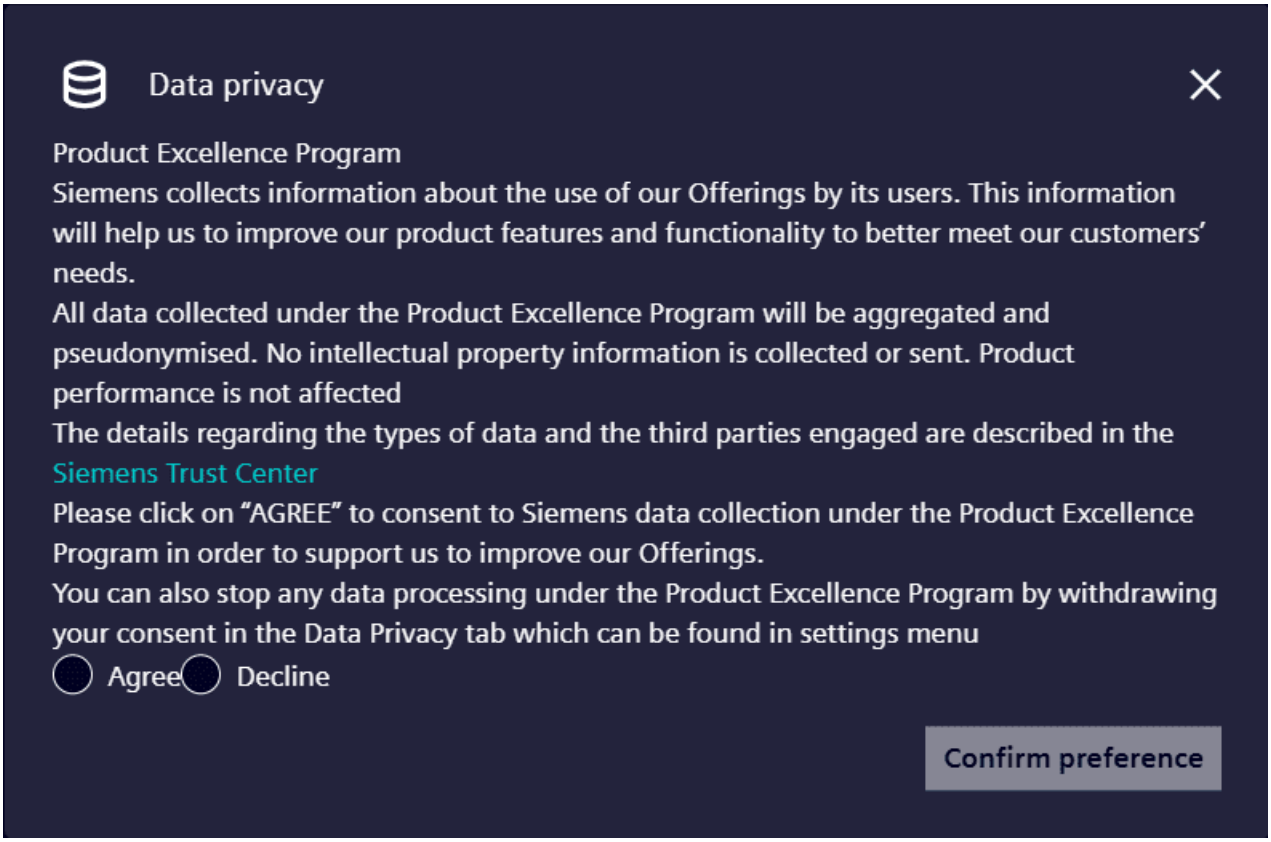
## Consent for the Product Excellence Program

The Product Excellence Program is a voluntary initiative designed to gather valuable insights into how our offerings are used. By participating, you contribute to the continuous improvement of our product features and functionality, helping us better meet the evolving needs of our customers.

By analyzing aggregated and anonymized usage patterns, we gain crucial insights into how our products are used in real-world scenarios. This information is vital for identifying areas for improvement, prioritizing new features, and optimizing existing ones.

You can provide your consent to participate in the Product Excellence Program either through:

- When you log in to an ECA for the very first time, a **Data Privacy** pop-up will automatically appear. To enable data collection, please read the terms, select **Agree**, and then click **Confirm preference**.




- You can also manage your preference at any time through the application's settings:

1. Click on your profile icon.

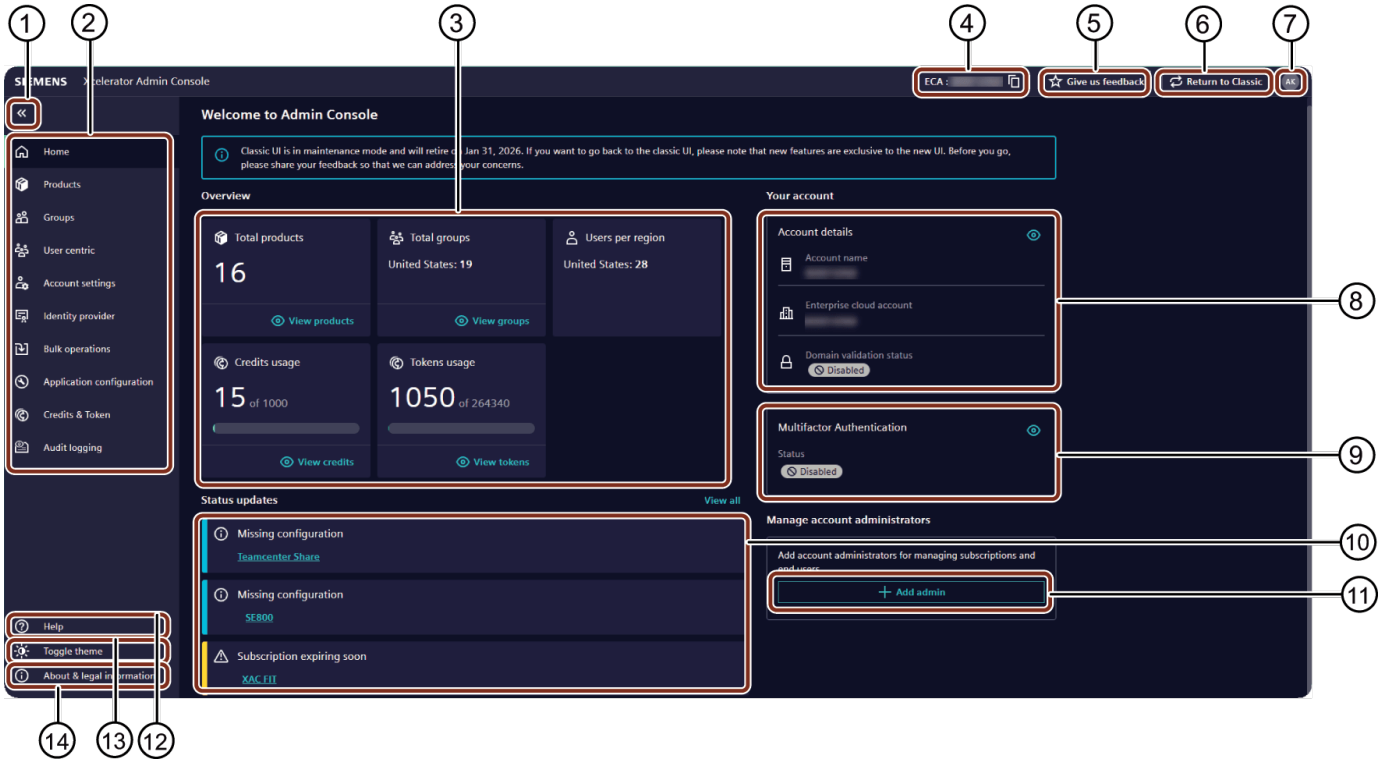
2. Select **Settings**.
3. Enable or disable the "Product Excellence Program" toggle switch and toggle the switch in the **Analytics & Privacy** section.

# User Interface

The Siemens Xcelerator Admin Console user interface enables Enterprise Cloud Account (ECA) administrators to manage purchased subscriptions and control user access to products.

## Home

The Home screen of the Siemens Xcelerator Admin Console provides a centralized dashboard for administrators to manage and monitor their Enterprise Cloud Account (ECA) environment. It displays account details, the status of the configured identity provider, and options for managing additional administrators. Additionally, it highlights product status updates, such as missing configurations, expired subscriptions, and upcoming expirations.




① Allows you to expand or collapse the navigation panel

② Navigation tabs include the following application features:

- **Products**: Provides a complete list of all subscribed products

- **Groups**: Allows you to configure and manage synchronization of groups and users from a custom identity provider (IdP)
- **User centric**: Allows you to access a centralized, region-based view of user information.
- **Account settings**: Allows you to manage account settings, including editing account information, managing domain validation, and enabling multifactor authentication (MFA)
- **Identity provider**: Allows you to manage user authentication and control access within the ecosystem
- **Bulk operations**: Allows you to import multiple users to a product
- **Application configuration**: Allows you to configure a product for desktop applications using predefined templates
- **Credits & token**: Allows you to configure and manage product resources
- **Audit logging**: Allows you to monitor and download the reports

③ Displays the following system monitoring details:

- **Total products**: Shows the total number of configured products
- **Total groups**: Shows the total number of configured groups
- **User per region**: Shows the total number of assigned users segmented by region
- **Tokens usage**: Shows the number of tokens used out of the total number of tokens available

④ Displays the Enterprise Cloud Account (ECA) ID

⑤ Allows you to provide feedback using an intuitive interface with options of star ratings and text comments

⑥ Allows you to switch back to the legacy user interface if preferred

⑦ Displays the logged-in users email address and allows you to log out of the Siemens Xcelerator Admin Console account

⑧ Displays account details, such as the account name, account ID (ECA) and status of domain validation

⑨ Displays the details of the currently configured identity provider, including its name, type, and configuration status. If no identity provider is configured, the card displays the status of multifactor authentication.

⑩ Displays the following product status updates:

- **Missing Configuration**: Shows the list of products that require configuration
- **Subscription Expired**: Shows the list of products with expired subscriptions
- **Subscription Expiring Soon**: Shows the list of products whose subscriptions are expiring soon

⑪ Allows you to add and manage additional account administrators

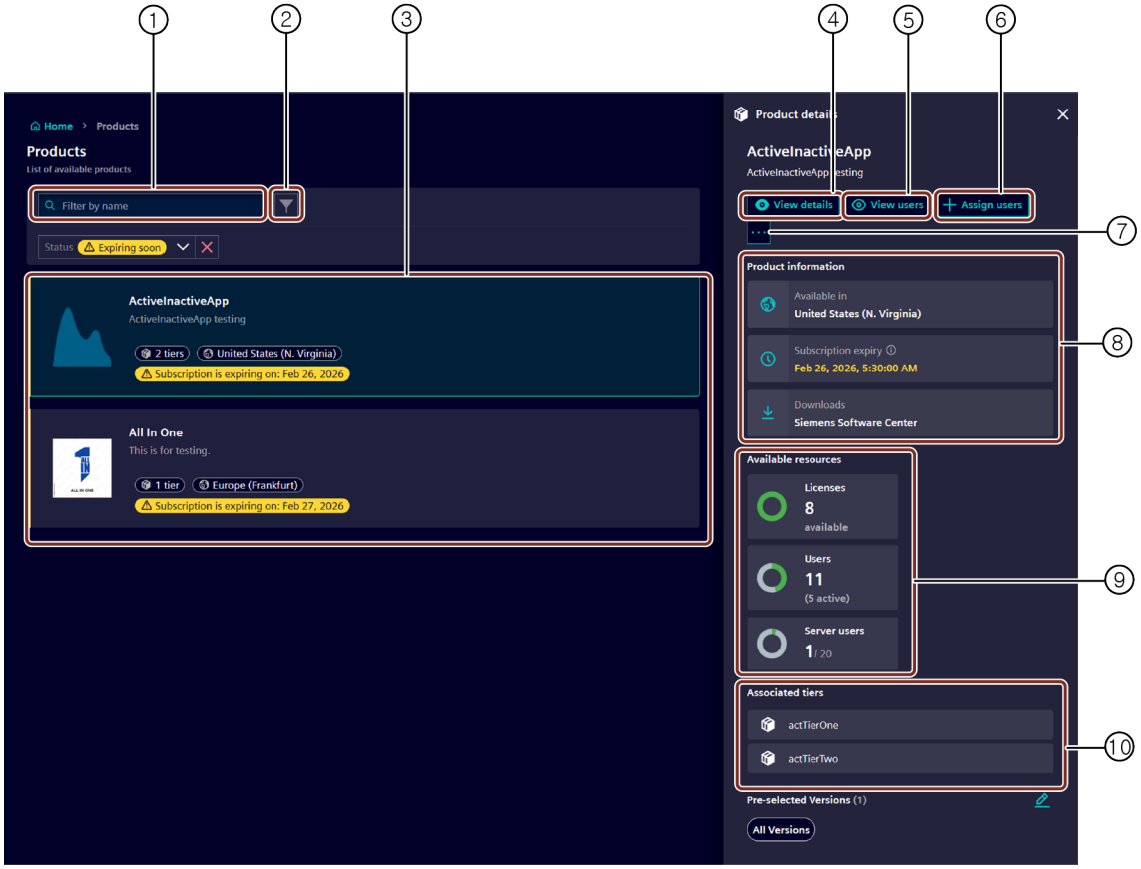
⑫ Allows you to access interactive tours, support resources, product information, and FAQs using WalkMe

⑬ Allows you to switch between dark mode and light mode for personalized viewing

⑭ Allows you to access legal details and policies related to the Siemens Xcelerator Admin Console

## Products

The Products section displays a list of added products and the total number of available products, including their internal names, descriptions, statuses, and assigned regions. Once you select a product, the **Product details** section provides detailed information about the selected product and allows you to assign and manage user assignments.




① Allows you to search for the application of your choice, either by the display name or the internal name.

② Allows you to filter the application list by its status:

- **Active**: Shows products with active subscriptions in the Siemens Xcelerator Admin Console
- **Expired**: Shows products that have expired in the Siemens Xcelerator Admin Console

- **Expiring Soon**: Shows products that are about to expire in the Siemens Xcelerator Admin Console
- **Missing Configuration**: Shows products that are not configured in the Siemens Xcelerator Admin Console

③ Provides a list of all the products

④ Allows you to view detailed information about the selected product

⑤ Allows you to view the list of assigned users

⑥ Allows you to assign users to the selected product

⑦ Allows you to navigate to the following features:

- **View Server Users**: Allows you to navigate to Server Users screen
- **View Subscription Details**: Allows you to navigate to the Subscription Details screen

⑧ Displays the product information:

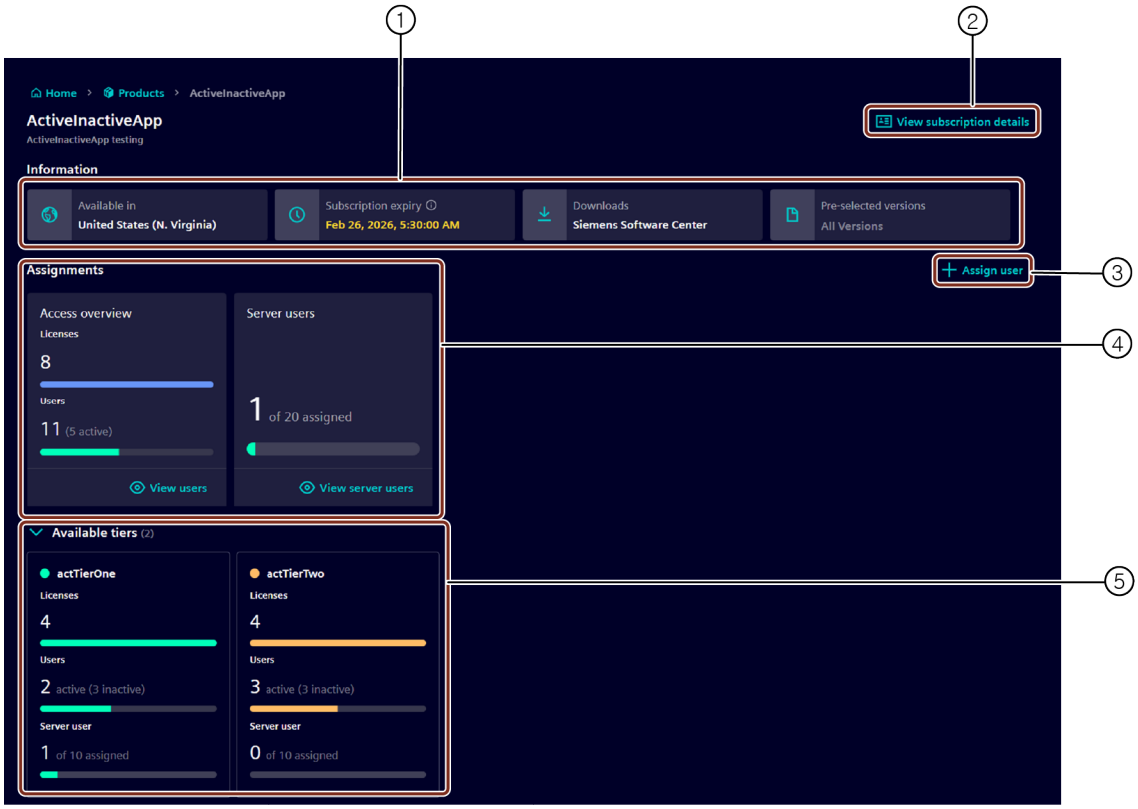
- **Available in**: Displays the region where the product is configured
- **Subscription Expiry**: Displays the product expiration date
- **Downloads**: Allows you to download the Siemens Software Center

⑨ Displays the resources available to the product and the number of resources added

⑩ Displays the associated tiers or sub-products, depending on the product

## View Details

The View details screen allows you to view and manage product metadata information, user assignments, and available resources. It also displays the product subscription details.




① Displays the product information:

- **Available in**: Displays the region where the product is configured
- **Subscription Expiry**: Displays the product expiration date
- **Downloads**: Allows you to download the Siemens Software Center
- **Pre-selected versions**: Displays the pre-selected versions of the product

② Allows you to view detailed product subscription information, such as license name, license quantity, validity period, assigned users, and their statuses.

③ Allows you to assign users to the product.

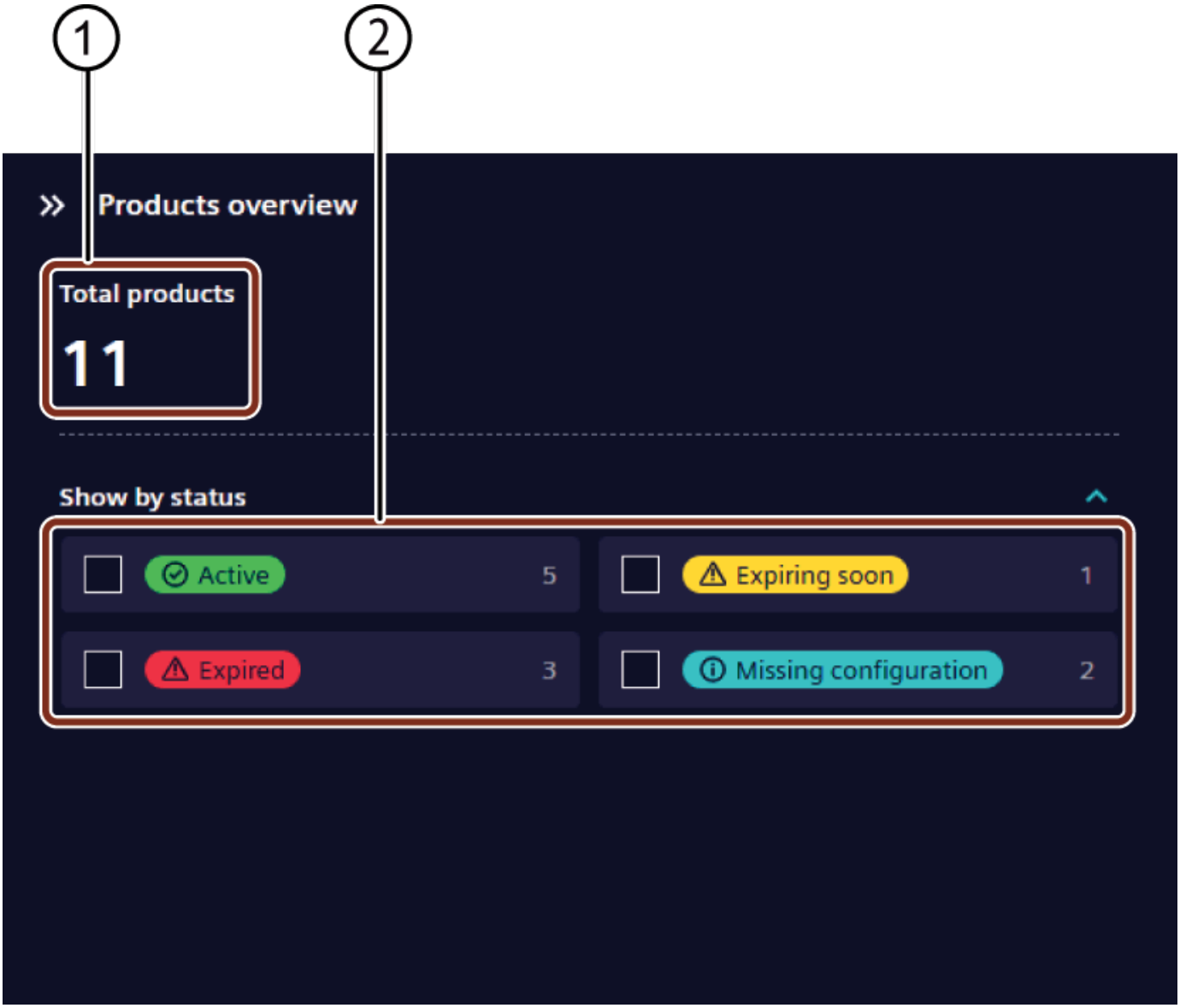
④ Displays the details of the license and user allocation for the product, showing license, user counts as well as server user assignments for the product.

⑤ Displays the details of the license and user allocation for each available tier, showing active and inactive user counts as well as server user assignments per tier.

> **Note**
>
> For Teamcenter Share (Indirect), detailed license and user allocations by tier are not available. Instead, **Available tiers** section displays the total assigned users and maximum capacity for the product.

## Product Overview

The Product overview section displays the total number of products available in the Siemens Xcelerator Admin Console and allows you to filter the application by its status.




① Displays the total number of products configured

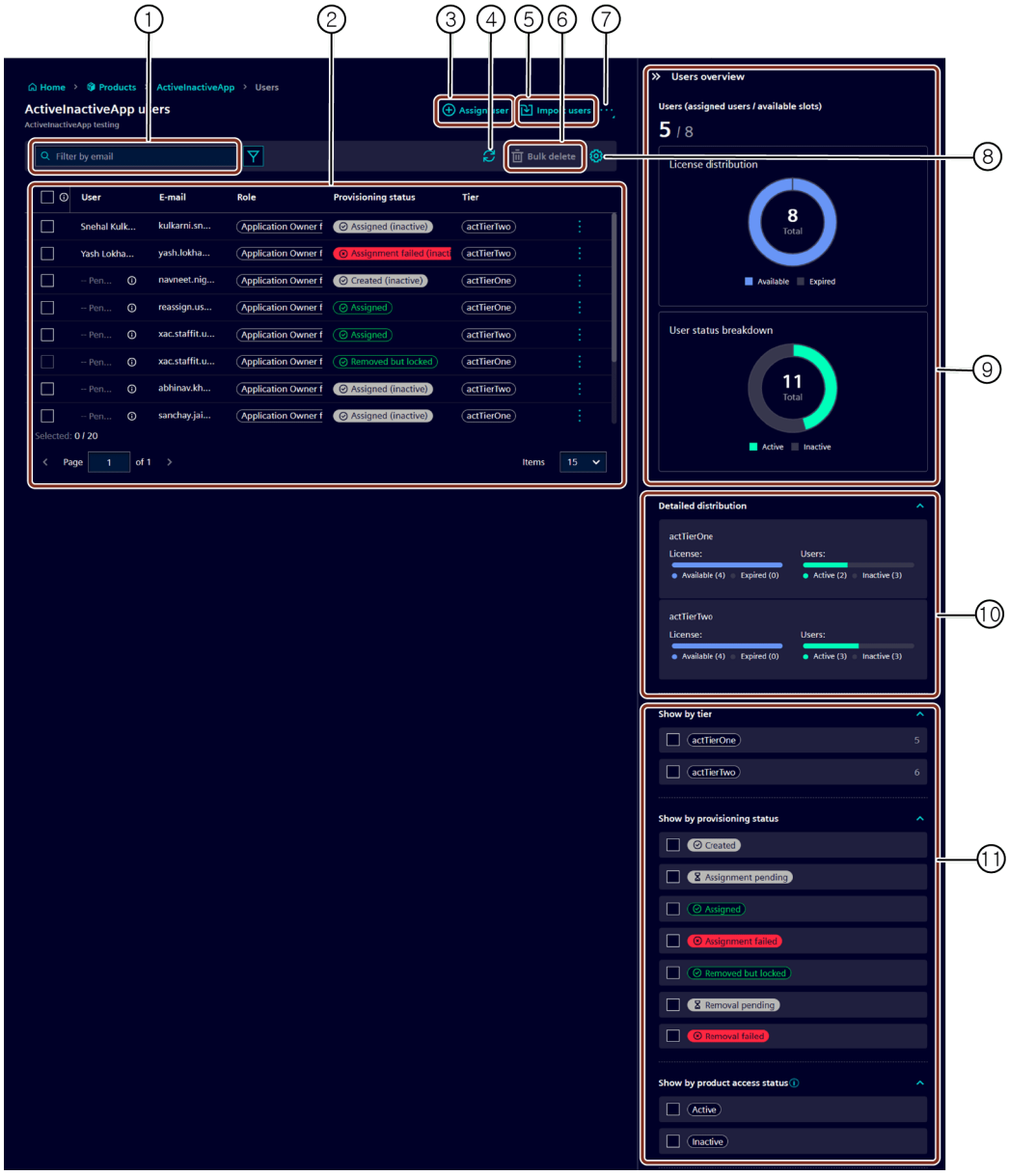
② Allows you to filter the application list by its status:

- **Active**: Shows products with active subscriptions in the Siemens Xcelerator Admin Console
- **Expired**: Shows products that have expired in the Siemens Xcelerator Admin Console
- **Expiring Soon**: Shows products that are about to expire in the Siemens Xcelerator Admin Console

- **Missing Configuration**: Shows products that are not configured in the Siemens Xcelerator Admin Console

## User Details

The user details section offers a comprehensive list of all the users assigned to the product including their names, email addresses, roles, provisioning status, and assigned tiers. This section also provides on overview of distribution of license between users among the available tiers.




① Allows you to search for the application of your choice, either by the display name or the internal name.

② Provides a list of all the users

③ Allows you to assign users to the product

④ Refreshes the users list

⑤ Allows you to bulk import users to the product

⑥ Allows you to bulk delete users from the product

⑦ Allows you to download user list, view user downloads, Bulk environment edit

⑧ Allows you to customize the table columns of your choice

⑨ Displays an overview of user status breakdown and license distribution

- **Assigned Users/Available Slots**: Displays the current user count against the total available slots
- **License Distribution**: A pie chart visualization of the distribution of available and expired licenses
- **User Status Breakdown**: Displays a pie chart illustration of the proportion of active and inactive users

⑩ Displays the information of license and user status by different tiers (e.g., "actTierOne," "actTierTwo"), showing available licenses and active/inactive user counts for each

⑪ Allows you to filter the users list by tier, provisioning status, and product access status

## Personalization Settings

Personalization settings allows you to configure the user interface to your preferences. You can customize table columns, apply filters, and change the application theme. Most of the settings are saved automatically and restored when you return.

## Column Settings

Column settings allows you to customize the columns displayed in tables across the Admin Console.

- You can show or hide columns.
- You can change the order of columns.
- Column customizations in the table are saved globally across the application. These personalized display settings will persist across other products, if both products use the same table columns.

> **Note**
>
> If a product uses different columns, the Admin Console loads the default columns for that table.

### Filter Settings

Filters allow you to narrow the information displayed in a table.

- Filter settings persist when you refresh the page, when you navigate away and return to the same page, unless you switch tabs. But they will automatically reset when you navigate to a different tab or feature of **Admin Console**.

## Understand ECA Admin Roles and Responsibilities

Enterprise Cloud Account (ECA) administrators are automatically assigned with the Admin role and can perform the following actions:

- Add or remove other ECA administrators.
- Configure products in supported regions.
- Assign, edit, or remove product access for users.
- View order details of product subscriptions.
- Create and delete server users.
- Create, download, or delete app credentials for product configurations.
- Generate and download audit reports.
- View account credits, allocate or remove credits per user.
- Check token balance and allocate or remove tokens per user.

## Configure a Product for an ECA

This section explains how to configure a product for a user in the Siemens Xcelerator Admin Console. You can check the product status to see if it is:

- **Provisioned**: Configuration is complete.
- **In Progress**: Configuration is currently underway.

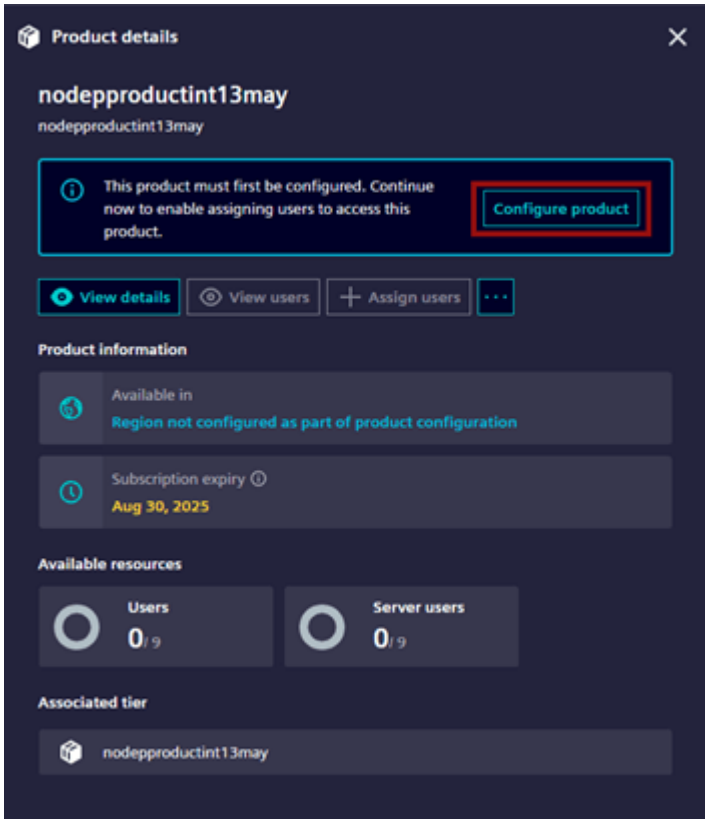
**Note**

- The Configure Product option is unavailable if the product is configured through a Service Engagement and the region status will display "Configuration in Progress".
- You will receive an email notification when the product is configured and ready for user assignment.

## Configure a Product

To configure a product:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. Go to the **Products** tab in the left navigation pane and select the product.
   - Search for the product using its display name or internal name, or use the filter options.
3. In the **Product details** section, click **Configure product**.




4. In the **Product configuration** tab, select the region to store the data and click **Next**.


**Note**

- The selected region cannot be changed after configuration.
- In the **User assignment preview** section, you can preview the assignment or configuration process being performed.

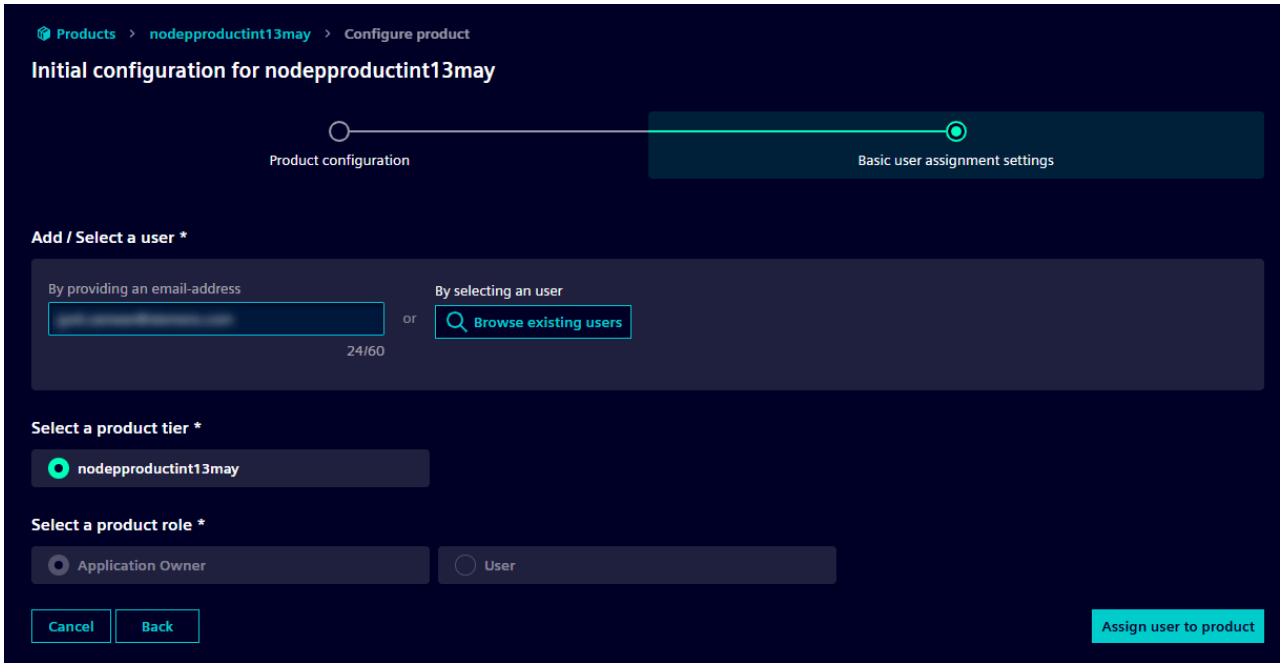
5. In the **Basic user assignment settings** tab, enter the following:

   - Enter the users email address or click **Browse existing users** to select an existing user from the list.

     **Note**

     - If group syncing is enabled, only existing users can be selected. For more information, refer to **Manage Groups and User Synchronization**.
     - If group syncing is disabled, you can select from the list of existing users or add new users. For more information, refer to **Manage Groups and User Synchronization**.
     - If domain validation is enabled, only approved domains are accepted. For more information on validating domain, refer to **Multifactor Authentication**.

   - Select the available product tier.
   - Select the required product role.




6. Click **Assign user to product**.

The product is now configured and ready for user assignment.

Click  button to update the provisioning status to **Active**.

# 2. Manage User Assignments

## Manage User Assignments to Products

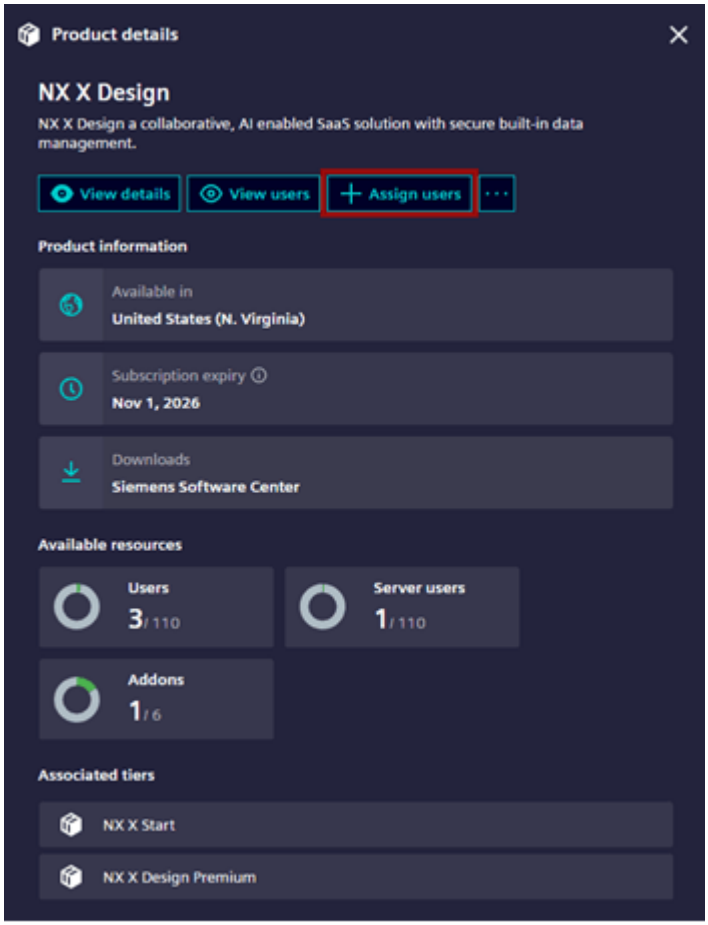
This section explains how to manage users for product tiers and subscriptions. This interface enables administrators to control user access permissions within the product, assigning roles and assignments as required. This ensures that users have the necessary permissions to perform their responsibilities.

### Assign Users to a Product

Assign a user to a product to grant access based on role, tier, add-ons, and environment. This enables the management of user access permissions within the product, providing flexibility in adjusting roles and assignments as needed.

To assign a user to the product:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. Go to the **Products** tab in the left navigation pane.
3. In the **Products** list, select the product.
   - Search for the product by its display name or internal name, or use the filter options.
4. Go to the **Product details** screen and click **Assign users**.




**Tip**

In the **User assignment preview** screen, you can preview the user assignment process being performed.

5. In the **Basic user assignment settings** tab, enter the following:

   - Enter the user email address or click **Browse existing users** to select an existing user from the list.

     **Note**

     - If group syncing is enabled, only existing users can be selected. For more information, refer to **Manage Groups and User Synchronization**.
     - If group syncing is disabled, you can select from the list of existing users or add new users. For more information, refer to **Manage Groups and User Synchronization**.
     - If domain validation is enabled, only approved domains are accepted. For more information on validating domain, refer to **Multifactor Authentication**.

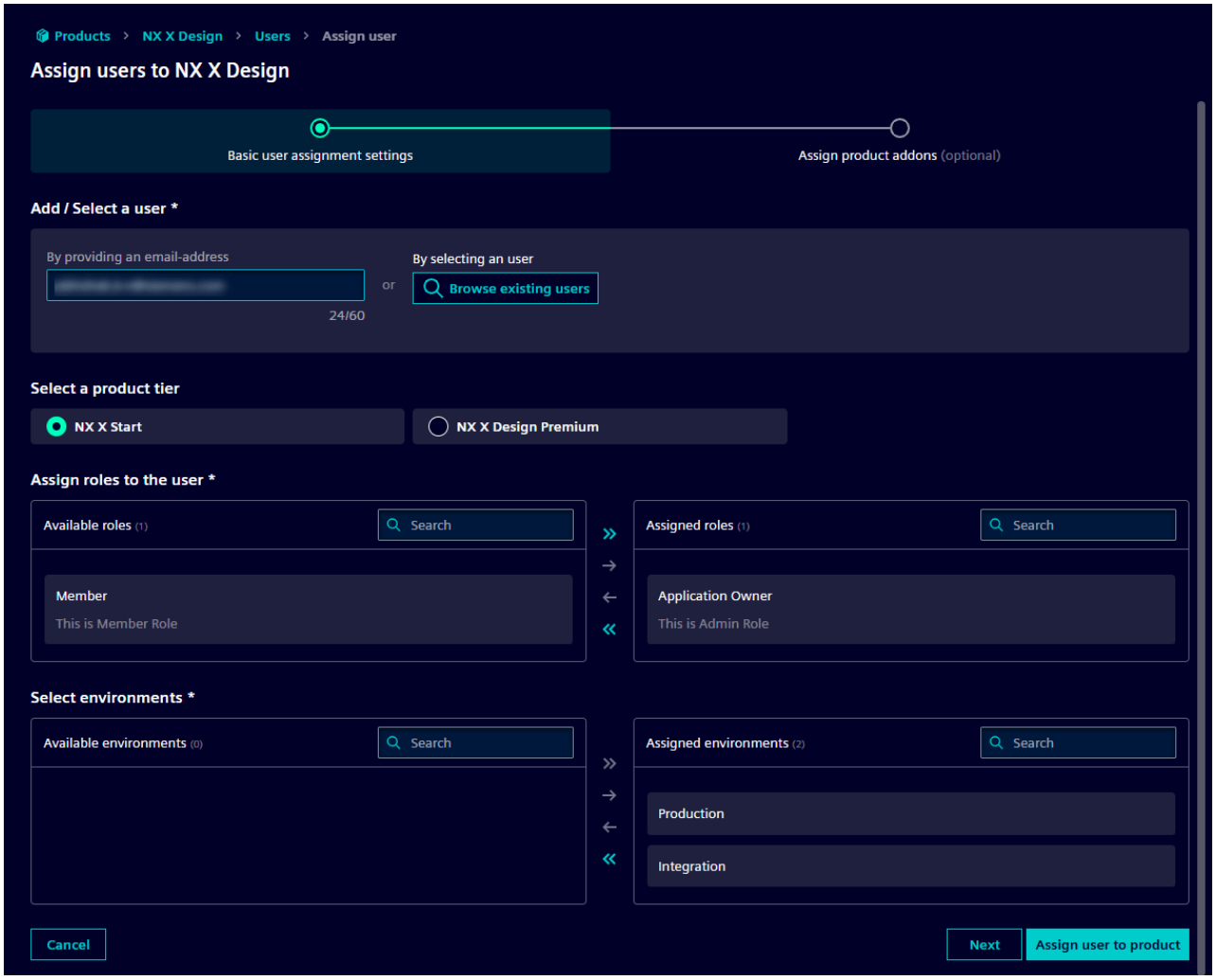
   - Select the product tier.

- Select required roles from the "Available roles" list and click  . To assign all available roles, click  .

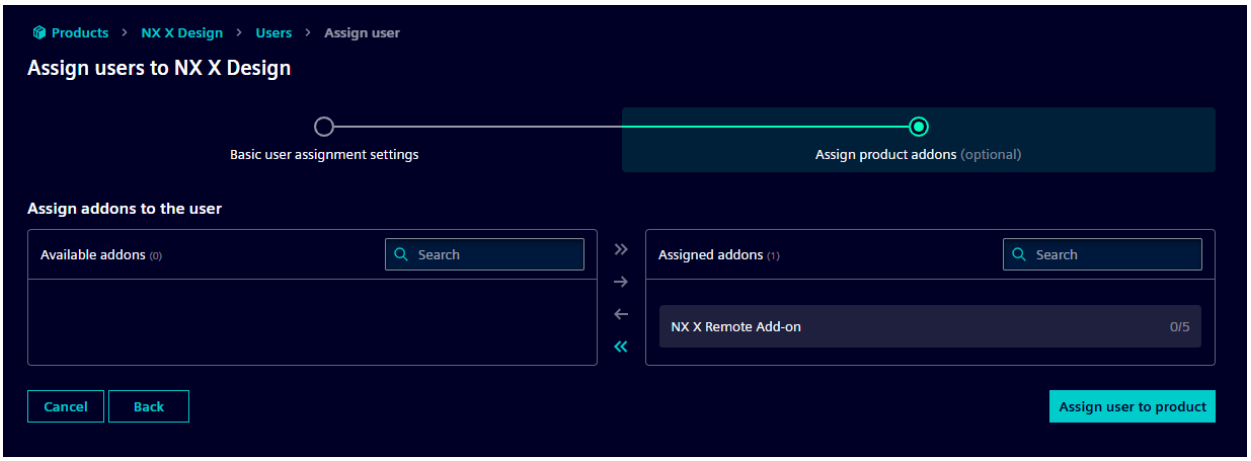
  **Note**
  - If only one user is assigned to the product, the "Admin" role is mandatory and cannot be removed.
  - Available roles depend on the region where the product is provisioned.
  - When configuring a non-decoupled product, the **Admin** role is automatically assigned by default.

- In the product supports environments: Select environments from the "Available environments" list and click  . To assign all available environments, click  .

  **Note**
  - Users must be assigned to at least one environment.
  - Users can also be assigned to all available environments. Some products include multiple environments, including one for production use, and one or more for testing or other purposes.




- Click **Next** or navigate to the **Assign product addons (optional)** tab, if the product supports add-ons. To assign add-ons to the user:
  - Select add-ons from the"Available addons" list and click →. To assign all the add-ons, click ».




6. Click **Assign user to product**.

The user is assigned to the product.

**Note**

- When a user is assigned to the product, their status changes to **Assigned**. The user receives an email with their role details and a link to access the product.
- If your product supports user pooling and exceeds the license limit, additional users are marked as **Inactive**.
- If the assigned list has only one user and that user status is **Created (Inactive)**, you cannot assign more users. To assign users, change the existing user status to **Active**. For more information on activating user status, refer to Edit User.
- If a user is created and the user has not signed in to the assigned product, the **Name** column shows **Pending sign-in**. Once the user signs in, the first and last name appears in the column.

**User Status Types**:

The different "User Status" badges are:

| Status | Description |
|---|---|
| Created | The user is created but not yet assigned to the product. |
| Created (Inactive) | The user is created but not yet assigned. If the assigned list contains only one user with this status, you cannot assign more users. |
| Assignment Pending | The user assignment to the product is in progress. |
| Assignment Failed | The user assignment to the product was unsuccessful. |
| Assigned | The user is assigned to the product. |
| Assigned (Inactive) | The user was previously assigned but has released their license, making the slot available for another user. |
| Removal Pending | The user removal from the product is in progress. |
| Removed but locked | The user is removed from the product, but the assigned license remains locked. |
| Removal Failed | The user removal from the product was unsuccessful. |
| Updating Roles | The users roles are being updated. |

If you see an indicator "**i**" next to the status, click it to view additional details about the users status.

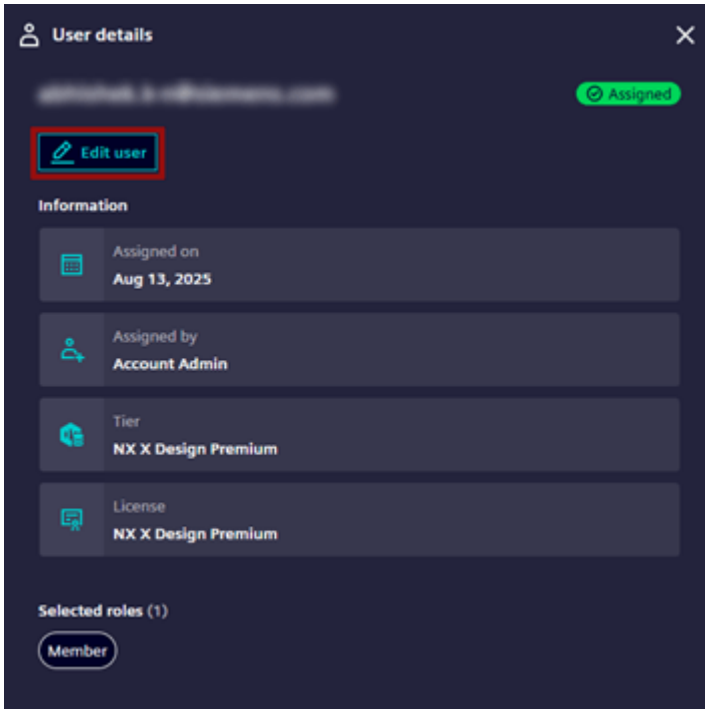
## Edit a User Assignment

To manage user roles efficiently, you can edit existing roles and assign multiple roles to a user in a streamlined process.

> **Note**
>
> The **Edit user** button is disabled if the product is expired or if the user assignment is in "Assignment pending" status.

To edit the roles assigned to a user:

1. In the **Users** section, select the user to edit.
2. In the **User details** screen, click **Edit user**.




3. In the **Basic user assignment settings** tab, update the following:
   - Select the user status:
     - **Active**: An active user counts towards the total number of users subscribed to the product.
     - **Inactive**: An inactive user cannot access the product and does not count towards the user subscription limit.
   - Select the product tier.
   - In the **Assign roles to the user** section, modify the roles:
     - To assign roles: Select from the "Available roles" list and click →. To assign all, click ».
     - To unassign roles: select from the "Assigned roles" list and click ←. To unassign all, click «.

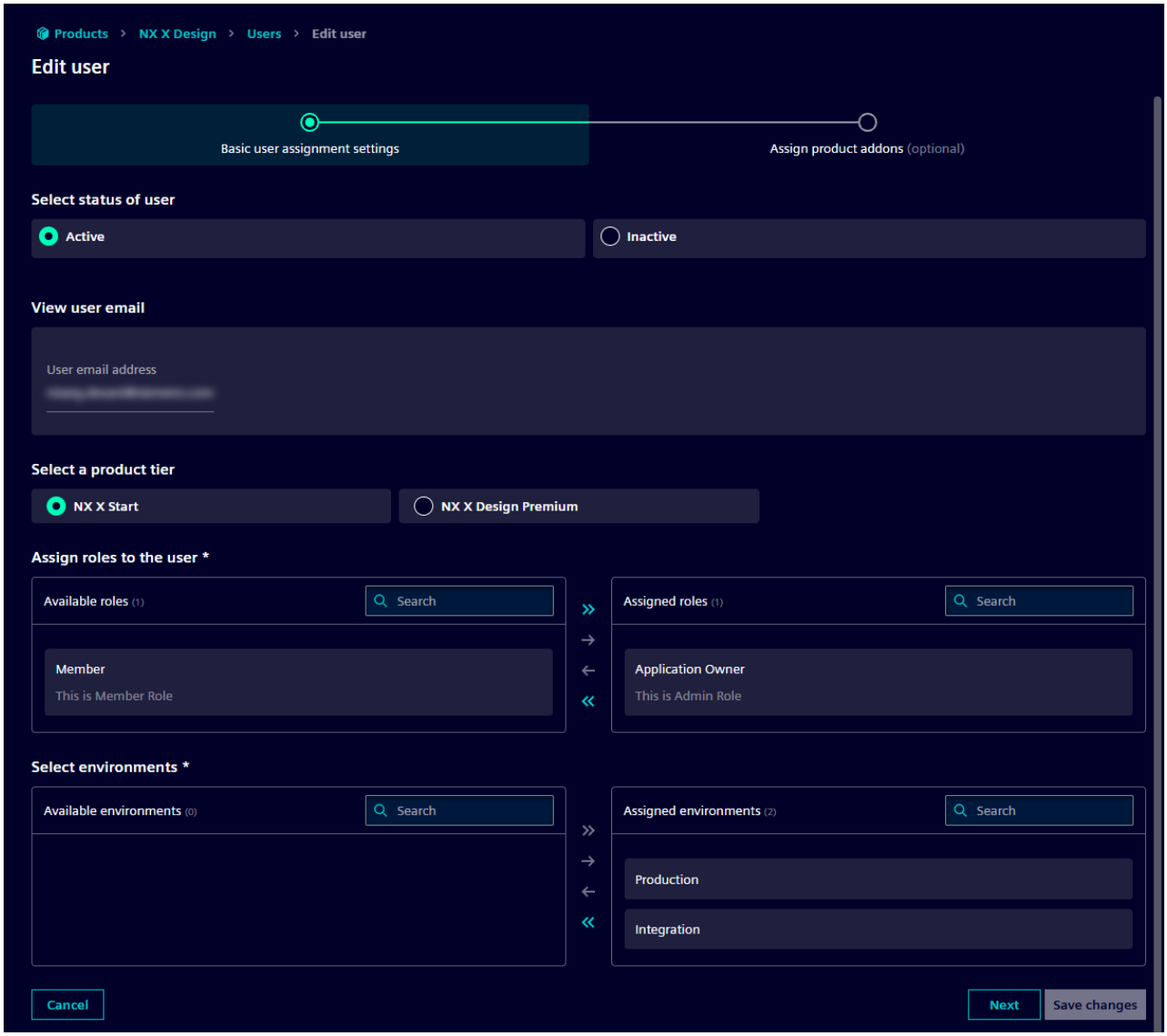
**Note**

- The option to edit roles or assign multiple roles may not be available if the product has an external dependency.
- The **Admin** or **Application Owner** role is mandatory and cannot be revoked if there is only one user associated with the product.
- Available roles depend on the region where the product is provisioned.
- Roles determine the level of access a user has within the product.

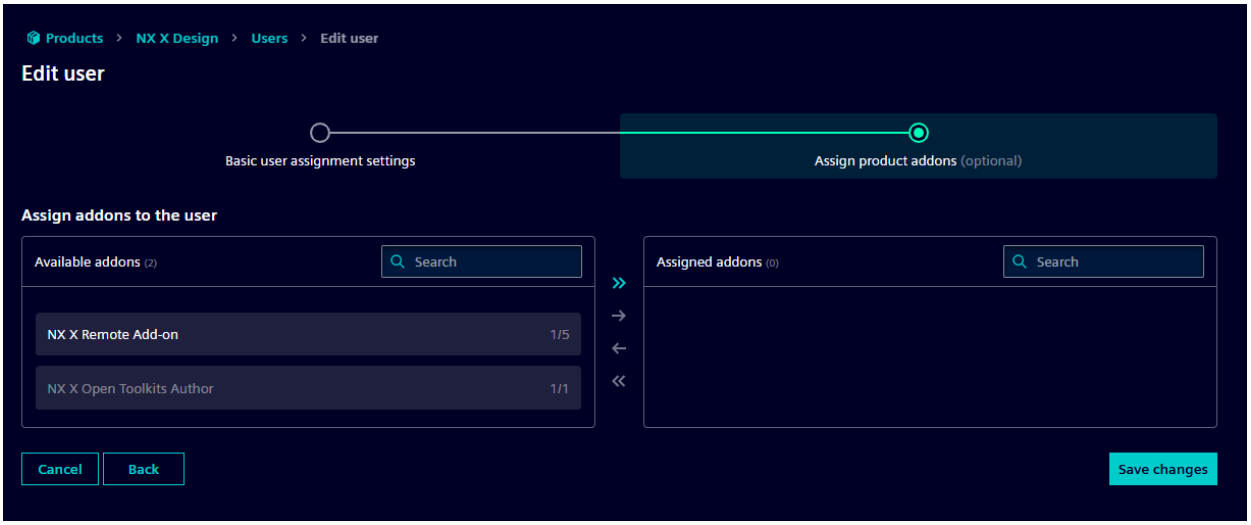
- In the **Select environments** section, modify the environments (applicable if product supports environments):
  - To assign environments: Select from the "Available environments" list and click  . To assign all, click  .
  - To unassign environments: select from the "Assigned environments" list and click  . To unassign all, click  .

**Note**

- Select environments available within the same tier.
- You can only edit this field for 1.0 products if they are in the same tier.




- Click **Next** or navigate to the **Assign product addons(optional)** to update addons if it is supported by product.
  - To assign addons: Select from the "Available addons" list and click →. To assign all, click ».
  - To unassign addons: select from the "Assigned addons" list and click ←. To unassign all, click «.




4. Click **Save changes**.

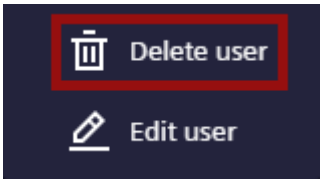
The user is updated with the modified changes.

## Remove Assigned Users from the Product

To remove a user from the product or revoke their access and privileges:

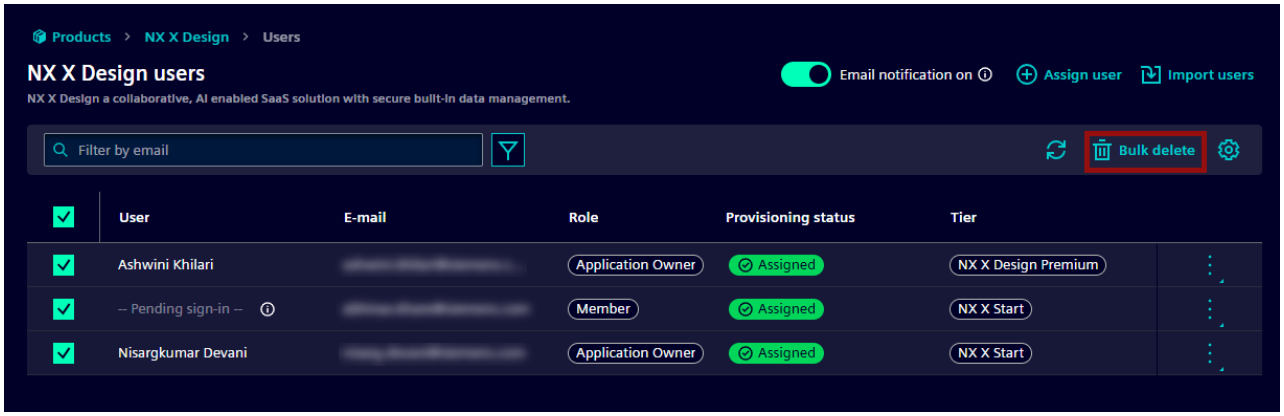
1. Select the user or multiple users to remove from the product.

   - For single user: Click ⋮ and select **Delete user**.

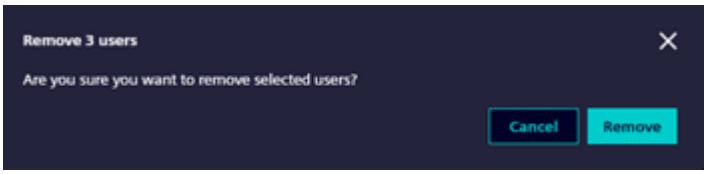



     - In the **Remove** pop-up, click **Remove**.


   - For multiple users, click **Bulk delete**.




- In the **Remove** popup, click **Remove**.




The selected user or multiple users associated with the product are removed.

**Note**

- A user cannot be removed if their product assignment is pending.
- The last user associated with a product cannot be deleted.
- User removal is supported even within expired products or deprecated tiers.
- If the product has configured an email template for user removal, the removed user will receive an email notification.
- The bulk delete function allows you to delete up to 20 users simultaneously.
- If a users license is locked and their provisioning status is **Removal complete**, you can reassign the user. For more information on reassigning the user, refer to **Reassign a License-Locked User**.
- To edit environments for multiple users at once, refer to **Edit Bulk Environment**.

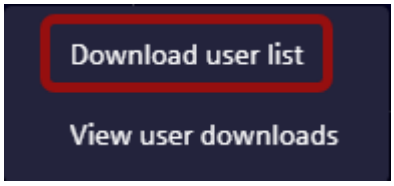
## Export Users list

Export users list allows you to download the list of users data in a CSV file. The list can be exported in two ways:

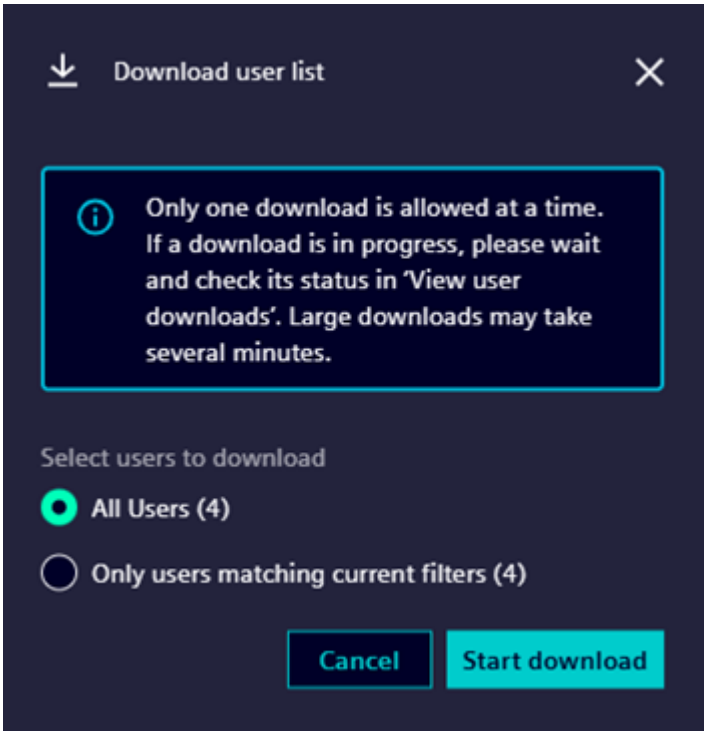
- **All Users**: Includes comprehensive list of all users within the system, providing a complete overview of user data.
- **Only users matching current filters**: Includes list of users that match specific criteria based on applied filters.

To download the list of users:

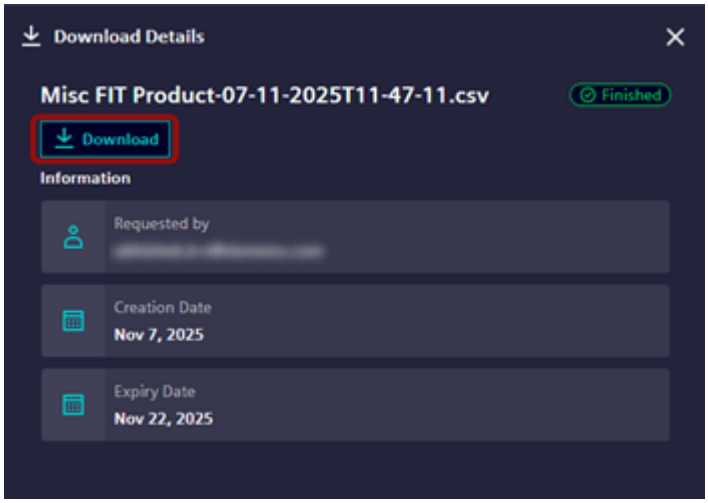
1. In the **Users** section, click ⋯.
2. Select **Download user list**.




3. In the **Download user list** pop-up, select one of the following options:
   - **All Users**: Downloads the complete list of users.
   - **Only users matching current filters**: Downloads only the filtered users.




4. Click **Start download**.
5. The page redirects to the **View user downloads** page.
6. Click ↻ to update the download status.
7. When the status changes to **Finished**, select the file to download.
8. In the **Download Details** section, click **Download** to download the CSV file.




The CSV file is downloaded.

**Note**

- Preparing the file for download may take several minutes, depending on the amount of user data.
- The download link is available only for 2 days.

## Configure High-Value Addons

High-Value Addons enhance product functionality with specialized features through addon subscriptions. As an Enterprise Cloud Account (ECA) administrator, you can manage user assignments to addons and modify these assignments through the Siemens Xcelerator Admin Console.

**Requirements**:

To use these features:

- Users must first be assigned to a product tier.
- Users can then be assigned to specific addons for additional features.

**Shared Addons**: Shared addons work across multiple products purchased under an ECA, using a single shared addon count.

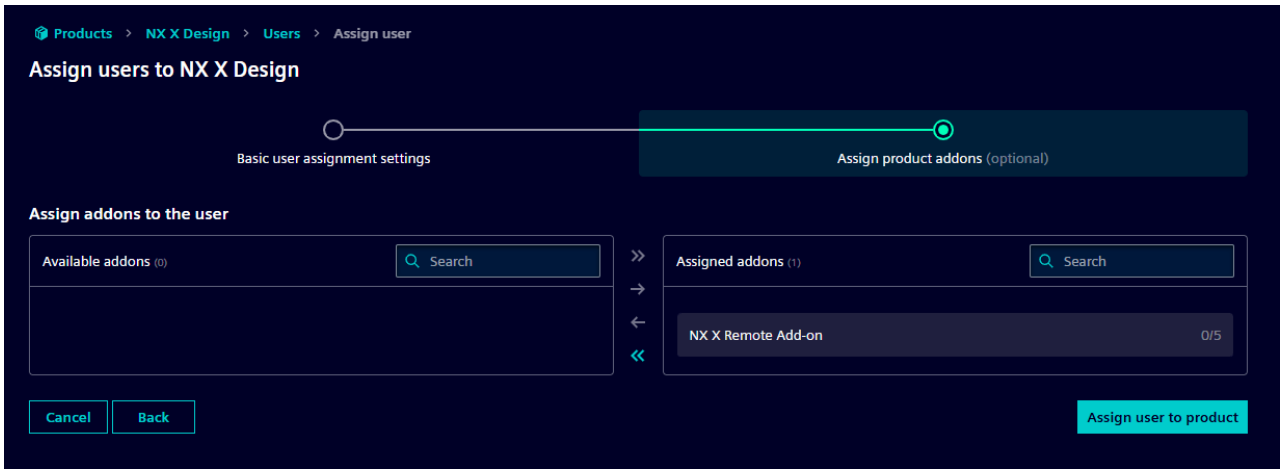
The Addons card on the Products overview displays:

- Available addons for the product
- Usage count
- Shared Addons have an icon to indicate that they are shared.

## Assign a User to Addons

To assign a user to addons:

1. In the **Products** list, select the product.
   - Search for the product by its display name or internal name, or use the filter options.
2. Go to the **Product details** section and click **Assign User**. For more information on assigning a user to product tiers, refer to **Manage User Assignments to Products**.
3. In the **Assign product addons (optional)** tab:
   - Select addons from the "Available addons" list and click →. To assign all the addons, click ».




4. Click **Assign user to product**.

The user is assigned to the selected product tier with addons.

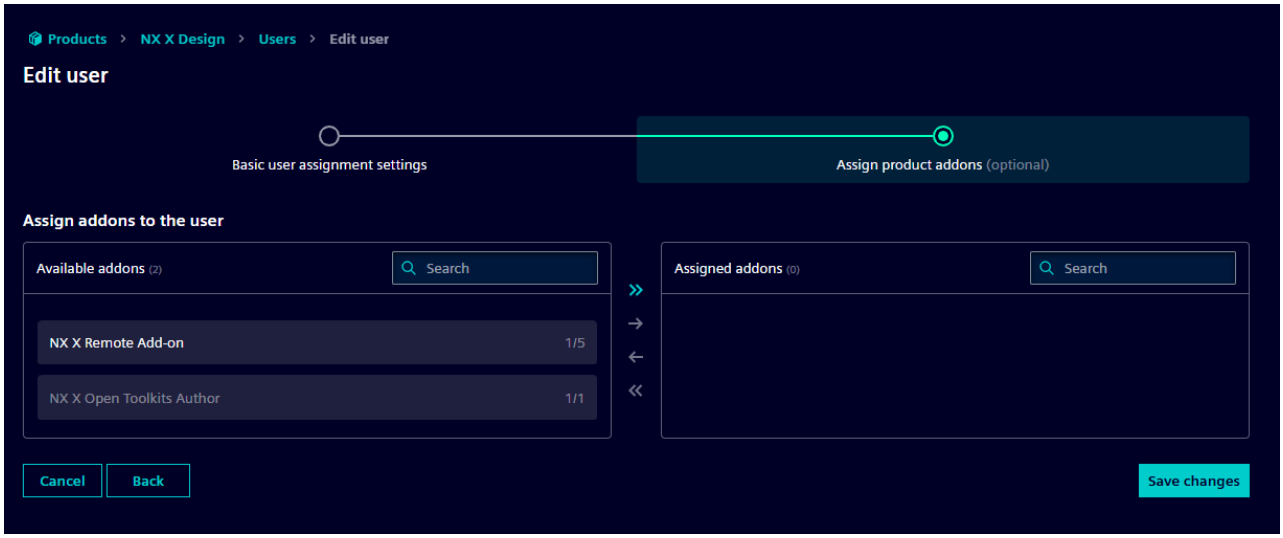
## Edit a User Assignment

The Edit User option allows ECA administrators change which addons are assigned to a user. It displays a list of addons assigned or purchased by the user.

To edit the user addon selection:

1. In the **Users** section, select the user.
2. In the **User details** section, click **Edit user**. For more information on editing a user, refer to **Edit a User Assignment**.
3. In the **Assign product addons (optional)** tab, modify the addons:
   - To assign addons: Select from the "Available addons" list and click →. To assign all, click ».

- To unassign addons: Select from the "Assigned addons" list and click . To unassign all the addons, click .




4. Click **Save changes**.

The users addons are successfully updated.

# Server Users

Server users (known as machine users) are system accounts that run automated processes and scheduled jobs. Use server users to:

- Run non-interactive jobs, such as cron jobs.
- Support compliance and security requirements.
- Execute scheduled and asynchronous jobs without affecting human user session limits.

> **Note**
> Server users consume a license or not depends on the selected product configuration.

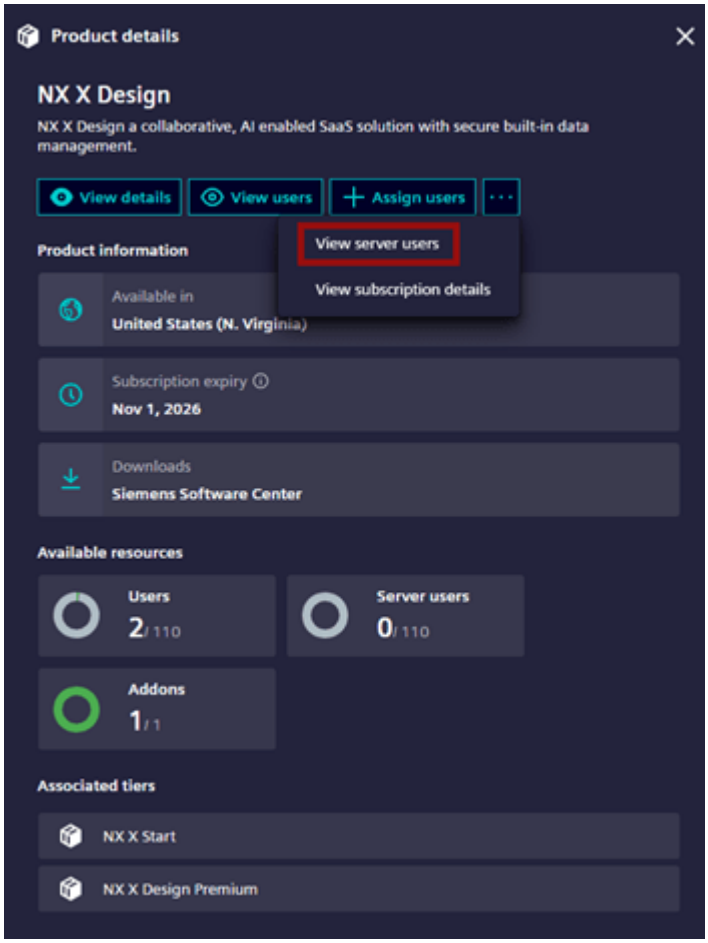
## Limits

- You can create up to 10 server users per product tier if the product does not require a license for server users.
- If the product requires a license for server users, the number of server users you can create depends on your purchased license count.

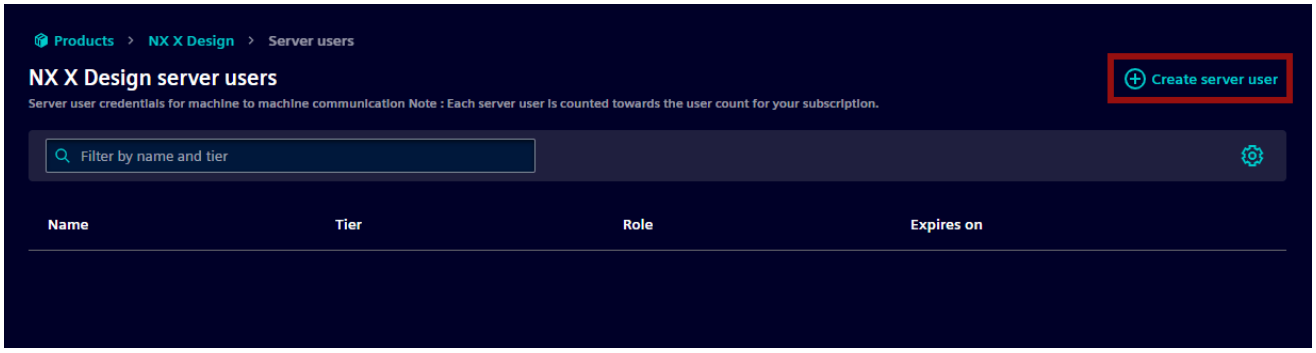
## Add a Server User

To add a server user to the product tier:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. In the **Products** list, select the product.
   - Search for the product by its display name, internal name, or use the filter options.
3. In the **Product details** screen, click ··· and select **View server users**.




4. Click **Create server user**



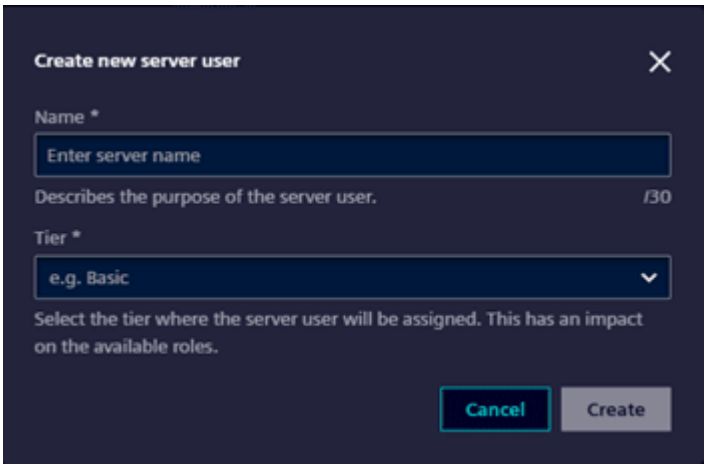

5. For products registered in SAM 1.0:

   - In the **Create new server user** popup, enter the required fields:

| Parameters | Description |
|---|---|
| Name | Enter the server name (5-30 characters). |
| Tier | Select the product tier from the dropdown list. |

> **Note**
>
> If only one tier is available, it is selected by default. If there are multiple tiers, choose the required tier from the list.

   - Click **Create**.




6. For products registered in SAM 2.0:

   - In the **Create new server user** popup, enter the required fields:

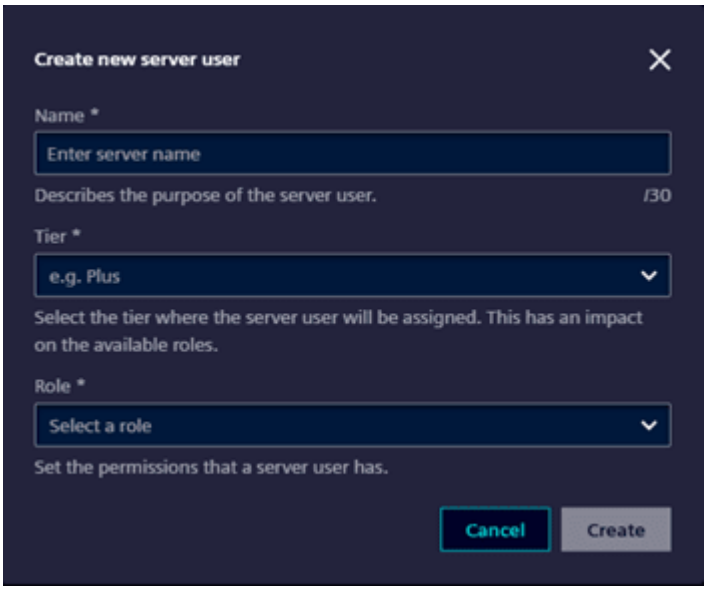
| Parameters | Description |
|---|---|
| Name | Enter the server name (5-30 characters). |

| | |
|---|---|
| Tier | Select the product tier from the dropdown list. |
| Role | Select the role applicable to the server user. |

**Note**

If only one tier is available, it is selected by default. If there are multiple tiers, choose the required tier from the list.

- Click **Create**.

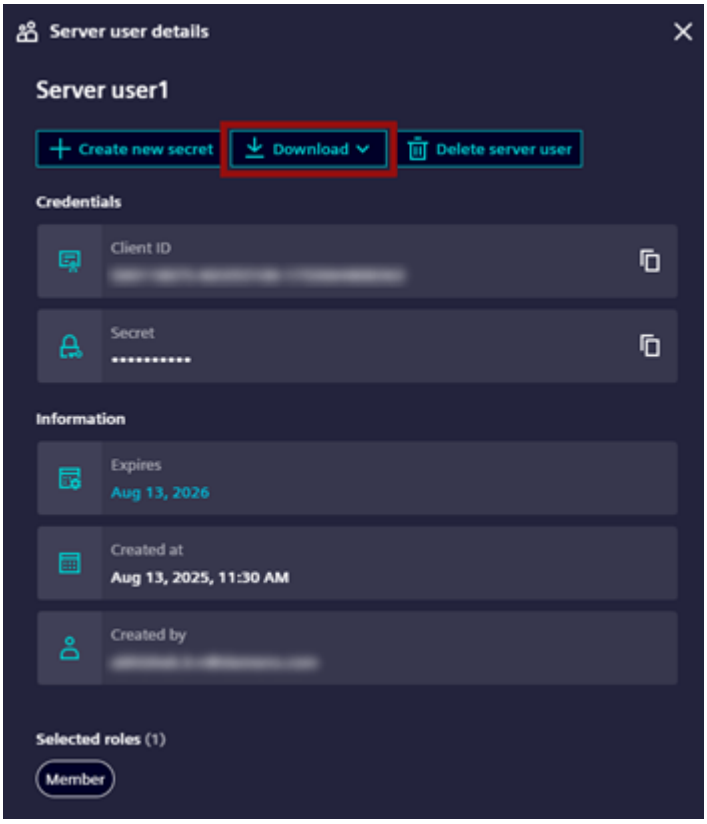



The server user is now added to the selected tier.

## Download Server User Credentials

To download credentials for a server user:

1. Select the server username to download credentials.
2. In the **Server user details** screen, copy the **Credentials** (Client ID and Secret) obtained, or you can download credentials.
   - To download credentials, click **Download** and choose one of the following:
     - **Download credentials**: Downloads a text file with the required credentials (Client ID and Client secret).
     - **Download postman collection**: Downloads a .json file containing both the API collection and the credentials.




The server user can now access the product application using the generated token and credentials.

**Note**

A server user expires on the earlier of:

- The product expiration date, or
- One year after the server user is created.

After expiration:

- You cannot download server user credentials for the server user.
- The associated Client ID is deactivated, and token generation stops.

## Create New Secret (Secret Rotation)

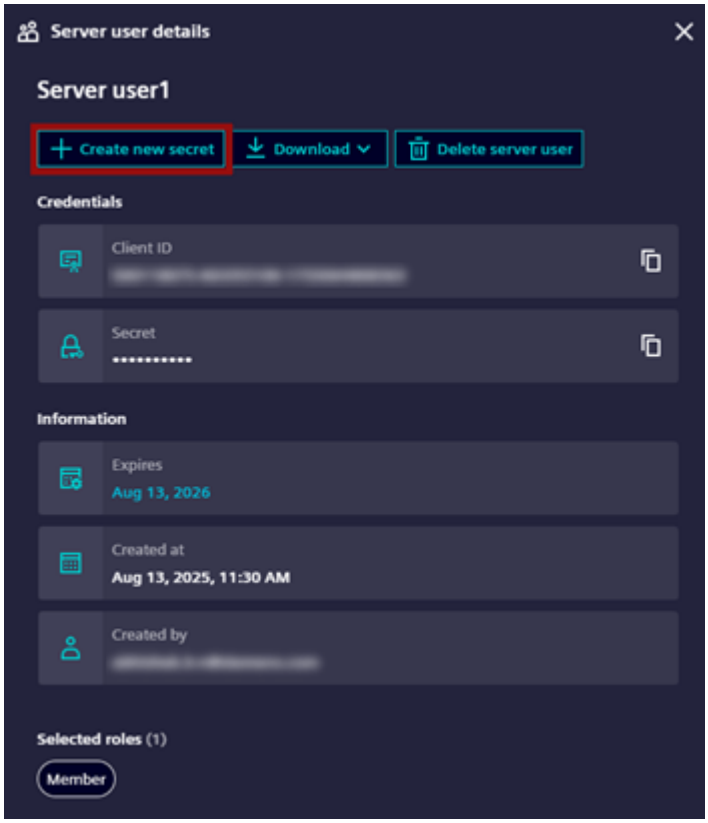
Secret rotation is a security practice that involves periodically updating server user credentials (secrets) to maintain system security and prevent unauthorized access. This process ensures that expired credentials are properly replaced while maintaining application functionality and preventing service disruptions. Server user credentials are essential components that require periodic rotation due to credential expiration.

**Note**

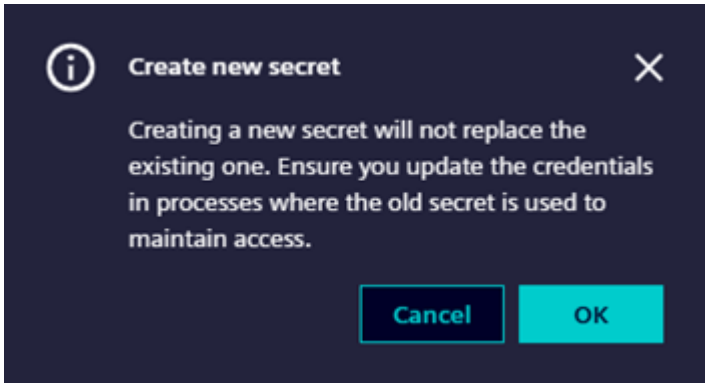
- Secret rotation applies to 2.0 products.
- If the server user product has expired, the "Create New Secret" functionality is disabled.

To create a new secret for credentials:

1. Select the server user to create a new secret.
2. In the **Server user details** screen, click **Create new secret**.



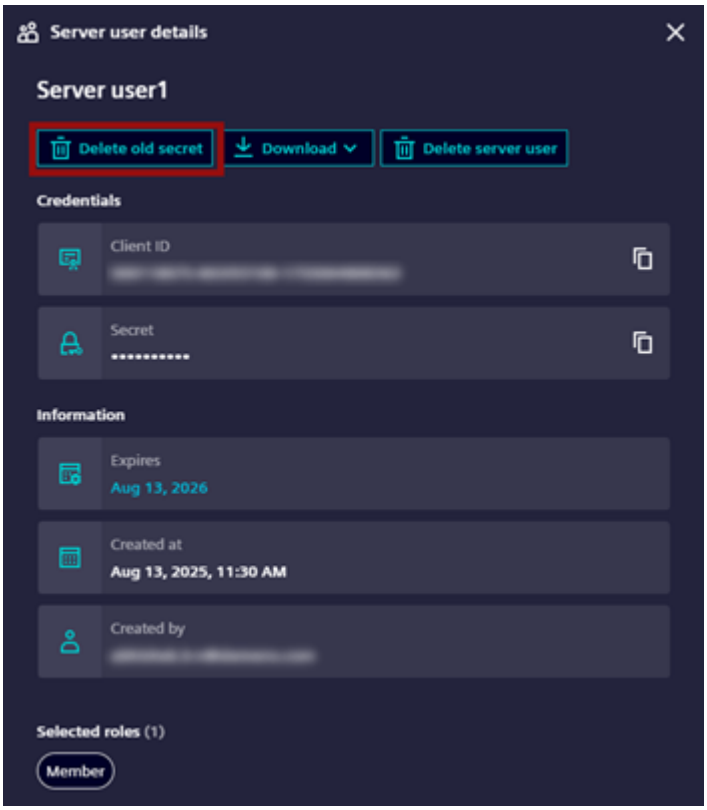

3. In the **Create new secret** pop-up, click **OK**.



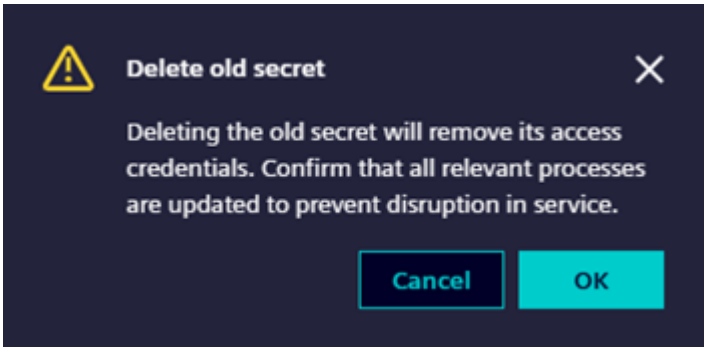
4. A new secret ID is created for the selected server user.

> **Note**
>
> - Use the new secret in your application.
> - Verify there are no disruptions in service.
> - Do not delete the old secret until you have verified the new secret is working properly.
> - Deleting an existing secret before proper replacement and verification may disrupt application functionality.

5. Once you have confirmed everything is working properly with the new secret:
   - In the **Server user details** screen, click **Delete old secret**.



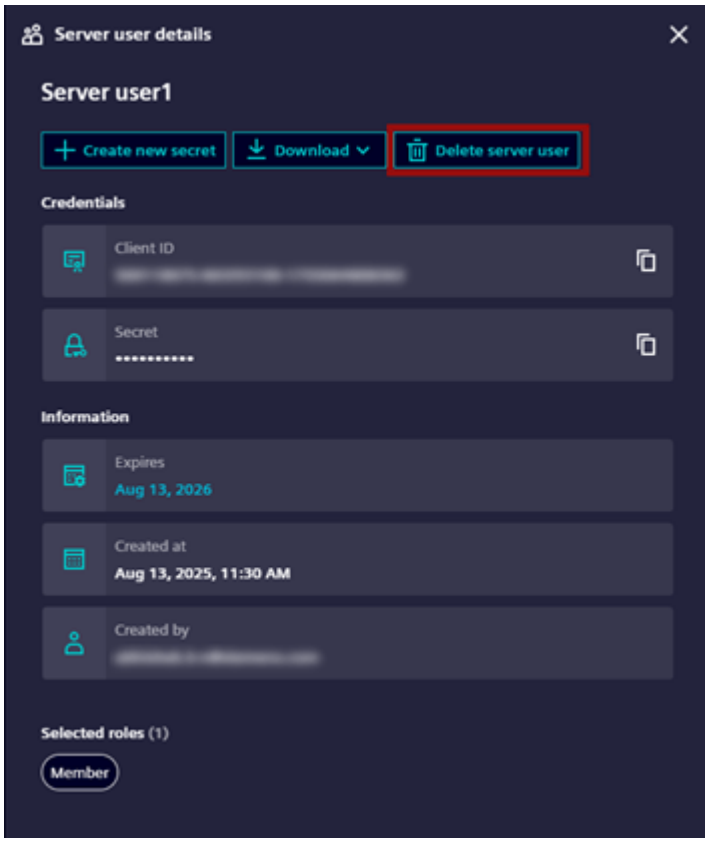

   - In the **Delete old secret** pop-up, click **OK**.



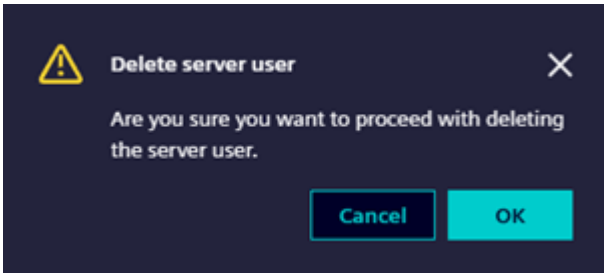
## Delete a Server User

To delete a server user:

1. Select the server username to delete.
2. In the **Server user details** screen, click **Delete server user**.




3. In the **Delete server user** popup, click **OK**.




The server user is removed from the product tier.

## Invoke CustomerAPI Using Server User Credentials

Follow the steps below to invoke customer api using server user credentials:

1. Create a server user in the Siemens Xcelerator Admin Console. For more information, refer to **Add a server user**.
2. Download the credentials to access the product and invoke customerAPI. For more information on downloading server user credentials, refer to **Download Server User Credentials**.
3. Get a Token
   - Use the /token endpoint to obtain an access token. Here is an example token request:

```
-X POST https://xc.<region>.sws.siemens.com/oauth/token \
-H "Content-Type: application/x-www-form-urlencoded" \
-d
"grant_type=client_credentials&client_id=YOUR_CLIENT_ID&client_secret=
YOUR_CLIENT_SECRET&tenant=YOUR_TENANT_ID"
```

   **Response Example**:

```
{
    "access_token": "exxxx...",
    "token_type": "Bearer",
    "expires_in": 3600
}
```

4. Make an API Call
   - Use the generated token to invoke the API. Use the following URL format to make API call, setting the obtained token as the authorization header:

```
curl -X GET https://cloud.<region>.sws.siemens.com/api/myapi/
<version>/<endpoint>
-H 'Authorization: Bearer <access_token>'
```

> **Note**
>
> The following URL format is discouraged and will be discontinued at the end of 2025. `https://<eca>.<region>.sws.siemens.com/myproduct/api/customerapi/v1/resource`.

# Manage User Access for Active or Inactive

Products like Teamcenter X support the ability to mark users as Active or Inactive, giving enterprise administrators greater flexibility in managing user access and license utilization.

**Key Features**:

- You can add more users than the number of licenses purchased.

- Only the number of users equal to the license count can be marked as Active and access the product.
- Inactive users do not consume licenses and cannot access the product.

This feature helps optimize license usage by allowing administrators to rotate access among users as needed.

## Key Benefits

Enabling the support for marking users as inactive provides the ECA Admin the following benefits:

- **Simplified User Management**: Add all potential users in advance without concern for license limits.
- **Operational Flexibility**: Switch users between active and inactive based on business priorities or project requirements.
- **License Optimization**: Ensure optimal usage by restricting active users to those who consume licenses.
- **Seamless Bulk Imports**: Import large user groups with the system automatically managing license allocations.
- **Support for Dynamic Teams**: Retain inactive users for quick activation as team needs change.
- **Audit Readiness**: Maintain complete visibility of all users (active or inactive) for compliance and audit tracking.
- **Scalability for Growth**: Prepare for future license expansions by preloading users in the pool.

## Key Concepts

**Active vs Inactive Users**:

- Active Users: Count against the license quota and can access the product.
- Inactive Users: Do not count against the license quota and cannot access the product.

> **Note**
> - Administrators can manually update user status between active and inactive based on license availability.
> - Access is limited if the number of users exceeds the available licenses. To allow more users to access the application, purchase additional licenses.

## Configure Active and Inactive Users

To configure active and inactive users, follow the steps below:

1. Select the user you want to update the status in the "Assigned Users" list and click **Edit User**. For more information, refer to **Edit a User Assignment**.
2. Check or uncheck the "Active" checkbox in the **Edit User** pop-up to update the user status.

3. Click **Save**.

The user status is updated.

**License Count**:

Upon adding users individually or through bulk import:

- The first "**X**" users (where **X** = license count) are set as **active**.
- Additional users are added as **inactive**.

## User Management with Pooling

| Feature | Behavior | Effect |
|---|---|---|
| User Addition | First **X** users | Status: **Active** (Consumes license) |
| | Users beyond **X** | Status: **Inactive** (No license consumed) |
| Status Change | Change Status to **Active** | Allowed only if licenses are available |
| | Change Status to **Inactive** | License released only if license locking is OFF |
| User Deletion | Delete Active user (Locking OFF) | License released immediately |
| | Delete Active user (Locking ON) | License retained until month-end |
| Bulk Import | Any number of users | Follows same rules as individual user management |

## License Locking

Products like Teamcenter X also enforce License Locking along with the ability to set users as inactive.

When License Locking is enabled:

- An active user license is locked until the end of the calendar month.
- If an active user is deleted, the license is not released immediately.

## Edit License-Locked User Status and Details

When modifying the license locked users, you have the flexibility to either toggle the user status between Active and Inactive, or update other fields in user details.

**Note**

- Changing the user status will temporarily disable other editable fields.

- Modifying other fields will temporarily disable the user status field.

To make both types of changes, first save your initial edits (either user status or other fields), then click Edit user again to complete the remaining modifications. For more information on editing user details, refer to **Edit a User Assignment**

## Reassign a License-Locked User

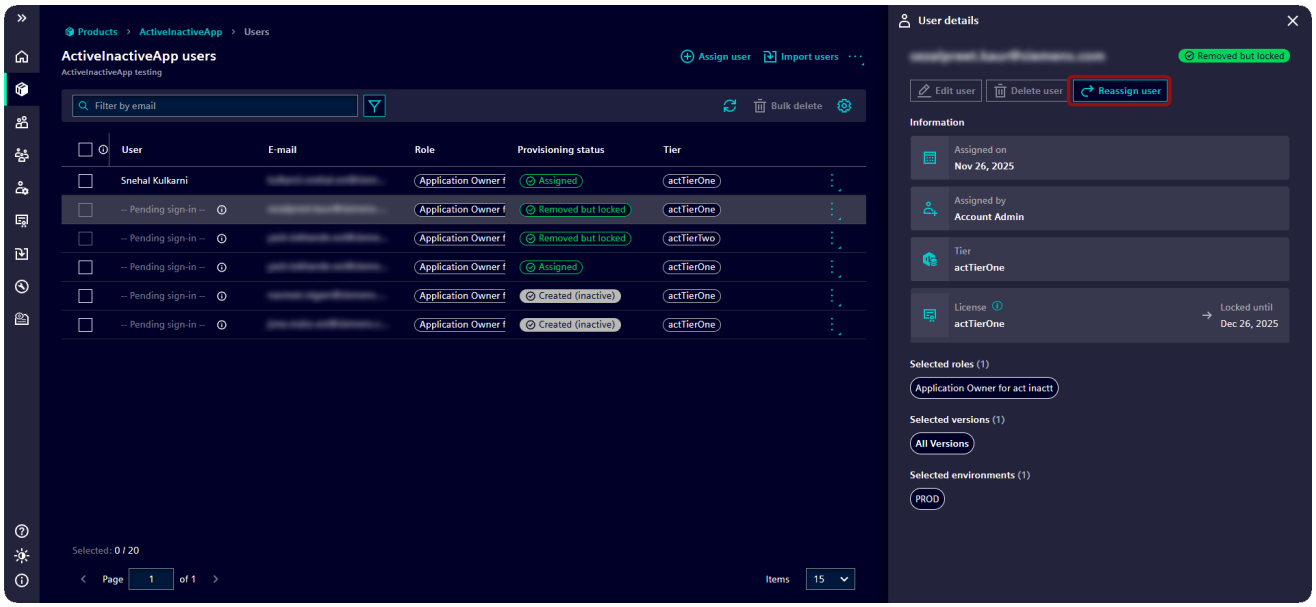
You can reassign a user whose license is locked and whose provision status is **Removed but locked**.

**Prerequisites**:

- The user license is locked.
- The user provisioning status is **Removed but locked**.

To reassign the user:

1. Select the user.
2. In the **User details** section, click **Reassign user**.




3. In the **Reassign** pop-up, click **Reassign**.

The user is reassigned, and the status changes to **Assigned**.

> **Note**
> Reassigning a user does not extend the original license lock period.

## Edit Tier for License-Locked Users

When you edit the tier of a license-locked user, the system creates two entries for that user:

- **Old tier entry**: Shows **Removed but locked** status with all actions disabled (reassign, edit, delete).
- **New tier entry**: Shows **Assigned** status and functions as a normal assigned user.

This ensures that the license lock remains active for the old tier while allowing full access and management for the new tier.

To edit the tier of a license-locked user:

1. In the **Users** section, select the license-locked user.
2. In the **User details** screen, click **Edit user**.
3. In the **Basic user assignment settings** tab, select the new tier. For more information, refer to **Edit a User Assignment**.
4. Click **Save changes**.

The user is now assigned to the new tier, and the old tier entry shows **Removed but locked** status with all actions disabled.

> **Note**
> - Editing a license-locked user's tier does not remove the license lock. The license lock remains active for both the old and new tier entries until the license expires.
> - The **Removed but locked** entry for the old tier remains in the user list until the license expires or is manually removed.
> - You cannot reassign or edit the old tier entry. To manage the user, use the new tier entry.
> - To reassign the user after the license expires, refer to **Reassign a License-Locked User**.

## Impact of License Locking

| Scenario | Behavior |
|---|---|
| Active user is deleted | The license is retained until end of month |

| | |
|---|---|
| New user added while all licenses are locked | The user is added as **inactive** |
| License availability updated at month-end | Locked licenses are released and can be assigned to new users |

### Best Practices for Admins

To ensure efficient and effective use of the Siemens Xcelerator Admin Console, follow these best practices:

- Monitor license usage regularly using the Siemens Xcelerator Admin Console.
- Use bulk import carefully. If you need to prioritize active access, plan the order of users in advance.
- If using License Locking, schedule user rotations at the beginning or end of the month for optimal results.
- Retain inactive users in the user pool for easy reactivation.

### Frequently Asked Questions (FAQs)

**Q: Can I activate a user mid-month if all licenses are locked?**
**A:** No. You can only activate a new user after a locked license is released at the end of the calendar month.

**Q: What happens to a license if I delete an active user?**
**A:** If license locking is disabled, the license is released immediately. If license locking is enabled, the license remains locked until the end of the month.

**Q: Can I turn off license locking later?**
**A:** License locking is a product-level configuration and should be decided during the initial setup. Changes may require coordination with your support team.

## User Management for Direct or Indirect Product Licenses

This section explains how to assign and manage users for direct and indirect product licenses. If you are an ECA admin, you can assign users to products with two types of licenses:

- **Direct License**
- **Indirect License**

### Direct license

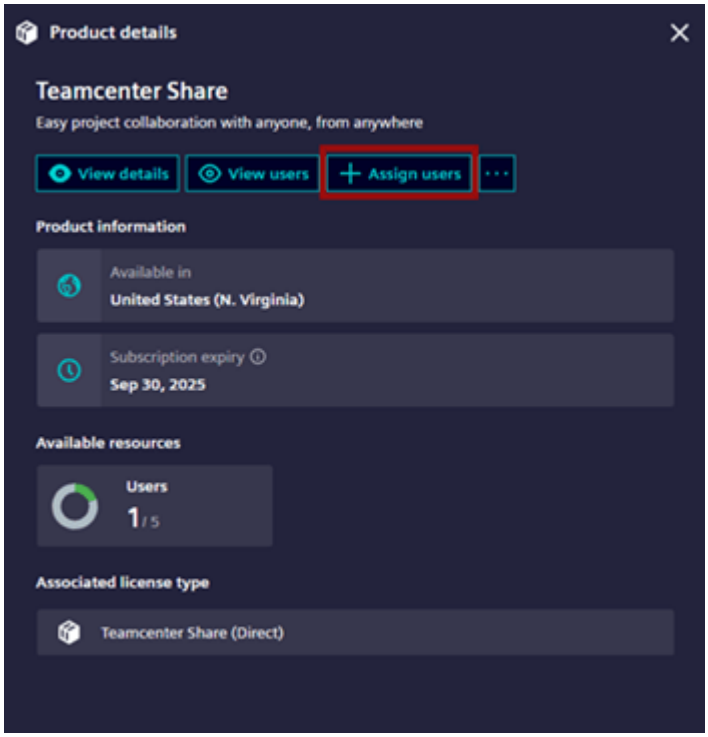
Direct license allows you to assign users directly to the product.

## Assign a User for Direct License

The **Assign User** tab is enabled if your region has provisioned the product.

To assign a user:

1. In the **Products** list, select the product.
   - Search for the product using its display name or internal name, or use the filter options.
2. Go to the **Product details** screen and click **Assign User**.

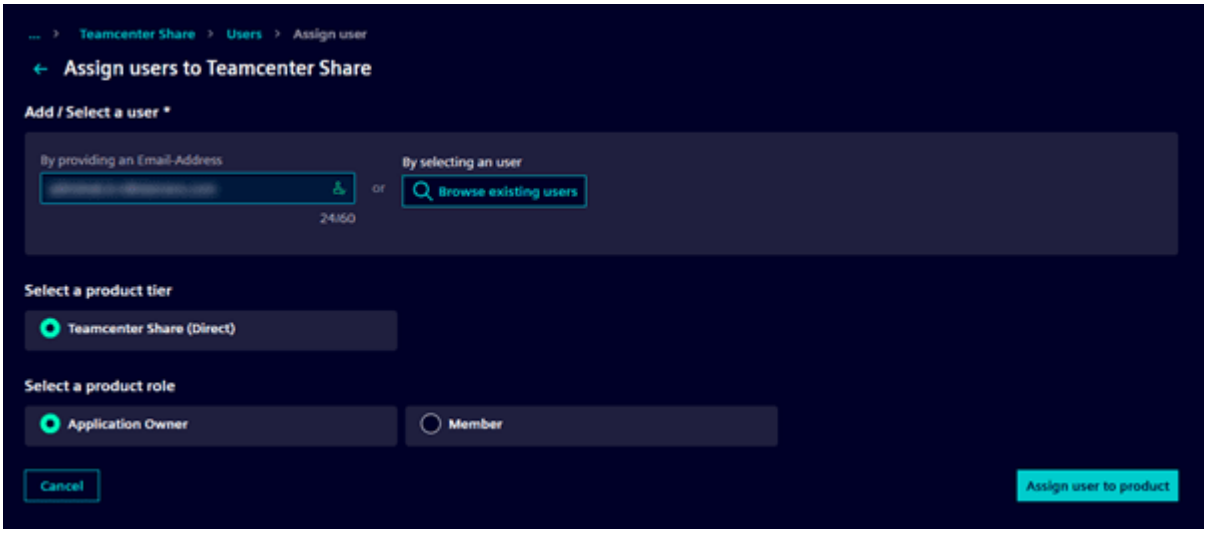



3. In the **Basic user assignment settings** section:
   - Enter the user email address, or click **Browse existing users** to select an existing user from the list.

     **Note**

     If domain validation is enabled, only approved domains are accepted. For more information on validating domain, refer to **MultiFactor Authentication**.

   - Select the required product tier.
   - Select the required product role.




4. Click **Assign user to product**.

The user is now assigned to the product with a direct license.

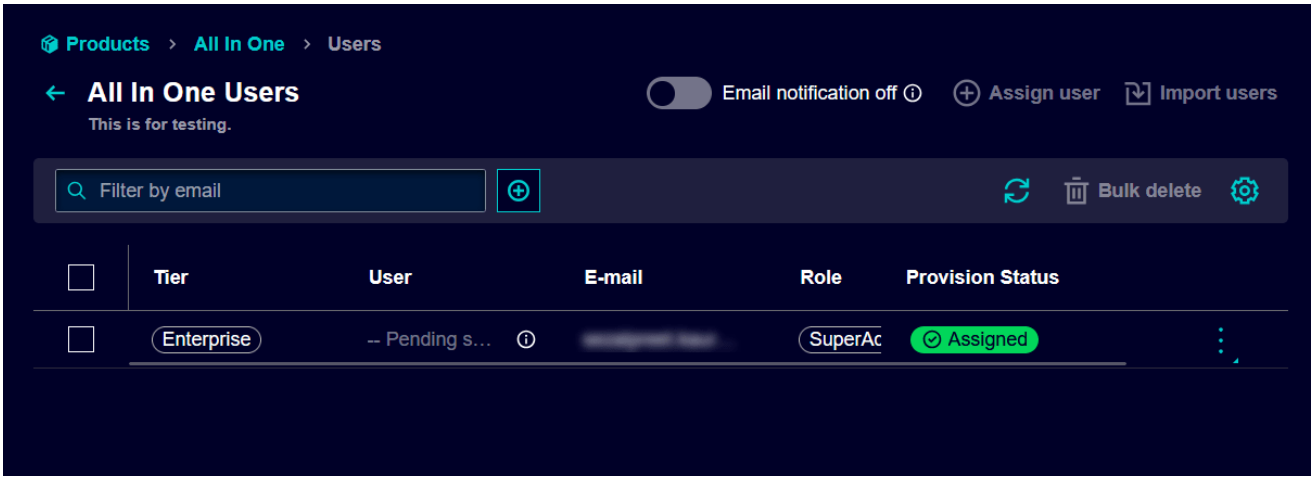
## Indirect license

Indirect licenses appear for products sold with a base product indirectly to the customer. Assigning users to the base product will also assign them to indirect license automatically. You cannot edit or delete these users directly. If a user is deleted or edited in the base product, the same changes are reflected in the indirect licenses.

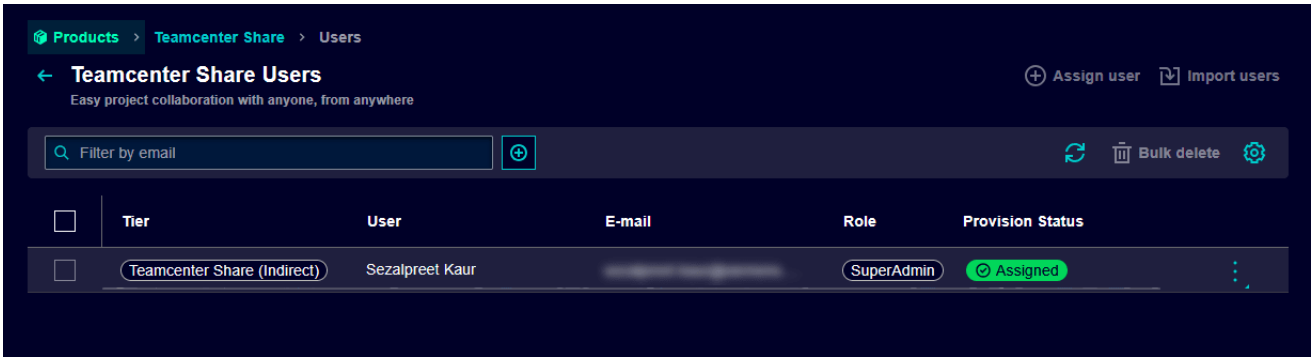
**Example**: Assigning a User to Indirect Licenses

When you purchase a product license (All In One), it also provides an indirect license for a related product, like Teamcenter Share.

1. When a user is added to the primary product license (All In One), they are automatically assigned as an indirect user to the related product (Teamcenter Share).



2. You can view the indirect users assigned to the related product (Teamcenter Share) by navigating to that product in the Siemens Xcelerator Admin Console and click **Assigned Users** tab.




**Note**

You cannot make any direct changes to the indirect users in the related product interface. Users can manage their accounts only through the base product license.

3. To remove a users access, delete them from the base product license (All In One). This will automatically remove their indirect access to the related product (Teamcenter Share).

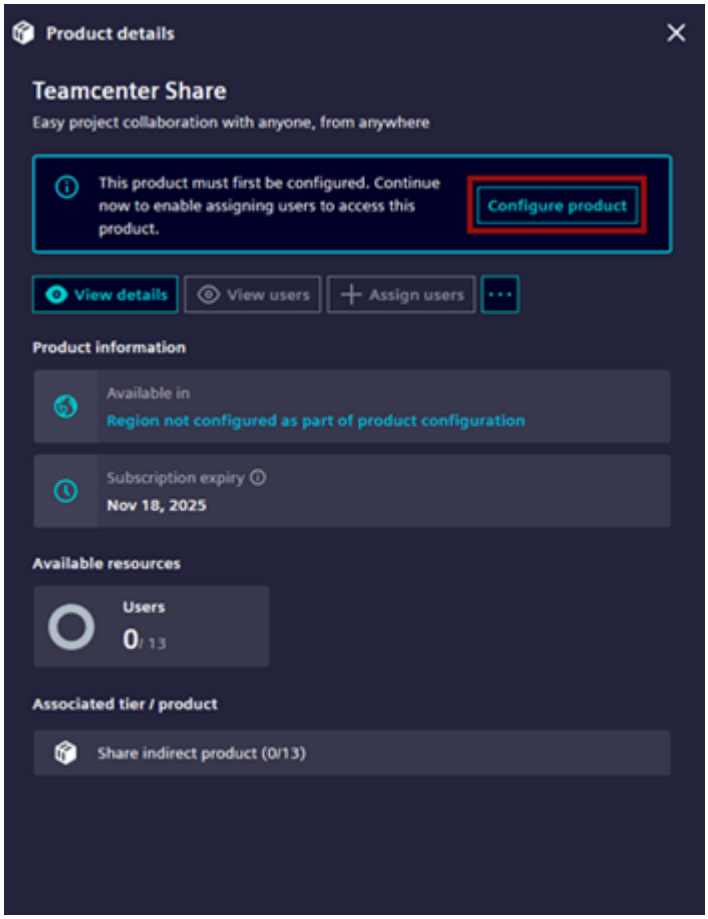
# User Management for Non-Administered Products in Teamcenter Share

This section explains how to configure and assign users for Teamcenter Share, which applies to products not managed through the Admin Console.

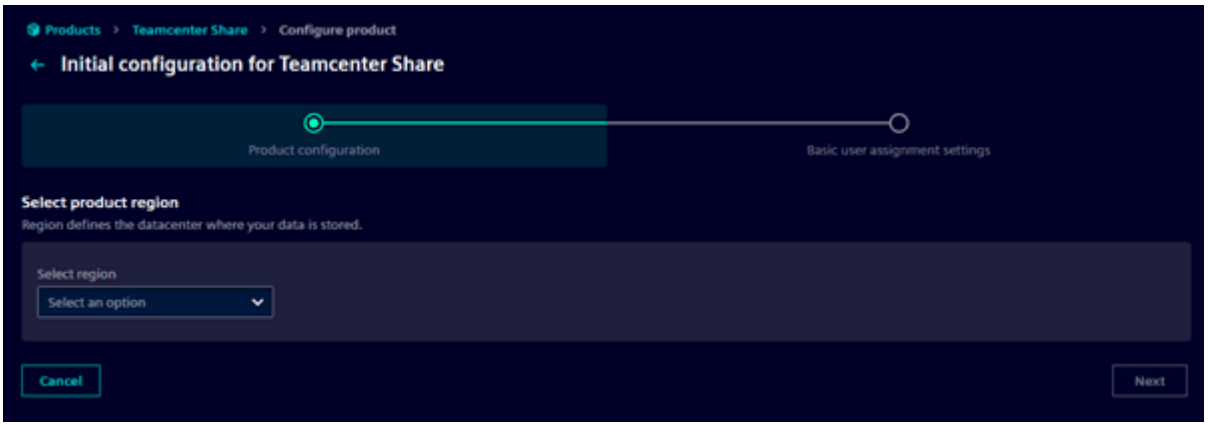
## Configure Teamcenter Share

To configure Teamcenter Share:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. Go to the **Products** tab in the left navigation pane and select the product to configure.
   - Search for the product by its display name or internal name, or use the filter options.
3. In the **Product details** screen, click **Configure Product**.




4. In the **Product configuration** tab, select the region to store the data and click **Next**.




**Note**

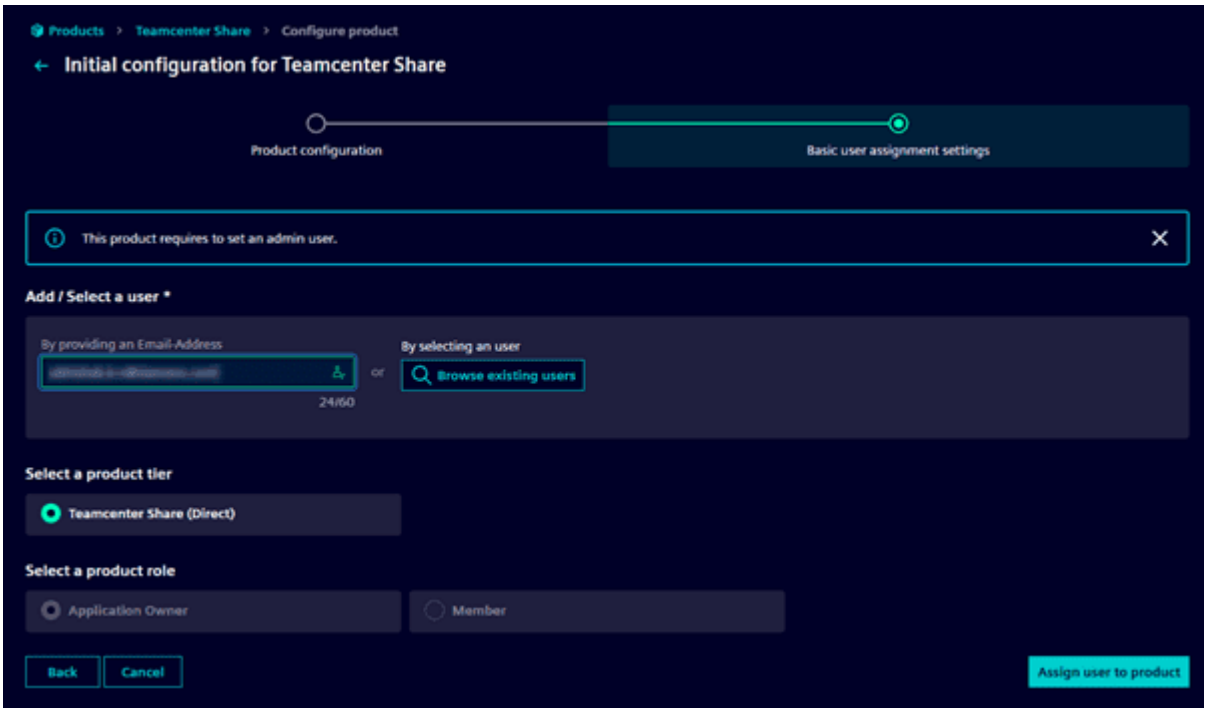
- Once a region is selected, the "Region" field becomes non-editable and cannot be modified.
- In the **User Assignment Preview** section, you can preview the assignment or configuration process being performed.

5. In the **Basic user assignment setting** tab, enter the following:

- Enter the users email address, or click **Browse existing user** to select an existing user.

> **Note**
>
> If domain validation is enabled, only users from approved domains are accepted. For more information on validating domain, refer to **MultiFactor Authentication**.

- Select the required product tier.
- Select the required product role.



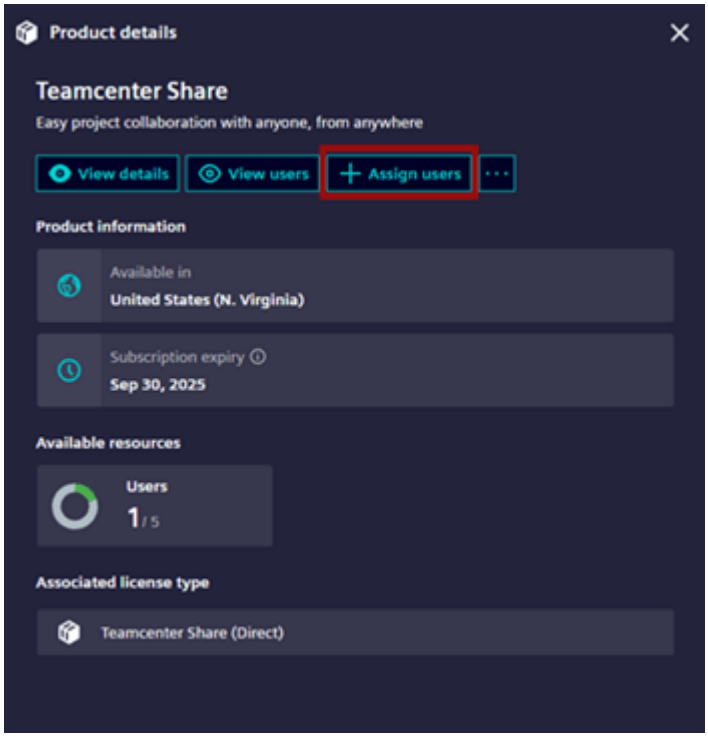

6. Click **Assign user to product**.

The user is now provisioned for Teamcenter Share.

## Assign a User

To assign a user:

1. In the **Products** list, select the product.
   - Search for the product using its display name or internal name, or use the filter options.
2. In the **Product details** screen, click **Assign users**.



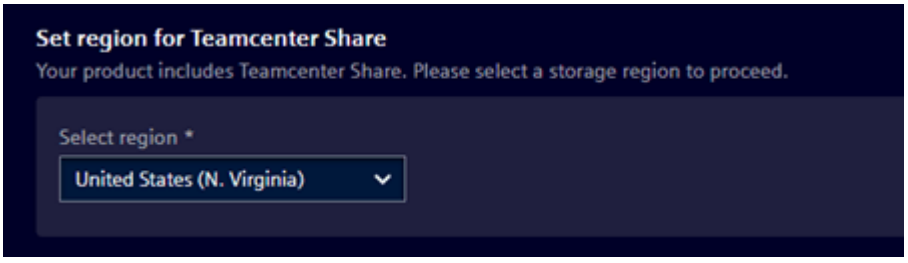

3. In the **Assign user** screen:
   - Enter the user email address, or click **Browse existing users** to select an existing user from the list.

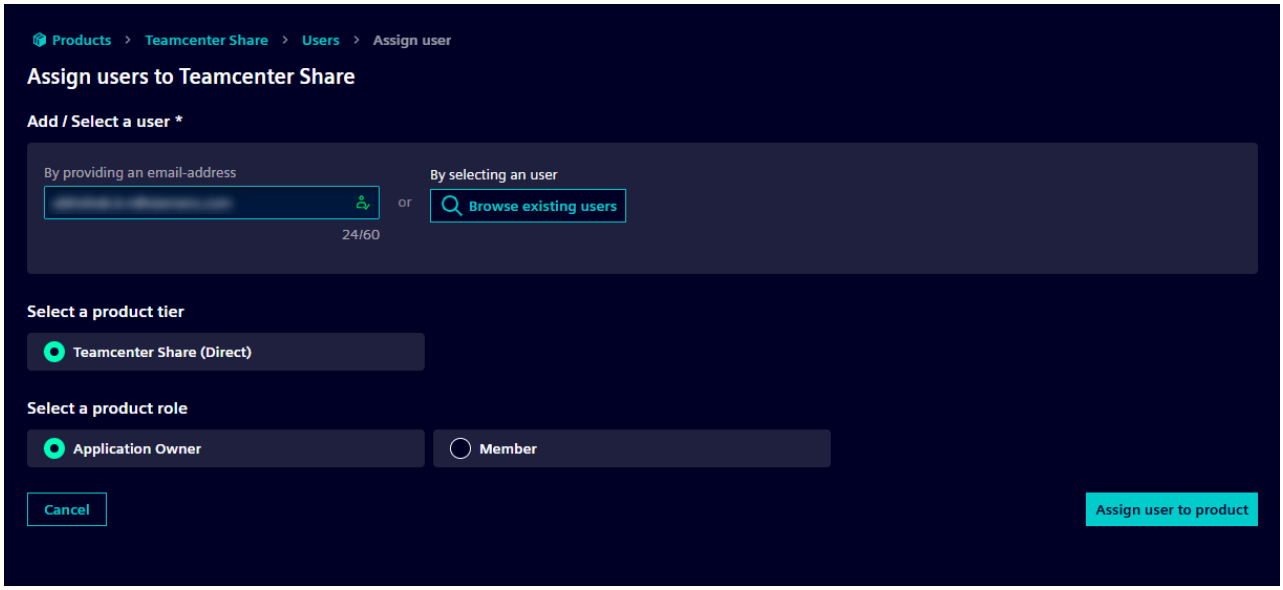
     **Note**

     If domain validation is enabled, only approved domains are accepted. For more information on validating domain, refer to **MultiFactor Authentication**.
   - Select the product tier.
   - Select the product role.
   - Select the region.

     **Note**

     Region selection is required on the base product if it supports co-administration for Teamcenter Share.




4. Click **Assign user to product**.

The user is now assigned to Teamcenter Share.

**Note**

- After assignment, users cannot be edited but can be deleted if needed.
- If hybrid Share licenses are in use, Teamcenter Share will appear in the product dropdown.

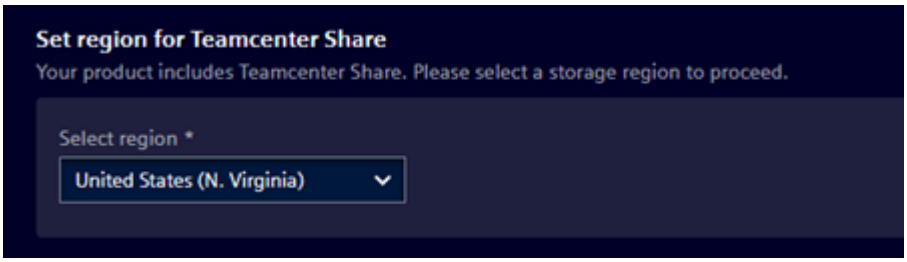
## Edit a Assigned User

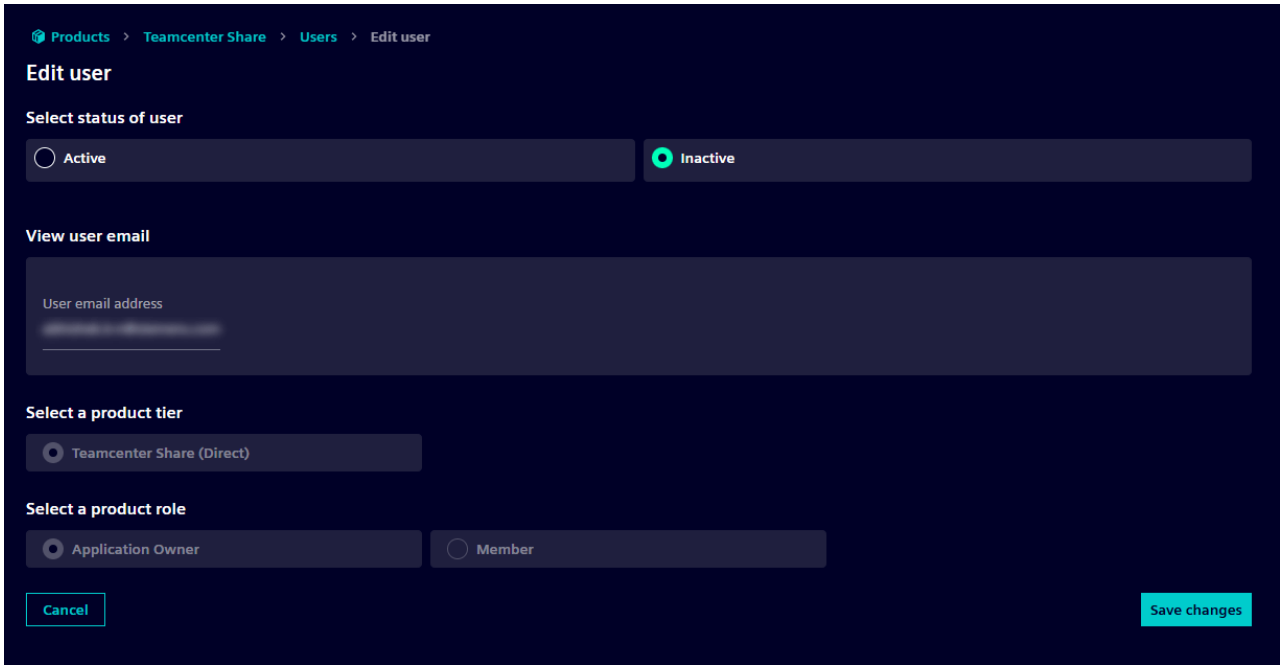
To edit a assigned users status and product tier:

1. Select the user from the list of assigned user to edit.
2. In the **Edit user** screen:
   - Select the user status:
     - **Active**: An active user counts towards the total number of users subscribed to the product.
     - **Inactive**: An inactive user cannot access the product and does not count towards the user subscription limit.
   - Select the product tier.
   - Select the product role.
   - Select the region.

**Note**

Region selection is required on the base product if it supports co-administration for Teamcenter Share.




3. Click **Save changes**.

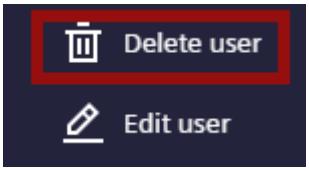
The user is updated with modified changes.

## Remove an Assigned User

To remove a user:

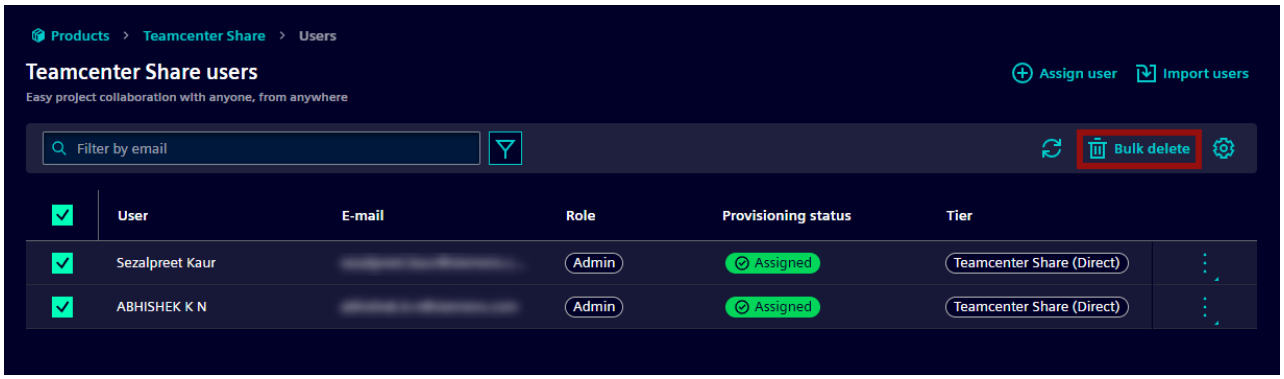
1. Select the user or multiple users to remove from the list of assigned users.

   - For single user: Click  and select **Delete user**.

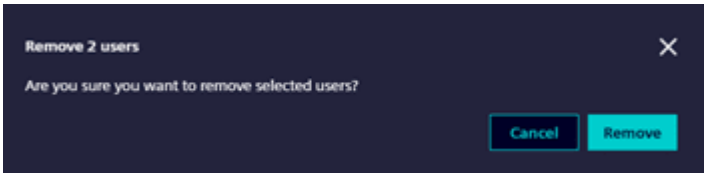


- In the **Remove** pop-up, click **Remove**.


- For multiple users, click **Bulk delete**.




- In the **Remove users** popup, click **Remove**.




The selected user or multiple users are removed from Teamcenter Share.

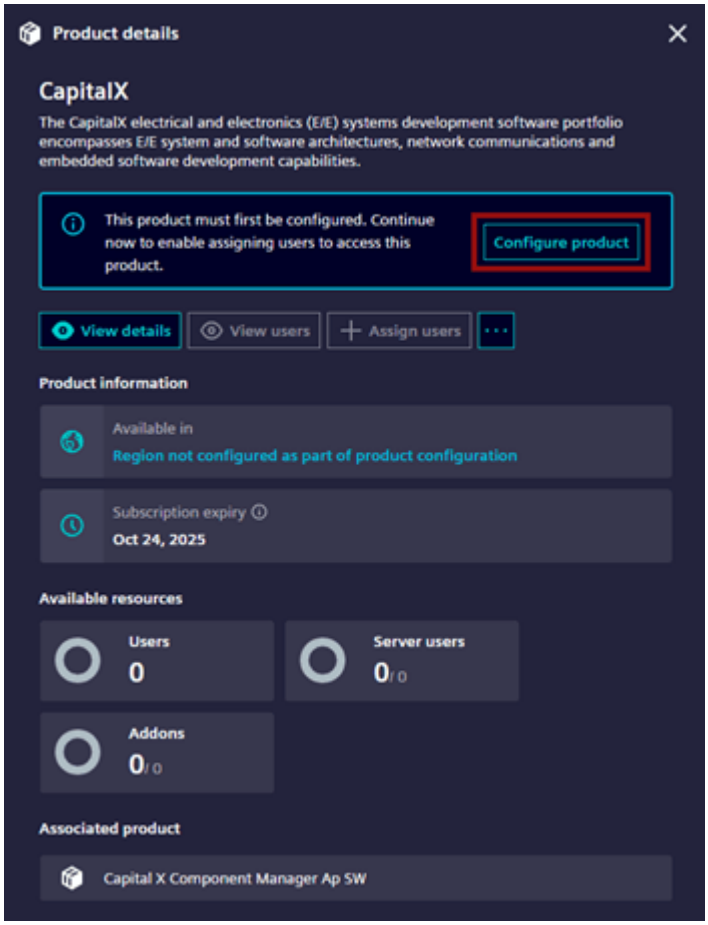
# User Configuration and Management for Product Family

This section explains how to configure and manage users for the product family.

## Configure a Product Family

To configure a product family:

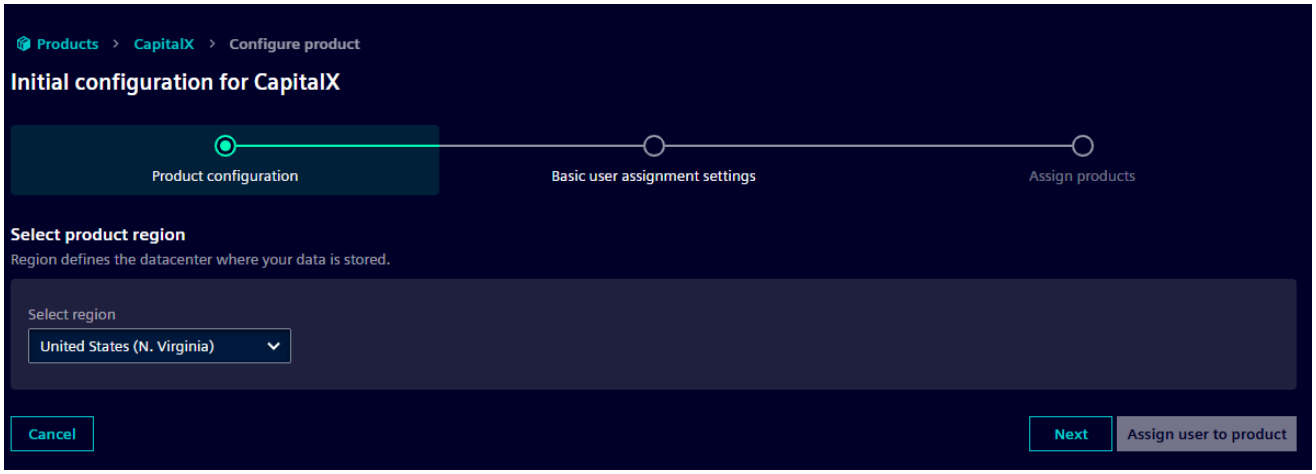
1. Sign in to **Siemens Xcelerator Admin Console**.
2. Go to the **Products** tab in the left navigation pane and select the product family.
   - Search for the product by its display name or internal name, or use the filter options.
3. In the **Product details** section, click **Configure product**.




4. In the **Product configuration** tab, select the "region" to store the data and click **Next**.

> **Note**
> Once a region is selected, the "Select region" field becomes non-editable and cannot be changed.

> **Tip**
> In the **User assignment preview** screen, you can preview the user assignment process being performed.

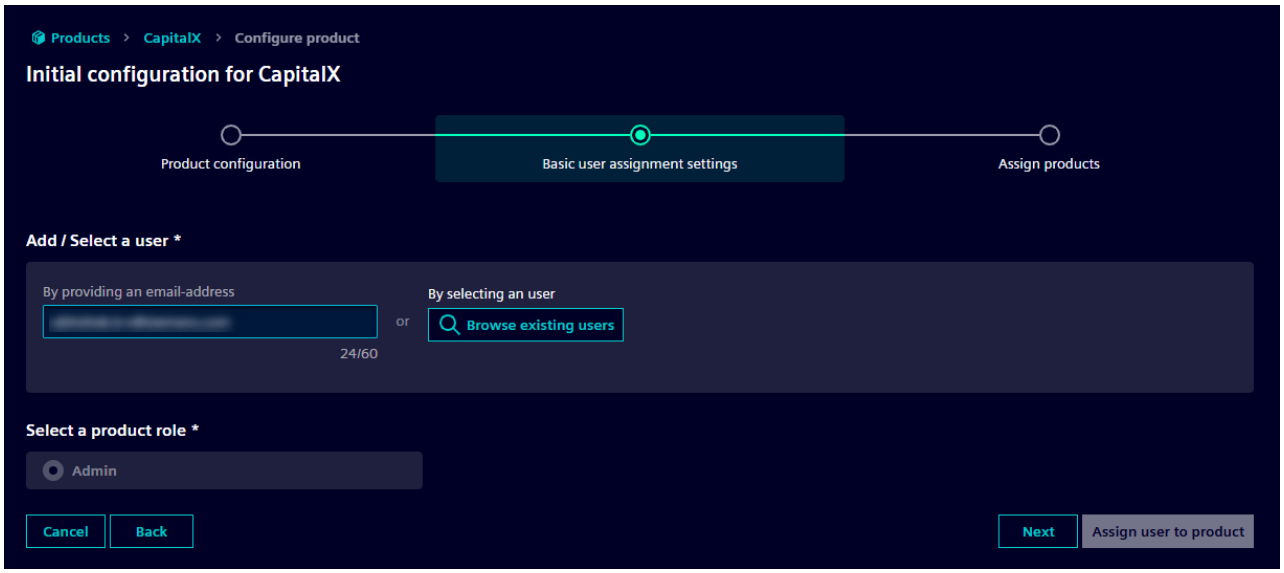



5. In the **Basic user assignment setting** tab, enter the following:

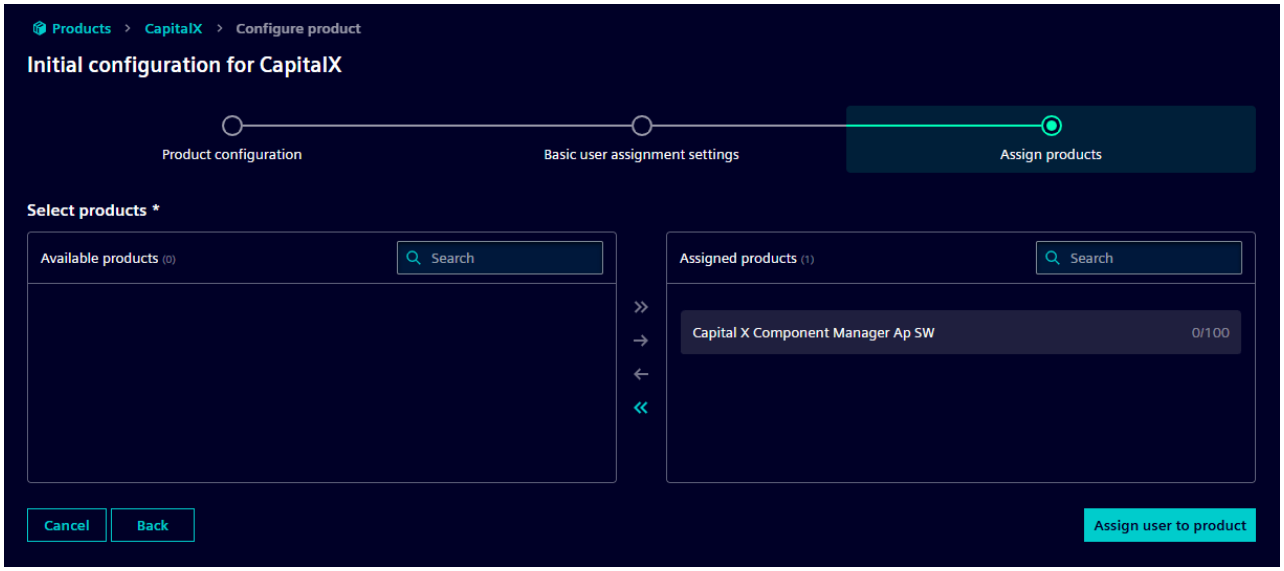
- Enter the users email address, or click **Browse existing users** to select an existing user.

> **Note**
>
> - If group syncing is enabled, only existing users can be selected. For more information, refer to **Manage Groups and User Synchronization**.
> - If group syncing is disabled, you can add a new user or select from the existing list. For more information, refer to **Manage Groups and User Synchronization**.
> - If domain validation is enabled, only approved domains are accepted. For more information on validating domain, refer to **Multi-Factor Authentication and Domain Validation**.

- Select the required product role.
- If the product supports environments: Select environments from the "Available environments" list and click → . To assign all environments, click » .
- Click **Next**.



6. In the **Assign products** tab:
   - Select products from the "Available products" list and click →. To assign all products, click ».



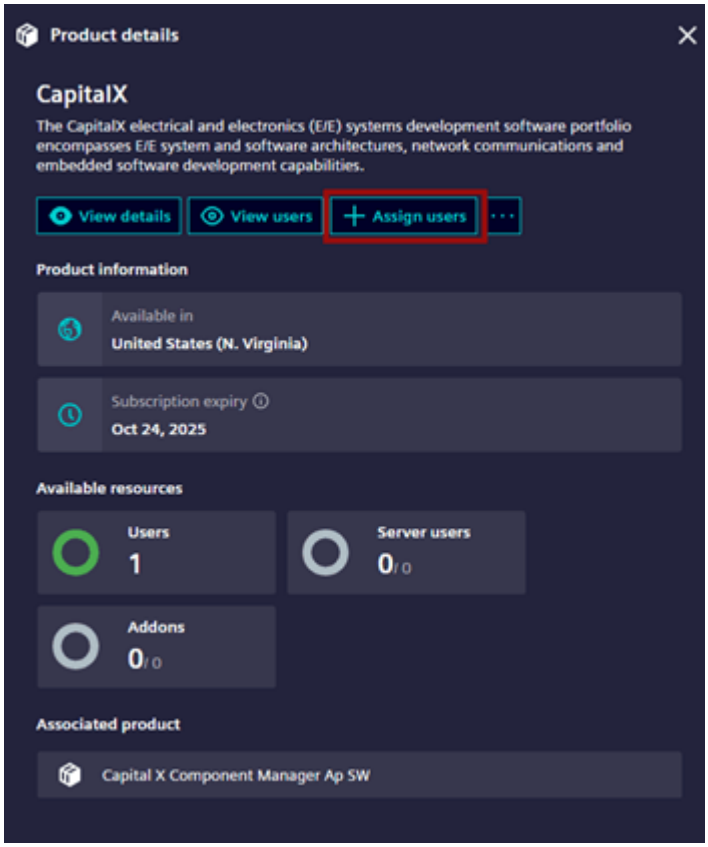

7. Click **Assign user to product**.

The product and user are now configured to the product family.

## Assign a User to a Product Family

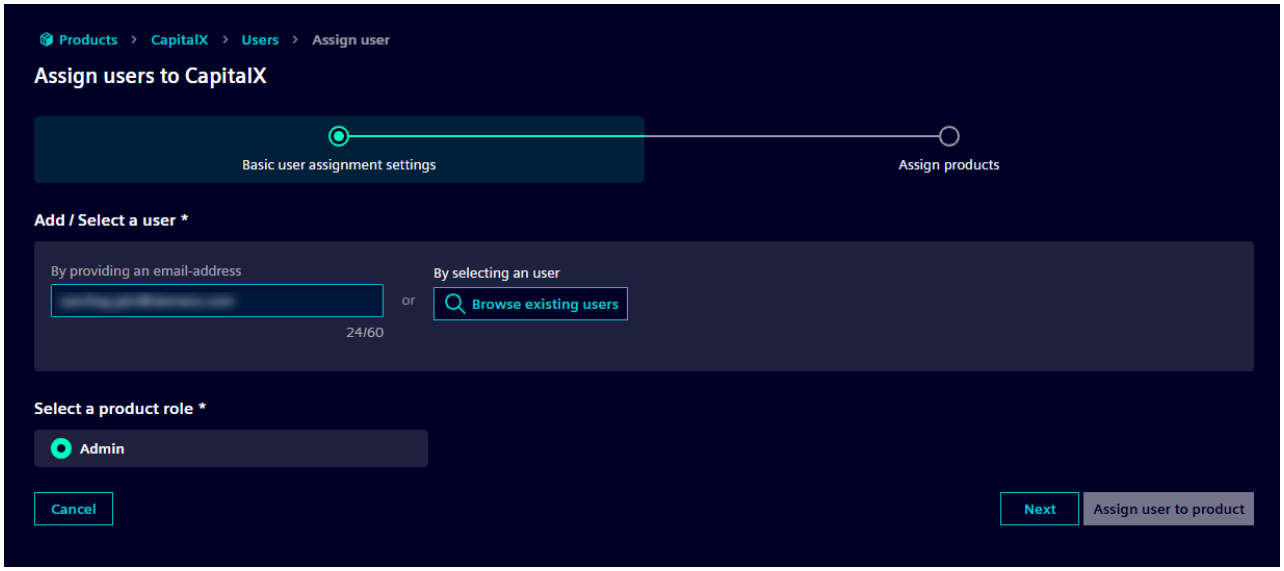
To assign a user to the product family:

1. In the **Products** list, select your product.
   - Search for the product using its display name or internal name, or use the filter options.
2. Go to the **Product details** screen and click **Assign users**.



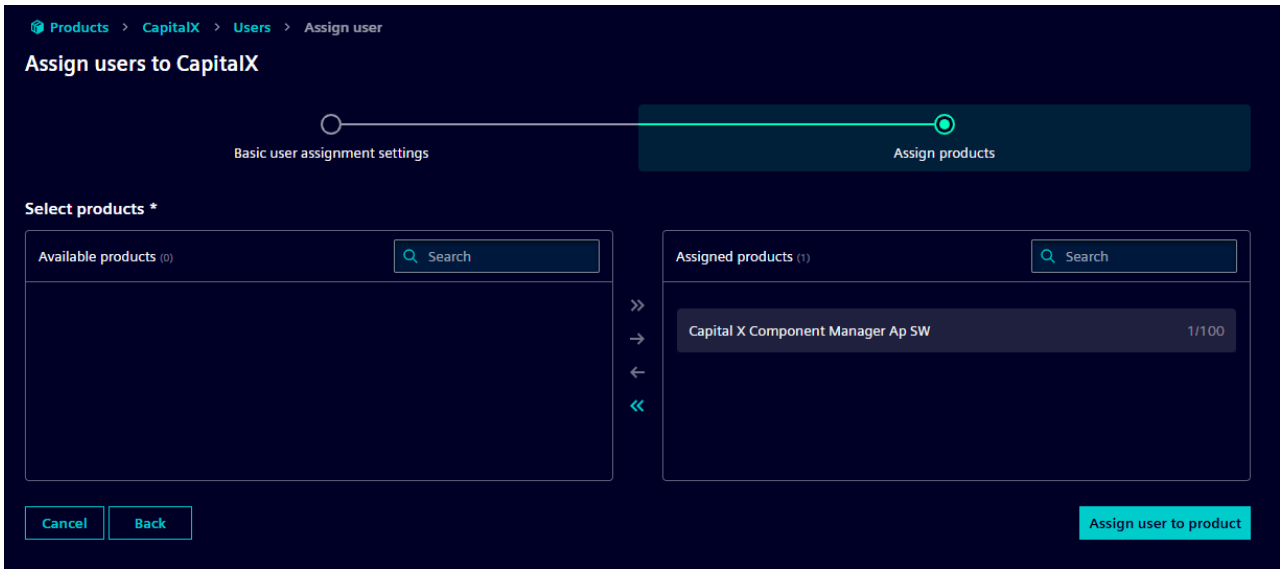

3. In the **Basic user assignment settings** tab, enter the following:
   - Enter the users email address, or click **Browse existing user** to select an existing user.

     **Note**
     - If group syncing is enabled, only existing users can be selected. For more information, refer to **Manage Groups and User Synchronization**.
     - If group syncing is disabled, you can add a new user or select from the existing list. For more information, refer to **Manage Groups and User Synchronization**.
     - If domain validation is enabled, only approved domains are accepted. For more information on validating domain, refer to **MultiFactor Authentication**.
   - Select a required product role for the user.
   - If the product supports environments: Select environments from the "Available environments" list and click →. To assign all environments, click ».
   - Click **Next**.




4. In the **Assign products** tab:

   - Select products from the "Available products" list and click → . To assign all products, click » .



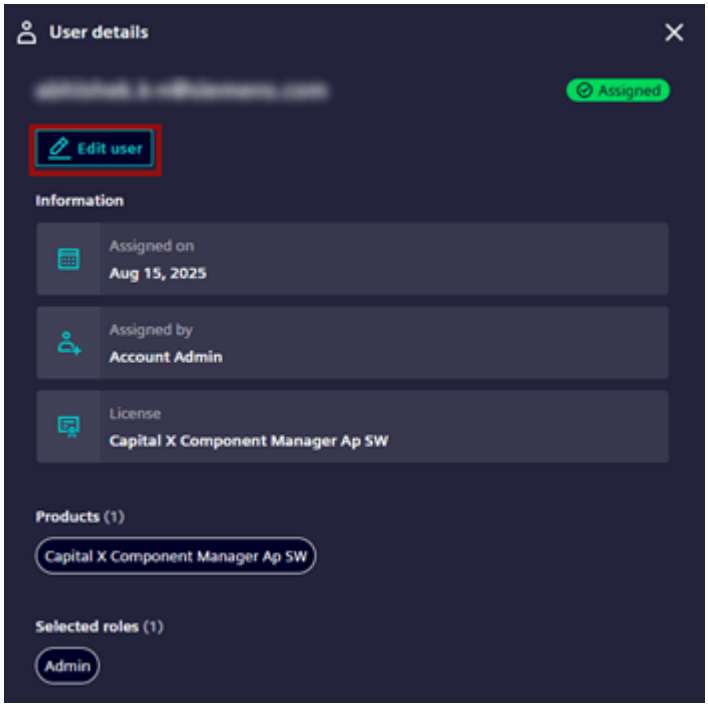

5. Click **Assign user to product**.

The user is now assigned to the product family.

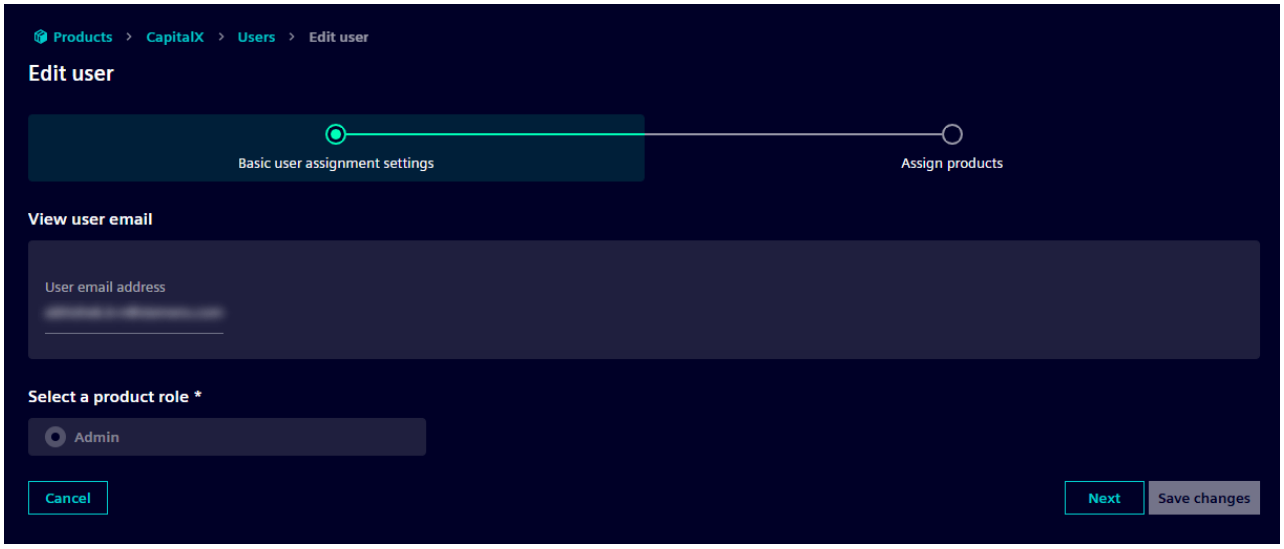
## Edit a User for the Product Family

To edit the user assigned products or add-ons for a product family:

1. In the **Users** section, click on the user to edit.
2. In the **User details** screen, click **Edit user**.

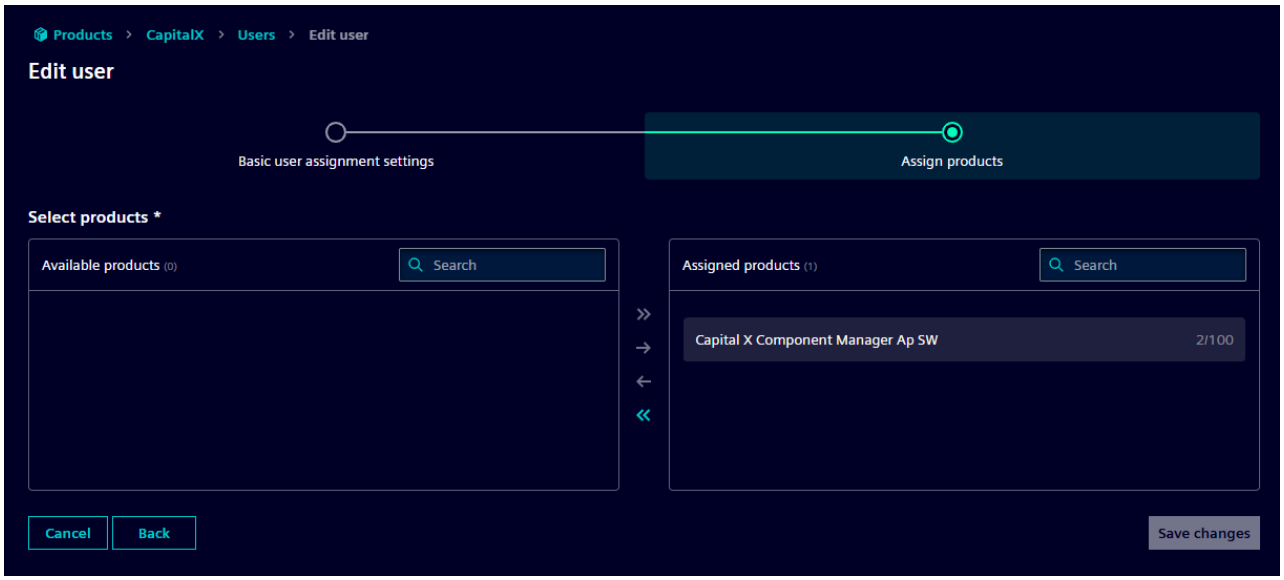



3. In the **Basic user assignment settings** screen, update the following:
   - Select the required product role.
   - If the product supports environments:
     - To assign environments: Select from the "Available environments" list and click →. To assign all, click ».
     - To unassign environments: select from the "Assigned environments" list and click ←. To unassign all, click «.
   - Click **Next**.




4. In the **Assign products** tab:

   - To assign products: Select products from the "Available products" list and click →. To assign all products, click ».
   - To unassign products: select from the "Assigned products" list and click ←. To unassign all, click «.




5. Click **Save changes**.

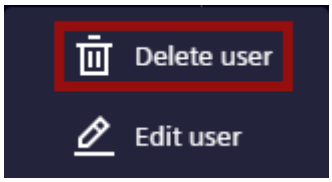
The user assigned products and environments are updated.

## Remove Users from the Product Family

To remove users or revoke their access and privileges from a product family:

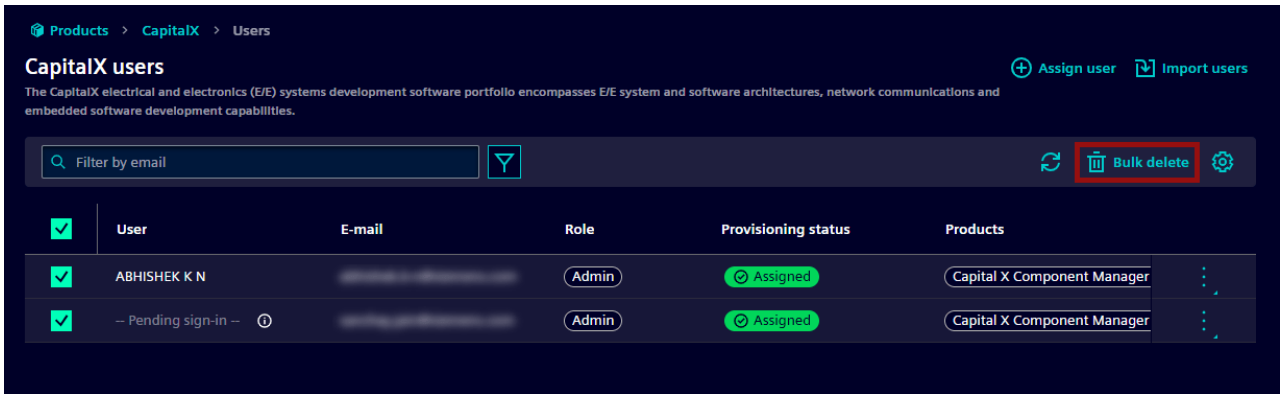
1. Select the user or multiple users to remove from the product family.

   - For single user: Click ⋮ and select **Delete user**.

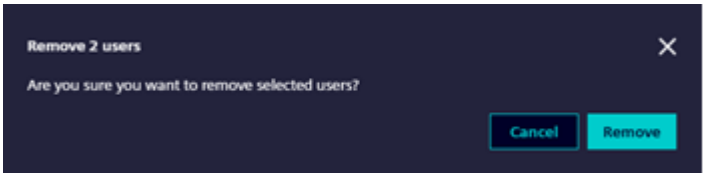



   - In the **Remove** pop-up, click **Remove**.


   - For multiple users, select the users you want to remove and click **Bulk delete**.




   - In the **Remove** popup, click **Remove**.

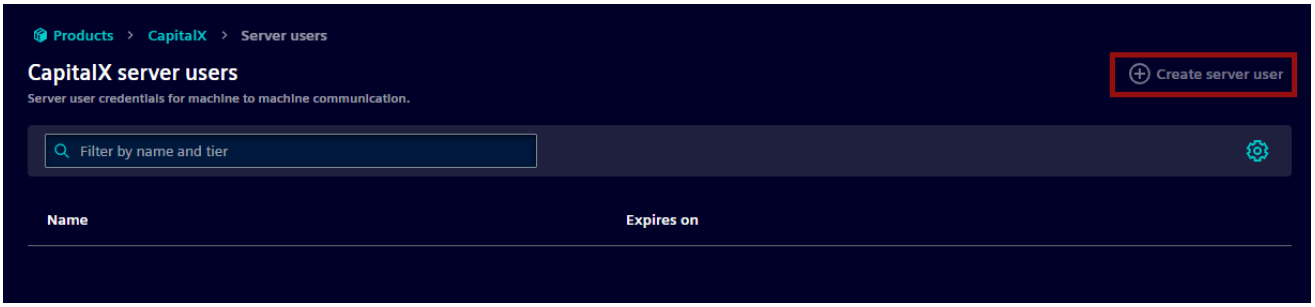



The selected user or multiple users associated with the product family are removed.

## Add a Server User to the Product Family

To add a server user:

1. In the **Product details** screen, click  and select **View server users**.
2. Click **Create server user**. For more information on managing server users, refer to **Server Users**




3. Click **Save**.

The server user is added to the product family.

## Bulk Import Users into the Product Family

This section explains how to import multiple users to a product using a CSV (Comma-Separated Values) template to streamline the bulk assignment process.

After uploading the CSV file, the data is processed and users are assigned to the product based on the specified tiers, roles, add-ons, and environments.

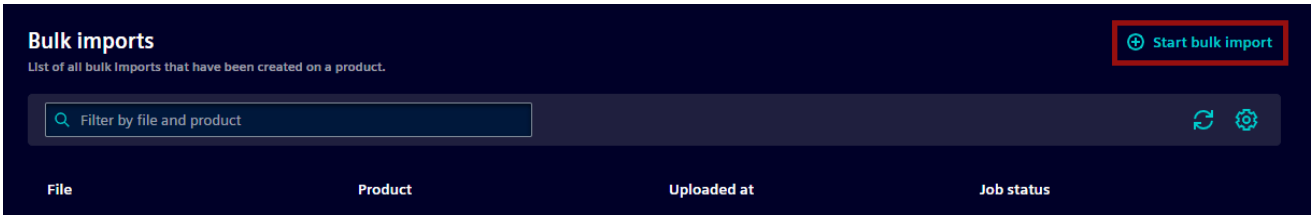
## Prerequisites

Ensure the CSV template contains the following data to import users to the specified product:

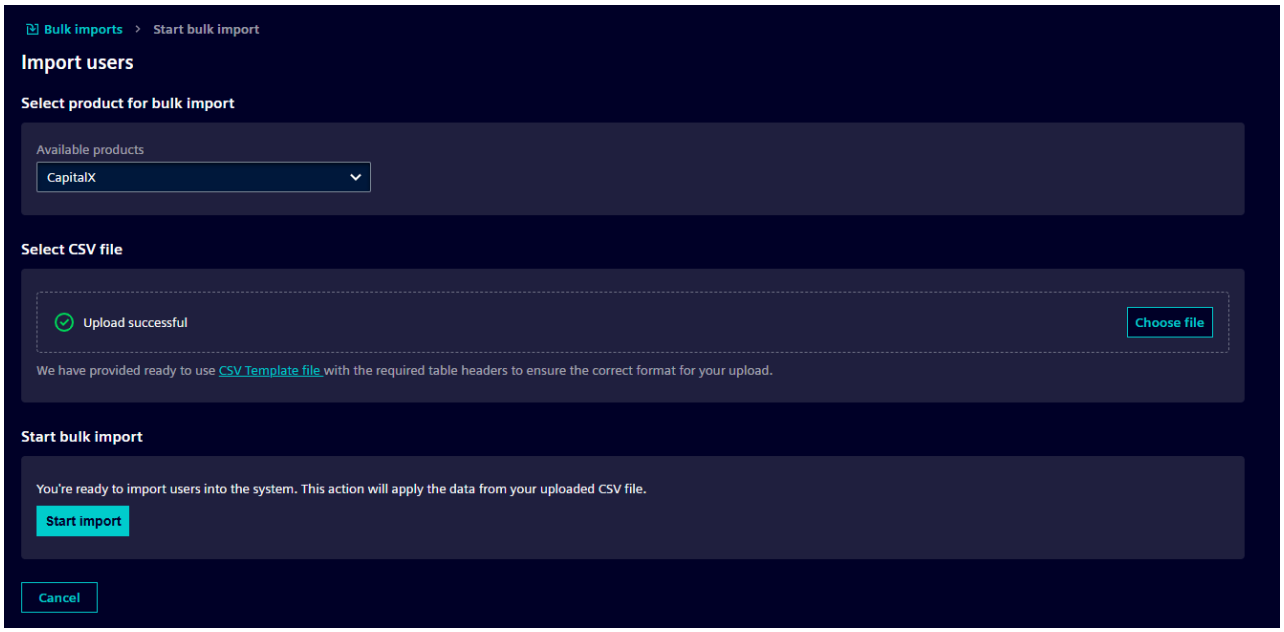
- **Email Address**: Valid email addresses of the users intended for import.
- **Roles**: Specify the required roles for each user.
- **Products**: Specify the required products for each user.
- **Addons**: Specify the required addons to assign to the user if the products support addons.

To import users to the product family:

1. Go to the **Bulk imports** tab in the left navigation pane.
2. In the **Bulk imports** screen, click **Start bulk import**.



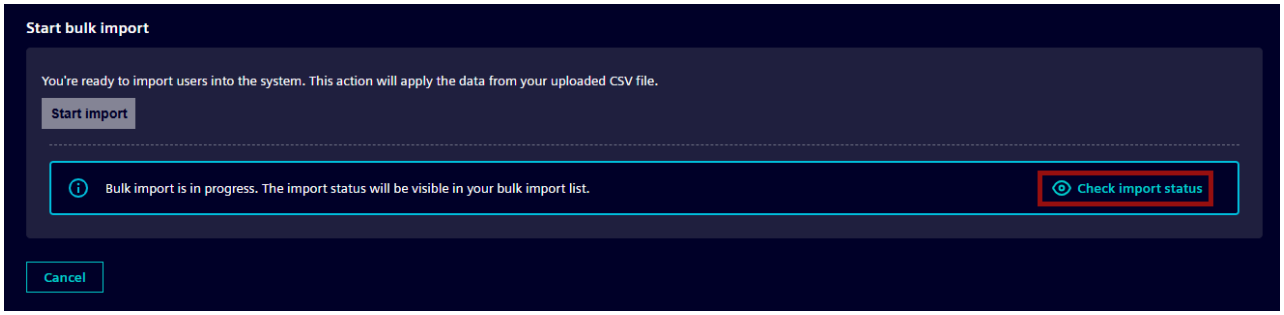
3. In the **Start bulk import** screen, select the product family to import users.
4. In the **Select CSV file** section:
   - Click **Choose file** and select the CSV file containing user details.
   - Click **Start import** to begin the import process.




**Note**

- Click **CSV Template file** to download a default CSV template in the **Select CSV file** section.
- Duplicate entries in the CSV file are marked as errors during the bulk import process.
- If the uploaded CSV template file has errors, such as invalid roles, product names, or issues related to domain validation, the upload process is flagged as an error.
- Each CSV file can include up to 1000 valid email addresses and must include at least one user.

   - In the **Start bulk import** section, click **Check import status** to monitor progress.




5. The system redirects you to the **Bulk imports** screen, which displays detailed information about the import job, including their respective statuses. Status includes:
   - **Import Successful**: The CSV file is imported successfully.

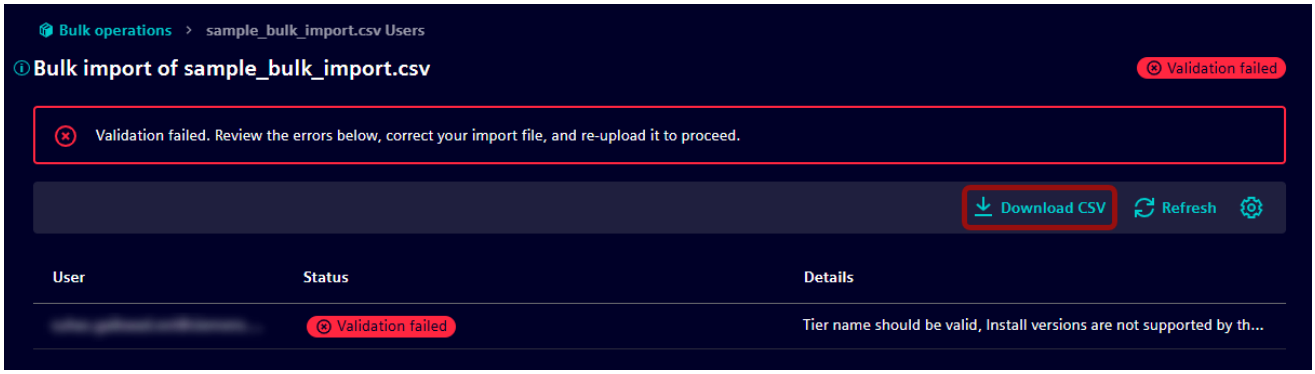
- **Validation Failed**: The validation process failed. Review the errors and retry the import.
- **Validation In Progress**: The system is currently validating the imported data.

6. Click **Refresh** button to update the list of bulk import jobs.

### Failed Imports

If the bulk import fails or contains errors:

1. Click **Download CSV** to retrieve the uploaded file for correction.
2. Fix the issues in the CSV file and import.




## Version Management in the Siemens Xcelerator Admin Console

Version management enables administrators to control the product versions assigned to specific users. This feature is applicable to products that support versioning across tiers. Users can access and download their assigned product versions from the Siemens Software Center.

**Prerequisites**:

- Administrator access to the Siemens Xcelerator Admin Console.
- Products with version support enabled.

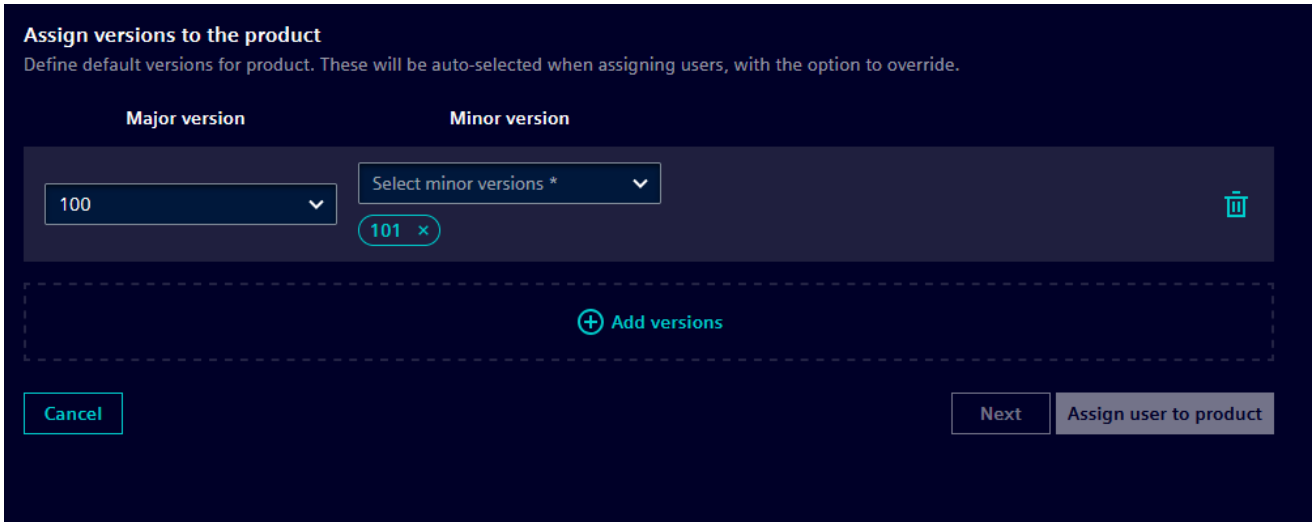
### Set the Default Product Version

Setting a default versions for tiers are pre-selected when users are assigned to that tier. This enhancement streamlines the process for ECA administrators, eliminating the need to manually select versions each time.

To set the default product version:

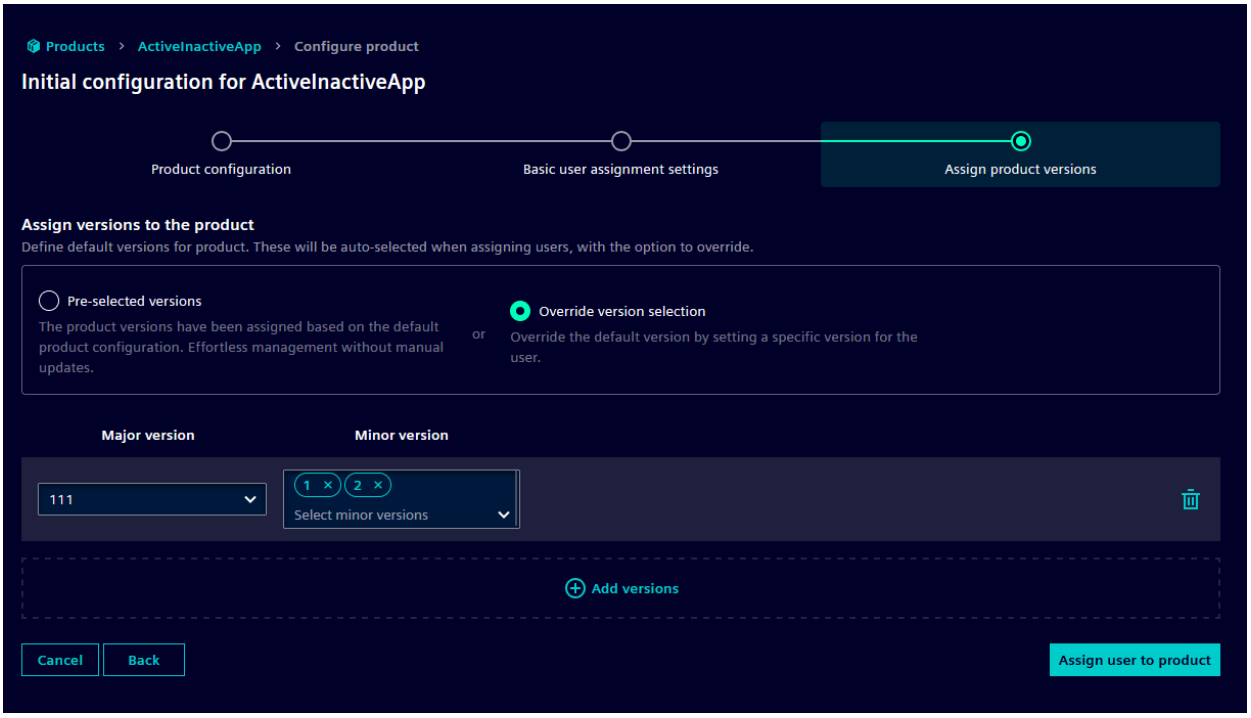
1. Sign in to the **Siemens Xcelerator Admin Console**.

2. Go to the **Products** tab in the left navigation pane and select the product to configure.
   - Search for the product by its display name or internal name, or use the filter options.
3. In the **Product details** screen, click **Configure product**. For more information on configuring the product, refer to **Configuring a Product for an ECA**.
4. In the **Assign versions to the product** section, add a default version and click **Next**.




> **Note**
> Setting a default version is optional.

5. In the **Basic user assignment settings** tab, enter the required fields. For more information on configuring the product, refer to **Configure a Product for an ECA**.
6. Click **Next**.
7. In the **Assign product versions** tab, select either of the option:
   - **Pre-selected Versions**: Assigns the default version.
   - **Override version selection**: Allows selection of specific major and minor versions.
     - Enter the major and minor version. If you select **Override version selection**.



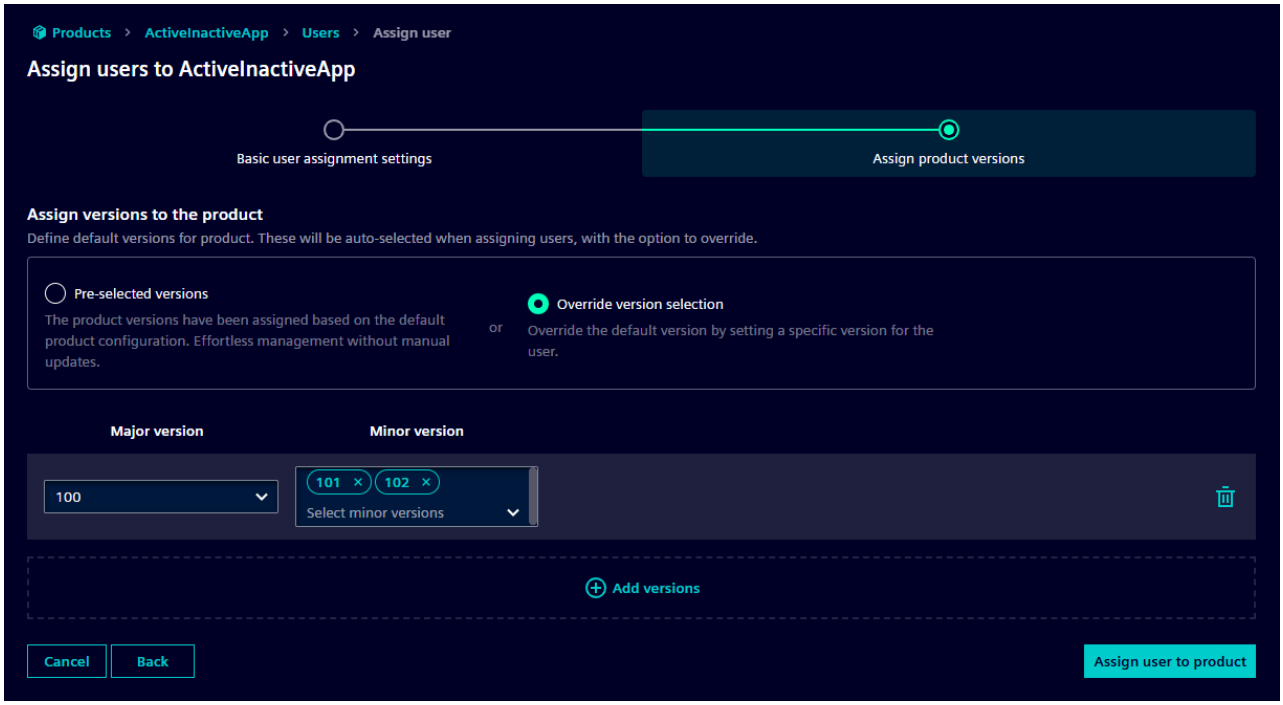

8. Click **Assign user to product**.

The default version with user assignment is configured.

## Assign a User to a Specific Product Version

To assign a user to a specific product version:

1. In the **Products** list, select the product.
   - Search for the product by its display name or internal name, or use the filter options.
2. Go to the **Product details** screen and click **Assign User**. For more information on assigning user to the product, refer to Assigning Users to the Product.
3. In the **Assign product versions** tab:
   - If the product default versions are set, they are pre-selected. You can override these selections by clicking on **Override version selection** and assign different versions as needed.
   - Enter the major and minor version, if you select **Override version selection** option.




> **Note**
>
> If no default version is set, all versions are applicable to the user.

4. Click **Assign user to product**.

The user is assigned to a product with a version.

## Edit Product Version

The Edit User option allows you to edit either the default version or a user-specific product version.

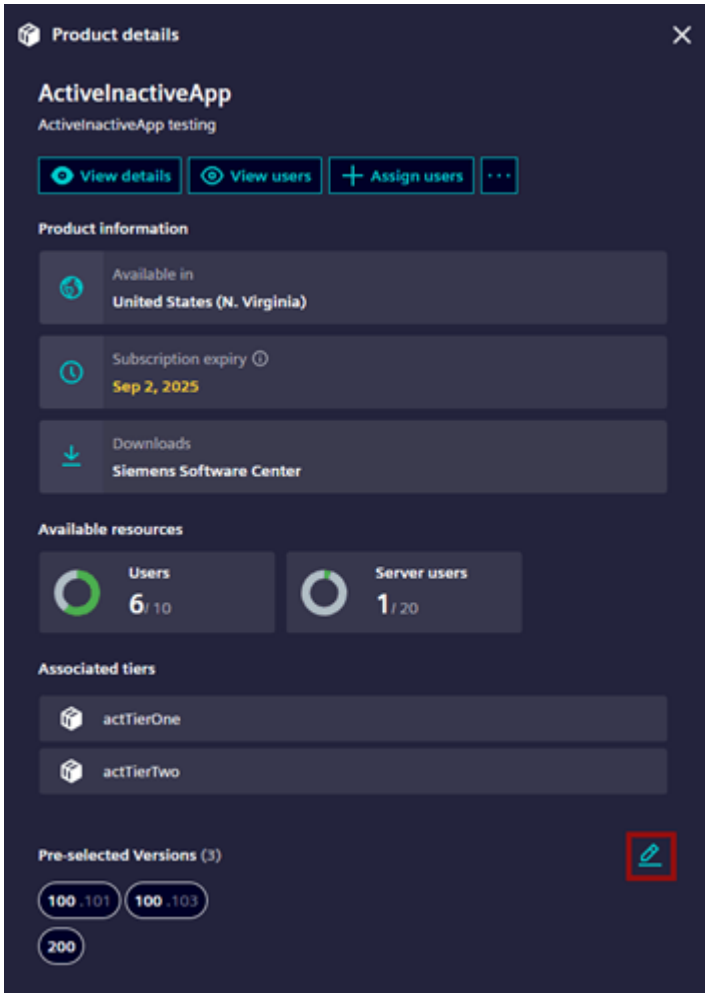
> **Note**
>
> - Changes to the default version apply only to new users. Existing users with the default version are not affected.
> - Existing users with the "All versions" badge are affected only if no user-specific or default version is set.
> - Changes to the default version apply to existing users when an admin removes all user-specific versions using the "Edit User" feature and a default version is set.

## Edit the Default Version

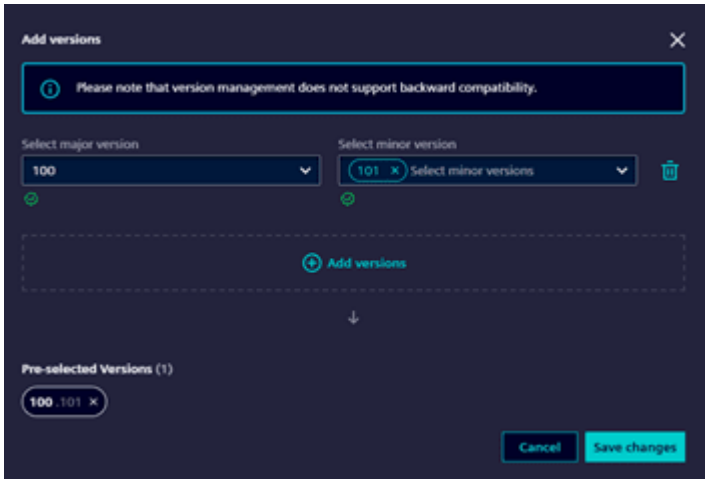
Editing the default version updates all user assignments linked to it.

To edit the default version:

1. In the **Products** list, select the product.
2. In the **Product details** screen, click **Edit** icon.




3. In the **Add versions** pop-up, update the major and minor versions as needed and click **Save changes**

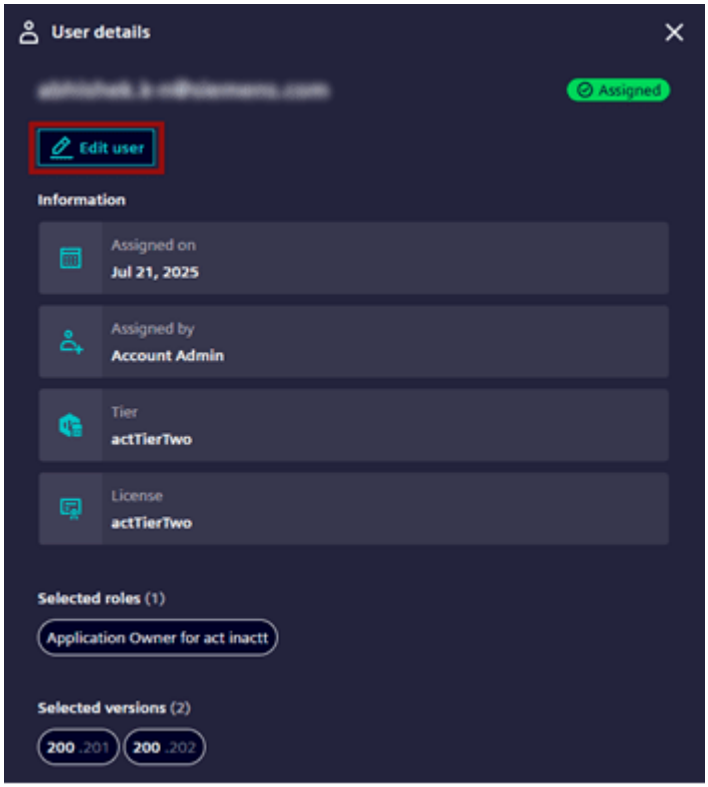



The default version is updated with the changes.

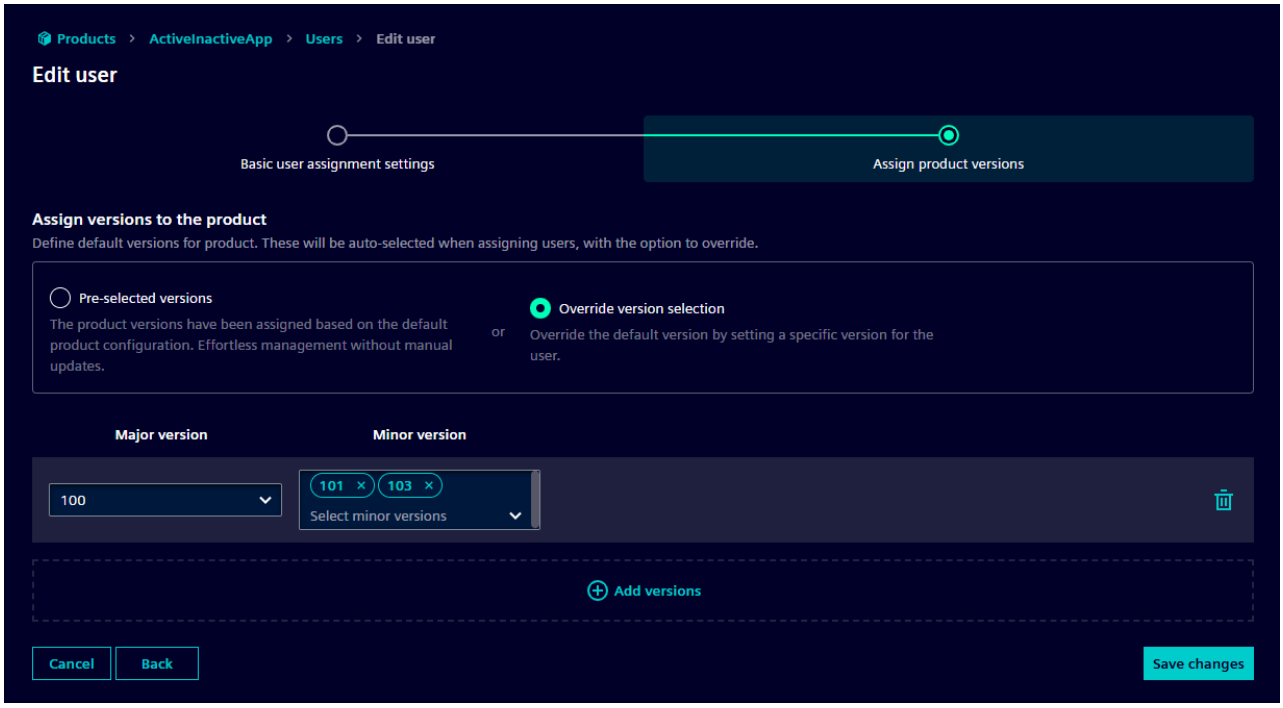
## Edit a User-Specific Product Version

To edit the user to a specific product version:

1. Select the user from the list of assigned users.
2. In the **User details** screen, click **Edit User**. For more information, refer to **Editing a User Assignment**.




3. In the **Assign product versions** tab:
   - If the product default versions are set, they are pre-selected. You can override these selections by clicking on **Override version selection** and assign different versions as needed.
   - Enter the major and minor version or modify the existing versions as needed, If you select **Override version selection** option.




**Note**

If the user version is not set, a default version is automatically pre-selected.

4. Click **Save changes**.

The user is updated with the modified changes.

## Import Bulk Users to Specific Product Version

To import bulk users to specific product versions, follow the steps below:

1. Go to the **Bulk import** tab in the left navigation pane.
2. Click **Start bulk import**.
3. In the **Start bulk import** screen, select the product for which you want to import users. For more information on importing Bulk Users to the Product, refer to **Import Bulk Users to the Product**.

**Note**

- If the uploaded CSV template file contains errors, such as an empty version column or incorrect version, the upload process is flagged as an error.
- When entering the version in the CSV file, ensure it is formatted as text using the format major.minor. If you do not want any minor versions, you can add a dot (example: 2024.).

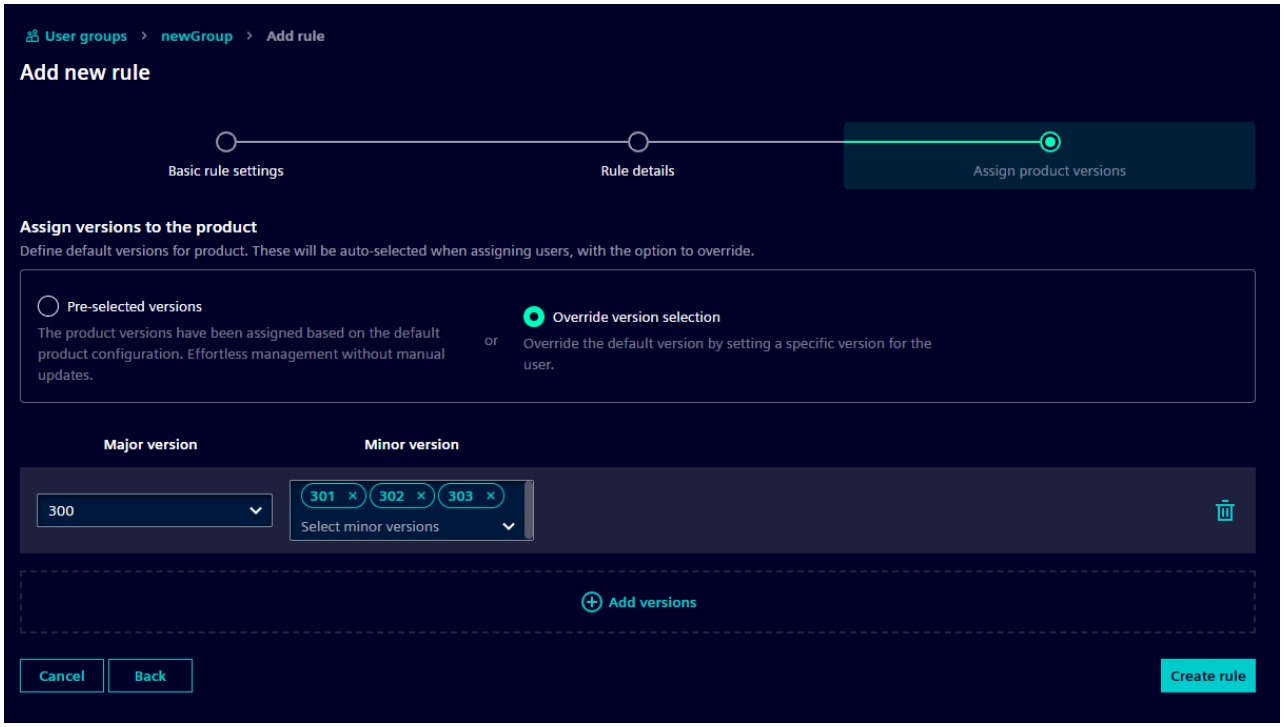
After completing the bulk import, the system redirects you to the **Bulk imports** screen. This displays detailed information about the import job. For more information, refer to **Import Bulk Users to the Product**.

## Automated User Assignment in Rules to Specific Product Version

## Create a Rule for a Specific Product Version

To create a rule for a specific product version:

1. Go to the **Groups** tab in the left navigation pane and select the group to add the rule.
2. Click **Add rule**. For more information on creating a rule, refer to **Automated User Assignment in Rules**.
3. In the **Assign product versions** tab:
   - If the product default versions are set, they are pre-selected. You can override these selections by clicking on **Override version selection** and assign different versions as needed.
   - Enter the major and minor version or modify the existing versions as needed, If you select **Override version selection** option.




> **Note**
>
> If no default version is set, all versions are applicable to the user.

4. Click **Create rule**.

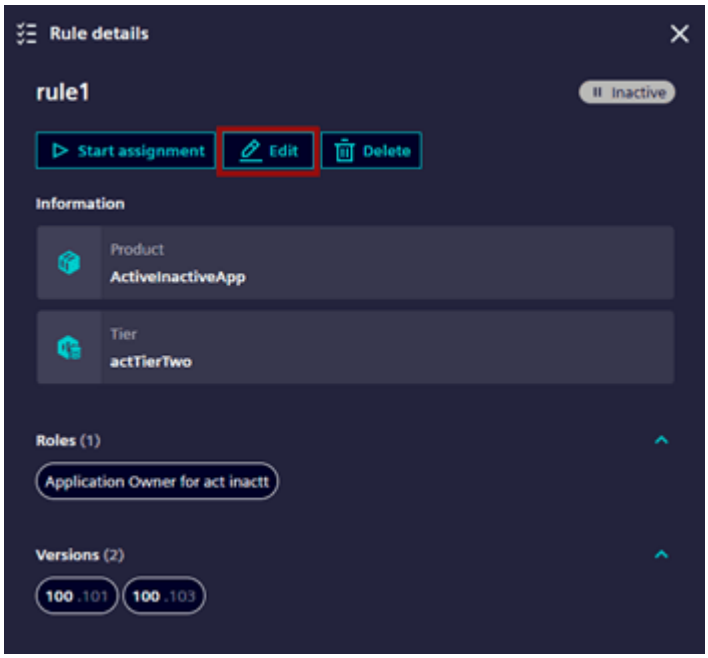
The rule is assigned with a version.

## Edit a Rule to a Specific Product Version

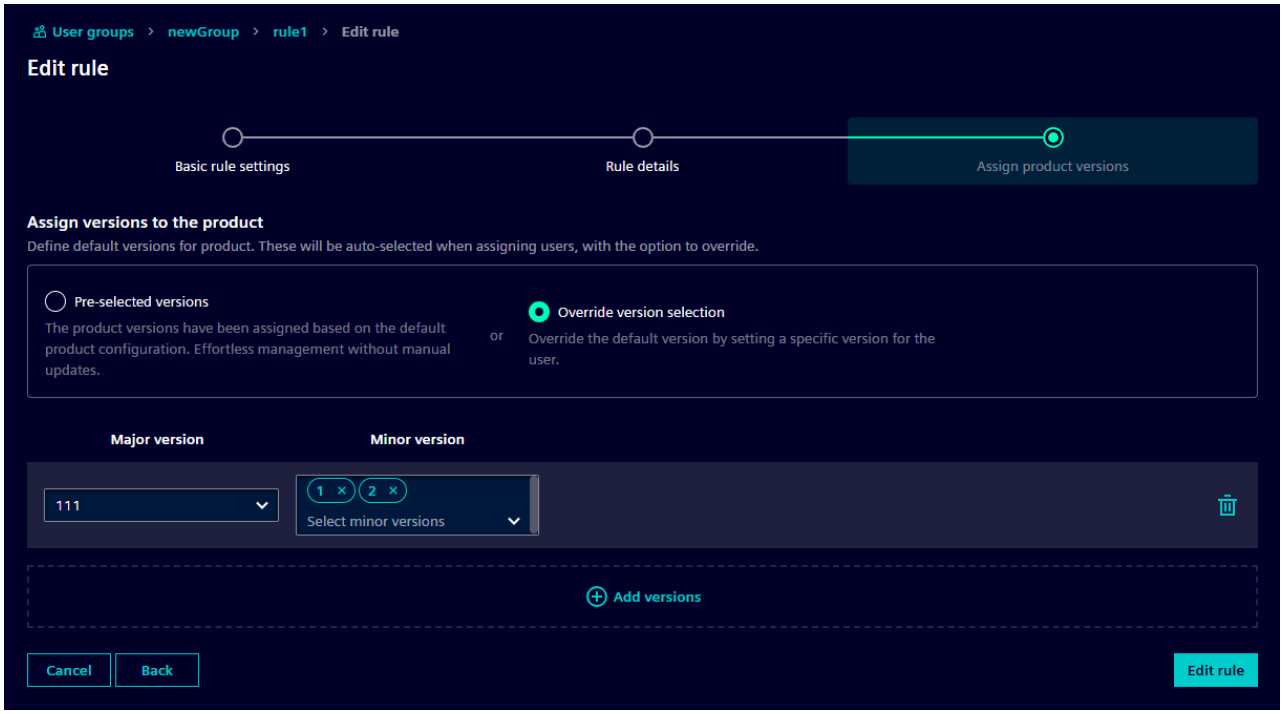
> **Note**
> The admin can edit all the fields, when the rule is either active or inactive.

To edit a rule to a specific product version, follow the steps below:

1. Select the rule to edit.
2. In the **Rule details** screen, click **Edit** button. For more information, refer to **Edit a Rule**.




3. In the **Assign product versions** tab:
   - If the product default versions are set, they are pre-selected. You can override these selections by clicking on **Override version selection** and assign different versions as needed.
   - Enter the major and minor version or modify the existing versions as needed, If you select **Override version selection** option.




4. Click **Edit rule**.

The rule is updated with the modified changes.

# User Centric

## Overview

User Centric dashboard provides a centralized, region-based view of user information. It allows administrators to support teams to locate and review user details, add new user, download user list. When you select a region, it displays the user list for that region.

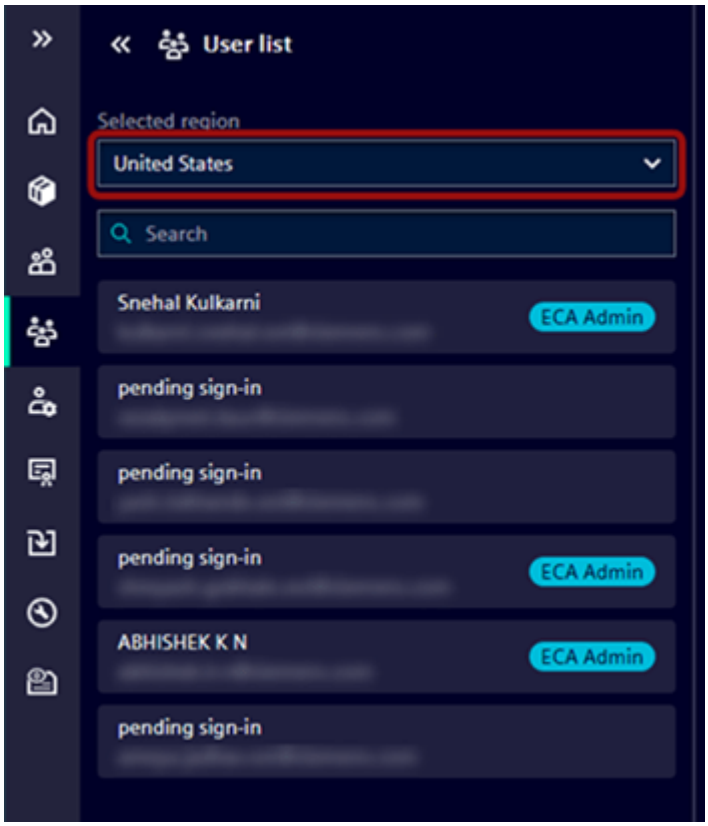
From the User Centric dashboard, you can:

- Add new user.
- View all users in the selected region.
- Access a read-only view of user assignments, including products, roles, and groups.
- View products assigned to each user and their current status (such as active or inactive).
- Download user list for the selected region.

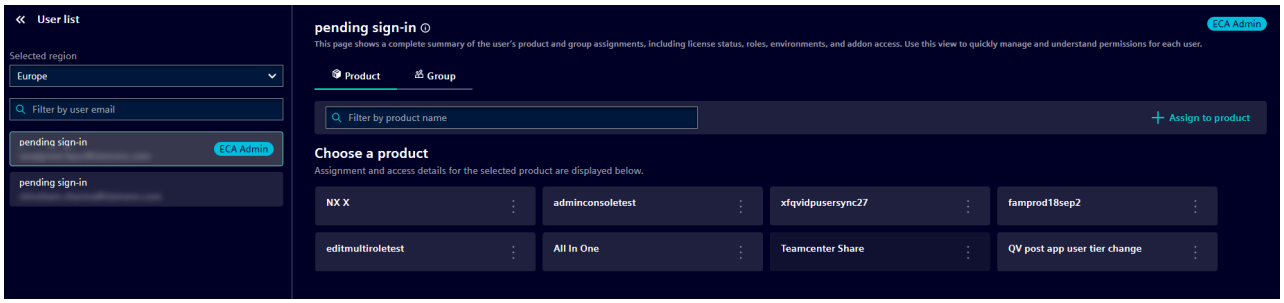
## Access the User Centric Dashboard

To access the User Centric dashboard:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. In the left navigation pane, select the **User centric** tab.
3. Select a region from the dropdown list.




4. Select a user to view details.
   - Search for a user by name or email.




5. Select a tab to view additional details.
   - **Product**:

     The **Product** tab shows all products assigned to the user, along with assignment details and access settings.

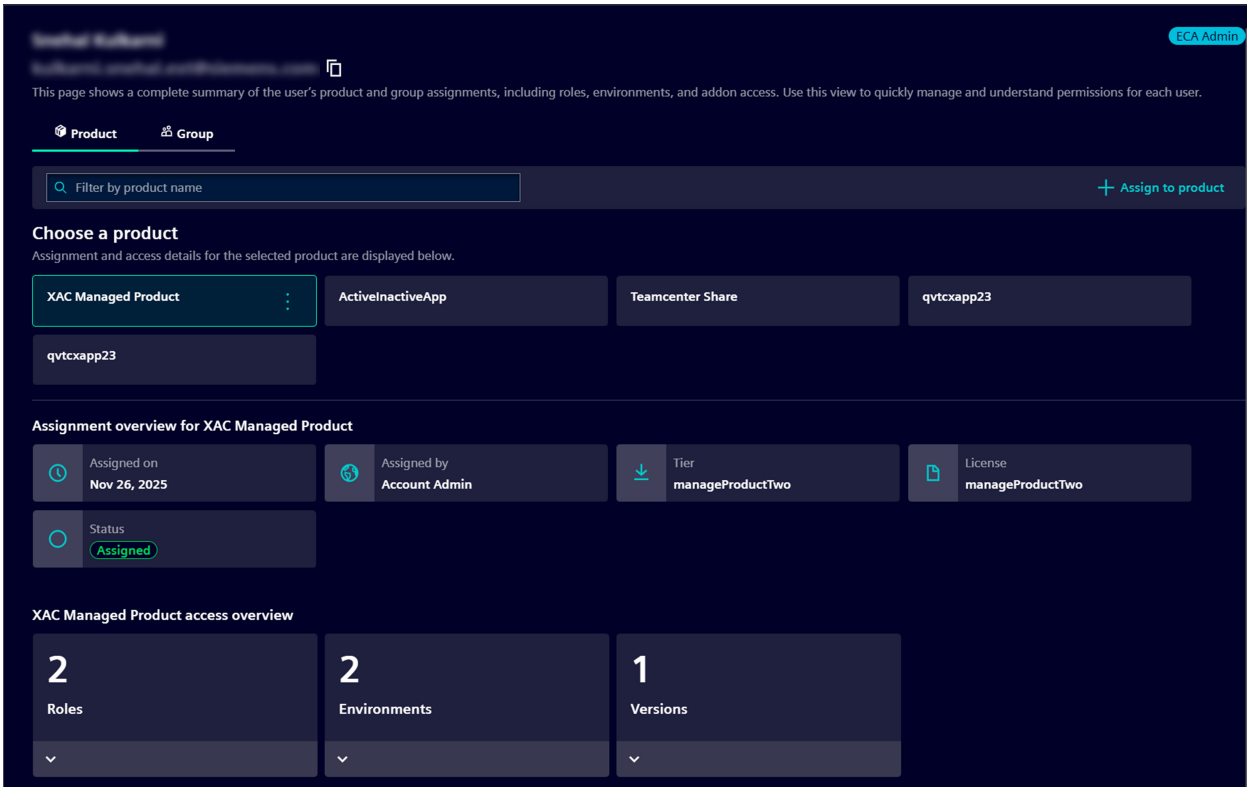
## View Product Details

To view product details:

- In the **Product** tab, select a product.
- View the following assignment details:
  - **Assigned on**: Date the product was assigned.
  - **Assigned by**: Name of the user who assigned the product.
  - **Tier**: License tier assigned to the user.

    > **Note**
    > The tier is not displayed for products associated with a product family.

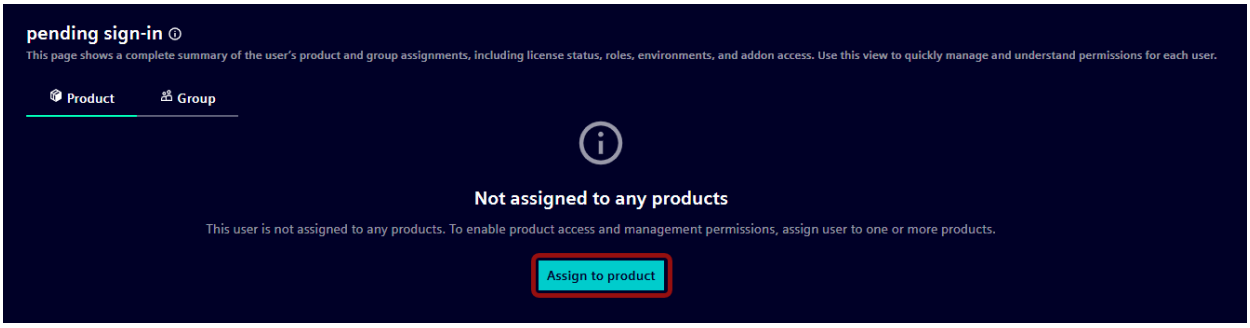
  - **License**: Product for which the user has a license.
  - **Status**: Provisioning status of the user.
- View product access details for the selected user:
  - **Roles**: User roles within the product.
  - **Addons**: Additional addons assigned to the user (if applicable).
  - **Versions**: Product versions the user can access (if the product supports and assigned with versions).
  - **Environments**: Deployment environments available to the user (if the product supports and assigned with environments).
  - **Products**: Sub-products assigned to the user (applicable only for product family).




## Assign a Product (First-Time Assignment)

If the user is not assigned to any product:

- Click **Assign to product**.



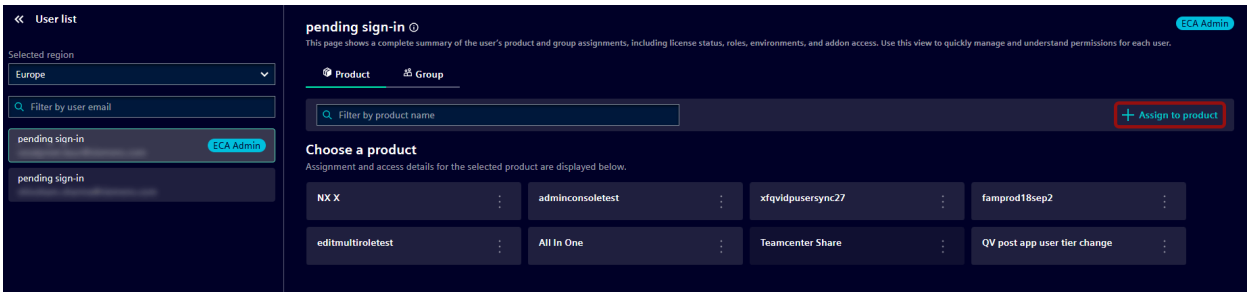

- Select a product. For more information on assigning a product to a user, refer to **Assign Users to a Product**.

> **Note**
>
> The product list displays only products configured in the selected region.


## Assign Additional Products

To assign additional products to a user who already has product assignments:

- Click **Assign to product**.




- Select a product. For more information on assigning a product to a user, see **Assign Users to a Product**.

> **Note**
>
> The product list displays only products configured in the selected region.

### Remove a user from a product

To remove a user from a product:

- In the **Product** tab, select the product.
- Click  , select **Remove from product**.

> **Note**
> You cannot remove a user from a product if the assignment is pending.

- In the **Remove user** pop-up, click **Remove**.

The user is removed from the product.

- **Group**:

The **Group** tab lists all groups assigned to the user and allows you to manage group assignments by selecting a group. For more information on managing group assignments, refer to **Manage Groups and User Synchronization**.

### View Group Details

To view group details:

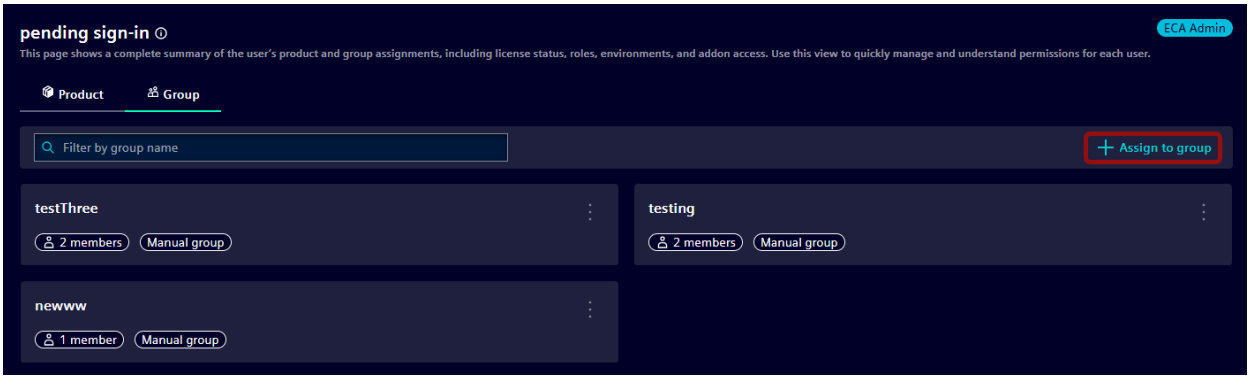
- In the **Group** tab, select a group.
- View the following group information:
  - Group name
  - Group type
  - Number of users in the group

### Assign a User to a Group

To assign a user to a group:

- Click **Assign to group**. For more information, refer to **Manual Groups**.

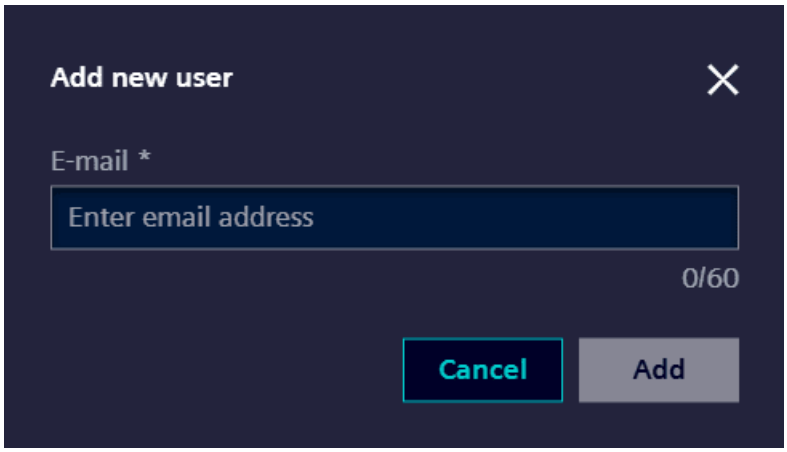
> **Note**
> The group list displays only groups configured in the selected region.




## Add a New User

To add a new user:

1. Select a region from the dropdown list.
2. Click ⋮ and select **Add new user**.
3. In the **Add new user** pop-up, enter the user's email address, click **Add**.




The user is added to the selected region.

## Download user list

Downloading a user list allows you to view information about assigned users, including product name, tier name, roles, sub products, addons, versions, deployment environment, region, assignment date, assigned by, license, and groups.

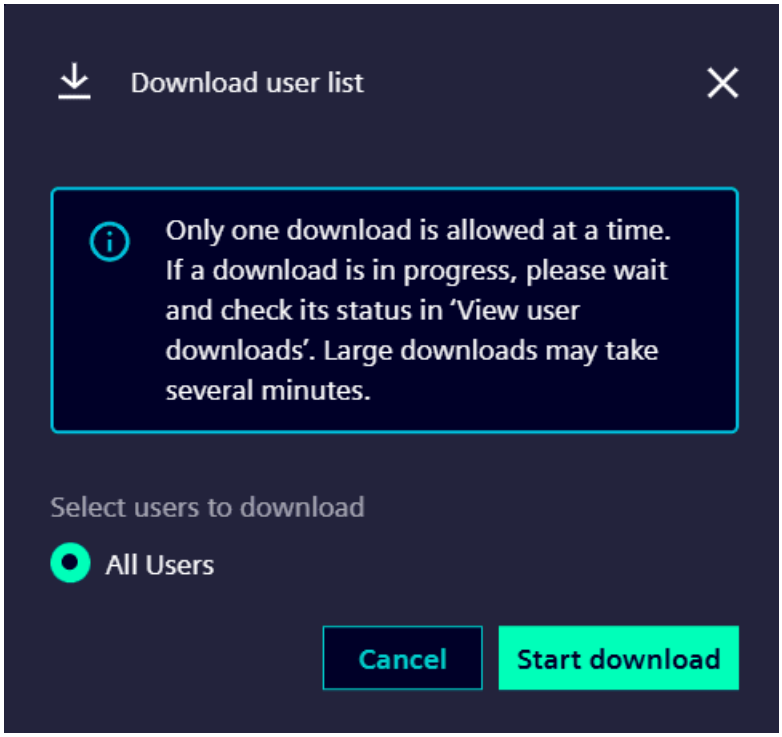
**Note**

- You can download one file at a time. If a download is already in progress, the option to download user list is disabled.

- The file is downloaded in CSV format.
- Preparing the file for download may take several minutes, depending on the amount of user data.

To download a user list:

1. Select a region from the dropdown list.
2. Click  and select **Download user list**.
3. In the **Download user list** pop-up, click **Start download**.




4. Once the file is ready, the page redirects to the **View downloads** screen.
5. Click the download icon for the selected file.

**Note**

After creation, the file can be downloaded for 2 days since its creation date from the View downloads screen.

## View downloads

View downloads allows you to view the list of download requests. For each request, you can see the requester name, creation date, expiry date, and status.

To view downloads:

1. Select a region from the dropdown list.
2. Click  and select **View downloads**.
3. Select the file you want to download and click the download icon.

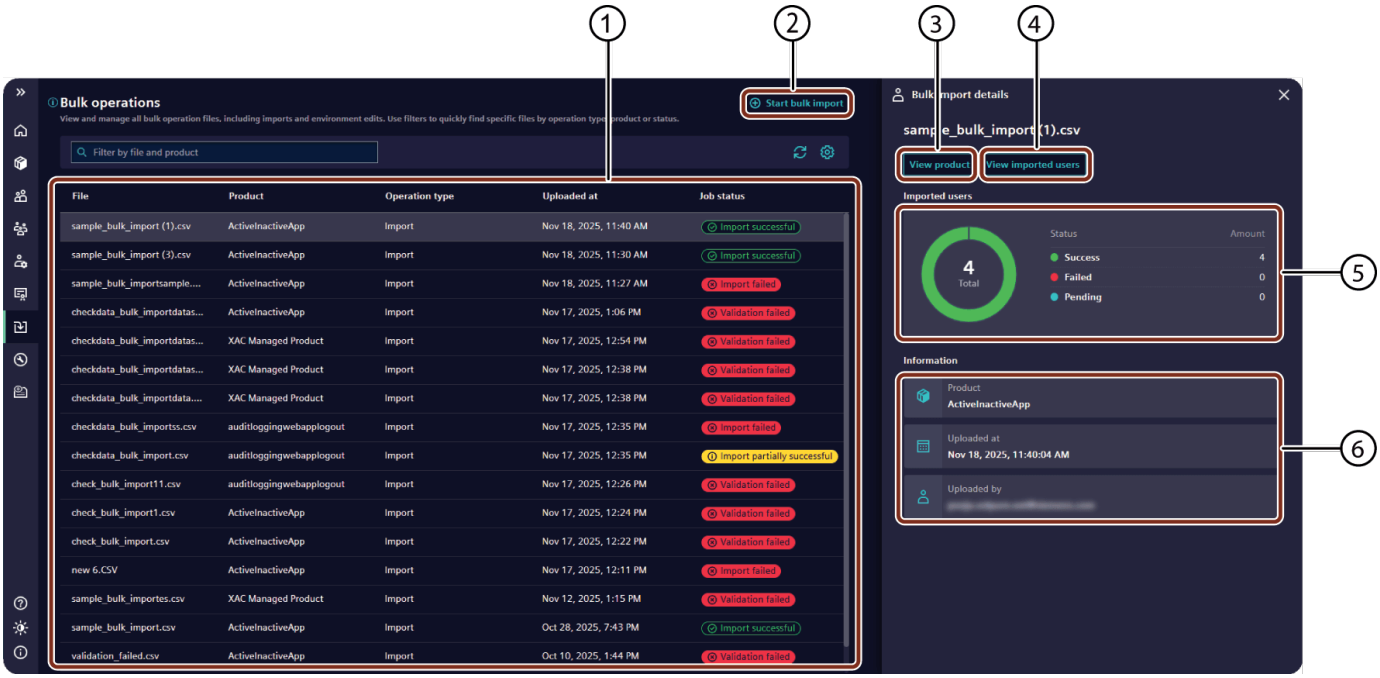

The file is downloaded successfully.

# 3. Bulk Import of Users

## Bulk Operations

This section explains how to import multiple users to a product, streamlining the bulk assignment process through a CSV (comma separated values) template.

After you upload the CSV file, the system processes the data and assigns users to the product based on the specified tier and role details.




① View a complete list of uploaded CSV files, including product name, upload date and time, and job status.

② Allows you to start a new bulk operation.

③ Allows you to view detailed information related to the selected product and bulk import assignment.

④ Allows you to view the list of users imported from the selected CSV file, including email addresses, assigned tiers, roles, and current provisioning statuses.

⑤ Shows the number of users in each category for the selected file:

- **Success**: Number of users successfully added.
- **Pending**: Number of users being processed.

- **Failed**: Number of users that failed to import.

⑥ Displays metadata for each uploaded file:

- **Product**: Name of the product associated with the bulk operation.
- **Uploaded at**: Date and time the file was uploaded.
- **Uploaded by**: Name of the user who uploaded the file.

## Prerequisites

Ensure the CSV template includes the following data to import users to the desired product:

- **Email Address**: Valid email addresses for each user.
- **Roles**: Specify the desired roles for each user.
- **Tier Name**: Specify the desired tier for each user.
- **Addons**: Specify the addons, if supported by the product.
- **Environments**: Specify an environment if the product supports deployment environments.
- **Versions**: Specify the installation versions if the product supports versions.

> **Note**
>
> To assign multiple roles, tiers, versions, or environments to a user, separate each value with a comma (,) in the CSV template.

## Import Users

To import users in bulk:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. Go to the **Bulk import** tab in the left navigation pane.
3. Click **Start bulk import**.

4. In the **Start bulk import** screen, select the product to import users.


**Note**

If the selected product includes Teamcenter Share, you must select the region. If you do not set the region, provisioning fails for all users assigned through this rule. For more information on selecting the region, refer to **Assign a User**

5. In the **Select CSV file** section:

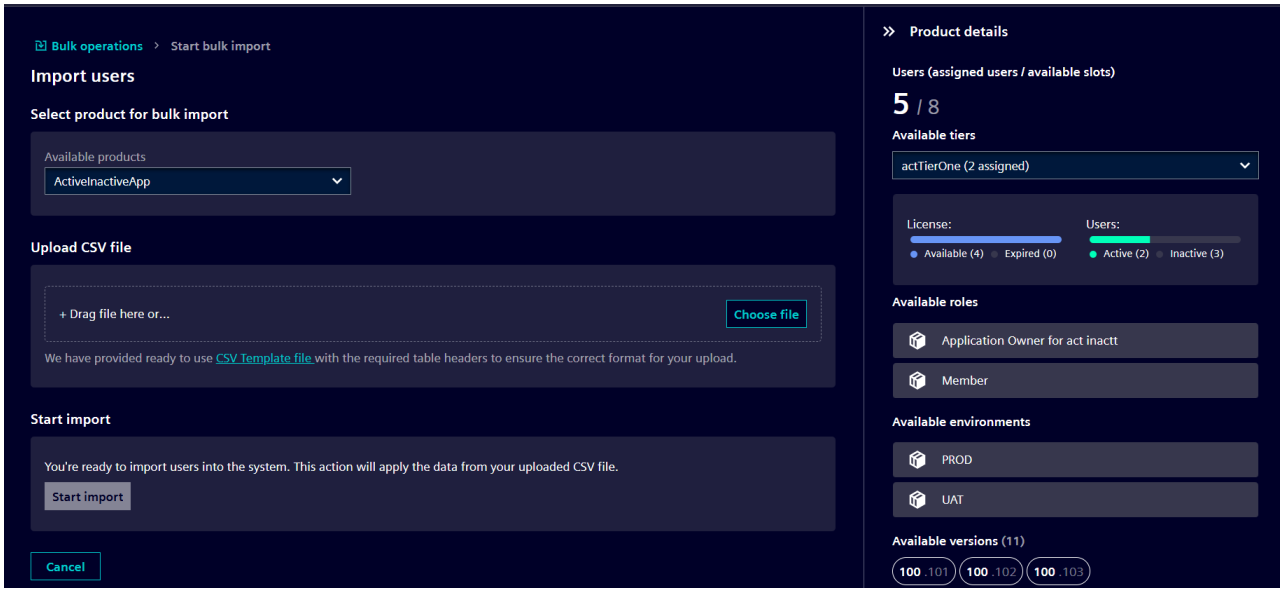
- Click **Choose file** and select the CSV file containing user details.
- Click **Start import** to begin the import process.

**Note**

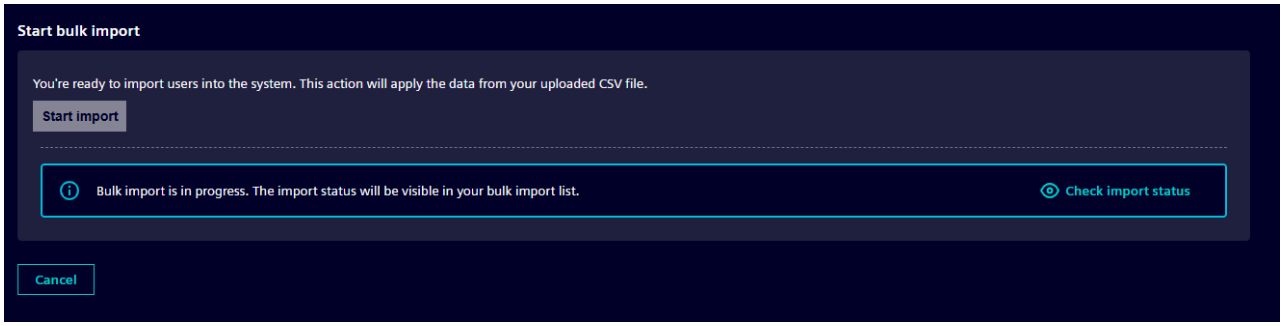
- The **CSV Template file** link in the **Select CSV file** section provides the default CSV template for download.
- Duplicate entries in the CSV file are marked as errors during the bulk import process.
- If the uploaded CSV template file has errors, such as invalid roles, tier names, or issues related to domain validation, the upload process is flagged as an error.
- Each CSV file can include up to 1000 valid email addresses and must include at least one user.

**Note**

**Malware Scanning**: When you start a bulk import, the system scans the uploaded CSV file for malware in the background. The scan duration depends on the file size. During this process, the import status displays **Malware scan in progress**. If malware is detected, the status changes to **Failed with malware detection** and the import stops. Review the error details and upload a clean file to continue.




- In the **Start bulk import** section, click **Check import status** to monitor progress.




6. The system redirects you to the **Bulk imports** screen, which displays detailed information about the import job, including their respective statuses. Status includes:
   - **Import successful**: The CSV file is imported successfully.
   - **Import in progress**: The system is currently processing the CSV file.
   - **Import partially Successful**: The CSV file is imported with some errors. Review the failed entries and correct them if needed.
   - **Import failed**: The import process failed because the bulk import operation either called another service while still importing is in-progress or the entire CSV file format was invalid (for example, due to data errors or schema mismatch).
   - **Validation failed**: The validation process failed. Review the errors and retry the import.
   - **Validation in progress**: The system is currently validating the imported data.
   - **Malware scan in progress**: The system is scanning the CSV file for malware.
   - **Failed with malware detection**: The validation process failed due to the detection of malware in the uploaded file.
7. Click **Refresh** to update the bulk import jobs.

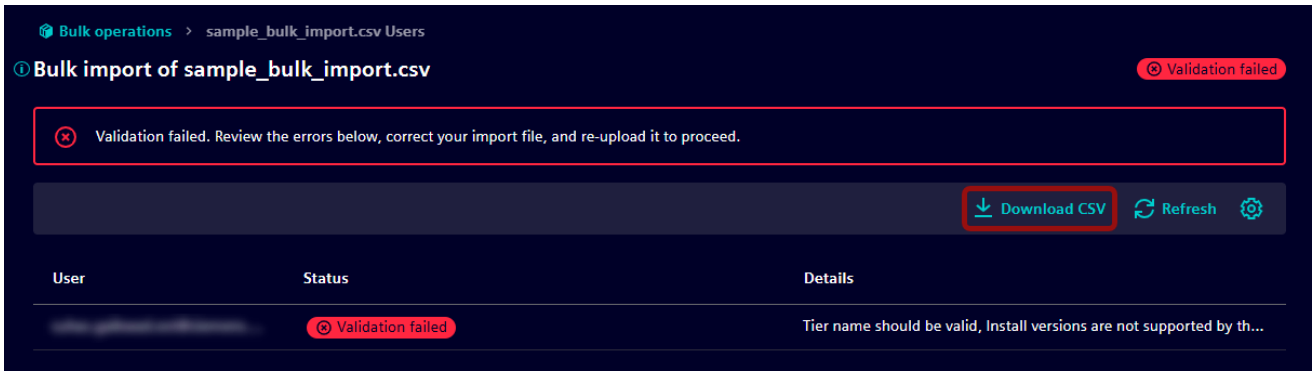
The users are imported successfully through bulk operation.

## Failed Imports

If the bulk import fails or contains errors:

> **Note**
> If the bulk import status is **Import failed**, the **Download CSV** file option will be unavailable.

1. Click **Download CSV** to retrieve the uploaded file for correction.
2. Fix the issues in the CSV file and import the CSV file.

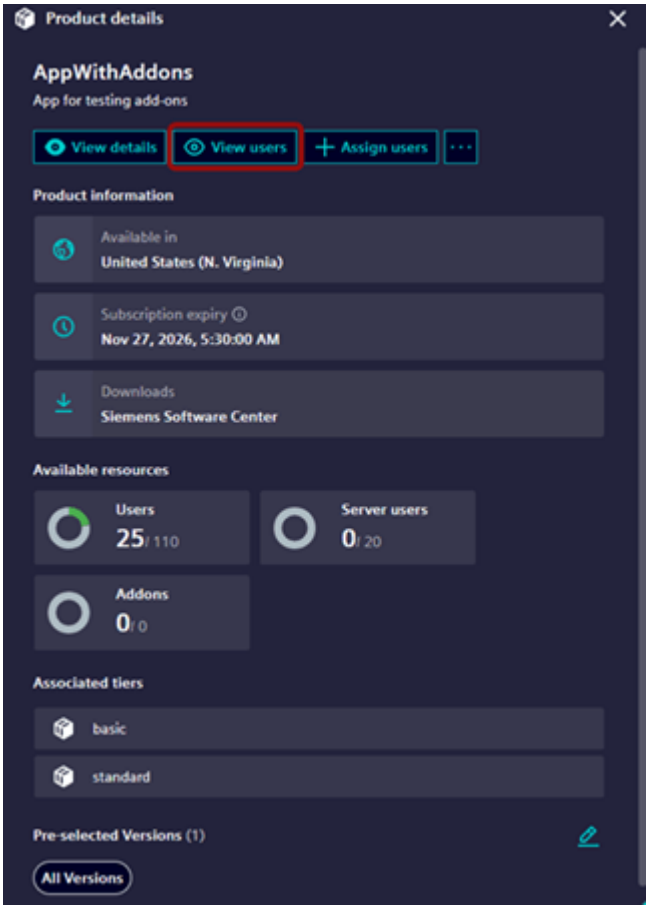



## Edit Bulk Environment

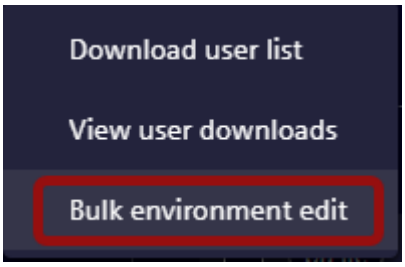
Edit bulk environment enables you to update environments for multiple users through bulk import. This function is available only for products that support environments.

To edit environments in bulk:

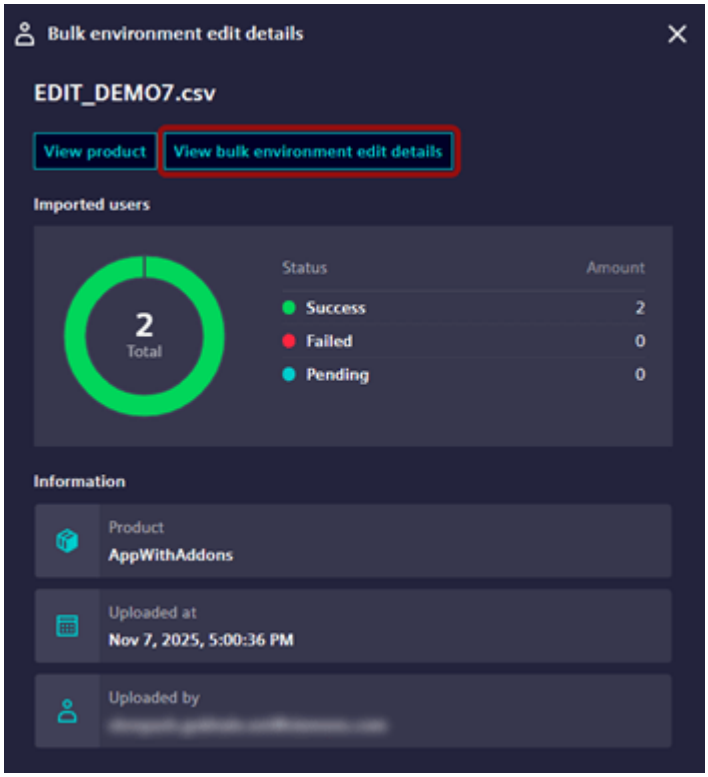
1. Go to the **Products** tab in the left navigation pane.
2. In the **Products** list, select the product.
   - Search for the product by its display name or internal name, or use the filter options.
3. In the **Product details** section, click **View users**.




4. Click ··· button, select **Bulk environment edit**.




5. Import the CSV file with the updated environments. For more information, refer to **Import Users**.
6. After the file is updated, select the file and click **View bulk environment edit details** to review the updated environments.




The environments for the selected users are updated.

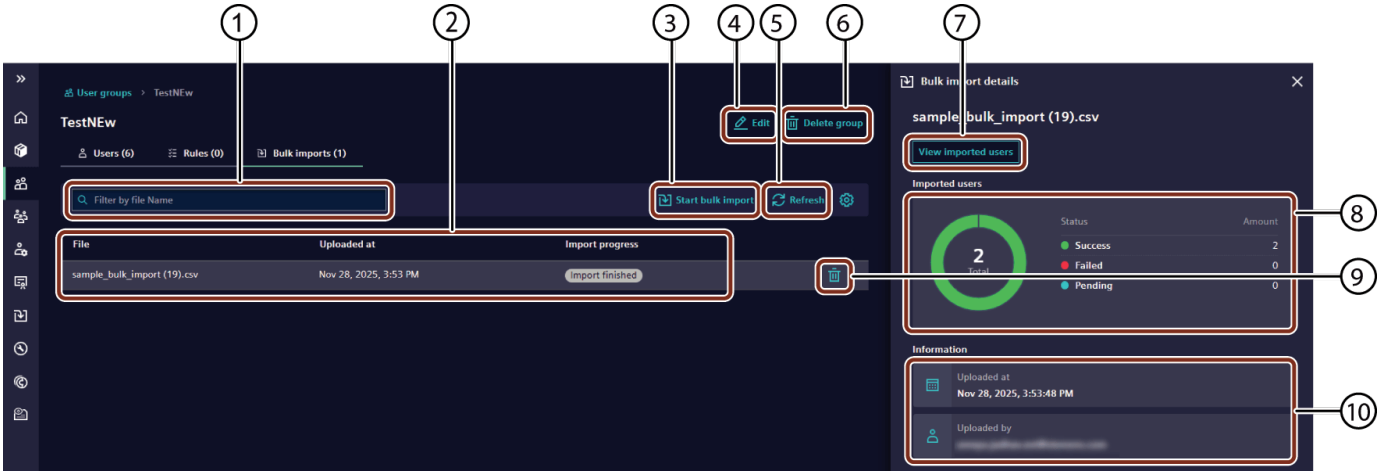
## Import Bulk Users into Groups

The bulk import option enables the ECA Admin to add multiple users to a group. When you upload the CSV file, the system processes the data and assigns users to the specific group.

**Prerequisites**:

Ensure the CSV template has valid email addresses for the users you want to import.

**Overview of "Bulk Imports in Groups" screen**:




① Allows you to search the required file by CSV file name

② View the list of CSV files imported

③ Allows you to update the list of bulk import jobs

④ Allows you to edit the group description

⑤ Allows you to import bulk users to the group

⑥ Allows you to delete the group

⑦ Allows you to view the list of users imported from the CSV file, including email address, import progress status, and failure reason for failed assignments

⑧ Shows the number of users in each category for the selected file:

- **Success**: Number of users successfully added.
- **Failed**: Number of users that failed to import.
- **Pending**: Number of users being processed.

⑨ Allows you to delete the associated CSV file

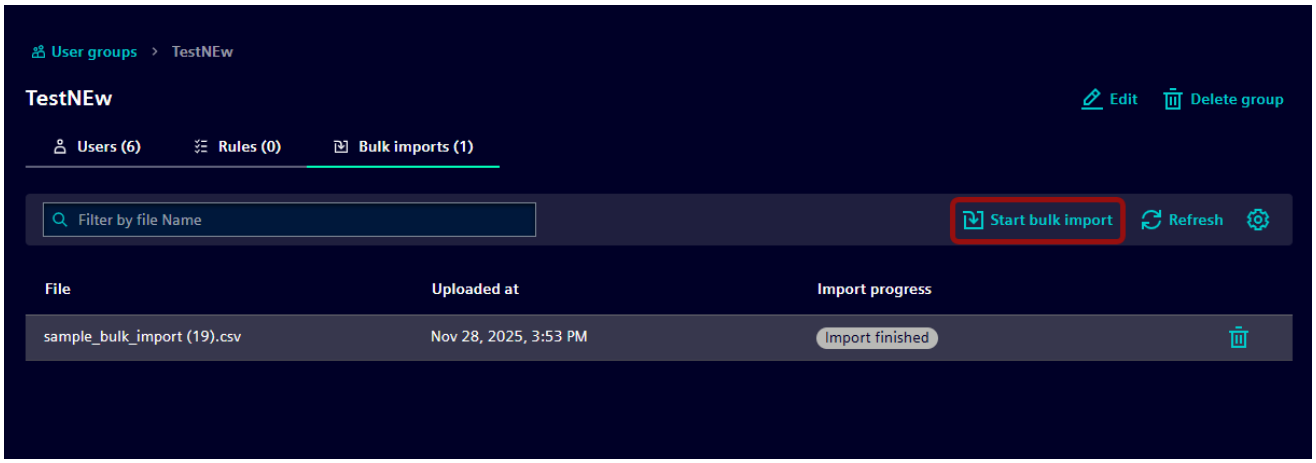
⑩ Provides metadata for each uploaded file:

- **Uploaded at**: Date and time the file was uploaded.
- **Uploaded by**: Name of the user who uploaded the file.

## Import Users

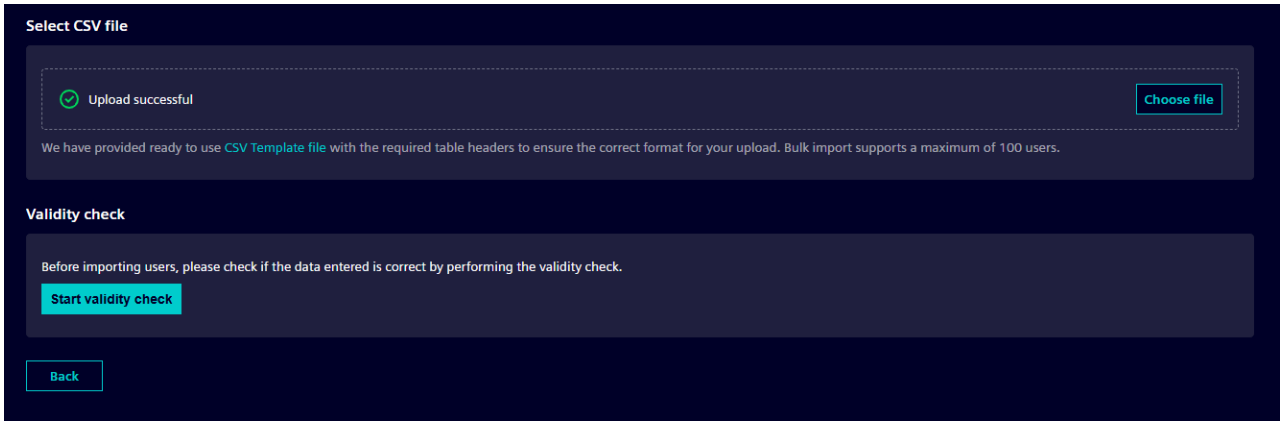
To import bulk users in groups:

1. Go the **Groups** tab in the left navigation pane and select a group.
2. In the **Bulk imports** tab, click **Start bulk import**.

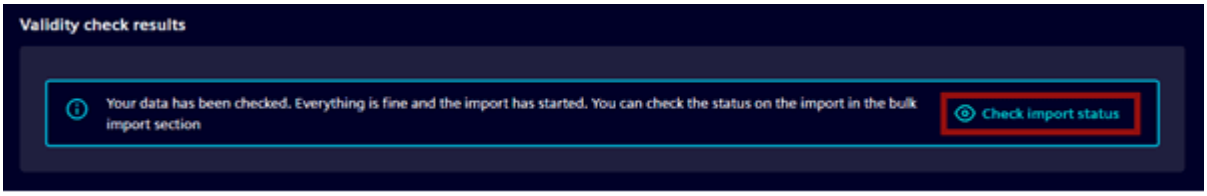



3. In the **Start bulk import** screen:
   - Click **Choose file**, select the CSV file containing user details.
   - Click **Start validity check** to verify the data in the CSV file.

> **Note**
> - The **CSV Template file** link in the **Select CSV file** section provides the default CSV template for download.
> - Duplicate entries in the CSV file are marked as errors during the bulk import process.
> - If the uploaded CSV template file has errors, such as invalid email address or issues related to domain validation, the upload process is flagged as an error.
> - Each CSV file can include up to 100 valid email addresses. The template must include at least one user.




- If **Validity Check** is successful, the bulk import assignment will begin processing.
- Click **Check import status** to view the bulk import overview screen, which details the bulk import assignment triggered for different product tiers and their respective statuses.




- Click **Refresh** to update the list of bulk import jobs.

The bulk import is completed and users are added to the group. Files processed successfully are automatically deleted after 30 days.

## Failed Validity Check

If the **Validity check** fails:

1. In the **Validity check results**, the errors or duplicate entries in the uploaded CSV file are displayed.


2. Fix the errors or duplicate entries in the CSV file and import the CSV file.

**Track Bulk Import Status**:

After completing the bulk import. The "Import progress" column shows the status of the imported CSV file.

The following bulk import statuses:

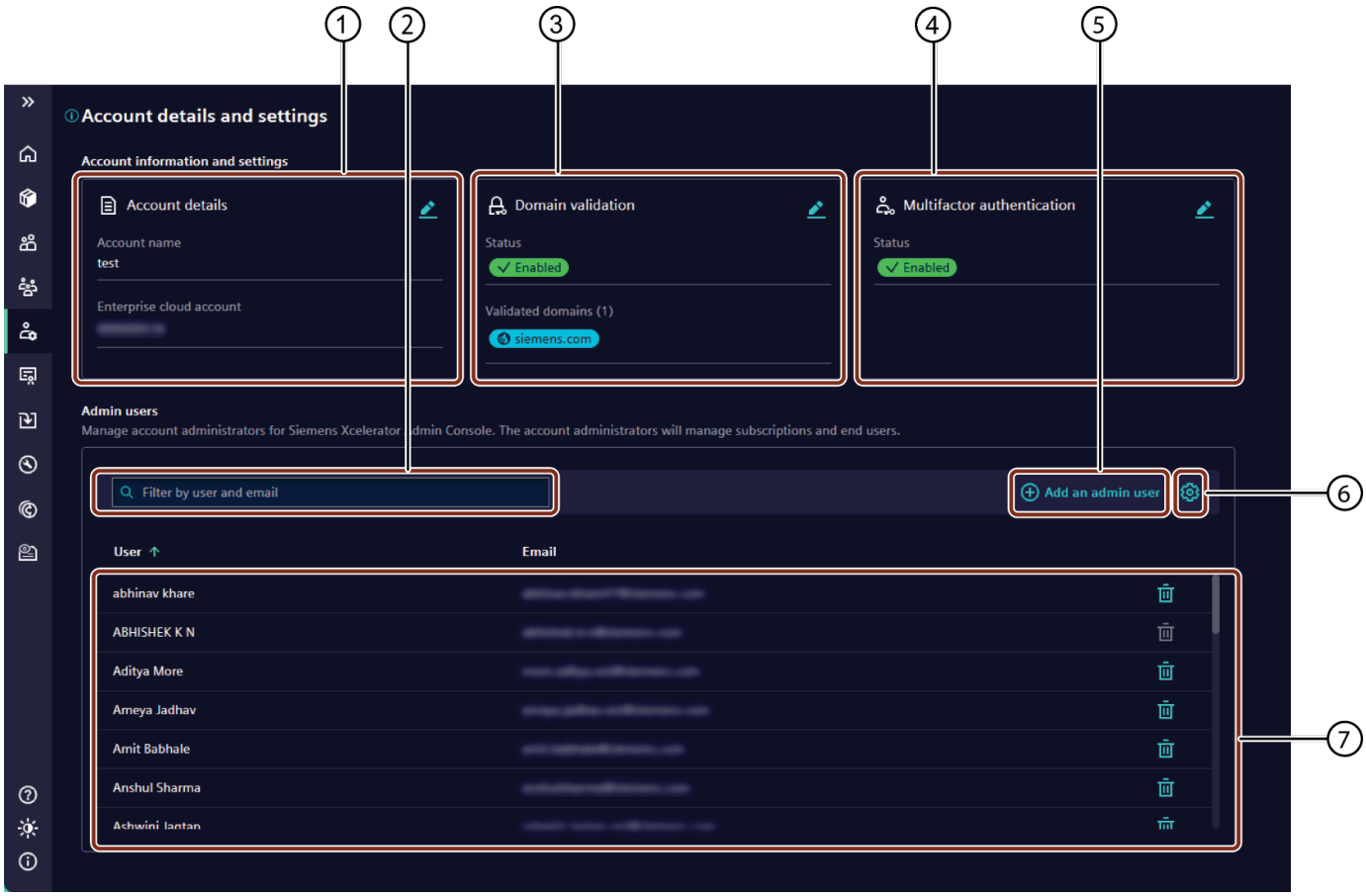
- **Import finished**: All users listed in the file are added to the group.
- **In Progress**: Indicates that users are still being added to the group.

# 4. Configure Security and Authentication

## Account Details and Settings

This section explains how to manage account settings, including editing account information, managing domain validation, and enabling multifactor authentication (MFA).

**Overview of "Account Details and Settings" Screen**:




Allows you to edit specific details for the selected setting

① Displays account details

② Allows you to search for an admin user by username or email

③ Displays domain validation details

④ Displays multifactor authentication details

⑤ Allows you to add an additional admin user

⑥ Allows you to customize the table list to display your preferred columns

⑦ Displays the list of admin users for the selected Enterprise Cloud Account (ECA)

## Account Information and Settings

Account settings include three main settings: Account Details, Domain Validation, and Multifactor Authentication.

## Account Details

Account Details provides information about the configured Enterprise Cloud Account (ECA). It displays the following:

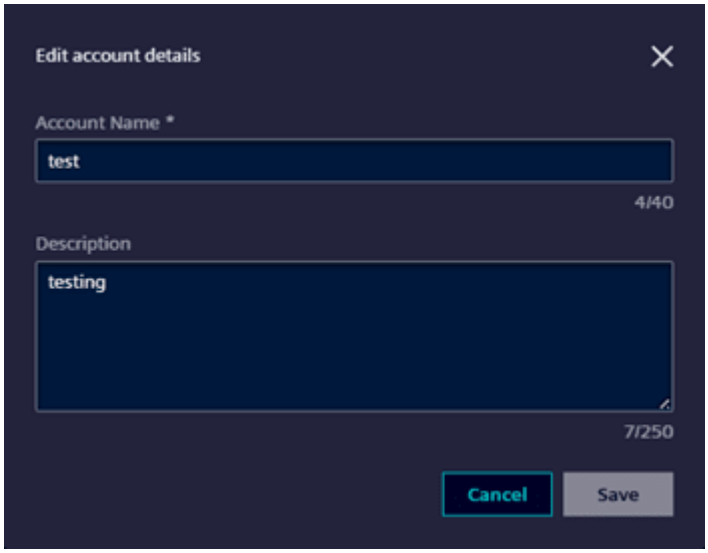
- **Account Name**: The name of the ECA.
- **Enterprise Cloud Account**: The unique ID for the account.
- **Description**: A brief summary or purpose of the account.

### Edit Account Details

To edit the account details settings:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. Go to **Account Settings** in the left navigation pane.
3. Click  icon in the **Account Details** section.
4. In the **Edit account details** pop-up, enter the required fields:

| Parameters | Description |
|---|---|
| Account Name | Enter the name for the ECA. |
| Description | Enter a brief summary or purpose of the account. |




5. Click **Save**.

The edited changes are updated in the account details.

## Domain Validation

Domain validation enhances Siemens Xcelerator Admin Console security, allowing you to control which email domains can access your products by:

- Limiting product access to authorized users from approved domains only.
- Restricting Enterprise Cloud Account (ECA) administrator assignments to validated domains.
- Allowing access to new users only from approved domains.

It displays the following:

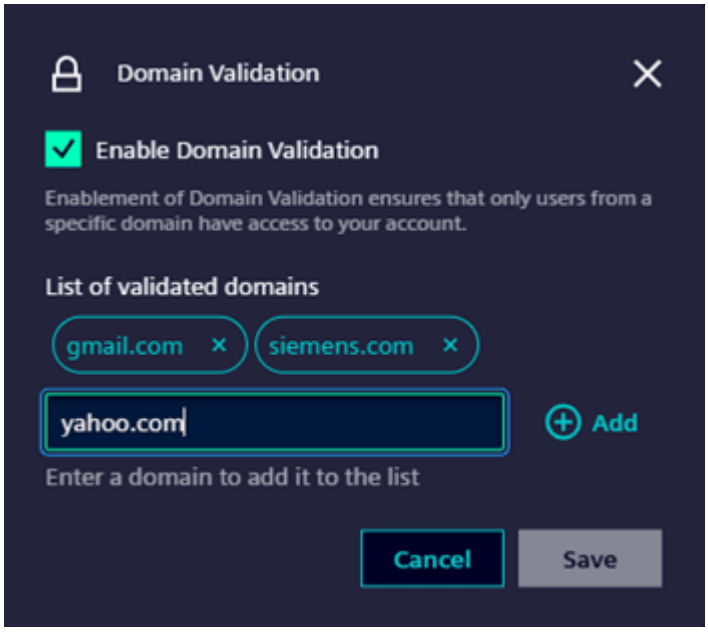
- **Status**: Shows if domain validation is enabled or disabled.
- **Validated Domains**: Shows the domains that are validated.

### Edit Domain Validation

To edit the domain validation settings:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. Go to **Account Settings** in the left navigation pane.
3. Click  icon in the **Domain Validation** section.
4. In the **Domain Validation** pop-up, enter the required field:

- Check or Uncheck **Enable Domain Validation**.
- Enter a domain name.
- Click Add to add it to the list of validated domains.
- Click **Save**.




The edited changes are updated in the domain validation.

## Multifactor Authentication

MultiFactor Authentication (MFA) is a security measure designed to enhance access control and protect sensitive data. Users must provide two or more authentication factors to access the system. MFA strengthens security by adding layers of authentication, protecting Siemens Xcelerator products even if one security factor (such as a password) is compromised.

> **Note**
> MFA works only with Siemens ID. It does not support custom identity providers (IDPs).

It displays the following:

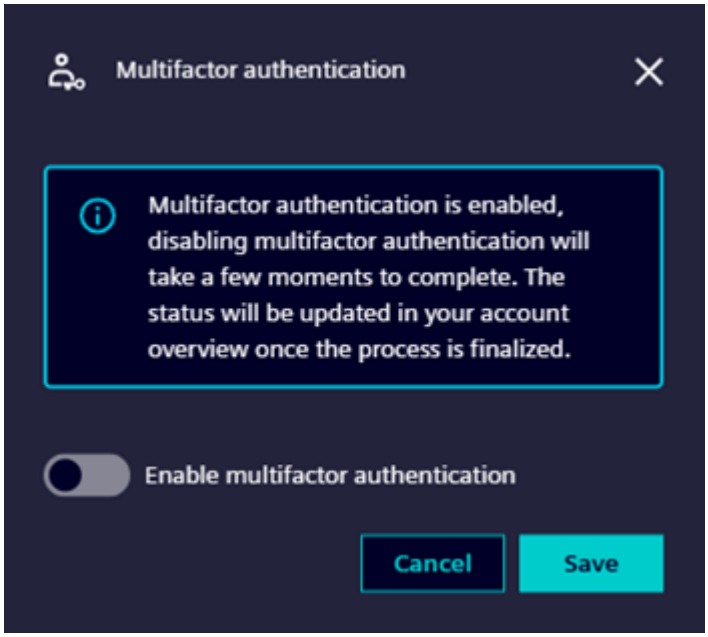
- **Status**: Shows if multifactor authentication is enabled or disabled.

### Edit Multifactor Authentication

To edit multifactor authentication settings:

1. Sign in to **Siemens Xcelerator Admin Console**.

2. Go to **Account Settings** in the left navigation pane.
3. Click  icon in the **Multifactor Authentication** section.
4. In the **Multifactor Authentication** pop-up, click **Enable multifactor authentication** toggle to enable MFA for the ECA.
5. Click **Save**.




The edited changes are updated in the multifactor authentication.

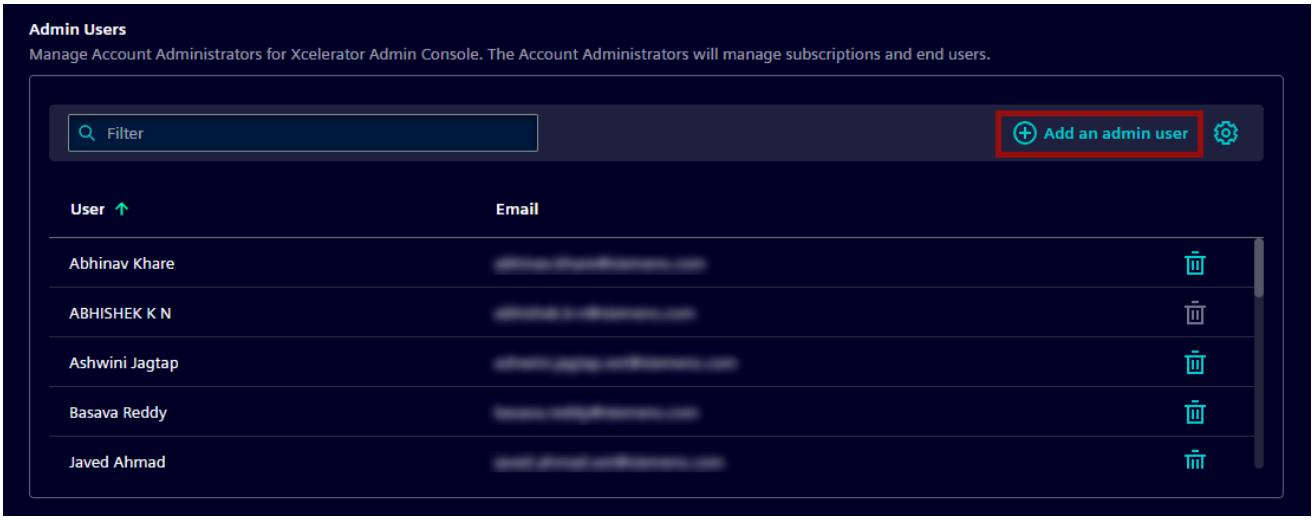
## Manage Additional Administrators

This section explains how to add and remove administrators to manage product subscriptions within an Enterprise Cloud Account (ECA). Add more than one ECA administrator to ensure continuous account management.

## Add an Administrator

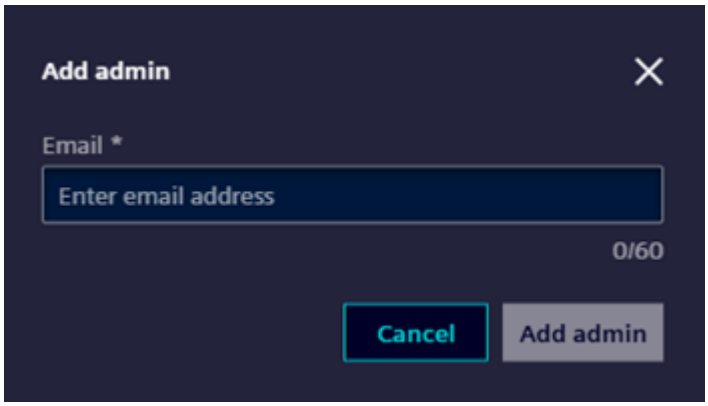
To add an administrator:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. Go to **Account Settings** in the left navigation pane and click **Add an admin user**.




3. In the **Add admin** pop-up, enter the new administrators email address.

> **Note**
>
> If Domain Validation is enabled, users with unsupported domains are not accepted. For more information on validating domains, refer to **Domain Validation**.




4. Click **Add admin**.

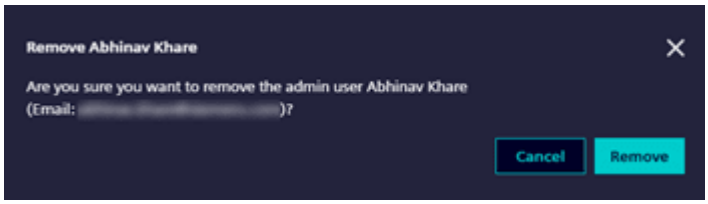
The new administrator is added to the list of administrators for the account.

> **Note**
>
> New administrators receive welcome emails confirming their access as an ECA administrator for that account.

## Remove an Administrator

To remove an administrator:

1. In the **Admin users** section, select the administrators to remove and click icon associated with the user.
2. Click **Remove** to confirm the removal of the user.




The admin user is now removed from the administrator account list.

**Note**

- Administrators cannot remove themselves. Request removal from another administrator if needed.
- Removed administrators receive notification emails confirming that they no longer have administrative access to the ECA.

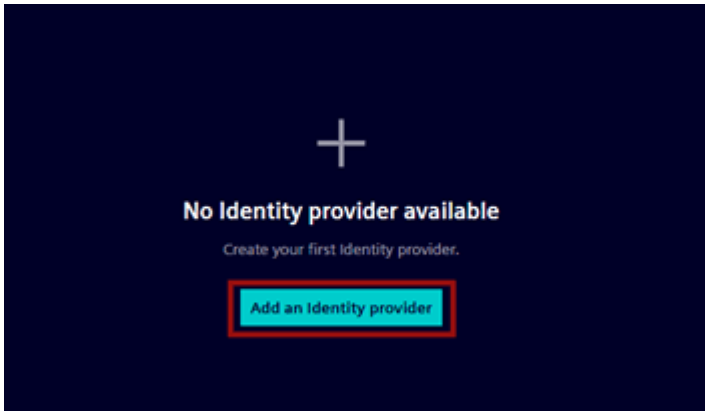
# Identity Provider

Identity Provider (IdP) is a centralized system that manages user authentication and control access within an ecosystem. It provides a secure solution for user authentication and access authorization to various applications and services.

## Add an Identity provider

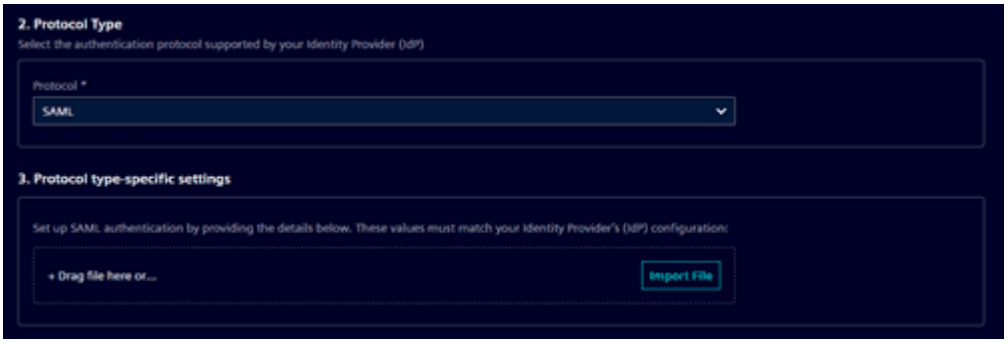
To add an identity provider to the Siemens Xcelerator Admin Console, follow these steps:

1. Sign in to the **Siemens Xcelerator Admin Console**.
2. In the left navigation pane, click **Identity provider** tab.
3. Click **Add an Identity provider** or click Add.




4. In the **Add new Identity Provider** screen:
   - In the **General** section:
     - Enter a unique name, which acts as the key identifier for the identity provider.
     - Enter the display name.
       *(uppercase letters are not allowed)*
     - Enter a description of the identity provider.
     - Enter the logout URL.


   - In the **Protocol Type** section:
     - Select the required protocol type from the drop-down menu.
     - For **SAML** Protocol Type:
       - Choose and upload an XML configuration file for the identity provider.




- For **OIDC 1.0** Protocol Type:
  - Enter the **Client ID**.
  - Enter the **Client Secret**.
  - Enter the **Issuer URL**.


- Click **Add identity provider**.

**Note**

- The IdP status initially displays as "Creating". Click **Refresh** to update the current status.
- Creating a new OAuth IdP is not supported, use the existing IdP created under version 1.0.
- For successful SAML Identity Provider activation, it's crucial to use a distinct SAML metadata file for each IdP. Reusing a metadata file across different IdPs is not supported within the ECA boundary.

## Identity Provider Configuration Updates

Depending on the region and product, and whether the Identity Provider uses OIDC or SAML, specific callback URLs and identifiers must be configured within the chosen IdP. For instance, if you are using Microsoft Entra, these settings would be applied directly in its configuration.

**Regional Callback URLs & SAML Identifiers**:

**US Region**:

```
```
        Callback URL:
            - "https://default.us1.sws.siemens.com/saml/SSO/alias/
default.us1.sws.siemens.com"
            - "https://<<ECA ID>>.us1.sws.siemens.com/saml/SSO/alias/<<ECA
ID>>.us1.sws.siemens.com"
            - "https://<<ECA ID>>.ciam.us1.sws.siemens.com/saml/SSO/alias/
<<ECA ID>>.ciam.us1.sws.siemens.com"
            - "https://samauth.us-east-1.sws.siemens.com/interaction/
callback"

        SAML Identifiers (Entity ID for SAML based IdP):
            - default.us1.sws.siemens.com
            - urn:sam:auth-useast1
            - <<ECA ID>>.us1.sws.siemens.com
            - <<ECA ID>>.ciam.us1.sws.siemens.com
    ```
```

**EU Region:**

```
```
        Callback URL:
            - "https://default.us1.sws.siemens.com/saml/SSO/alias/
default.us1.sws.siemens.com"
            - "https://<<ECA ID>>.eu1.sws.siemens.com/saml/SSO/alias/<<ECA
ID>>.eu1.sws.siemens.com"
            - "https://<<ECA ID>>.ciam.eu1.sws.siemens.com/saml/SSO/alias/
<<ECA ID>>.ciam.eu1.sws.siemens.com"
            - "https://samauth.us-east-1.sws.siemens.com/interaction/
callback"

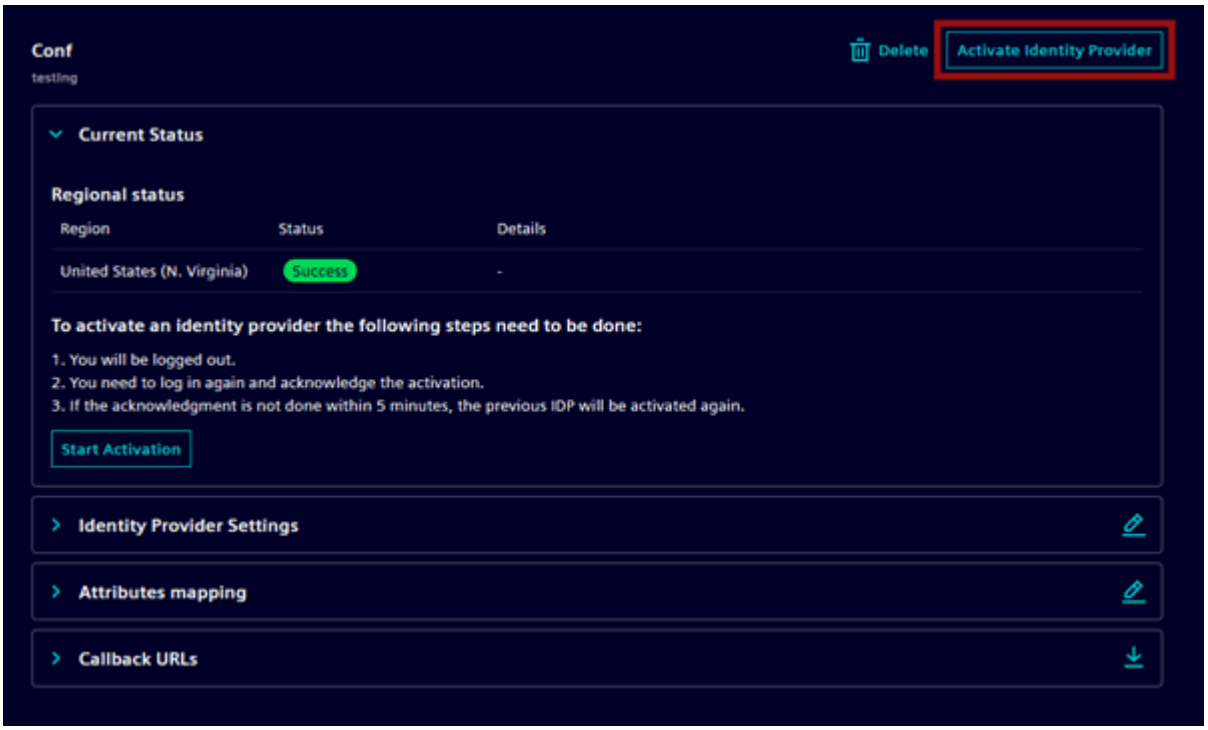
        SAML Identifiers (Entity ID for SAML based IdP):
            - default.us1.sws.siemens.com
            - urn:sam:auth-useast1
            - <<ECA ID>>.eu1.sws.siemens.com
            - <<ECA ID>>.ciam.eu1.sws.siemens.com
    ```
```

**AP Region:**

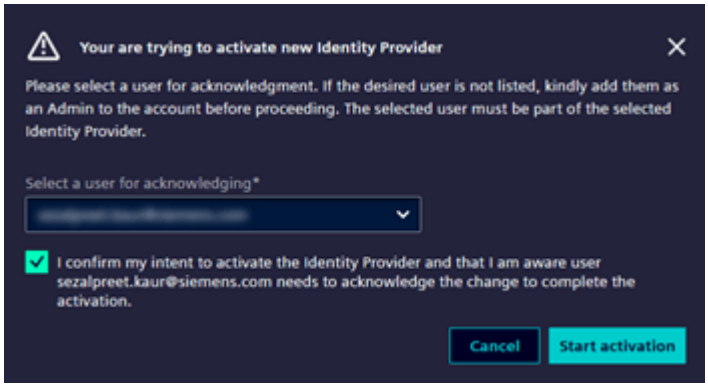
```
```
        Callback URL:
            - "https://default.us1.sws.siemens.com/saml/SSO/alias/
default.us1.sws.siemens.com"
            - "https://<<ECA ID>>.ap1.sws.siemens.com/saml/SSO/alias/<<ECA
ID>>.ap1.sws.siemens.com"
            - "https://<<ECA ID>>.ciam.ap1.sws.siemens.com/saml/SSO/alias/
```
```

```
<<ECA ID>>.ciam.ap1.sws.siemens.com"
            - "https://samauth.us-east-1.sws.siemens.com/interaction/
callback"

        SAML Identifiers (Entity ID for SAML based IdP):
            - default.us1.sws.siemens.com
            - urn:sam:auth-useast1
            - <<ECA ID>>.ap1.sws.siemens.com
            - <<ECA ID>>.ciam.ap1.sws.siemens.com
    ```
```

**CN Region:**

```
```
        Callback URL:
            - "https://default.us1.sws.siemens.com/saml/SSO/alias/
default.us1.sws.siemens.com"
            - "https://<<ECA ID>>.cn1.sws.siemens.com/saml/SSO/alias/<<ECA
ID>>.cn1.sws.siemens.com"
            - "https://<<ECA ID>>.ciam.cn1.sws.siemens.com/saml/SSO/alias/
<<ECA ID>>.ciam.cn1.sws.siemens.com"
            - "https://samauth.us-east-1.sws.siemens.com/interaction/
callback"

        SAML Identifiers (Entity ID for SAML based IdP):
            - default.us1.sws.siemens.com
            - urn:sam:auth-useast1
            - <<ECA ID>>.cn1.sws.siemens.com
            - <<ECA ID>>.ciam.cn1.sws.siemens.com
    ```
```

**Note**

- For the FDS Admin Console, which is hosted in the US region, ECA administrator authentication is processed accordingly in the US.
- To ensure seamless authentication flow, the Identity Provider must be configured with the US callback URL.
- We want to emphasize that while this specific authentication step occurs in the US, all product and user provisioning, as well as product data, are entirely hosted and operated within the respective region (e.g., EU products stay in the EU).
- For non-US products, no product data is migrated or processed in the US; the US callback is exclusively for authenticating ECA administrators for Admin Console access.

## Activate an Identity provider

To activate an identity provider:

1. Select the IdP which you want to activate.
```

2. Click **Activate Identity Provider** or click **Start Activation** in the "Current Status" section.




3. In the pop-up, select a user to acknowledge and click **Start activation**.




**Note**

- This action logs out your current session and requires you to sign-in again to the Siemens Xcelerator Admin Console.
- If Domain Validation is enabled, only users from validated domains are listed for acknowledgment.

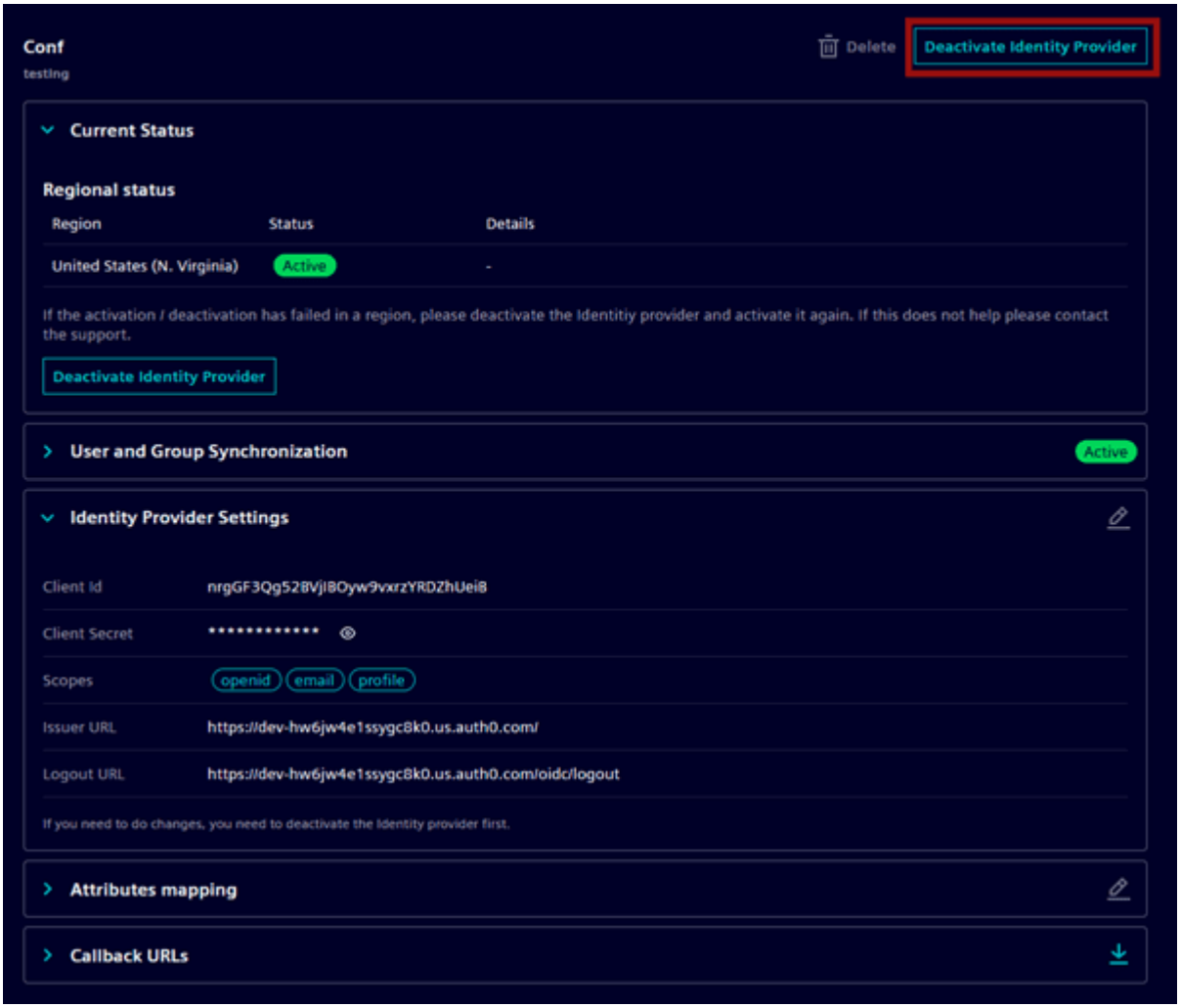
4. After logging in again, click **Accept** to acknowledge the IdP activation.
5. A confirmation pop-up appears when the IdP activation is successful.

The selected identity provider is now activated.

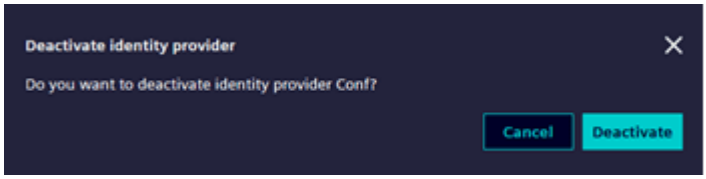
## Deactivate an Identity Provider

To deactivate an identity provider:

1. Select the identity provider you want to deactivate.
2. Click **Deactivate Identity Provider** or click **Deactivate Identity Provider** in the "Current Status" section.




3. In the **Deactivate identity provider** pop-up, click **Deactivate**.

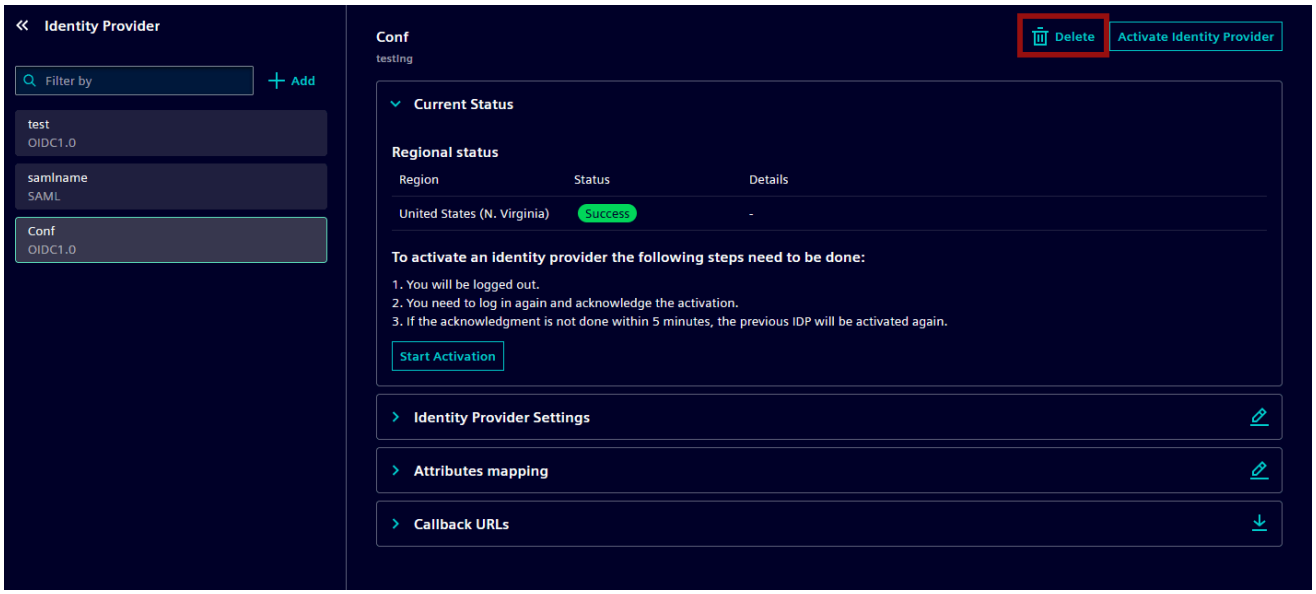



The selected identity provider is now deactivated.

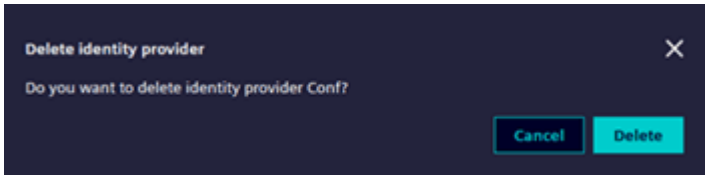
## Delete an Identity provider

To delete an identity provider:

1. Select the identity provider to delete.
2. Click **Delete** button associated with the identity provider.




3. In the **Delete identity provider** pop-up, click **Delete**.




The selected identity provider is now deleted from the Siemens Xcelerator Admin Console.

## Security capabilities

A secure way to integrate with a third-party Identity provider (IdP) is provided using standard protocols and frameworks. If a custom IdP (identity provider) is used instead of our standard IdP solution, the customer assumes responsibility for the secure operation and management of the chosen IdP, including physical security, the host operating system and virtualization layer, the guest operating system (including updates and security patches), and network configuration, in accordance with **ISO 27001**.

It is required to change the password regularly. For Tenant administrators, using Multi-Factor Authentication (MFA) is recommended.

# 5. Automate User Management

## Manage Groups and User Synchronization

The Siemens Xcelerator Admin Console supports synchronization of groups and users from a custom identity provider (IdP). Customers can also create groups manually, allowing them to organize account users within the tenant.

There are two types of groups:

**Synced Groups**: For synced groups, customers must activate a custom identity provider (IdP), generate authentication credentials, and trigger a sync job from the respective custom IdP.

**Manual Groups**: You can create groups in regions where the products in the Enterprise Cloud Account (ECA) are provisioned. You can select your preferred region to create or sync groups.

**Prerequisites**:

You need at least one provisioned product in the Enterprise Cloud Account (ECA).

### Create an Auth Client and Synchronize Groups

Customers can synchronize groups when using their own identity provider (IdP) for authentication, allowing them to manage users and groups through the IdP. If a customer already has a group, they can synchronize it to display all users within the group in the system.

**Note**

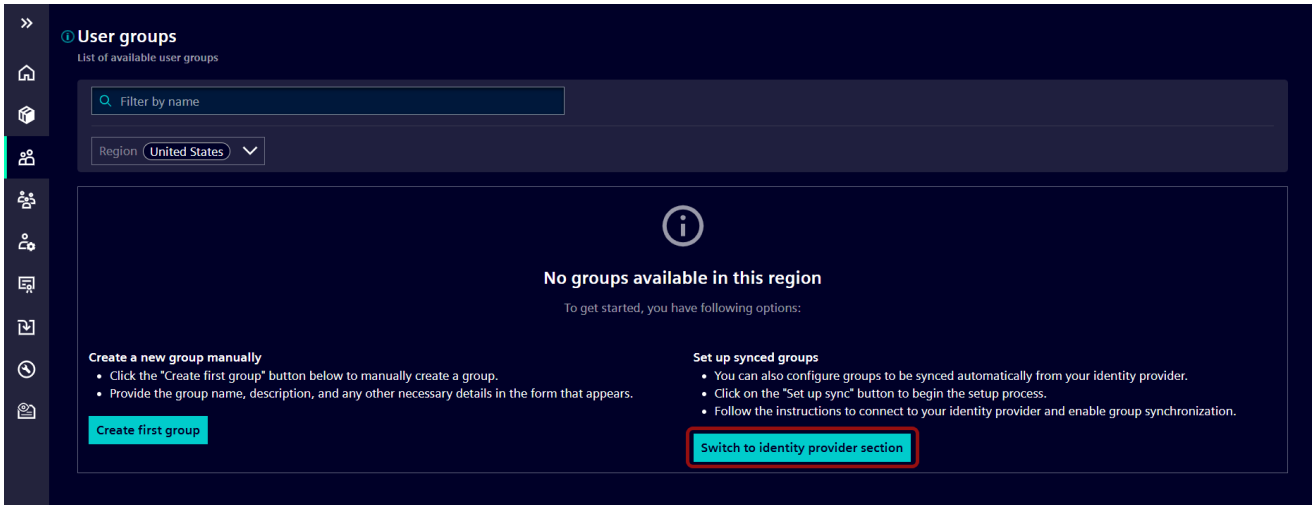
- You cannot edit or delete synced groups in the Siemens Xcelerator Admin Console.
- You cannot add or remove users from synced groups in the Siemens Xcelerator Admin Console.

**Prerequisites**:

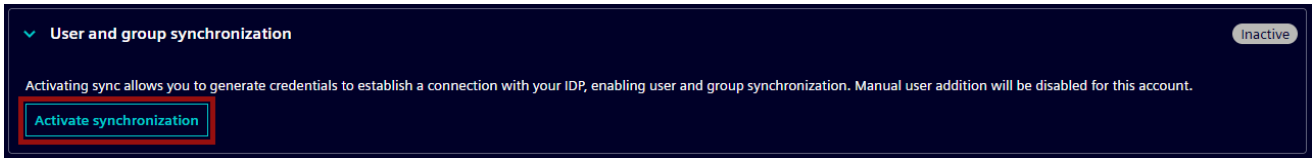
An Auth client is required to enable synchronization.

To create an Auth client and synchronize groups:

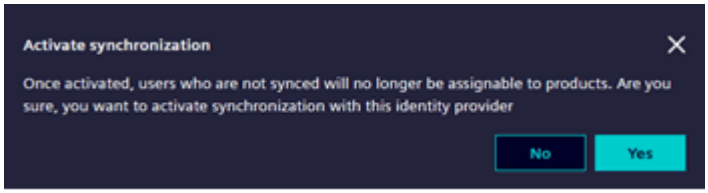
1. Go to the **Groups** tab in the left navigation pane and click **Switch to identity provider section**.




2. Select the IdP marked with the "Active" badge.
3. In the **User and group synchronization** section, click **Activate synchronization**.



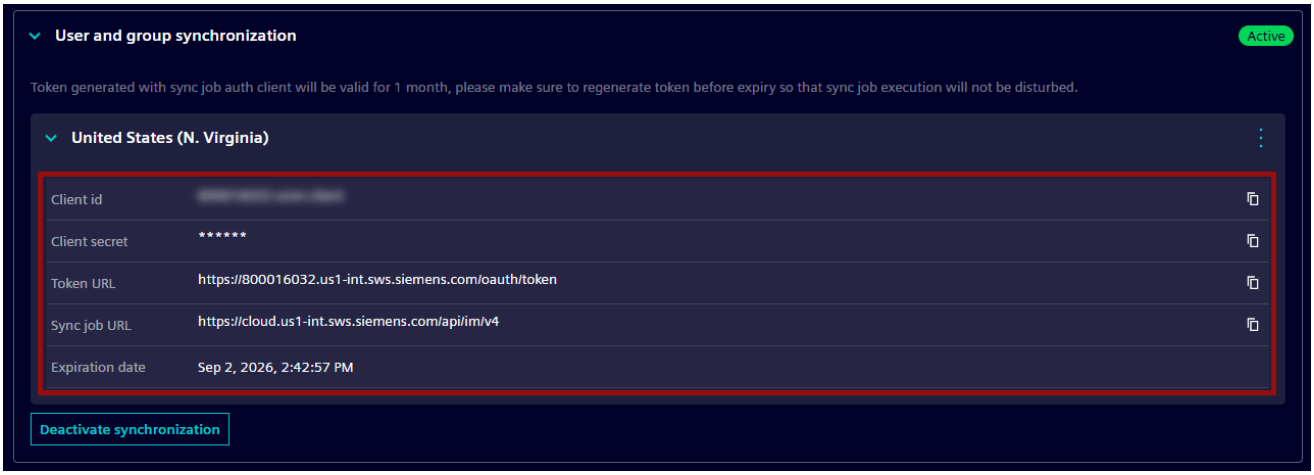

4. In the **Activate synchronization** pop-up, click **Yes**.




> **Note**
>
> When you activate the sync, you cannot add new users to the product. You can only choose from existing users. To add new users who are not part of your identity provider, you must deactivate the sync.

5. The user and group synchronization is now activated.
6. Now in the **User and group synchronization** section, click **Add auth client**.


7. After creation, the Auth client is available for use.




**Note**

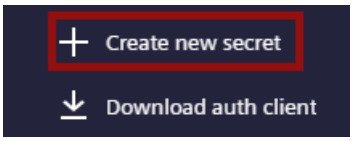
- You can download the Auth client properties. Then, set them up in the custom IdP to start synchronization. Groups that sync through this process will get the **EXT** badge. This indicates that they are synced groups in the Groups list.
- You cannot create a new user in these synced groups. You can only view the synced users.

## Create New Secret (Secret Rotation)

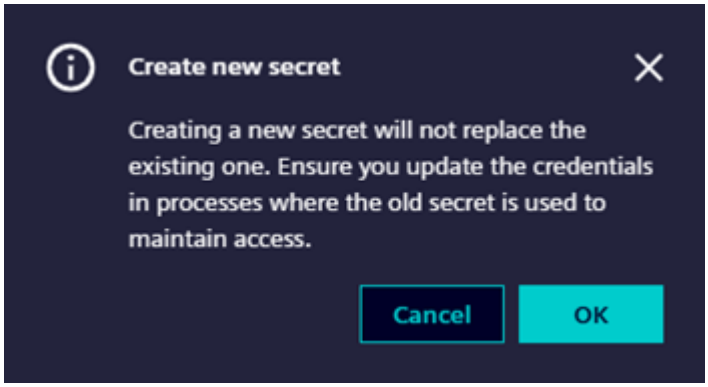
Secret rotation is a security practice that involves periodically updating user credentials (secrets) to maintain system security and prevent unauthorized access. This process ensures that expired credentials are properly replaced while maintaining application functionality and preventing service disruptions.

To create a new secret:

1. Select the identity provider for which you want to create a new secret.
2. In the **User and group synchronization** section, click ⋮ and select **Create new secret**.



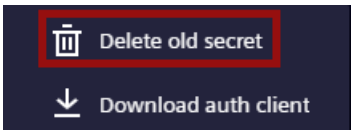

3. In the **Create new secret** pop-up, click **OK**.



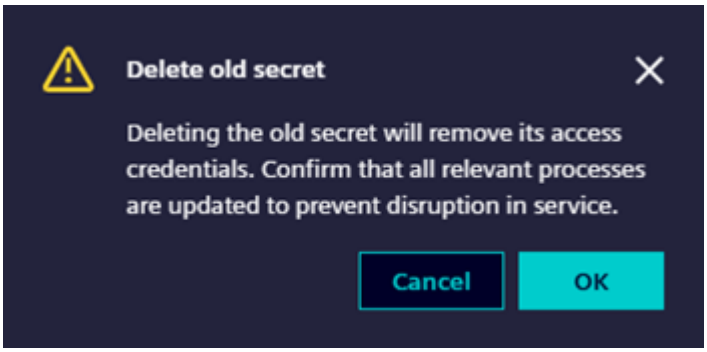

4. A new secret is generated.

> **Note**
> - Use the new secret in your application.
> - Verify there are no disruptions in service.
> - Do not delete the old secret until you have verified the new secret is working properly.
> - Deleting an existing secret before proper replacement and verification may disrupt application functionality.

5. Once you have confirmed everything is working properly with the new secret:
   - In the **User and group synchronization** section, click ⋮ and select **Delete old secret**.




   - In the **Delete old secret** pop-up, click **OK**.

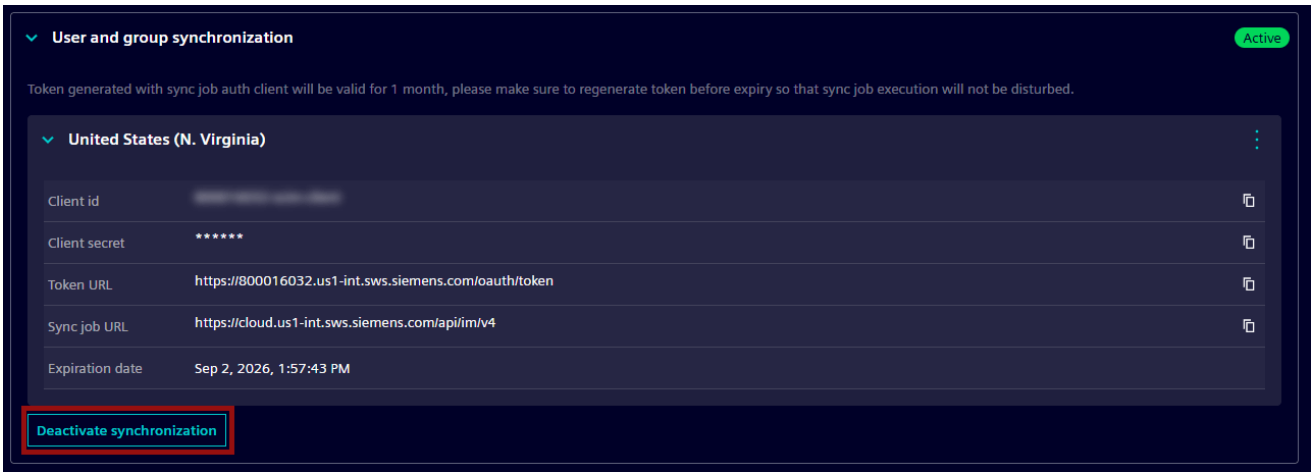



   - The old secret ID is deleted.

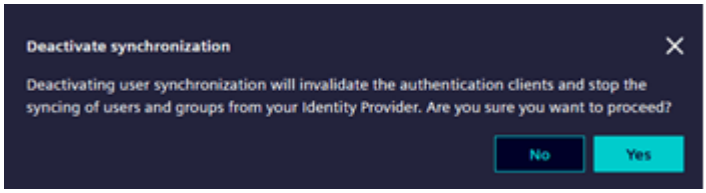
## Deactivate Synchronization

To deactivate group synchronization:

1. In the **User and group synchronization** section, click **Deactivate synchronization**.




2. In the **Deactivate synchronization** pop-up, click **Yes**.




**Note**

- Deactivating synchronization removes the Auth client and the credentials will become invalid.
- If the IdP is deactivated, the auth client properties will also be deleted, making the credentials invalid.

The user and group synchronization is now deactivated.

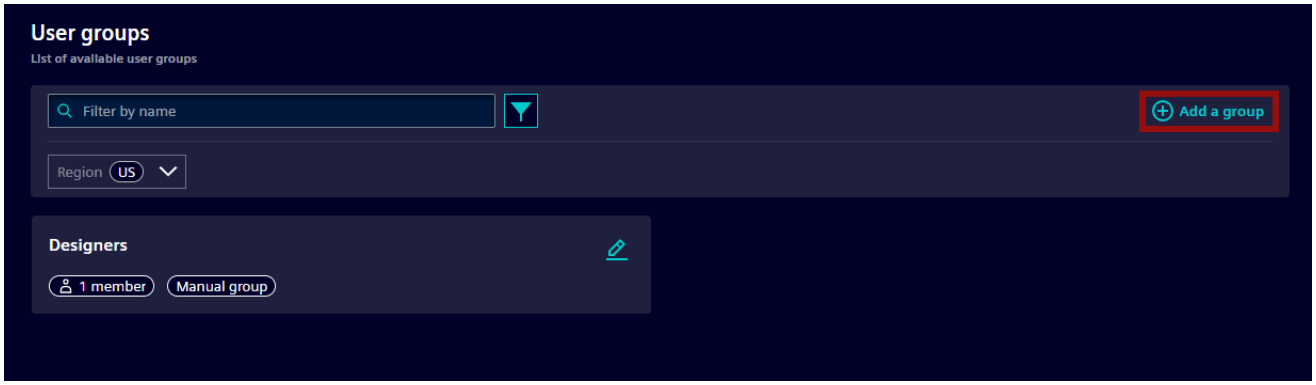
## Manual Groups

Manual groups are created and managed directly in the Siemens Xcelerator Admin Console, only in regions where products are provisioned.

## Create a New Group Manually

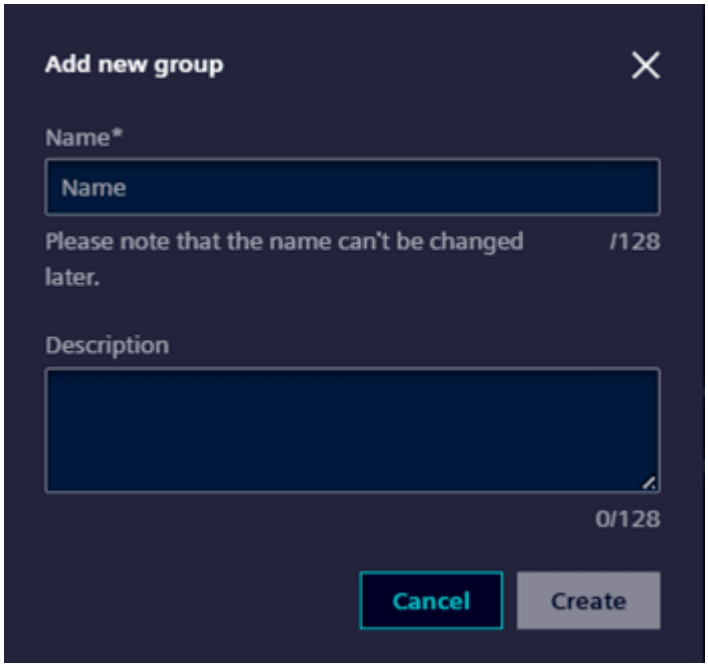
To create a new group manually:

1. Click **Add a group**.




2. In the **Add new group** pop-up, enter the required fields:

| Attribute Name | Description |
|---|---|
| Name | Enter the group name. |
| Description | Enter a brief description of the group(optional). |




3. Click **Create**.

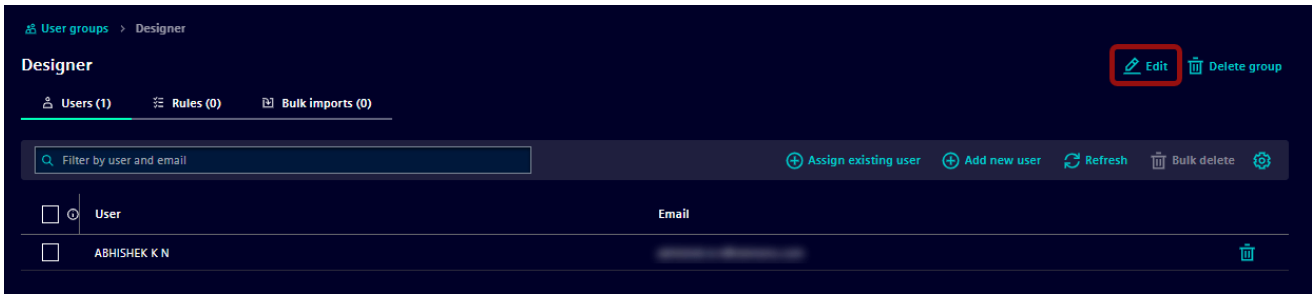
The new group is successfully created.

## Edit a Group Description

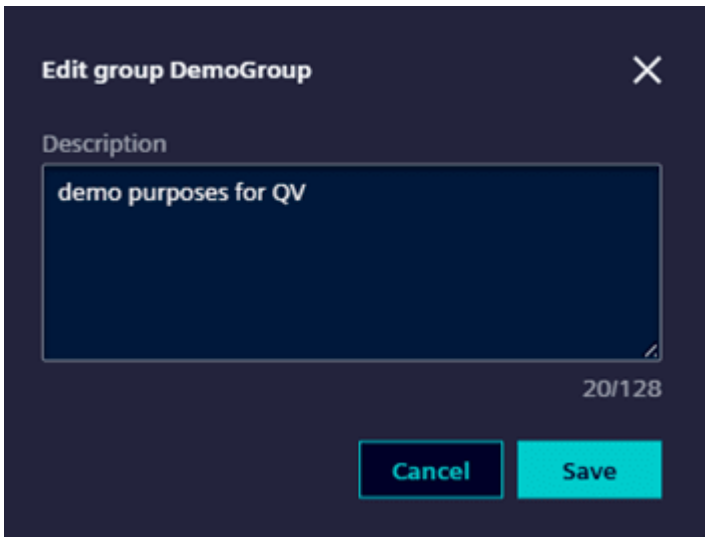
Editing a group description allows you to add or update the existing description of the group.

To edit a group description:

1. Click **Edit**.




2. In the **Edit group** pop-up, add or update the description.



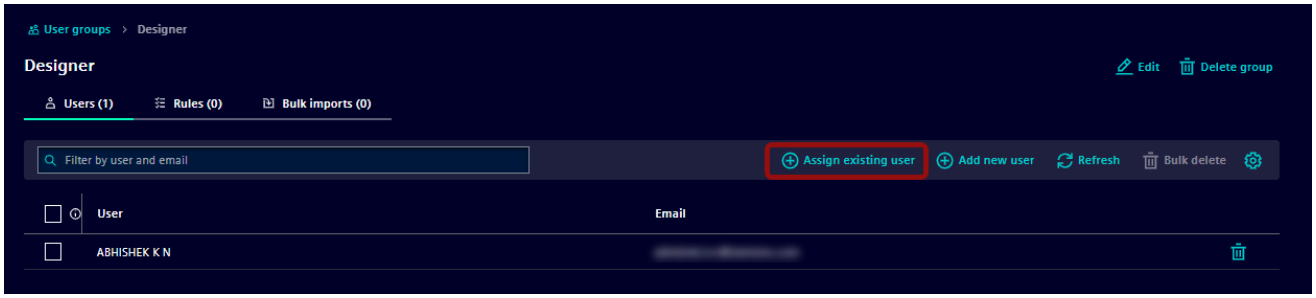

3. Click **Save**.

The group description is updated.

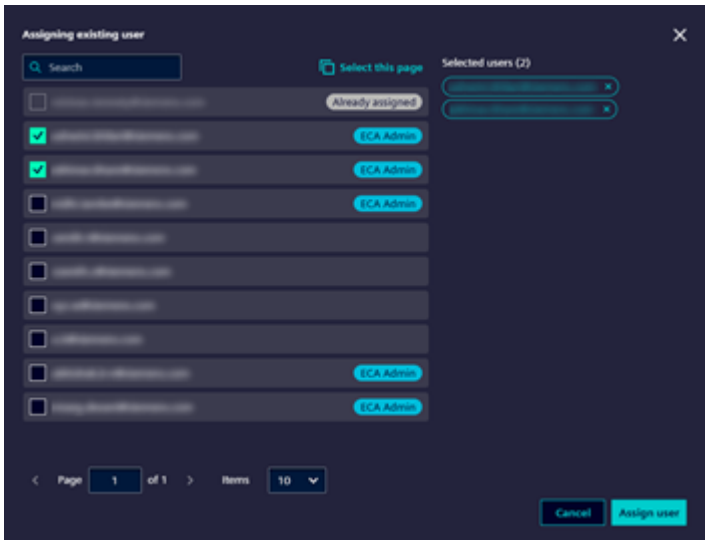
## Add Existing Users to a Group

To add existing users to a group:

1. Click **Assign existing user**.



2. In the **Assign existing user** pop-up, select users from the available user list and click **Assign user**.




> **Note**
> You can select up to 20 users at once.

3. Click **Check status**, to monitor user assignment progress.


This displays the status of the list of users being added to the group:

- **In Progress**: The process of adding the user to the group is ongoing.
- **Failed**: The process of adding the user to the group was unsuccessful.

4. In the **Failed and pending users** screen, click **Refresh** to update the group user list.

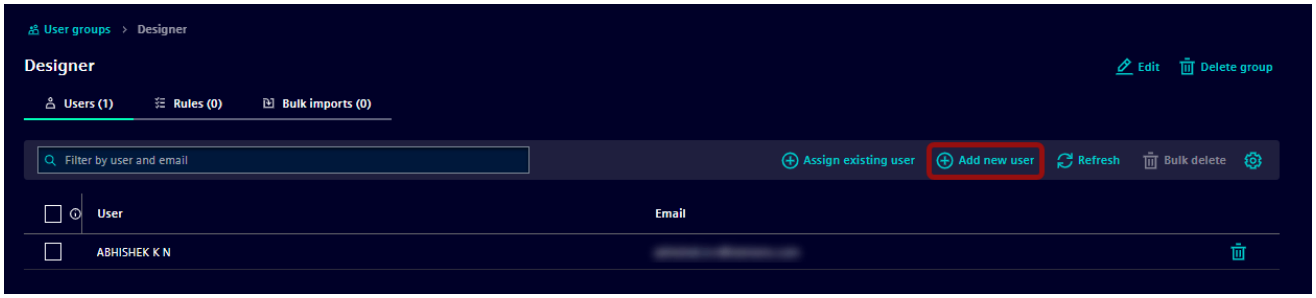
The existing users are assigned to the group.

> **Note**
> Users who were not added remain in the failed user list. Click **Dismiss list** to remove failed entries from the list view.

## Add a New User to the Group

To add a new user to the group:

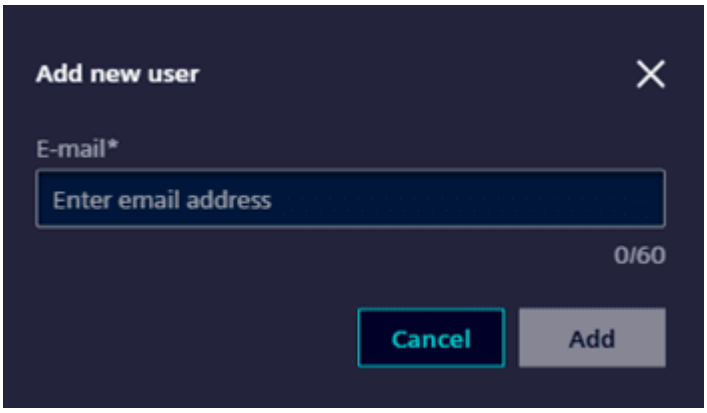
1. Click **Add new user**.




2. In the **Add new user** pop-up:
   - Enter a valid email address of the user.
   - Click **Add**.

   **Note**

   If Domain Validation is enabled, only approved domains are accepted. For more information on validating domain, refer to **Multi-Factor Authentication and Domain Validation.**




The new user is added to the group.

**Note**

- If synchronization is active, the **Add new user** option is disabled.
- Users who are ECA admins are tagged with the "ECA Admin" badge.
- Bulk user import is available only for manual groups.

## Remove Users from a Group

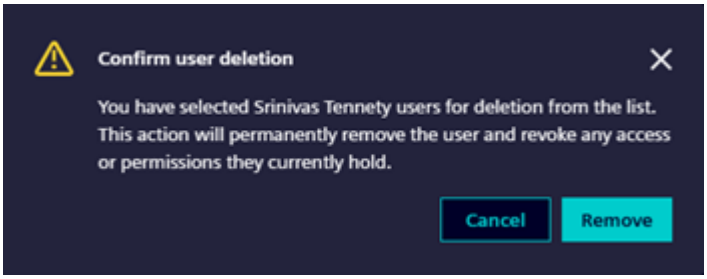
To remove a user from a group:

**Note**

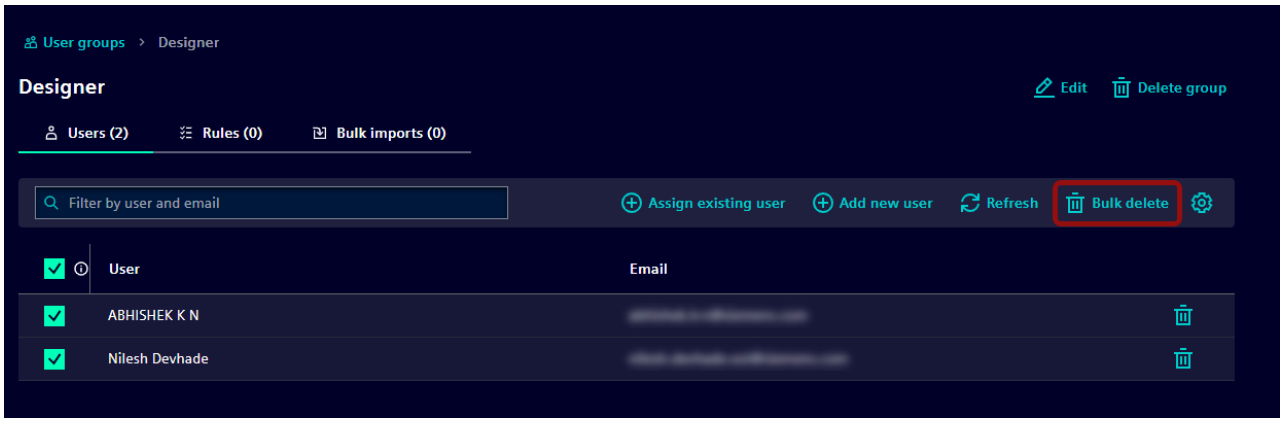
You can select up to 20 users for bulk deletion.

1. Select the user or multiple users to remove from the users list.

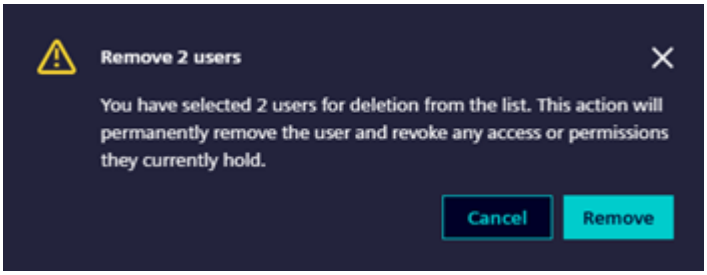
   - For single user, click  icon associated with the user.
     - In the **Confirm user deletion** pop-up, click **Remove**.




   - For multiple users, click **Bulk delete**.




     - In the **Remove users** pop-up, click **Remove**.




The user is removed from the group.

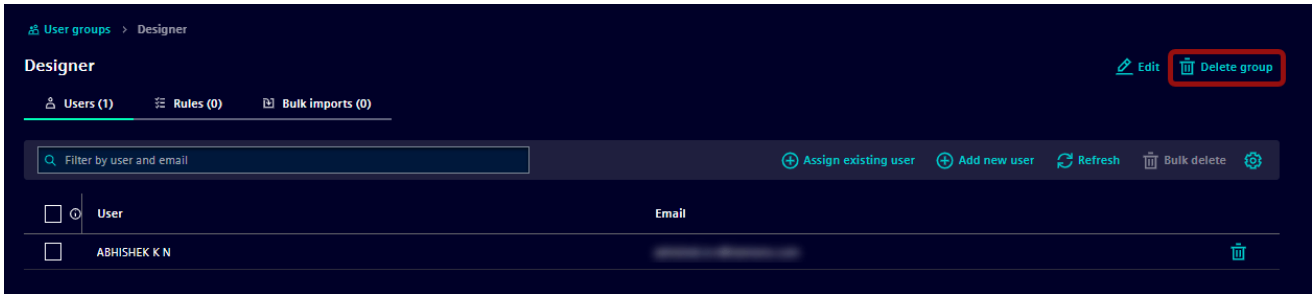
## Delete a Group

To delete a group:

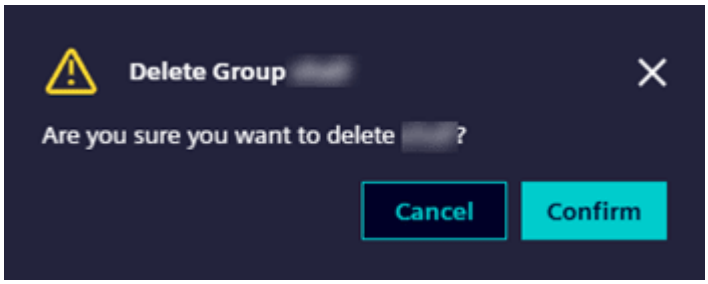
**Note**

Group cannot be deleted if it has active rules associated with it. You have to deactivate the associated rules first.

1. Select the group in the **Groups** list.
2. In the selected group screen, click **Delete group**.




3. In the **Delete Group** pop-up, click **Confirm**.




The group is deleted.

## Automate User Assignment in Rules

The Rules feature allows Enterprise Cloud Account (ECA) administrators to automatically assign users to products based on predefined rules. This eliminates the need for manual user assignments.

When a rule is active, any new user added to the group is automatically assigned to the specified product.

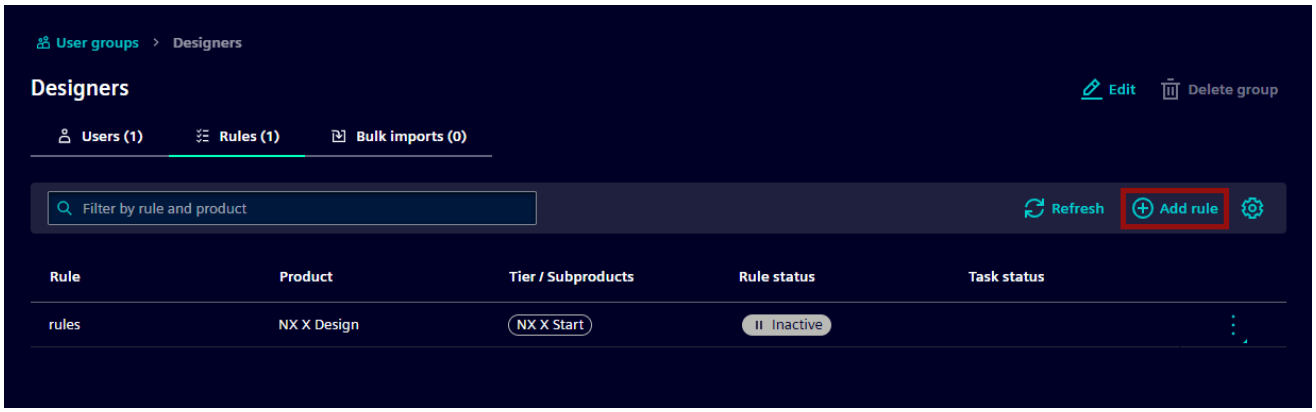
**Note**

The system pauses rules when all available slots are occupied. This prevents new assignments when no slots are available. When additional slots are purchased, the system automatically reactivates and auto plays rules in 24 hours. Alternatively, the administrator can manually restart the rules once the license is restored.

## Create a Rule

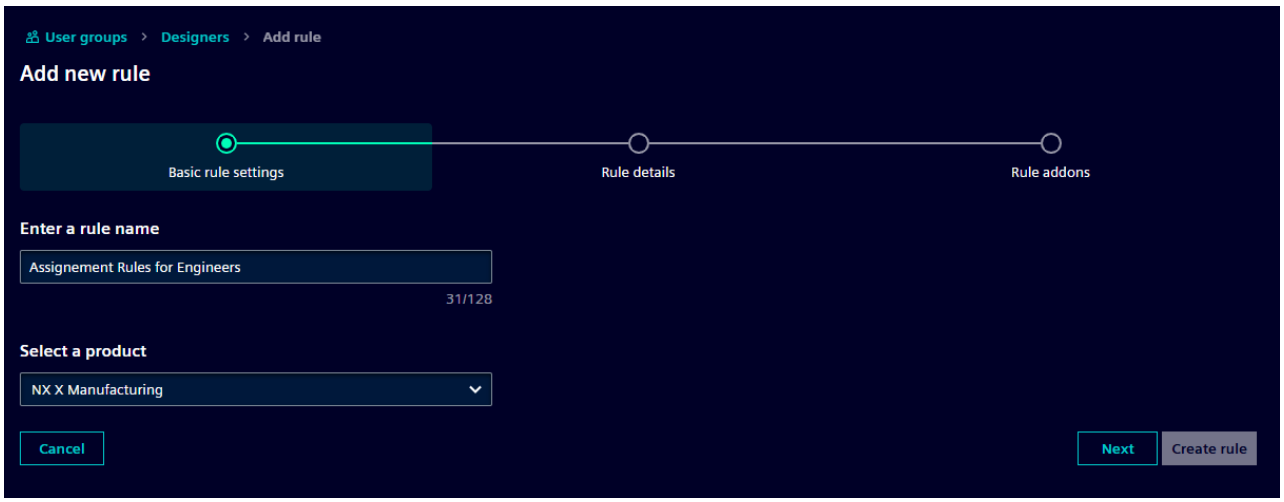
To create a rule:

1. Go to the **Groups** page in the left navigation pane and select the group to add the rule.
2. In the **Rules** tab, click **Add rule**.



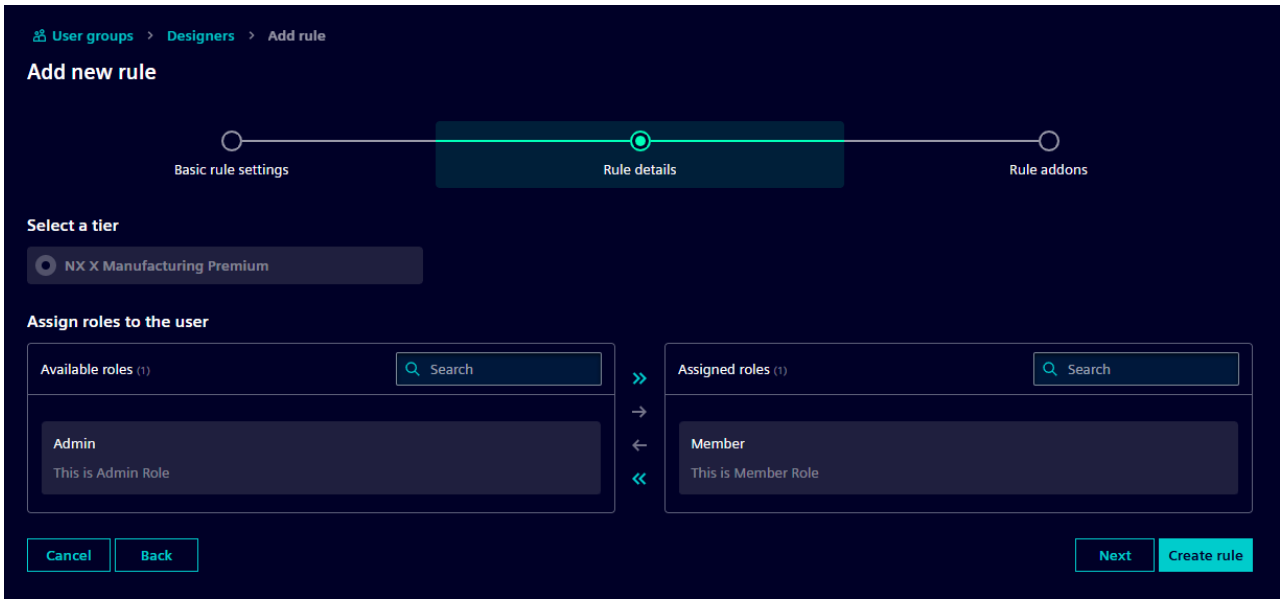

3. In the **Basic rule settings** tab:
   - Enter the name of the rule.
   - Select the product.

> **Note**
> - You can select only products that are already configured.
> - If the selected product includes Teamcenter Share, you must select the region. If you do not set the region, provisioning fails for all users assigned through this rule. For more information on selecting the region, refer to **Assign a User**.




   - Click **Next**.

4. In the **Rule details** tab:
   - Select the tier.
   - Select roles from the "Available roles" list and click →. To assign all roles, click ».
   - If the product supports environments: Select environments from the "Available environments" and click →. To assign all environments, click ».




5. Click **Next**, if your product supports add-ons.
   - In the **Rule addons** tab:
   - Select addons from the "Available addons" list and click →. To assign all add-ons, click ».


6. Click **Create rule**.

The rule is now created.

## Start Assignment for a Rule

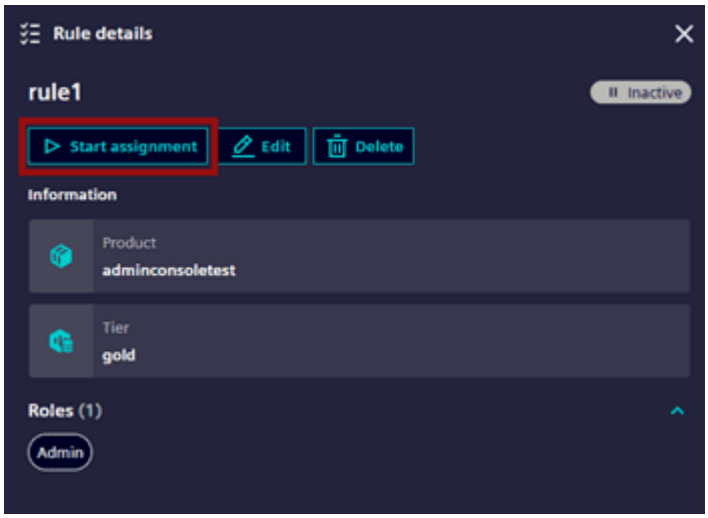
Starting an assignment for a rule assigns all users in the group to the product specified in the rule. When a new user is added to the group, all active rules are applied, and the user is automatically assigned to the products specified in those active rules.

**Note**

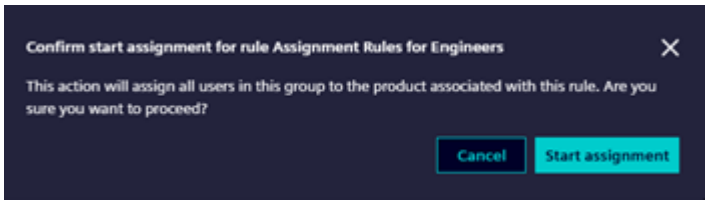
- The rule does not apply to users who already have access to the product.
- The new configuration does not override existing assignments with the new configuration.

To start the assignment:

1. Select the rule to start assignment.
2. In the **Rule details** screen, click **Start assignment**.




3. In the **Confirm start assignment** pop-up, click **Start assignment**.




The rule is now active.

**Note**

- If the group has no users, provisioning will not proceed to entitlement, and the status will show as **Activity in Progress**.

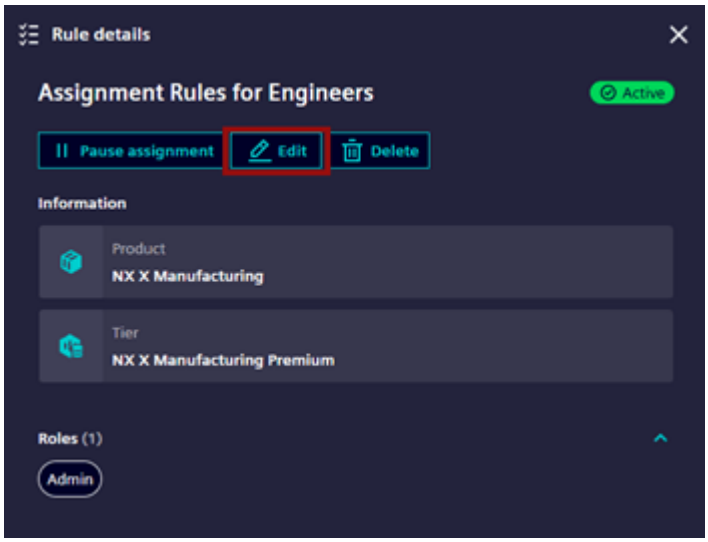
- When users are added to a group with existing users, the sync operation takes some time. When the sync is complete, the status changes to **Active**.

## Edit a Rule

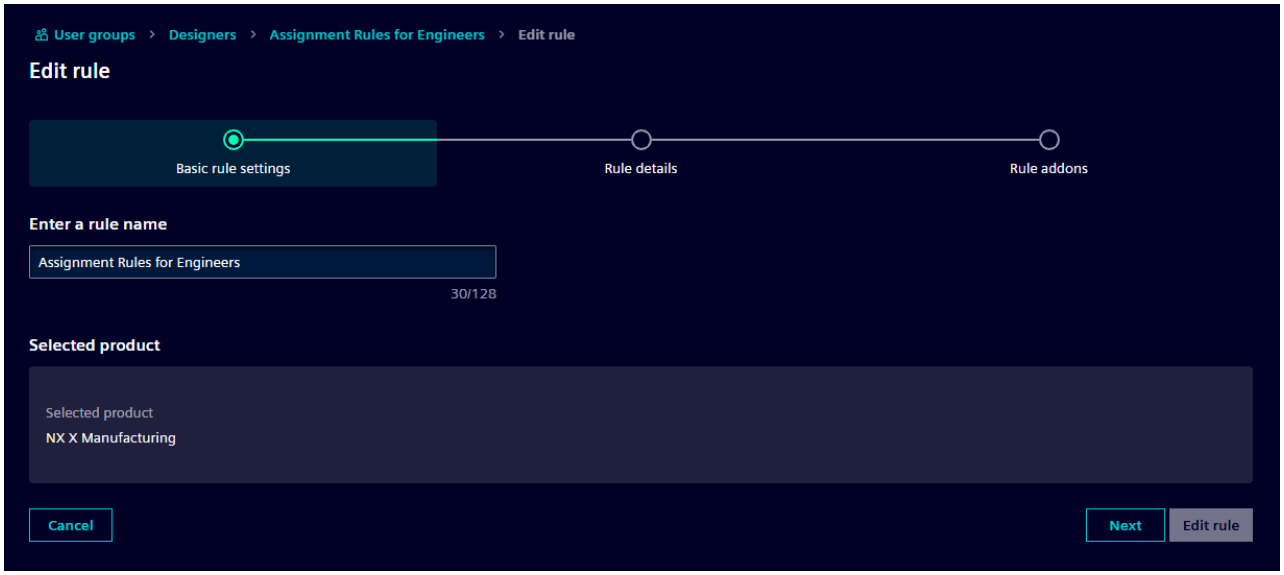
Editing a rule allows you to modify all fields for both active and inactive rules.

To edit a rule:

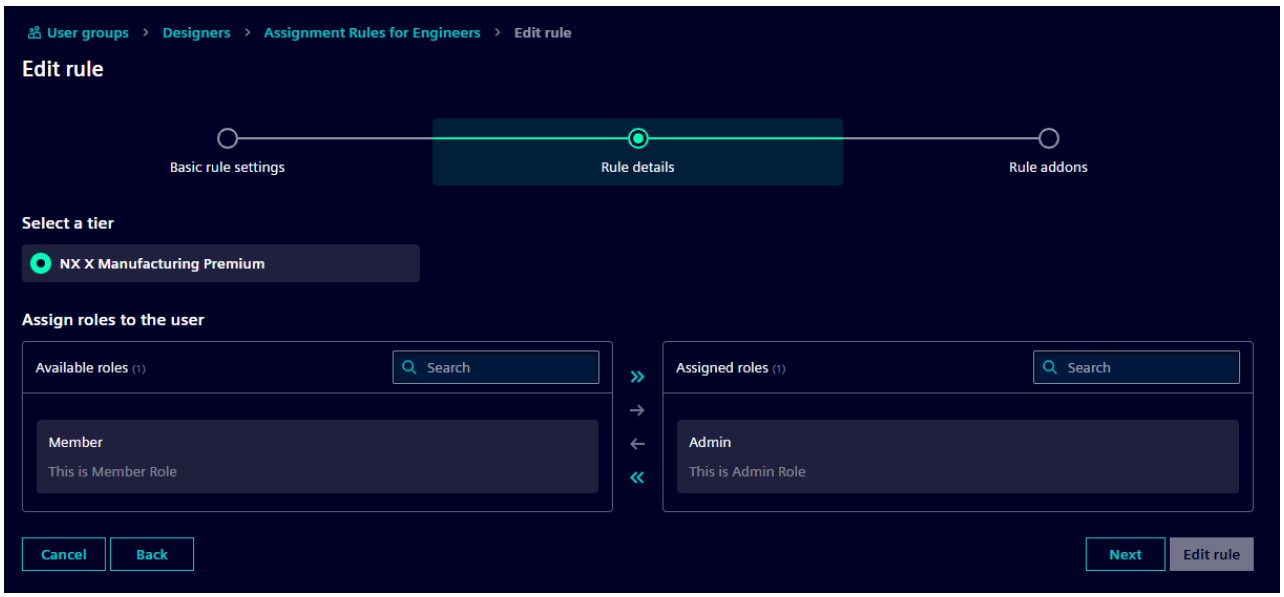
1. Select the rule to edit.
2. In the **Rule details** screen, click **Edit**.




3. In the **Basic rule settings** tab:
   - Edit and update the rule name.
   - Displays the selected product for rule assignment.
   - Click **Next**.




4. In the **Rule details** tab:
   - Select the tier.
   - In the **Assign roles to the user** section, modify the roles:
     - To assign roles: Select from the "Available roles" list and click →. To assign all, click ».
     - To unassign roles: select from the "Assigned roles" list and click ←. To unassign all, click «.




5. Click **Next**, if your product supports addons.
   - In the **Rule addons** tab:
     - To assign addons: Select from the "Available addons" list and click →. To assign all, click ».

- To unassign addons: Select from the "Assigned addons" list and click . To unassign all, click .


6. Click **Edit rule**.

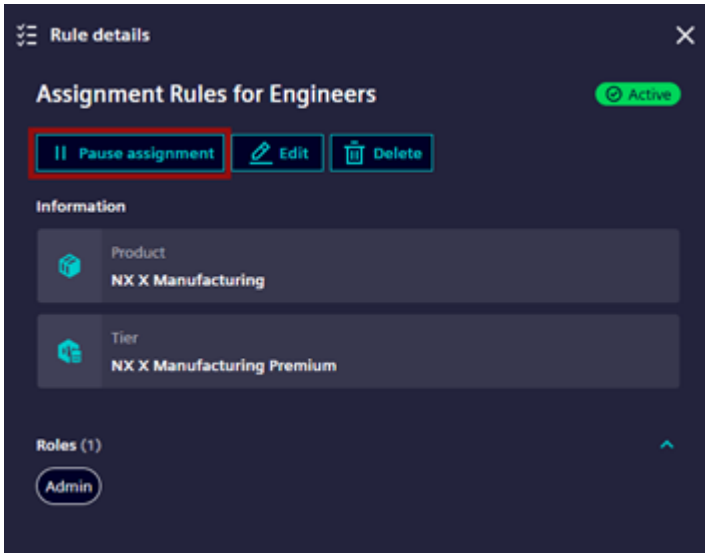
The rule is updated successfully.

## Pause Assignment for a Rule

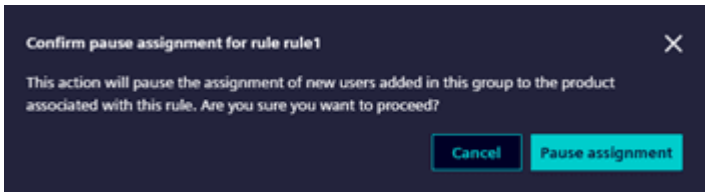
Pause assignment for a rule prevents new users from being assigned under that rule. When you reactivate the rule, it resumes assigning new users to the group without any manual intervention.

To pause assignment for a rule:

1. Select the rule to pause.
2. In the **Rule details** screen, click **Pause assignment**.



3. In the **Confirm pause assignment** pop-up, click **Pause assignment**.



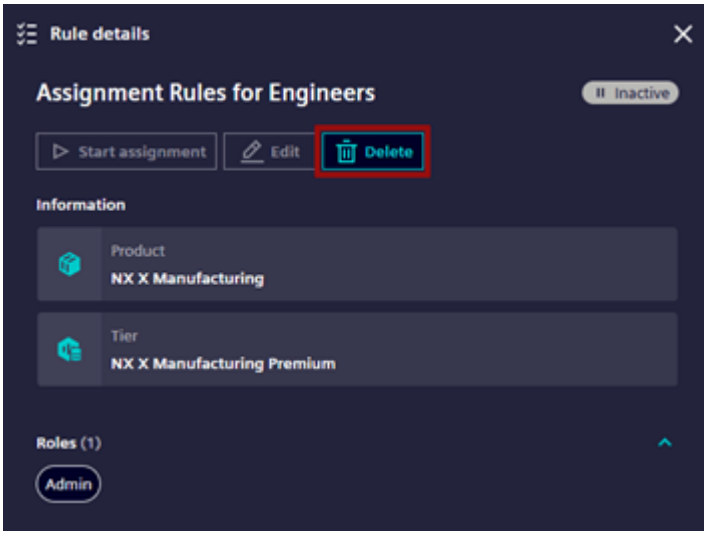

The rule is paused (deactivated).

## Delete a Rule

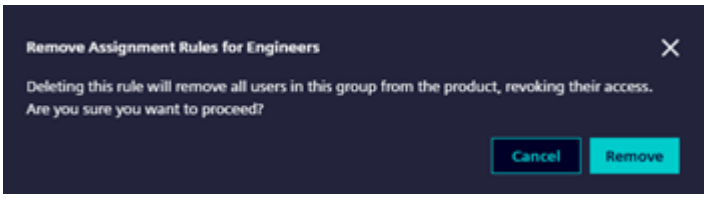
Deleting a rule removes product access for users who were assigned through that rule.

> **Note**
> Only one rule applies to each group-product pair. You can create multiple rules for different products.

1. To delete a rule:
   - Select the rule to delete.
   - In the **Rule details** screen, click **Delete**.




   - In the **Remove** pop-up, click **Remove**.

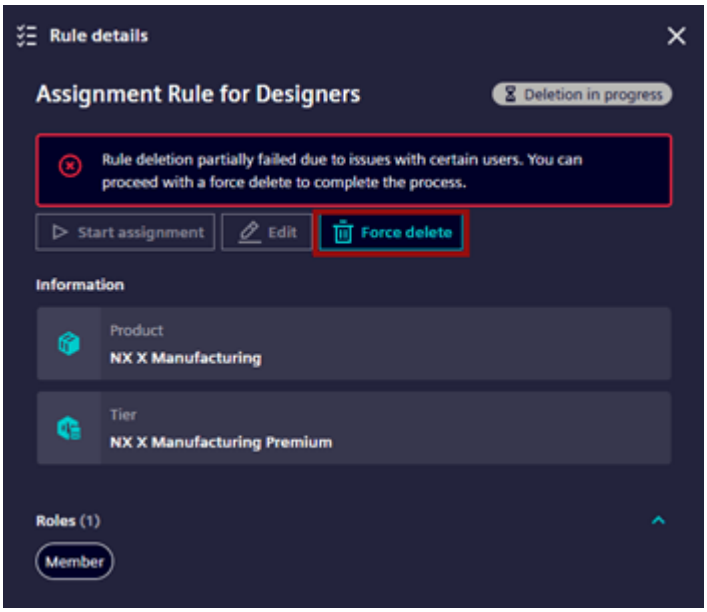



   The rule is deleted.

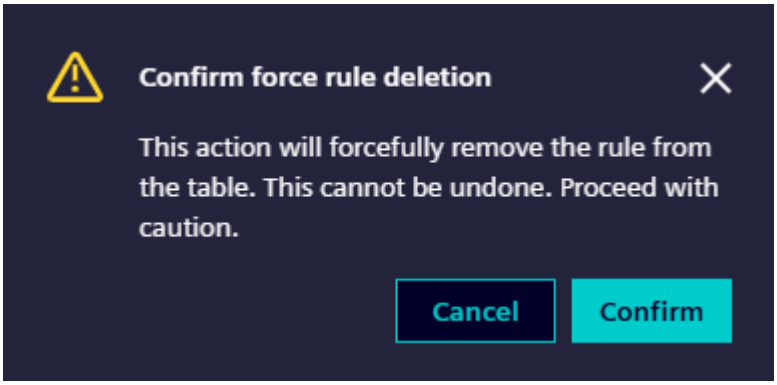
2. Force Delete a Rule

   If a rule has a pending or failed status:

   - In the **Rule details** screen, click **Force delete**.




   - In the **Confirm force rule deletion** pop-up, click **Confirm**.




   The rule is deleted.

## Monitor Rule Status

The "Rule Status" column for a rule displays the current status of the rule and the status of user assignments triggered by it.

Rule statuses:

- **Active**: The rule is operational.
- **In-Queue**: Users are in a pending assignment.

- **Paused**: The rule is temporarily halted due to an error or an unmet condition (for example, product license slots are exhausted or expired).
- **Failed**: User assignments have failed.
- **Inactive**: The rule is not active.

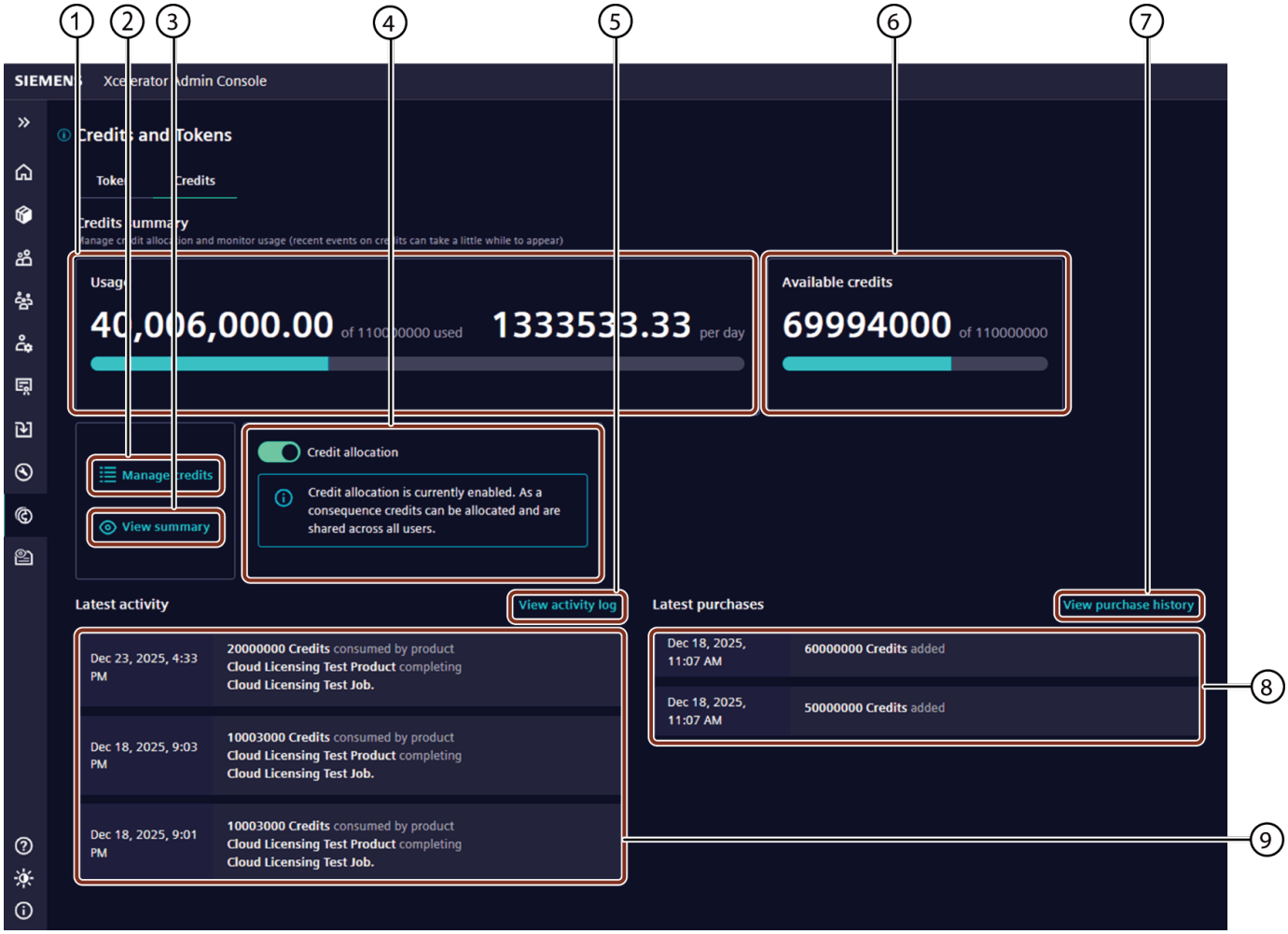
# 6. Manage Resources

## Manage Credits

The credits dashboard shows information about credit consumption, purchases, and allocation. This feature is available only when the associated Enterprise Cloud Account (ECA) has purchased credits. You can allocate credits only to users assigned to a credits-enabled product.

**Note**

- The credits dashboard notifies the tenant admin when the credit balance is less than 100.
- To enable credit allocation, users need to complete their initial sign in.
- A users name appears in the allocation list only after they sign in to the assigned application.




① Displays the number of credits used from the total purchased credits, and the number of credits used per day

② Allows you to allocate, edit and remove credit allocation

③ Allows you to navigate to the summary of credit usage

④ Allows you to enable credit allocation and navigates to the allocation screen to allocate credits

⑤ Allows you to view information about the credits activity log

⑥ Displays the total number of available credits out of total number of credits

⑦ Allows you to view information about the credits purchase history

⑧ Displays the latest credit purchase history

⑨ Displays the latest credit activity log

> **Note**
>
> To navigate to another detailed page, such as the activity log, purchase history, or credit allocation, click **Switch to** and select the information page you want to view.

## Allocate Credits to Individual Users

Allocating credits to individual users enables tenant admins to switch from account pool to user pool allocation. This provides better control over credit distribution and allows customization of resource access based on user roles and needs.

- Enable allocation mode to limit credits to selected users, allowing tenant admins to allocate credits individually.
- Disabling allocation mode allows all users in the account to access credits without specific allocation.

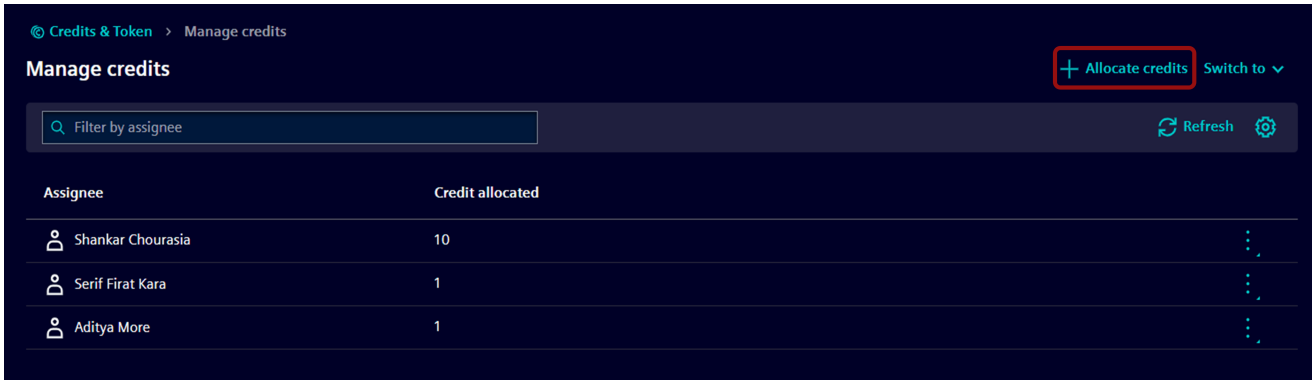
> **Note**
>
> Disabling this feature prevents allocation or deallocation of credits to individual users. When disabled, the assigned credit quota for each user becomes inactive.

## Allocate credits

Allocating credits to individual users allows tenant admins to add, allocate, or remove credits for selected users.

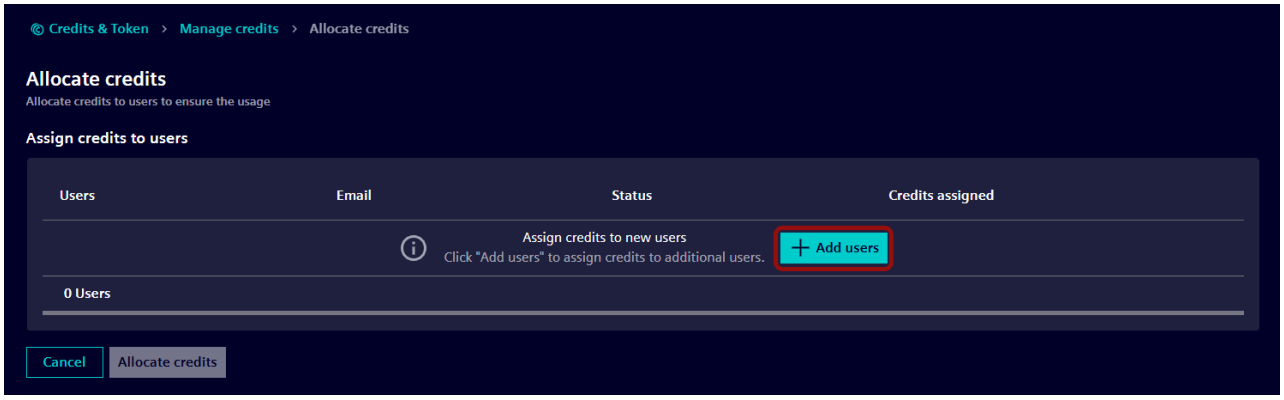
To allocate credits to individual users:

1. In the Credits overview page, click **Manage credits**.
2. Click **Allocate credits**.

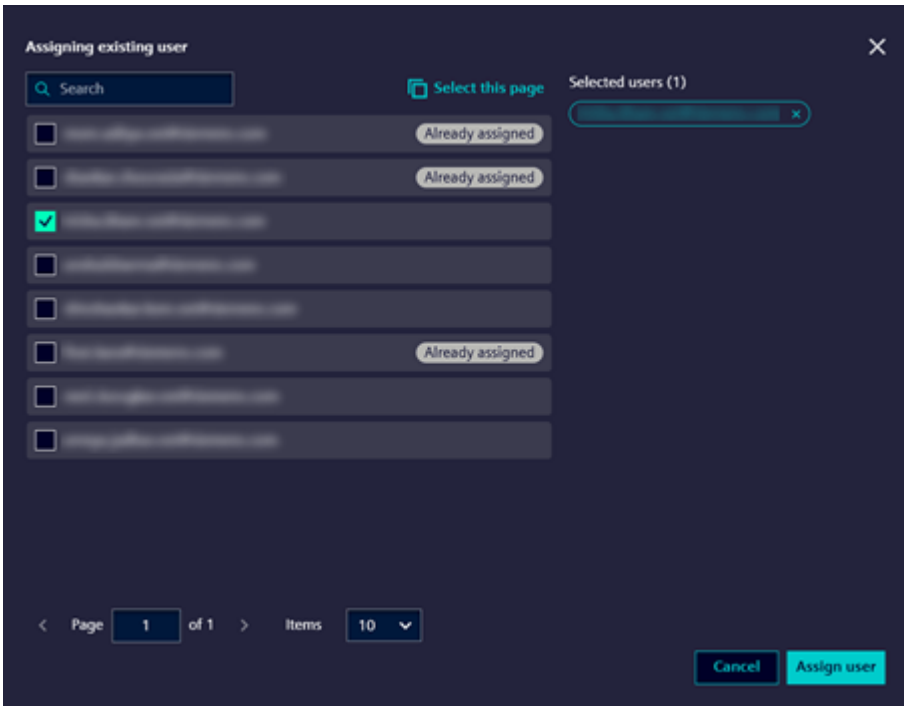



3. In the **Allocate credits** screen:

   - Click **Add users**.

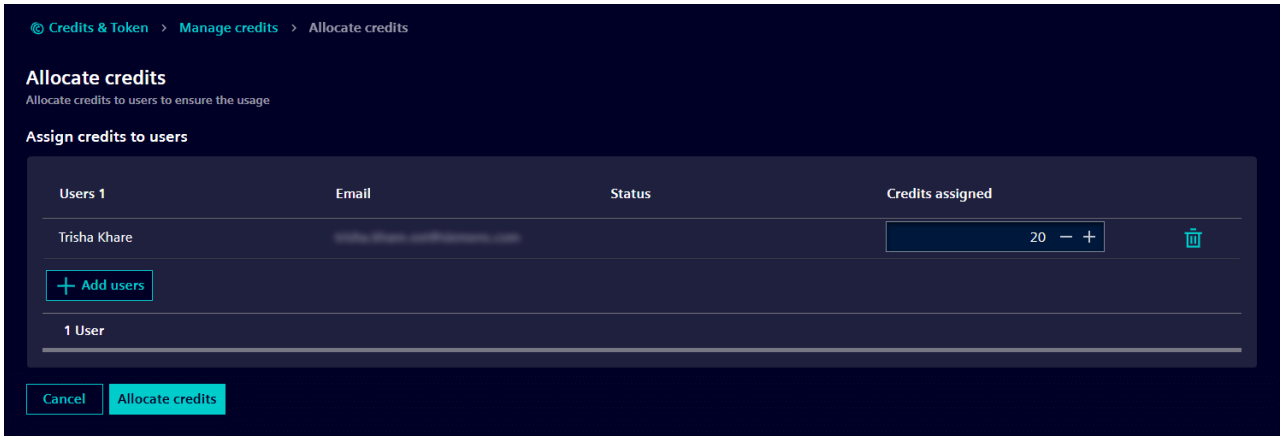



   - In the **Assigning existing user** pop-up, select one or more users and click **Assign user**.



> **Note**
>
> The **Assigning existing user** pop-up shows a list of users provisioned to use credits-enabled products.

- In the **Credits assigned** column, enter or add the number of credits.




4. Click **Allocate credits**.

The selected users are assigned with the allocated credits.

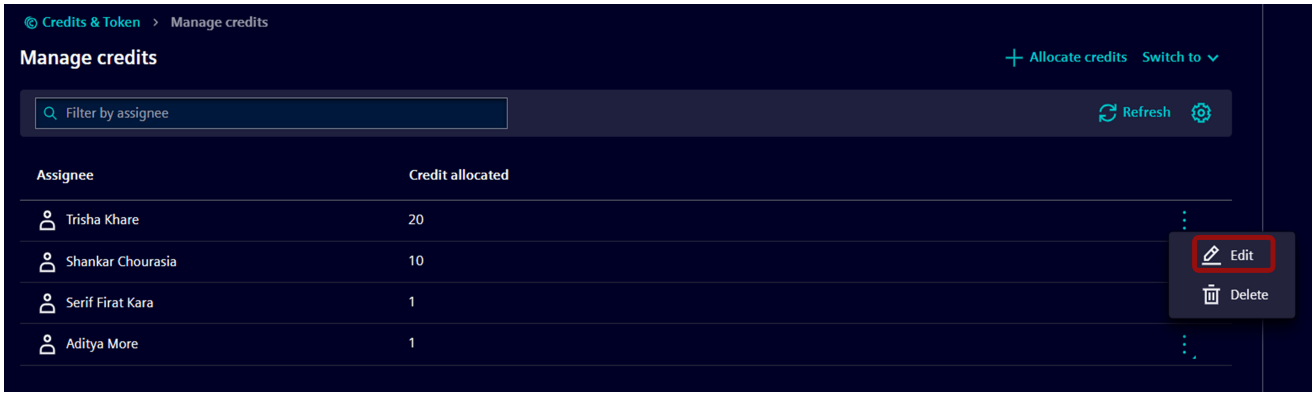
> **Note**
>
> If the user list does not update with usernames and their respective credit balances, click Refresh button to update the list.

## Edit Credit Allocation

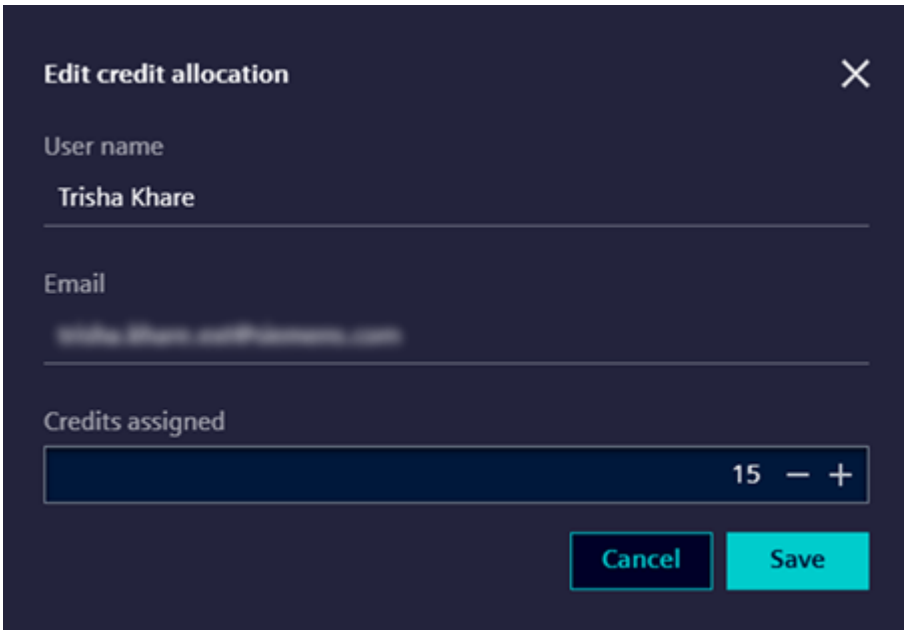
Editing credit allocation allows you to increase or decrease the credits allocated to a specific user.

To edit credit allocation:

1. In the **Manage credits** screen, select a user.
2. Click ⋮ button and select **Edit**.




3. In the **Edit credit allocation** pop-up, click **+** sign to increase or **-** sign to decrease the credits.




4. Click **Save**.

The credit allocation is updated for the user.

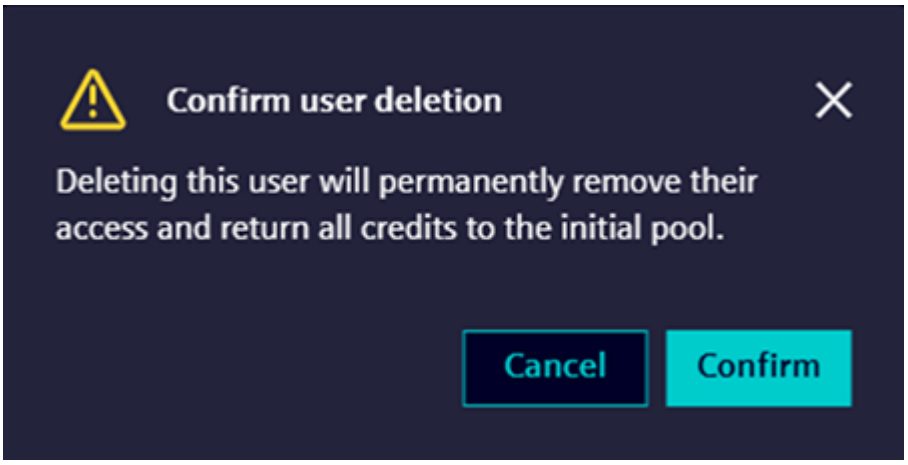
## Remove a user from credit allocation (de-allocate)

Removing a user from the allocation list prevents them from running credit-specific jobs.

To remove a user from credit allocation:

1. In the **Manage credits** screen, select users from the list.
2. Click  button and select **Delete**.


3. In the **Confirm user deletion** pop-up. Click **Confirm**.



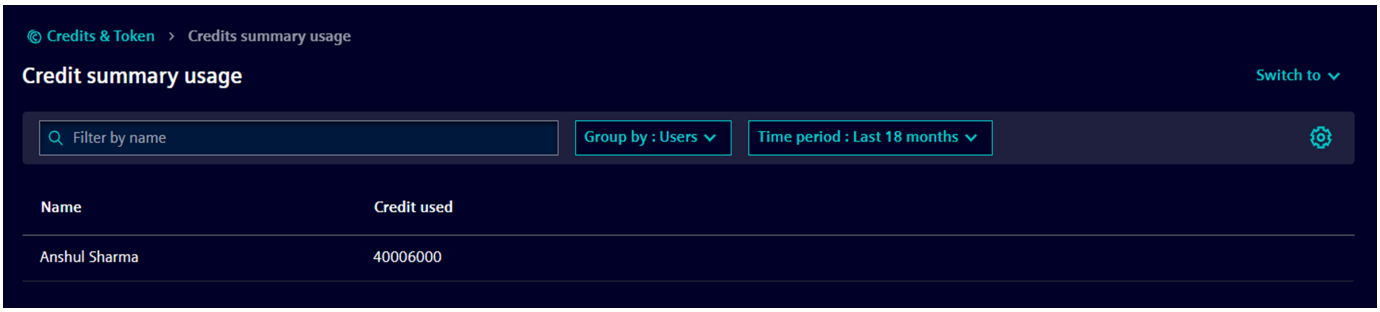

The selected user is removed from credits allocation and can no longer run credit-specific jobs.

## Credits Summary Usage

The credits summary usage screen shows a consolidated view of credits consumption by categories such as users, product, or job type.

| Parameters | Description |
|---|---|
| Group by | Select a category to view consolidated credits consumption grouped by:<br>**Users**: View credits consumed by each user.<br>**Job type**: View credits consumed by different job types.<br>**Product**: View credits consumed by each product. |
| Time Period | Select a time period from the dropdown to filter or retrieve credits activity data. Available options include:<br>Current month<br>Last 2 months<br>Last 3 months<br>Last 6 months |

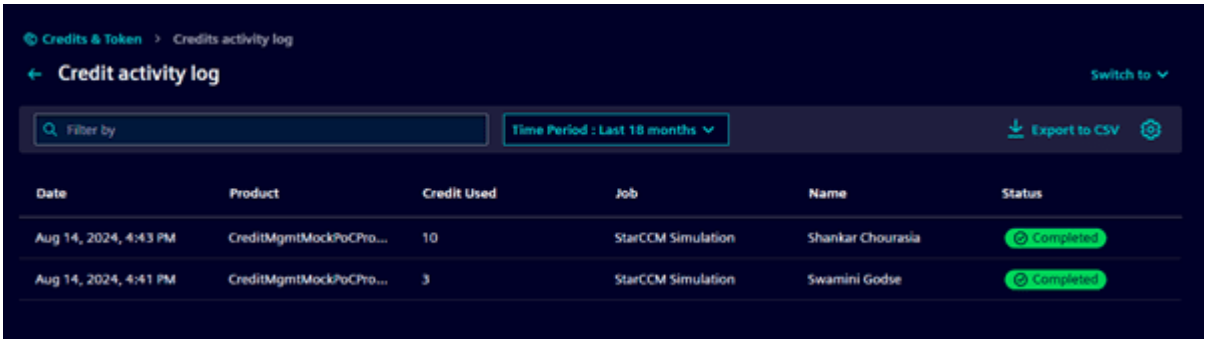
| | |
|---|---|
| | Last 12 months<br>Last 18 months |
| Search | Search credit activity data by product name or job type. |




## Credits Activity Log

The credits activity log screen provides detailed information on credits consumption, including various statuses such as completed, in progress, and Assignment failed.

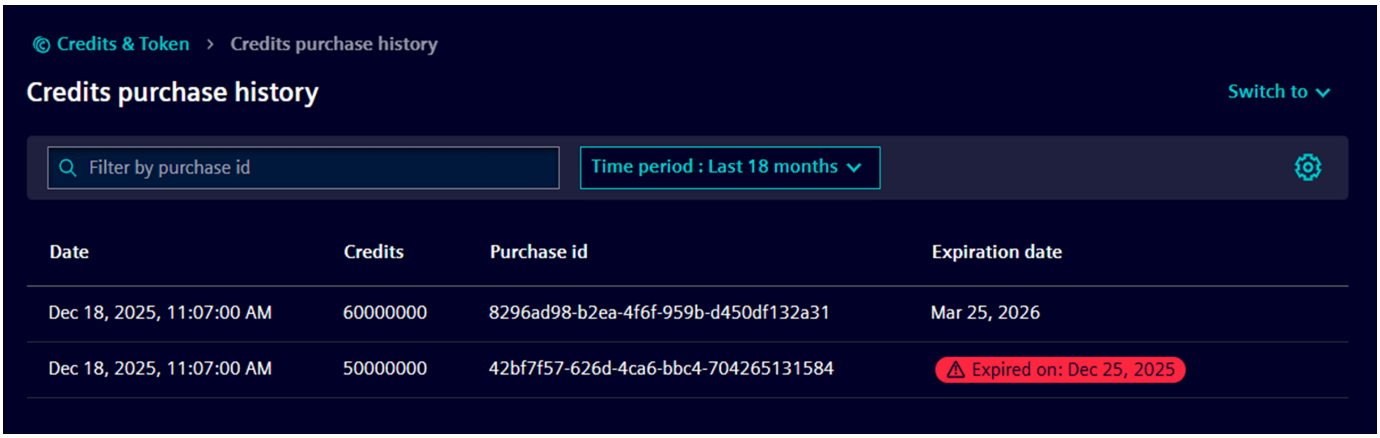
| Parameters | Description |
|---|---|
| Status | Select the status to view the transactions based on:<br>**Completed**: View transactions with a completed status.<br>**In Progress**: View transactions with an in-progress status.<br>**Canceled**: View transactions with a canceled status. |
| Time Period | Select a time period from the dropdown to filter or retrieve credits activity data. Available options include:<br>Current month<br>Last 2 months<br>Last 3 months<br>Last 6 months<br>Last 12 months<br>Last 18 months |
| Search | Search credit activity data by product name or job type. |
| Export to CSV | Export all transactions based on the selected criteria in CSV format. |




## Credits Purchase History

The credits purchase history screen shows information about credits purchases, including the number of credits purchased, activation date, expiration date, and Purchased ID.

- Time Period: Select a period from the dropdown to filter or retrieve credits activity data. Available options include:
  Current month
  Last 2 months
  Last 3 months
  Last 6 months
  Last 12 months
  Last 18 months

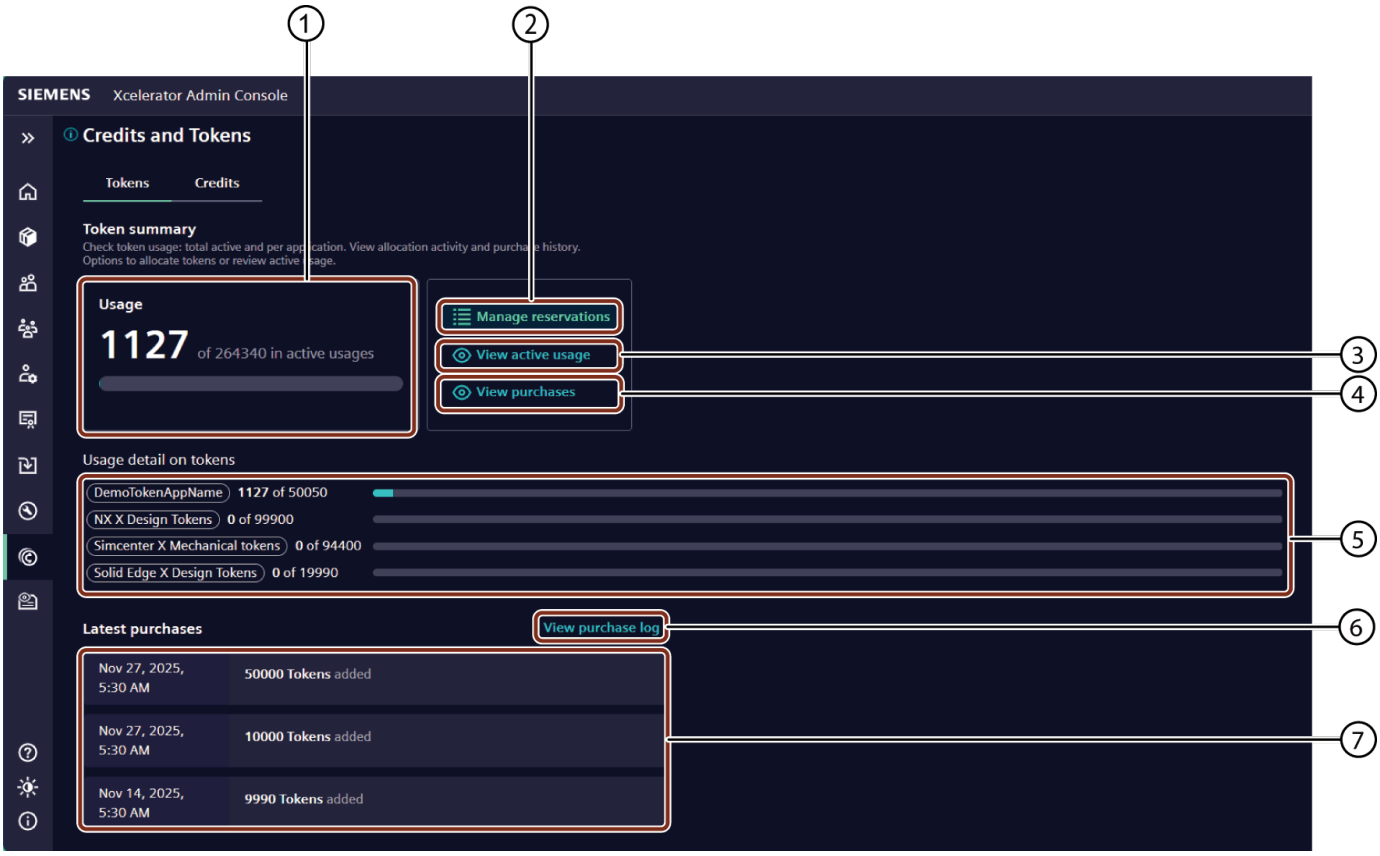



# Tokens

The tokens dashboard allows application owners to manage add-on feature usage. Using a floating license model, owners can reserve tokens for individual users or user groups.

> **Note**
>
> **Floating License Model**: This model provides flexibility to customers through token usage. Customers pre-purchase tokens, which are then reserved to individual users or user groups.

For individual users, the feature is enabled once they receive the required tokens. For user groups, tokens are shared by allowing multiple users to access the feature provided that sufficient tokens are available.




① Displays the number of active use tokens out of the total tokens available

② Allows you to manage tokens, including reserve tokens, edit and removal of tokens

③ Displays a list of active tokens in use, including list of user and user group, token name and tokens in use

④ Allows you to view detailed information of purchased tokens including start date, number of tokens purchased, token name and expiration date

⑤ Displays the number of tokens currently used within the product

⑥ Displays the list of token purchased history, including date and time of purchase, tokens purchased, token name and expiration date

⑦ Displays the information of recently purchased tokens, including date and time of purchase and number of tokens added

**Note**

To navigate to another detailed page, such as Token Usage and Token Purchase History, click **Switch to** and select the information page you want to view.

## Reserve Tokens

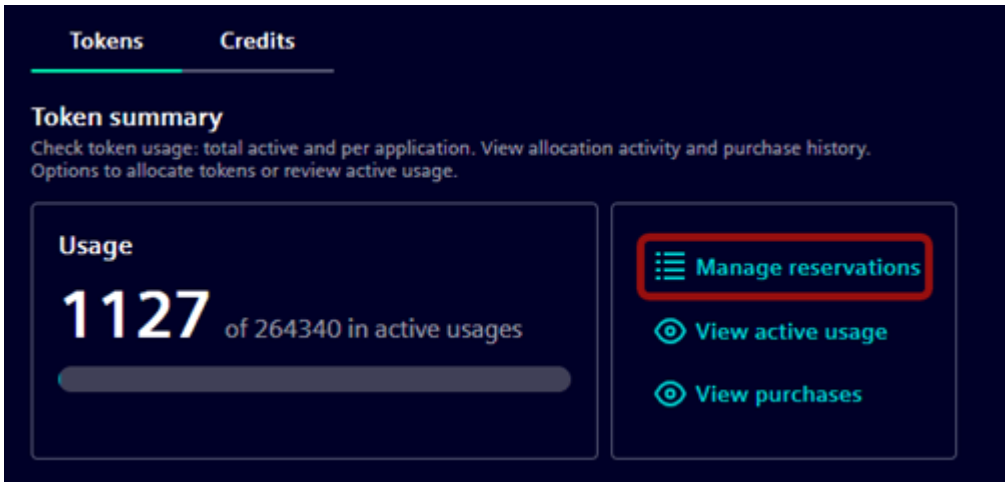
Reserve tokens allows you to reserve a specific number of tokens for individual users or user groups.

**Note**

- Token reservation is not supported for **NX X** products.
- Token reservation is allowed only for users assigned to a product, and only for the tokens associated with that product.
- To enable token reservation, users need to complete their initial sign in.
- A users name appears in the manage reservations list only after they sign in to the assigned application.

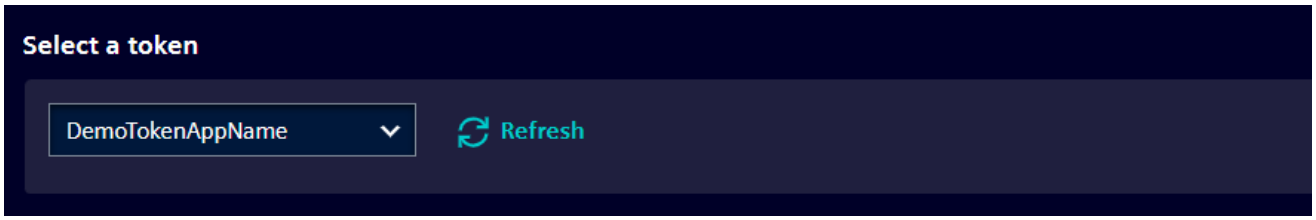
To reserve tokens:

1. In the **Token** tab, click **Manage reservations**.

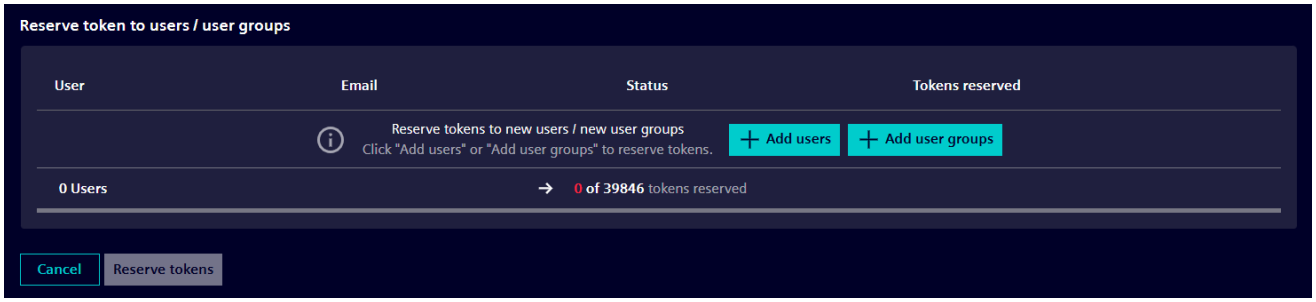



2. In the **Manage reservations** section, click **Reserve tokens**.

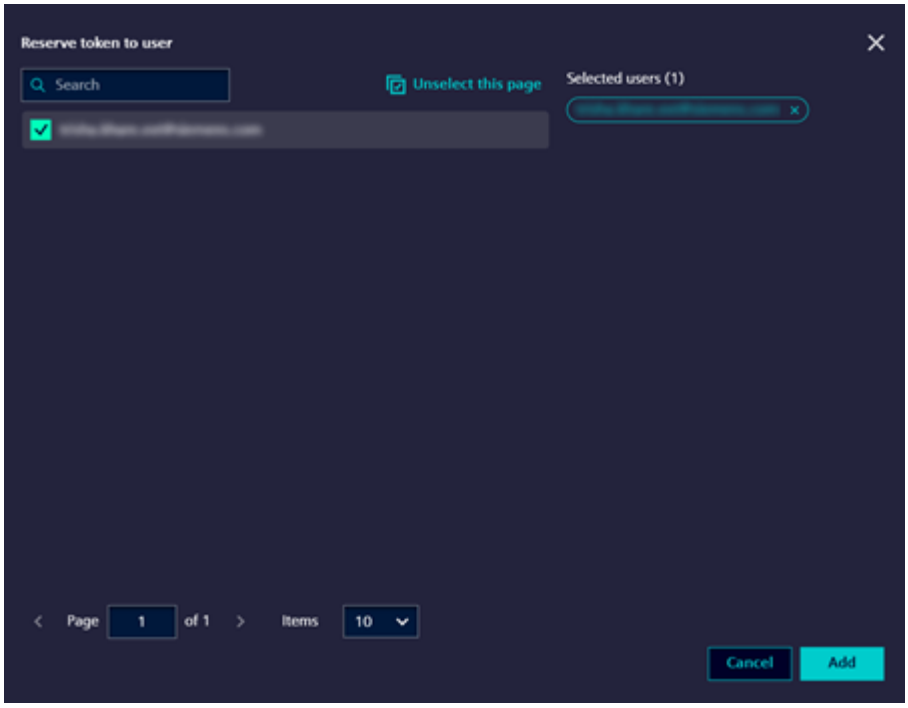

3. Select a token name from the dropdown.




4. Select an option to reserve tokens.



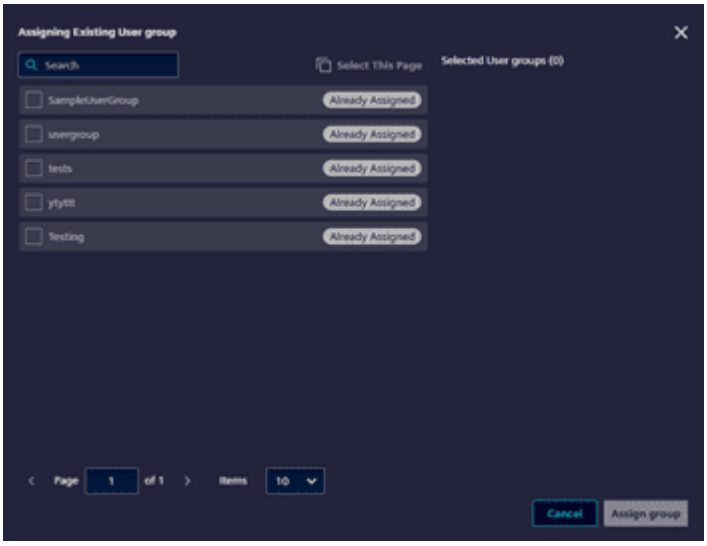

- To reserve tokens for individual users:
  - Click **Add users**.
  - In the **Reserve token to user** pop-up, select one or more users and click **Add**.



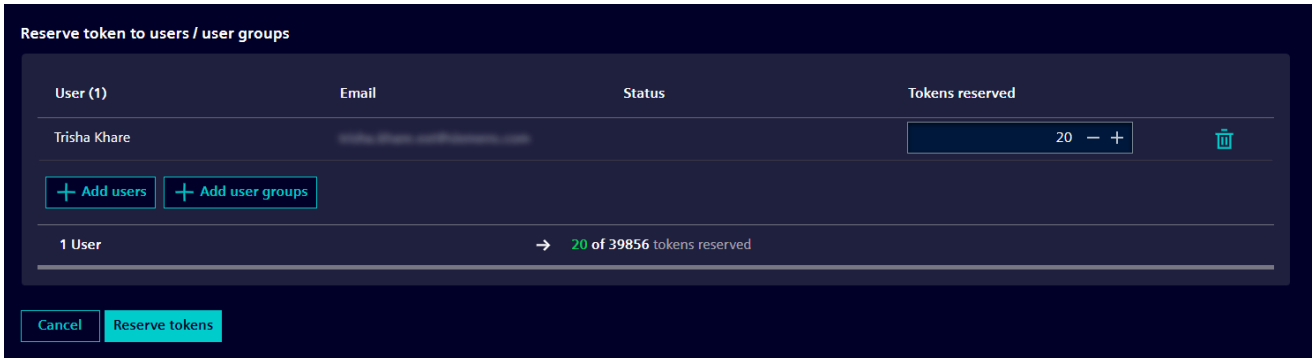

**Note**

The **Reserve token to user** pop-up shows a list of users assigned to the selected product. Users who have not signed in cannot reserve tokens.

- To reserve tokens for user groups:
  - Click **Add user groups**.
  - In the **Reserve token to user group** pop-up, select one or more user groups and click **Add**.




5. In the **Tokens reserved** column, add the number of tokens.




6. Click **Reserve tokens**.

The tokens are reserved successfully.

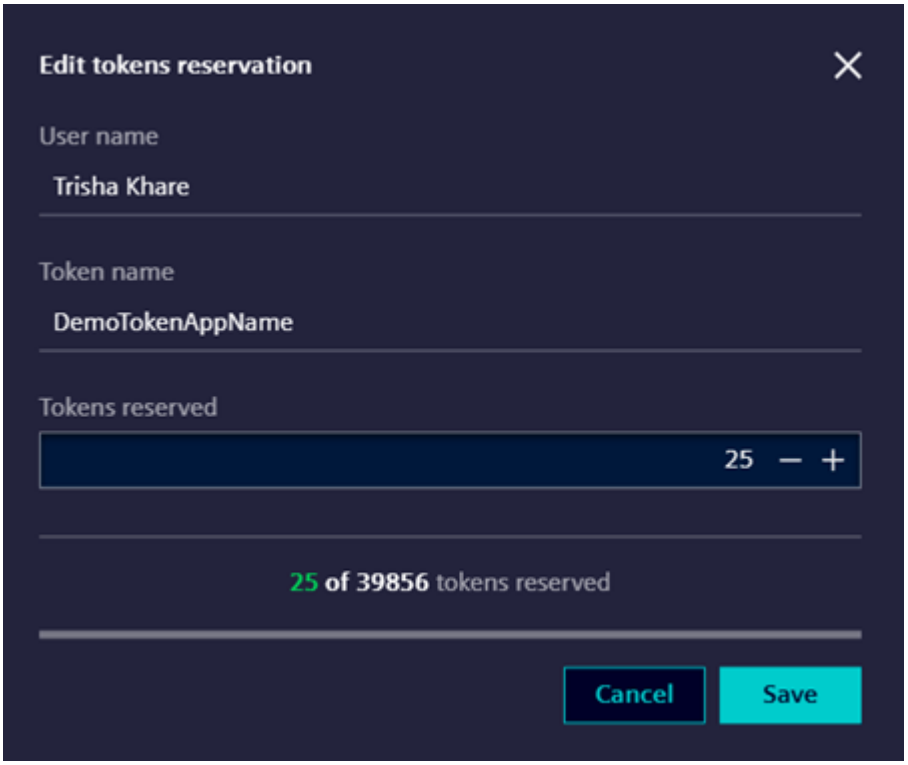
## Edit Reserve Tokens

Editing reserved tokens allows you to increase or decrease the number of tokens reserved for a specific users or user groups.

To edit reserved tokens for users or user groups:

1. In the **Manage reservations** screen, select the user or user group.
   - To view the list of users or user groups, click **Group by** and select the user or user group.
2. Click ⋮ and select **Edit**.


3. In the **Edit tokens reservation** pop-up, click "**+**" sign to increase or "**-**" sign to decrease the number of reserved tokens.

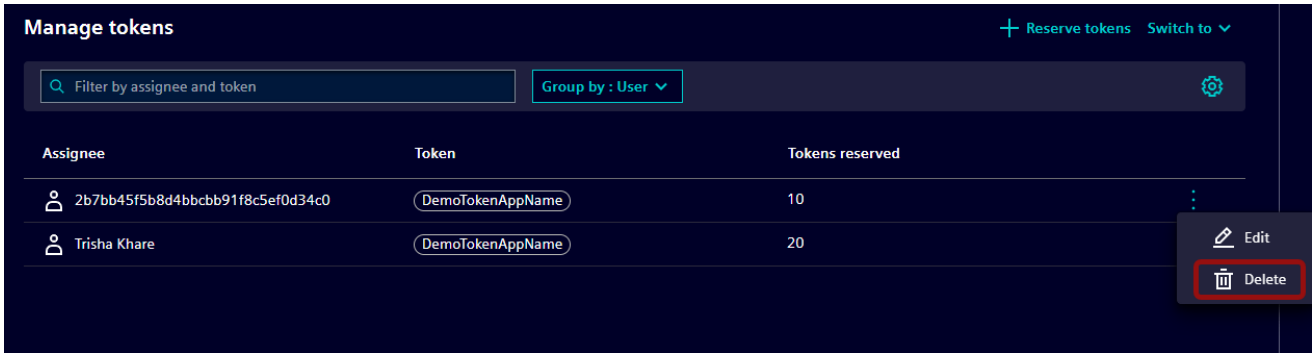



4. Click **Save**.

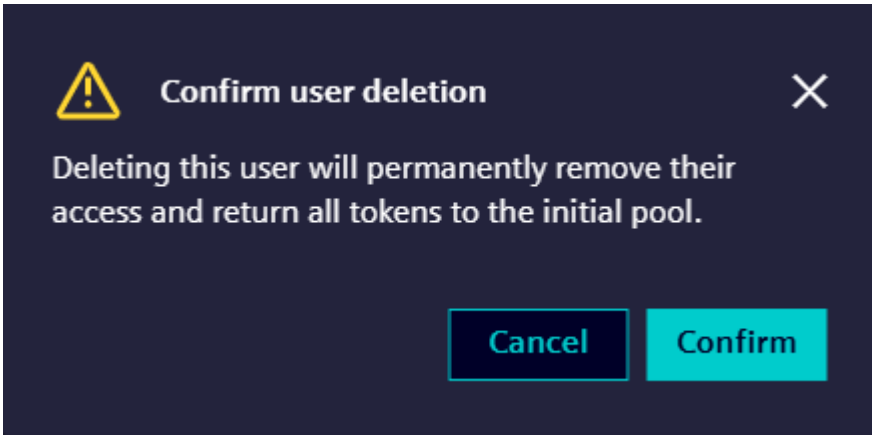
The reservation is updated.

## Remove Reserved Tokens

1. In the **Manage reservations** screen, select the user or user group.
   - To view the list of users or user groups, click **Group by** and select the user or user group.
2. Click ⋮ and select **Delete**.




3. In the **Confirm user deletion** pop-up, click **Confirm**.




The selected user or user group is removed from reserved tokens, and the tokens are returned to the common pool.

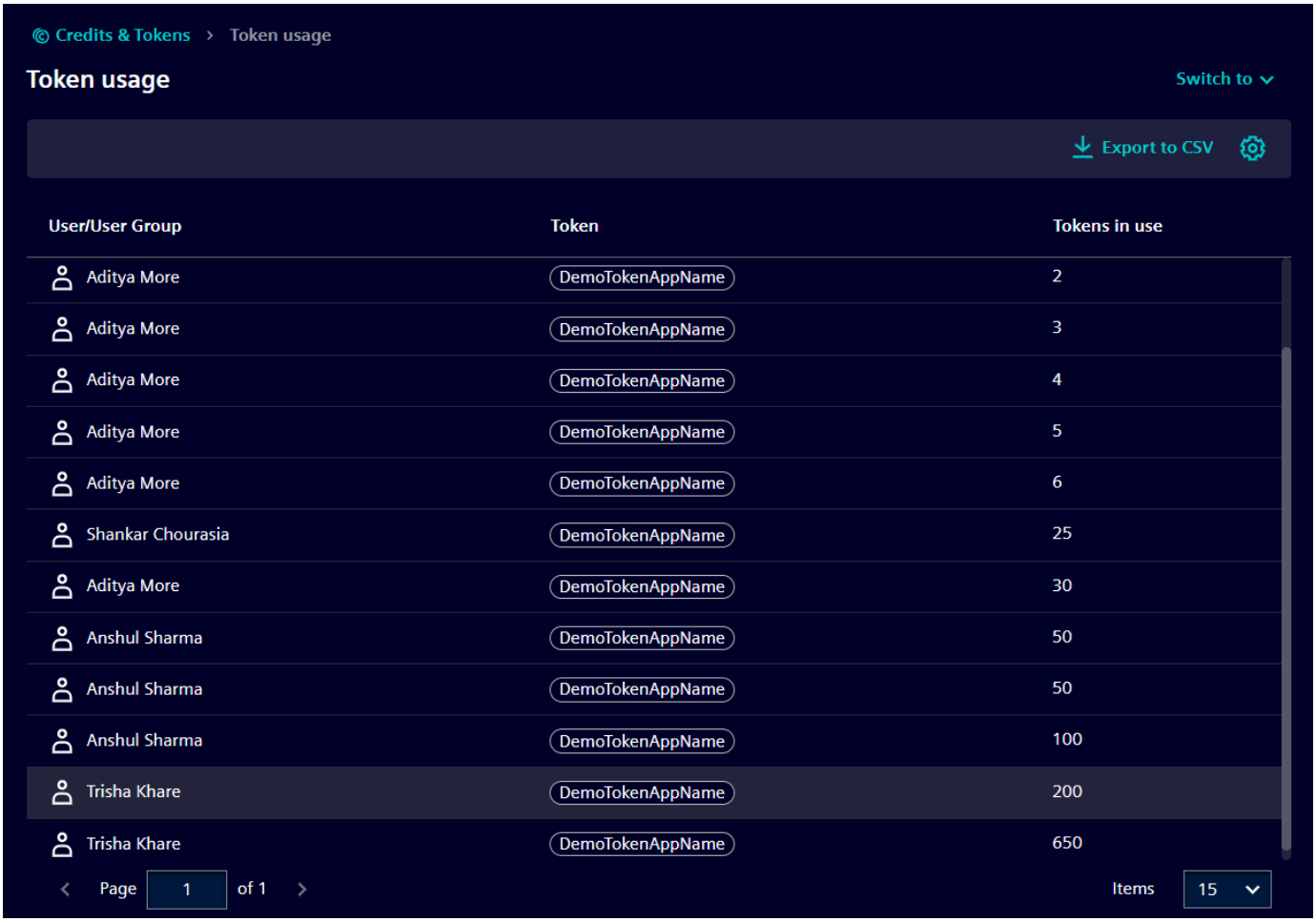
**Note**

If a user runs multiple token executions simultaneously, each job and its token usage are shown separately.

## Token Usage

The token usage screen shows detailed information about token reservations, including a list of users and user groups, token name and tokens in use.

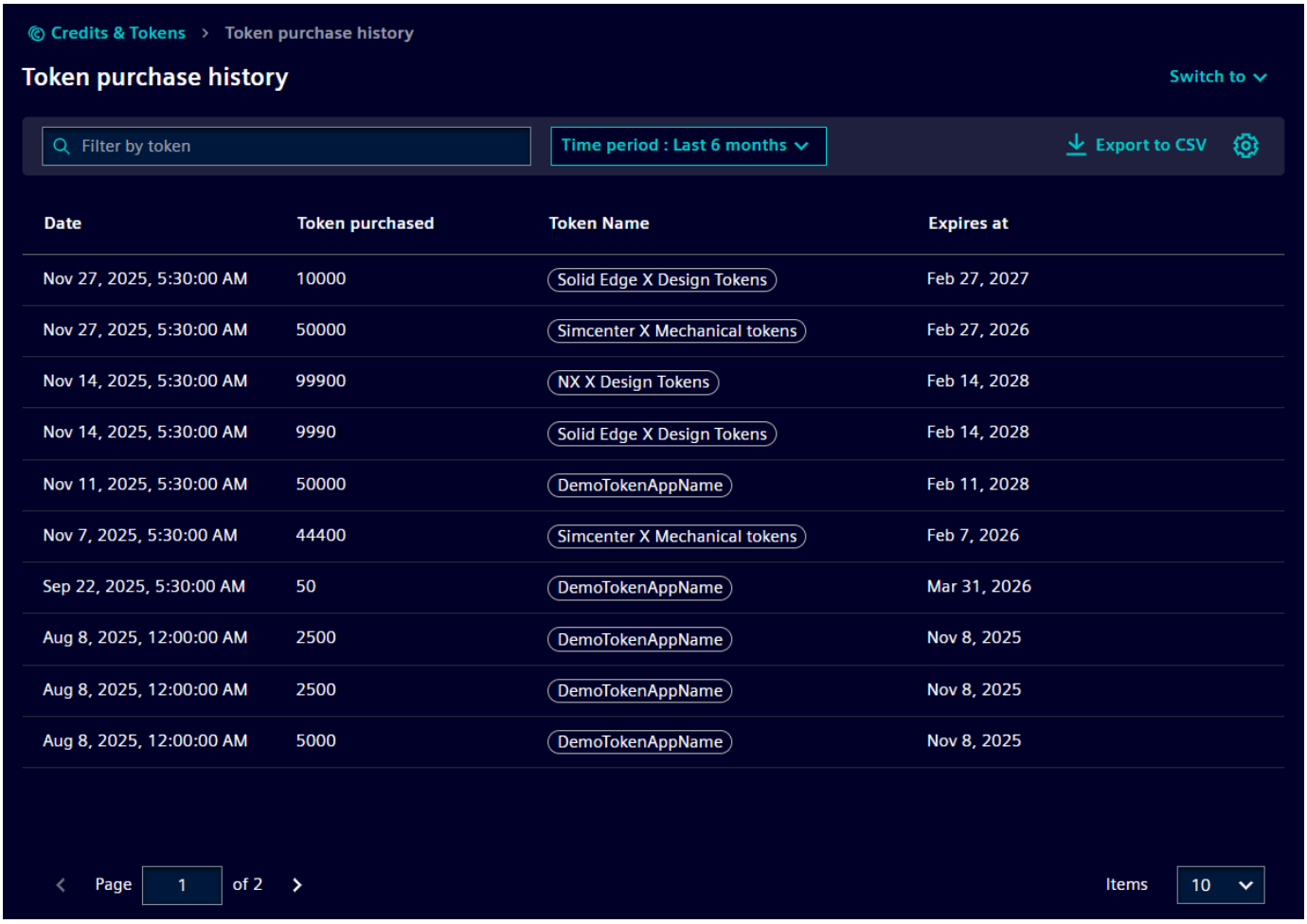
To export token usage transactions in CSV format, click **Export to CSV**.




## Token Purchase History

The token purchase history screen shows information about token purchases, including the activation date, number of tokens purchased, token names and expiration date.

- Time Period: Select a period from the dropdown to filter or retrieve tokens activity data. Available options include:
  Last 6 months Last 12 months Last 18 months
- Export to CSV: Exports the token purchase history in CSV format based on the selected criteria.



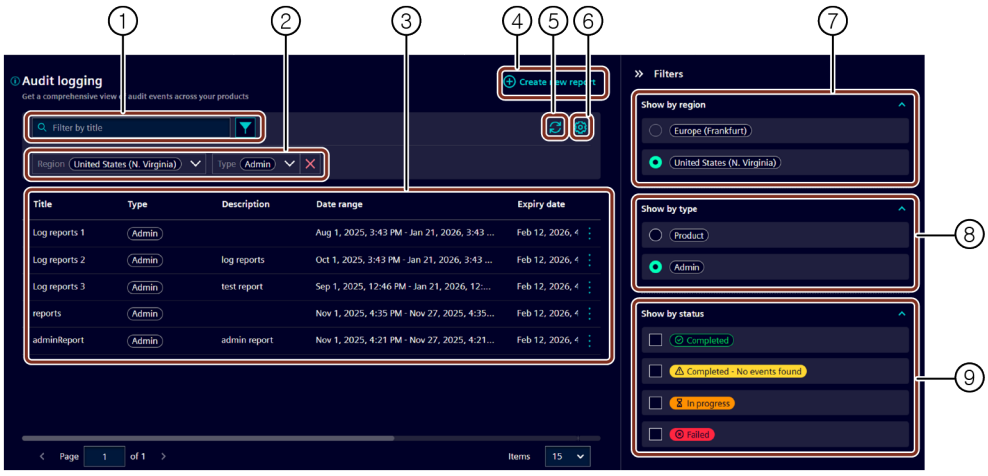
# 7. Monitor and Report

## Generate and Download Audit Logging Reports

This section explains how to generate and download admin and product reports.

- **Admin Reports**: Admin reports details account-level operations, such as:
  - Opting in for user consent data
  - Configuring the ECA name and description
  - Creating, editing, or deleting ECA admins
  - Creating, updating, deleting, activating, deactivating, and acknowledging IDP configurations
  - Assigning, editing, or deleting product users
  - Creating, downloading, and deleting server users
  - Creating, downloading, and deleting credentials for product configuration
- **Product Reports**: Product reports detail product-level operations, such as user logins, user logouts, and other user actions. Product teams must register events in advance to make them available in audit logging reports.

**Overview of the Audit Logging Screen**:




① Allows you to search for a report by name

② Displays the selected filter

③ Displays a list of reports

④ Allows you to generate a new report

⑤ Allows you to refresh the page to update the report list

⑥ Allows you to customize the table columns of your choice

⑦ Allows you to filter the reports list as per the region. By default, United States region will be selected for **Admin** reports

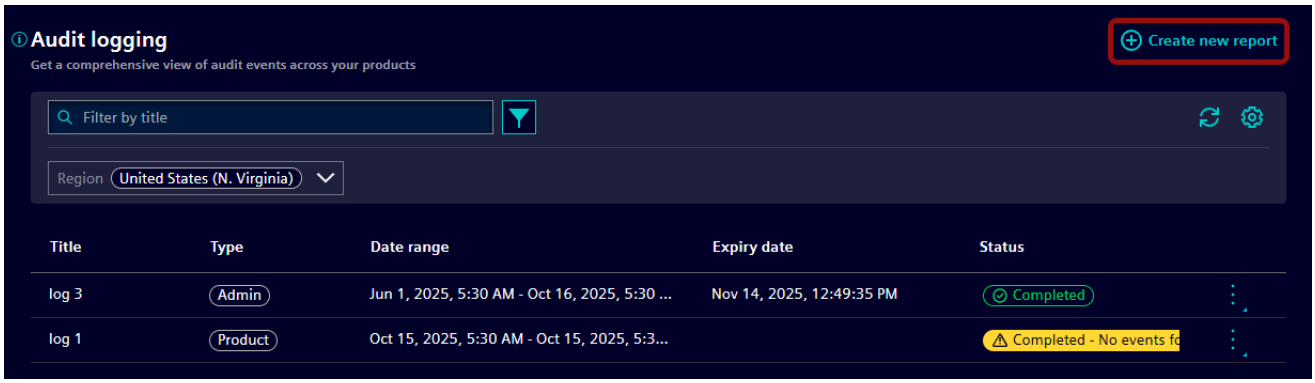
⑧ Allows you to filter the list based on the report type.

⑨ Allows you to filter the list based on the report status.

## Generate Audit Logging Reports

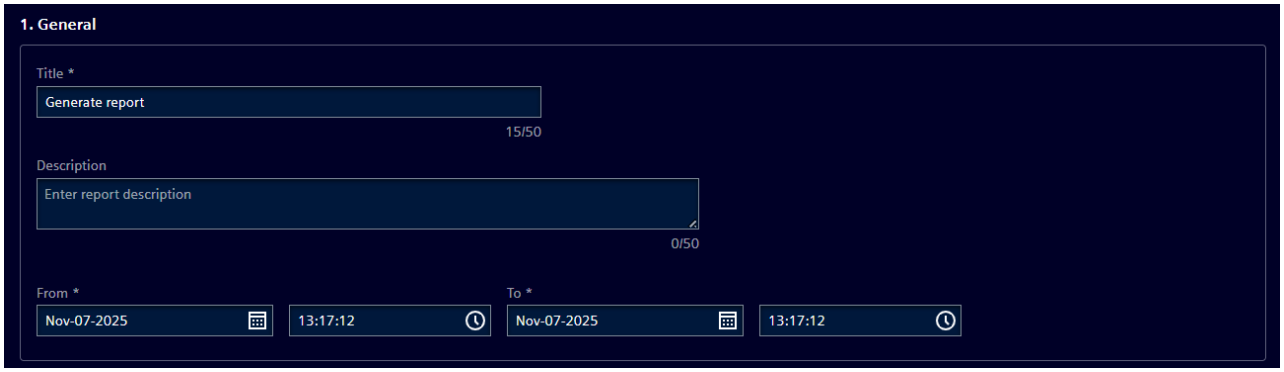
To generate audit logging reports:

1. Go to the **Audit Logging** tab in the left navigation pane and click **Create new report**.

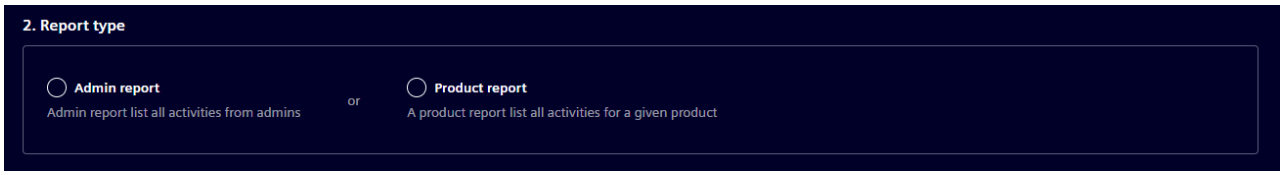



2. In the **Create new report** screen, enter the required fields:
   - In the **General** section:
     - Enter a title for the report.
     - Enter a brief description of the report.
     - Select a date range and time within the last 6 months. After you select the **To** time from the dropdown, click **Confirm**.

> **Note**
> - The report will cover account-level operations for the past 6 months.
> - Dates must be within the last 6 months.
> - The **From** date should not be greater than the **To** date.
> - The **To** time should not be greater than the current time.




- In the **Report Type** section, select the type of the report you want to create.
  - **Admin Report**
  - **Product Report**




- In the **Report type-specific settings** section (applicable for "Product Report" type only):
  - Select the **Region** of the report.
  - Select the **Products** available in the specified region from the drop-down.


3. Click **Generate report**.

The report is generated and an email notification is sent to the ECA admin user.

> **Note**
> The generated reports are valid for 7 days.

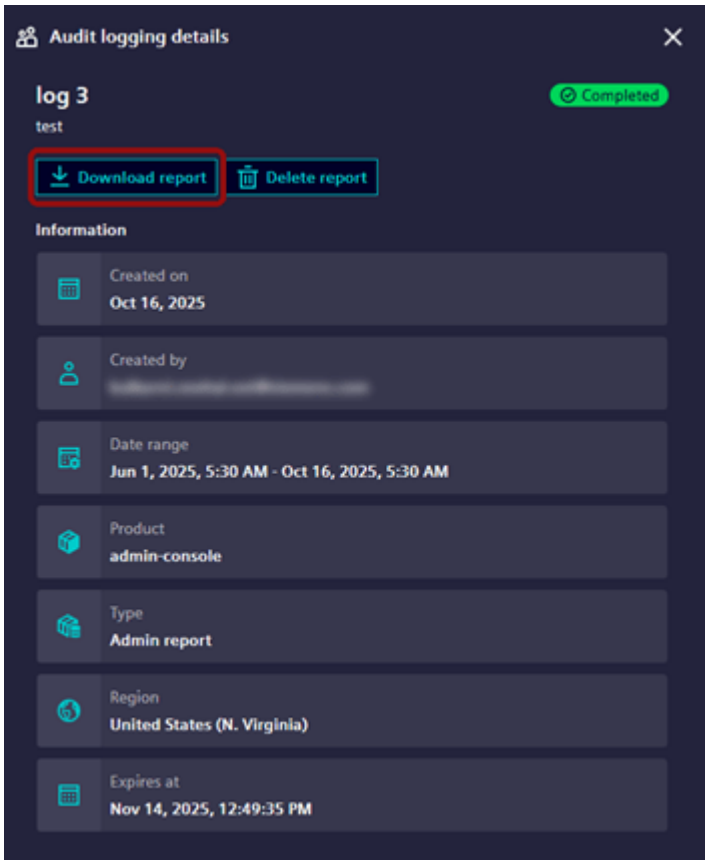
## Download Audit Logging Reports

To download generated audit logging reports:

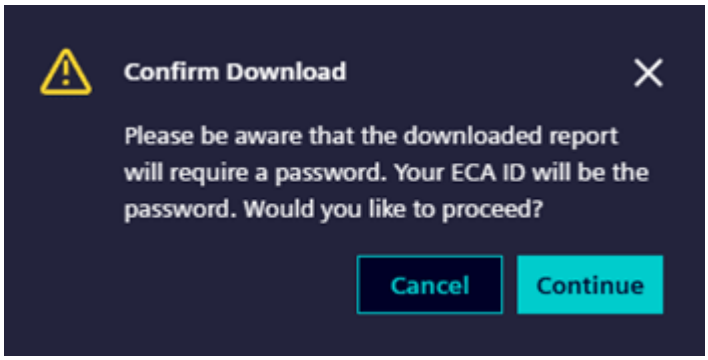
1. Select the report you want to download.

> **Note**
> The **Download report** button is active only when the report status is **Completed**.

2. In the **Audit logging details** screen, click **Download report**.




3. In the **Confirm Download** pop-up, click **Continue**.




The report is downloaded as a password-protected CSV file.

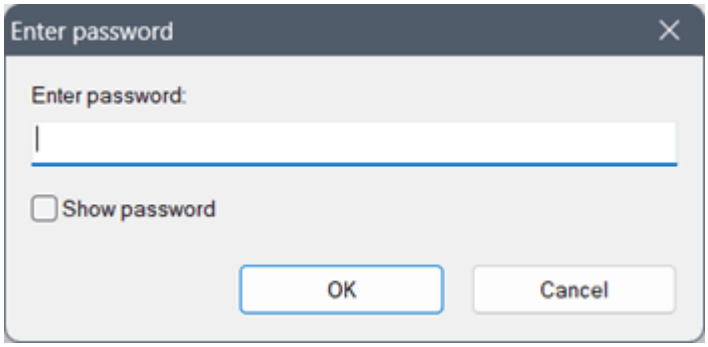
**Report Status Guide**:

| Status | Details |
|---|---|
| Completed | The report is generated and available for download. |
| In Progress | The report is being generated. |
| Completed - No events found | The report is generated but contains no events (the report is empty and cannot be downloaded). |
| Failed | The report is not generated. |

## Extract the Audit Logging Reports

To extract the downloaded audit logging report:

1. Find the report in your machines **Downloads** folder.
2. Extract the report file.
3. Enter the password associated with the report file when prompted. Use the **ECA ID** of the user who generated the report in the password field.




> **Note**
>
> Entering an incorrect password will cause the extraction process to fail, and the file will remains inaccessible.

4. Click **OK**.

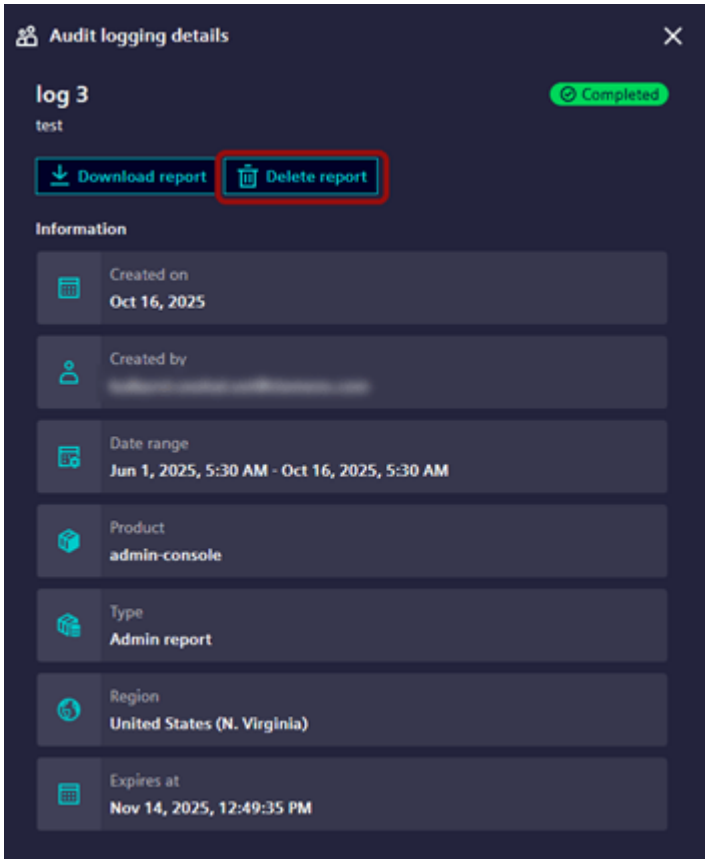
The report file is successfully extracted.

For additional details on Audit Events, refer to **Audit logging Service**.

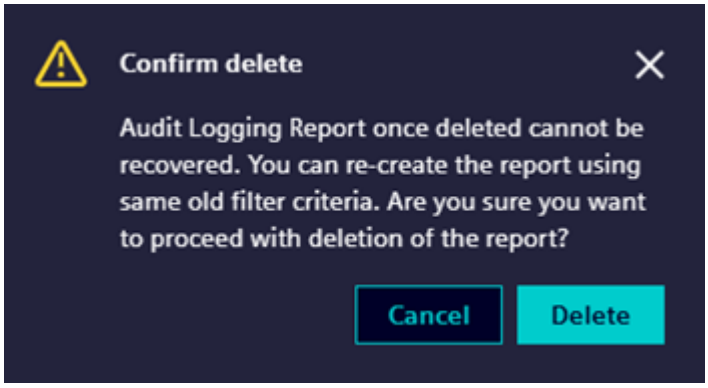
## Delete Audit Logging Reports

To delete audit logging reports:

1. Select the report you want to delete.
2. In the **Audit logging details** screen, click **Delete report**.




3. In the **Confirm delete** pop-up, click **Delete**.




The audit logging report is deleted.

**Note**

Deleted audit logging reports cannot be recovered. To create a new report, refer to **Generate Audit Logging Reports**

# Usage Details

The Usage Details section provides information about how a selected product is used by the logged-in Enterprise Customer Administrator (ECA). This feature is available under the following conditions:

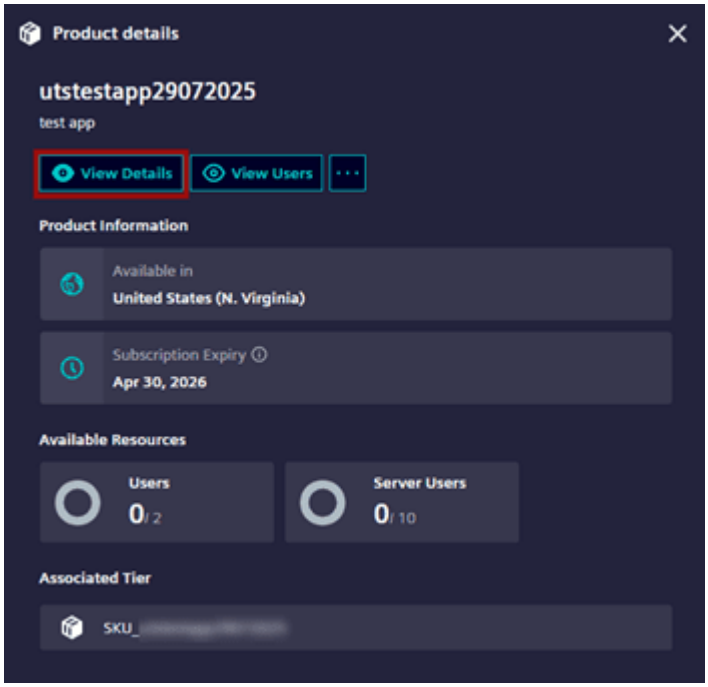
- A usage-based metric with an aggregation policy is defined for the selected product.
- The selected product is in a provisioned state.

> **Note**
> The Usage Details dashboard provides a read-only view of applications usage data.

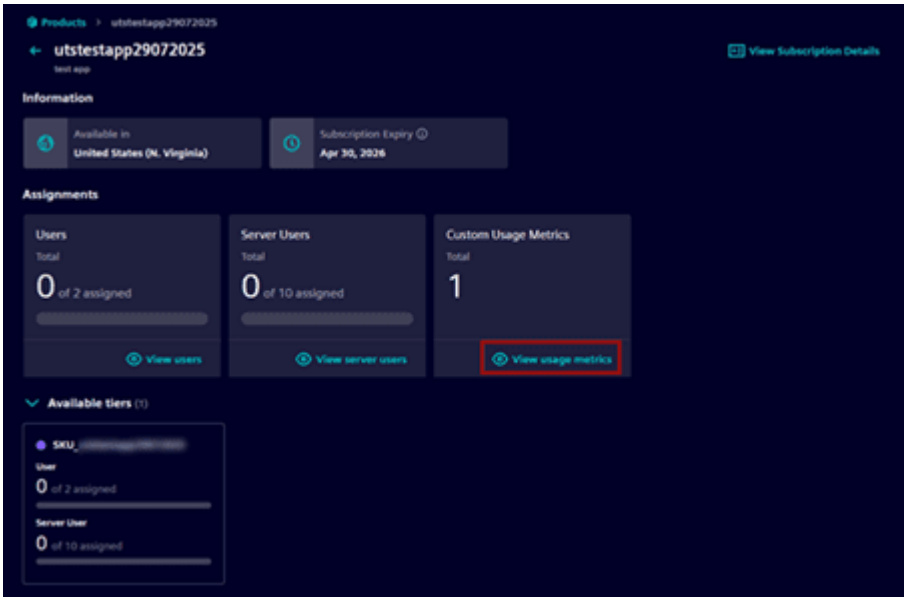
## Access Usage Details

To view usage details:

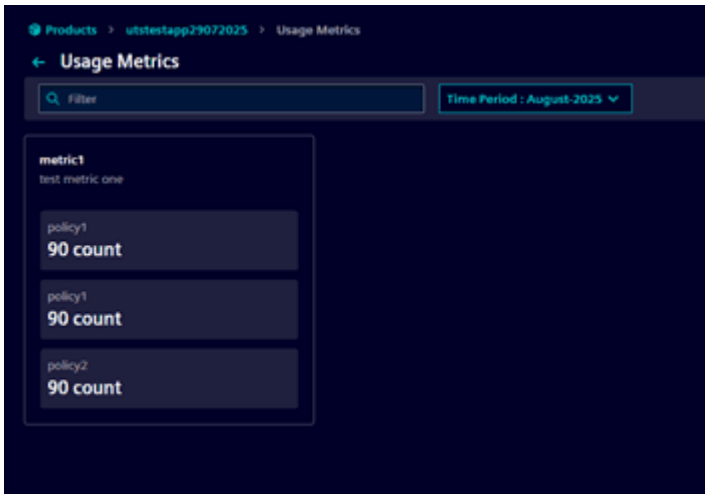
1. Go to the **Product** screen and select the product.
2. On the **Product Details** screen, click **View Details**.




3. In the **Product** overview page. Click **View usage metrics**.

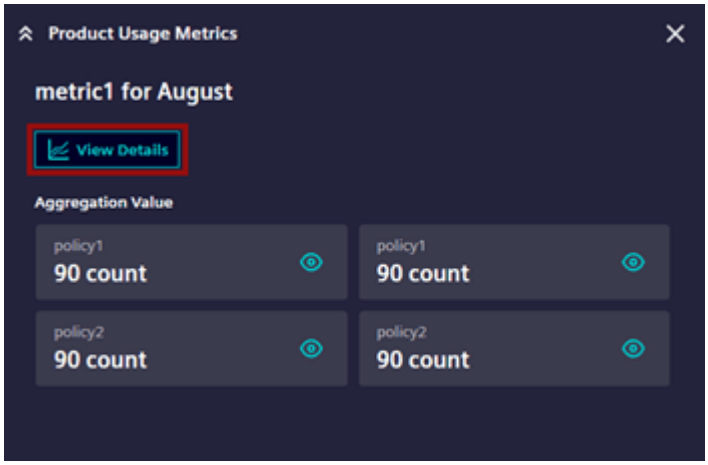



4. Select the time period and metric to view aggregation value policies.




> **Note**
>
> The current time period is selected by default.

5. In the **Product Usage Metrics** section, select **View Details** or click  button next to a specific aggregation value policy to view usage data.



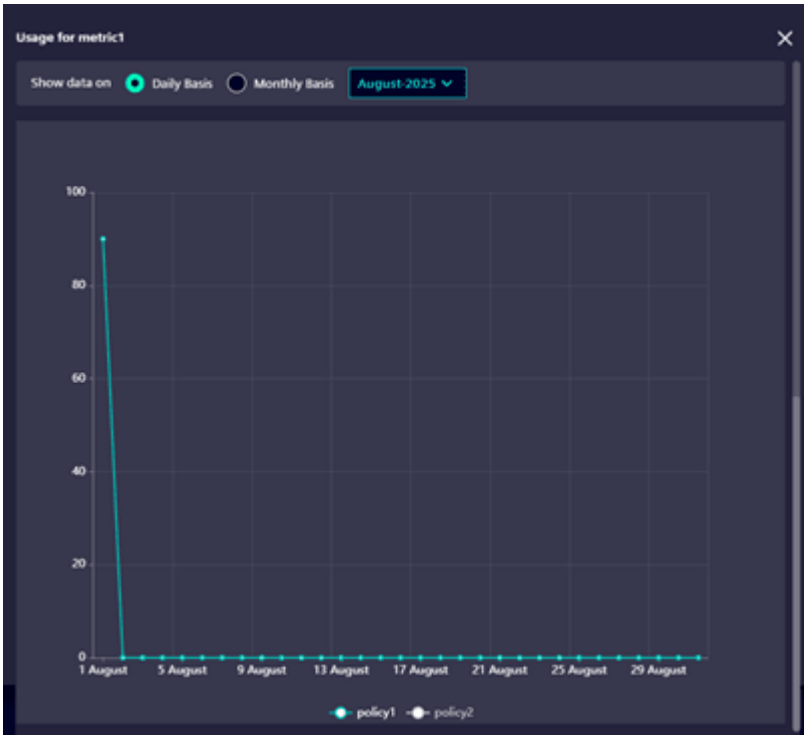

## View Product Usage History or Trend Graphs

The product usage history for a specific metric is viewed in a graphical format.

## Daily Product Usage History or Trend Graph

To view daily usage data:

1. In the pop-up, select **Daily Basis** option.
2. Select the desired month from the dropdown menu.



> **Note**
> You can view data for the current month and the previous two months.

The graph displays usage data on the y-axis and dates on the x-axis.

### Monthly Product Usage History or Trend Graph

To view monthly usage data:

1. In the pop-up, select **Monthly Basis** option.
2. Select the desired month from the dropdown menu.


> **Note**
> The current month is selected by default. The dropdown includes data for the last 13 months.

The graph displays usage data on the y-axis and months on the x-axis.

## Application Configuration

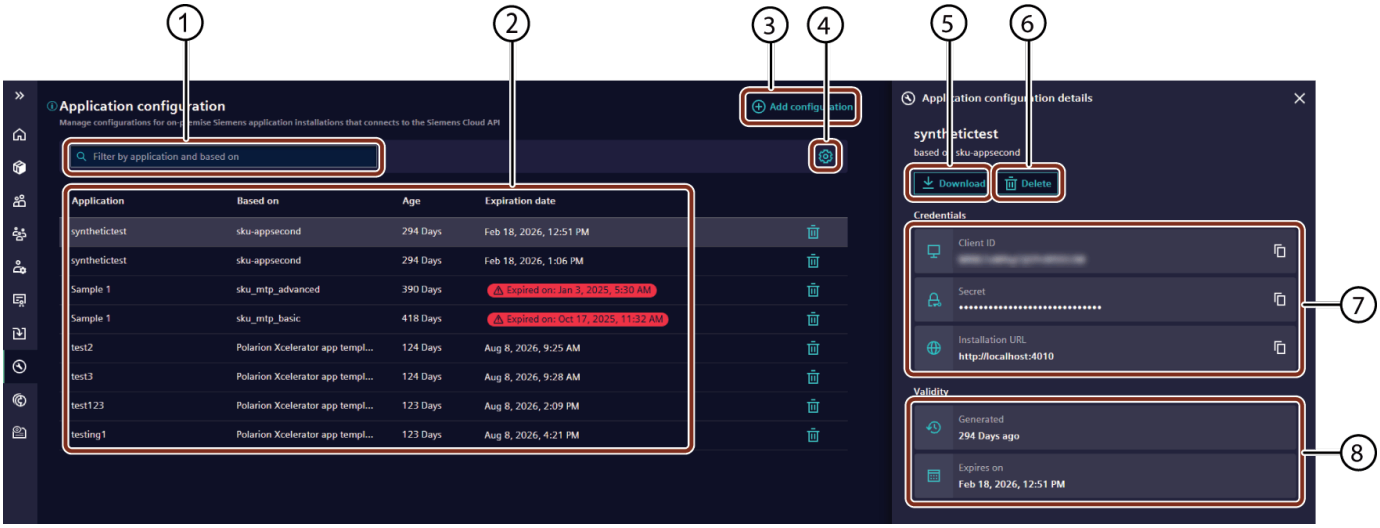
This section explains how to configure a product for desktop applications using predefined templates. Product teams can register templates that include approved scopes. These templates appear on the Add Configuration screen when a product is selected.

After configuring an application, the Siemens Xcelerator Admin Console generates client credentials (Client ID and Client Secret). These credentials are used to authenticate the desktop application.

**Note**

- Each template supports up to 15 product configurations.
- Product configuration functionality only supports desktop applications.

**Overview of the Application Configuration Screen**:




① Allows you to search application by name

② Displays a list of configured applications, including the application name, age and expiration date

③ Allows you to add a new application configuration

④ Allows you to customize the table list to display your preferred columns

⑤ Allows you to download credentials in `.txt` format

⑥ Allows you to delete an application configuration

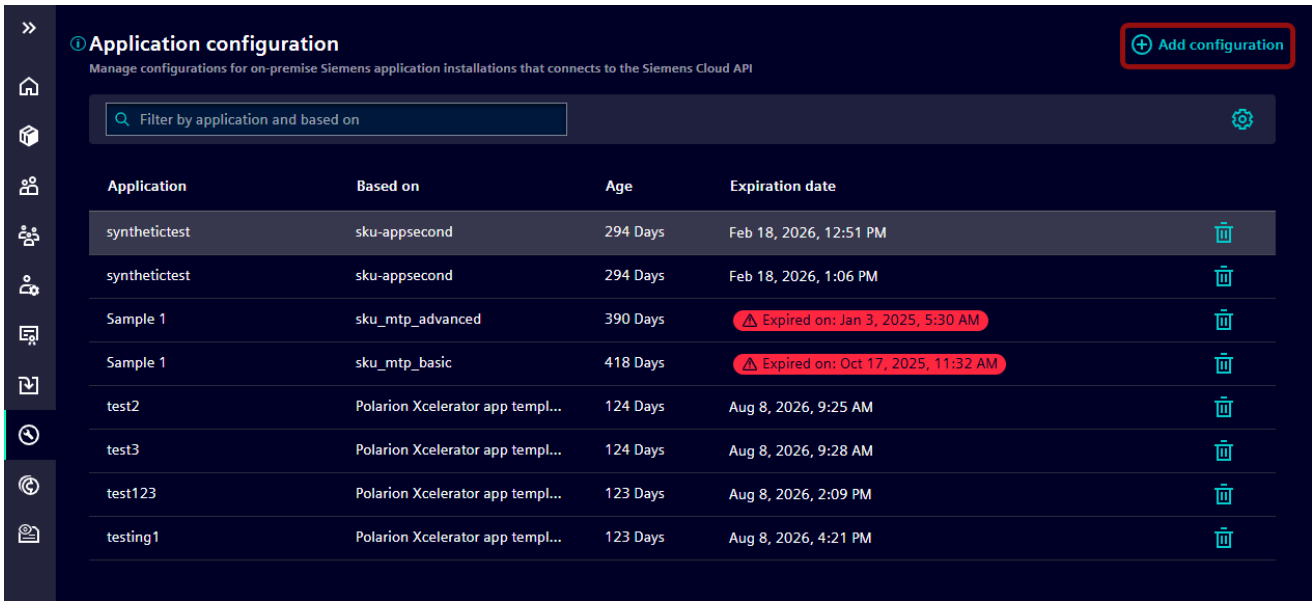
⑦ Shows the generated credentials (Client ID and Secret) and installation URL

⑧ Shows the validity details of the configured application

## Configure an Application

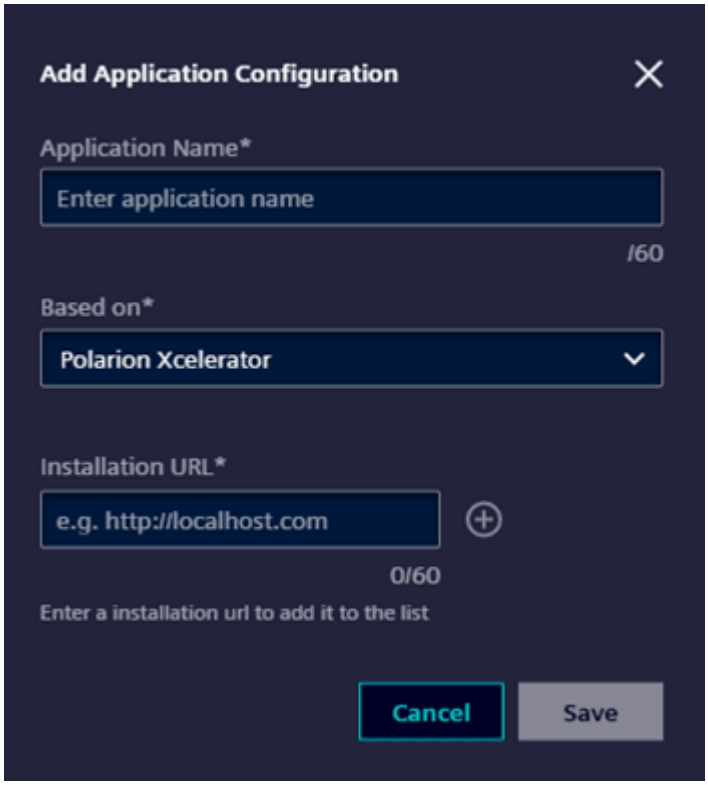
To configure an application:

1. Sign in to **Siemens Xcelerator Admin Console**.
2. Go to **Application configuration** in the left navigation pane.
3. Click **Add configuration**.




4. In the **Add Application Configuration** pop-up, enter the required fields:

| Parameters | Description |
|---|---|
| Application Name | Enter the name of the application. |
| Based on | Select the template from the drop-down list to create the application. |
| Installation URL | Enter the URLs to be added to list and click ⊕ |




5. Click **Save**.

The application is now configured.

After configuring the application, credentials (Client ID and Secret) are generated to authenticate your desktop application.

To copy or download credentials:

- In the **Application Configuration** list, select the configured application.
- Under **Application configuration details** section, copy the Client ID and Secret, Or click **Download** button to get credentials in `.txt` format.

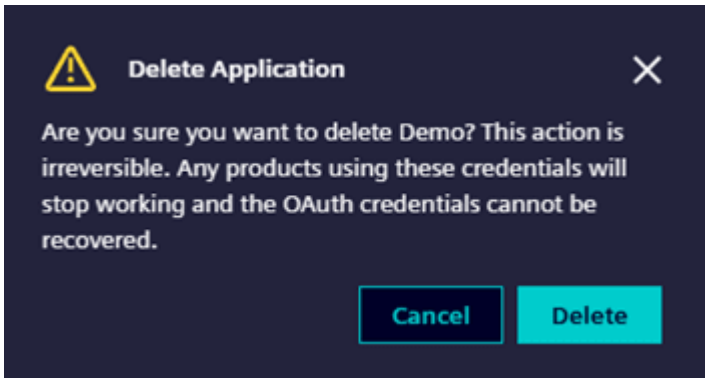
> **Note**
> The credentials have an expiration date that matches the product expiration date for the registered template. After expiration, you cannot download or use these credentials.

## Delete a Configured Application

To delete an existing configured application:

1. Select the configured application from the list, and click icon associated with that application.

2. In the **Delete Application** pop-up, click **Delete**.




The selected application configuration is now deleted from the Application Configuration screen.

# 8. Terms

## C

### Credits

A prepaid unit that allows customers to use services based on metered usage. Credits are deducted as services are used and can be refilled through purchases. They enable flexible, pay-as-you-go pricing models.

## E

### Enterprise Cloud Account (ECA)

This is the account that Siemens creates for you when you purchase a SaaS solution. You will use this account to manage the products and their users.

## H

### High Value Add-ons (HVAs)

High-value add-ons are special features offered in addition to the base tier functionalities and are sold separately based on customer needs.

## I

### Identity Provider (IdP)

An identity provider (IdP) is a system that creates, stores, and manages digital identities for users. IdPs can also authenticate users or provide authentication services to third-party services.

## T

## Tokens

A token is a unit-based licensing mechanism that enables concurrent (**floating**) licensing. Tokens are pooled and allocated to users to access a product feature, allowing multiple users to share a limited number of licenses. Once a user finishes their session, the token is released back into the pool for others to use.