



Proficiency User Account and Authentication (UAA)

User Documentation



Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of General Electric Company. Information contained herein is subject to change without notice.

© 2021, General Electric Company. All rights reserved.

Trademark Notices

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

Microsoft® is a registered trademark of Microsoft Corporation, in the United States and/or other countries.

All other trademarks are the property of their respective owners.

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:

doc@ge.com

Chapter 1. UAA Overview.....	4
About User Account and Authentication (UAA).....	4
Proficy UAA Install and Components.....	4
Log in to the UAA Configuration Tool.....	5
Chapter 2. Connectivity.....	7
Service Providers and Identity Providers.....	7
Group Mappings.....	7
UAA Group Mappings.....	7
Map Existing UAA Groups With Proficy UAA.....	8
Map LDAP Groups With Proficy UAA.....	10
Map SAML Groups With Proficy UAA.....	12
Chapter 3. Manage UAA Groups.....	17
About UAA Groups.....	17
Create UAA Groups.....	17
Delete Groups.....	18
Add or Remove Members from Groups.....	19
Chapter 4. Manage UAA Users.....	21
About UAA Users.....	21
Create UAA Users.....	21
Modify or Delete Users.....	22
Change Password.....	23
Reset Password for a User.....	23

Chapter 1. UAA Overview

About User Account and Authentication (UAA)

Proficy UAA (User Account and Authentication) provides identity-based security for Proficy based applications and APIs. It supports open standards for authentication and authorization, including OAuth2.

When a user is created or deleted in a product that uses Proficy UAA, the associated user account is created or deleted in the UAA instance, respectively.

Several Proficy products use Proficy UAA, including Historian, Plant Applications, and Operations Hub. To use Proficy UAA, you must install one of these products. Each product can install an independent instance of UAA, or it can reuse an existing instance of UAA which was previously installed by another Proficy product. When more than one product uses the same instance of Proficy UAA, this is called a shared or common UAA.

Shared UAA means that if you have a Proficy product installed that uses UAA, additional Proficy products installed after that initial product can also share that existing, already configured UAA architecture.

Proficy UAA can additionally be configured to use an external identity provider. This includes identity providers which use Lightweight Directory Access Protocol (LDAP) or Security Assertion Markup Language (SAML). When you integrate Proficy UAA with an external identity provider, you can provide the users and groups from that identity provider with access to Proficy products and their features.

Proficy UAA Install and Components






To use Proficy UAA, you must install one of the products which bundles Proficy UAA, such as Historian, Plant Applications, or Operations Hub. At the time of install, you can choose from the following options:

- **Creating a new instance of UAA:** Use this option if you are not currently using another UAA instance. For instance, use this option if you are installing your first Proficy product, or if the product you are installing is a stand-alone instance which does not need to share users and groups with another Proficy product.
- **Using an existing UAA:** Use this option if you are currently using an instance of Proficy UAA which contains users and groups that you want to reuse. For instance, use this option if you are already using Historian and you want to install Plant Applications and Operations Hub, and you

want your existing Historian users to have access to Plant Applications and Operations Hub. To use an existing instance of UAA, you must provide the details while installing Proficy UAA.

! Important: The decision of whether to share a UAA must be made at the time of product install; there is currently no post-install option to change what UAA a product is using, nor is there a utility to migrate users from one instance of UAA into another.

As part of install, a basic UI for configuring UAA is provided along with the instance of UAA. This includes a number of required services and other components. You can see the associated services when you open the services pane. These will start automatically after install.

	GE Operations Hub Httpd Reverse Pro...	This is an ins...	Running	Manual	NT SERVICE...
	GE Operations Hub UAA PostgreSQL ...		Running	Automatic	NT SERVICE...
	GE Operations Hub UAA Tomcat Web ...	This is an ins...	Running	Automatic	NT SERVICE...
	GE Security App Service	GE Security ...	Running	Automatic	Local System
	GE UAA External IdP Configuration Ser...	GE UAA LDA...	Running	Automatic	Local System

Note: Proficy UAA supports UAA version 4.30.0 or later.

Log in to the UAA Configuration Tool

The UAA Configuration Tool is a basic UI which can be used to perform UAA configuration tasks.

1. In a web browser, enter the `server name/securityadministrationapp`. Alternatively, you can use the shortcut provided on the desktop after installation.

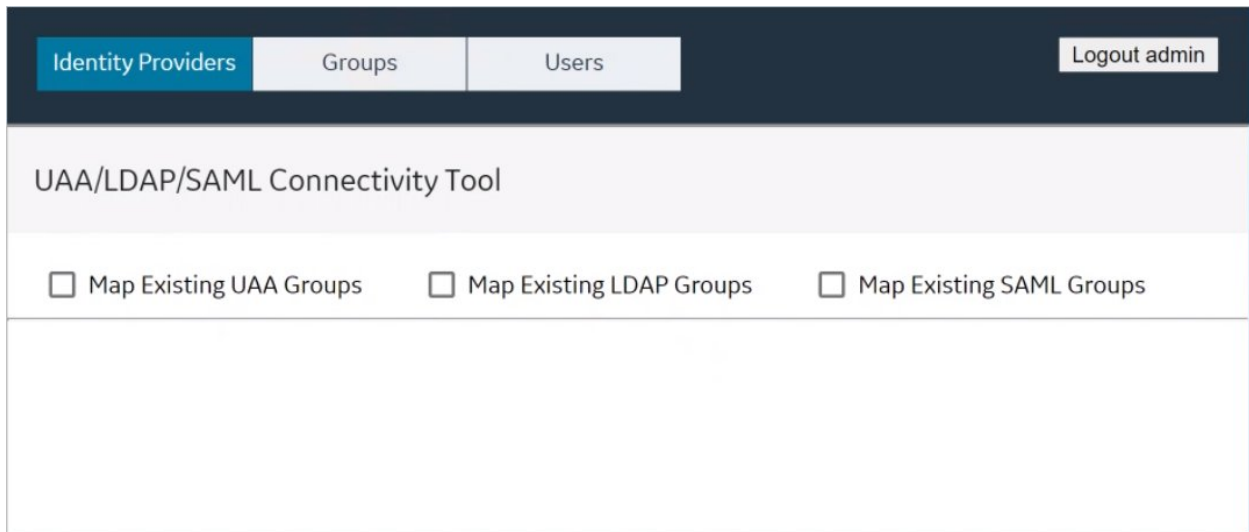


2. Log in with the client ID and client secret that you specified when you installed your Proficy product. Alternatively, you can provide the username and password of a user with sufficient privileges.



The UAA Configuration Tool home page appears. There are sections for configuring connectivity (including external identity providers), group management, and user management.

Note: After installing a product which uses Proficy UAA, you may see new entries in the groups and/or users areas.



Chapter 2. Connectivity

Service Providers and Identity Providers

When products use UAA, there is a distinction between two types of providers:

- **Service Provider (SP)** is the server that receives the assertion.
- **Identity Provider (IDP)** is the server that receives the authentication request, authenticates the user and sends the assertion to the SP.

Out of the box, Proficy UAA is configured to be an IDP. This means that you can create users and groups directly in Proficy UAA, and Proficy UAA will authenticate those users.

In addition, Proficy UAA can be configured to integrate with other Identity Providers, including LDAP Providers and SAML Providers. In these cases, Proficy UAA uses chained authentication – It will first attempt to authenticate a user against the UAA user store before it attempts authentication through the LDAP or SAML provider.

IDP integration can be configured in the Connectivity section of the UAA Configuration Tool.

Group Mappings

UAA Group Mappings

When a product with Proficy UAA is installed, it provisions Proficy UAA with the groups which the product uses. Access to the Proficy product and its features is managed in part by which of these UAA groups a user is a member of.

Users can gain membership to a UAA group by being directly added to the target group, or they can gain membership by being part of a group which is mapped to or a member of the target group. Two common cases for group mapping are:

- **UAA group to UAA group:** In the case of shared UAA, users of one Proficy product may be granted access to another Proficy product by mapping the UAA groups from the first product to UAA groups in the second product. One example of this is mapping Plant Application groups to Operations Hub groups.
- **External IDP group to UAA group:** In the case of external IDP integration, users in the external IDP may be granted access to a Proficy product by mapping the IDPs groups to the


product's Proficity UAA groups. One example of this is mapping LDAP groups to Operations Hub groups.

Group mapping and membership can be configured in the Connectivity section of the UAA Configuration Tool.

Map Existing UAA Groups With Proficity UAA

This topic describes the process to map existing UAA groups with Proficity UAA groups.



1. Double-click  on your desktop.
The icon appears on your desktop after you install Proficity UAA.
2. Select the **Identity Providers** tab.
The **UAA/LDAP/SAML Connectivity Tool** appears.
3. Select the **Map Existing UAA Groups** check box.
4. In the **UAA Connection** section, provide values as specified in the following table.

! **Important:** The values that you provide in this step must match the values that you provided while installing your Proficity product. These values are required to connect to the Proficity UAA.

Field	Description
URL	This information is read-only. The authorization server URL of the Proficity UAA server is populated by default. This is the UAA Base URL that you specified during installation.
Client ID	Enter the client ID of the Proficity UAA server that you specified for Admin Client ID during installation.
Client Secret	Enter the client secret configured for the OAuth client that you specified for Admin Client Secret during installation.

1 UAA Connection



URL *
https://operationshub:8443

Client ID *
admin

Client Secret *
admin123

Test Continue

5. Select **Test**.

If connection to the UAA server is established, a message appears, confirming the same.


6. Select **Continue**.

In the **UAA Mapping** section, the drop-down list box contains a list of groups in Proficity UAA. In the **Filter** box, a list of groups in the existing UAA instance appear.

7. In the drop-down list box, select the Proficity UAA group to which you want to map the existing UAA groups.

8. In the **Filter** box, select the check boxes corresponding to the existing UAA groups that you want to map.

 **Note:** If a group is already mapped to the Proficity UAA group that you have selected, the check box is already selected.

 **Tip:** Clear the check boxes corresponding to the UAA groups for which you want to remove the mappings.

9. Select **Map Members**.

A message appears, confirming that the Proficity UAA group is mapped to the existing UAA groups that you have selected.

10. Repeat steps 7-9 for all the Proficity UAA groups that you want to map.

The existing UAA groups are mapped with the Proficity UAA UAA groups.

Map LDAP Groups With Proficy UAA

If you want LDAP users to use Proficy UAA, you must map the corresponding LDAP groups with the Proficy UAA group created during the Proficy product installation.



1. Double-click **UAA IdP Configuration tool** on your desktop.
The icon appears on your desktop after you install Proficy UAA.
2. Select the **Identity Providers** tab.
The **UAA/LDAP/SAML Connectivity Tool** appears.
3. Select the **Map Existing LDAP Groups** check box.
4. In the **UAA Connection** section, provide values as specified in the following table.

! **Important:** The values that you provide in this step must match the values that you provided while installing your Proficy product. These values are required to connect to the Proficy UAA. Proficy UAA works only with a single instance of UAA, which is specified during Proficy UAA installation. After installation, you cannot change the instance of UAA that Proficy UAA will use.

Field	Description
URL	This information is read-only. The authorization server URL of the Proficy UAA server is populated by default. This is the UAA Base URL that you specified during installation.
Client ID	Enter the client ID of the Proficy UAA server that you specified for Admin Client ID during installation.
Client Secret	Enter the client secret configured for the OAuth client that you specified for Admin Client Secret during installation.

5. Select **Test**.
If connection to the UAA server is established, a message appears, confirming the same.

📌 Note: Currently, the Test Button displays a successful connection for LDAP even when no security certificate or a bad certificate is found.

6. In the **LDAP Connection** section, provide values as specified in the following table.

Field	Description
URL	Enter the base URL of the LDAP server (for example, https://localhost).

Field	Description
Bind User DN	Enter the distinguished name of the bind user (for example, cn=admin,ou=Users,dc=test,dc=com).
Password	Enter the password for the LDAP user ID that searches the LDAP tree for user information.
Skip SSL Verification (UAA restart required)	Select this check box if you do not have the certificate to access the LDAP server. Messages are still encrypted, but the certificate is not verified for correctness. Do not select this option if you are not confident of the direct connection to the LDAP server; it could result in redirected traffic outside of your controlled network.
User Search Filter	Enter the subdirectories to include in the search (for example, cn={0}).
User Search Base	Enter the starting point for the LDAP user search in the directory tree (for example, dc=developers,dc=com).
Group Search Base	Enter the starting point for the LDAP group search in the directory tree (for example, ou=scopes,dc=developers,dc=com).
Max Group Search Depth	Enter a value to define the maximum depth for searching LDAP groups. (This may impact performance for very large systems.) By default this value is 10.
Group Search Filter	Enter the subdirectories to include in the search (for example, member={0}).

UAA/LDAP/SAML Connectivity Tool

Map Existing UAA Groups
 Map Existing LDAP Groups
 Map Existing SAML Groups

1 UAA Connection

2 LDAP Connection

Base url *	user search base *
ldap://localhost:389/ 🔒	dc=test,dc=com
bind user dn *	user search filter *
cn=admin,dc=test,dc=com	cn={0}
password *	group search base *
<input checked="" type="checkbox"/> Skip SSL verification (UAA restart required)	max group search depth *
	10
	group search filter *

7. Select **Test**, and then select **Submit**.

If connection to the LDAP server is established, a message appears, confirming the same.

8. Select **Test** again, and then select **Continue**.

In the **LDAP Mapping** section, the drop-down list box contains a list of groups in Proficy UAA.

- In the drop-down list box, select the Proficy UAA group to which you want to map LDAP groups. You can also search for a group in the **LDAP Groups Search Filter** box. When searching, be sure to use the standard LDAP query language for your search.

3 LDAP Mapping

UAA Group * ▼

LDAP Groups Search Filter
(objectclass=*)

Search

ldapGroups

<input type="checkbox"/>	DC=ophub,DC=internal
<input type="checkbox"/>	CN=Users,DC=ophub,DC=internal
<input type="checkbox"/>	CN=Computers,DC=ophub,DC=internal
<input type="checkbox"/>	OU=Domain Controllers,DC=ophub,DC=internal
<input type="checkbox"/>	CN=System,DC=ophub,DC=internal

Map Groups

Back

Continue

 **Note:** If a group is already mapped to the Proficy UAA group that you have selected, the check box is already selected.

10. Select **Map Groups**.

A message appears, confirming that the LDAP groups are mapped to the Proficy UAA group.


- Repeat steps 8-10 for all the Proficy UAA groups that you want to map.

The LDAP groups are mapped with the Proficy UAA groups.

Map SAML Groups With Proficy UAA

If you want SAML users to use Proficy UAA, you must map the corresponding SAML groups with the Proficy UAA group created during the Proficy product installation.



1. Double-click  on your desktop.
The icon appears on your desktop after you install Proficy UAA.
2. Select the **Identity Providers** tab.
The **UAA/LDAP/SAML Connectivity Tool** appears.
3. Select the **Map Existing SAML Groups** check box.
4. In the **UAA Connection** section, provide values as specified in the following table.

! **Important:** The values that you provide in this step must match the values that you provided while installing your Proficy product. These values are required to connect to the Proficy UAA. Proficy UAA works only with a single instance of UAA, which is specified during installation. After installation, you cannot change the instance of UAA that Proficy UAA will use.

Field	Description
URL	This information is read-only. The authorization server URL of the Proficy UAA server is populated by default. This is the UAA Base URL that you specified during installation.
Client ID	Enter the client ID of the Proficy UAA server that you specified for Admin Client ID during installation.
Client Secret	Enter the client secret configured for the OAuth client that you specified for Admin Client Secret during installation.

5. Select **Test**.

Map Existing UAA Groups
 Map Existing LDAP Groups
 Map Existing SAML Groups

1 UAA Connection

URL *
https://localhost

Client ID *
admin


Client Secret *

✓ Successfully Connected

If connection to the UAA server is established, a message appears, confirming the same.

6. In the **Existing SAML Identity Provider** section, select the Identity Provider.
7. Click **Show IDP Details**, or **Create New IDP** and provide values as specified in the following table.

Field	Description
Metadata Location	Specify the SAML Metadata – either an XML string or a URL that will deliver XML content. Optionally, you can select Instead Upload Metadata Xml to enter the metadata location using a file you downloaded from your SAML Identity Provider.
Name	Specify the name of your SAML provider.
Origin Key	Specify the unique alias for the SAML provider.
SAML Group Attribute Names	Specify the names of the attributes that contain the group membership information about a user in a SAML assertion.
NameID	Optionally, enter a SAML Name ID and associated fields that you want to use in a Link Test.
Link Text	Specify the text you want to appear in a link test.
Enable SAML Link	Select this check box to enable the SAML Link; clear to disable.

 **Note:** It is recommended to use the same Name and Origin Key (not mandatory).

Existing SAML IdentityProviders

oktalocal

Show IDP Details Create New IDP

metaDataLocation *

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor entityID="http://ww
```

[↑ Instead upload metadata xml](#)

Name *

oktalocal

OriginKey *

oktalocal

SAML Group Attribute Names

iqp

nameID *

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

linkText *

HarshaLabs

Enable SAML Link

Delete IDP Back Update

8. Select **Add** or **Update** to save your changes.

i **Tip:** Click **Delete IDP** to remove the existing IDP, and instead create a new one (using the Create New IDP button).

The **SAML Mapping** screen appears.

9. In the drop-down list box, select the Proficiency UAA group to which you want to map SAML groups.

10. Enter a **SAML Group** and click **Add Group**. Repeat this step for each SAML group you want to add.

The screenshot shows a configuration page for SAML Mapping. On the left, a vertical navigation pane contains three items: 'UAA Connection' (checked), 'Saml Connection' (checked), and 'SAML Mapping' (selected with a '3' in a circle). The main content area is a form with the following elements:

- A dropdown menu labeled 'UAA Group *' with the value 'uaamygroup' selected.
- A text input field labeled 'SAML Groups' which is currently empty.
- An 'Add Group' button located below the 'SAML Groups' input field.
- A 'Map Groups' button located at the bottom left of the form.
- 'Back' and 'Continue' buttons located at the bottom right of the form.

11. When finished adding SAML groups, click **Map Groups**.

12. Next, select **Continue** to complete.

A message appears, confirming that the SAML groups are mapped to the Proficiency UAA group.

Chapter 3. Manage UAA Groups

About UAA Groups

If you design your application to authorize using specific scopes, you can create groups corresponding to those scopes in UAA and assign users to those groups. When the users log into your web application, the application redirects them to UAA. If a user is in the specified group and you chose to authorize the web application with that scope, the web application gets a signed token that contains that scope.

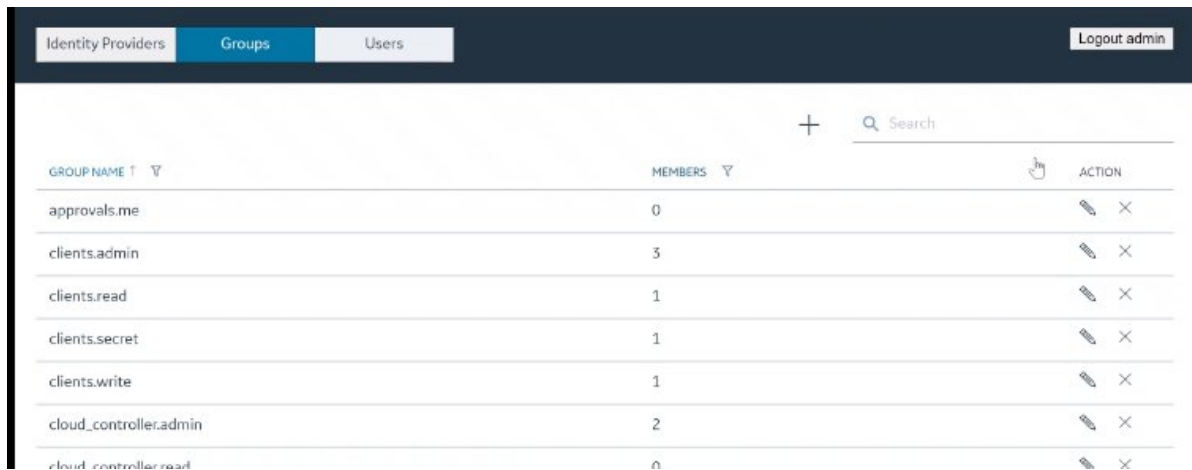
A user can belong to more than one group. For example, a user can belong to a Historian UAA group as well as a Plant Apps UAA group, each providing access to their respective products.















You can add groups and manage group membership users in Proficy UAA.

Create UAA Groups

As an administrator, you can create new UAA groups based on your requirement. Example: You can create a group for the users who perform the same task on the same resource. You can have a group of supervisors for each line such as, Supervisors_LineA, Supervisors_LineB, Supervisors_LineC.

1. Select **Groups**.



GROUPNAME ↑ ▾	MEMBERS ▾	ACTION
approvals.me	0	 
clients.admin	3	 
clients.read	1	 
clients.secret	1	 
clients.write	1	 
cloud_controller.admin	2	 
cloud_controller.read	0	 

The **Groups** page appears, displaying the list of the previously created groups.

2. Select **+**.

The **Add Group** window appears.

3. In the **GROUP NAME** text box, enter a name for the group.
4. In the **DESCRIPTION** text box, enter a description for the group.
5. Select **Add**.

The group is created and added to the list of groups on the **Groups** page.

Delete Groups

1. Select **Groups**.

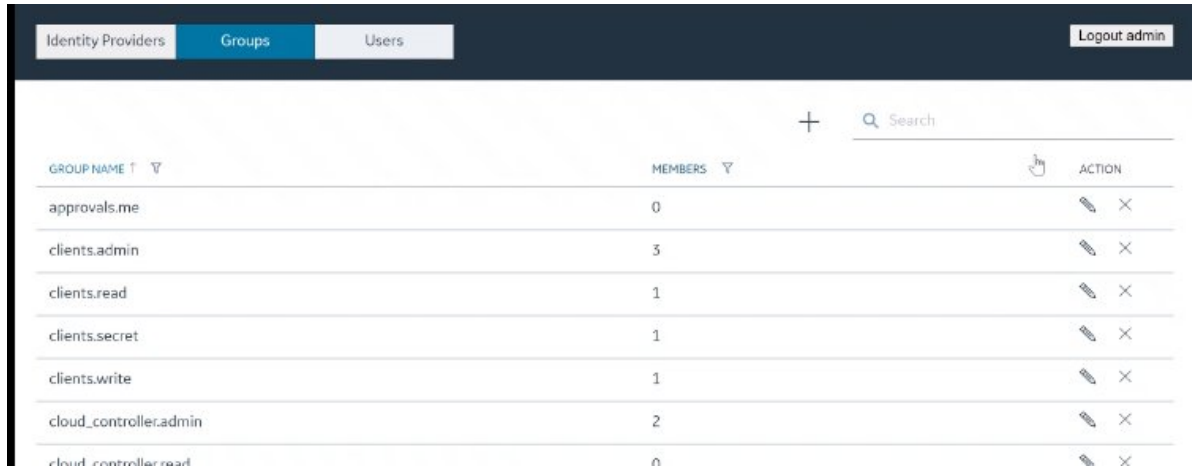
GROUP NAME	MEMBERS	ACTION
approvals.me	0	
clients.admin	3	
clients.read	1	
clients.secret	1	
clients.write	1	
cloud_controller.admin	2	
cloud_controller.read	0	

The **Groups** page appears, displaying the list of groups.

2. In the row containing the group that you want to delete, select .

Add or Remove Members from Groups

1. Select **Groups**.



GROUP NAME ↑ ▾	MEMBERS ▾	ACTION
approvals.me	0	
clients.admin	3	
clients.read	1	
clients.secret	1	
clients.write	1	
cloud_controller.admin	2	
cloud_controller.read	0	

The **Groups** page appears, displaying the list of groups.

2. In the row containing the group that you want to modify, select .



< Back Group Details

Group Name uaamygroup Members 0

Members

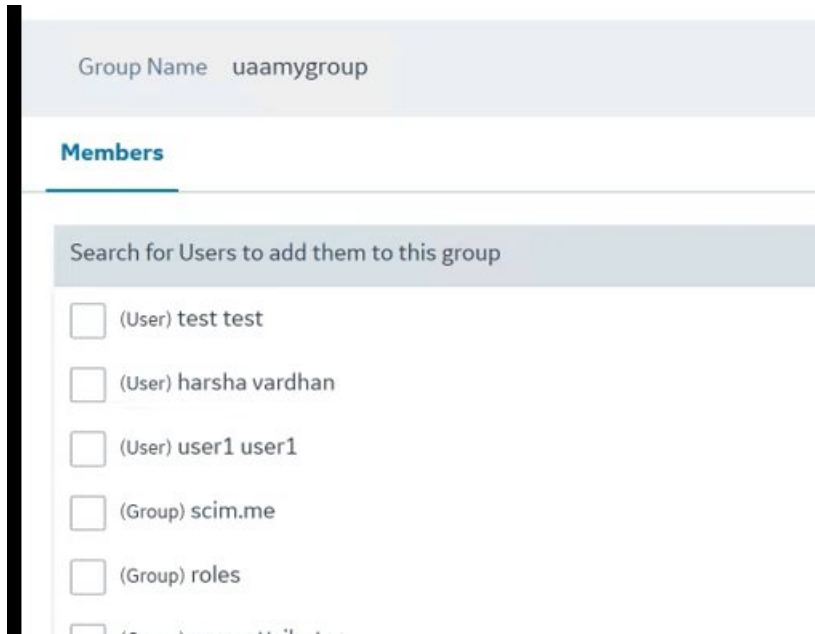
Search for Users to add them to this group +

Search

MEMBER NAME ↑ ▾	DISPLAY NAME ▾	ACTION
-----------------	----------------	--------

The **Members** page appears, displaying the members added to the group.

3. Select **Search for Users to add to this group**.



The list of available users and groups appears.

4. Select the check box next to each user or group that you want to add.

5. To add the members to the group, select **+**.

The members (users or groups) are added to the group. The count of the total members of the group is updated.

6. To delete a member from the group, select **X** in the row containing the member you want to delete.

The member is deleted from the group. The count of the total members of the group is updated.

! **Important:** Exercise caution in modifying the membership of a user because it is possible for a user to remove their privileges to access Proficy UAA, including the user management section, thus preventing themselves from accessing Proficy UAA.

Chapter 4. Manage UAA Users

About UAA Users

The user is an individual with privileges for your Proficy application.

You can create users locally in UAA for authentication and assign them to the required groups from the UAA Configuration Tool.

Users can added to Proficy UAA in two ways:

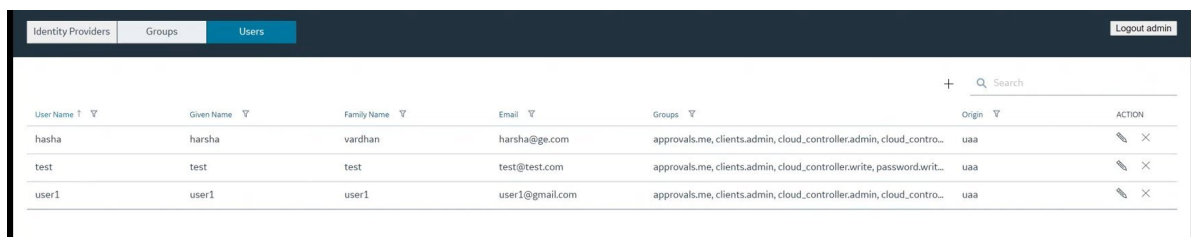
- **Directly adding users:** You can create a new user using the UAA Configuration Tool, or using any UI provided by a product which uses Proficy UAA.
- **Mapping existing user groups:** If you have user groups in an existing UAA instance, LDAP service, or SAML service, you can map these groups with the Proficy UAA group. The users of these groups can then use Proficy UAA.

You can directly add users to Proficy UAA by accessing the Users section of the UAA Configuration Tool.

Create UAA Users

As an administrator, you can create new UAA users based on your requirements.

1. Select **Users**.



User Name	Given Name	Family Name	Email	Groups	Origin	ACTION
hasha	harsha	vardhan	harsha@ge.com	approvals.me, clients.admin, cloud_controller.admin, cloud_contro...	uaa	
test	test	test	test@test.com	approvals.me, clients.admin, cloud_controller.write, password.writ...	uaa	
user1	user1	user1	user1@gmail.com	approvals.me, clients.admin, cloud_controller.admin, cloud_contro...	uaa	


The **Users** page appears, displaying the list of the previously created users.

2. Select **+**.

The **Add User** window appears.







3. Enter a user name, password, first name, last name, and email for the user.
4. Select **Add**.

The user is created and added to the list of users on the **Users** page.


 **Note:** Users who originate in UAA can be immediately seen after creation in the users list. Users who originate in LDAP or SAML need to successfully log in to UAA first. Upon a successful log in, a shadow UAA user is created and can be subsequently seen in the UAA users list.

Modify or Delete Users

1. Select **Users**.

User Name	Given Name	Family Name	Email	Groups	Origin	ACTION
hasha	harsha	vardhan	harsha@ge.com	approvals.me, clients.admin, cloud_controller.admin, cloud_contro...	uaa	 
test	test	test	test@test.com	approvals.me, clients.admin, cloud_controller.write, password.writ...	uaa	 
user1	user1	user1	user1@gmail.com	approvals.me, clients.admin, cloud_controller.admin, cloud_contro...	uaa	 

The **Users** page appears, displaying the list of the previously created users.

2. In the row containing the group that you want to modify, select  and enter your changes.

- To delete a user, select **X** in the row containing the user you want to delete.
The user is deleted from the group. The count of the total members of the users is updated. The count of the total members of users is updated.

Note: Only users who originate in UAA can be edited or deleted. Users who originate from an external Identity Provider such as LDAP or SAML can be seen but not edited or deleted.

Change Password

UAA local users can log in to their accounts and change password.

You must know your current password to log in to UAA and change it.

- Log in to UAA on a web browser.
- Go to your **Account Settings** screen.
- Select **Change Password**.
- Provide the following information:

Current password	Enter the password that is currently used for UAA login.
New password	Enter a new password to replace the current password.
Confirm new password	Enter the new password again for confirmation.

- Select **CHANGE PASSWORD**.


The password is changed successfully.

Reset Password for a User

Administrators can reset the password for UAA users.

You must have administrator access to log in to the application.




- Double-click  on your desktop.
The icon appears on your desktop after you install Proficy UAA.

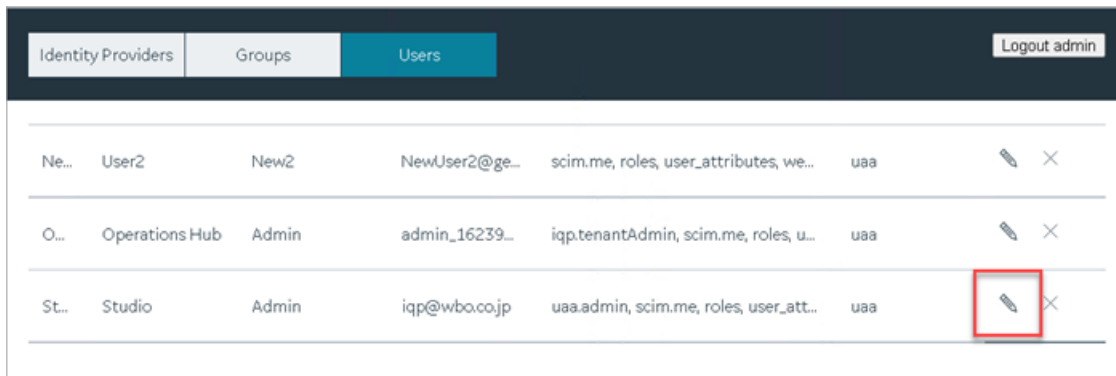
2. Log in to UAA using `admin` account.







3. Select the **Users** tab.

The list of all UAA users appears.

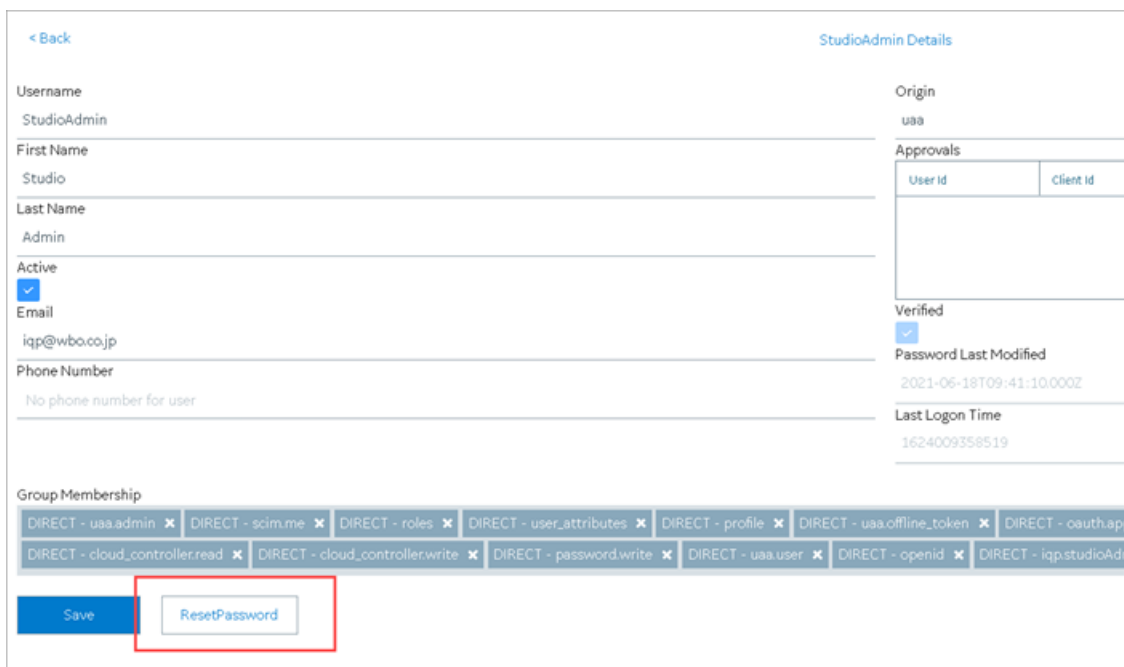
4. Select  for the username you want to reset the password.

The pencil icon to edit the respective user is available under the **Action** column.



Identity Providers	Groups	Users	Logout admin			
Ne...	User2	New2	NewUser2@ge...	scim.me, roles, user_attributes, we...	uaa	 
O...	Operations Hub	Admin	admin_16239...	iqp.tenantAdmin, scim.me, roles, u...	uaa	 
St...	Studio	Admin	iqp@wbo.co.jp	uaa.admin, scim.me, roles, user_att...	uaa	 

5. Select **Reset Password**.



[< Back](#) StudioAdmin Details

Username: StudioAdmin Origin: uaa

First Name: Studio Approvals

Last Name: Admin User Id: Client Id

Active: Verified:

Email: iqp@wbo.co.jp Password Last Modified: 2021-06-18T09:41:10.000Z

Phone Number: No phone number for user Last Logon Time: 1624009358519

Group Membership

DIRECT - uaa.admin x DIRECT - scim.me x DIRECT - roles x DIRECT - user_attributes x DIRECT - profile x DIRECT - uaa.offline_token x DIRECT - oauth.ap... x

DIRECT - cloud_controller.read x DIRECT - cloud_controller.write x DIRECT - password.write x DIRECT - uaa.user x DIRECT - openid x DIRECT - iqp.studioAd...

6. Enter a new password for the user and confirm the new password.

7. Select **RESET PASSWORD**.

Password: *

.....

Confirm Password: *

.....

Cancel RESET PASSWORD

The password for the user is reset successfully.