



GE VERNOVA

PROFICY® SOFTWARE & SERVICES

PROFICY AUTHENTICATION

User Guide

Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, GE Vernova 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 GE Vernova. Information contained herein is subject to change without notice.

© 2024 GE Vernova and/or its affiliates. All rights reserved.

Trademark Notices

“VERNOVA” is a registered trademark of GE Vernova. “GE VERNOVA” is a registered trademark of GE Aerospace exclusively licensed to GE Vernova. The terms “GE” and the GE Monogram are trademarks of GE Aerospace, and are used with permission. All other trademarks are the property of their respective owners.

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

Proficiency Authentication

Contents

- Chapter 1. Proficy Authentication 4**
- About Proficy Authentication..... 4
- Set up Proficy Authentication..... 4
- Get Started With Proficy Authentication..... 10
- Manage Identity Providers..... 15
 - LDAP..... 15
 - SAML..... 24
 - Enable Multi-Factor Authentication..... 48
 - Delete Identity Provider..... 51
- Manage Groups..... 52
 - Overview of Managing Groups in Proficy Authentication..... 52
 - Create Groups..... 58
 - Modify Groups..... 60
 - Map Groups..... 61
 - Add/Remove Users in a Group..... 64
 - Add/Remove Sub-Groups in a Group..... 65
 - Delete Group..... 66
- Manage Users..... 67
 - Create Users..... 67
 - Add/Remove Groups for a User..... 69
 - Reset User Password..... 71
 - Delete User..... 72
- Windows Integrated Authentication / Auto-login..... 73
 - Configure Security Policy..... 76
 - Create Service Principal Name..... 78
 - Generate Keytab File..... 81
 - Proficy Authentication Service Configuration..... 84

Configure Browser.....	85
Example Configuration for Multi-domain and Auto-login Functionality.....	86
High Availability.....	89
Configure High Availability for Proficy Authentication.....	89
Configure iSCSI Target.....	91
Configure iSCSI Initiator.....	91
Create a Virtual Disk.....	94
Initialize a Virtual Disk.....	95
Create a Cluster.....	97
Configure Role.....	102
Configure Proficy Authentication Installation.....	107
Prerequisites for Installing Operations Hub with External Proficy Authentication.....	112
Customize Login Screen.....	117
Backup and Restore.....	119
Back Up the Proficy Authentication Database.....	119
Restore the Proficy Authentication Database.....	121
Troubleshooting Proficy Authentication.....	121
Error 431: Request Header Fields Too Large.....	121
Windows Auto-login Error Logs.....	122
Issue: Duplicate LDAP User Creation in Proficy Authentication Database.....	129

Chapter 1. Proficy Authentication

About Proficy Authentication

Proficy Authentication (UAA) provides identity-based security for Proficy based applications and APIs. It supports open standards for authentication and authorization, including OAuth2. Proficy Authentication is designed to operate on a cloud-native architecture, aligning with Cloud Foundry's principles for agility and efficiency. Visit [Cloud foundry](#) for more information. Organizations can easily deploy, manage, and scale Proficy Authentication within the Cloud Foundry environment, streamlining the operational aspects of authentication and access management. The application also offers a secure and efficient user authentication experience, making it ideal for mission-critical applications where reliability is paramount.

Several Proficy products use Proficy Authentication, including Historian, Plant Applications, and Operations Hub. You can configure Proficy Authentication from within Configuration Hub.

Proficy products can share an existing common Proficy Authentication (UAA) instance, which allows for all products to use a central User store for authentication and authorization.

Proficy Authentication can be configured to collaborate with external identity providers that use these two common protocols:

- Lightweight Directory Access Protocol (LDAP)
- Security Assertion Markup Language (SAML)

When Proficy Authentication is integrated with an external identity provider, it enables users and groups managed by that provider to access Proficy products and features. This means that the authentication and authorization established by the external identity provider extend to various services within the ecosystem.

OAuth is designed as an authorization protocol permitting a user to share access to specific resources with a service provider.


Benefits of using OAuth:

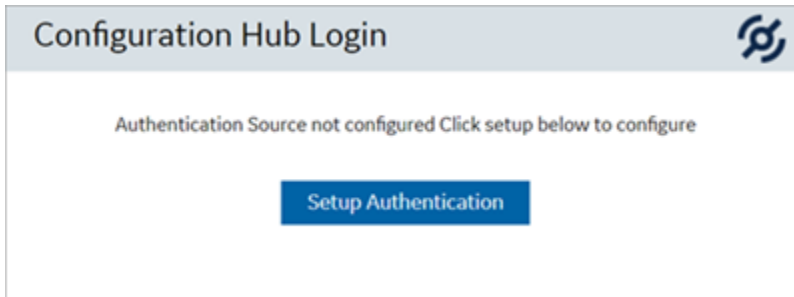
- Enables third-party application access
- Controlled access to APIs
- Adaptable and flexible user interactions

Set up Proficy Authentication

This topic describes how to set up Proficy Authentication in Configuration Hub.

The following steps describe how to set up Proficy Authentication in Configuration Hub. Setting up authentication provides access to all the products (Historian, iFIX) registered with Configuration Hub. You use the same Proficy Authentication server to authenticate.

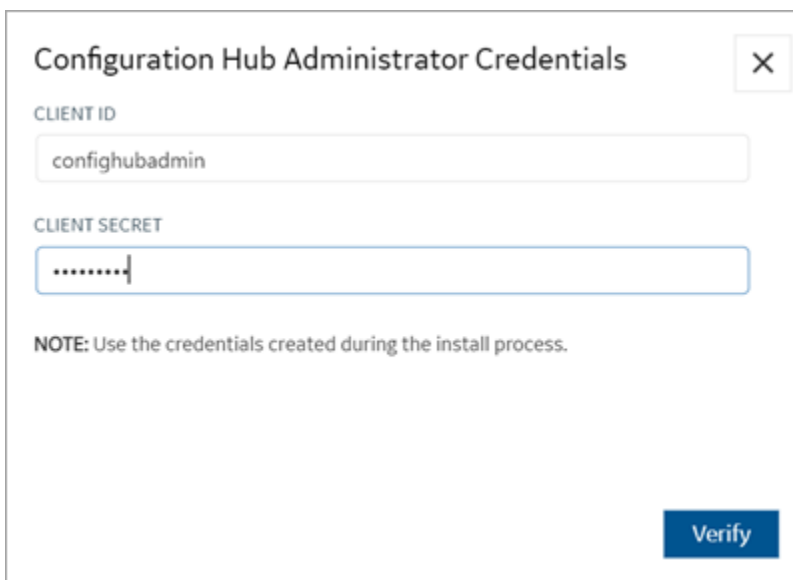
1. Double-click  desktop icon to launch the Configuration Hub application.
2. Select **Setup Authentication**.



The **Configuration Hub Administrator Credentials** screen appears.

3. Enter the details for logging in to the Configuration Hub application.

Field	Description
Client ID	The client ID provided during installing Configuration Hub. Example: <code>con-fighubadmin</code>
Client Secret	The client secret provided during installing Configuration Hub.



4. Select **Verify**.


If the credentials are correct, the **Register with Proficy Authentication** screen appears.

5. Provide these details to configure the Proficy Authentication application.

These fields are populated automatically if you opted for installing Proficy Authentication along with Configuration Hub. You have the option to edit and update the details.

Field	Description
Server Name (Fully Qualified Name)	<p>The host name of the machine where Proficy Authentication is installed.</p> <p>Enter a fully qualified domain name. For example, <code>desktop-sahfg5f.logon-.ds.ge.com</code></p> <p>Refer to step 6 to establish a trust with this server connection.</p>
Server Port	<p>The port number to communicate with the host machine. The default port where UAA is installed is <code>443</code>.</p> <p>The server connection is automatically tested on entering the port. You can also select Test to test the connection.</p>
Use Configuration Hub Administration credentials for Proficy Authentication	<p>Select this check box to populate the same login credentials you entered for Configuration Hub Admin account.</p> <p>If you want to use unique login credentials for Proficy Authentication, clear the check box and enter CLIENT ID and CLIENT SECRET.</p>
Client ID	<p>The administrator client identifier that has permission (authority) to log in to Proficy Authentication.</p>
Client Secret	<p>The administrator client secret to log in to Proficy Authentication.</p>

Register with Proficy Authentication ✕

SERVER NAME (FULLY QUALIFIED NAME)
  [Not trusted](#)

SERVER PORT

Proficy Authentication Credentials

Use Configuration Hub Administration credentials for Proficy Authentication

CLIENT ID

CLIENT SECRET

NOTE: Use the credentials created during the install process.

6. Select **Not trusted** to establish a trust connection between Configuration Hub and Proficy Authentication.
The **Certificate Details** screen appears.


Certificate Details

Attribute Name	Root Certificate
Subject	CN=SACHINAUTHGUARD Root CA 202112241544, OU=Operations Hub Site, O=GE Customer
Thumbprint	0B8B85FDA172C1DCF7A6C48F127085EF1338119C
Serial Number	3F678CC3732C8A69
Issuer	CN=SACHINAUTHGUARD Root CA 202112241544, OU=Operations Hub Site, O=GE Customer
Valid From	2021-12-24 00:00:00 GMT
Valid To	2026-12-23 00:00:00 GMT

7. Select **Trust**.

The trusted certificate(s) are added to the windows store on the machine where Configuration Hub is installed.

Register with Proficy Authentication ✕

SERVER NAME (FULLY QUALIFIED NAME)
  **Trusted**

SERVER PORT

Proficy Authentication Credentials

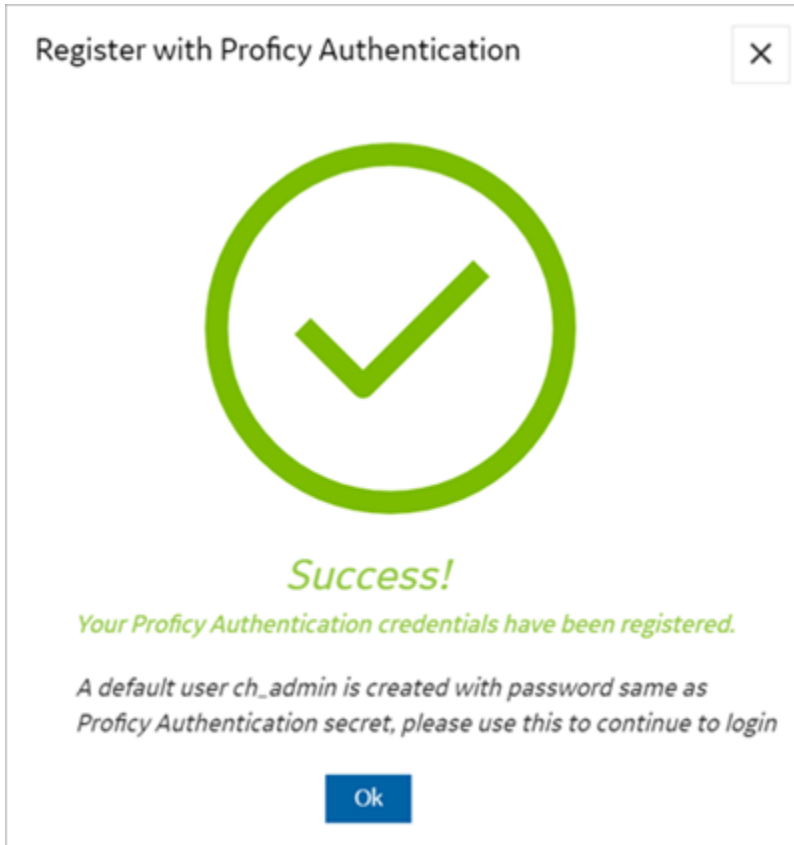
Use Configuration Hub Administration credentials for Proficy Authentication

CLIENT ID

CLIENT SECRET

NOTE: Use the credentials created during the install process.

8. Select **Register**.



9. Select **Ok**.

The **Configuration Hub Login** screen appears.

Configuration Hub is set up as a client for Proficy Authentication. The following default user is created to log in to the Configuration Hub application.

User ID	Password
ch_admin	The client secret you entered for Proficy Authentication.

Log in to Configuration Hub and perform operations related to Proficy Authentication.

Get Started With Proficy Authentication

This topic helps you to get started with the application.

Proficy Authentication provides identity-based security for Proficy based applications and APIs.

You can perform the following tasks in Proficy Authentication:

- Configure UAA/LDAP ([on page 15](#))/SAML ([on page 24](#)) identity providers
- [Create new user accounts \(on page 67\)](#)
- [Create new group accounts \(on page 58\)](#) and add users/other groups as members
- Perform UAA/LDAP/SAML [group mapping \(on page 61\)](#)

Task Roadmap

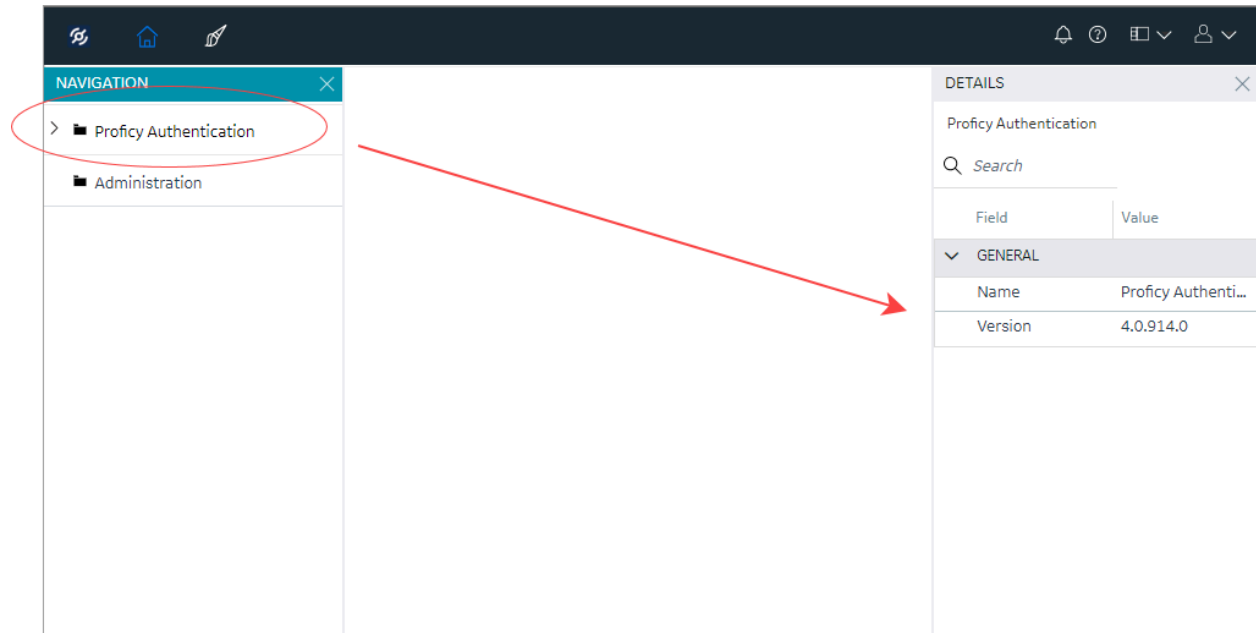
The roadmap is designed to guide you through a sequence of task workflows within Proficy Authentication.

#	Task	Description
1	Install and set up Proficy Authentication.	Set up Proficy Authentication (on page 4)
2	Enhance security by implementing multi-factor authentication.	Enable Multi-Factor Authentication (on page 48)
3	(Optional) For seamless user experience, consider implementing auto-login. But make sure that your system operates within a trusted network to reduce the risk of unauthorized access.	Windows Integrated Authentication / Auto-login (on page 73)
4	(Optional) For continuous, reliable, and scalable access to authentication and authorization systems, consider implementing high availability.	Configure High Availability for Proficy Authentication (on page 89)
5	Define scopes and permissions to control access to resources.	Overview of Managing Groups in Proficy Authentication (on page 52)
6	Develop a backup and recovery plan to ensure data integrity and availability.	Backup and Restore (on page 119)

Check Installed Version

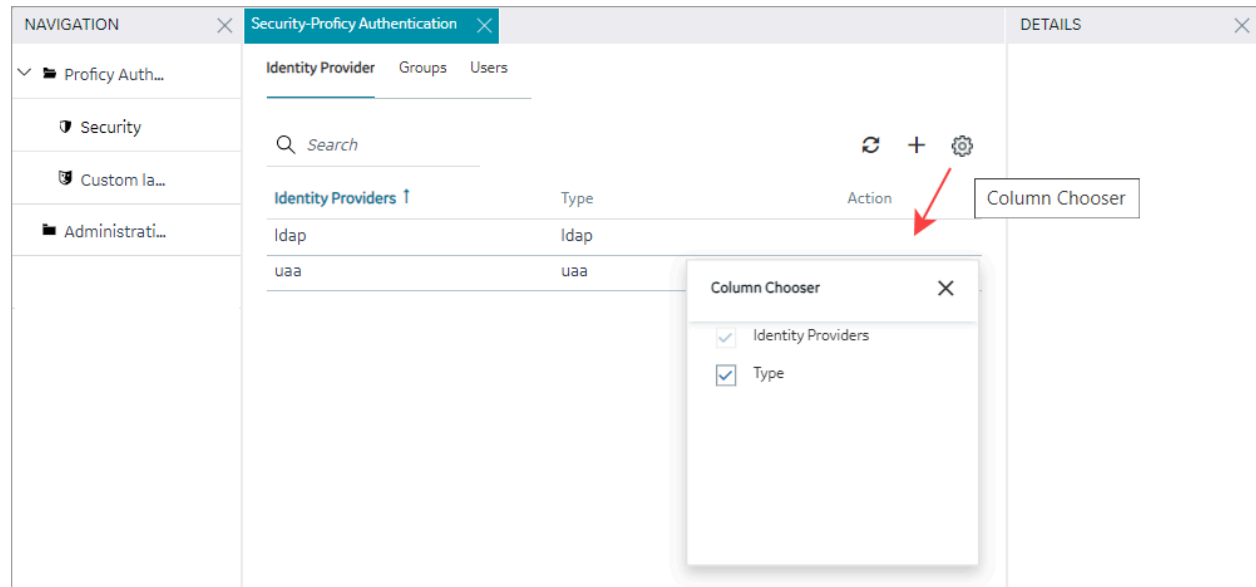
To check the version of the Proficy Authentication application within Configuration Hub, select the application name on the **NAVIGATION** menu. The version information appears under **DETAILS**.


The following screenshot shows Proficy Authentication 2024 installed, highlighting its specific build version.



Show or Hide Data Columns

Customize the display of data by choosing which columns to display and which to hide. You can show or hide columns based on your needs, making it easier to focus on relevant information and de-clutter the display.





1. Select  for the respective data. The **Column Chooser** dialog appears with a list of available columns.
2. Select the check box for the column you want to show. To hide a column, clear its check box.
3. Close the dialog to apply the changes.

Sort by Columns

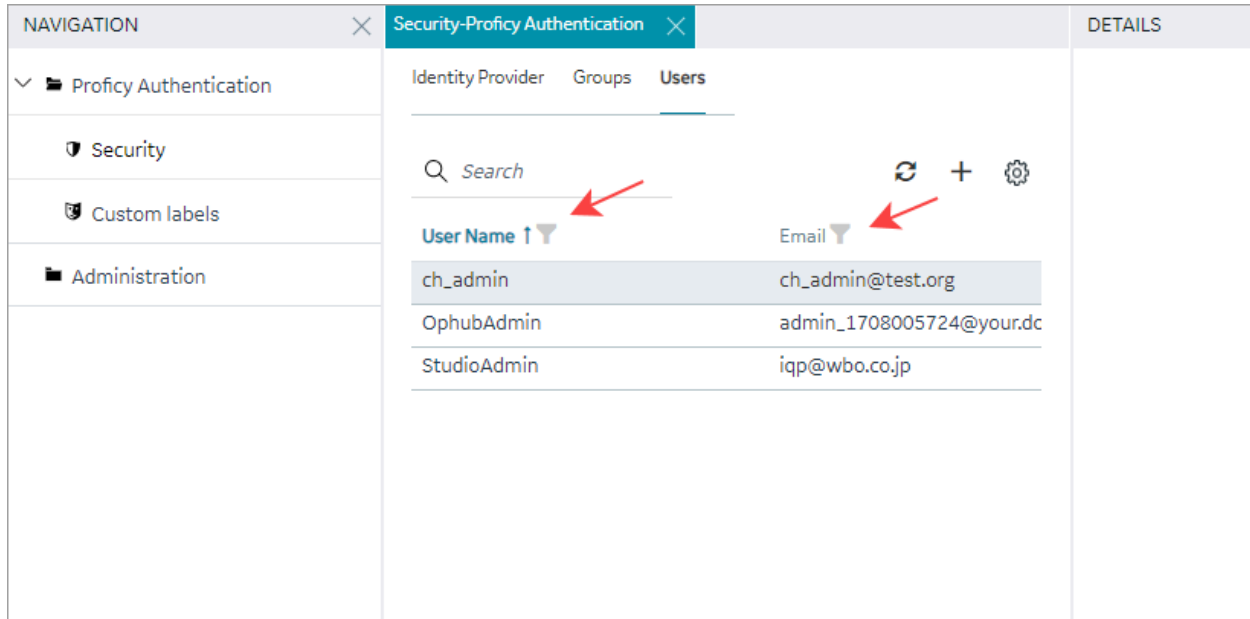
Use the sorting option to sort data in columns by ascending or descending order. When dealing with large datasets, it is easier to analyze, compare, and understand the information when the data is organized in a meaningful way. The sorting option appears when you select a data column.

NAVIGATION	Security-Proficy Authentication	DETAILS									
<ul style="list-style-type: none"> Proficy Auth... Security Custom Ia... Administrati... 	<p>Identity Provider Groups Users</p> <p>Search</p> <p>Identity Providers ↑</p> <table border="1"> <thead> <tr> <th></th> <th>Type</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>ldap</td> <td>ldap</td> <td></td> </tr> <tr> <td>uaa</td> <td>uaa</td> <td></td> </tr> </tbody> </table>		Type	Action	ldap	ldap		uaa	uaa		
	Type	Action									
ldap	ldap										
uaa	uaa										

- Select  to sort data in an ascending order.
- Select  to sort data in a descending order.

Filter by Columns

Use the filter option to narrow down a dataset and focus on specific information. The filtering option appears next to each data column.



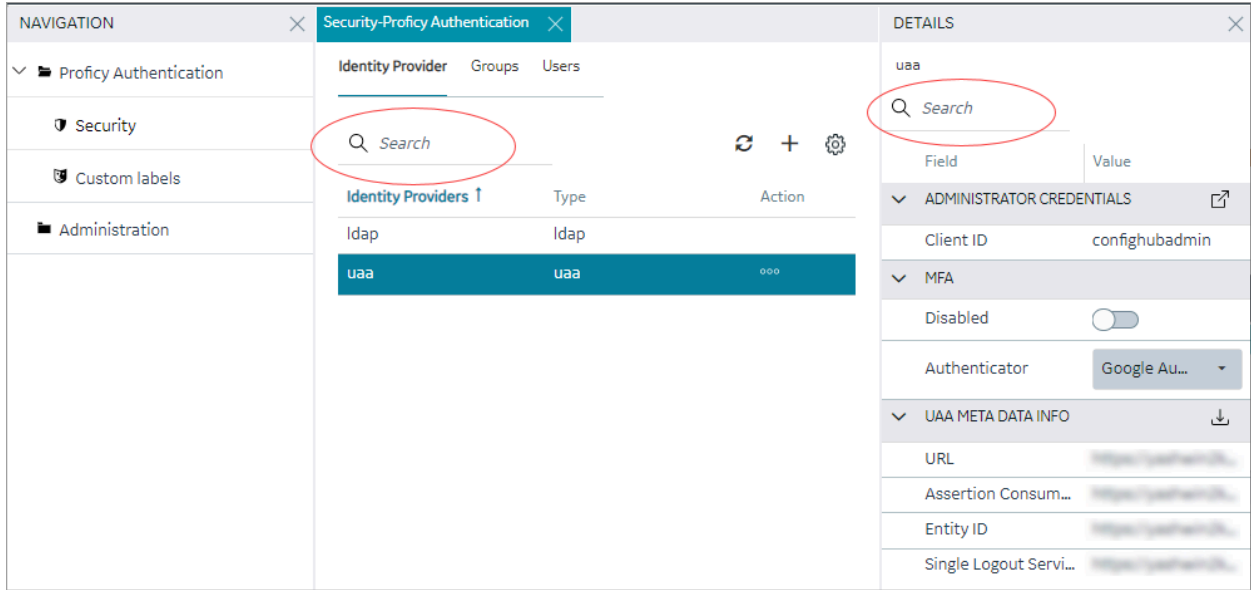
1. Select the filter icon for the data you want to filter. A screen appears with a list of existing data in that column.
2. Select the check box for the data you want to filter.

To undo filtering, you can **Select All**.

3. Select **OK** to apply.

Search with Keywords

Use the search option to search within a dataset using keywords or specific terms that match with the existing accounts in Proficy Authentication. You can also filter account details using search keywords.



Manage Identity Providers

LDAP

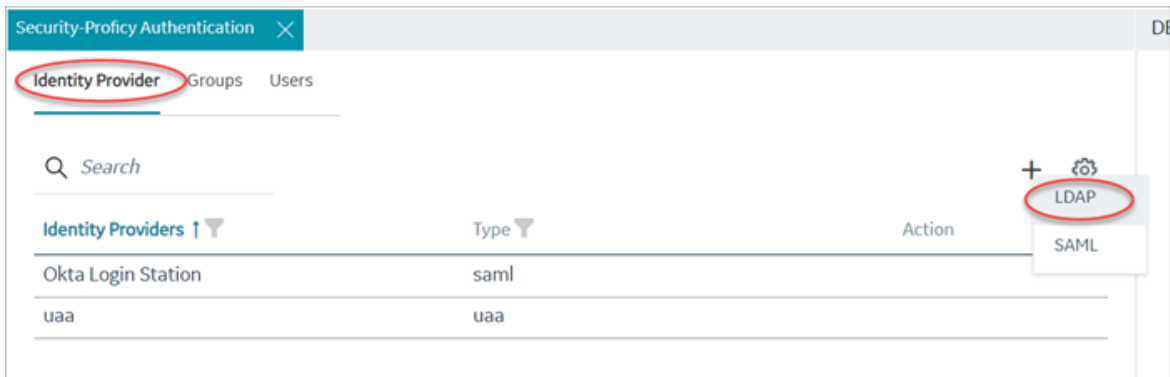
Add LDAP Identity Provider

This topic describes how to add a LDAP account in Proficy Authentication.

Log in to Configuration Hub with user/client having write access for admin and clients.


You can add multiple LDAP connections.

1. Go to **Proficy Authentication > Security > Identity Provider**.
2. Select **+** and then select **LDAP**.



The **LDAP Identity Provider** screen appears.

3. Enter the following details:

Field	Description
Name	A unique name to help identify your LDAP connection.
URL	<p>The URL of the LDAP server. The trailing slash (/) must be included at the end of the URL.</p> <p>You can use LDAP with or without secure authentication in the following format:</p> <ul style="list-style-type: none"> ◦ Insecure port: <code>ldap://100.100.100.2:389/</code> ◦ Secure port: <code>ldaps://100.100.100.2:636/</code> <div style="border: 1px solid orange; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Important: In a URL address, ensure that <code>ldap</code> is in lowercase. Using uppercase letters will render the address non-functional.</p> </div> <p>You can also use a fully qualified domain name instead of an IP address.</p> <p>For a secure port, provide user credentials.</p>
Bind User Distinguished Name	<p>This is a distinguished LDAP user name to represent various entities within an LDAP directory hierarchy, including users, groups, and organizational units.</p> <p>The canonical format consists of CN (Common Name), DC (Domain Component), and OU (Organization Unit Name). CN and DC are mandatory, while OU is optional.</p> <p>Enter the LDAP Distinguished Name in compliance with LDAP standards to ensure proper processing by the system. In the following example, each component (CN, OU, DC) is correctly formatted, separated by commas without any spaces, and is case sensitive.</p> <p><code>CN=John Smith,OU=Factory,DC=Company,DC=COM</code></p> <p>Play the video: <i>How to retrieve the User Distinguished Name required for establishing or modifying the LDAP connection</i> video/LDAP_UserDistinguishedName.mp4</p>

Field	Description
Password	The password to log in to the LDAP server if you choose secure authentication.
Test	Tests the connection to the LDAP server. If the URL and login details are correct, you will receive a test successful message.
Skip SSL Verification	This option appears only when you choose a secure port for LDAP. Select this check box if you want to skip establishing a secure connection between client and server for exchanging LDAP data. Clear the check box to allow SSL verification. Refer to step 4.

LDAP Identity Provider

Name*

DSFREE50KFORUM


URL*


ldap://10.181.215.2:389/

Bind User Distinguished Name *

CN=spcuser1,CN=Users,DC=pa,DC=com


Password *

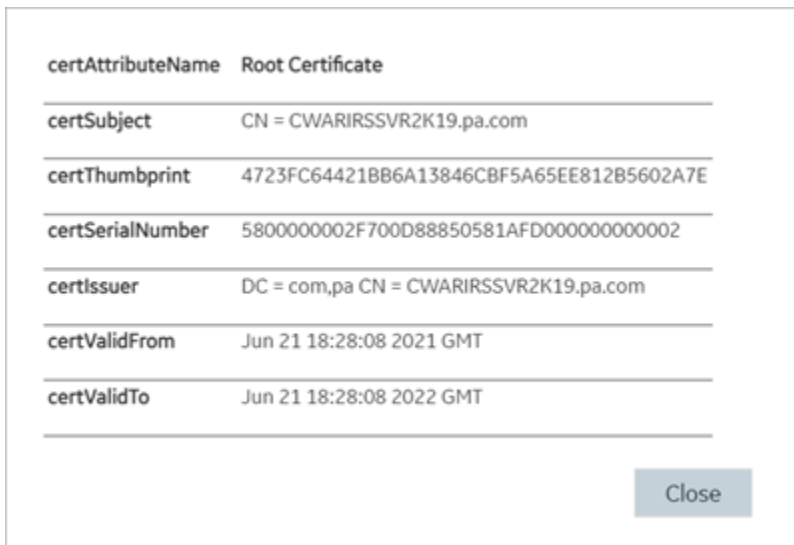
..... 

4. If you choose to secure LDAP, select  for SSL verification.
A message appears when the security certificate is trusted and added to the store.
- In case the certificate is not added automatically, the following message appears.



Select **Browse** to navigate and choose the server certificate from your local system.

5. **Optional:** Select  next to the lock icon to view the certificate.



6. Select **Save**.

LDAP Identity Provider

Name*

CWARIRSSVR2K191

URL*

ldaps://CWARIRSSVR2K19.pa.com:636/ 🔒 👁

Bind User Distinguished Name *

CN=sachin2,CN=Users,DC=htcophub,DC=internal

Password *

***** 🔒


Skip SSL Verification

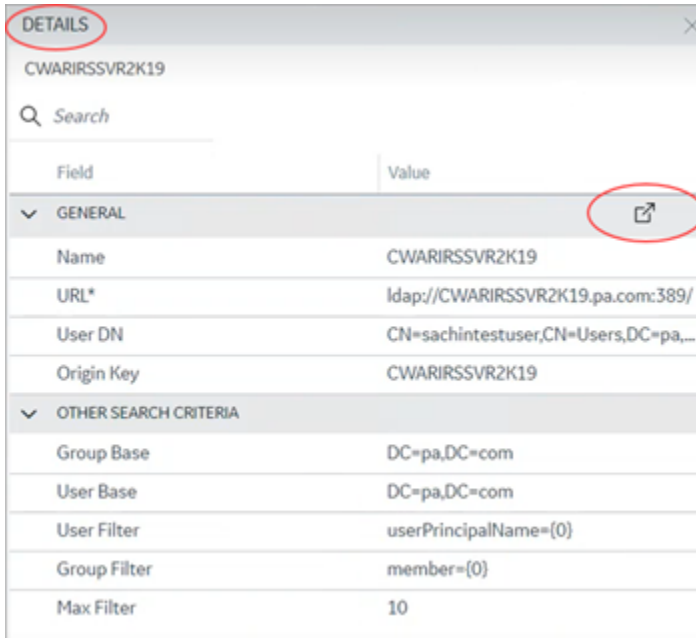
Test
Cancel
Save

Modify LDAP Identity Provider

This topic describes how to modify the existing details for the LDAP account.

[Add LDAP Identity Provider \(on page 15\)](#)

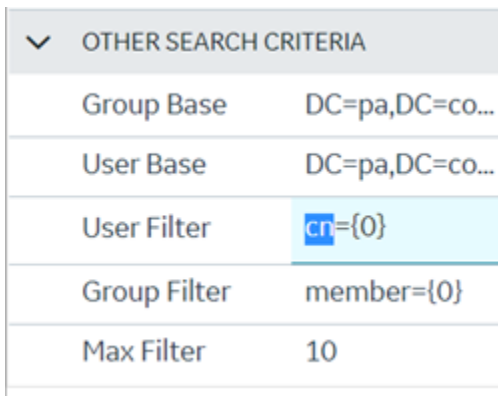
1. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Identity Provider**.
The existing list of identity providers appear.
3. Select the LDAP identity provider.
The existing information for the identity provider appears on the **DETAILS** panel.
4. To modify the **GENERAL** details, select  to open a pop-up screen with the existing information.



5. If you modify any existing information, save the changes.



The general details are required to configure LDAP authentication.

6. To modify **OTHER SEARCH CRITERIA** details, place your cursor and enter the new value for the respective criteria.



Use these settings to enable the sub-directories in your search criteria.

Search Criteria	Example Value	Description
Group Base	OU=Sales,OU=Groups,OU=Enterprise,DC=company,DC=com	Defines the starting point for the LDAP group search in the active directory tree.

Search Criteria	Example Value	Description
		<ul style="list-style-type: none"> ◦ CN is Common Name (required) ◦ DC is Domain Component (required) ◦ OU is Organization Unit Name (optional) <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: If you use only <code>DC=Ge,DC=com</code>, timeout may occur due to slow system response. Use the exact <code>OU</code> to avoid timeout. </div> <p>See Optimizing LDAP Directory Search (on page 22)</p>
User Base	<code>OU=Sales,OU=Users,OU=Enterprise,DC=company,DC=com</code>	Defines the starting point for the LDAP group user search in the active directory tree. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 10px;">  Note: If you use only <code>DC=Ge,DC=com</code>, timeout may occur due to slow system response. Use the exact <code>OU</code> to avoid timeout. </div> <p>See Optimizing LDAP Directory Search (on page 22)</p>
User Filter	<code>userPrincipalName={0}</code>	Allows the LDAP user (active directory user) to login into Configuration Hub with their email address.
User Filter	<code>cn={0}</code>	Allows the LDAP user (active directory user) to login with their display name. This is field is populated by default.
User Filter	<code>sAMAccountName={0}</code>	Allows the LDAP user (active directory user) to login with their account name (Windows login name). This is field is populated by default.

Search Criteria	Example Value	Description
Group Filter	<code>member={0}</code>	Retrieves the <code>memberOf</code> attribute values for the specific user. This field is populated by default.
Max Filter	<code>10</code>	Defines the maximum depth for searching the LDAP groups. The default value is <code>10</code> . For very large systems, set the value to <code>2</code> as it may impact system performance.

Optimizing LDAP Directory Search

This topic describes how to efficiently perform searches for objects (such as users and user groups) in an Active Directory service.

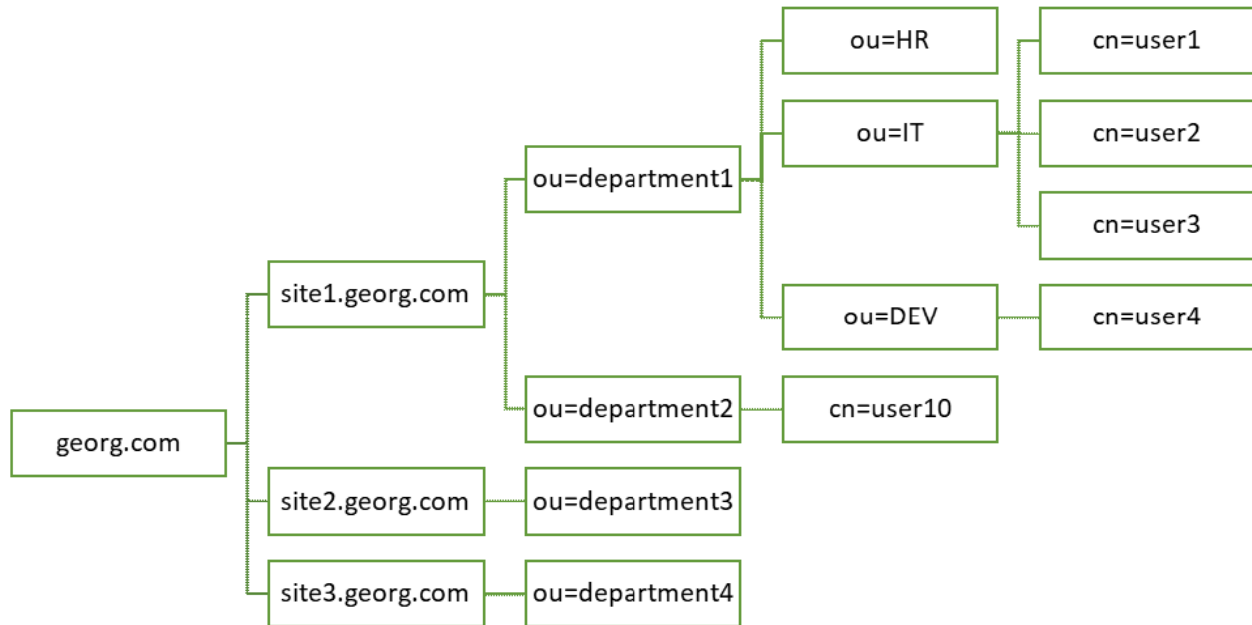
In Active Directory, resources are organized into structures called classes.

Classes are logical groupings of objects such as:

- User accounts
- User groups
- Computers
- Domains
- Organizational units

Some objects, referred to as 'containers', can hold other objects. For example, an organizational unit is a container object. Therefore, the organization of objects in Active Directory follows a hierarchical structure.

The following illustration depicts a hierarchical arrangement of a tree with three domains, each having its own set of organizational units (OUs) for users and groups.



User Search Base and Group Search Base

The User Search Base and Group Search Base set the scope for searching the respective objects in Active Directory's hierarchical structure. Therefore, it is recommended to select values in such a way that they are specific enough to reduce the scope of the search only to the intended area in the tree structure, while ensuring no intended User or Group is missed within the search scope.

Maximum Search Depth

The `Max Filter` parameter determines the maximum depth or level applied when searching the Active Directory hierarchy. This value specifies the number of recursive levels at which the search for contained Group objects is performed for each Group object encountered while searching in Active Directory's hierarchy structure.

Example: Consider a containment hierarchy consisting of a nested structure of user groups (UG1 to UG4) in a hierarchical format, wherein:

- UG1 contains UG2
- UG2 contains UG3
- UG3 contains UG4

UG1

└ UG2

L UG3

L UG4

If the logged-in user has direct group membership in UG4, and:

if <code>Max Filter</code> is set to 4	then, the search for the user's group membership returns all groups in the hierarchy, including UG1, UG2, UG3, and UG4.
if <code>Max Filter</code> is set to 3 (or less)	then, the user's group membership returns only UG2, UG3, and UG4. It does not go beyond the third level in the hierarchy.
if <code>Max Filter</code> is set to 10	then, the search returns all groups (UG1 to UG4) as specified, but it involves unnecessary recursive calls (10 in total, out of which 6 are unnecessary). This can impact performance.

In summary:

1. The default value for `Max Filter` is 10.
2. It is recommended to choose a value aligned with the maximum nested level in your Active Directory's Group hierarchy to avoid unnecessary recursive calls and performance issues.
3. Typically, customers choose values like '1' or '2' based on common nested level/depth of User Groups in most scenarios. However, the choice ultimately depends on your specific requirements.



Tip:

You can use third-party tools like [Softerra LDAP Browser](#) or [AD Explorer](#) to check connectivity to the LDAP server. You can also explore the organizational hierarchy and locate specific Users and Groups within the directory.

SAML

Enable SAML

This topic describes how to configure SAML identity providers for Proficy Authentication.

You should enable SAML prior to [adding SAML IDP accounts \(on page 46\)](#) in Proficy Authentication.

To enable SAML, you will need to download the Proficy Authentication service provider's metadata file.

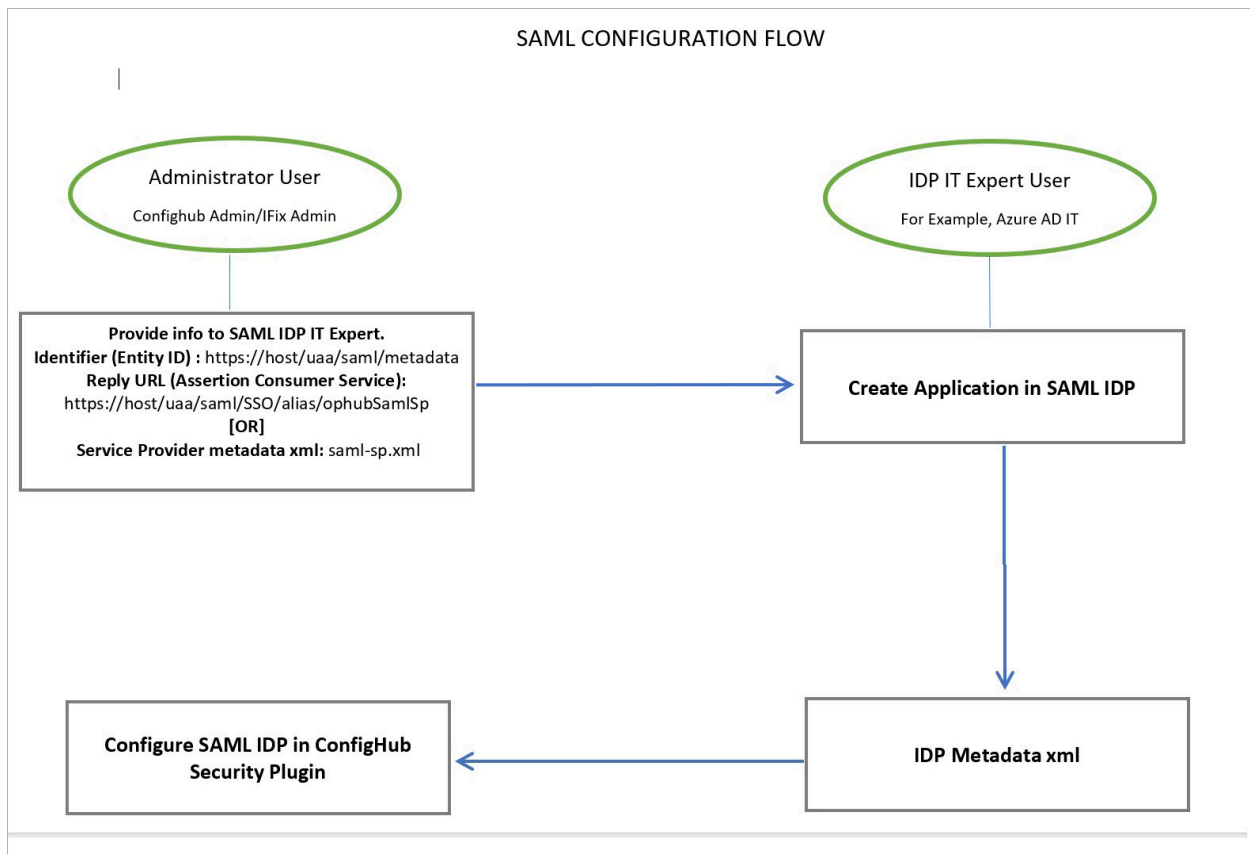
1. Visit `https://enter FQDN of the machine where Proficy Authentication is installed/uaa/saml/metadata` to download the `saml-sp.xml` file.
2. To configure any SAML identity provider, gather information from the downloaded `saml-sp.xml` file.
3. Generate a metadata XML file from the configured identity providers, and use the file to [add a SAML IDP account \(on page 46\)](#) in Proficy Authentication.

Refer to the following examples on how to set up SAML identity providers for Proficy Authentication:

- [Configure Okta as SAML IDP \(on page 26\)](#)
- [Configure Azure AD as SAML IDP \(on page 32\)](#)

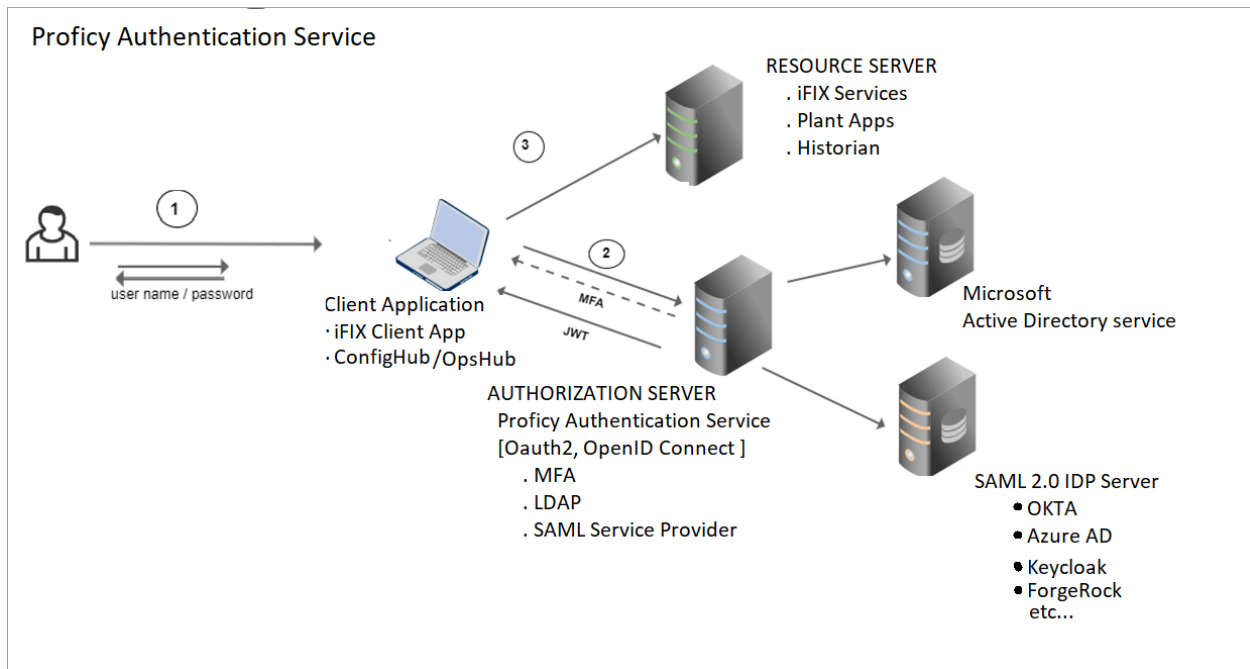
SAML Configuration Flow

The following diagram is a visual representation of the key components involved in the SAML configuration flow.



In the SAML configuration flow, Proficy Authentication Service acts as a SAML Identity Provider (IDP). You must configure Proficy Authentication Service as an IDP by providing it with the necessary SAML metadata and settings.

The following figure illustrates how the data flows and interacts to ensure secure access to resources.



1. Users provide their credentials, which includes a user name and password.
2. When users attempt to access a protected application, they are redirected to the Proficy Authentication Service for authentication.

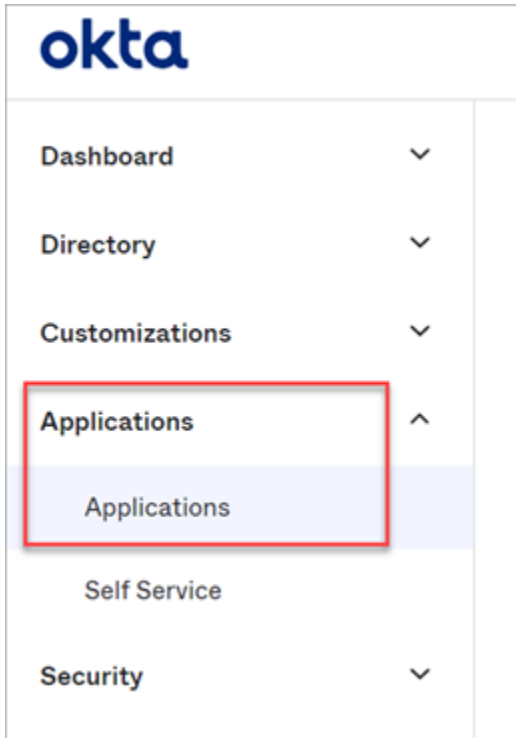
Proficy Authentication Service generates a SAML authentication request and sends it to the user's browser. This request is sent to the configured IdP endpoint.

3. If users are successfully authenticated, they gain access without the need to log in separately.

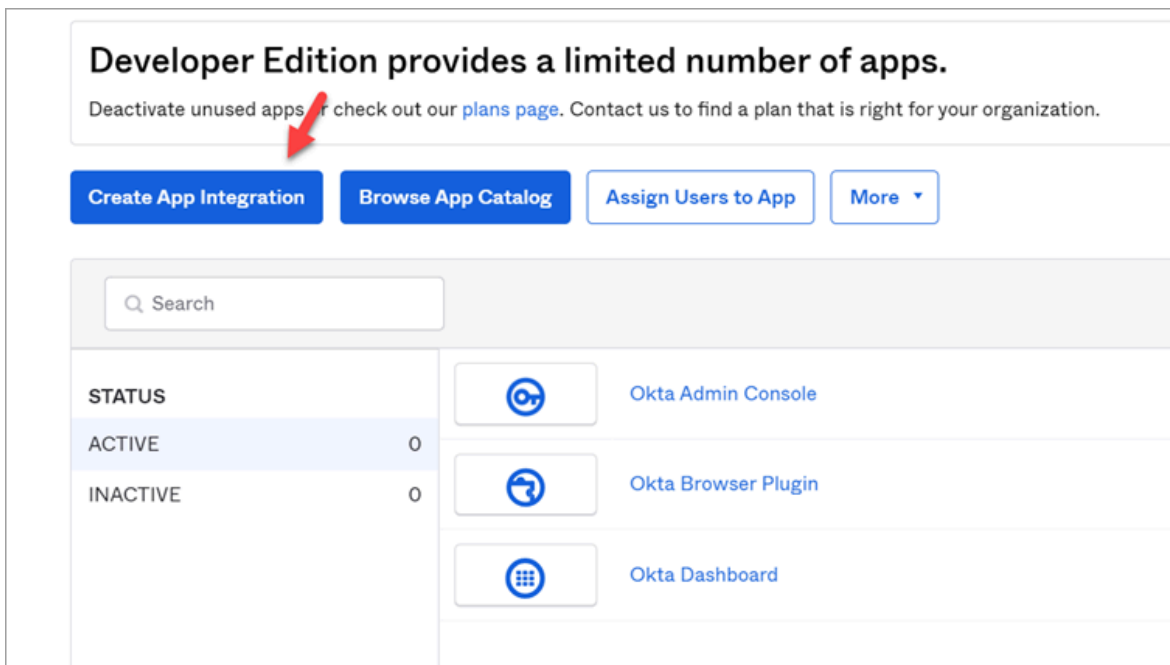
Configure Okta as SAML IDP

This topic describes SAML configuration with Okta.

1. Create an account in Okta.
 - a. Visit <https://developer.okta.com/>.
 - b. Sign up for an Okta account using your email address.
2. Log in to your newly created Okta account.
3. Navigate to **Applications > Applications**.



4. Select **Create App Integration**.



The **Create a new app Integration** screen appears.

5. Select **SAML 2.0**, then select **Next**.

Create a new app integration ✕

Sign-in method [Learn More](#)

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

[Cancel](#) [Next](#)


The **Create SAML Integration** screen appears.

6. Under **General Settings**, provide a name and logo for your application, then select **Next**.

1 General Settings **2** Configure SAML

1 General Settings

App name

App logo (optional)  [Upload](#) [Delete](#)

App visibility Do not display application icon to users

[Cancel](#) [Next](#)

7. Under **Configure SAML**, fill out these details:

<p>Single sign on URL</p>	<p>Use the downloaded Proficy Authentication metadata file (on page 24) <code>saml-sp.xml</code> to get the URL for this field. It should look something like this:</p> <pre><md:AssertionConsumerService Location="https://ghldz593e.logon.ds.ge.com/uaa/saml/SSO/alias/ophubSamlSp" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" isDefault="true" index="0"/> <md:AssertionConsumerService Location="https://ghldz593e.logon.ds.ge.com/uaa/oauth/token/alias/ophubSamlSp" Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI" index="1"/></pre>												
<p>Audience URI (SP Entity ID)</p>	<p>Refer to <code>saml-sp.xml</code> to get the logout URL. It should look something like this:</p> <pre><?xml version="1.0" encoding="UTF-8"?> - <md:EntityDescriptor entityID="https://ghldz593e.logon.ds.ge.com/uaa/saml/metadata" ID="https://ghldz593e.logon.ds.ge.com/uaa_saml_metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"> - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></pre>												
<p>Enable Single Logout</p>	<ol style="list-style-type: none"> Select Show Advanced Settings. Select the check box for Allow application to initiate Single Logout. Enter Single Logout URL. Refer to <code>saml-sp.xml</code> to get the logout URL. It should look something like this: <pre></md:KeyDescriptor> <md:SingleLogoutService Location="https://ghldz593e.logon.ds.ge.com/uaa/saml/SingleLogout/alias/ophubSamlSp" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/> <md:SingleLogoutService Location="https://ghldz593e.logon.ds.ge.com/uaa/saml/SingleLogout/alias/ophubSamlSp" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/> <md:NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</pre>												
<p>Attribute Statements (optional)</p>	<p>Add user attribute statements such as email, first name, and last name as shown here:</p> <div data-bbox="509 1157 1312 1556" style="border: 1px solid #ccc; padding: 10px;"> <p style="text-align: right;">LEARN MORE</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Name</th> <th style="width: 20%;">Name format (optional)</th> <th style="width: 50%;">Value</th> </tr> </thead> <tbody> <tr> <td>email</td> <td>Unspecified ▼</td> <td>user.email ▼</td> </tr> <tr> <td>first name</td> <td>Unspecified ▼</td> <td>user.firstName ▼ ×</td> </tr> <tr> <td>last name</td> <td>Unspecified ▼</td> <td>user.lastName ▼ ×</td> </tr> </tbody> </table> <p style="text-align: left; margin-top: 10px;">Add Another</p> </div>	Name	Name format (optional)	Value	email	Unspecified ▼	user.email ▼	first name	Unspecified ▼	user.firstName ▼ ×	last name	Unspecified ▼	user.lastName ▼ ×
Name	Name format (optional)	Value											
email	Unspecified ▼	user.email ▼											
first name	Unspecified ▼	user.firstName ▼ ×											
last name	Unspecified ▼	user.lastName ▼ ×											
<p>Group Attribute Statements (optional)</p>	<p>Add group attribute statements such as groupA and groupB as shown here:</p>												

Group Attribute Statements (optional)		
Name	Name format (optional)	Filter
groupA	Unspecified ▾	Contains ▾ manager
groupB	Unspecified ▾	Contains ▾ operator ×
Add Another		



Note:

The setting option mentioned in this topic is the minimum requirement for setting up the SAML identity provider. Refer to the [Okta documentation](#) for information on using additional settings.

8. Select **Next**.


9. Provide your feedback and select **Finish**.

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

 Once you have a working SAML integration, submit it for Okta review to publish in the OIN. [Submit your app for review](#)

[Previous](#) [Finish](#)

Your application is created.

10. Under **Sign On**, select **Identity Provider metadata**.

Multiverse Paradigm

Active View Logs Monitor Imports

Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

General **Sign On** Import Assignments

Settings Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

Credentials Details

The metadata opens in a new tab.

11. Save the metadata as an .xml file.

Use the metadata xml file to [configure a SAML identity provider \(on page 46\)](#) in Proficy Authentication.

12. Under **Assignments**, you can assign the app to groups and individual users.

If there are no users/groups, navigate to **Directory > People** to create and activate new users/groups in Okta.

Configure Azure AD as SAML IDP

This topic describes how to configure Azure AD (Active Directory) as a SAML identity provider.

To configure SAML as an authentication scheme for single sign-on, you must have the following:

Pre-requisite	Description
Create Your Azure Account	If you don't already have an Azure account, you should create one to proceed with the SAML configuration. Visit https://azure.microsoft.com/en-us/free/ to sign up for a free account. Make sure your account has sufficient privileges to perform the SAML configuration.
Set Up Your Enterprise Application	Do the following to set up an enterprise application in Azure with the necessary configuration. <ol style="list-style-type: none"> 1. Log in to your Azure account. 2. Refer to the steps described in Microsoft Azure documentation on how to create a new enterprise application. In the steps that follow, we shall refer to an example enterprise application called <code>bobtestsaml</code>.
Associate Users and Groups	For the SAML setup to work, you have to associate at least one user and one group with the enterprise application. This is important for the authentication process. <ol style="list-style-type: none"> 1. Log in to your Azure account and navigate to the enterprise application you created earlier (<code>bobtestsaml</code> is our example application). 2. Select Users and groups > Add user/group. 3. Search and assign the user/group to the application.

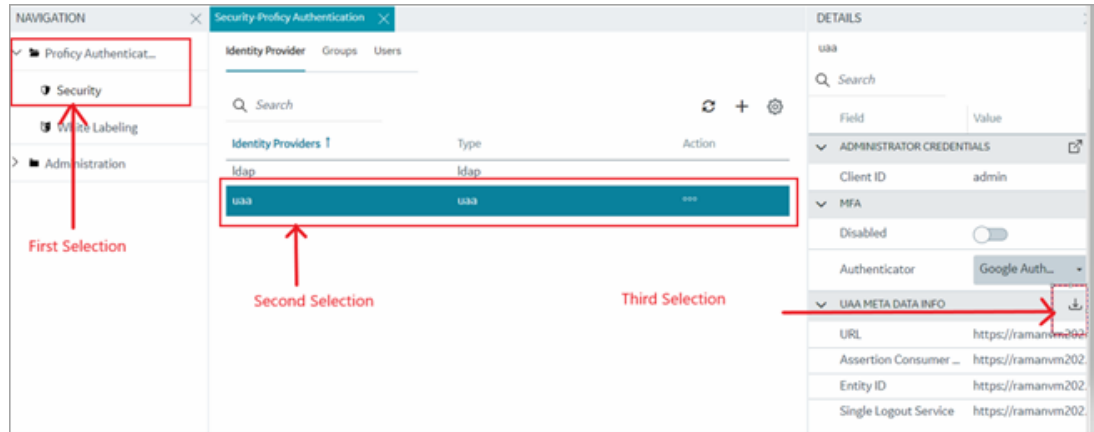
In the steps that follow, we shall accomplish the following:

- Create a SAML App in Azure (performed by your skilled IT Azure Expert).
 - [Download the SAML Metadata file \(on page 33\)](#)
 - [Upload the saml-sp.xml File to Azure AD \(on page 33\)](#)
 - [Perform User and Group Attribute Mapping in Azure \(on page 36\)](#)
- Configure Azure Metadata XML in Proficy Authentication. (performed by the Application Administrator.)
 - [Create SAML Connection in Proficy Authentication \(on page 39\)](#)
 - [Adding and Mapping UAA and SAML Groups \(on page 42\)](#)
 - [Test SAML Authentication \(on page 44\)](#)

See also, [Troubleshooting \(on page 44\)](#).

1. Download the SAML Metadata file

- a. Log in to Configuration Hub.
Use valid credentials, preferably the default `clientID`.
- b. Navigate to **Proficy Authentication > Security > Identity Provider** and download the UAA `saml-sp.xml` metadata file.

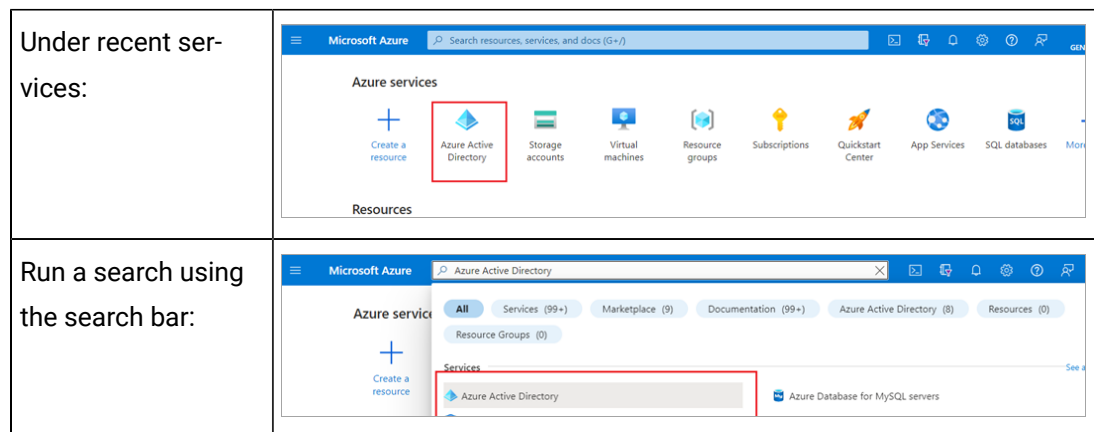


The metadata file is downloaded to your browser's Download section.

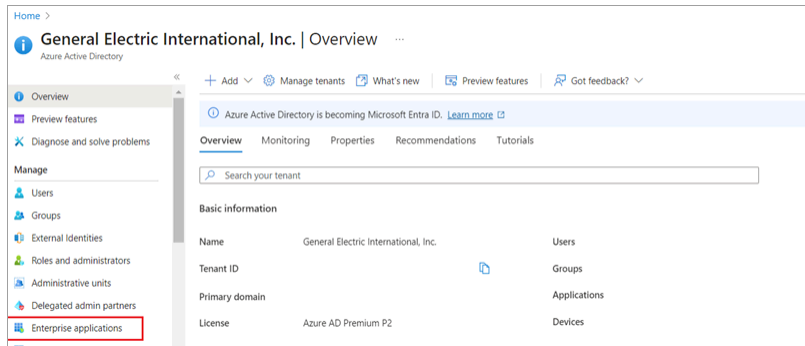
2. Upload the saml-sp.xml File to Azure AD

- a. Visit <https://portal.azure.com> and login with your valid credentials.
- b. After logging in, select **Azure Active Directory**.

i Tip:
You can find it under recent services, or by using the search option.



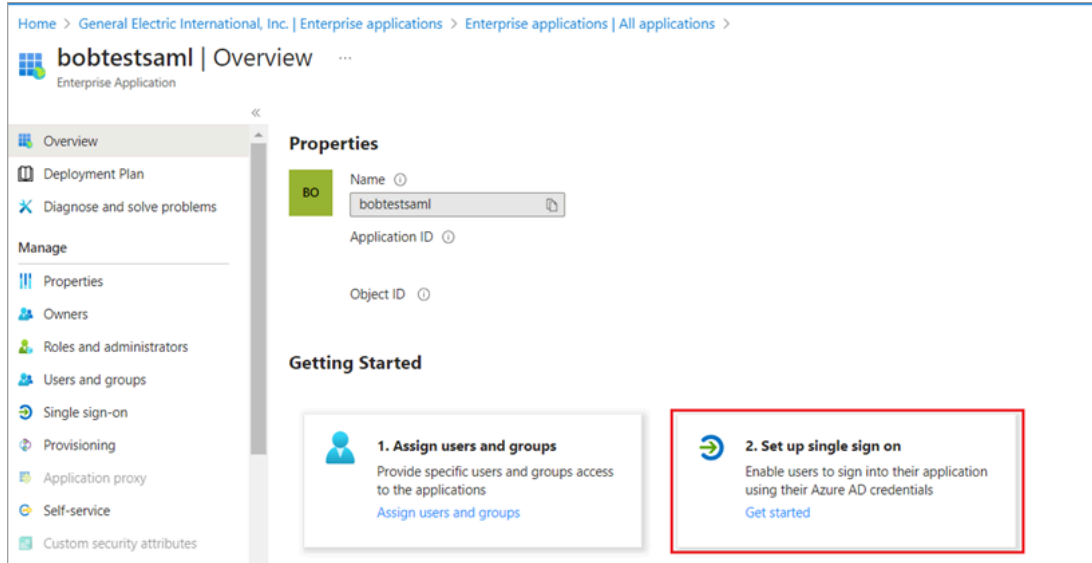
- c. Under Azure Active Directory, locate the enterprise application to which you want to establish a SAML connection.



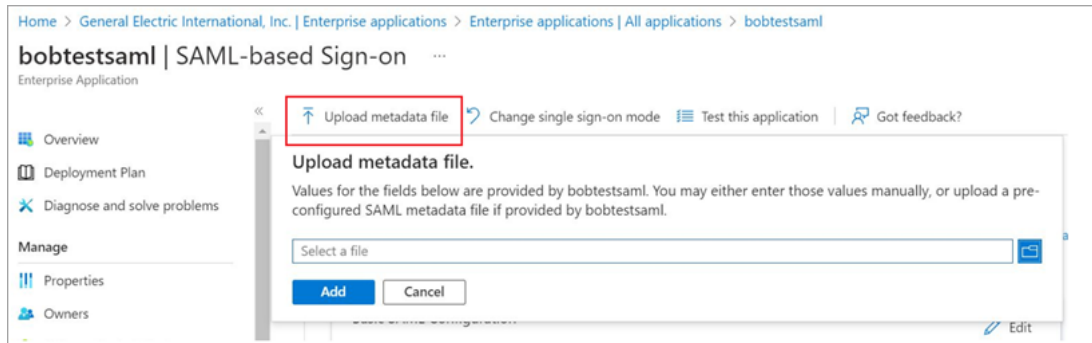
i Tip: You can locate the application from recent searches, or running a search.

<p>Searching application:</p>	<table border="1"> <thead> <tr> <th>Name</th> <th>Object ID</th> <th>Application ID</th> <th>Homepage URL</th> <th>Created on</th> <th>Certificate Expiry St...</th> <th>Identifier URI (I...</th> </tr> </thead> <tbody> <tr> <td>bobtestaml</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry St...	Identifier URI (I...	bobtestaml						
Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry St...	Identifier URI (I...									
bobtestaml															
<p>If needed, request your IT Azure Expert team to create a new application from here:</p>															

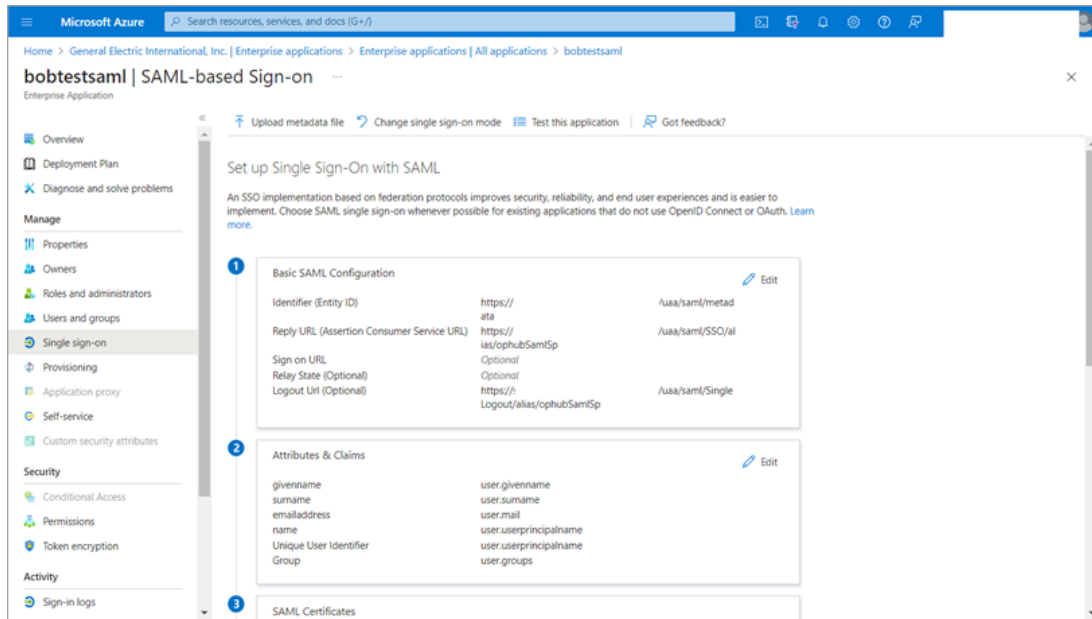
- d. Open the enterprise application and select **Set up single sign on**.



e. Select **Upload metadata file** and upload the `saml-sp.xml` file we downloaded in the earlier step.

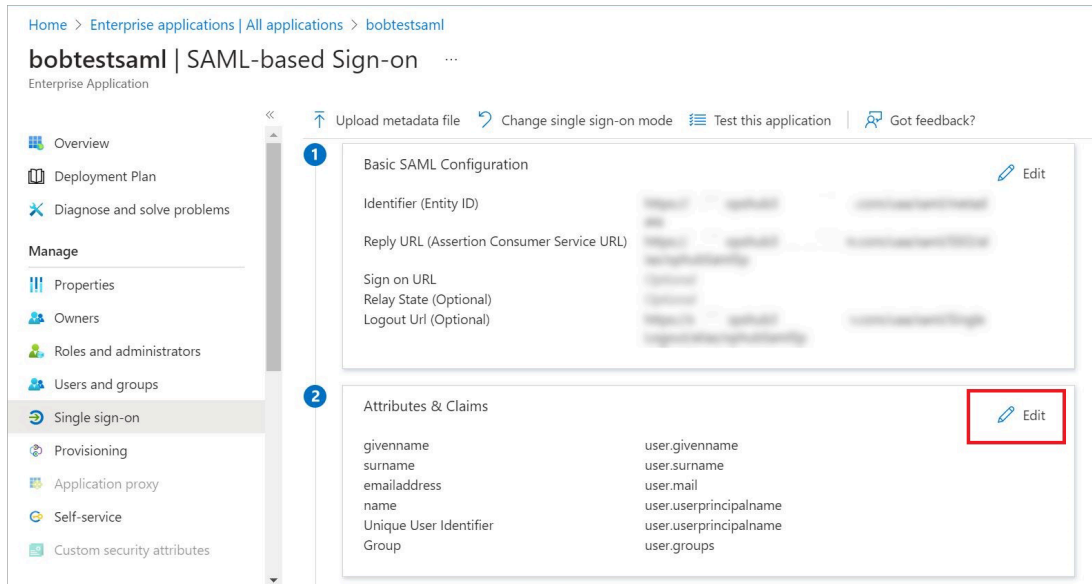


f. After the file is uploaded successfully, Azure displays the information from the `saml-sp.xml` file.



3. Perform User and Group Attribute Mapping in Azure

a. In the enterprise application, under **User Attributes & Claims** section, select **Edit**.



b. Select **Add new claim**.

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications > Enterprise applications | All applications > bobtestsaml | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims

Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [nameid-format:emai... **

Additional claims

Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [SecurityGroup] ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***

Advanced settings

c. Enter claim details, and save the information.

Microsoft Azure Search resources, services, and docs (G+)

Enterprise applications | All applications > bobtestsaml | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims > Manage claim

Manage claim

Save Discard changes Got feedback?

Name * givenName

Namespace http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name format

Source * Attribute Transformation Directory schema extension (Preview)

Source attribute * user.givenname

Claim conditions

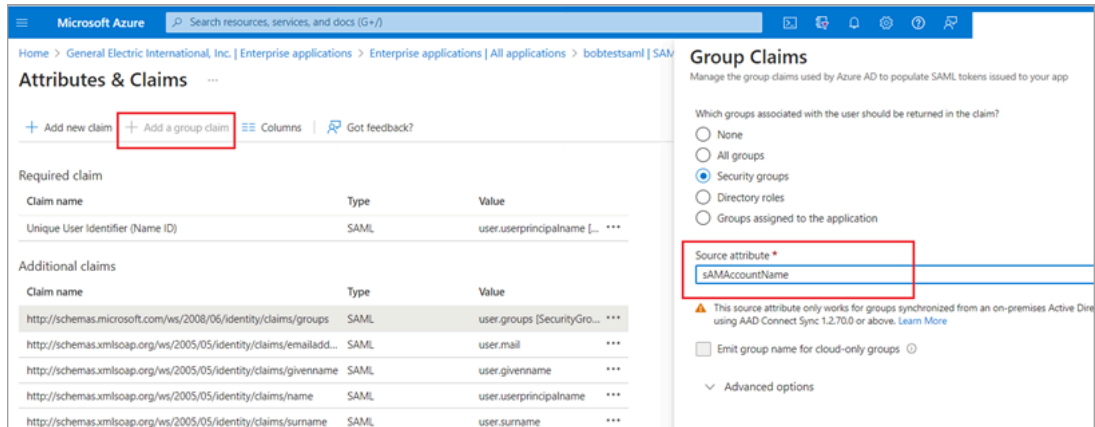
Advanced SAML claims options



Note:

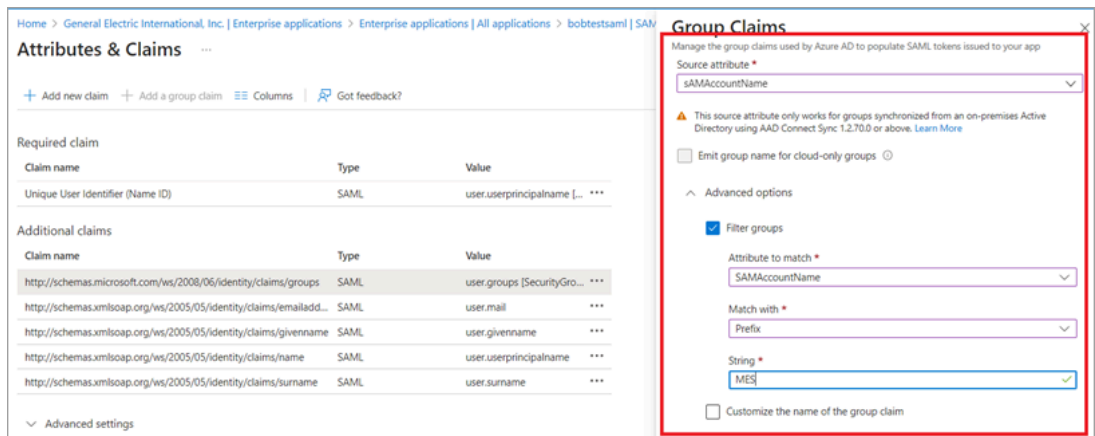
Make a note of the **Namespace** value. This value will be used later while setting up SAML Connection in Proficy Authentication.

d. To set up group claims, select **Add a group claim**.

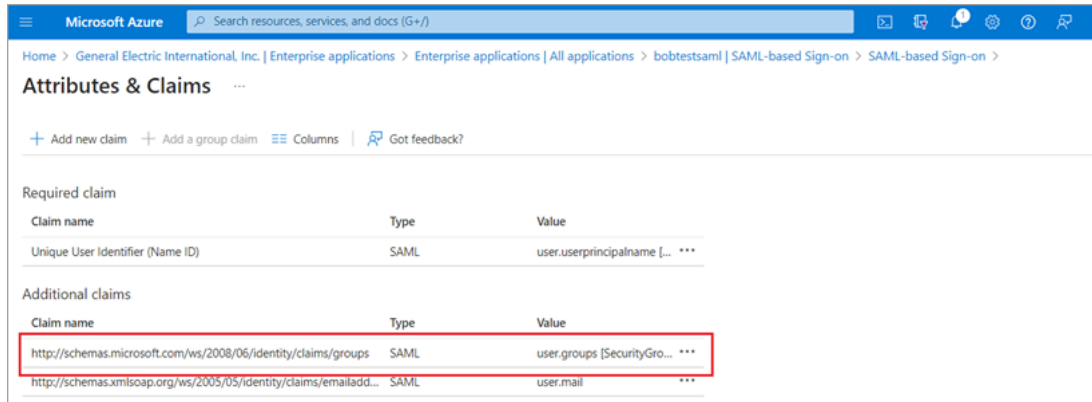


You can choose to provide **Advanced options** for the group claim as shown in the following screen shot.

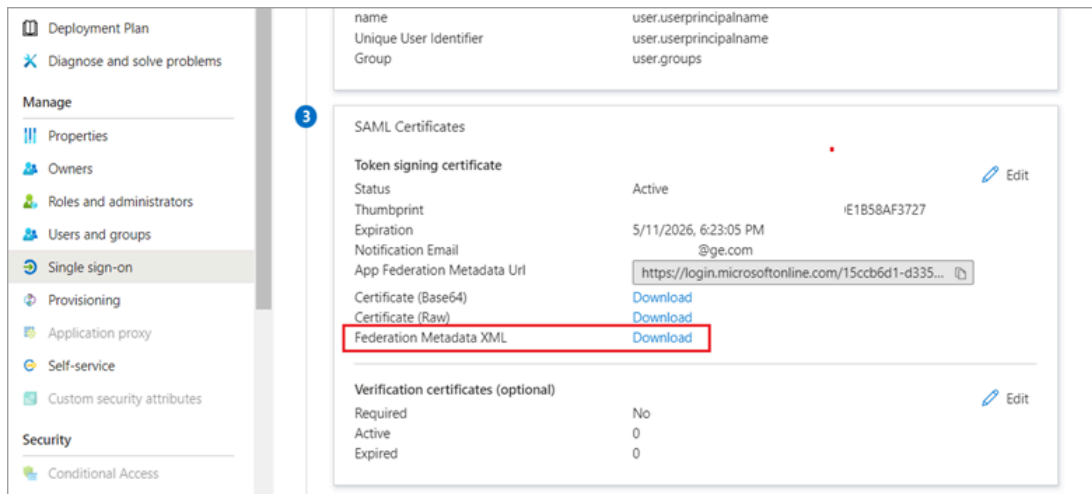
For example, string type is selected as **MES** because we want to cast our groups to start with MES, You can select as per your choice.



After updating the group claim, **Attribute & Claims** screen should look like as shown in the following screen shot. The highlighted claim name needs to be same while creating SAML Connection in Proficy Authentication.

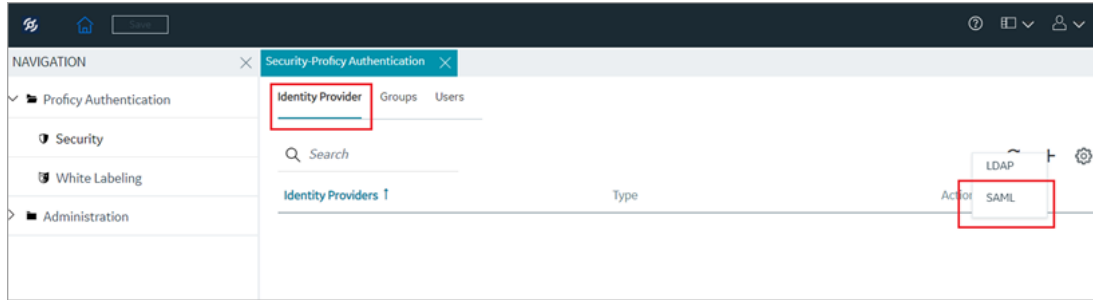


- e. Under the **SAML Signing Certificate** section, download the **Federation Metadata XML** file. We shall upload this file later when creating a SAML Connection from Proficy Authentication.



4. Create SAML Connection in Proficy Authentication

- a. Log in to Configuration Hub as an administrator.
- b. Go to **Proficy Authentication > Security > Identity Provider**.
- c. Select **+**, then select **SAML**.



d. In the **SAML Identity Provider** pop-up screen, enter details.

Field Name	Description
Upload XML File	Upload the Federation XML downloaded from Azure. Refer to this step (on page 39).
Name	Name of the SAML application. You can provide any name.
Attribute Name	Enter the Group Name mapping. Refer to this screen shot (on page 38).
Name ID	From drop down, select <code>format:unspecified</code> .
Enable SAML Link	Select the check box.

SAML Identity Provider

NOTE: All fields are mandatory

Upload XML File Provide File Location

Upload XML File

```
<?xml version="1.0" encoding="utf-8"?><EntityDescriptor ID="c82426a5-0106-40b8-a0f8-cab3a1288529" entityID="https://sts.windows.net/b072267b-2965-4512-8905-nfcb070e0eb00" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><Signature
```

Name*
Azure AD SAML

Attribute Name*
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

Name ID*
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

Enable SAML Link

Cancel Save

Microsoft Azure

Attributes & Claims

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user:principalname [...]

Additional claims

Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.group Security...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail [...]

After successful SAML connection, the application screen should look something like this:

NAVIGATION

Security-Proficy Authentication

Proficy A...

Security

White La...

Identity Provider Groups Users

Search


Identity Providers ↑	Type	Action
Azure AD SAML	saml	...
NewLdap	ldap	
OKTA-SAML	saml	
uaa	uaa	
UAA LDAP	ldap	

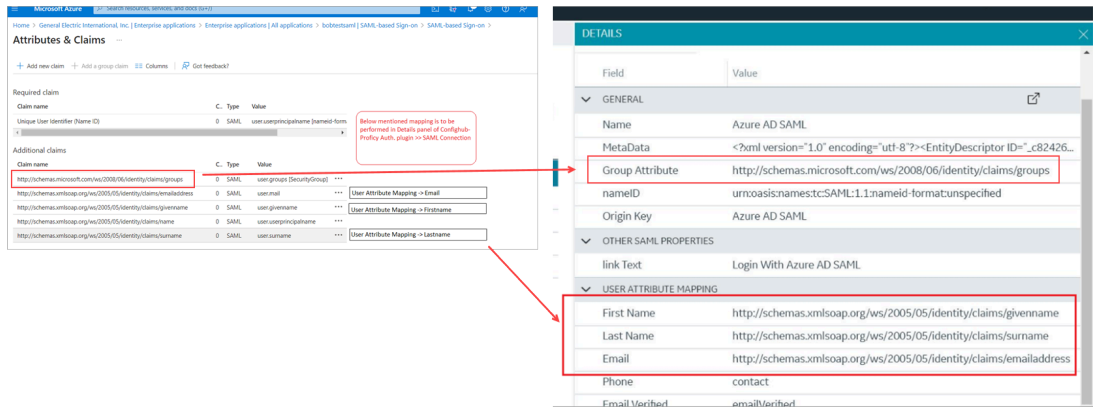
DETAILS

Field	Value
GENERAL	
Name	Azure AD SAML
MetaData	<?xml version="1.0" encoding="utf-8"?><EntityDescriptor ID="c82426...
Group Attribute	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
nameID	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Origin Key	Azure AD SAML
OTHER SAML PROPERTIES	
link Text	Login With Azure AD SAML
USER ATTRIBUTE MAPPING	
First Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Phone	contact
Email Verified	emailVerified

! **Important:**

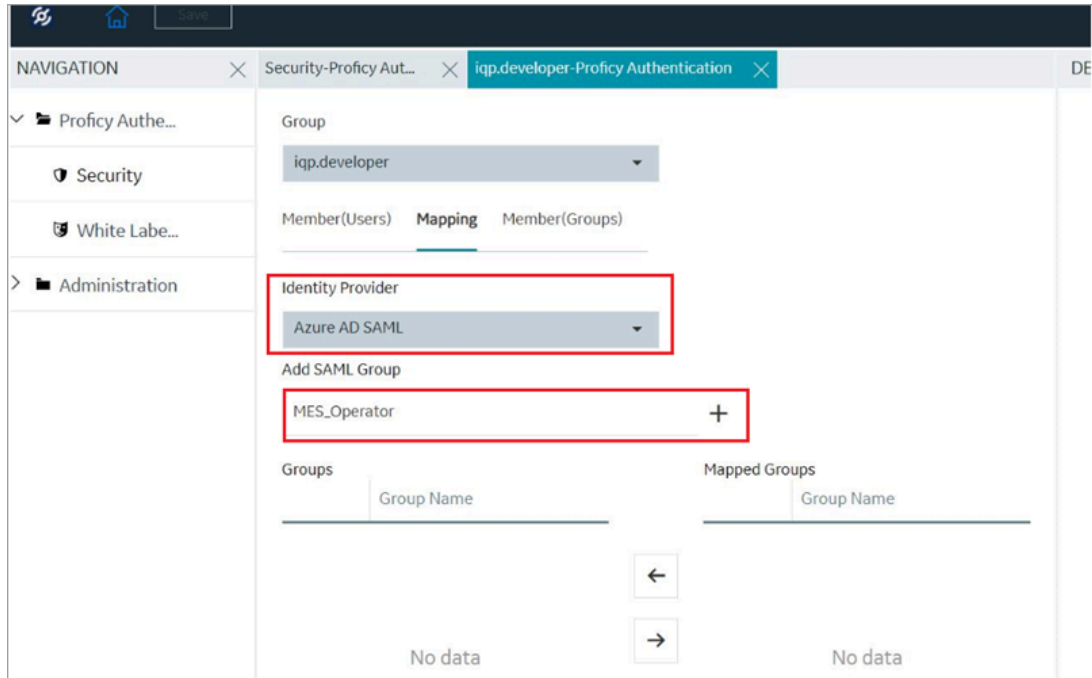
You must perform User Attribute Mapping, which involves taking values from the Azure **Attributes & Claims** page and linking them to the Details section of the

 established SAML Connection in Proficy Authentication. Refer to the example screen shots below.




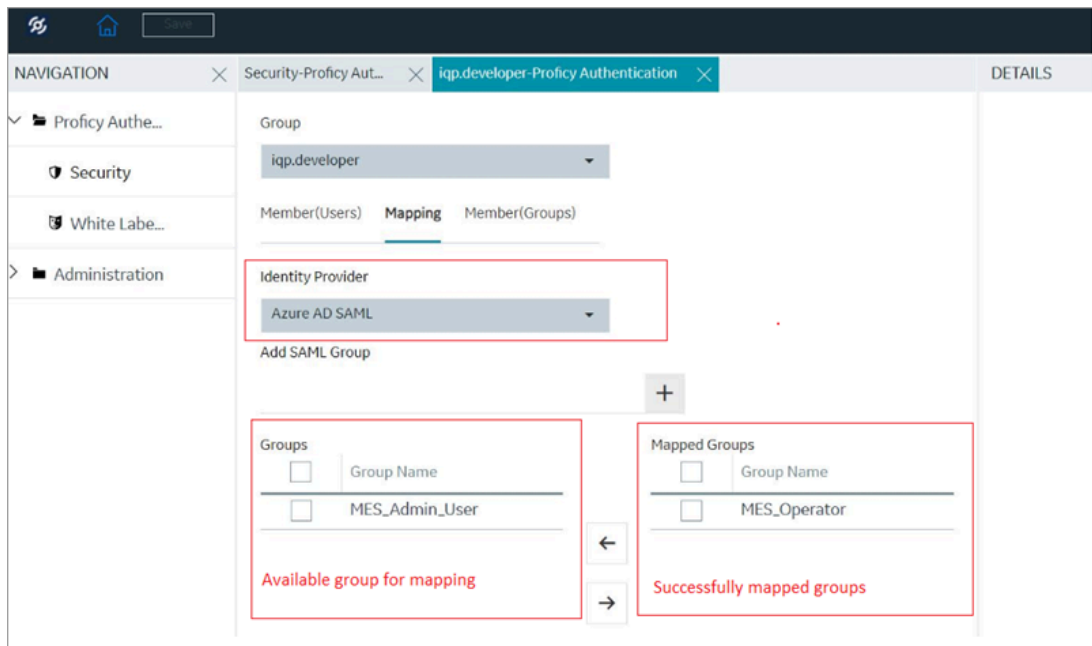
5. Adding and Mapping UAA and SAML Groups

- a. Go to **Proficy Authentication > Security > Groups**.
- b. Double-click and open the group you want to map to SAML.
- c. Select the **Mapping** tab.
- d. Map SAML groups: From the **Identity Provider** drop down list, select the SAML record.
- e. To create SAML groups, enter the valid SAML group name in the **Add SAML Group** field and select the plus icon.



f. Select the check box for the groups you want to map to the Proficy Authentication group selected in step 5(b).

g. Select  to move the selected items from **Groups** to **Mapped Groups**.



If the mapped SAML groups are valid, then all their users become a member of the Proficy Authentication group selected in step 5(b).

6. Test SAML Authentication

- a. Visit Operations Hub login page.
- b. Select **Sign In With Azure**.



Troubleshooting SAML-Related Issues

Addressing Login Issues With Azure:

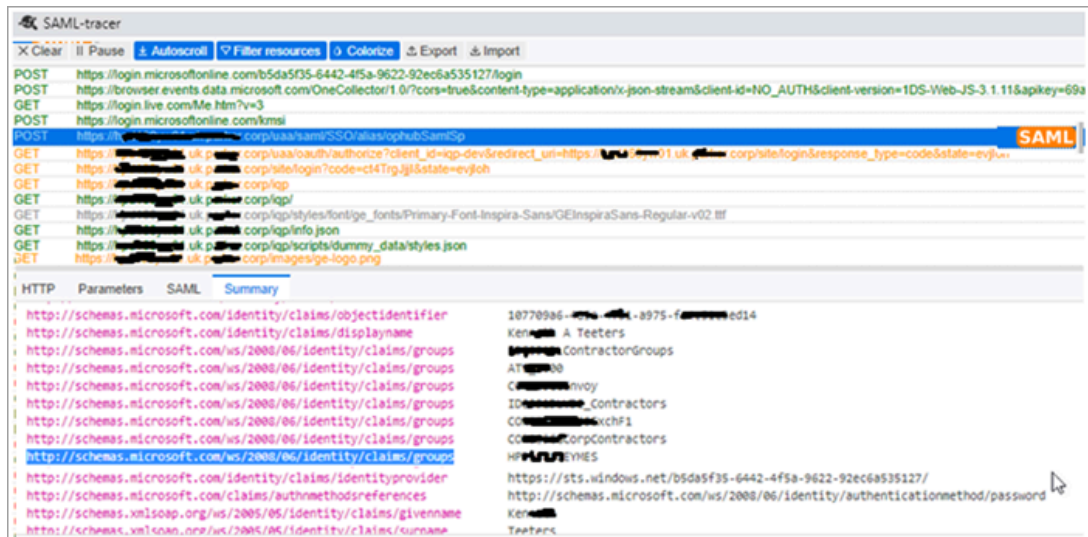
In Azure portal, you can access the logs to verify successful logins. This will help establish a baseline for successful authentication. Whenever login access is denied, closely review the login attempts in the logs.

Date	Request ID	User	Application	Status	IP address	Location
9/5/2023, 10:01:30 PM	7aa	i...	z (... bobtestsaml)	Success	2	17 Fa Connect
9/5/2023, 9:54:36 PM	0cb	i...	z (... bobtestsaml)	Failure	2	18 Fa Connect
9/5/2023, 6:16:56 PM	633	s...	z (... bobtestsaml)	Success	2	18 Fa Connect
9/5/2023, 6:16:55 PM	a7a	s...	z (... bobtestsaml)	Success	2	18 Fa Connect
9/5/2023, 6:16:54 PM	6ec	...	z (... bobtestsaml)	Success	2	18 Fa Connect
9/5/2023, 6:16:54 PM	be8	s...	z (... bobtestsaml)	Failure	2	18 Fa Connect
9/5/2023, 4:45:12 PM	3e2	...	z (... bobtestsaml)	Failure	2	13 Fa Connect
9/5/2023, 4:45:11 PM	1d7	s...	z (... bobtestsaml)	Failure	2	13 Fa Connect

Addressing Login Issues Without Azure:

You can use the SAML-tracer extension for Chrome to diagnose and resolve SAML-related problems in Operations Hub. Follow these steps:

1. **Install SAML-tracer:** Add the [SAML-tracer](#) extension to your Chrome browser.
2. **Access SAML-tracer:** Open SAML-tracer from your browser extensions.
3. **Reproduce the Issue:** Log in to Operations Hub as you normally would to reproduce the SSO login issue.
4. **Inspect SAML Messages:** In SAML-tracer, look for `POST` messages.
 - a. Select the specific POST message related to the SSO login attempt.
 - b. Next select the **Summary** tab for detailed information about the SAML attributes exchanged.
 - c. Review the SAML attribute names and values exchanged during the SSO attempt, and compare them against the expected values.
 - d. If you notice that the SAML group attribute names are incorrect (refer to screen shot), this could be the cause of the login issue.



- e. Replace the incorrect attribute names with the correct ones to fix the login issue.

Retrieving Azure Login Screen:

In case you encounter a situation where the Azure login screen does not appear, then do the following to address this issue:

- Check your SAML Azure configuration. Verify the group attribute name and the corresponding group name. Any mismatch in attribute names can lead to access issues.
- Clear your browser cache and login again.

Add SAML Identity Provider

This topic describes how to add multiple SAML accounts in Proficy Authentication.

[Enable a SAML identity provider \(on page 24\)](#). For example, Okta or Azure AD or any other IDP.

You can add multiple SAML connections.

1. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Identity Provider**.
3. Select **+**, then select **SAML**.



The **SAML Identity Provider** screen appears.

4. Enter the following details:



Note:

The XML file contains the metadata to interact with SAML enabled identity providers (Azure, ADFS, or Okta). Refer to [Configure Okta as SAML IDP \(on page 26\)](#).

Field	Description
Upload XML File	Choose this option if you want to upload an XML document. Select Upload XML File to browse and locate the XML document from your local system. The uploaded data appears in a text box, and is read-only.
Provide File Location	Choose this option if you want to provide an external URL to the XML document.

Field	Description
	Enter the URL in the text field, and select Load . The data from the URL appears in a text box, and is read-only.
Name	Name of the SAML identity provider. You can provide any name. For example, <code>okta_123</code> or <code>demo_mach_azure</code> .
Attribute Name	The attribute that contains the group membership information about a user in a SAML assertion.
Name ID	SAML Name identifier and associated fields that you want to use in a link test.
Enable SAML Link	Select the check box.

SAML Identity Provider

NOTE: All fields are mandatory

Upload XML File
 Provide File Location

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor
entityID="http://www.okta.com/exk2uugkc5PUxlfaa5d7"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"><md:IDPSSODescriptor
```

Name*

okta_123

Attribute Name*

email

Name ID*

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

Enable SAML Link


5. Select **Save**.

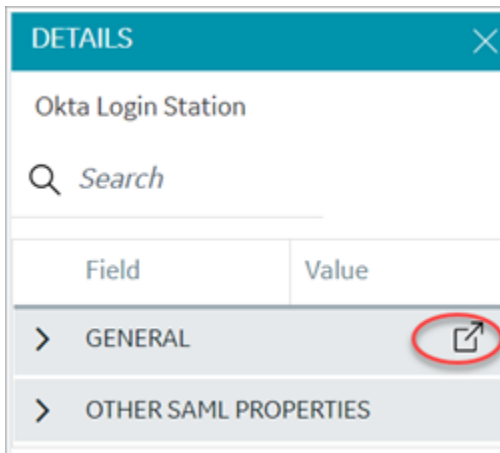
The SAML identity provider is created.

Modify SAML Identity Provider

This topic describes how to modify the existing details for a SAML account.

[Add SAML Identity Provider \(on page 46\)](#)

1. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Identity Provider**.
The existing list of identity providers appear.
3. Select the SAML identity provider you want to modify.
The existing information for the identity provider appears on the **DETAILS** panel.
4. Select  to display the details in a pop-up screen.



The **SAML Identity Provider** screen appears.

5. You can modify the existing information and save the changes.
6. You can also modify items under **OTHER SAML PROPERTIES** section. Enter a new value to replace the existing value.

Enable Multi-Factor Authentication

This topic describes how to enable multi-factor authentication for users.

Install the [Google Authenticator](#) app on your mobile device.

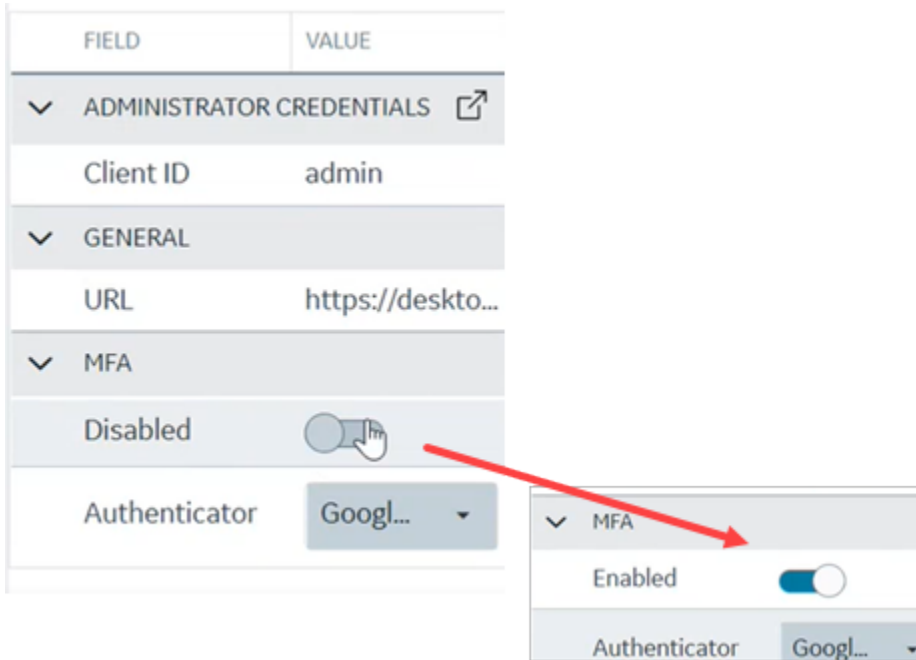
Only administrators can enable multi-factor authentication (MFA) for users.



Note:

Enabling MFA also enables two-factor authentication for UAA and LDAP users as both the identity providers have a common login entry point.

1. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Identity Provider**.
The existing list of identity providers appear.
3. Select the **UAA** record for which you want to enable the multi-factor authentication.
The option to enable MFA appears on the **DETAILS** panel under the **MFA** section.
4. Enable the toggle switch for MFA.
By default, MFA is disabled.




The multi-factor authentication for **UAA** is enabled.

5. Select **Authenticator**.
Currently, Google authenticator is the only available authenticator.
6. Restart the **GE Proficy Authentication Tomcat Web Server** service.
7. Activate multi-factor authentication for user logins.
You need to perform the following steps only for the first time for every user login.
 - a. Log in to Configuration Hub with UAA user credentials.
The MFA setup screen appears with a barcode.

Setup Multifactor Authentication

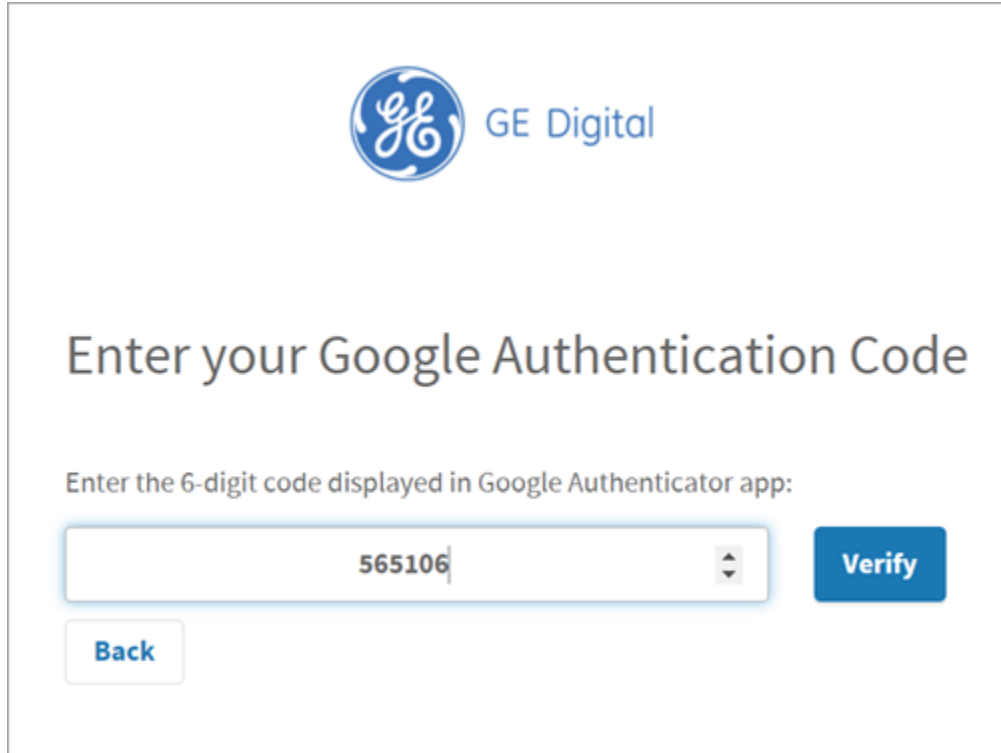
1. Install Google Authenticator on your mobile device from the [App Store on your iPhone](#) or [Google Play on your Android](#).
2. Open Google Authenticator on your mobile device.
3. Tap the "+" button.
4. Tap "Scan barcode".
5. Scan this barcode:



Can't scan barcode? See [manual setup instructions](#).

[Back](#) [Next](#)

- b. Open the Google Authenticator app on your mobile device and scan the barcode.
The authentication app validates the user login and displays a 6-digit code. Barcode scanning appears only for the first time validation for every user login.
- c. On your browser, select **Next** on the MFA setup screen.
The code verification screen appears.
- d. Enter the 6-digit code in the passcode field and select **Verify**



The screenshot shows the GE Digital login interface. At the top center is the GE logo, a blue circle with the letters 'GE' inside, followed by the text 'GE Digital' in a blue sans-serif font. Below this, the main heading reads 'Enter your Google Authentication Code' in a large, dark grey font. Underneath the heading is a smaller instruction: 'Enter the 6-digit code displayed in Google Authenticator app:'. A white input field with a light blue border contains the code '565106' and a small dropdown arrow on the right. To the right of the input field is a blue button with the white text 'Verify'. Below the input field is a white button with a blue border and the blue text 'Back'.


You are logged in successfully.

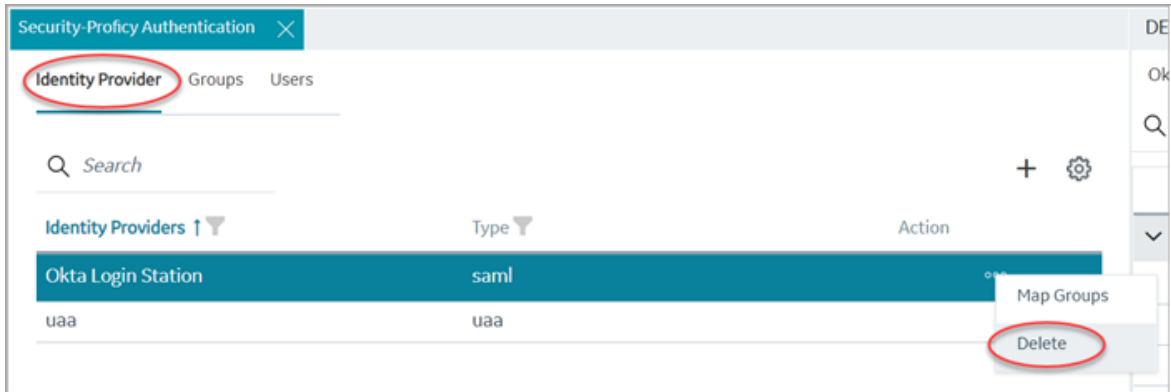
Multi-factor authentication is enabled for both UAA and LDAP users.

Delete Identity Provider

This topic describes how to delete identity providers.

[Add SAML Identity Provider \(on page 46\)](#)

1. Log in to Configuration Hub as an administrator.
2. Go to **Proficy Authentication > Security > Identity Provider**.
The existing list of identity providers appear.
3. Select the identity provider you want to delete.
Additional options appear under the **ACTION** column.
4. Select , then **Delete**.



A message appears to confirm the delete action.

5. Select **Delete**.

The identity provider record is deleted from the Proficy Authentication database.

Manage Groups

Overview of Managing Groups in Proficy Authentication

Groups are a collection of users who share common roles or responsibilities. Administrators can assign permissions and policies to entire groups, rather than individual users.

Groups make it easier to manage access control for multiple users with common requirements. Depending on your group membership, you will have access to different areas of an application. You can create groups and assign scopes that define the permission level granted to a client application.

- [Scopes for Proficy Authentication Users/Groups \(on page 53\)](#)
- [Scopes for Operations Hub Users/Groups \(on page 53\)](#)
- [Scopes for iFIX Users/Groups \(on page 54\)](#)
- [Scopes for Historian Users/Groups \(on page 55\)](#)
- [Scopes for Plant Applications Users/Groups \(on page 57\)](#)

Refer to these topics on how to work with groups within Proficy Authentication:

- [Create Groups \(on page 58\)](#)
- [Modify Groups \(on page 60\)](#)
- [Map Groups \(on page 61\)](#)
- [Add/Remove Users in a Group \(on page 64\)](#)

- [Add/Remove Sub-Groups in a Group \(on page 65\)](#)
- [Delete Group \(on page 66\)](#)

Scopes for Proficy Authentication Users/Groups

This topic provides a list of scopes you can assign to users/groups for accessing Proficy Authentication.

Refer to the Cloud Foundry's documentation for a complete list of UAA scopes.


<https://docs.cloudfoundry.org/concepts/architecture/uaa.html#uaa-scopes>

Scopes for Operations Hub Users/Groups

This topic provides a list of scopes you can assign to users/groups for accessing Operations Hub.

To access both the designer and runtime features in Operations Hub, a user must possess, at a minimum, the `iqp.developer` and `iqp.user` scopes.

Scope	Description
<code>iqp.developer</code>	<p>This scope is assigned to developer users.</p> <p>When a developer account is created, an associated application user account is automatically generated, sharing the same login credentials. Users with this scope have the ability to access pages for application creation, granting them access to both application design and runtime functionality.</p>
<code>iqp.user</code>	<p>This scope is assigned to application users.</p> <p>Users with this scope can only access those applications in Operations Hub to which they have been granted access. These users do not have the ability to access pages for application creation. Their access is solely restricted to the runtime functionality of the applications.</p>
<code>iqp.clouduser</code>	<p>This scope is assigned to users who want to use the REST API, mainly the M2M Device RESTful APIs.</p>
<code>iqp.nodered</code>	<p>This scope is assigned to users who want to access the Dataflow Editor.</p>
<code>iqp.studioAdmin</code>	<p>This scope is assigned to privileged users.</p>

Scope	Description
	<p>Users with this scope can access the Administrator Console to configure global settings for an Operations Hub instance, such as the settings for email servers and the MQTT brokers for MQTT data interoperability.</p> <div data-bbox="574 426 1421 604" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: This scope does NOT grant access to Operations Hub designer or runtime. </div>
<code>iqp.tenantAdmin</code>	<p>This scope is assigned to privileged users.</p> <p>Users with this scope gain administrative authority at the Tenant or System level (in our case, we have one tenant). They enjoy full administrative access to the Operations Hub instance, with the exception of scenarios requiring membership in the <code>iqp.studioAdmin</code> group. Administrators with this scope have the ability to unlock an application that may be locked by another user.</p>

Scopes for iFIX Users/Groups

This topic provides a list of scopes you can assign to users/groups for accessing iFIX.

Refer to the following table to assign access to specific areas/functionalities of iFIX:

Scope	Description
<code>scada.fix.shared_IFIX_PROFICY_AUTH_ADMIN</code>	<p>Allows access to all iFIX application features. Any Proficy Authentication user who is a member of this group will have privileges similar to a native iFIX ADMIN user (except the access to security areas). Proficy Authentication users who want to directly log in to iFIX can use this group.</p> <p>This group is not available by default when you upgrade from iFIX 6.1 or 6.5. You must manually create this group with all the iFIX application features as needed.</p>
<code>scada.fix.shared.APPLICATION_DESIGNER</code>	<p>Allows a user to access Configuration Hub and provides use of iFIX features such as iFIX connection, database, and model management.</p>

Scope	Description
	<p>! Important:</p> <p><code>scada.fix.shared.APPLICATION_DESIGNER</code> is not available by default when you upgrade from iFIX 6.1 or 6.5. You must manually create the group with the required iFIX application features, or update your existing groups to include the following iFIX application features (if you want users in these groups to have access to and use Configuration Hub).</p> <ul style="list-style-type: none"> • Database Block Add-Delete • Database Manager • Database Reload • Database Save • Security Configuration • System Configuration
<code>scada.fix.shared.OPERATORS</code>	Allows run mode only access for a user in iFIX.
<code>scada.fix.shared.SUPERVISORS</code>	Allows access to WorkSpace run and configure mode, as well as access to background task exit, iFIX system shut down, and iFIX system user login.
<code>scada.proficy.admin:</code>	Allows the Proficy Authentication user access to the iFIX Projects panel and to the Deploy operations from Configuration Hub. This group is for Proficy Authentication only; this group is not linked to any iFIX group and has no permissions in iFIX.

Scopes for Historian Users/Groups

This topic provides a list of scopes you can assign to users/groups for accessing Historian.

Refer to the following table to assign access to specific areas/functionalities of Historian:

Scope	Description
<code>historian_visualization.admin</code>	Provides access to Trend Client and the Web Admin console.
<code>historian_visualization.user</code>	Allows access to Trend Client.
<code>historian_rest_api.read</code>	Provides read access to public REST API.
<code>historian_rest_api.write</code>	Provides write access to public REST API.
<code>historian_rest_api.admin</code>	Provides read/write access to public REST API.
<code>historian_enterprise.admin</code>	Provides read/write access to Configuration Hub APIs.
<code>historian_enterprise.user</code>	Allows access to Configuration Hub APIs.
<code>ih_archive_admins</code>	Provides the ability to create, modify, and remove archives.
<code>ih_audited_writers</code>	Allows data writes and to produce a message each time a data value is added or changed.
<code>ih_collector_admins</code>	Allows the ability to add collector instances and change their destination.
<code>ih_readers</code>	Provides access to the ability to read data and system statistics. Also allowed access to Historian Administrator.
<code>ih_security_admins</code>	Provides access to Historian power security users. Security administrators have rights to all Historian functions.
<code>ih_tag_admins</code>	Provides access to allow the ability to create, modify, and remove tags. Tag-level security can override rights given to other Historian security groups. Tag admins can also browse collectors.
<code>ih_unaudited_logins</code>	Allow connections to the Data Archiver without creating login successful audit messages.
<code>ih_unaudited_writers</code>	Provides the ability to write data without creating any messages. Tag, archive, and collector changes log

Scope	Description
	messages regardless of whether the user is a member of the ih_audited_writers group.
historian_visualization.admin	Provides access to Trend Client and the Web Admin console.
historian_visualization.user	Allows access to Trend Client.

Scopes for Plant Applications Users/Groups

This topic provides a list of scopes you can assign to users/groups for accessing Plant Applications.

By default, Plant Applications administrative users are granted all the scopes. For other type of users, you need to assign the specific scope to grant access to the respective module.

These are the scopes associated with the different modules of Plant Applications:

Scope	Applies To
mes.route_management.user	Route Editor
mes.security_management.user	Security
mes.time_booking.user	Time Booking
mes.operations.user	Unit Operations
mes.waste.user	Waste
mes.order_management.user	Work Order Manager
mes.work_queue.user	Work Queue
mes.lineoverview.user	Line Overview
mes.my_machines.user	My Machines
mes.ncm_management.user	Non Conformance
mes.equipment.user	OEE Dashboard
mes.operatorlog.user	Operator Log
mes.process_orders.user	Process Orders
mes.property_definition.user	Property Definition
mes.receiving_inspection.user	Receiving Inspection

Scope	Applies To
<code>mes.reports.user</code>	Reports
<code>mes.genealogy.user</code>	Genealogy
<code>mes.activities.user</code>	Activities
<code>mes.alarms.user</code>	Alarm Notifications
<code>mes.alarms.user</code>	Alarms
<code>mes.analysis.user</code>	Analysis
<code>mes.approval_cockpit.user</code>	Approval Cockpit
<code>mes.autolog.user</code>	Autolog
<code>mes.bom_editor.user</code>	BOM Editor
<code>mes.configuration_management.user</code>	Configuration
<code>mes.downtime.user</code>	Downtime
<code>mes.engineeringChangeOrder.user</code>	Engineering Change Orders

Create Groups

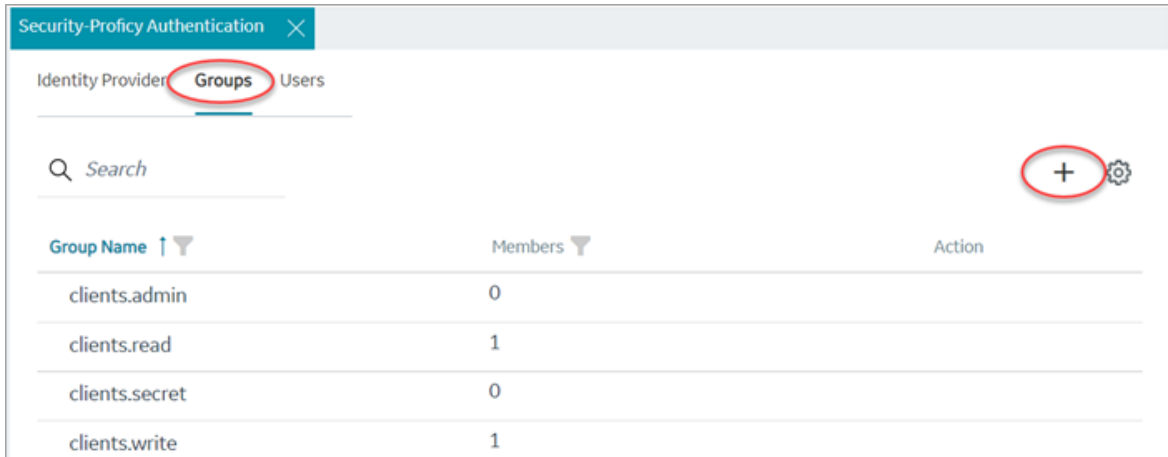
This topic describes how to create new groups in Proficy Authentication.

Log in to Configuration Hub as an administrator.

For example, you can create a group for 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. Go to **Proficy Authentication > Security > Groups**.
2. Select **+**



The **Add Group** screen appears.

- Enter the following details for the new group.

Field	Description
Group Name	A unique name of the group that does not match with any existing Proficy Authentication groups. For example, <code>Supervisors_LineA</code>
Description	A brief description of the group.

Add Group

Group Name*

Supervisors_LineA

Description

Members to monitor LineA

Cancel
Add

- Select **Add**.

The group is created successfully.

The newly created group is added to the list of groups on the **Groups** tab.

Modify Groups

This topic describes how to modify existing groups in Proficy Authentication.

Log in to Configuration Hub as an administrator.


You can modify a group to:

- [Add/Remove Users in a Group \(on page 64\)](#)
- [Add/Remove Sub-Groups in a Group \(on page 65\)](#)
- [Map Groups \(on page 61\)](#)

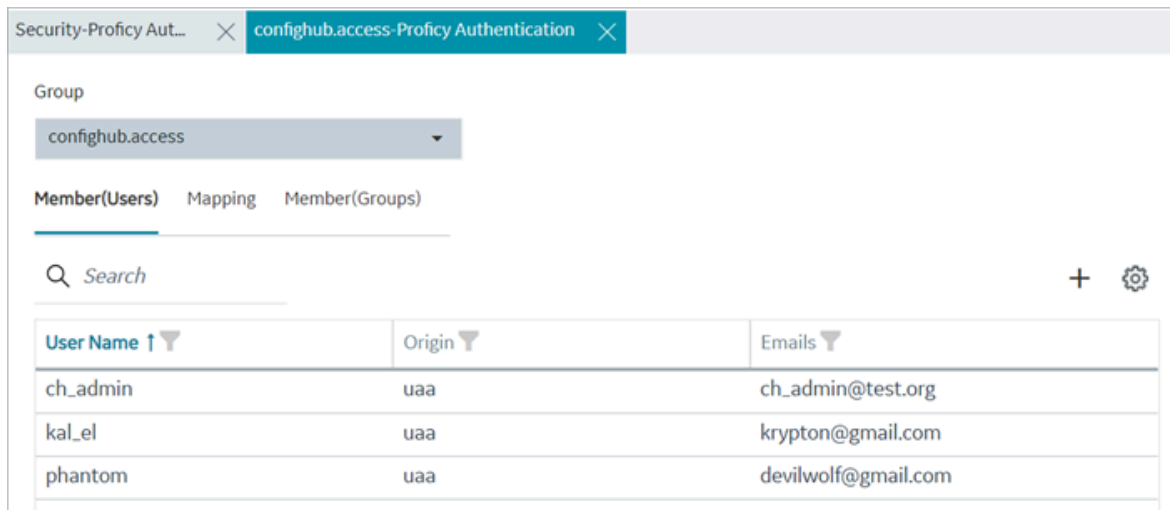
1. Go to **Proficy Authentication > Security > Groups**.

The existing list of Proficy Authentication groups appear.

2. Use any of these options to open a group.

- Double-click the group name you want to modify.
- For the group you want to modify, from its **ACTION** column, select , then **Edit**.

The group opens in a new tab.



User Name ↑	Origin	Emails
ch_admin	uaa	ch_admin@test.org
kal_el	uaa	krypton@gmail.com
phantom	uaa	devilwolf@gmail.com

3. You can modify the following:

Tab	Description
Member (Users)	Displays the list of users added to this group. Add/Remove Users in a Group (on page 64) .

Tab	Description
Mapping	Displays the list of mapped groups for this group. You can add/remove mapped groups (on page 61) .
Member (Groups)	Displays the list of sub-groups added to this group. Add/Remove Sub-Groups in a Group (on page 65) .

Map Groups

This topic describes how to perform group mapping.

Log in to Configuration Hub as an administrator.

You can map any of the following to a Proficy Authentication group. The users belonging to these groups gain access to Proficy Authentication, and become a member of the target group.

- UAA groups
- LDAP
- SAML groups

1. Go to **Proficy Authentication > Security > Groups**.

The existing list of Proficy Authentication groups appear.

2. Double-click and open the group you want to map to UAA/LDAP/SAML groups.


3. Select the **Mapping** tab.

4. Map UAA groups.

a. From the **Identity Provider** drop down list, select the UAA record.

The groups from the UAA record appear.



b. Select the check box for the groups you want to map to the Proficy Authentication group selected in step 2.

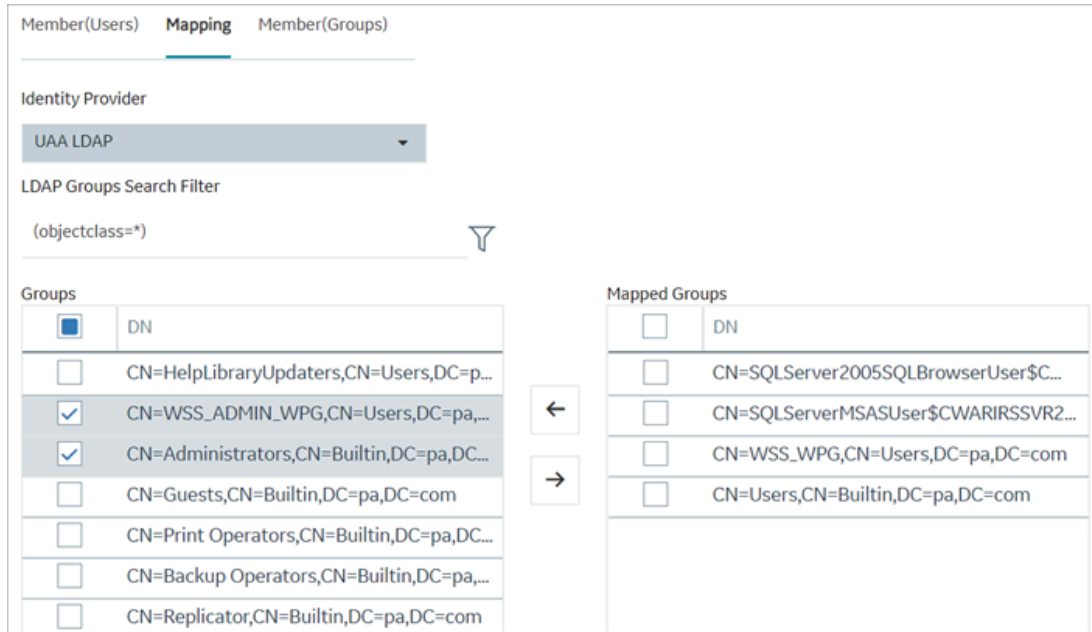
c. Select  to move the selected items from **Groups** to **Mapped Groups**.

The screenshot shows a web interface for mapping groups. At the top, there's a 'Group' dropdown menu with 'confighub.access' selected. Below it are three tabs: 'Member(Users)', 'Mapping' (which is active), and 'Member(Groups)'. Underneath the tabs is an 'Identity Provider' dropdown menu with 'uaa' selected. The main area is divided into two columns: 'Groups' and 'Mapped Groups'. The 'Groups' column has a table with a 'Display Name' header and several rows: 'cloud_controller.admin' (with a checked checkbox), 'clients.read', 'clients.secret', 'uaa.admin', and 'clients.admin'. The 'Mapped Groups' column has a similar table with 'Display Name' header and rows for 'scim.invite' and 'uaa.resource'. Between the two columns are two arrow buttons: a left-pointing arrow and a right-pointing arrow.

The users belonging to the mapped UAA groups are now a member of the Proficy Authentication group selected in step 2.

5. Map LDAP groups.

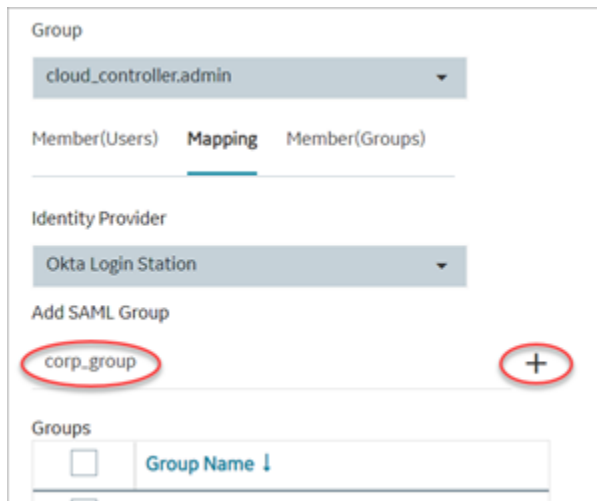
- a. From the **Identity Provider** drop down list, select the LDAP record.
The groups from the LDAP server appear.
- b. Select the check box for the groups you want to map to the Proficy Authentication group selected in step 2.
- c. **Optional:** To search for an LDAP group, enter the keyword in the **LDAP Groups Search Filter** field and select .
- d. Select  to move the selected items from **Groups** to **Mapped Groups**.




The users belonging to the mapped LDAP groups are now a member of the Proficy Authentication group selected in step 2.

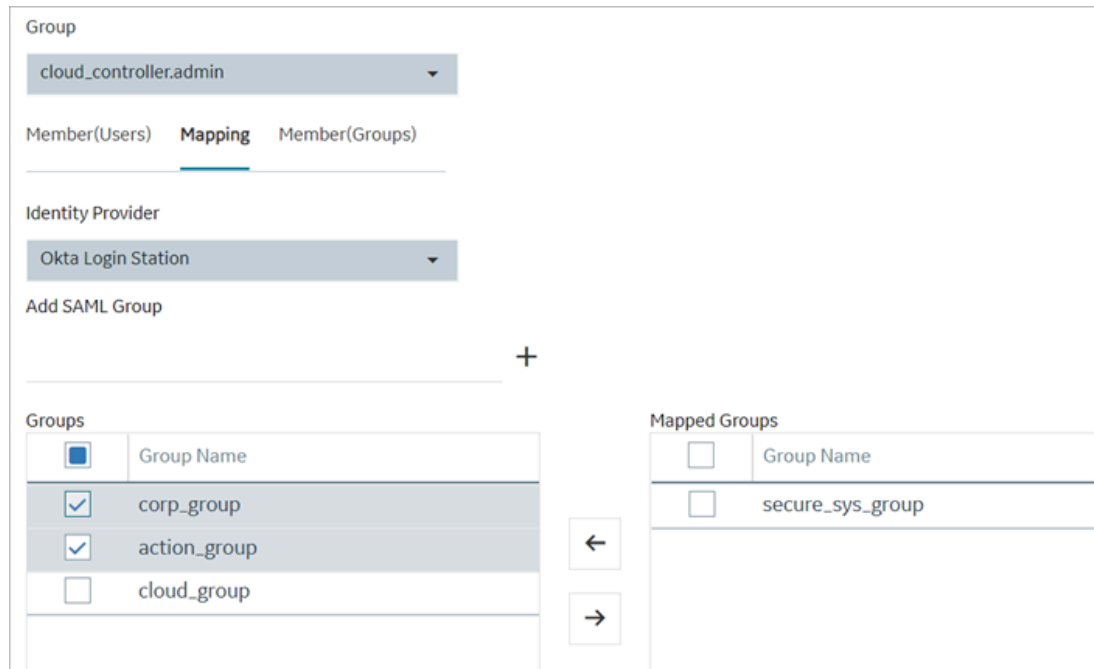
6. Map SAML groups.

- a. From the **Identity Provider** drop down list, select the SAML record.
- b. To create SAML groups, enter the valid SAML group name in the **Add SAML Group** field and select the plus icon.



- c. Select the check box for the groups you want to map to the Proficy Authentication group selected in step 2.

d. Select  to move the selected items from **Groups** to **Mapped Groups**.



The screenshot shows the 'Mapping' configuration page. At the top, the 'Group' is set to 'cloud_controller.admin' and the 'Identity Provider' is 'Okta Login Station'. Below this, there are two tables for group management. The 'Groups' table on the left contains a list of groups with checkboxes: 'corp_group' (checked), 'action_group' (checked), and 'cloud_group' (unchecked). The 'Mapped Groups' table on the right contains 'secure_sys_group' (unchecked). Between the two tables are left and right arrow buttons for moving items between the lists.

If the mapped SAML groups are valid, then all their users become a member of the Proficy Authentication group selected in step 2.


7. To unmap any of the mapped groups, select and move them back to **Groups**.

UAA/LDAP/SAML groups are successfully mapped.

Add/Remove Users in a Group

This topic describes how to add or remove users from a group.

[Modify a group \(on page 60\)](#) to add or remove users.

1. Select the **Member (Users)** tab.
2. Select .

The **Map User** screen appears.
3. Select the check box for the user account you want to add to the group.

To remove user from a group, clear the check box.

Map User

Q Search

<input checked="" type="checkbox"/>	User List ↑
<input checked="" type="checkbox"/>	ch_admin
<input checked="" type="checkbox"/>	kal_el
<input type="checkbox"/>	mandrake_01
<input checked="" type="checkbox"/>	phantom

NOTE: Mapping supported for UAA users only.

Cancel Apply

4. Select **Apply**.

The users are added to (or removed from) the group.

Add/Remove Sub-Groups in a Group

This topic describes how to add or remove sub-groups from a group.

[Modify a group \(on page 60\)](#) to add or remove sub-groups.

1. Select the **Member (Groups)** tab.
2. Select **+**.
The **Group Membership** screen appears.
3. Select the check box for the group/s you want to add as a sub-group.
To remove a sub-group from a group, clear the check box.

Group Membership

🔍 Search

<input checked="" type="checkbox"/>	GROUPNAME ↑
<input type="checkbox"/>	clients.admin
<input type="checkbox"/>	clients.read
<input checked="" type="checkbox"/>	clients.secret
<input type="checkbox"/>	clients.write
<input checked="" type="checkbox"/>	cloud_controller.admin
<input type="checkbox"/>	confighub.admin



Important:

Do not select the check box for `igp.studioAdmin` group for any users or groups. As this group is for reserved purposes, make sure no user accounts or groups are assigned to this group to avoid runtime errors.

4. Select **Apply**.

The groups are added (or removed) as sub-groups in the group.

The users added to the sub-groups are automatically associated to the main group.

Delete Group

This topic describes how to delete Proficy Authentication groups.

Log in to Configuration Hub as an administrator.

1. Go to **Proficy Authentication > Security > Groups**.

The existing list of groups appear.

2. Select the group you want to delete.

Additional options appear under the **ACTION** column.

3. Select , then **Delete**.

Group Name	Members	Action
clients.admin	0	
clients.read	1	<div style="border: 1px solid gray; padding: 2px;"> Edit Delete </div>
clients.secret	0	
clients.write	1	
cloud_controller.admin	0	

A message appears to confirm the delete action. The message also informs if users are associated to the group being deleted.

4. Select **Delete**.

The group account is deleted from the Proficy Authentication database.

Manage Users

Create Users

This topic describes how to create new users in Proficy Authentication.

Log in to Configuration Hub as an administrator.

1. Go to **Proficy Authentication > Security > Users**.
2. Select **+**

User Name	Email	Origin	Action
ch_admin	ch_admin@test.org	uaa	
ka_l_el	krypton@gmail.com	uaa	
mandrake_01	magician@gmail.com	uaa	
phantom	devilwolf@gmail.com	uaa	

The **Add User** screen appears.

- Enter the following details for the new user account.

Field	Description
User Name	The user name to log in to Proficy Authentication.
Password	The password to log in to Proficy Authentication.
Confirm Password	Enter the password again for confirmation.
Email	User's email address.

Add User

User Name*
sys_admin

Password*
.....

Confirm Password*
.....

Email*
pacman@gmail.com


Cancel Add

- Select **Add**.

The user is created and added to the list of user accounts on the **Users** tab.

The new user is associated to default Proficy Authentication groups. These default groups cannot be deleted or modified: `approvals.me`, `cloud_controller.read`, `cloud_controller.write`, `cloud_controller_service_permissions.read`, `oauth.approvals`, `openid`, `password.write`, `profile`, `roles`, `scim.me`, `scim.userids`, `uaa.offline_token`, `uaa.user`, `user_attributes`.

Every user/client must possess the following three scopes to access the Security plug-in via Configuration Hub. If these scopes are not added, then a warning message alerts the user to contact Admin.

Scope	Description
<code>uaa.admin</code>	This scope indicates that this is a superuser.
<code>clients.write</code>	This scope resets the Security plug-in's admin client secret.
<code>password.write</code>	This admin scope enables to change the user password. <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;">  Note: This scope is assigned to all the UAA/LDAP/SAML users by default without the need to assign manually. </div>

Default `ch_admin` has all the three scopes.

For user accounts originating from LDAP or SAML, refer to [Add LDAP/SAML Users \(on page 69\)](#).

Add LDAP/SAML Users

This topic describes how to add LDAP/SAML users to Proficy Authentication.

You must have an LDAP or SAML user account.

Only user accounts created in Proficy Authentication are immediately visible in the users list. LDAP or SAML users must perform the following steps to create user accounts in Proficy Authentication.

Log in to Proficy Authentication with LDAP/SAML user credentials.

A shadow user is created in Proficy Authentication, and can be subsequently seen in the Proficy Authentication users list.

The LDAP/SAML user account is added to the list of accounts on the **Users** screen.

Add/Remove Groups for a User

This topic describes how to modify group membership for existing user accounts.

[Create Users \(on page 67\)](#)

While it is possible to assign multiple scopes/groups to clients and users, it is advisable to exercise caution and follow these recommendations:

- **Adhere to the principle of least privilege:** Applying this principle helps to minimize potential security risks. It advocates to grant users only the necessary privileges and permissions to perform their tasks effectively. If you assign too many scopes to users, it can lead to unnecessary privileges, thus increasing the attack surface and potential for unauthorized access.
- **Keep the token size within acceptable limits:** The size of an Access token or JWT (JSON Web Token) commonly used for authentication and authorization purposes, can vary depending on the number of scopes assigned to a user. If a user has an excessive number of scopes, the size of the JWT can become significant. As a result, when the user attempts to access an application, the HTTP requests made by the application to validate the token may get impacted. In case the default settings of the web server hosting the application has limitations on request size, then the request can get blocked or rejected if the token size exceeds the set limit.

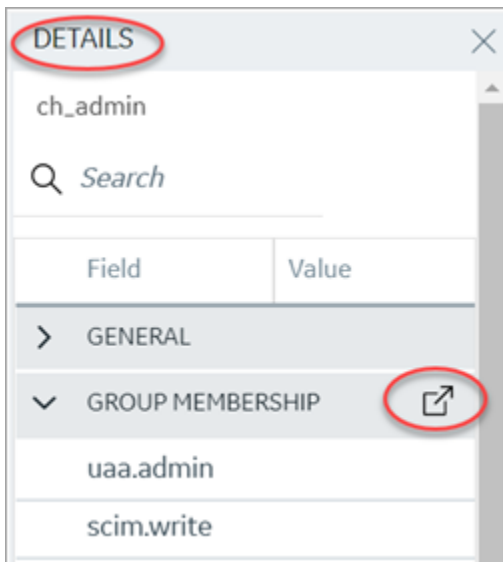
1. Go to **Proficy Authentication > Security > Users**.

The existing list of user accounts appear.

2. Select the user account for which you want to modify group membership.

The existing information for the user appears on the **DETAILS** panel.

3. Select  next to the **GROUP MEMBERSHIP** section.



The **Group Membership** screen appears.

4. Select the check box for the groups you want to add the user as a member.

To remove a group, clear the check box.

Group Membership

🔍 Search

<input checked="" type="checkbox"/>	GROUPNAME ↑
<input type="checkbox"/>	clients.admin
<input checked="" type="checkbox"/>	clients.read
<input type="checkbox"/>	clients.secret
<input checked="" type="checkbox"/>	clients.write
<input type="checkbox"/>	cloud_controller.admin
<input checked="" type="checkbox"/>	confighub.access

Cancel Apply



Important:

Do not select the check box for `iqp.studioAdmin` group for any users or groups. As this group is for reserved purposes, make sure no user accounts or groups are assigned to this group to avoid runtime errors.

5. Select **Apply**.

The groups are added (or removed from) for the user.



Note:

If a logged-in user attempts to remove his/her own scopes/groups, the remove operation may fail and result in an error: `Error while assigning the group`. In such instances, the user should log out of the Configuration Hub application and log-in again. We recommend that logged-in users should avoid removing their own scopes.

Reset User Password

This topic describes how to reset passwords for Proficy Authentication users.

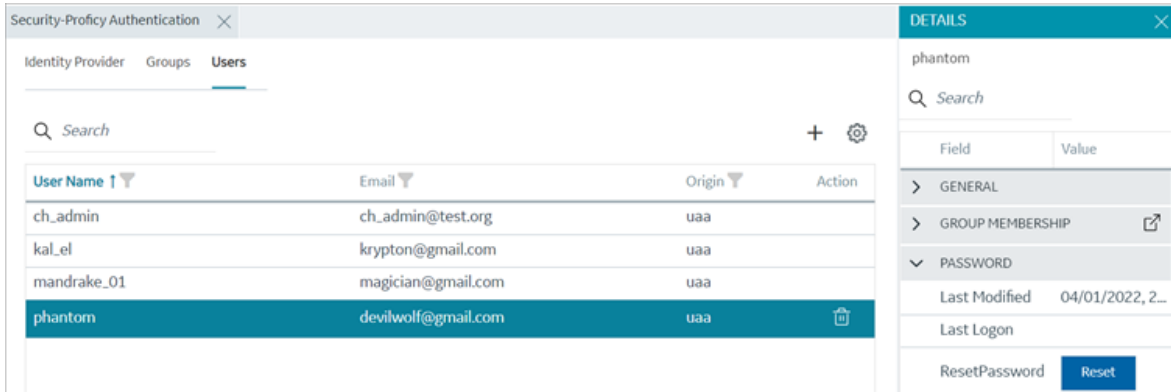
Log in to Configuration Hub as an administrator.

1. Go to **Proficy Authentication > Security > Users**.

The existing list of user accounts appear.

2. Select the user account for which you want to reset the password.

The option to reset password appears on the **DETAILS** panel under the **PASSWORD** section.



3. Select **RESET**.

The **Password Reset** screen appears.

4. Enter the new **Password** and **Confirm Password** for the user account.

The screenshot shows the 'Password Reset' form. It has three input fields: 'User Name*' with the value 'phantom', 'Password*' with masked characters and a toggle icon, and 'Confirm Password*' with masked characters and a toggle icon. At the bottom, there are two buttons: 'Cancel' and 'ResetPassword'.

5. Select **Reset Password** to apply the changes.

The password is reset for the user.

Delete User

This topic describes how to delete Proficy Authentication user accounts.

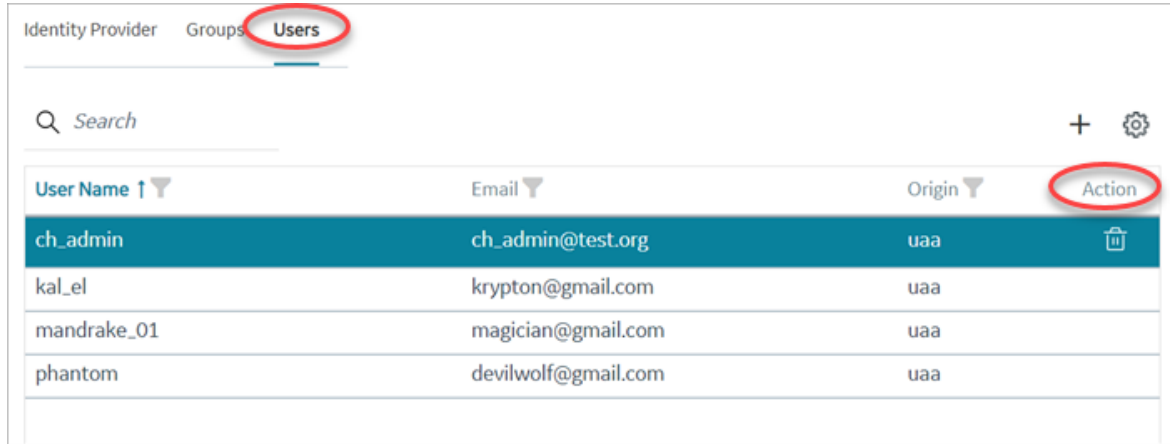
Log in to Configuration Hub as an administrator.

1. Go to **Proficy Authentication > Security > Users**.

The existing list of user accounts appear.

2. Select the user you want to delete.

Delete option appears in the **ACTION** column.



User Name ↑	Email	Origin	Action
ch_admin	ch_admin@test.org	uaa	
kal_el	krypton@gmail.com	uaa	
mandrake_01	magician@gmail.com	uaa	
phantom	devilwolf@gmail.com	uaa	

3. Select .

A message appears to confirm the delete action.

4. Select **Delete**.

The user account is deleted from the Proficy Authentication database.

Windows Integrated Authentication / Auto-login

Windows Integrated Authentication is a new capability added to Proficy Authentication Service from version 2022.

When Windows Integrated Authentication or Auto-login is enabled, users logged into any Windows machine in a domain are able to access Operations Hub and/or hosted Proficy applications without the need to type in their Windows credentials again. The same Windows logged-in user context is used for authenticating the user. Based on the user's privileges, access is provided to Operations Hub and/or its hosted applications.

This document describes the steps to configure the 'Windows Integrated Authentication' functionality in an instance of Proficy Authentication service. After configuring auto-login, when you attempt to log into Operations Hub / hosted Proficy applications, the **Select Authentication** screen appears (see figure below) to choose between `Standard Proficy Authentication Login` Or `Active Directory (Windows) Integrated Login`.

If you choose `Active Directory (Windows) Integrated Login`, the authentication option will follow the new flow and you will not be prompted for providing credentials. Whereas choosing `Standard Proficy Authentication Login` will take you through the normal authentication flow and prompt for your credentials.



Note:

- The auto-login capability is only for authenticating the users. For authorization or access permissions, you have to configure LDAP IDP. To accomplish this, select the same active directory service / LDAP server, which brings the authentication service node, application accessing nodes in the network, and the users seeking auto-login, into the same Windows scope.
- For configuring LDAP IDP, refer to [Add LDAP Identity Provider \(on page 15\)](#).

Select Authentication

Standard Proficy Authentication Login

Active Directory (Windows) Integrated Login

Don't ask me again.

<p>Standard Proficy Authentication Login</p>	<p>Choose this option if you want to use the standard login (username/password or SAML).</p> <p>This is a regular login, which is based on username/password, including LDAP, or SAML.</p>
<p>Active Directory (Windows) Integrated Login</p>	<p>This option appears only if Windows auto-login is configured.</p> <p>This allows to automatically log into Operations Hub using the user's domain login session that was used to log in to Proficy Authentication.</p>
<p>Don't ask me again</p>	<p>Select this check box, if you don't want to display the Select Authentication screen every time you login.</p> <p>The system remembers the last selected authentication (between regular and autologin) and applies it for future logins.</p>

	<p>With Don't ask me again enabled, you can clear the last selected authentication only during logout.</p> <div data-bbox="537 296 1118 678" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>You have logged out</p> <hr/> <p>You should now close the browser,</p> <p>or click here to login again.</p> <p>You may also click here to clear the previously selected authentication option.</p> </div> <p>Select You may also click here to clear the previously selected authentication option to clear the saved selection. Once cleared, the clearing option is hidden from the logout screen.</p> <p>Select click here to login again to return to the login page.</p>
Defer	<p>Select to dismiss this screen, and skip selecting an authentication. You have the choice to select authentication next time you login.</p>

To configure Windows Auto-login, an administrator performs the following tasks only for the first time. The first task is performed on all the participating nodes (Active Directory service node, Proficy Authentication service node, and the client nodes). The second and third are performed on the Windows Active Directory Server machine. The fourth task is performed on the machine where Proficy Authentication is installed.

1. [Configure Security Policy \(on page 76\)](#).
2. [Create a service principal for your user account \(on page 78\)](#).
3. [Generate the Kerberos keytab file \(on page 81\)](#).
4. [Update the Proficy Authentication .yml file \(on page 84\)](#).
5. [Add LDAP Identity Provider \(on page 15\)](#) for the Active Directory service used in Steps 2 and 3.



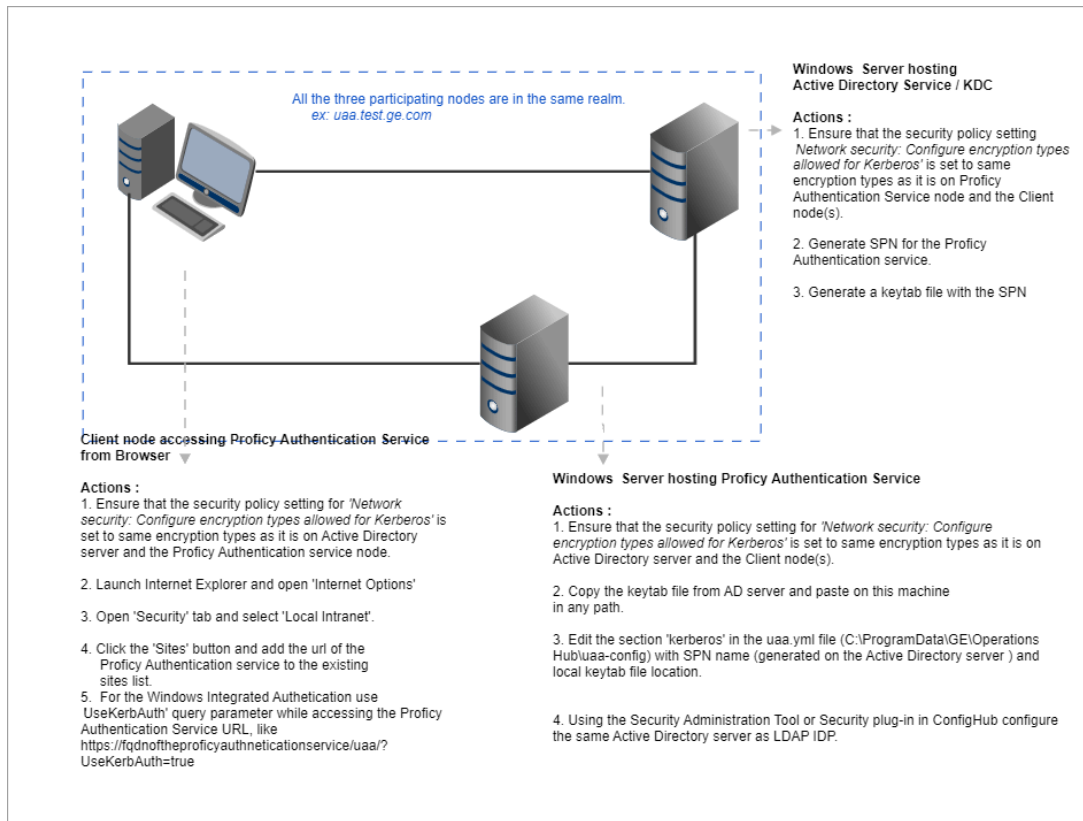
Note:

Users logging into DPM products using Windows Auto-login are authorized / get the scopes based on the LDAP configuration performed in Step 5.

To configure the browser settings for Windows Auto-login, the following task is performed on the end-user machine.

- Configure the browser settings for Kerberos authentication (on page 85).

Figure 1. Windows Auto-login - Deployment Topology and Configuration



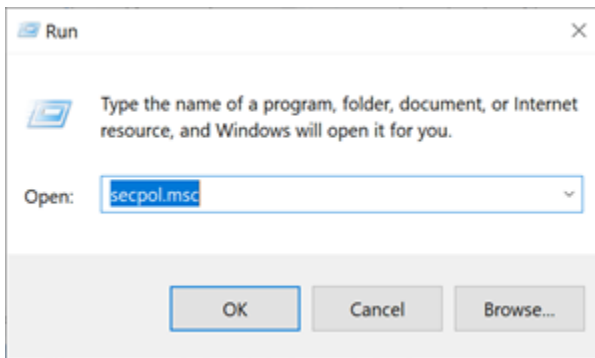
Configure Security Policy

This topic describes how to configure security policy setting associated to Kerberos authentication.

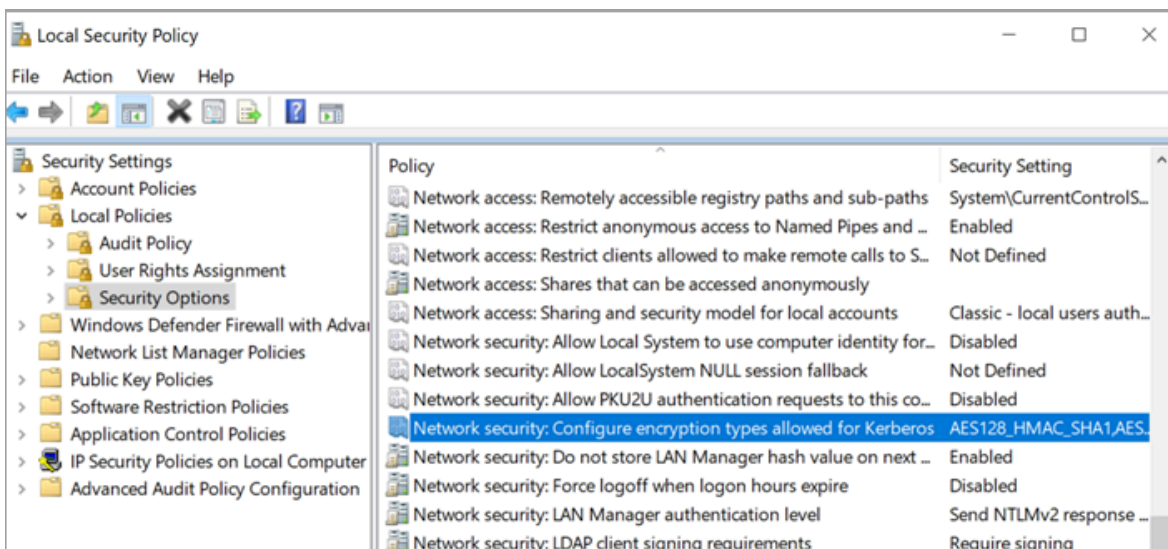
It is possible that you may not have access to your computer's local security policy settings, if it is governed by a group policy (controlled by your domain administrator). In any case, make sure that these security options are enabled for your computer.

If your environment is not governed by a group policy, then follow these steps to configure local security policy:

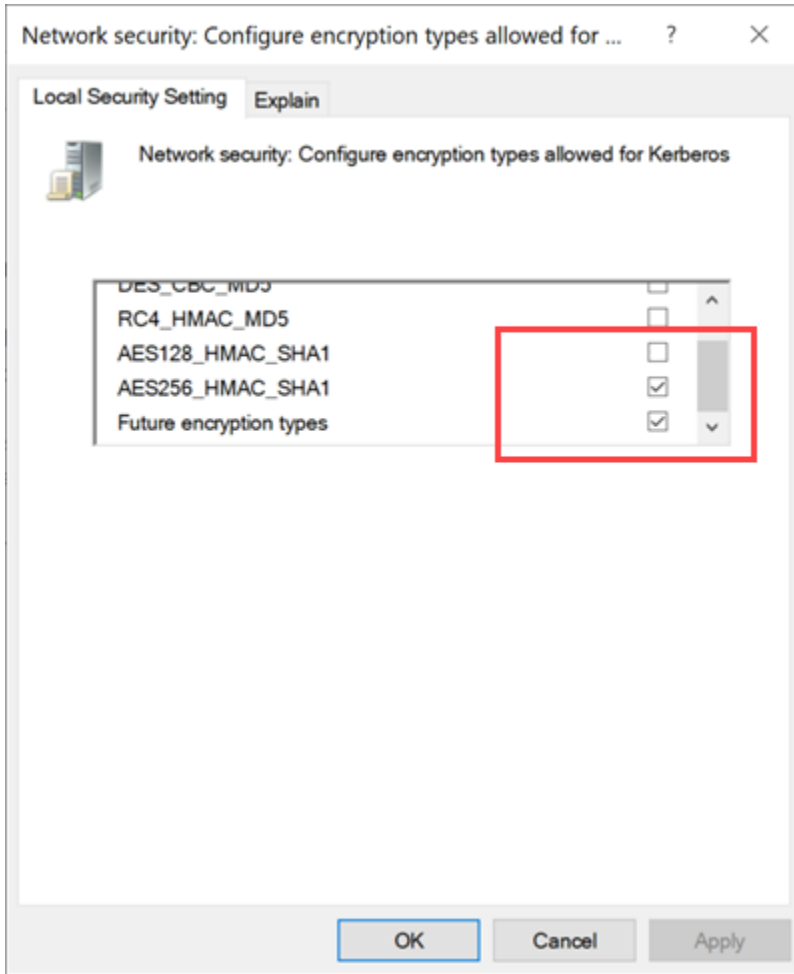
1. To access Local Security Policy, enter `secpol.msc` in Windows Run dialog and select **OK**.



2. Navigate to **Security Settings > Local Policies > Security Options**.



3. Double-click and open `Network security: Configure encryption types allowed for Kerberos` security policy setting.
4. Select the valid encryption types that you want to use as shown in the figure. Ensure that the selection is same across all the participating nodes.
You can select either `AES128_HMAC_SHA1` or `AES256_HMAC_SHA1` as the encryption type. Also select the `Future encryption types` option.



Note:

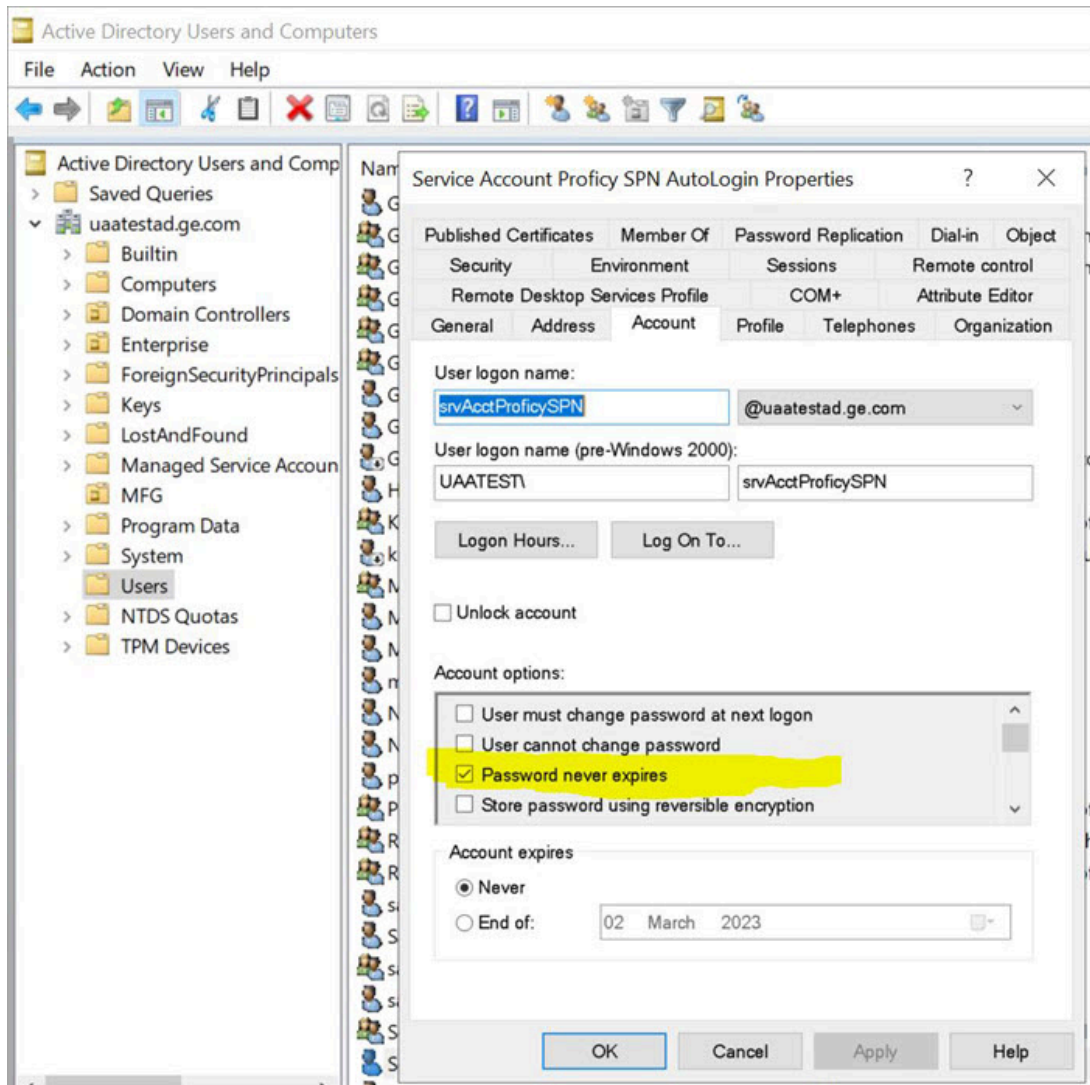
In our current documentation, we use `AES256_HMAC_SHA1` encryption type in our example code to [generate the keytab file \(on page 81\)](#).

For more information refer to [Microsoft documentation](#) on security policy settings.

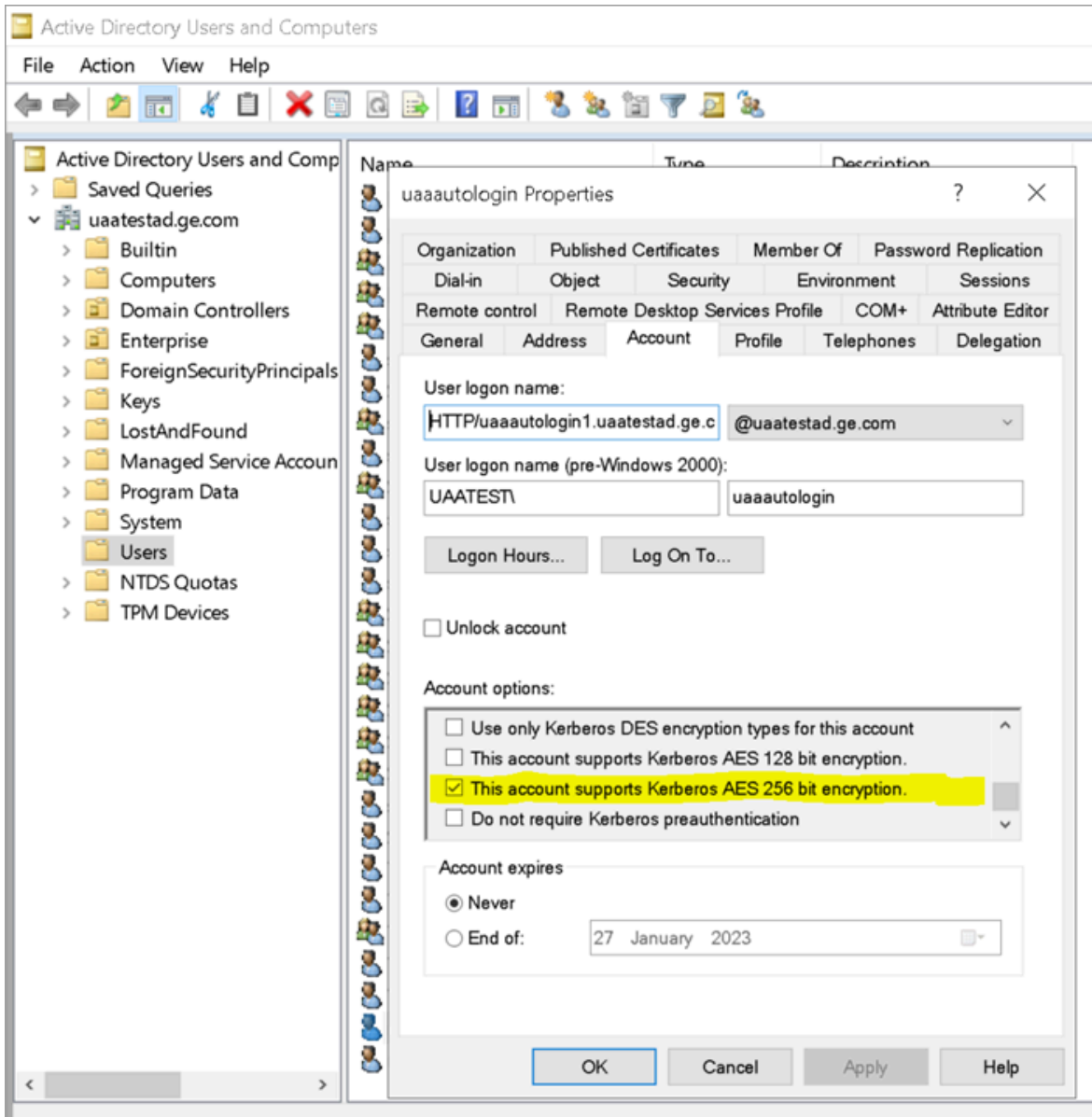
Create Service Principal Name

This topic describes how to create a service principal name.

- Create a managed service user account on the Active Directory Server node to represent the Proficy Authentication application in the active directory registry. Make sure to implement these settings for the account:
 - It is mandatory user is a member of the domain user group. Refer to [Microsoft documentation](#) for more information.
 - Set the account password to never expire. To do so, access the domain user account properties dialog: **Account > Account options > Password never expires**.



- [Configure Security Policy \(on page 76\)](#)




Note:

Delete existing SPNs, if any. Refer to [Useful SPN commands \(on page 126\)](#).

You must be an administrator to perform this task.

1. Log in to the machine where Proficy Authentication is installed.
2. Open the Windows Command Prompt application.

3. Run the following command replacing with the appropriate code: `setspn -S HTTP/<FQDN> <user account>`

Code	Replace With
<FQDN>	<p>Fully Qualified Domain Name (FQDN) of the server on which Proficy Authentication service is running.</p> <p>For example, <code>HTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM</code></p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: These should be in capital letters:</p> <ul style="list-style-type: none"> ◦ HTTP ◦ UAATESTAD.GE.COM (the domain name that follows @) </div>
<user account>	<p>Dedicated managed service user account created for Proficy Authentication service.</p> <p>For example, <code>ghost1</code>.</p>

Based on the above examples, your code should look like this: `setspn -S HTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM ghost1`

The service principal name (SPN) is created.

[Generate Keytab File \(on page 81\)](#)




Generate Keytab File

Generate the Kerberos keytab file.

[Create Service Principal Name \(on page 78\)](#)

You must be an administrator to perform this task.

1. Log in to your system and open the Windows Command Prompt application.
2. Run the following command replacing with the appropriate code: `ktpass -out <filename> -princ HTTP/<service principal name> -mapUser <user account> -mapOp set -pass <password> -crypto AES256-SHA1 -pType KRB5_NT_PRINCIPAL`

Code	Replace With
<filename>	<p>Name of the keytab file.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: Keytab file name can be any given name. </div> <p>The file is created at the default location. You also have the option to specify an absolute path for file creation. For example, <code>-out c:\Documents\myskullcave.keytab</code>.</p>
<service_principal_name>	<p>Enter the service principal name that was created in the following format: <code>HTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM</code></p>
<User account>	<p>Enter the same managed service user account that was used during creating the service principal name.</p> <p>For example, <code>ghost1</code>.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: If you want to use a different user account, delete the existing user account, (or) rename the logon name in the user account. </div>
<password>	<p>Proficy Authentication managed service user account password.</p>
AES256-SHA1	<p>Encryption algorithm you want to use.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin: 10px 0;">  Note: GE recommends <code>AES256-SHA1</code>. But you can also use <code>AES128-SHA1</code>. </div>
KRB5_NT_PRINCIPAL	<p>Encryption type you want to use.</p>

If the keytab is successfully created, the log should look something like this:

```
C:\Users\Administrator>ktpass -out c:\Temp\SACHINJOHUB21VM.uaatestad.ge.com.keytab -princ
HTTP/SACHINJOHUB21VM.uaatestad.ge.com@UAATESTAD.GE.COM -mapUser Mark -mapOp set -pass Gei321itc -crypto
AES256-SHA1 -pType KRB5_NT_PRINCIPAL
Targeting domain controller: uaatestad.uaatestad.ge.com
```

```

Using legacy password setting method

Successfully mapped HTTP/SACHINJOHUB21VM.uaatestad.ge.com to Mark.

Key created.

Output keytab to c:\Temp\SACHINJOHUB21VM.uaatestad.ge.com.keytab:

Keytab version: 0x502

keysize 105 HTTP/SACHINJOHUB21VM.uaatestad.ge.com@UAATESTAD.GE.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x12
(AES256-SHA1) keylength 32 (0x3fb2a2824864a6b3617bfa4a6458af83534efdb8a3eac08b02316cce9c4ee7fc)

```

Example of a failed log:

```

C:\Windows\system32>ktpass -out c:\Temp\win16-sachin.uaatestad.ge.com.keytab -princ

HTTP/sachin.uaatestad.ge.com@UAATESTAD.GE.COM -mapUser John -mapOp set -pass Gei32litc -crypto AES256-SHA1
-pType KRB5_NT_PRINCIPAL

Targeting domain controller: uaatestad.uaatestad.ge.com

Using legacy password setting method

Failed to set property 'userPrincipalName' to 'HTTP/sachin.uaatestad.ge.com@UAATESTAD.GE.COM' on Dn
'CN=John,CN=Users,DC=uaatestad,DC=ge,DC=com': 0x13.

WARNING: Failed to set UPN HTTP/sachin.uaatestad.ge.com@UAATESTAD.GE.COM on
CN=John,CN=Users,DC=uaatestad,DC=ge,DC=com.

kinits to 'HTTP/sachin.uaatestad.ge.com@UAATESTAD.GE.COM' will fail.

Successfully mapped HTTP/sachin.uaatestad.ge.com to John.

Key created.

Output keytab to c:\Temp\win16-sachin.uaatestad.ge.com.keytab:

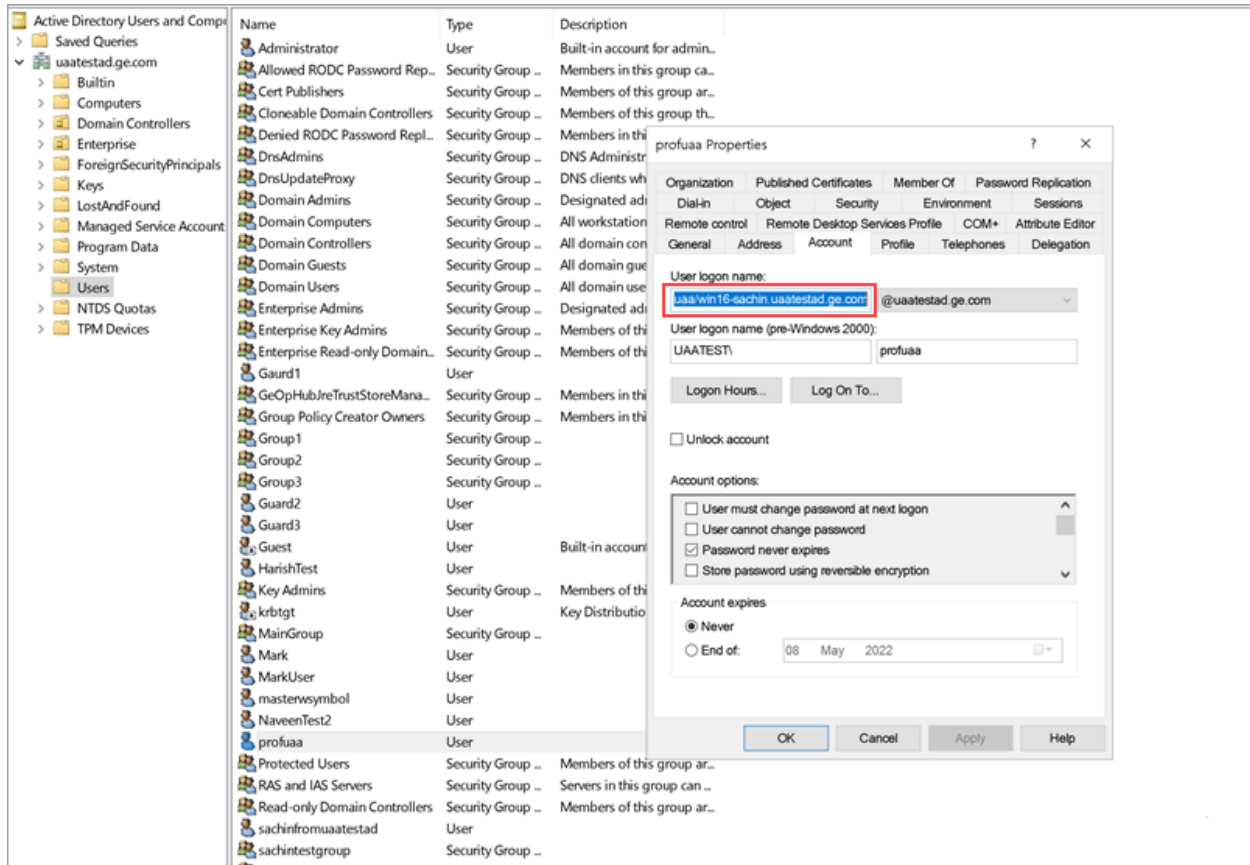
Keytab version: 0x502

keysize 102 HTTP/sachin.uaatestad.ge.com@UAATESTAD.GE.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 9 etype 0x12
(AES256-SHA1) keylength 32 (0x8b551a22050935e9ace848cacbacc86a4eb845e63b6461d4f31b7d815158cf6c)

```

You can also do the following to verify if the service principal is mapped to the managed service user account, and a keytab is created:

1. Go to **Active Directory Users and Computers > Users**.
2. Access the properties of the user account for which you created the keytab file.
3. On the **Account** tab, verify **User logon name**. is pointing to your service principal name.



- Copy the keytab file on the machine, where Proficy Authentication is installed.
- [Update the Proficy Authentication uaa.yml file \(on page 84\).](#)

Proficy Authentication Service Configuration

This topic provides steps to update the Proficy Authentication `uaa.yml` file.

Make sure you have completed the following tasks:

- [Generate Keytab File \(on page 81\).](#)
- Copy the keytab file from the Active Directory server, and paste it anywhere on the Proficy Authentication machine.
- Make a note of the keytab file location on the Proficy Authentication machine.

You must be an administrator to perform this task.

1. Log in to the computer machine where Proficy Authentication is installed.
2. Access the `uaa.yml` file.

The file is located at `C:\ProgramData\Proficy\Operations Hub\uaa-config\uaa.yml`

3. To modify, open `uaa.yml` in any text editor.

Example: Notepad++

4. Search for `kerberos` and enter values for the following keys:

service-principal	Enter the service principal name. For more information, refer to Create Service Principal Name (on page 78) .
keytab-location	Enter the location path where you copied the keytab file on this machine.

For example:

```
kerberos:
  service-principal: HTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM
  keytab-location: 'file:///C:/ProgramData/GE/Proficy Authentication/uaa-config/myskullcave.keytab'
```

5. Save and close the modified file.

6. Restart the `GE Proficy Authentication Tomcat Web Server` service.

- a. Access the Windows Run dialog.
- b. Enter `services.msc` to open the **Services** screen.
- c. Right-click `GE Proficy Authentication Tomcat Web Server` and select **Restart**.

The Proficy Authentication service configuration is updated .

Configure Browser

Configure the browser settings for Kerberos authentication.

Windows Auto-login works if the following tasks are accomplished.

- [Create Service Principal Name \(on page 78\)](#)
- [Generate Keytab File \(on page 81\)](#)
- [Proficy Authentication Service Configuration \(on page 84\)](#)

The steps describe how to configure the browser settings on Internet Explorer (IE). Since IE settings are shared by Chrome, you do not have to configure it separately for the Chrome browser.



Important:

Windows Auto-login is not supported on the node where the Proficy Authentication service is running. To enable auto-login, configure the browser settings on a node different from the Proficy Authentication service node.

1. Go to **Control Panel > Internet Options**

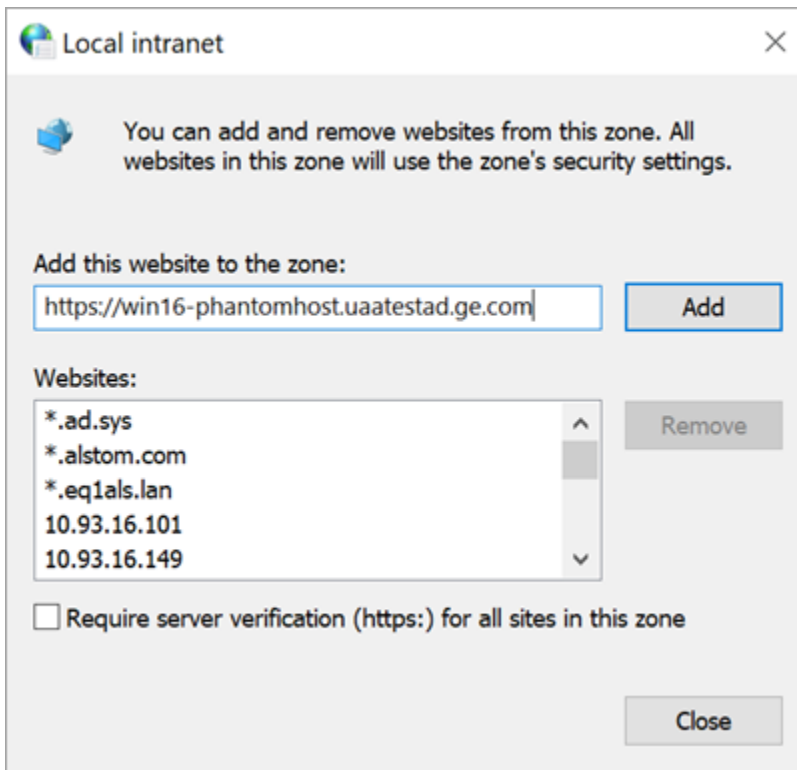
The **Internet Properties** dialog appears.

2. On the **Security** tab, select **Local intranet > Sites**.

The **Local intranet** window appears.

3. Select **Advanced**.

4. In **Add this website to the zone**, enter the URL of the Proficy Authentication service, and then select **Add**.



5. Select **Close**.

6. Select **OK** to close the open windows.

Kerberos supported SPNEGO authentication is enabled on your IE browser.

For Windows Auto-login, use `UseKerbAuth` query parameter while accessing the Proficy Authentication service URL. For example, `https://FQDN of the Proficy Authentication Service Node/uaa/?UseKerbAuth=true`

Example Configuration for Multi-domain and Auto-login Functionality

This topic describes how to set up the auto-login with multi-domain functionality so that users can automatically log in to multiple domains without having to enter their credentials for each domain login.

You should have administrative access to perform the steps described below. You need virtual machines (VM servers) to host the following:

- Forest1 VM server named FORESTPLANT in this topic.
- Forest2 VM server named FORESTCORP in this topic.
- VM server where Proficy Authentication is installed, and can also be utilized for testing purposes.
- However in this topic, we use a separate VM server for testing auto-login with multi-domain functionality.

Benefits of Auto-login with multi-domain functionality:

- eliminates the need for users to remember and enter separate user names and passwords for each domain.
- seamless user experience by automatically logging them across multiple domains with a single authentication event.
- users can save time and effort by avoiding repetitive login procedures.
- while auto-login simplifies the login process, it can also enhance security. It allows for the use of stronger, complex passwords since users don't need to remember them. It reduces the risk of password reuse or weak passwords, which are common security vulnerabilities.

1. Identify the domains where you want to enable auto-login with multi-domain functionality. We shall use the following domains:

- FORESTPLANT
- FORESTCORP

2. Create a domain trust between FORESTPLANT and FORESTCORP.

You can refer to the following links for more information.

- <https://www.youtube.com/watch?v=F7DgXAXNnC8>
- [How trust relationships work for forests in Active Directory](#)
- [Understanding the Global Catalog](#)
- [Global Catalog and LDAP Searches](#)
- [Nesting groups](#)

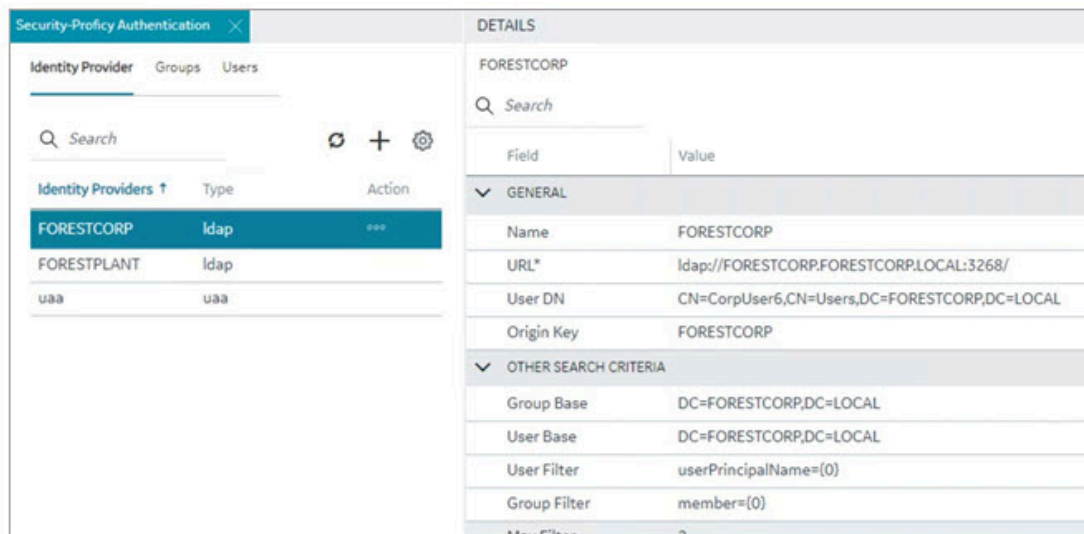
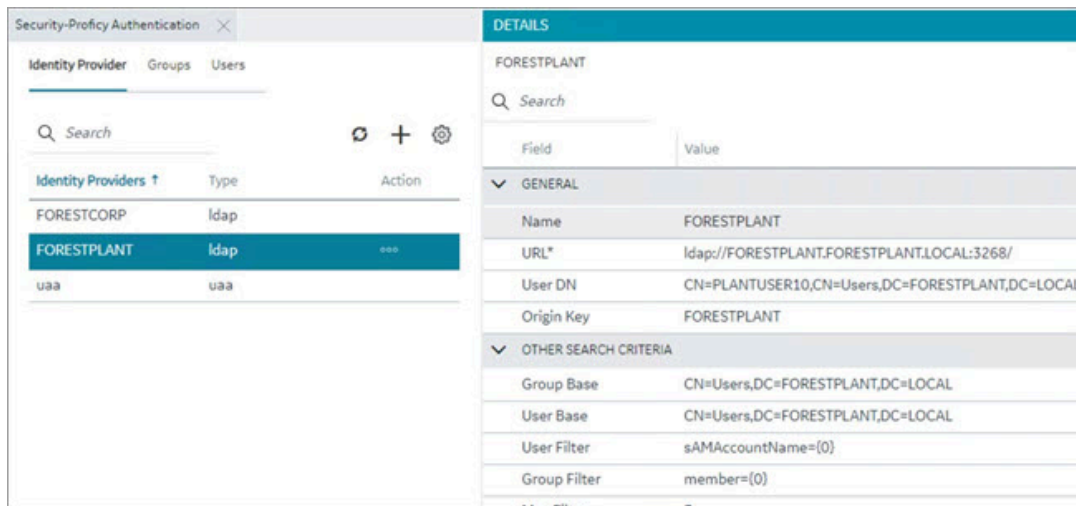
3. Log in to the VM server where you can access Proficy Authentication, and create two LDAP accounts, one for each Forest.

Refer to [Add LDAP Identity Provider \(on page 15\)](#) for steps to create a LDAP account.

While creating the LDAP accounts, make sure you do the following:

- For LDAP server URL address, use port 3268 if the global catalog is enabled. This port provides access to a broader range of directory information across multiple domains within the forest. For example: user attributes, group memberships, and other directory objects. In case the global catalog is not enabled, then use 389 or 636 ports.
- Include the Active Directory forest name in the URL. For example:

- ldap://ad1.forestplant.ge.com:3268/
- ldap://ad2.forestcorp.ge.com:3268/



4. Log in to any one of the Active Directory forest, and perform the steps described in the following topics:
 - a. [Configure Security Policy \(on page 76\)](#)
 - b. [Create Service Principal Name \(on page 78\)](#)
 - c. [Generate Keytab File \(on page 81\)](#)

- d. [Proficy Authentication Service Configuration \(on page 84\)](#)
 - e. [Configure Browser \(on page 85\)](#)
5. Log in to the test VM and validate the trust relationship for authentication and accessing resources across multiple domains.



High Availability

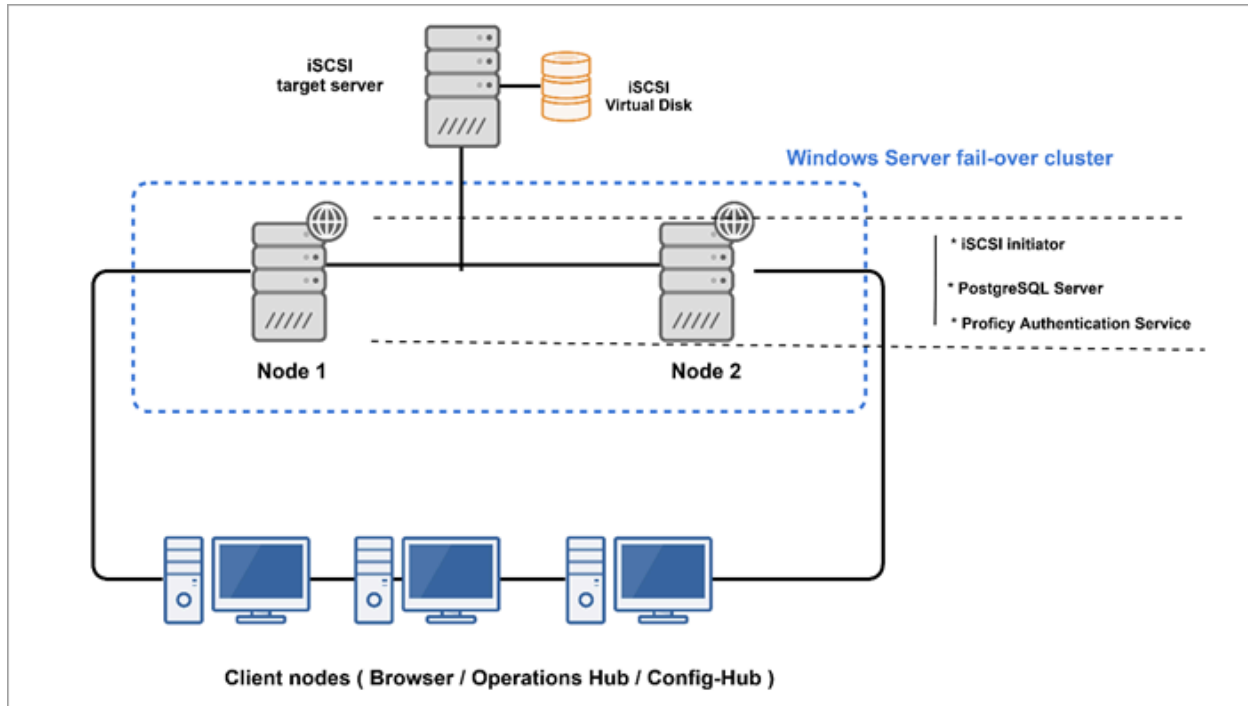
Configure High Availability for Proficy Authentication

This topic describes how to set up a highly available server for the Proficy Authentication service that is based on the Windows failover cluster and iSCSI technologies.

You need:

- One Windows Server 2019 virtual machine to serve as iSCSI Target.
- Two Windows Server 2019 virtual machines to serve as iSCSI Initiators:
 - A primary node (Node1) server
 - A secondary node (Node2) server

The following image illustrates the simplest form of deploying the Windows failover cluster and iSCSI technology-based high available solution for the Proficy Authentication Service.



In failover cluster technology, a group of independent computers work together to increase the availability and scalability of clustered roles (identified as nodes in a cluster). Nodes are clustered server machines running applications and services.

Failover cluster feature and file server roles are installed on the Node1 and Node2 servers (also called iSCSI initiators). A virtual disk is created on the iSCSI target server for shared storage. Failover clustering technology arranges for a backup server whenever the primary server has failed for any reason. So, if the primary server Node1 is down, then the backup server Node2 is automatically activated to replace the role of the primary server. This ensures uninterrupted access to shared storage and continuity of services even during failure of the primary server.

1. Set up the iSCSI Target.
 - a. [Configure iSCSI Target \(on page 91\)](#)
 - b. [Create a Virtual Disk \(on page 94\)](#)
2. Set up the iSCSI initiators: Node1 and Node2.
 - a. [Configure iSCSI Initiator \(on page 91\)](#)
 - b. [Initialize a Virtual Disk \(on page 95\)](#)
3. Open Failover Cluster Manager on any of the iSCSI initiator nodes in a cluster (Node1 or Node2), and [create a cluster \(on page 97\)](#).
4. Create and configure a role for the failover cluster. See [Configure Role \(on page 102\)](#).
5. Install Proficy Authentication on both the nodes.

See [Configure Proficy Authentication Installation \(on page 107\)](#).

If you are installing Operations Hub in a highly available cluster, follow the steps as described in [Prerequisites for Installing Operations Hub with External Proficy Authentication \(on page 112\)](#).

- Restart the services on both the nodes.

Configure iSCSI Target

This topic describes how to configure an iSCSI target server.

You can configure an external storage using Windows 2019.

- Log in to the virtual machine where you want to set up the iSCSI target server.
- Go to **Start > Administrative Tools > Server Manager**.
- From the Server Manager dashboard, select **Manage > Add roles and features**.
- Complete **Add Roles and Features Wizard** with these options:

Section	What To Do
Before You Begin	Skip to the next section.
Installation Type	Select Role-based or feature-based installation .
Server Selection	<ol style="list-style-type: none"> Choose the option Select a server from the server pool. Under the server pool section, select your target server. You will be installing the role/feature on this server.
Server Roles	In the roles list box: <ol style="list-style-type: none"> Expand File and Storage Services > File and iSCSI Services. Select the check box for iSCSI Target Server.
Confirmation	Select Install .

When the installation is complete, restart the machine.

Log in to the same server again and [create a virtual disk \(on page 94\)](#).

Configure iSCSI Initiator

This topic describes how to configure an iSCSI initiator and connect to the target server.

[Configure iSCSI Target \(on page 91\)](#).

You must perform these steps on all the initiator server nodes you want to add to a cluster. Let us assume you are setting up a basic two-node cluster, where there are two iSCSI initiators:

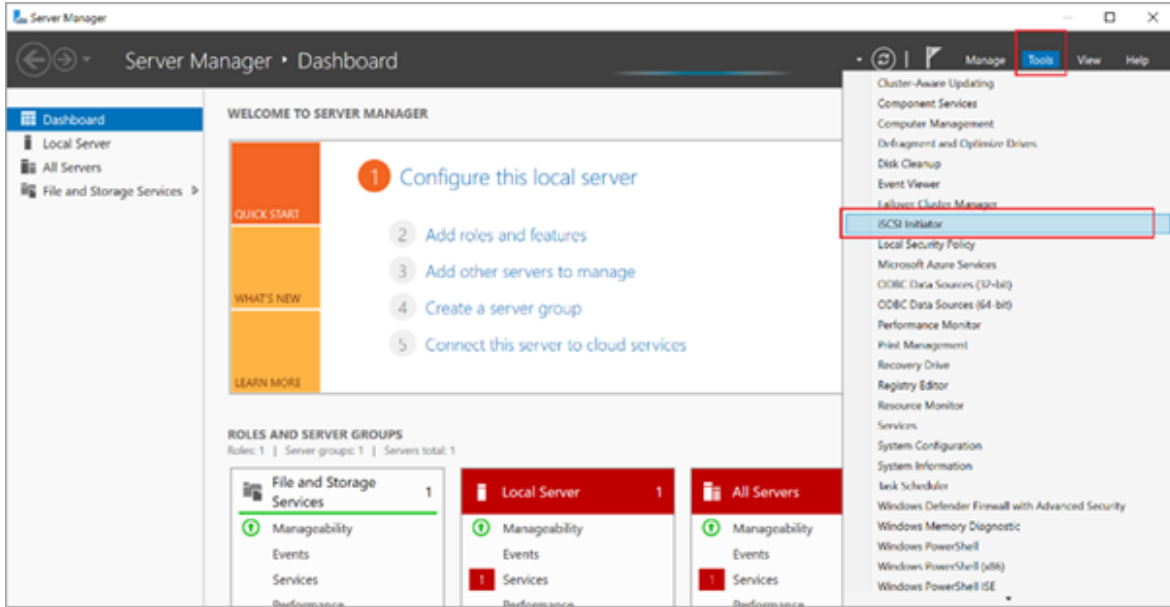
- A primary server called Node1
- A secondary server called Node2

1. Log in to the Node1 server.
2. Go to **Start > Administrative Tools > Server Manager**.
3. From the Server Manager dashboard, select **Manage > Add roles and features**.
4. Complete **Add Roles and Features Wizard** with these options:

Section	What To Do
Before You Begin	Skip to the next section.
Installation Type	Select Role-based or feature-based installation .
Server Selection	<ol style="list-style-type: none"> a. Choose the option Select a server from the server pool. b. Under the server pool section, select your Node1 server. You will be installing the role/feature on this server.
Server Roles	In the roles list box: <ol style="list-style-type: none"> a. Expand File and Storage Services > File and iSCSI Services. b. Select the check box for iSCSI Target Server.
Features	To allow the installation of Failover Cluster Manager: <ol style="list-style-type: none"> a. In the features list box, select the check box for Failover Clustering. <p style="text-align: center;">The Add features that are required for Failover Clustering? screen appears, which shows the dependencies that are installed with this feature.</p> <ol style="list-style-type: none"> b. Select Add Features.
Confirmation	Select Install .

The selected role and feature is installed on the Node1 server.

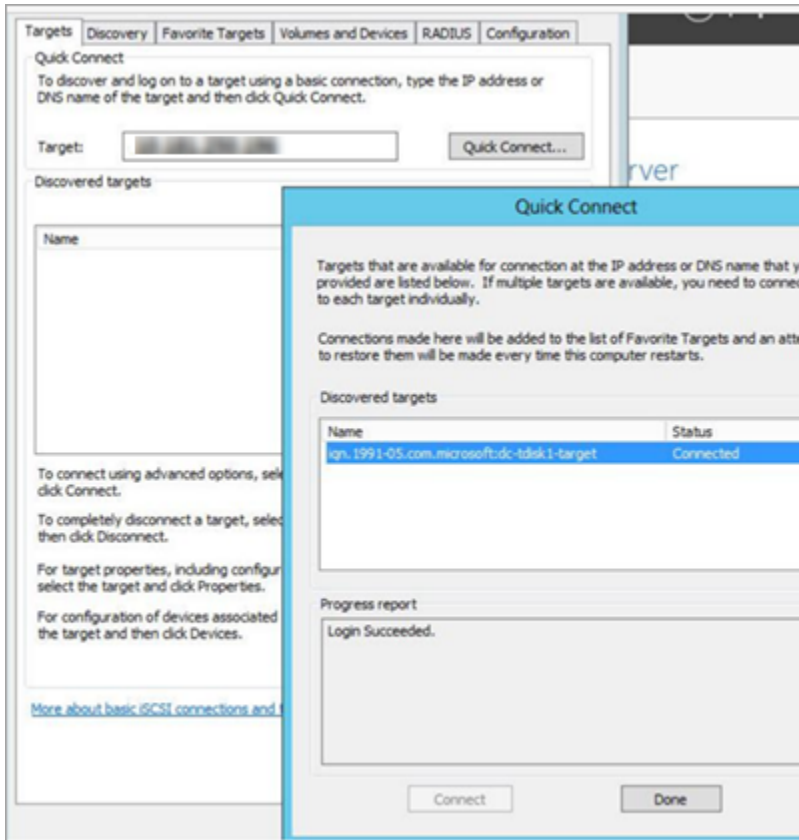
5. When the installation is complete, restart the machine.
6. Log in to the same server again and launch **Server Manager**.
7. From the **Tools** menu, select **iSCSI Initiator**.



8. In the **Target** field, enter the iSCSI target server address.

9. Select **Quick Connect**.

If connected, the login success appears as shown in the following figure:



10. Select **Done**, then **OK** to exit.
11. Log in to the Node2 server and repeat steps 1-9.

[Initialize a Virtual Disk \(on page 95\)](#)

Create a Virtual Disk

This topic describes how to create an iSCSI virtual disk and configure the access server.

You must first [configure the iSCSI target server \(on page 91\)](#).

1. Log in to the iSCSI target server.
2. Go to **Start > Administrative Tools > Server Manager**.
3. Go to **File and Storage Services > iSCSI**.
4. From the **TASKS** drop-down menu, select **New iSCSI Virtual Disk**.
5. Complete **New iSCSI Virtual Disk Wizard** with these options:

Section	What To Do
iSCSI Virtual Disk Location	The iSCSI target server and volume details are displayed.
iSCSI Virtual Disk Name	Enter a name for the virtual disk. For example, <code>sharedDisk</code>
iSCSI Virtual Disk Size	<ol style="list-style-type: none"> a. Enter the disk size. For example, <code>10GB</code>. The disk size depends on your database utilization and number of users. b. Select Dynamically expanding.
iSCSI Target	<p>Select New iSCSI target.</p> <p>If the target is new, then it should be assigned later as described in step 8.</p>
Target Name and Access	Enter a name for the iSCSI target server. For example, <code>hauaatarget</code>
Access Servers	<p>Add the iSCSI initiators (Node1 and Node2) and enable them to access the iSCSI virtual disk. Follow these steps to add the servers one at a time:</p> <ol style="list-style-type: none"> a. Select Add. The Add initiator ID screen appears. b. Select Enter a value for the selected type. c. From the Type drop-down menu, choose any of the following options to enter a value:

Section	What To Do
	<ul style="list-style-type: none"> ▪ If you select DNS Name, enter the DNS name of the computer where the iSCSI initiator is installed. ▪ If you select IP Address, then enter the IP address of the computer where the iSCSI initiator is installed. ▪ If you select Mac Address, then enter the MAC address of the computer where the iSCSI initiator is installed. <p>d. Select OK to exit.</p> <p>e. To add Node2, repeat the above steps.</p>
Enable authentication	Skip to the next section.
Confirmation	Select Create .

When the iSCSI virtual disk is created successfully, select **Close** to exit the wizard.

6. In Server Manager, go to **File and Storage Services > iSCSI** and verify the newly created virtual disk is listed under iSCSI virtual disks.

The virtual disk status appears as `Not Connected`. This occurs when a new iSCSI target is selected during iSCSI virtual disk creation.

7. Right-click the `Not Connected` iSCSI virtual disk and select **Assign iSCSI Virtual Disk**.
8. Complete **Assign iSCSI Virtual Disk Wizard** with these options:

Section	What To Do
iSCSI Target	Select Existing iSCSI target and select the target server to connect.
Confirmation	Select Assign .

When the iSCSI virtual disk is assigned successfully, select **Close** to exit the wizard.

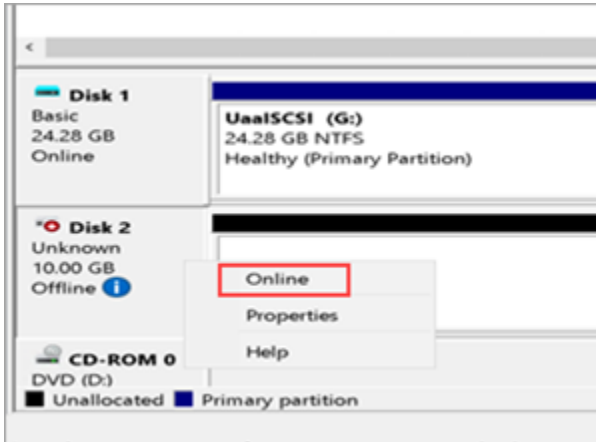
Initialize a Virtual Disk

This topic describes how to initialize a disk and create a volume.

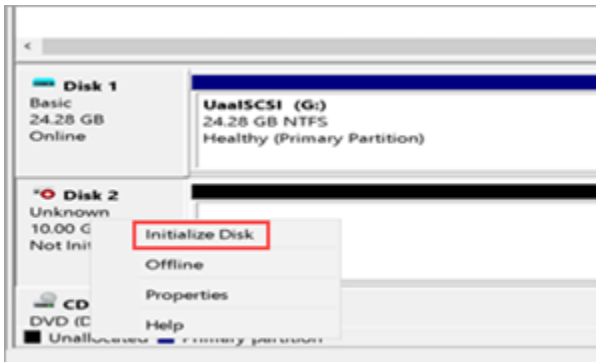
[Create a Virtual Disk \(on page 94\)](#).

You need to perform the following tasks only once on any of the iSCSI initiator nodes and it applies to the other nodes in a cluster. Suppose there are two nodes in a cluster, Node1 and Node2. If you initialize a virtual disk on the Node1 server, then you don't need to do it again on the Node2 server.

1. Log in to any of the server nodes in a cluster (Node1 or Node2).
2. Go to **Control Panel > Administrator Tools > Computer Management > Storage > Disk Management**.
3. Look for the unknown disk, right-click and select **Online**.
If the unknown disk is offline, you must bring it online.

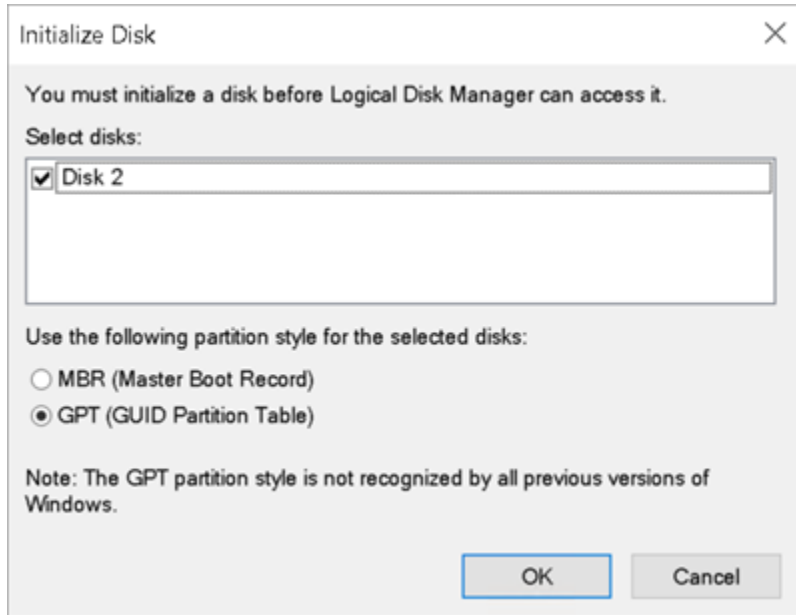


4. Right-click the unknown disk again and select **Initialize disk**.

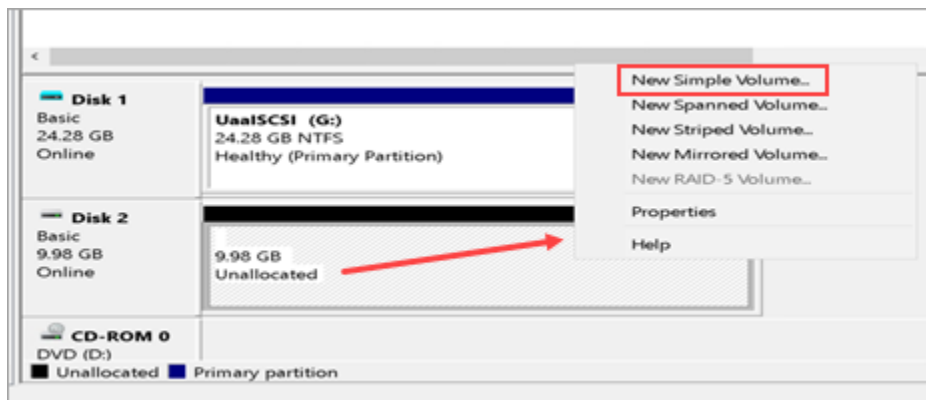


The **Initialize Disk** screen appears.

5. Select **OK**.



6. Right-click the unallocated space on the disk, and select **New Simple Volume**.



The **New Simple Volume Wizard** screen appears.

7. Complete the steps in the wizard to create a new volume.

You need to:

- Specify the size of the volume you want to create in megabytes (MB).
- Assign a drive letter to identify the partition.
- Format the volume with default settings.

The newly created volume should appear under **This PC** on the logged-in machine.

Create a Cluster

This topic describes how to create a failover cluster.

Install Failover Cluster Manager on the iSCSI initiator nodes. Refer to steps 1-4 in [Configure iSCSI Initiator \(on page 91\)](#).

You can perform these steps on either Node1 or Node2. Suppose you perform these steps on Node1, they are automatically applied to Node2.

1. Log in to the iSCSI initiator node.
2. Go to **Start > Administrative Tools > Failover Cluster Manager**.
3. In Failover Cluster Manager, select **Validate a Configuration**.

Before starting to create a cluster of nodes, you should validate whether the nodes that you are adding to the cluster are compatible with the cluster hardware requirement. For more information, refer to the [Microsoft documentation](#).

4. Complete **Validate a Configuration Wizard** with these options:

Section	What To Do
Before You Begin	Skip to the next section.
Select Servers or a Cluster	Browse and locate the servers you want to add to the cluster. Refer to Add Server Nodes for Validation (on page 99) .
Testing Options	Select Run all tests (recommended) .
Confirmation	Review the list of tests run on the selected servers. The number of tests run are based on the roles installed on the server nodes.
Validating	This process may take several minutes depending on your network infrastructure, and the number of server nodes selected for validation.
Summary	<ol style="list-style-type: none"> a. Select View Report. b. Review Failover Cluster Validation Report and fix any failed validations. You can ignore expected warnings. The validation report should be free of any errors, otherwise the cluster setup will not be successful. c. Select Finish.

5. In Failover Cluster Manager, select **Create a Cluster**.
6. Complete **Create Cluster Wizard** using these options:

Section	What To Do
Before You Begin	Skip to the next section.

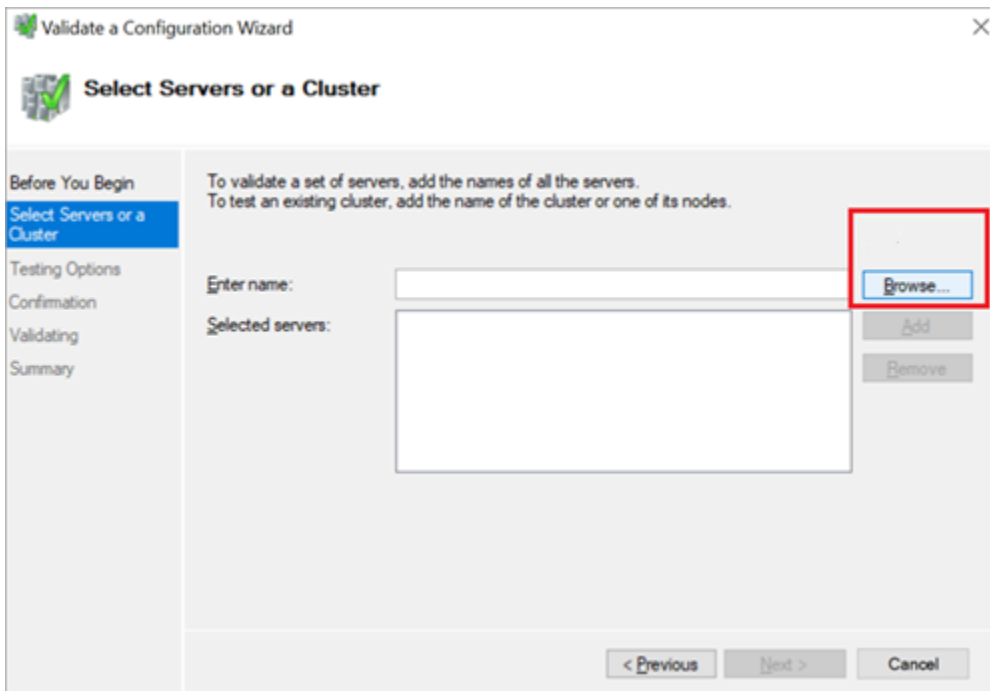
Section	What To Do
Select Servers	Nodes were already added during validating the configuration process.
Validation Warning	Select No .
Access Point for Administering the Cluster	Enter a unique name for your cluster. For example, <code>hauaacluster</code>
Confirmation	Clear the check box for Add all eligible storage to the cluster .
Creating New Cluster	This process may take a while as there are several checks that must be run, and tests that are conducted while the system is configured.
Summary	Select Finish .

Add Server Nodes for Validation

This topic describes how to select computers during validating a cluster configuration.

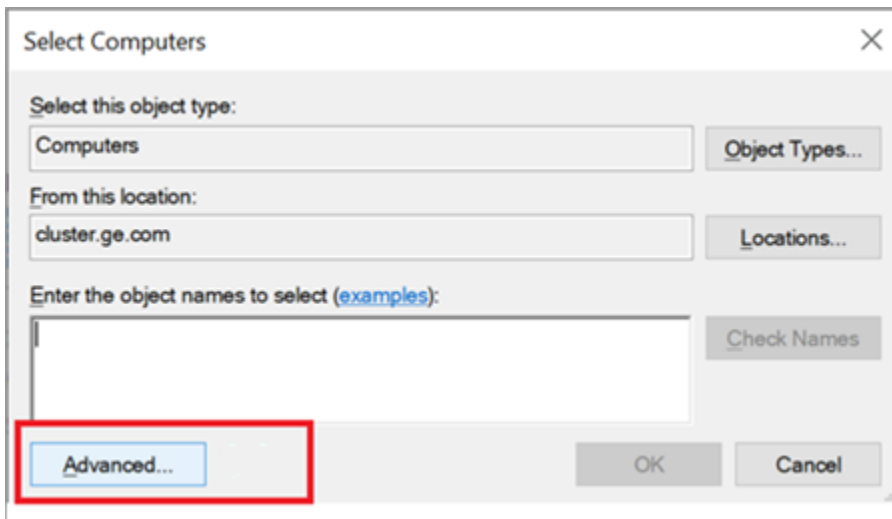
In the following steps, `UAAHANODE1` (Node1 server name) and `UAAHANODE2` (Node2 server name) are used as example server nodes in a cluster.

1. On the **Select Servers or a Cluster** tab, select **Browse**.

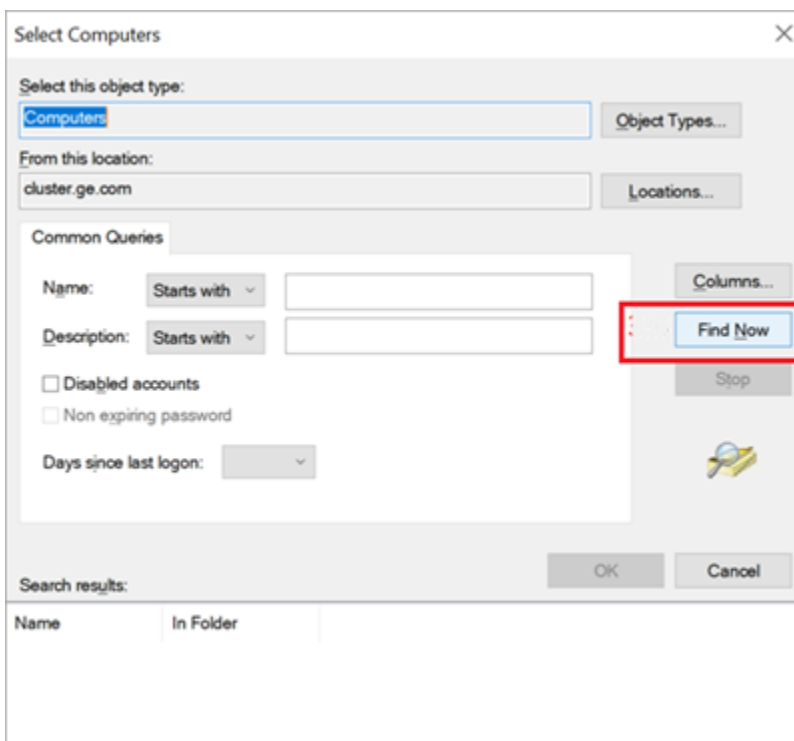


The **Select Computers** screen appears.

2. Select **Advanced**.

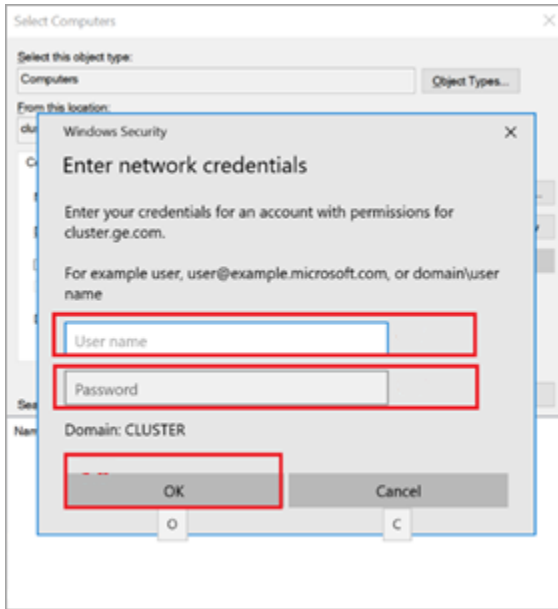


3. Select **Find Now**.



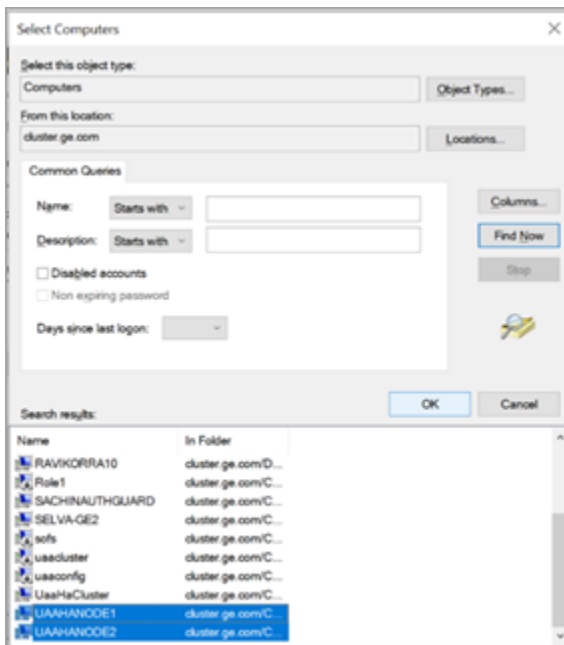
A screen appears prompting to enter the network credentials.

4. Enter the user name and password of the domain where the cluster validation is being performed, and select **OK**.

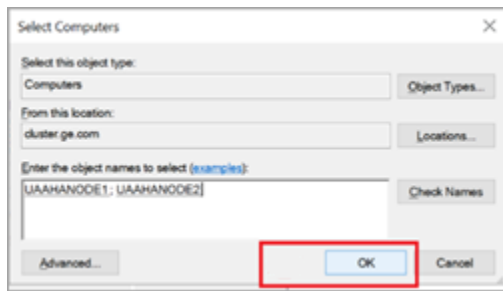


After successful login, you can see the associated nodes.

5. Select UAAHANODE1 and UAAHANODE2, and select **OK**.



6. Select **OK** to exit.



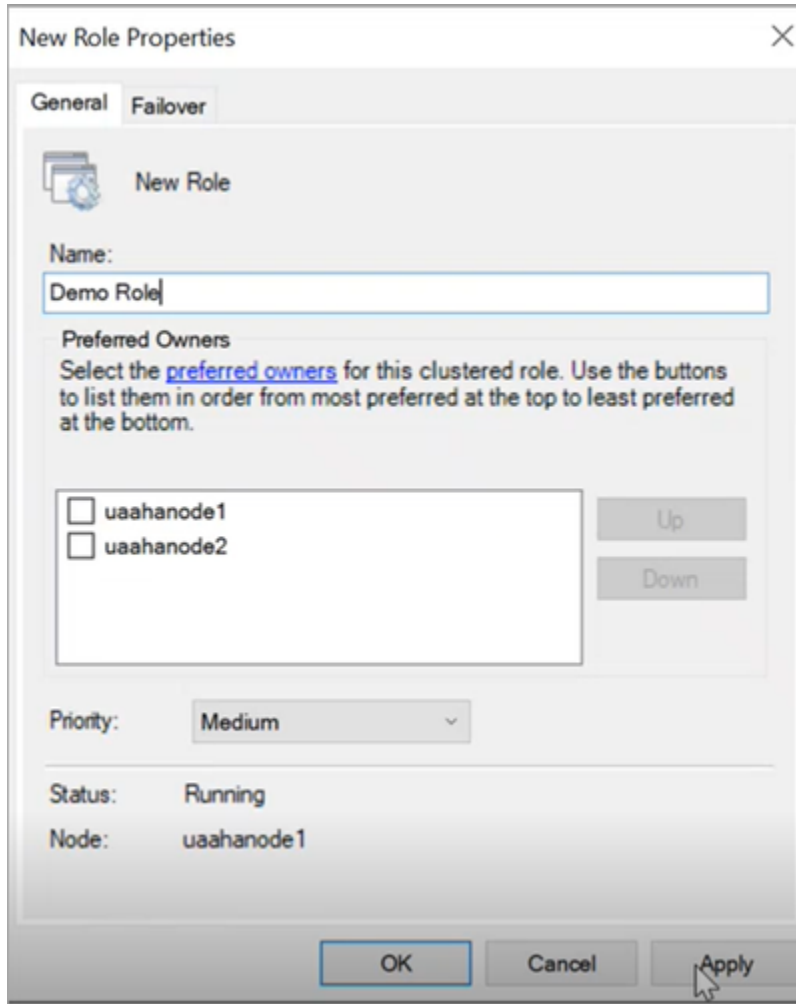
Configure Role

This topic describes how to configure a highly available virtual machine.

In failover cluster technology, each highly available virtual machine is considered to be a role.


You can perform the following steps on either Node1 or Node2. Suppose you perform these steps on Node1, they are automatically applied to Node2.

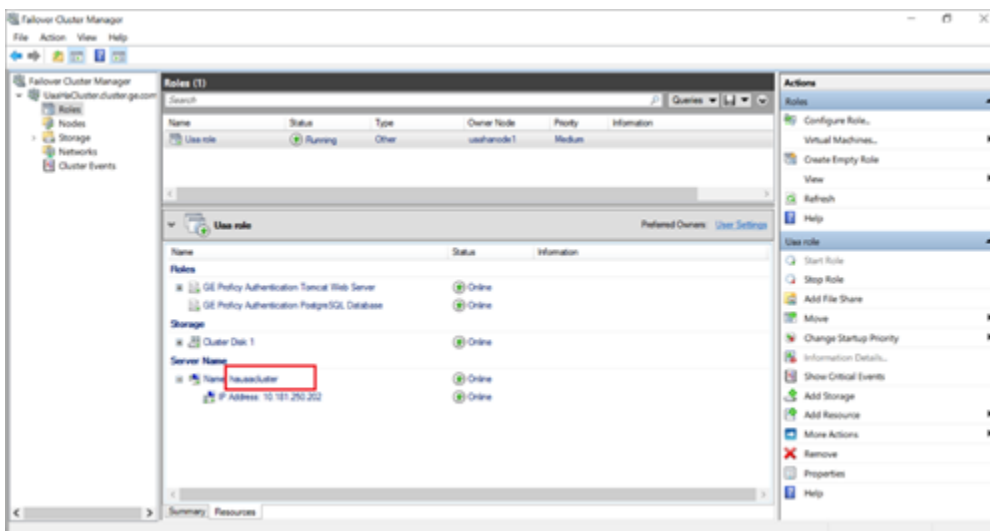
1. Log in to any of the iSCSI initiator nodes.
2. Go to **Start > Administrative Tools > Failover Cluster Manager**.
3. In Failover Cluster Manager, expand your cluster name and go to **Storage > Disks**.
The cluster name is the unique name entered when creating your cluster. Refer to step 6 in [Create a Cluster \(on page 97\)](#).
4. Right-click **Disks** and select **Add Disk**.
The **Add Disks to a Cluster** screen appears.
5. Select the disk you want to add, and select **OK**.
6. In Failover Cluster Manager, expand your cluster name and select **Roles**.
7. Right-click **Roles** and select **Create Empty Role**.
The newly created role appears in the Roles pane with the name `New Role`.
8. Right-click `New Role` and select **Properties**.
The **New Role Properties** screen appears.
9. Enter a name for the new role, and select **Apply**.
You can assign the role to multiple node servers and set an order of preference.
For example, the new name is `Demo Role`.



10. Right-click `Demo Role` and select **Add Storage**.
The **Add Storage** screen appears.
11. Select the storage that is already associated to the cluster, and select **OK**.
12. Right-click `Demo Role` and select **Add Resource > Client Access Point**.
13. Complete **New Resource Wizard** with the following options.

Section	What To Do
Client Access Point	<p>Enter a name. For example, <code>hauaacluster</code></p> <p>Make a note of this name. You need to provide the fully qualified domain name while installing Proficy Authentication. See step 3a in Configure Proficy Authentication Installation (on page 107). For example, <code>hauaacluster.cluster.ge.com</code> wherein <code>cluster.ge.com</code> is the</p>

Section	What To Do
	domain where cluster is installed. Make sure all the initiator nodes are in the same domain name.
Confirmation	<p>The network name and IP address are displayed for confirmation.</p> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: After creating this resource, the IP address and the name should be added to the <code>hosts</code> file on the node servers configured for high availability.</p> </div>
Configure Client Access Point	Verifies the validity of the client access point settings and creates a new resource.
Summary	Select Finish .



On the node servers configured for high availability, go to `.. \Windows\System32\Drivers\etc\hosts` and open the file in a text editor to add the network IP address and name as follows.

```
<ipaddress>  hauaacluster.cluster.ge.com
                <ipaddress>  hauaacluster
```

In the above example, `<ipaddress>` should be replaced with the actual ip address of your machine.

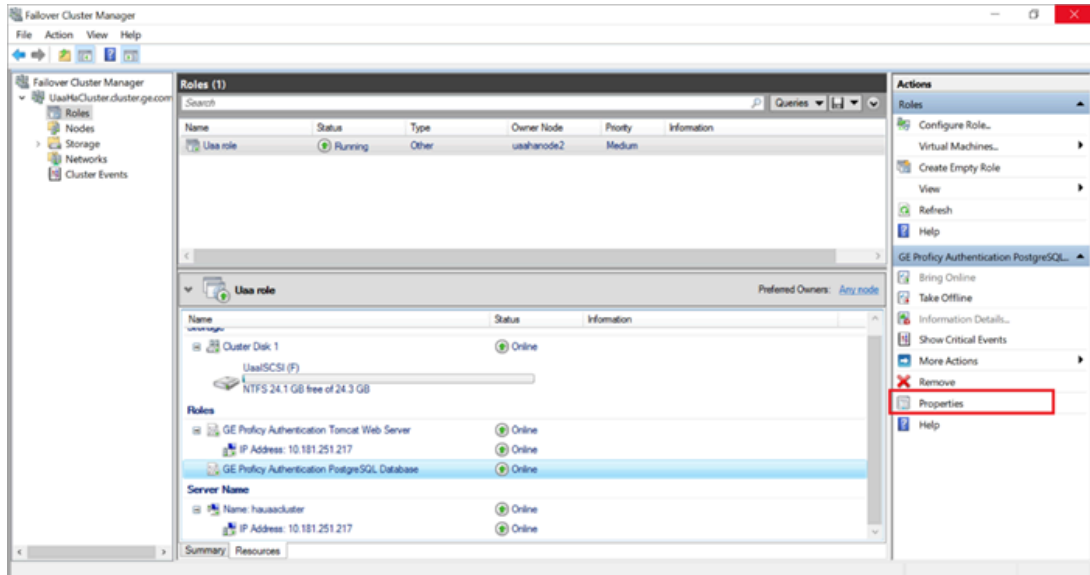
14. Right-click `Demo Role` and select **Add Resource > Generic Service**.
15. Complete **New Resource Wizard** with the following options:

Section	What To Do
Select Service	In the services list, select <code>GE Proficy Authentication Tomcat Web Service</code> .
Confirmation	Skip to the next section.
Configure Generic Service	Skip to the next section.
Summary	Select Finish .

16. Add the dependency service to role using properties of the added service, so that services restart when switching the node (failover condition).

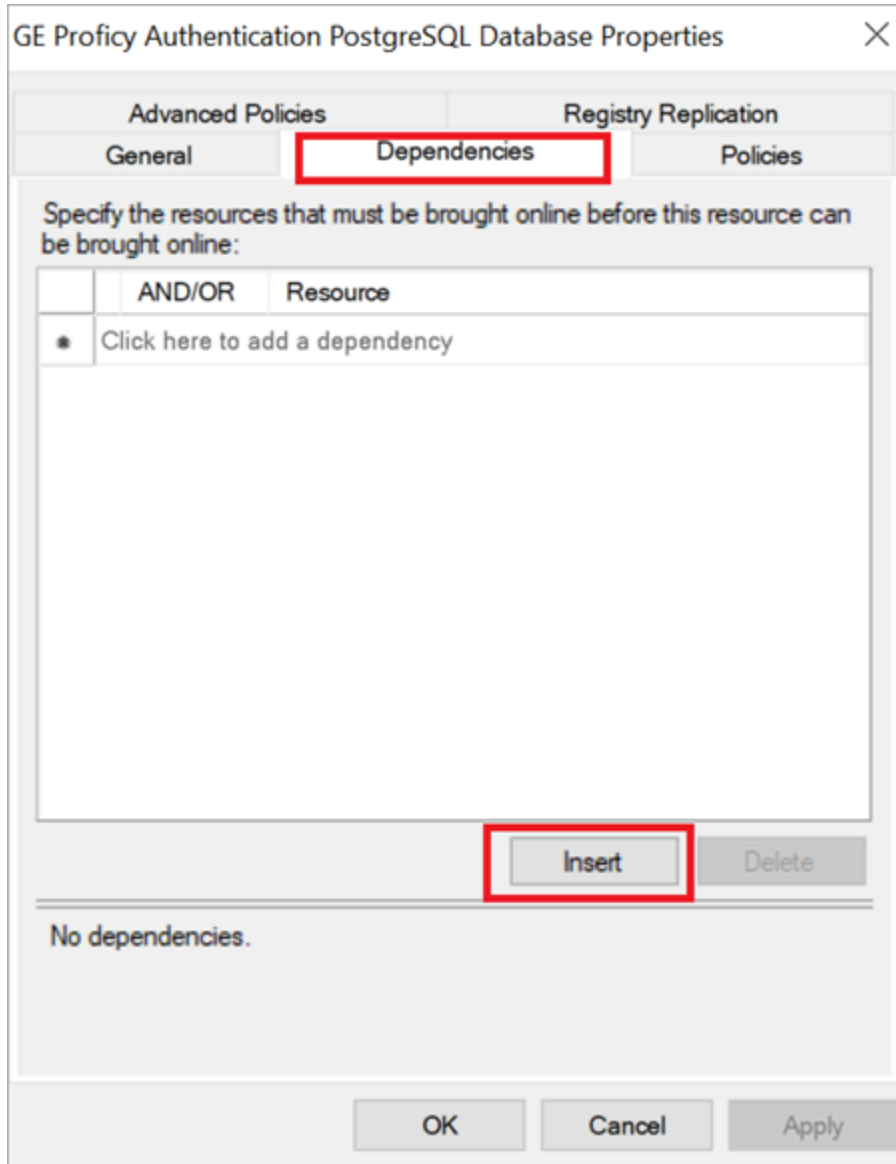
a. In Failover Cluster Manager, select the added service.

b. Select **Properties**.



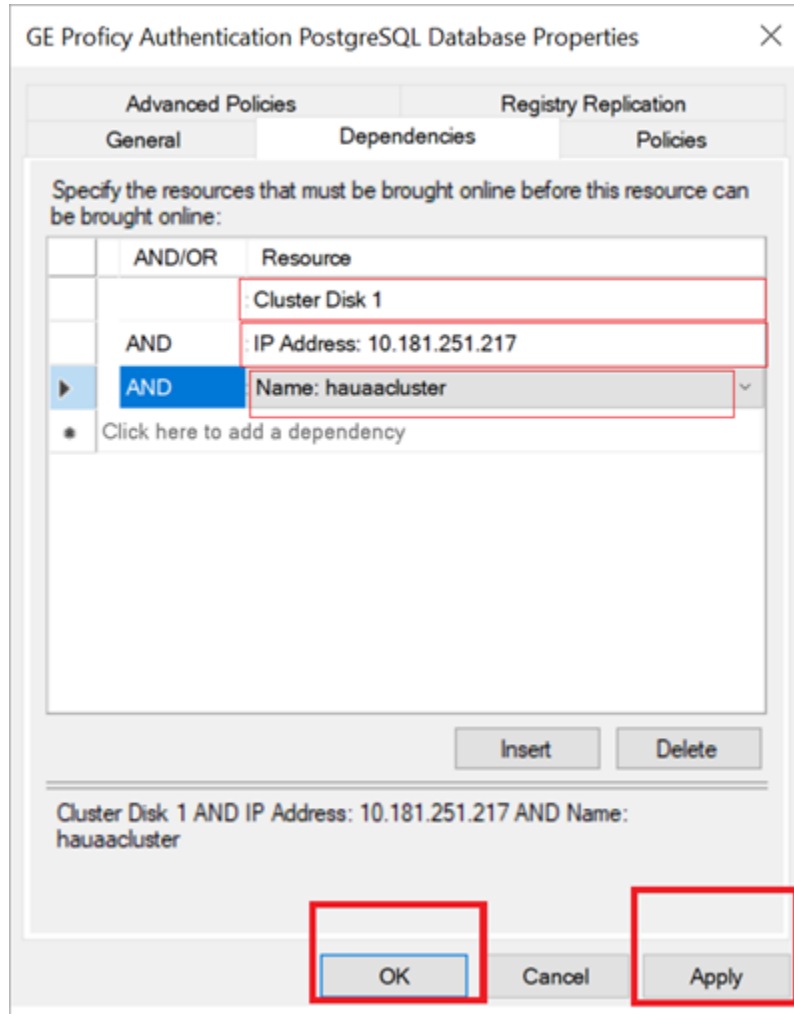
The properties screen for that service appears.

c. Select the **Dependencies** tab, and select **Insert**.



A row is added to specify our required dependencies.

- d. From the drop-down, select the required resource one by one to be added as part of dependencies.



e. After inserting the resource, select **Apply** and then **OK**.

Configure Proficy Authentication Installation

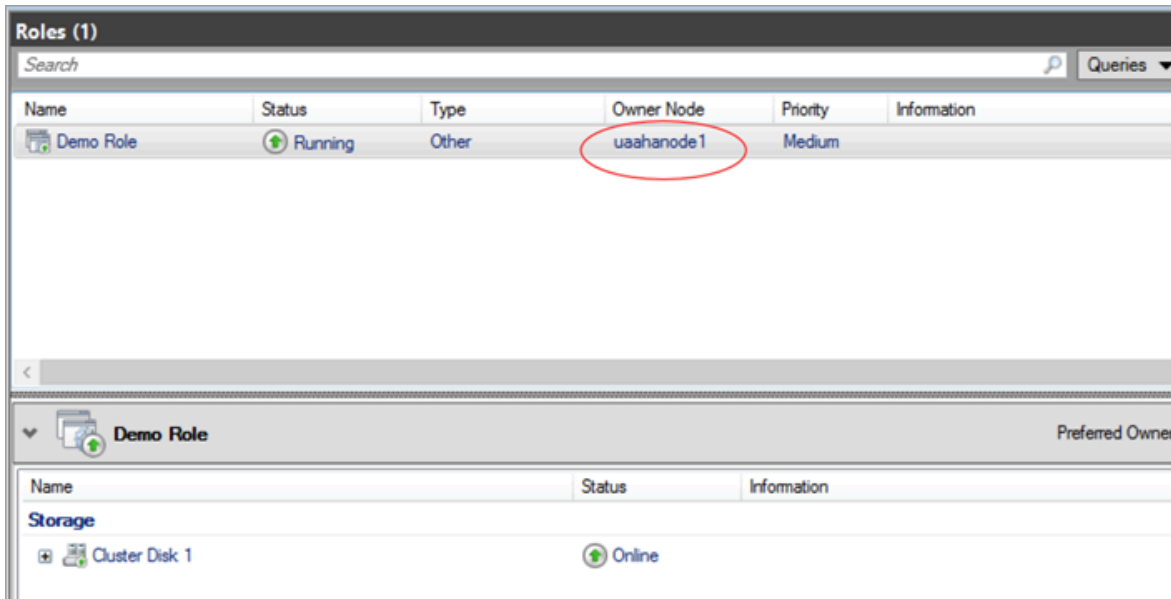
This topic describes Proficy Authentication installation setup in a high available environment.

For fresh installation, you can straightaway proceed with the procedural steps in this topic. But, if you want to use an existing database, do the following before you start with the procedural steps:

1. Copy your Proficy Authentication existing database (found in the Postgress database location) from wherever installed to the shared drive created using the iSCSI server. When you copy, make sure the cluster is pointing to the drive before copying the database. For example, if the cluster is pointing to Node1, then copy the database to Node1.
2. Make a note of the location path where you copied the database in the iSCSI server. For example, `F:\UaaConf`. You need to provide this path for installing Proficy Authentication on Node1 and Node2 machines.

To install Proficy Authentication on the iSCSI initiators (Node1 and Node2), make sure the shared drive is available on the node where you want to run the installation.

1. Log in to the iSCSI initiator Node1 server.
2. Open Failover Cluster Manager and verify that the cluster role is associated to the node where you want to install Proficy Authentication.



If not, then follow these steps to associate the node server:

- a. Right-click your cluster role and select **Select Node**.
The **Move Clustered Role** screen appears.
 - b. Select the Node1 server, and select **OK**.
Once the cluster is mapped to Node1, the shared drive is available on Node1.
3. Run Proficy Authentication installation setup, and provide these details for the respective screens:

- a. In **All Host Names** field, enter `hauacluster.cluster.ge.com` as the leading hostname, followed by any other hostname/s.

GE Proficy Authentication 2022

Host Names

To allow secure access to the hosted web applications, please provide host names (fully qualified domain names and others) of this server, separated by comma.

All Host Names:

Primary Host Name:

Notes:

- The primary host name must be resolvable on all client nodes.
- IP addresses may be entered if you want users to be able to access web applications by IP address.
- Environment variables enclosed in percentage signs are allowed and must be evaluated to valid names.
- Entries are used to generate a server certificate and to configure Proficy Authentication. If additional Proficy Authentication zones (and hence subdomains) are to be created, use wildcard entries instead of listing subdomains individually.

Cancel Previous Next

- b. This step applies for associating existing database. Enter the iSCSI server shared drive location path where you copied the Proficy Authentication database. Refer to the [steps at the beginning of this topic \(on page 107\)](#).

For example, `F:\UaaConf`

GE Proficy Authentication 2022

Customize Log Files and Postgres Data Locations

Log Files Base Folder:

Proficy Authentication Database Folder:

Note: leave database folder entries blank if no customization is needed.

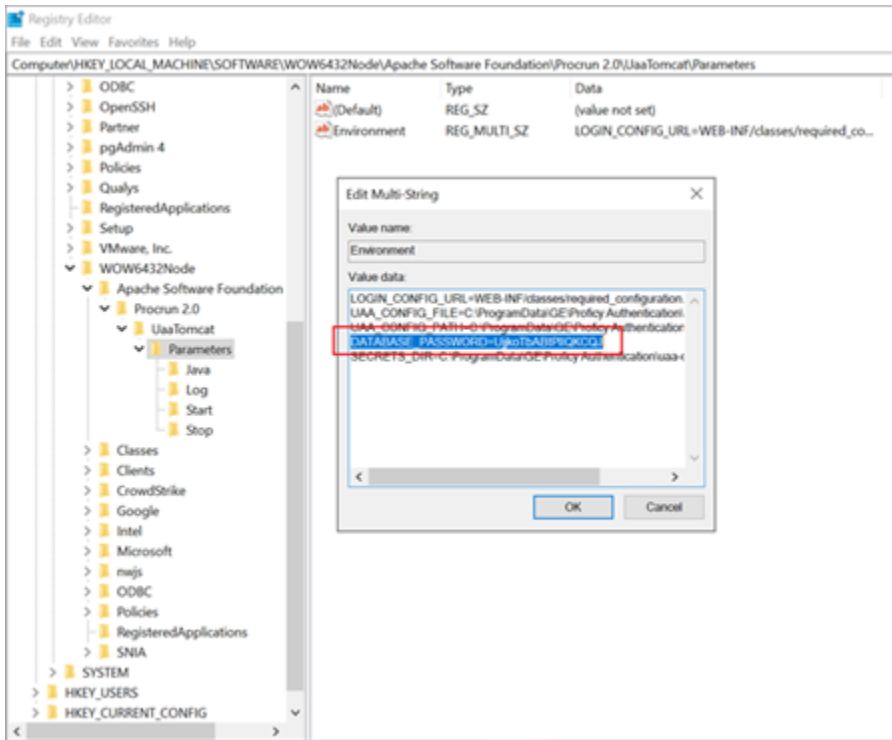
Cancel Previous Next

4. Log in to the iSCSI initiator Node2 server, and repeat the above steps to install Proficy Authentication on Node2.
5. After installing Proficy Authentication on both the nodes, copy the `DATABASE_PASSWORD` registry key from the last installed node to overwrite the registry key in the first installed node.

For example, in the following scenario:

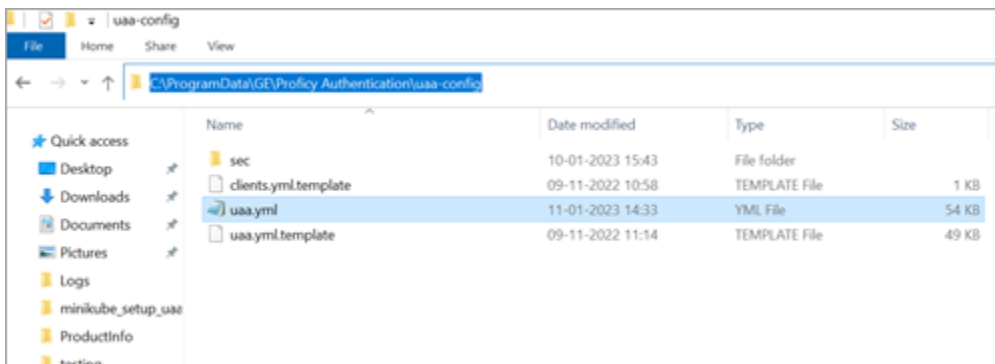
- a. First Proficy Authentication is installed successfully on the Node1 machine.
- b. Next Proficy Authentication is installed successfully on the Node2 machine.

Node2 is considered as the latest installation. Node1 is considered as the first installation. So, copy the Node2 registry key and overwrite the Node1 registry key.



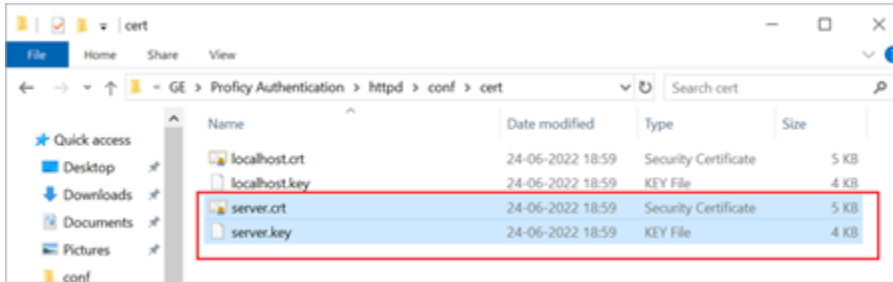
6. Copy and replace the `UAA.yaml` file from Node 2 (latest installation) to Node 1 (first installation).

The file is located here `C:\ProgramData\GE\Proficy Authentication\uaa-config`



7. Copy `server.crt` and `server.key` from Node 2 (latest installation) to Node 1 (first installation).

The certificates are located here: `C:\Program Files\Proficy\Proficy Authentication\httpd\conf\cert`



8. After copying the certificates (to Node1), rename `server.crt` to `server.pem`.



9. Open **Certificate Management Tool** on Node1 from the desktop shortcut, and import the certificates as follows:

- For **Certificate File**, select the `server.pem` file created in the earlier step.
- For **Key File**, select the `server.key` file.
- Select **Import**.



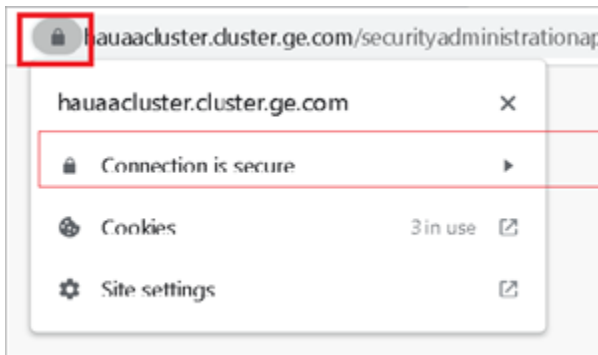
Prerequisites for Installing Operations Hub with External Proficy Authentication

This topic describes how to install Operations Hub with external Proficy Authentication in a high available environment.

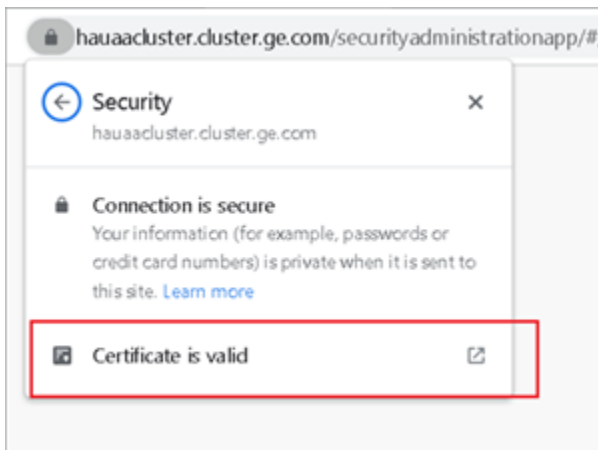
Set up a high available environment. See [Configure High Availability for Proficy Authentication \(on page 89\)](#).

These steps apply for installing Operations Hub with external Proficy Authentication. The steps include mandatory changes prior to installing Operations Hub on any highly available server.

1. Log in to the node server where you want to install Operations Hub.
2. Open a browser and enter `https://hauaacluster.cluster.ge.com /securityadministrationapp/`
3. Select the lock icon next to the web address, and then select **Connection is secure**.

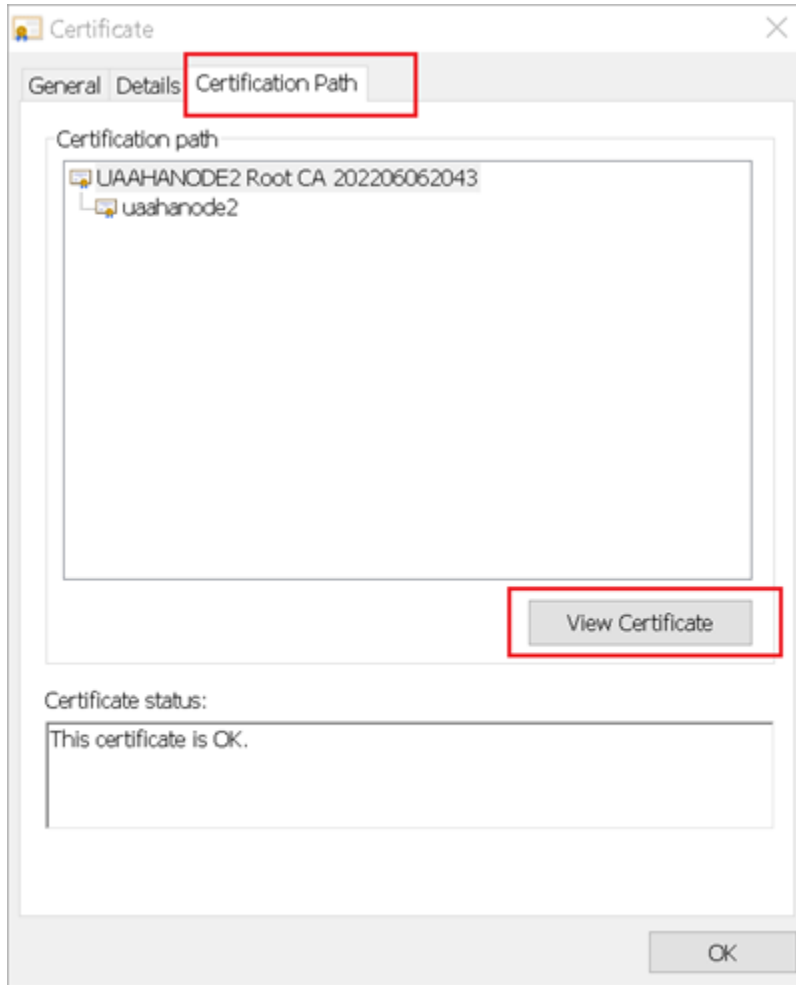


4. Select **Certificate is valid**.

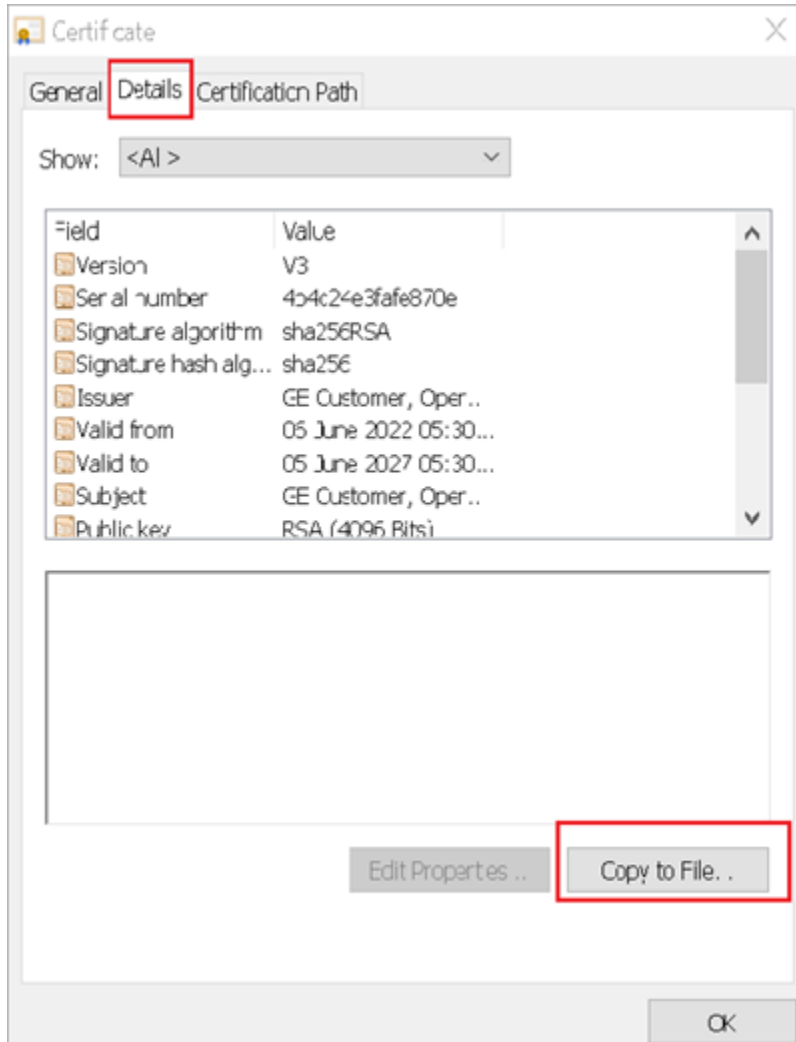


The issued certificate appears.

5. Select **Certificate Path > View Certificate**.

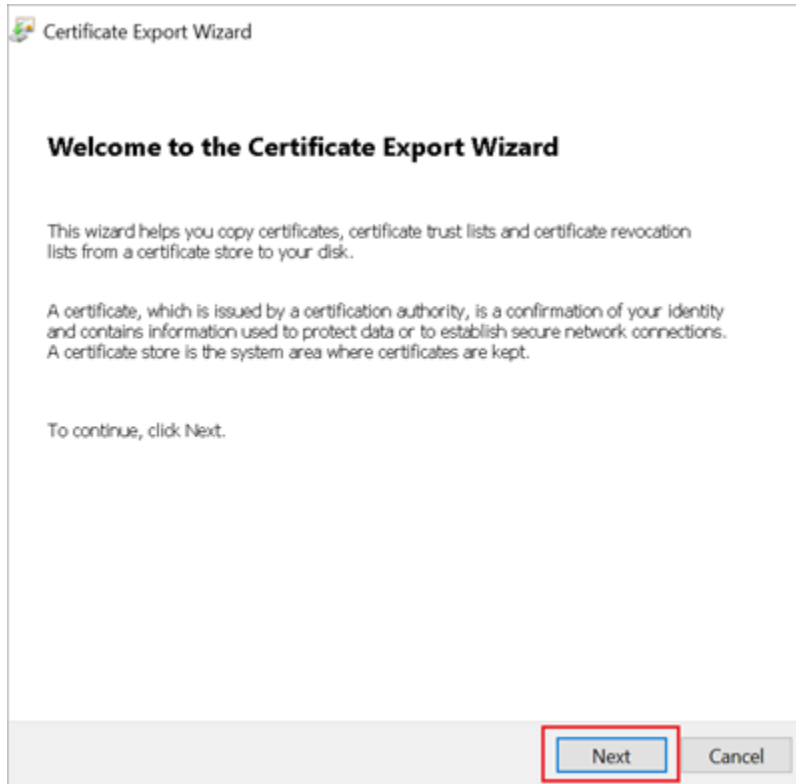


6. Select **Details > Copy to File**.

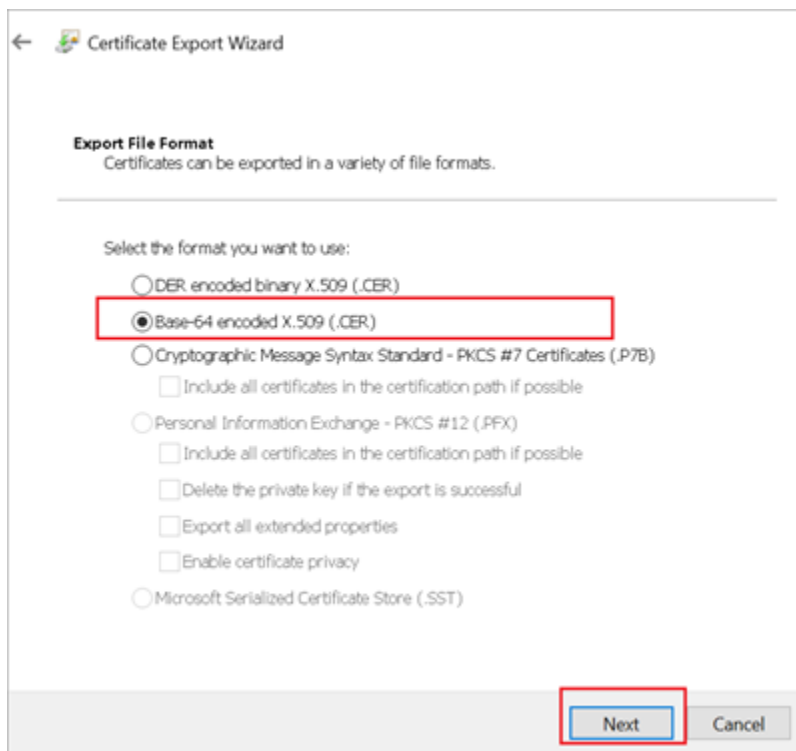


The **Certificate Export Wizard** appears.

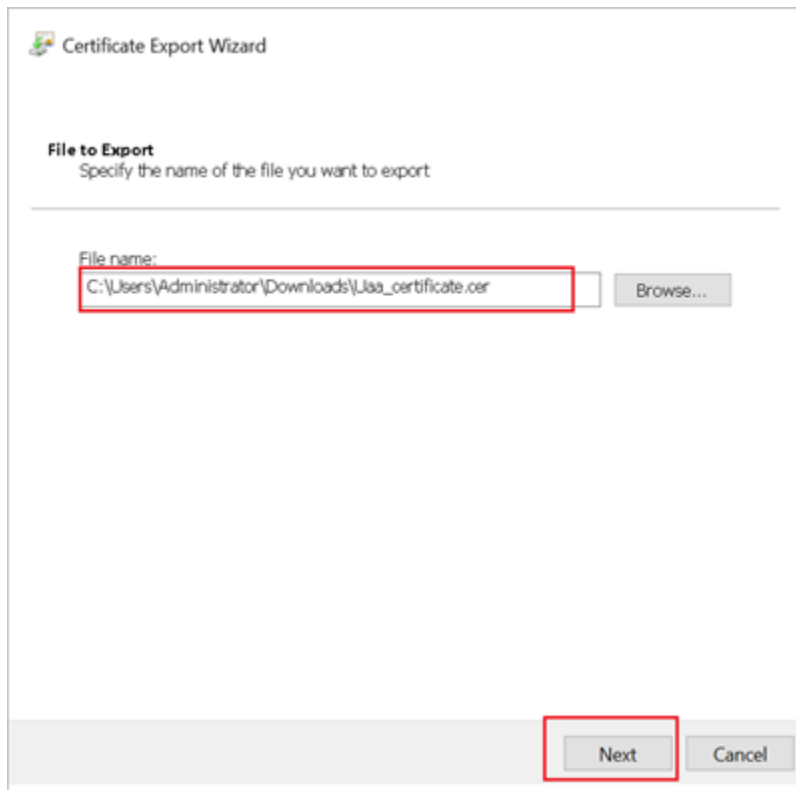
7. Select **Next**.



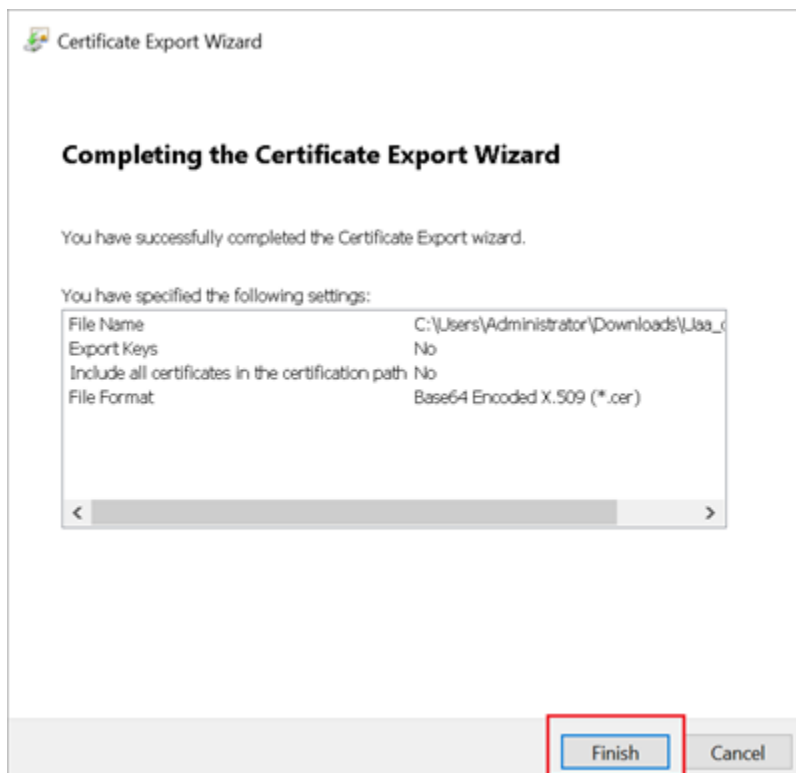
8. Select **Base-64 encoded X.509 (.CER)**, and select **Next**.



9. Browse and specify the file location, and select **Next**.

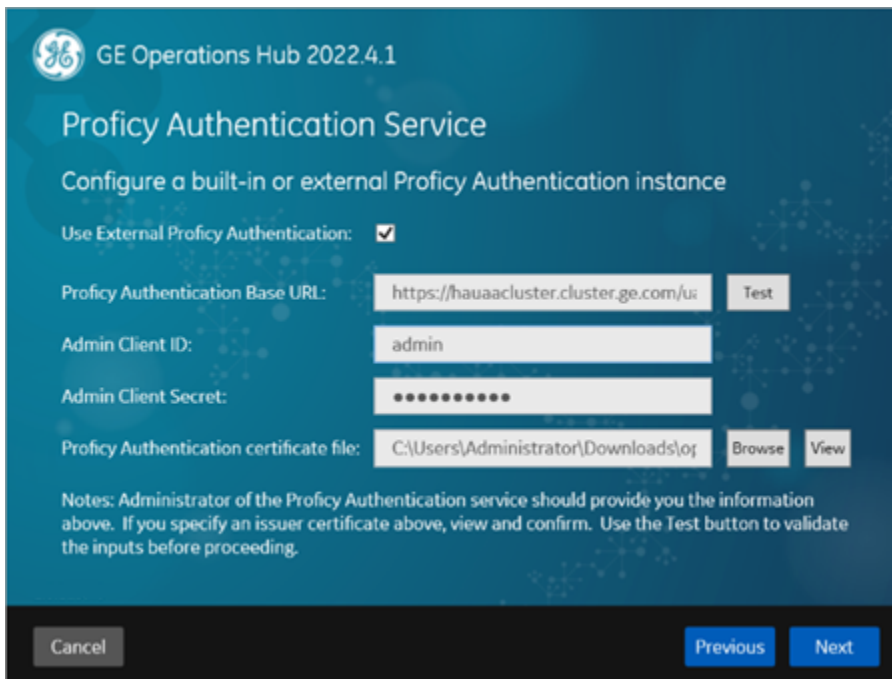


10. Select **Finish**.



11. Rename `Uaa_certificate.crt` to `Uaa_certificate.pem`.
12. Run Operations Hub installation setup, and provide these details for external Proficy Authentication fields:

Proficy Authentication Base URL	<code>https://hauaacluster.cluster.ge.com/uaa</code>
Admin Client ID	<code>admin</code>
Admin Client Secret	<code>Gei@321itc</code>



GE Operations Hub 2022.4.1

Proficy Authentication Service

Configure a built-in or external Proficy Authentication instance

Use External Proficy Authentication:

Proficy Authentication Base URL:

Admin Client ID:

Admin Client Secret:

Proficy Authentication certificate file:

Notes: Administrator of the Proficy Authentication service should provide you the information above. If you specify an issuer certificate above, view and confirm. Use the Test button to validate the inputs before proceeding.







Operations Hub is installed successfully.

Customize Login Screen

This topic describes how to customize the Proficy Authentication login screen.

You can customize the company name, logo, favicon, and include additional text/links to appear on the login screen.

1. Log in to Configuration Hub.
2. Go to **Proficy Authentication > Custom labels**.
The default login screen details appear.
3. Use the following fields to customize your login screen.
A quick preview appears on the **DETAILS** tab.

Field	Description
Company Name	Name of the company that appears on the login homepage.
Company Logo	<p>Select an image from your local system to upload as the company logo. Accepted file formats are PNG and JPG/JPEG. The file you're trying to upload cannot be larger than 1MB.</p> <div data-bbox="618 495 1419 716" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you've uploaded a company logo up to 2MB in size in the 2023 version, upgrading to the 2024 version will not cause any issues.</p> </div> <p>Select  to remove an existing image.</p>
Square Logo	<p>Select an image from your local system to upload as a favicon, which appears on the browser tab. Accepted file formats are PNG and JPG/JPEG. The file you're trying to upload cannot be larger than 1MB.</p> <div data-bbox="618 1037 1419 1260" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; background-color: #E6F2FF;"> <p> Note: If you've uploaded a square logo up to 2MB in size in the 2023 version, upgrading to the 2024 version will not cause any issues.</p> </div> <p>Select  to remove an existing image.</p>
Footer Legal Text	Use this space to enter any legal information.
Footer Links	<p>To add hyperlinks, create a label and provide a URL to connect.</p> <ol style="list-style-type: none"> a. Select  to add a row. b. Enter a label name. c. Enter a URL for the label name. <p>Select  to delete existing labels.</p>

4. Select **Save** to save the updates you made to the login screen appearance.

To undo the saved changes, select **Reset**. The login screen is reset to the previously saved appearance.

The screenshot displays the configuration interface for Proficy Authentication. The main area is titled 'Custom labels-Proficy Authentication'. It contains several sections:

- Company Name***: GE
- Company Logo***: Includes a 'Select Im...' button and 'Image Available' status. Below it, 'Allowed Image Extensions: .png, .jpg, .jpeg, .I Maximum File Size Limit: 1 MB' is shown.
- Square Logo**: Includes a 'Select Im...' button and 'Allowed Image Extensions: .png, .jpg, .jpeg, .I Maximum File Size Limit: 1 MB'.
- Footer Legal Text**: A text area containing 'copyright year'.
- Footer Links**: A table with the following data:

Label* ↑	URL*	Action
This is a footer link	https://www.ge.com/	🗑️

At the bottom right, there are 'Reset' and 'Save' buttons. On the right side, the 'DETAILS' section shows a 'UAA Login Preview' for 'GE Digital' with a 'Welcome!' message, input fields for 'User Identifier' and 'Password', a 'SIGN IN' button, and a footer with 'copyright year' and a 'footer link'.

5. Restart `GE Proficy Authentication Tomcat Web Server` to apply the changes.

Backup and Restore

This topic describes how to perform backups and restore the Proficy Authentication database.



Note:

Consider these restrictions while performing backup and restore:

- You can only restore data to the same host (or to a host with the same hostname).
- You should restore data to the same version of Proficy Authentication.

For steps to create a backup, refer to [Back Up the Proficy Authentication Database \(on page 119\)](#).

For steps to restore a backup, refer to [Restore the Proficy Authentication Database \(on page 121\)](#).

Back Up the Proficy Authentication Database

This topic provides steps to create a backup of the Proficy Authentication database.

You must have administrative access to perform the steps.

1. Log in to the machine where Proficy Authentication is installed.
2. [Download](#) the PowerShell scripts and unzip the file.
3. Open Windows 'Services Management Console' and stop the Proficy Authentication Tomcat Web Server service.
4. Launch Windows PowerShell as an administrator.
5. Use the command line to navigate to the location where the backup script file was downloaded.
6. Execute the following command to create a backup: `.\Backup_ProficyAuthentication.ps1`

For example,

```
C:\Users\Administrator\Desktop> .\Backup_ProficyAuthentication.ps1
```

The PROFICY_AUTHENTICATION_BKP_YYYYMMDD-HHMMSS.zip file is created and saved to C:\ProgramData location.

The YYYYMMDD-HHMMSS in the filename includes the respective backup's datetime value.

The following table details the files and folders selected by the PowerShell script and included in the backup zip file. It provides information on each item, its default location on the system, and the corresponding target location within the zip file.

File/Folder Name	Default Location	Target Folder
data-v13	C:\ProgramData\GE\Proficy Authentication\uaa-postgres	PROFICY_AUTHENTICATION_BKP_YYYYMMDD-HHMMSS\uaa-postgres
uaa.yml	C:\ProgramData\GE\Proficy Authentication\uaa-config	PROFICY_AUTHENTICATION_BKP_YYYYMMDD-HHMMSS\uaa-config
uaa-httpd.conf	C:\Program Files\GE\Proficy Authentication\httpd\conf\app-specific.d	PROFICY_AUTHENTICATION_BKP_YYYYMMDD-HHMMSS\uaa-config
server.xml	C:\Program Files\GE\Proficy Authentication\uaa-tomcat\conf	PROFICY_AUTHENTICATION_BKP_YYYYMMDD-HHMMSS\uaa-config
Certificate(if exist)	C:\ProgramData\GE\Proficy Authentication\cert-manager\extracalldap_SecAdminSrv	PROFICY_AUTHENTICATION_BKP_YYYYMMDD-HHMMSS\uaa-config
keytab file(if exist)	C:\ProgramData\GE\Proficy Authentication\uaa-config	PROFICY_AUTHENTICATION_BKP_YYYYMMDD-HHMMSS\uaa-config

Restore the Proficy Authentication Database

This topic provides steps to restore a backup on your system.

You must have administrative access to perform the steps.

The restore operation deletes everything from the current system database. Therefore, it is recommended to take a backup of your current database before proceeding with the restore operation. This backup will allow you to recover your current data in case you decide to cancel the restore operation. See [Back Up the Proficy Authentication Database \(on page 119\)](#).

1. Log in to the machine where Proficy Authentication is installed.
2. [Download](#) the PowerShell scripts and unzip the file.
3. Open Windows 'Services Management Console' and stop the `Proficy Authentication Tomcat Web Server` service.
4. Launch Windows PowerShell as an administrator.
5. Use the command line to navigate to the location of the backup file you want to restore.
6. Execute the following command to restore the backup: `.\Restore_ProficyAuthentication.ps1 C:`

```
\ProgramData\PROFICY_AUTHENTICATION_BKP_YYYYMMDD-HHMMSS.zip
```

For example,

```
C:\Users\Administrator\Desktop> .\Restore_ProficyAuthentication.ps1 C:
C:\ProgramData\PROFICY_AUTHENTICATION_BKP_20240228-143602.zip
```

The database is restored.

7. Perform [Set up Proficy Authentication \(on page 4\)](#) to start using the restored database.

Troubleshooting: Restoring Active Directory User Login

If Active Directory user login fails after a restore, then check if any LDAP connection is configured in the identity provider of the security plug-in. Do the following:

1. Navigate to the Security plug-in in Configuration Hub.
2. Open each LDAP connection, trust and save it again.

Troubleshooting Proficy Authentication

Error 431: Request Header Fields Too Large

The error indicates that the size of the HTTP request header exceeds the limit set by the server.

The 431 error can be a symptom of poor scopes administration. Ensure that you are following the principle of least privilege when assigning scopes to users. By limiting the number of scopes assigned to each user to only what is necessary, you can reduce the size of the request header. However, if you still receive the error in spite of optimizing the user scopes, you can adjust the HTTP request header size in the Tomcat server configuration. To do so, follow these steps:

1. Access the Operations Hub installation folder on your machine.
2. Navigate to `iqp-tomcat/conf/server.xml`.
3. In the `server.xml` file, look for Catalina service Connector section and locate the field `maxHttpHeaderSize` to modify its value.

The default value is `8192`. Increase the size to a higher value, such as `16384` or `24576`.

4. Save the changes to the file and close it.
5. Restart the `GE Operations Hub IQP Tomcat Web Server` service from the Management Console.

Windows Auto-login Error Logs

This topic describes Windows Auto-login success/failure scenarios.

User logs in successfully

Verify the `uaa.log` if the TGT/Kerberos token is generated properly. It should start with `YII`. You can ignore the lengthy token value in the log entries.

```
[2022-02-22 19:29:41.949] cloudfoundry-identity-server - 14188 [http-nio-9480-exec-8] ...  
DEBUG --- SpnegoAuthenticationProcessingFilter: Received Negotiate Header for request  
https://win16-sachin.uaatestad.ge.com/uaa/: Negotiate YIIHVQYGKwY*****
```

A local Windows (non-domain) user attempts Windows Auto-login (using query parameter in the URL) from a domain member machine

Browser displays an error. The error message also appears in `uaa.log`. The following error appears when attempting to login with domain name in the URL.

HTTP Status 500 – Internal Server Error

Type Exception Report

Message Servlet.init() for servlet [spring] threw exception

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Exception

```

javax.servlet.ServletException: Servlet.init() for servlet [spring] threw exception
    org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:5
    org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
    org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.jav
    org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769)
    org.apache.catalina.valves.rewrite.RewriteValve.invoke(RewriteValve.java:289)
    org.apache.catalina.valves.RequestFilterValve.process(RequestFilterValve.java:378)
    org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56)
    org.apache.coyote.connector.CoyoteAdapter.service(CoyoteAdapter.java:357)
    org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:382)
    org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65)
    org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:
    org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1722)
    org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
    org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.jav
    org.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.jav
    org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
    java.base/java.lang.Thread.run(Unknown Source)
  
```

Root Cause

```

java.lang.IllegalStateException: Listeners cannot be added to context [/uaa] as the context
    org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(
    org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(
    org.springframework.web.servlet.FrameworkServlet.applyInitializers(FrameworkServlet
    org.springframework.web.servlet.FrameworkServlet.configureAndRefreshWebApplicationC
    org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(Framew
    org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(Framew
    org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(Framewo
    org.springframework.web.servlet.FrameworkServlet.initServletBean(FrameworkServlet.j
    org.springframework.web.servlet.HttpServletBean.init(HttpServletBean.java:170)
    javax.servlet.GenericServlet.init(GenericServlet.java:158)
    org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:5
    org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
    org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.jav
    org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769)
    org.apache.catalina.valves.rewrite.RewriteValve.invoke(RewriteValve.java:289)
    org.apache.catalina.valves.RequestFilterValve.process(RequestFilterValve.java:378)
    org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56)
  
```

The following error appears when attempting to login with non-domain name in the URL.

HTTP Status 500 – Internal Server Error

Type Exception Report

Message Servlet.init() for servlet [spring] threw exception

Description The server encountered an unexpected condition that prevented it from fulfilling the request.

Exception

```

javax.servlet.ServletException: Servlet.init() for servlet [spring] threw exception
org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:540)
org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.java:687)
org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769)
org.apache.catalina.valves.rewrite.RewriteValve.invoke(RewriteValve.java:289)
org.apache.catalina.valves.RequestFilterValve.process(RequestFilterValve.java:378)
org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56)
org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:357)
org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:382)
org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65)
org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:895)
org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1722)
org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1191)
org.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:659)
org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
java.base/java.lang.Thread.run(Unknown Source)

```

Root Cause

```

java.lang.IllegalStateException: Listeners cannot be added to context [/uaa] as the context has been initialised
org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(YamlServletProfileInitializer.java:86)
org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(YamlServletProfileInitializer.java:54)
org.springframework.web.servlet.FrameworkServlet.applyInitializers(FrameworkServlet.java:764)
org.springframework.web.servlet.FrameworkServlet.configureAndRefreshWebApplicationContext(FrameworkServlet.java:701)
org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(FrameworkServlet.java:716)
org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(FrameworkServlet.java:591)
org.springframework.web.servlet.FrameworkServlet.initServletBean(FrameworkServlet.java:530)
org.springframework.web.servlet.HttpServletBean.init(HttpServletBean.java:170)
javax.servlet.GenericServlet.init(GenericServlet.java:158)
org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:540)
org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)
org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.java:687)
org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769)
org.apache.catalina.valves.rewrite.RewriteValve.invoke(RewriteValve.java:289)
org.apache.catalina.valves.RequestFilterValve.process(RequestFilterValve.java:378)
org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56)
org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:357)

```

Bad or missing keytab file (or) Bad SPN in `uaa.yml` file

The following errors appear in `uaa.log`.

```

[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] ... ERROR ---
DynamicKerberosAuthenticationManager: Kerberos validation not successful. Encountered Bad Credentials Exception :
Kerberos validation not successful
[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] ... ERROR ---
DynamicKerberosAuthenticationManager: Kerberos validation not successful. Encountered Bad Credentials Exception :
Kerberos validation not successful
[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] ... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

```

```
[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Defective token detected (Mechanism
level: GSSHeader did not find the right tag)

[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Defective token detected (Mechanism
level: GSSHeader did not find the right tag)

[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] ....
WARN --- SpnegoAuthenticationProcessingFilter: Negotiate Header was invalid: Negotiate
TlRMTVNTUABAAAAA14II4gAAAAAAAAAAAAAAAAAAAAAAAAAKADk4AAAAADw==
org.springframework.security.authentication.BadCredentialsException: Bad Credentials excption. It could be due to
keytab file and the SPN configuration.
```

Crypto Mismatch

A crypto mismatch occurs if the encryption algorithm specified while using `ktpass.exe` to generate keytab does not match what is supported by the service account.

```
[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Kerberos validation not successful. Encountered Bad Credentials Exception :
Kerberos validation not successful

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Kerberos validation not successful. Encountered Bad Credentials Exception :
Kerberos validation not successful

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
level (Mechanism level: Invalid argument (400) - Cannot find key of appropriate type to decrypt AP-REQ - RC4 with
HMAC)

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
level (Mechanism level: Invalid argument (400) - Cannot find key of appropriate type to decrypt AP-REQ - RC4 with
HMAC)
```

```
[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Invalid argument (400) - Cannot
find key of appropriate type to decrypt AP-REQ - RC4 with HMAC

[2022-02-22 11:39:18.326] cloudfoundry-identity-server - 6084 [http-nio-9480-exec-3] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Invalid argument (400) - Cannot
find key of appropriate type to decrypt AP-REQ - RC4 with HMAC
```

Clock skew between client and server

The following errors appear in `uaa.log`.

```
[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
level (Mechanism level: Clock skew too great (37))

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
level (Mechanism level: Clock skew too great (37))

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Clock skew too great (37)

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Clock skew too great (37)
```



Note:

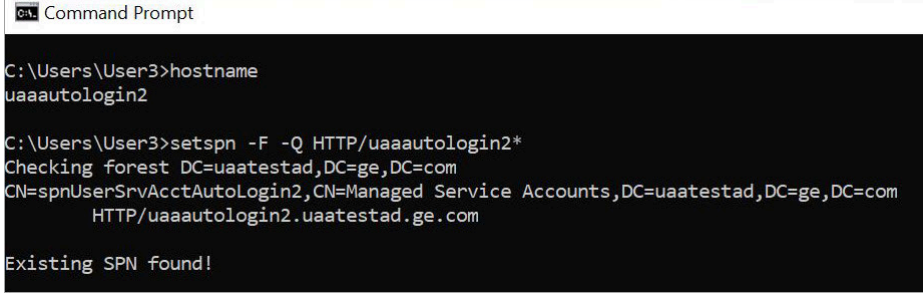
Make sure the clocks on all the three systems are synchronized.

Useful SPN commands

To view existing SPNs


```
setspn -F -Q HTTP/<FQDN>
```

Example: `setspn -F -Q HTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM`

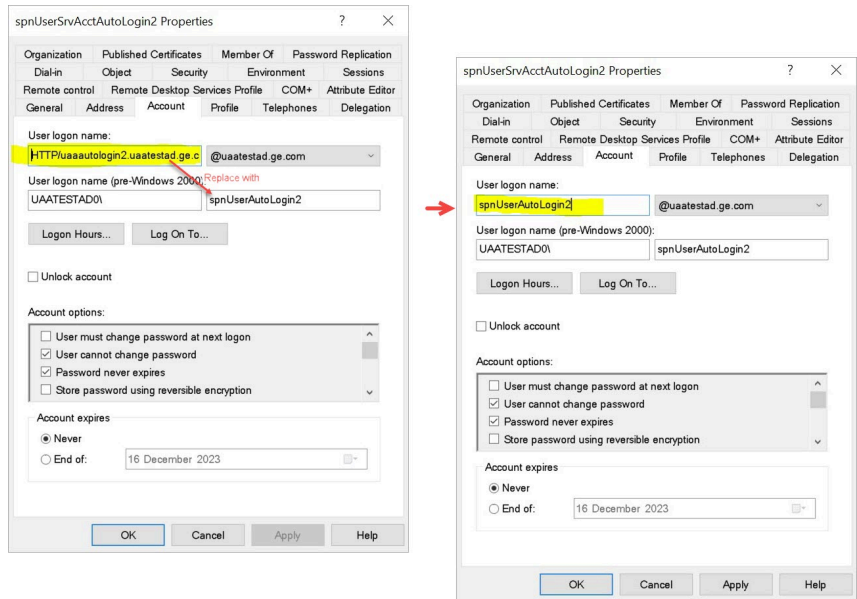
	 <pre> C:\Users\User3>hostname uaaautoLogin2 C:\Users\User3>setspn -F -Q HTTP/uaaautoLogin2* Checking forest DC=uaatestad,DC=ge,DC=com CN=spnUserSrvAcctAutoLogin2,CN=Managed Service Accounts,DC=uaatestad,DC=ge,DC=com HTTP/uaaautoLogin2.uaatestad.ge.com Existing SPN found! </pre>
<p>To delete SPN</p>	<pre>setspn -D HTTP/<FQDN> <user account></pre> <p>Example: <code>setspn -D HTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM</code> ghost1</p>

How to Un-Register an Existing Service Principal Name (SPN)

The following steps ensure the un-registration of the existing SPN and the necessary updates in Active Directory.

<p>Step 1: Delete Any Other SPN (if exists)</p>	<p>Run the command <code>setspn -D HTTP/thenameyougavetothespn spnUserName</code></p> <p>Replace:</p> <ul style="list-style-type: none"> • thenameyougavetothespn with the SPN you want to unregister • spnUserName with the user who created the SPN being un-registered.  <pre> C:\Users\User3>setspn -D HTTP/uaaautoLogin2.uaatestad.ge.com@UAATESTAD.GE.COM spnUserAutoLogin2 Unregistering ServicePrincipalNames for CN=spnUserSrvAcctAutoLogin2, CN=Managed Service Accounts, DC=uaatestad, DC=ge, DC=com HTTP/uaaautoLogin2.uaatestad.ge.com@UAATESTAD.GE.COM Updated object C:\Users\User3> </pre>
<p>Optional step: Verify Un-Registration</p>	<p>Run the command <code>setspn -F -Q HTTP/thenameyougavetothespn*</code></p>
<p>Step 2: Update Logon Name in Active Directory</p>	<ol style="list-style-type: none"> 1. Go to Active Directory. 2. Open the properties of the existing <code>spnUserName</code>.

3. Change the logon name from `HTTP/uaaautologin2.uaatestad.ge.com` to `SAMAccountName` or `User logon name (pre-Windows 2000)`.



Resolving JWT Token Size and Autologin Challenges

When a user is assigned to many groups, there are issues with JWT token size, leading to rejection of requests by Tomcat due to the exceeded header size limit. Additionally, there are problems configuring autologin and logging into Operations Hub with the autologin feature, resulting in a "Bad Request" error.

This issue arises when a user is a member of many Active Directory user groups. The size of the HTTP request header, which contains the Kerberos token in the WWW-Authenticate header, increases with the number of user groups. If the header size exceeds the server-configured limits, the server rejects the request.

To resolve the issue, do the following:

<p>Update HTTPD Configuration File</p>	<ol style="list-style-type: none"> 1. Visit the location <code>C:\Program Files\GE\Proficy Authentication\httpd\conf\app-specific.d\uaa-httpd.conf</code> and open <code>uaa-httpd.conf</code> in a text editor. 2. Add the following code: <pre data-bbox="609 1680 1412 1774">#SPNEGO authentication HTTP request header size LimitRequestFieldSize 16384</pre> 3. Save and close the httpd configuration file.
---	---

Update Tomcat Configuration File

1. Visit the location `C:\Program Files\GE\Proficy Authentication\uaa-tomcat\conf\server.xml` and open `server.xml` in a text editor.

2. Locate the Connector element and change the `maxHttpHeaderSize` attribute.

Change `maxHttpHeaderSize="8192"` to `maxHttpHeaderSize="16384"`.

```
<Connector connectionTimeout="20000" redirectPort="8443"
port="9480" maxPostSize="2097152" maxHttpHeaderSize="16384"
protocol="HTTP/1.1"></Connector>
```

3. Save and close the tomcat configuration file.



Note:

- The default value for the header size is `LimitRequestFieldSize` 8192 bytes (8k).
- The default value for `maxHttpHeaderSize` is 8192.

Issue: Duplicate LDAP User Creation in Proficy Authentication Database

This topic describes potential LDAP IDP configuration choices that may lead to the issue and offers guidance on how to avoid it.

The issue can occur when using multiple LDAP IDP configurations, especially in scenarios involving 'multi-domain support' introduced in version 2023.

Leveraging Multi-Domain Support

The introduction of 'multi-domain support' aimed to allow the configuration of multiple LDAP IDPs, primarily to support user authentication and authorization across *different domains* (multiple LDAP servers) through a single instance of the Proficy Authentication service.

Secondary Use-case: The 'multi-domain support' feature can also be utilized to configure multiple LDAP IDPs for a *single domain* (single LDAP server). This is often done when dealing with large domains with users spread across the directory structure.

Problem Scenario: A potential challenge arises when selecting a single User or Group Search Base in the IDP configuration. This choice may lead to a generic scope, resulting in timeout errors during user

authentication. The issue stems from the extensive search scope for both User and Group searches. To avoid these timeout errors, it is crucial to carefully consider and configure the User and Group Search Base values to align with the specific structure and distribution of users within the targeted domain.

Solution: When setting up multiple LDAP IDPs targeting a single domain or LDAP server, ensure that the 'User Search Base' values across the IDP configurations are distinct. In other words, a user from the configured domain should not be found in more than one LDAP IDP.

Neglecting this precaution can result in a user being authenticated from multiple LDAP IDPs, leading to the creation of multiple user records with different 'origin' names in the UAA Database. This situation can further cause authorization issues in applications like Operations Hub (or any other client application) if authorization selections are made at the individual user level rather than for user groups.