

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

Proficy 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	
Delete Identity Provider	51
Manage Groups	52
Overview of Managing Groups in Proficy Authentication	
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	

Configure Browser	85
Example Configuration for Multi-domain and Auto-login Functionality	
High Availability	89
Configure High Availability for Proficy Authentication	
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: con-fighubadmin
Client Secret	The client secret provided during installing Configuration Hub.

Configuration Hub Administrator Credentials	×	
CLIENT ID		
confighubadmin		
CLIENT SECRET		
NOTE: Use the credentials created during the install process.		
	Verify	

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	The host name of the machine where Proficy Authentication is installed.
Qualified Name)	Enter a fully qualified domain name. For example, desktop-sahfg5f.logon- .ds.ge.com
	Refer to step 6 to establish a trust with this server connection.
Server Port	The port number to communicate with the host machine. The default port where UAA is installed is $\frac{443}{2}$.
	The server connection is automatically tested on entering the port. You can also select Test to test the connection.
Use Configuration Hub Administration	Select this check box to populate the same login credentials you entered for Configuration Hub Admin account.
credentials for Profi- cy Authentication	If you want to use unique login credentials for Proficy Authentication, clear the check box and enter CLIENT ID and CLIENT SECRET .
Client ID	The administrator client identifier that has permission (authority) to log in to Proficy Authentication.
Client Secret	The administrator client secret to log in to Proficy Authentication.

SERVER NAME (FULLY QU	JALIFIED NAME)	
sachinauthguardian	/m01.htclab.ge.com	S Not trusted
SERVER PORT		
443		
Test Server Conne Proficy Authenticati	ection ion Credentials Hub Administration credentials	for Proficy Authentication
Test Server Conne Proficy Authenticati	ection ion Credentials Hub Administration credentials	for Proficy Authentication
Test Server Conne Proficy Authentication Use Configuration F CLIENT ID confighubadmin	ection ion Credentials Hub Administration credentials	for Proficy Authentication
Test Server Conne Proficy Authentication Use Configuration F CLIENT ID confighubadmin CLIENT SECRET	ection ion Credentials Hub Administration credentials	for Proficy Authentication
Test Server Conne Proficy Authentication Use Configuration H CLIENT ID confighubadmin CLIENT SECRET	ection ion Credentials Hub Administration credentials	for Proficy Authentication

6. Select **Not trusted** to establish a trust connection between Configuration Hub and Proficy Authentication.

The Certificate Details screen appears.

ALLIDULE Name	Root Certificate
Subject	CN=SACHINAUTHGUARD Root CA 202112241544, OU=Operations Hub Site,
	O=GE Customer
Thumbprint	0B8B85FDA172C1DCF7A6C48F127085EF1338119C
Serial Number	3F678CC3732C8A69
ssuer CN=SACHINAUTHGUARD Root CA 202112241544, OU=Operatio	
	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.

SERVER NAME (FULLY QUAL	IFIED NAME)	
sachinauthguardianvm	01.htclab.ge.com	
SERVER PORT		
443		
Test Server Connect Proficy Authentication Vse Configuration Hub	tion Credentials D Administration credentials for P	roficy Authentication
Test Server Connect Proficy Authentication Use Configuration Hub	tion Credentials D Administration credentials for P	roficy Authentication
Test Server Connect Proficy Authentication Use Configuration Hub CLIENT ID confighubadmin	tion n Credentials o Administration credentials for P	roficy Authentication
Test Server Connect Proficy Authentication Use Configuration Hub CLIENT ID confighubadmin CLIENT SECRET	tion n Credentials o Administration credentials for P	roficy Authentication
Test Server Connect Proficy Authentication Use Configuration Hub CLIENT ID confighubadmin CLIENT SECRET	tion n Credentials o Administration credentials for P	roficy Authentication

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 Authenti- cation.	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 expe- rience, consider implementing au- to-login. But make sure that your system operates within a trusted network to reduce the risk of unau- thorized access.	Windows Integrated Authentication / Auto-login <i>(on page 73)</i>
4	(Optional) For continuous, reliable, and scalable access to authenti- cation and authorization systems, consider implementing high avail- ability.	Configure High Availability for Proficy Authentication <i>(on page 89)</i>
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 <i>(on page 119)</i>

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.

59 🔝 🗹	\$ ®	◧▾◬▾
NAVIGATION	DETAILS	×
> Proficy Authentication	Proficy Authentication	
Administration	Q Search	
	Field	Value
	✓ GENERAL	
	Name	Proficy Authenti
	Version	4.0.914.0

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.

NAVIGATION \times	Security-Proficy Authentication $~~ imes~$		D	etails ×
✓ ► Proficy Auth	Identity Provider Groups Users			
Security	Q. Search		<mark>c +</mark> ©	
🖲 Custom Ia	Identity Providers 1	Туре	Action	nn Chooser
🖿 Administrati	ldap	ldap		
	uaa	uaa	Column Chooser X	
			🗹 Туре	

- 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 \times	Security-Proficy Authentication $~~ imes~$			DETAILS
✓ ► Proficy Auth	Identity Provider Groups Users			
Security	Q Search		2 + ©	
🕑 Custom la	Identity Providers	Туре	Action	
🖿 Administrati	ldap	Idap		
	uaa	uaa		
-				

- Select 1 to sort data in an ascending order.
- Select \downarrow 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.

NAVIGATION \times	Security-Proficy Authentication $~~ imes~~ imes~$		DETAILS
✓ ► Proficy Authentication	Identity Provider Groups Users		
Security	Q Search	2 + ©	
😻 Custom labels	User Name 1	Email 🝸 🖌	
Administration	ch_admin	ch_admin@test.org	
	OphubAdmin	admin_1708005724@your.dc	
	StudioAdmin	iqp@wbo.co.jp	

- 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.

NAVIGATION ×	Security-Proficy Authentication	\times		DETAILS	×
✓ ➤ Proficy Authentication	Identity Provider Groups	Users		uaa	
O Security	Q Search		c + ©	Q Search	
😻 Custom labels	Identity Providers	Туре	Action	Field ADMINISTRATOR CRED	ENTIALS
Administration	ldap	Idap		Client ID	confighubadmin
	uaa	uaa	000	✓ MFA	
				Disabled	\bigcirc
				Authenticator	Google Au 👻
				V UAA META DATA INFO	ل
				URL	https://pathairi26.
				Assertion Consum	Mps:/ps/with.
				Entity ID	https://pathairth.
				Single Logout Servi	https://patrairith.c

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.

Security-Proficy Authentication	×		DE
Identity Provider Groups	Users		
Q Search			+ 63
Identity Providers † 🝸	Туре 🍸	Action	SAML
Okta Login Station	saml		
uaa	uaa		

The LDAP Identity Provider screen appears.

3. Enter the following details:

Field	Description	
Name	A unique name to help identify your LDAP connection.	
URL	The URL of the LDAP server. The trailing slash (/) must be included at the end of the URL.	
	You can use LDAP with or without secure authentication in the follow- ing format:	
	 Insecure port: ldap://100.100.100.2:389/ Secure port: ldaps://100.100.100.2:636/ 	
	Important: In a URL address, ensure that Idap is in lowercase. Using uppercase letters will render the address non-functional.	
	You can also use a fully qualified domain name instead of an IP ad- dress.	
	For a secure port, provide user credentials.	
Bind User Distinguished Name	This is a distinguished LDAP user name to represent various entities within an LDAP directory hierarchy, including users, groups, and organizational units.	
	The canonical format consists of CN (Common Name), DC (Do- main Component), and OU (Organization Unit Name). CN and DC are mandatory, while OU is optional.	
	Enter the LDAP Distinguished Name in compliance with LDAP stan- dards to ensure proper processing by the system. In the following ex- ample, each component (CN, OU, DC) is correctly formatted, separat- ed by commas without any spaces, and is case sensitive.	
	CN=John Smith,OU=Factory,DC=Company,DC=COM	
	Play the video: How to retrieve the User Distinguished Name re- quired for establishing or modifying the LDAP connection	
	video/LDAP_UserDistinguishedName.mp4	

Field	Description
Password	The password to log in to the LDAP server if you choose secure au- thentication.
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 con- nection 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 *	
	2
Test	Cancel Save

4. If you choose to secure LDAP, select $\stackrel{\bigcirc}{=}$ 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 $^{\textcircled{o}}$ next to the lock icon to view the certificate.

certAttributeName	Root Certificate
certSubject	CN = CWARIRSSVR2K19.pa.com
certThumbprint	4723FC64421BB6A13846CBF5A65EE812B5602A7E
certSerialNumber	580000002F700D88850581AFD00000000002
certissuer	DC = com,pa CN = CWARIRSSVR2K19.pa.com
certValidFrom	Jun 21 18:28:08 2021 GMT
certValidTo	Jun 21 18:28:08 2022 GMT
	Clos

6. Select Save.

Name* CWARIRSSVR2K191		
URL*		
ldaps://CWARIRSSVR2K19.pa.com:636/		8 ©
Bind User Distinguished Name *		
CN=sachin2,CN=Users,DC=htcophub,DC=internal		
Password *		
		Ø
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 do open a pop-up screen with the existing information.

DE	TAILS	>
CV	VARIRSSVR2K19	
Q	Search	
	Field	Value
~	GENERAL	C 2
	Name	CWARIRSSVR2K19
	URL*	Idap://CWARIRSSVR2K19.pa.com:389/
	User DN	CN=sachintestuser,CN=Users,DC=pa,
	Origin Key	CWARIRSSVR2K19
~	OTHER SEARCH CRITERIA	
	Group Base	DC=pa,DC=com
	User Base	DC=pa,DC=com
	User Filter	userPrincipalName={0}
	Group Filter	member={0}
	Max Filter	10

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=En-	Defines the starting point for the LDAP group
	terprise,DC=company,DC=com	search in the active directory tree.

Search Criteria	Example Value	Description
		 CN is Common Name (required) DC is Domain Component (required) OU is Organization Unit Name (optional)
		Note: If you use only DC=Ge, DC=com, time- out may occur due to slow system response. Use the exact ou to avoid timeout.
		See Optimizing LDAP Directory Search (on page 22)
User Base	OU=Sales,OU=Users,OU=En- terprise,DC=company,DC=com	Defines the starting point for the LDAP group user search in the active directory tree.
		Note: If you use only DC=Ge, DC=com, time- out may occur due to slow system response. Use the exact ou to avoid timeout.
		See Optimizing LDAP Directory Search (on page 22)
User Filter	userPrincipalName={0}	Allows the LDAP user (active directory user) to login into Configuration Hub with their email address.
User Filter	cn={0}	Allows the LDAP user (active directory user) to login with their display name. This is field is populated by default.
User Filter	sAMAccountName={0}	Allows the LDAP user (active directory user) to login with their account name (Windows login name). This is field is populated by de- fault.

Search Criteria	Example Value	Description
Group Filter	member={0}	Retrieves the memberof attribute values for the specific user. This is field is populated by default.
Max Filter	10	Defines the maximum depth for searching the LDAP groups. The default value is 10. For very large systems, set the value to 2 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

L UG2

L UG3 L UG4

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

if Max Filter 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 Max Filter 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 hierar- chy.
if Max Filter 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.

i) 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.

- 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.

okta	
Dashboard	~
Directory	~
Customizations	~
Applications	^
Applications	
Self Service	
Security	~

4. Select Create App Integration.

Deactivate unused apps	check out our	plans page. C	Contact us to find a plan that is right for your organization.
Create App Integration	Browse Ap	p Catalog	Assign Users to App More 🔻
Q Search			
STATUS		©	Okta Admin Console
ACTIVE	0	-	
INACTIVE	0	0	Okta Browser Plugin
			Okta Dashboard

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 endpoints. Recommended if you intend to build a custom app integration the Okta Sign-In Widget. 	API with
	 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 SAML. 	or
	 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.

Г

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

1 General Settings		
App name	Multiverse Paradigm	
App logo (optional)	A CONTRACTOR OF	1
App visibility	 Do not display application icon to users 	
		New

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

Single sign on	Use the dowloa	ded Proficy Aut	nentication metadata	file (on pag	ge 24)		
URL	saml-sp.xml to get the URL for this field. It should look something like this:						
	<pre><md:assertioncons Location="http Binding="urn:c index="0"/> <md:assertioncons Location="http Binding="urn:c</md:assertioncons </md:assertioncons </pre>	umerService s://ghldz593e.log asis:names:tc:SAM umerService s://ghldz593e.log asis:names:tc:SAM	on.ds.ge.com/uaa/saml 1L:2.0:bindings:HTTP-PC on.ds.ge.com/uaa/oaut 1L:2.0:bindings:URI" inde	/SSO/alias/o DST" isDefault= h/token/alias ex="1"/>	<mark>phubSamISp"</mark> "true" :/ophubSamISp"		
Audience URI (SP	Refer to saml-s	p.xml to get the	logout URL. It should	look somet	hing like this:		
Entity ID)	<pre><?xml version=": - <md:entitydescri ID="httpsgh xmlns:md="urn: - <ds:signatur< pre=""></ds:signatur<></md:entitydescri </pre>	<pre><?xml version="1.0" encoding="UTF-8"?> - <md:entitydescriptor entityid="https://ghldz593e.logon.ds.ge.com/uaa/saml/metadata" id="httpsghldz593e.logon.ds.ge.com_uaa_saml_metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"></md:entitydescriptor></pre>					
Enable Single Lo-	a. Select S l	how Advanced S	Settings.				
gout	b. Select th	e check box for	Allow application to	initiate Sing	gle Logout.		
	c. Enter Sir	igle Logout URL	. Refer to saml-sp.xm	1 to get the	logout URL. It		
	should lo	ook something li	ke this:				
	<md:singlel< th=""><th>, escriptor> .ogoutService</th><th></th><th></th><th></th></md:singlel<>	, escriptor> .ogoutService					
	Location="https://ghldz593e.logon.ds.ge.com/uaa/saml/SingleLogout/alias/ophubSamlSp" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>						
	Location Binding=	="https://ghldz593e. "urn:oasis:names:tc:	logon.ds.ge.com/uaa/saml/ SAML:2.0:bindings:HTTP-Red	SingleLogout/al lirect"/>	ias/ophubSamlSp"		
			macifeiEAMLil linamaid.				
Attribute State-	Add user attribu	ute statements s	such as email, first na	ime, and las	t name as		
ments (optional)	shown here:						
	Attribute Stateme	nts (optional)		LEARN	MORE		
	Name	Name format (optional)	Value				
	email	Unspecified *	user.email	•			
	first name	Unspecified *	user.firstName	Ŧ	×		
	last name	Unspecified *	user.lastName	•	×		
	Add Another						
Group Attribute	Add group attri	oute statements	such as groupA and	groupB as	shown here:		
Statements (op-			-				
tional)							

Group Attribute	e Statements (optional)				
Name	Name format (optional)	Filter			
groupA	Unspecified *	Contains	٣	manager	
groupB	Unspecified +	Contains	Ŧ	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**.



Your application is created.

10. Under Sign On, select Identity Provider metadata.

Multiverse Paradigm Active View Logs Monitor Imports	5
i Once you have a working SAML integration, submit it for Okta revie	w 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 of application. Some sign-on methods require additional configuration in the	credentials for an 3 rd party application
Application username is determined by the user profile mapping. Configur	e profile mapping
SAML 2.0	
Default Dalau State	
Default Relay State	
SAML 2.0 is not configured until you complete the setup instru-	ctions.
View Setup Instructions	
Identity Provider metadata is available if this application suppor	ts dynamic configuration.

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 Enter- prise Application	Do the following to set up an enterprise application in Azure with the necessary con- figuration.
	 Log in to your Azure account. 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 bottestsaml.
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.
	 Log in to your Azure account and navigate to the enterprise application you created earlier (bobtestsaml is our example application). Select Users and groups > Add user/group. 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	metad	ata	file.

NAVIGATION \times	X Security Proficy Authentication X DETAILS						
 Proficy Authenticat 	Identity Provider Groups Users	Identity Provider Groups Users			ua	a	
Security					Q	Search	
	Q. Search		8	+ ©		Field	Value
• white cabeling	Identity Providers 1	Туре	Action		~	ADMINISTRATOR CREDENT	nals 🖸
Administration	ldap	ldap				Client ID	admin
	uaa	uaa	***		~	MFA	
First Selection						Disabled	
						Authenticator	Google Auth
	Second Selection		Third Selection	_	v	UAA META DATA INFO	
						URL	https://ramanvm202r
						Assertion Consumer _	https://ramanvm202.
						Entity ID	https://ramanvm202.
						Single Logout Service	https://ramanvm202.

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**.



Under recent ser-	■ Microsoft Azure P Search resources, services, and docs (G+/)	도 다 다 않 ⑦ 곳 _{en}
vices:	Azure services + Create a resource Azure Active Directory Storage Virtual groups Virtual groups Subscriptions Q	🚀 📀 📷 - ukkstart App Services SQL databases More Center
	Nesources	
Run a search using	Microsoft Azure Azure Active Directory	× 5 6 9 % 7
the search bar:	Azure service Create a resource All Services (99+) Marketplace (9) Documentation (99+) A Resource Groups (0) Services Azure Active Directory Create a	zure Active Directory (8) Resources (0) See a ase for MySQL servers

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

Hor	ne >					
0	General Electric Inte Azure Active Directory	ernational, Inc.	Overview			
	«	+ Add 🗸 🛞 Mar	nage tenants 🛛 What's new 🛛 🗔 Pre	eview features	🛜 Got feedback? 🗸	
0	Overview					
**	Preview features	 Azure Active Dire 	ctory is becoming Microsoft Entra ID. Learn	more 🛙		
×	Diagnose and solve problems	Overview Monitor	ing Properties Recommendation	s Tutorials		
Mai	nage	Search your tenar	nt			
8	Users					
24	Groups	Basic information				
0	External Identities	Name	General Electric International, Inc.		Users	
2	Roles and administrators	Tenant ID		D	Groups	
а	Administrative units			-		
•	Delegated admin partners	Primary domain			Applications	
Щ,	Enterprise applications	License	Azure AD Premium P2		Devices	
-						



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

Searching applica-	E Microsoft Ature P Search resources, services, and doos (G+/) Σ 🚱 Ο Θ 🖗 22200/0735@gr				
tions	Home > General Electric International. Inc. [Enterprise applications > Enterprise applications Enterprise applications All applications — —				
	Converse				
If needed, request	Microsoft Azure P Search resources, services, and doos (S+/) D D D D D D D D D				
your IT Azure Ex-	Total 2 - Contrain Deckins Internationals, Inc. Linearpoint applications - Contexprise applications The Enterprise International, Inc Annu Active Density Conneal Betwin Unc Annu Active Density				
pert team to create	+ New application Overview ▲				
a new application	Overview View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider. X Diagnose and solve problems The list of applications that are maintained by your organization registrations.				
from here:	Manage Dibblestaml Application type == Enterprise Applications Application ID starts with Implication ID starts with ImplicatiD starts with Implication ID starts				
	User settings Dotorstand Dotorstand Dotorstand				

d. Open the enterprise application and select Set up single sign on.
Home > General Electric International,	Home > General Electric International, Inc. Enterprise applications > Enterprise applications All applications >					
Bobtestsaml Over	view …					
~						
III. Overview	Properties					
Deployment Plan	Name ①					
X Diagnose and solve problems	BO bobtestsaml					
Manage	Application ID 💿					
Properties	Object ID ()					
A Owners	object to 0					
8 Roles and administrators	Cathing Shared					
Users and groups	Getting Started					
Single sign-on						
Provisioning	1. Assign users and groups \bigcirc 2. Set up single sign on					
Application proxy	Provide specific users and groups access Enable users to sign into their application to the applications using their Azure AD credentials					
 Self-service 	Assign users and groups Get started					
Custom security attributes						

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

Home > General Electric International, Inc. Enterprise applications > Enterprise applications All applications > bobtestsaml					
bobtestsaml SAML-based Sign-on					
 Werview Deployment Plan Diagnose and solve problems 	 Tupload metadata file Change single sign-on mode I Test this application R Got feedback? Upload metadata file. Values for the fields below are provided by bobtestsaml. You may either enter those values manually, or upload a preconfigured SAML metadata file if provided by bobtestsaml. 				
Manage	Select a file				
Properties	Add Cancel				
A Owners	Ledit				

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

= Microsoft Azure	arch resourc	es, services, and docs (G+/)			2	8	0		
Home > General Electric Internation	al, Inc. Ent	erprise applications > Enterprise applications	All applications > bobtestsaml					_	
bobtestsaml SAML-	based (Sign-on							×
Overview	▲ T	Upload metadata file 🂙 Change single sign-on	mode 🔚 Test this application	Got feedback?					
Deployment Plan	Set	up Single Sign-On with SAM							
K Diagnose and solve problems	An SS	O implementation based on federation protocols in	mproves security, reliability, and en	d user experiences and is	easier to				
Manage	more	ment. Choose SAML single sign-on whenever poss	ble for existing applications that d	o not use OpenID Connec	t or OAu	th. Learn			
Properties									
Owners	0	Basic SAML Configuration							
Roles and administrators					6 Edit				
Users and groups		Identifier (Entity ID)	ata	/uaa/sami/metad					
Single sign on		Reply URL (Assertion Consumer Service URL)	https://	/uaa/saml/SSO/al					
 Desidential 		Sign on URL	Optional						
Provisioning		Relay State (Optional)	Optional						
Application proxy		Logout Url (Optional)	https://: Looout/alias/oobubSam/So	/uaa/saml/Single					
Self-service			cogood anost opriod sorringp						
Custom security attributes									
		Attributes & Claims			🖉 Edit				
ecurity		givenname	user.givenname						
Conditional Access		surname	user.sumame						
Permissions		emailaddress	user.mail						
Taken economics		name Unique User Identifiar	user.userprincipalname						
· iower encryption		Group	user.groups						
Activity									
Sian-in loas									

- 3. Perform User and Group Attribute Mapping in Azure
 - a. In the enterprise application, under User Attributes & Claims section, select Edit.

	ed Sign-on	
Overview Deployment Plan Diagnose and solve problems Manage	 Upload metadata file Change single sign-on metadata Basic SAML Configuration Identifier (Entity ID) Reply URL (Assertion Consumer Service URL) 	ode 🔚 Test this application 🔊 Got feedback?
 Properties Owners Roles and administrators 	Sign on URL Relay State (Optional) Logout Url (Optional)	And
Users and groupsSingle sign-on	2 Attributes & Claims	🖉 Edit
 Provisioning Application proxy Self-service 	givenname us surname us emailaddress us name us Unique User Identifier us	ser.givenname ser.mail ser.userprincipalname ser.userprincipalname

b. Select Add new claim.

■ Microsoft Azure	and docs (G+/)			\sum	Ŗ	P	<u>نې</u>	?	ন্দ	GENER
Home > Enterprise appl Attributes & Claims	ications > Enter	prise applications All applications	> bobtestsaml	SAML-t	ased S	ign-on	> SA	ML-ba	sed Sig	n-on >
+ Add new claim + Add a group claim EE Columns	🖗 Got feedb	ack?								
Claim name	Туре	Value								
Unique User Identifier (Name ID)	SAML	user.userprincipalname [nameid-form	nat:emai **							
4			•							
Additional claims										
Claim name	Туре	Value								
http://schemas.microsoft.com/ws/2008/06/identity/claims/grou	ups SAML	user.groups [SecurityGroup]								
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emaile	address SAML	user.mail	•••							
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/given	name 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/surna	me SAML	user.surname								
✓ Advanced settings										

c. Enter claim details, and save the information.

··· > Enterprise application	ns All applications > bobtestsaml SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >
Manage claim	
Save X Discard chang	Jes ${\not\sim}$ 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
\checkmark Claim conditions	
\checkmark 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.

-				
	Microsoft Azure P Search resources, services, and o	docs (G+/)		
	Home > General Electric International, Inc. Enterprise application Attributes & Claims	tsaml SAV Group Claims Manage the group claims used by Azure AD to populate SAML tokens issued to your app		
	+ Add new claim + Add a group claim = Columns Ř	Which groups associated with the user should be returned in the daim?		
	Required claim			 Security groups
	Claim name	Туре	Value	 Directory roles
	Unique User Identifier (Name ID)	SAML	user.userprincipalname [Groups assigned to the application
				Source attribute *
	Additional claims			sAMAccountName
	Claim name	Туре	Value	
	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [SecurityGro ***	 This source attribute only works for groups synchronized from an on-premises Activusing AAD Connect Sync 1.2.70.0 or above. Learn More
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd	SAML	user.mail ····	Emit group name for cloud-only groups ③
	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 ***	Advanced options
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ····	

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.

Home > General Electric International, Inc. Enterprise applicatio	ns > Enterprise application	ns All applications > bob	itestsaml SAN	Group Claims		
Attributes & Claims				Manage the group claims used by Azure AD to populate SAML tokens issued to your app		
				Source attribute *		
Later water and the same state and statements in the	C			sAMAccountName 🗸		
+ Add new claim + Add a group claim == Columns X	Got feedback?					
				This source attribute only works for groups synchronized from an on-premises active Directory using AAD Connect Sync 1.2.70.0 or above. Learn More		
Required claim						
Claim name	Туре	Value		Emit group name for cloud-only groups ()		
Unique User Identifier (Name ID)	SAML	user.userprincipalname [Advanced options 		
Additional claims				Filter groups		
Claim name	Type	Value		Attribute to match *		
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [SecurityGro		SAMAccountName V		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd	SAML	user.mail		Match with *		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname		Prefix V		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname		String *		
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.sumame		MES		
✓ Advanced settings				Customize the name of the group claim		

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.

Microsoft Azure P Search resources, services, and description	ocs (G+/)			۶.	G.	Ø	۲	0	R
Home > General Electric International, Inc. Enterprise applications > Enterprise applications All applications > bobtestsaml SAML-based Sign-on > SAML-based Sign-on >									
Attributes & Claims									
+ Add new claim + Add a group claim ≣≣ Columns 🔗	Got feedback?								
Required claim									
Claim name	Туре	Value							
Unique User Identifier (Name ID)	SAML	user.userprincipalname [***							
Additional claims									
Claim name	Туре	Value	_						
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [SecurityGro ***							
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd	SAML	user.mail ***							

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.

Deployment Plan	name	user.userprincipalname	
copioyincine run	Unique User Identifier	user.userprincipalname	
Diagnose and solve problems	Group	user.groups	
anage			
Properties	3 SAML Certificates		
Owners	Token signing certificate	· · · · · ·	
omen	Status	Active	🖉 Ed
Roles and administrators	Thumbprint	E1B58AF3727	
Users and groups	Expiration	5/11/2026, 6:23:05 PM	
oscis una groups	Notification Email	@ge.com	
Single sign-on	App Federation Metadata Url	https://login.microsoftonline.com/15ccb6d1-d335	
Provisioning	Certificate (Base64)	Download	
	Certificate (Raw)	Download	
Application proxy	Federation Metadata XML	Download	
Self-service			
Custom security attributes	Verification certificates (optional)		🖉 Ed
custom security attributes	Required	No	₽ E0
curity	Active	0	
	Expired	0	
Conditional Access			

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**.

% 🔓 Save			⑦ ◧∨ 쓰∨
NAVIGATION	$ imes$ Security-Proficy Authentication $\ imes$		
 Proficy Authentication 	Identity Provider Groups Users		
Security	Q Search		~ L @
🕑 White Labeling	Identity Providers 1	Type	
Administration		.)**	June June

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 <i>(on page 39)</i> .
Name	Name of the SAML application. You can provide any name.
Attribute Name	Enter the Group Name mapping. Refer to this screen shot <i>(on page 38)</i> .
Name ID	From drop down, select format:unspecified.
Enable SAML Link	Select the check box.

		N 8 9 6 0 7
SAML Identity Provider	Home > General Electric International, Inc. [Enterprise applications > Enterprise applications M applications > bothestaml S Attributes & Claims –	AML-based Sign-on > SAML-based Sign-on >
NOTE : All fields are mandatory	$+$ Add rew daim $+$ Add a group claim \equiv Columns R Got feedbadd	
Upload XML File Provide File Location	Required claim Claim name Type Value	
	Unique User Identifier (Name ID) SAMA, user-userprincipalmane (, ***	
Upload XML File	Additional claims Claim name Type Value	
	http://tidenas.microsoft.com/vsi2008/05/denthy/claims/groups SAM, user.groups SecurityGro. *** http://tidenas.umtocac.org/vsi2008/05/denthy/claims/groups SAM, user.net	
Commercials and the second		
Attribute Name*		
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups		
Name ID*		
urn:oasis:namestc:SAML:1.1:nameid-format:unspecified $\timestc} X$. \bullet		
✓ Enable SAML Link		
Cancel Save		

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

NAVIGATION $ imes$	GATION × Security-Profixy Authentication × DETAILS					×
Proficy A	Identity Provider Group	os Users			Field	Value
Security	O Search		1 13	~	GENERAL	ď
White La	Q Search		T (9)		Name	Azure AD SAML
	Identity Providers 1	Туре	Action		MetaData	xml version="1.0" encoding="utf-8"? <EntityDescriptor ID="_c82426</td>
	Azure AD SAML	saml	000		Group Attribute	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
	NewLdap	ldap			nameID	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
	OKTA-SAML	saml			Origin Key	Azure AD SAML
	uaa	uaa		~	OTHER SAML PROPERTIES	
	UAA LDAP	ldap			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.

tributes & Claims					DE	TAILS	
Add new claim + Add a group claim III Columns 🔗 0	ot feedback?					Field	Value
quired claim	C. Type	Value			~	GENERAL	ß
ique User Identifier (Name ID)	0 SAML	user userprincipalname (nameid-form	Below mentioned mapping is to be performed in Details panel of Confighub-			Name	Azure AD SAML
itional claims			Proficy Auth. plugin >> SAML Connection			MetaData	xml version="1.0" encoding="utf-8"? <EntityDescriptor ID="_c8242</td>
im name	C. Type	Value			→ [Group Attribute	http://schemas.microsoft.com/ws/2008/06/identity/claims/groups
p://schemas.microsoft.com/ws/2008/06/identity/claims/groups p://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	0 SAML 0 SAML	user.groups [SecurityGroup] ····	User Attribute Mapping -> Email			namelD	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
c//schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	0 SAML	user.givenname ····	Jser Attribute Mapping -> Firstname	-		Origin Key	Azure AD SAML
//schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	0 SAML	user.sumarne ···· [Jser Attribute Mapping -> Lastname	- 1	~	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/emailaddr
						Dhana	contact

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.

💋 🔒 Save		
NAVIGATION >	imes Security-Proficy Aut $ imes$ iqp.developer-Proficy Authentication $ imes$	DE
✓ ► Proficy Authe	Group	
• Security	iqp.developer 👻	
🕲 White Labe	Member(Users) Mapping Member(Groups)	
> Administration	Identity Provider	
	Azure AD SAML 👻	
	Add SAML Group	
	MES_Operator +	
	Groups Mapped Groups	
	Group Name Group Name	
	←	
	No data No data	

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

💅 🎧 Save			
NAVIGATION \times	Security-Proficy Aut 🗙 iqp.developer-Prof	ficy Authentication $~~ imes~~$	DETAILS
Proficy Authe	Group		
• Security	iqp.developer	*	
🕑 White Labe	Member(Users) Mapping Member(Grou	ps)	
> Administration	Identity Provider		
	Add SAML Group	+	
	Groups Group Name	Mapped Groups Group Name	
	MES_Admin_User	MES_Operator	
	Available group for mapping	← Successfully mapped groups	

g. Select \rightarrow 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.

Bobtestsaml Sigr	n-in logs 🛷 …						×
Users and groups	× ↓ Download ∨ 8	🔅 Export Data Se	ttings 🗙 Troubleshoo	t 🕐 Refresh ΞΞ Columns			
Single sign-on	Want to switch b	ack to the default si	gn-ins experience? Click he	re to leave the preview. \rightarrow			
 Provisioning Application proxy 	Date : Last 7 days	Show dates	as : Local Applic	ation contains f46	7 +7	Add filters	
G Self-service	User sign-ins (inter	active) User si	gn-ins (non-interactive	Service principal sign-ins	Managed identity sign-ins		
Custom security attributes	Date	↓ Request ID	↑↓ User	\uparrow ↓ Application \uparrow ↓ S	tatus IP address	5 ↑↓	Location
Security	9/5/2023, 10:01:30	PM 7aa	i M	z (bobtestsaml St	uccess 2)7	Fa Connect
🍨 Conditional Access	9/5/2023, 9:54:36 P	M 0cb	i Me	z (bobtestsaml Fa	ailure 2	<u>'8</u>	Fa Connect
Permissions	9/5/2023, 6:16:56 P	M 633	Me	z (bobtestsaml S	uccess 2	;8	Fa Connect
Token encryption	9/5/2023, 6:16:55 P	M a7a	M	z (bobtestsaml S	uccess 2	;8	Fa Connect
Activity	9/5/2023, 6:16:54 P	M 6ec	M	z (bobtestsaml S	uccess 2	i8	Fa Connecti
Sign in logs	9/5/2023, 6:16:54 P	M be8	M	z (bobtestsaml Fa	ailure 2	i8	Fa Connect
	9/5/2023, 4:45:12 P	M 3e2	M	z (bobtestsaml Fa	ailure 2	'3	Fa Connect
Audit logs	♥/5/2023, 4:45:11 P	M 1d7	р М	z (bobtestsaml Fa	ailure 2	'3	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.

-SK SAN	IL-tracer	
× Clear	Il Pause ± Autoscroll ⊽ Filter resources 0 Colorize & Export &	Import
POST POST GET POST	https://login.microsoftonline.com/b5da5f35-6442-4f5a-9622-92ec6a53513 https://browser.events.data.microsoft.com/OneCollector/1.0/?cors=true&c https://login.microsoftonline.com/kmsi	27/login content-type=application/x-json-stream&client-id=NO_AUTH&client-version=1DS-Web-JS-3.1.11&apikey=69a
GET GET GET GET GET GET GET GET	https://www.wiki.com/usa/oauth/authorize?clent_id=igo-de https://www.wiki.com/com/usa/oauth/authorize?clent_id=igo-de https://www.wiki.com/com/app https://www.wiki.com/com/apits/state=ev/o https://www.wiki.com/com/apits/state=losts/Primary-Font- https://www.wiki.com/com/apits/state=losts/Primary-Font- https://www.wiki.com/com/apits/state=losts/Primary-font- state=losts/Primary-font- primary-font- primary-font- primary-font- ts/Primary-font- primary-font- primary-font- font- font-font- state=losts/Primary-font- font-font- font-font-font- font-font-font-font-font- font-font-font-font-font-font-font- font-font-font-font-font-font-font-font-	v&redrect_uri=https://www/kyw01.uk.getiee_corpisite/login&response_type=code&state=ev/low ah
нпр	Parameters SAML Summary	
http:// http:// http:// http:// http:// http:// http:// http:// http:// http://	/schemas.microsoft.com/identity/claims/displaymame /schemas.microsoft.com/ws/2000/06/identity/claims/groups /schemas.microsoft.com/ws/2000/06/identity/claims/groups /schemas.microsoft.com/ws/2000/06/identity/claims/groups /schemas.microsoft.com/ws/2000/06/identity/claims/groups /schemas.microsoft.com/ws/2000/06/identity/claims/groups /schemas.microsoft.com/ws/2000/06/identity/claims/groups /schemas.microsoft.com/ws/2000/06/identity/claims/groups /schemas.microsoft.com/ws/2000/06/identity/claims/groups /schemas.microsoft.com/identity/claims/groups /schemas.microsoft.com/identity/claims/identity/claims/groups /schemas.microsoft.com/identity/claims/identity/claims/groups /schemas.microsoft.com/identity/claims/identity/claims/groups /schemas.xmicrosoft.com/identity/claims/identity/claims/groups	Kenet A Teeters Pyrote ContractorGroups AT THE ContractorS ContractorS ContractorS ContractorS ContractorS ContractorS HPtTP://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password Kenet Kenet Kenet Kenet Kenet Ken

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**.

Security-Proficy Authentication $~~ imes~$			۵
Identity Provider Groups Users			
Q Search			+ 63
Identity Providers † 🝸	Туре 🝸	Action	SAML
Okta Login Station	saml		
uaa	uaa		

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 ex- ternal 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, $_{okta_123}$ or $_{de-}$
	mo_mach_azure.
Attribute Name	The attribute that contains the group member-
	ship information about a user in a SAML asser-
	tion.
Name ID	SAML Name identifier and associated fields
	that you want to use in a link test.
Enable SAML Link	Select the check box.

NOTE : All fields are man	ndatory		
Upload XML File	Provide File Location		
https://dev-38020232	.okta.com/app/exk2uugkc5PUxlfaa5d7/	sso/saml/meta	Load
xml version="1.0" er<br entityID="http://www. wmlocom/l="uroconsistent	ncoding="UTF-8"?> <md:entitydescriptor .okta.com/exk2uugkc5PUxlfaa5d7" >>>>>================================</md:entitydescriptor 	CODeceristor	- -
Name*			
okta_123			
okta_123 Attribute Name*			
okta_123 Attribute Name* email			
okta_123 Attribute Name* email Name ID*			
okta_123 Attribute Name* email Name ID* urn:oasis:names:tc:SA	ML:1.1:nameid-format:emailAddress		× •
okta_123 Attribute Name* email Name ID* urr:oasis:names:tc:SA ✓ Enable SAML Link	ML:1.1:nameid-format:emailAddress		× •

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 for display the details in a pop-up screen.

DE	TAILS		\times					
Ok	Okta Login Station							
Q	Search							
	Field	Value						
>	GENERAL							
>	OTHER SAML PROPERTIES							

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.



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.
- 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.

	FIELD	VALUE
~	ADMINISTRATOR	CREDENTIALS
	Client ID	admin
~	GENERAL	
	URL	https://deskto
~	MFA	
	Disabled	
	Authenticator	Googl 🗸

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.



- 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



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.
- Go to Proficy Authentication > Security > Identity Provider.
 The existing list of identity providers appear.
- Select the identity provider you want to delete.
 Additional options appear under the ACTION column.
- 4. Select **Doo**, then **Delete**.

Security-Proficy Authentication $~~ imes~$		DE
Identity Provider Groups Use	rs	O
		Q
Q Search		+ 🗇
Identity Providers † 🝸	Туре 🝸	Action
Okta Login Station	saml	Map Groups
uaa	uaa	Delete
		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
iqp.developer	This scope is assigned to developer users.
	When a developer account is created, an associated application user ac- count 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.
iqp.user	This scope is assigned to application users. 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 sole- ly restricted to the runtime functionality of the applications.
iqp.clouduser	This scope is assigned to users who want to use the REST API, mainly the M2M Device RESTful APIs.
iqp.nodered	This scope is assigned to users who want to access the Dataflow Edi- tor.
iqp.studioAdmin	This scope is assigned to privileged users.

Scope	Description	
	Users with this scope can access the Administrator Console to config-	
	the global settings for an operations Hub instance, such as the settings	
	for email servers and the MQTT brokers for MQTT data interoperability.	
	Note:	
	This scope does NOT grant access to Operations Hub designer	
	or runtime.	
iqp.tenantAdmin	This scope is assigned to privileged users.	
	Users with this scope gain administrative authority at the Tenant or Sys-	
	tem level (in our case, we have one tenant). They enjoy full administra-	
	tive access to the Operations Hub instance, with the exception of sce-	
	narios requiring membership in the $iqp.studioAdmin$ group. Administra-	
	tors with this scope have the ability to unlock an application that may be	
	locked by another user.	

Scopes for iFIX Users/Groups

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

Scope	Description
scada.fix_shared_IFIX_PROFICY_AUTH_ADMIN	Allows access to all iFIX application features. Any Profi- cy 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 Authenti- cation users who want to directly log in to iFIX can use this group.
	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.
scada.fix.shared.APPLICATION_DESIGNER	Allows a user to access Configuration Hub and provides use of iFIX features such as iFIX connection, database, and model management.

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

Scope	Description	
	 Important: scada.fix.shared.APPLICATION_DESIGNER 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). Database Block Add-Delete Database Reload Database Save Security Configuration System Configuration 	
scada.fix.shared.OPERATORS	Allows run mode only access for a user in iFIX.	
scada.fix.shared.SUPERVISORS	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.	
scada.proficy.admin:	Allows the Proficy Authentication user access to the iFIX Projects panel and to the Deploy operations from Configuration Hub. This group is for Proficy Authentica- tion 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
historian_visualization.admin	Provides access to Trend Client and the Web Admin console.
historian_visualization.user	Allows access to Trend Client.
historian_rest_api.read	Provides read access to public REST API.
historian_rest_api.write	Provides write access to public REST API.
historian_rest_api.admin	Provides read/write access to public REST API.
historian_enterprise.admin	Provides read/write access to Configuration Hub APIs.
historian_enterprise.user	Allows access to Configuration Hub APIs.
ih_archive_admins	Provides the ability to create, modify, and remove archives.
ih_audited_writers	Allows data writes and to produce a message each time a data value is added or changed.
ih_collector_admins	Allows the ability to add collector instances and change their destination.
ih_readers	Provides access to the ability to read data and system statistics. Also allowed access to Historian Adminis-trator.
ih_security_admins	Provides access to Historian power security users. Se- curity administrators have rights to all Historian func- tions.
ih_tag_admins	Provides access to allow the ability to create, modi- fy, and remove tags. Tag-level security can override rights given to other Historian security groups. Tag ad- mins can also browse collectors.
ih_unaudited_logins	Allow connections to the Data Archiver without creat- ing login successful audit messages.
ih_unaudited_writers	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
mes.reports.user	Reports
mes.genealogy.user	Genealogy
mes.activities.user	Activities
mes.alarms.user	Alarm Notifications
mes.alarms.user	Alarms
mes.analysis.user	Analysis
mes.approval_cockpit.user	Approval Cockpit
mes.autolog.user	Autolog
mes.bom_editor.user	BOM Editor
mes.configuration_management.user	Configuration
mes.downtime.user	Downtime
mes.engineeringChangeOrder.user	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 +

Security-Proficy Authentication $~~ imes~~ imes~$		
Identity Provider Groups Users		
Q Search		+@
Group Name † 🍸	Members 🍸	Action
clients.admin	0	
clients.read	1	
clients.secret	0	

The Add Group screen appears.

3. 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, Supervisors_LineA
Description	A brief description of the group.

Add Group		
Group Name*		
Supervisors_LineA		
Description		
Members to monitor LineA		
Members to monitor LineA		
	Cancel	Add

4. 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 **DOO**, then **Edit**.

The group opens in a new tab.

Security-Proficy Aut $ imes$ confighub.access	-Proficy Authentication $~~ imes~~$	
Group		
confighub.access	•	
Member(Users) Mapping Member(Grou	ips)	+ 🐵
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 <i>(on page 64)</i> .	

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

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 \rightarrow to move the selected items from **Groups** to **Mapped Groups**.

Group	
confighub.access -	
Member(Users) Mapping Member(Groups)	
Identity Provider	
uaa 👻	
Groups	Mapped Groups
Display Name	Display Name
✓ cloud_controller.admin	scim.invite
clients.read	← uaa.resource
clients.secret	
uaa.admin	\rightarrow
clients.admin	

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 \Im .
 - d. Select \rightarrow to move the selected items from **Groups** to **Mapped Groups**.

Member(Use	ers) Mapping Member(Groups)				
Identity Prov	ider				
UAA LDAP	•				
LDAP Groups	s Search Filter				
(objectclas	s=*)	\mathbb{Y}			
Groups				Mapped Grou	ups
	DN				DN
	CN=HelpLibraryUpdaters,CN=Users,D	С=р			CN=SQLServer2005SQLBrowserUser\$C
 Image: A start of the start of	CN=WSS_ADMIN_WPG,CN=Users,DC=	ра,	←		CN=SQLServerMSASUser\$CWARIRSSVR2
 Image: A start of the start of	CN=Administrators,CN=Builtin,DC=pa	,DC			CN=WSS_WPG,CN=Users,DC=pa,DC=com
	CN=Guests,CN=Builtin,DC=pa,DC=con	n	\rightarrow		CN=Users,CN=Builtin,DC=pa,DC=com
	CN=Print Operators,CN=Builtin,DC=pa	,DC			
	CN=Backup Operators,CN=Builtin,DC=	pa,			
	CN=Replicator,CN=Builtin,DC=pa,DC=	com			

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.

Group	
cloud_controller.admin 👻	
Member(Users) Mapping Member(Groups)	
Identity Provider	
Okta Login Station 👻	
Add SAML Group	
corp_group	+
Groups	
Group Name ↓	

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

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

+		
	Mapped Groups	
	Group Name	
	secure_sys_group	
←		
\rightarrow		
	+ ← →	Happed Groups Group Name Secure_sys_group →

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.

 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.

	User List †	
 Image: A set of the set of the	ch_admin	
~	kal_el	
	mandrake_01	
✓	phantom	

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.

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 Q Search			
	GROUPNAME †		
	clients.admin		
	clients.read		
	clients.secret		
	clients.write		
\checkmark	cloud_controller.admin		
	confighub.admin		
		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.

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 **Delete**.

Identity Provider Groups		
Q Search		+ 🗇
Group Name	Members	Y Action
clients.admin	0	
clients.read	1	600
clients.secret	0	Edit
clients.write	1	Delete
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 +

dentity Provider Groups			
Q Search			+
User Name † 🍸	Email 🍸	Origin 🍸	Actio
ch_admin	ch_admin@test.org	uaa	
kal_el	krypton@gmail.com	uaa	
mandrake_01	magician@gmail.com	uaa	
phantom	devilwolf@gmail.com	uaa	

The Add User screen appears.

3. 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*		Ø
Confirm Password*		Ø
Email*		
pacman@gmail.com		
	Cancel	Add
	Cancel	- Add

4. 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
uaa.admin	This scope indicates that this is a superuser.
clients.write	This scope resets the Security plug-in's admin client secret.
password.write	This admin scope enables to change the user password.
	Note: This scope is assigned to all the UAA/LDAP/SAML users by default without the need to assign manually.

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 C next to the **GROUP MEMBERSHIP** section.



The Group Membership screen appears.

 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 Q Sear	Membership		
	GROUPNAME 1		
	clients.admin		
~	clients.read		
	clients.secret		
~	clients.write		
	cloud_controller.admin		
\checkmark	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.

Security-Proficy Authentication	\times				DE	TAILS		\times
Identity Provider Groups	Users				ph	antom		
	_				Q	Search		
Q Search				+ 💿		Field	Value	
User Name 1 🝸		Email 🝸	Origin T	Action	>	GENERAL		
ch_admin		ch_admin@test.org	uaa		>	GROUP MEMBERSH	HIP	ď
kal_el		krypton@gmail.com	uaa		~	PASSWORD		
mandrake_01		magician@gmail.com	uaa			Last Modified	04/01/2023	2.2
phantom		devilwolf@gmail.com	uaa	۵		Last Logon	04/01/2022	- , t
						ResetPassword	Reset	

3. Select RESET.

The Password Reset screen appears.

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

Password Reset		
User Name* phantom		
Password*		Ø
Confirm Password*		Ø
	Cancel	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.

Identity Provider Groups			
Q Search		+	ŝ
User Name 1 🍸	Email 🍸	Origin 🍸 🛛 🦱	ction
ch_admin	ch_admin@test.org	uaa	۵
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 Of 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.



- 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).



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



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).





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)





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</pre>

Code	Replace With
<fqdn></fqdn>	Fully Qualified Domain Name (FQDN) of the server on which Proficy Authentication service is running.
	For example, HTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM Note: These should be in capital letters:
<user account=""></user>	Dedicated managed service user account created for Proficy Au- thentication service. For example, ghost1.

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 pincipal name> -mapUser <user account> -mapOp set -pass password> -crypto AES256SHA1 -pType KRB5_NT_PRINCIPAL

Code	Replace With
<filename></filename>	Name of the keytab file.
	Note: Keytab file name can be any given name.
	The file is created at the default location. You also have the option
	\Documents\myskullcave.keytab.
<service name="" pincipal=""></service>	Enter the service principal name that was created in the following format: hTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM
<user account=""></user>	Enter the same managed service user account that was used dur- ing creating the service principal name. For example, ghost1.
	Note: If you want to use a different user account, delete the ex- isting user account, (or) rename the logon name in the user account.
<password></password>	Proficy Authentication managed service user account password.
AES256-SHA1	Encryption algorithm you want to use.
	Note: GE recommends AES256-SHA1. But you can also use AES128-SHA1.
KRB5_NT_PRINCIPAL	Encryption type you want to use.

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 Gei321itc -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.

Proficy Authentication | 1 - Proficy Authentication | 84

Active Directory Users and Comp	Name	Туре	Description						
> Saved Queries	🛃 Administrator	User Built-in accour		r admin					
✓ m uaatestad.ge.com	Allowed RODC Password Rep	Security Group Members in thi		roup ca					
> Builtin	A Cert Publishers	Security Group	Members of this g	roup ar					
> Computers	Read Cloneable Domain Controllers	Security Group	Members of this g	roup th_					
 Domain Controllers Entermice 	Repl_ Denied RODC Password Repl_	Security Group	Members in thi	enfron December				· ·	
Enterprise	Regional Dris Admins	Security Group	DNS Administr						
ForeignsecuntyPrincipals	Register DrsupdateProxy	Security Group	DNS clients wh	Omanization I	Published C	Certificates M	ember Of Passa	ord Replication	
> Contraction	B Domain Admins	Security Group	Designated adu	Dial-in (Object	Security	Environment	Sessions	
> Managed Service Account	B Domain Computers	Security Group	All workstation	Remote control	Remote D	Desktop Services	Profile COM+	Attribute Editor	
> Program Data	B Domain Controllers	Security Group	All domain con	General Add	dress Ad	ccount Prof	le Telephones	Delegation	
> System	B Domain Guests	Security Group	All domain que						
Users	B Domain Users	Security Group	All domain use	User logon name	e:				
> NTDS Quotas	Enterprise Admins	Security Group	Designated adu	uaa/win16-sach	iin.uaatesta	d.ge.com @u	aatestad.ge.com	~	
> I TPM Devices	Enterprise Key Admins	Security Group	Members of thi	User logon name	e (pre-Wind	lows 2000):			
	Enterprise Read-only Domain_	Security Group	Members of thi	UAATEST		profi	uaa		
	Saurd1	User							
	SeOpHubJreTrustStoreMana_	Security Group	Members in thi	Logon Hours	in L	.og On To			
	Scroup Policy Creator Owners	Security Group	Members in thi						
	Scoup1	Security Group		Unlock accou	unt				
	Scoup2	Security Group		_					
	Sroup3	Security Group		Account options:	ĸ				
	Guard2	User			change na	equeral at payt k	0000	^	
	Guard3	User			ot chance r	naeewoord	ogon		
	Suest .	User	Built-in account	Paenword	neuer expire	pasoworu			
	A HarishTest	User		Store pase	sword using	reversible encry	ntion		
	Key Admins	Security Group	Members of thi		onora aorig		provid	•	
	Se krbtat	User	Key Distributio	Account expire	95				
	A MainGroup	Security Group	,	Never					
	A Mark	User		O End of:	08	May 2022			
	AnrkUser	User							
	anasterwsymbol	User							
	AnaveenTest2	User							
	S profuaa	User			OK	Cancel	Apply	Help	
	Reprotected Users	Security Group	Members of this a	roup ar					
	RAS and IAS Servers	Security Group _	Servers in this arou	up can					
	Read-only Domain Controllers	Security Group	Members of this a	roup ar					
	Sachinfromuaatestad	User	and the second						
	A sachintestgroup	Security Group	urity Group _						
	A								

- 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

- 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 <i>(on page 78)</i> .			
keytab-location	Enter the location path where you copied the keytab file on this ma- chine.			

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**.

음 Loca	Cocal intranet ×						
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.							
Add th	is website to the zone:						
https:	//win16-phantomhost.uaatestad.ge.com	Add					
Websit	es:						
*.ad.s	ys ^	Remove					
*.alsto	om.com						
10.93	16.101						
10.93	16.149 ~						
Require server verification (https:) for all sites in this zone							
		Close					
		0.036					

- 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.
- \circ Include the Active Directory forest name in the URL. For example:
 - ldap://adl.forestplant.ge.com:3268/
 - ldap://ad2.forestcorp.ge.com:3268/

Security-Proficy Authenticat	ion X		DE	TAILS	
Identity Provider Group	s Users		FO	RESTPLANT Search	
Q Search		Ø + Ø		Field	Value
Identity Providers 1	Туре	Action	~	GENERAL	
FORESTCORP	ldap			Name	FORESTPLANT
FORESTPLANT	ldap	000		URL*	ldap://FORESTPLANT.FORESTPLANT.LOCAL:3268/
uaa	uaa			User DN	CN=PLANTUSER10,CN=Users,DC=FORESTPLANT,DC=LOCAL
				Origin Key	FORESTPLANT
			~	OTHER SEARCH CRI	TERIA
				Group Base	CN=Users,DC=FORESTPLANT,DC=LOCAL
				User Base	CN=Users,DC=FORESTPLANT,DC=LOCAL
				User Filter	sAMAccountName={0}
				Group Filter	member={0}
					-

ecurity-Proficy Authentica	stion $ imes$				DE	TAILS	
Identity Provider Grou	ups Users				FO	RESTCORP Search	
Q Search		Ø	+	0		Field	Value
Identity Providers †	Туре		Action	1	~	GENERAL	
FORESTCORP	ldap					Name	FORESTCORP
FORESTPLANT	ldap					URL*	Idap://FORESTCORP.FORESTCORP.LOCAL:3268/
uaa	uaa					User DN	CN=CorpUser6,CN=Users,DC=FORESTCORP,DC=LOCAL
						Origin Key	FORESTCORP
					~	OTHER SEARCH CRI	TERIA
						Group Base	DC=FORESTCORP,DC=LOCAL
						User Base	DC=FORESTCORP,DC=LOCAL
						User Filter	userPrincipalName=(0)
						Group Filter	member={0}
						May Films	2

- 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)*.

6. 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.

- 1. Log in to the virtual machine where you want to set up the iSCSI target 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	 a. Choose the option Select a server from the server pool. b. 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: a. Expand File and Storage Services > File and iSCSI Services . b. 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	 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: 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: a. In the features list box, select the check box for Failover Clus- tering .
	The Add features that are required for Failover Clustering? screen appears, which shows the dependencies that are in- stalled with this feature. 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.

🛴 Server Manager		– 🗆 X
€∋ - Server Ma	anager • Dashboard	
Dashboard	WELCOME TO SERVER MANAGER	Component Services Computer Management Defourment and Cotingin Delves
All Servers	1 Configure this local server	Detragreen and Opened Ones Disk Cleanup Event Viewer Tallover Cholor Manager
	WHATS NEW 2 Add roles and features 3 Add other servers to manage 4 Create a server group 5 Connect this server to cloud services	ISCSI Initiator Local Security Policy Microsoft Azure Services CORC Data Sources (I2-bit) ODBC Data Sources (I2-bit) Performance Monitor Print Management Recovery Drive
	LEARN MORE ROLES AND SERVER GROUPS Roles: 1 Server groups: 1 Servers total: 1 Image: File and Storage 1 Services 1	Registry Editor Resource Monitor Services System Enformation Lesk Scheckler Windows Defender Finwall with Advanced Security Windows Defender Finwall with Advanced Security Windows PowerShell Windows PowerShell Windows PowerShell (dift) Windows PowerShell (SE

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:

DNS nat	me of the t	arget and then dick	Quick Connect.	Quick Conne	ect	
Discover	red targets			0	ick Connect	
Name			Targets that a provided are is to each target Connections in to restore the	re available for conne sted below. If multiple t individually. nade here will be adde m will be made every	ction at the IP address or DN e targets are available, you r d to the list of Favorite Targe time this computer restarts.	IS name that need to conne ets and an at
			Discovered ta	rgets		
To comp dick Cor To comp then dic For targ	nect using a nnect. pletely disco di Disconne get properti	dvanced options, se onnect a target, sele ct. es, including configu	ign:1991-05	.com.microsoft.dc-tde	Status k1-target Conne	cted
select t	he target a	nd click Properties.	Progress repo	art		
For con the targ	figuration o get and the	f devices associated n click Devices.	Login Succes	eded.		
Cord Cord	nn 1005, 50			Connect	Done	

- 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 Loca-	The iSCSI target server and volume details are displayed.
tion	
iSCSI Virtual Disk Name	Enter a name for the virtual disk. For example, sharedDisk
iSCSI Virtual Disk Size	a. Enter the disk size. For example, 10gB. The disk size depends
	on your database utilization and number of users.
	b. Select Dynamically expanding.
iSCSI Target	Select New iSCSI target.
	If the target is new, then it should be assigned later as described in step 8.
Target Name and Access	Enter a name for the iSCSI target server. For example, hauaatarget
Access Servers	Add the iSCSI initiators (Node1 and Node2) and enable them to ac-
	cess the iSCSI virtual disk. Follow these steps to add the servers one
	at a time:
	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
	 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.
	d. Select OK to exit.
	e. To add Node2, repeat the above steps.
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.

Disk 1		
Basic	UaalSCSI (G:)	
24.28 GB	24.28 GB NTFS	
Online	Healthy (Primary Partition)	
10.00 GB	Online	
•	Properties	

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

Disk 1	
Basic 24.28 GB Online	UaalSCSI (G:) 24.28 GB NTFS Healthy (Primary Partition)
O Disk 2 Unknown	
Not Init	Offline
and co	Properties
DVD (C	Help

The Initialize Disk screen appears.

5. Select OK.

Initialize Disk	\times
You must initialize a disk before Logical Disk Manager can access it. Select disks: ✔ Disk 2	
Use the following partition style for the selected disks: O MBR (Master Boot Record) ③ GPT (GUID Partition Table)	
Note: The GPT partition style is not recognized by all previous versions of Windows.	

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

	-	New Simple Volume
Disk 1		New Spanned Volume
4.28 GB	24.28 GB NTES	New Striped Volume
Online	Healthy (Primary Partition)	New Mirrored Volume
		New RAID-5 Volume
Disk 2		Properties
asic		+ Help
nline	9.98 GB Unallocated	
CD-ROM 0	1	
VD (D:)		

The New Simple Volume Wizard screen appears.

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

You need to:

- \circ 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.

Section	What To Do
Before You Begin	Skip to the next section.
Select Servers or a Clus- ter	Browse and locate the servers you want to add to the cluster. Refer to Add Server Nodes for Validation <i>(on page 99)</i> .
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 valida-tion.
Summary	 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.

4. Complete Validate a Configuration Wizard with these options:

- 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 Adminis- tering the Cluster	Enter a unique name for your cluster. For example, hauaacluster
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.

Validate a Configu	ervers or a Cluster		×
Before You Begin Select Servers or a Cluster	To validate a set of server To test an existing cluster,	s, add the names of all the servers. add the name of the cluster or one of its nodes.	
Testing Options Confirmation Validating Summary	Enter name: Selected servers:		Browse
		< Previous	Next > Cancel

The **Select Computers** screen appears.

2. Select Advanced.

Select Computers	\times
Select this object type:	
Computers	Object Types
From this location:	
cluster.ge.com	Locations
Enter the object names to select (<u>examples</u>):	
1	Check Names
Advanced OK	Cancel

3. Select Find Now.

Select Comput	ers	×
Select this object	t type:	
Computers		Object Types
From this location	n:	
cluster.ge.com		Locations
Common Que	ries	
N <u>a</u> me:	Starts with ~	<u>C</u> olumns
Description:	Starts with ~	Find Now
Disabled a	occounts	Stop
Non expir	ng password	
Days since k	ist logon: v	//
		OK Canad
Search results:		Cancer
Name	In Folder	

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**.

Sele	lect Computers	×	
Sele	elect this object type: computers	Qbject Types	
Eve	om this location:		
du	Windows Security	×	
c	Enter network credentials		
	Enter your credentials for an account with permissions cluster.ge.com.	for ,	
	For example user, user@example.microsoft.com, or domain\user name		
	User name		
Sea	Password		
Nam	Domain: CLUSTER		
	OK Cancel		
	0 C		

After successful login, you can see the associated nodes.

5. Select UAAHANODE1 and UAAHANODE2, and select OK.

Select Computers		×
Select this object type:		
Computers		Object Types
From this location:		
cluster.ge.com		Locations
Common Queries		
Name: Starts wit	h ×	<u>C</u> olumns
Description: Starts with	h ~	Find Now
Disebled accounts	đ	Stop
Days since last logon:	×	%
Search resylts:		OK Cancel
Name	In Folder	^
RAVIKORRA10	cluster.ge.com/D	
Role1	cluster.ge.com/C	
SACHINAUTHQUAHD	duster.ge.com/C	
in our works	duster ge.com/C	
ueacluster	cluster.ge.com/C	
🔣 uaaconfig	cluster.ge.com/C	
UaaHaCluster	cluster.ge.com/C	
UAAHANODE1	duster ge com/C	
UANHANODE2	duster ge.com/C	*

6. Select OK to exit.

Select Computers			×
Select this object type:			
Computers		9	bject Types
From this location:			
cluster.ge.com			Locations
Enter the object names to select (examples):			
UAAHANODE1; UAAHANODE2]		ç	heck Names
Advanced	0	ĸ	Cancel

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.

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.

New Role Properties				×
General Failover				
New Role				
Name:				
Demo Role				
Preferred Owners				
Select the <u>preferred owners</u> for to list them in order from most at the bottom.	or this cluste preferred at	red role. Use th the top to least	e buttons preferred	
uaahanode1 uaahanode2			Up Down	
Priority: Medium	*			
Status: Running				
Node: uaahanode1				
	ОК	Cancel	Apply	

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	Enter a name. For example, hauaacluster
	Make a note of this name. You need to provide the fully qualified do- main name while installing Proficy Authentication. See step 3a in Configure Proficy Authentication Installation <i>(on page 107)</i> . For ex- ample, hauaacluster.cluster.ge.com wherein cluster.ge.com is the

Section	What To Do
	domain where cluster is installed. Make sure all the initiator nodes are in the same domain name.
Confirmation	The network name and IP address are displayed for confirmation. Note: After creating this resource, the IP address and the name should be added to the hosts file on the node servers configured for high availability.
Configure Client Access Point	Verifies the validity of the client access point settings and creates a new resource.
Summary	Select Finish.

Tallover Ouster Manager								- 0	×
Particle Cluster Manager Tailour Cluster Manager Tailour Cluster Manager Within Nodes Storage Storage Cluster Storage Cluster Events	Roles (1) Search Name Roles min	Satura Ramong	Tgan Other	Owner Node usafhanode1	Proty Neturi	P Queles ▼ Homaton	1 • •	Actions Roles Ry Configure Role, Vitual Machines, Conte Empty Role Vere	•
	v 🕞 Use nie Nare			Satur	Homator	Performed Churrens: 1) her.Setinas	Retroh Help Use role Sect Role	
	Reach R E GE Proficy Automication Tornost Web Server E GE Proficy Automication Policy/sGL Database Storage R E Duster Dek 1			 Onive Onive Onive 			0 6 8 9	Stop Role Add File Share Move Orange Startup Priority	;
<>	Server Name II P Name Name Name Name	ar 0.101.250.202		Onine Onine				Information Details Show Ortical Events Add Storage Add Resource	
	c Summary Resources						>	More Actions Kenove Proporties Help	

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.



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 GE Proficy Authentication Tomcat Web Service.					
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.

ar Cluster Manager	Roles (1)								Actions
UaaHaCluster.duster.ge.com	Search						🔎 Queries 🔻 📊	••	Roles
Nodes	Name	Status	Туре	Owner Node	Priority	Information		_	Ronfigure Role
Storage	Usa role	Running	Other	usahanode2	Medium				Virtual Machines
Cluster Events									Create Empty Role
									View
									G Refresh
									Help
	<							>	GE Proficy Authentication Postg
									🚰 Bring Online
	Vaa role						Preferred Owners: At	ty node	Take Offline
	Name			Status	Information			^	Information Details
	R			Online				- H	Show Critical Events
	UaalSC	SI (F)		0					More Actions
	NTES 2	4.1 GB free of 24.3 GB)					🗙 Remove
	Rolea								Properties
	B 🗟 GE Prokoy A	thentication Tomcat Web S	ever	Online					Help
	IP Addres	a: 10.181.251.217		Online					
	GE Proficy Authentication PostgreSQL Database			() Online					
	Server Name								
	B 🦉 Name: hauaacluster			Online					
	a P Address: 10.181.251.217			0.00					

The properties screen for that service appears.

c. Select the Dependencies tab, and select Insert.

GE Proficy Authentication PostgreSQL Database Properties $\qquad imes$								
Advanced Policies Registry Replication								
	General	Dependen	cies	Policies				
Spe be b	cify the resource brought online:	es that must be brough	nt online before	this resource can				
	AND/OR	Resource						
	Click here to a	dd a dependency						
No	dependencies.		Insert	Delete				
		OK	Cance	Apply				

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.
	Advanced F	Policies	Registry	Replication
	General	Dependencie	3	Policies
Spec be br	ify the resource rought online:	es that must be brought o	nline before	this resource can
	AND/OR	Resource		
		Cluster Disk 1		
AND		IP Address: 10.181.25	1.217	
•	AND	Name: hauaacluster		~
Clus	ter Disk 1 AND) IP Address: 10.181.251	Insert 217 AND N	Delete ame:

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:

- 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.
- 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 in 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.

Roles (1)						
Search						🔎 Queries 🔻
Name	Status	Туре	Owner Nod	e Priority	Information	
To Demo Role	(1) Running	Other	uaahanode	1 Medium		
<						
V Demo Role						Preferred Owner
Name			Status	Information		
Storage						
🗉 📇 Cluster Disk 1			Online			

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 hauaacluster.cluster.ge.com as the leading hostname, followed by any other hostname/s.

Broficy Authe	ntication 2022
Host Names	
To allow secure of host names (fully separated by cor	access to the hosted web applications, please provide qualified domain names and others) of this server, mma.
All Host Names:	hauaacluster.cluster.ge.com.g261gjl3e,localhost,127.0.0.1,ophub-host
Primary Host Name:	hauaacluster.cluster.ge.com
Notes:	
- The primary host name r	nust be resolvable on all client nodes.
- IP addresses may be ent	ered if you want users to be able to access web applications by IP address.
- Environment variables e	nclosed in percentage signs are allowed and must be evaluated to valid names.
 Entries are used to gene Authentication zones (and subdomains individually. 	rate a server certificate and to configure Proficy Authentication. If additional Proficy I hence subdomains) are to be created, use wildcard entries instead of listing
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

Broficy Authentication 2022	
Customize Log Files and	d Postgres Data Locations
Log Files Base Folder:	%ProgramData%\ProficyAuthenticationLogs
Proficy Authentication Database Folder:	F:\UaaConf
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.

📑 Registry Editor				
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\	WO	W6432Node\Apache	Software Foundation/	Procrun 2.0\UaaTomcat\Parameters
> COBC	^	Name	Type	Data
> DenSSH		et (Default)	REG_SZ	(value not set)
> 🧎 Partner		Environment	REG_MULTI_SZ	LOGIN_CONFIG_URL=WEB-INF/classes/required_co
> pgAdmin 4				
Policies				
> 🧎 Qualys		Edit Multi-Strin	a	×
RegisteredApplications				
> 3 Setup		Value name:		
> NWware, Inc.		Environment		
✓		Value data:		
Apache Software Foundation		LOGIN CONFI	G URL+WEB-INF/data	estequired configuration
V Procrun 2.0		UAA_CONFIG	FILE-C:ProgramDatal	GE Proficy Authentication
V UaaTomcat		TATA CONTROL	PATH-O ProgramData ISSNIDGDU LikoTSAU	CC Profey Astheniscation
V Parameters		SECRETS_DIP	C Pogar Data GEP	toficy Authentication/uaa-c
- 📕 Java				
- Log				
- Sart				
Stop				
Casses				× .
> Clients		<		>
> CrowdStrike				Of Created
> Google				Ch Canon
> A Intel				
> Microsoft				
2 A majs				
D D D D D D D D D D D D D D D D D D D				
Projets				
 Registered/ppications CNIA 				
A SVETEM				
> HKEY CURRENT CONFIG	~			
(-			

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\Proficy\Proficy Authentication\uaa-config

Image: Provide the second	View ogramData\GE\Proficy Authentication\usa	config		
1011	Name	Date modified	Туре	Size
Cuuck access Desktop * Downloads * Documents * Documents * Logs minikube_setup_uaa	 sec clients.yml.template uaa.yml uaa.yml.template 	10-01-2023 15:43 09-11-2022 10:58 11-01-2023 14:33 09-11-2022 11:14	File folder TEMPLATE File YML File TEMPLATE File	1 K8 54 K8 49 K8
Productinfo				

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

ile Home	Share	View			~
· → • ↑ 🖡	- GE :	Proficy Authentication > httpd > conf > cer	. v	ບ Search cert	
Quick access	^	Name	Date modified	Туре	Size
Desktop		localhost.ort	24-06-2022 18:59	Security Certificate	5 KB
Description	<u> </u>	localhost.key	24-06-2022 18:59	KEY File	4 K8
 Downloads 	1	a server.crt	24-06-2022 18:59	Security Certificate	5 KB
Documents	1	C second here	24-06-2022 18-59	KEY Ella	4 KB

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

🙀 GE Operations Hub Certificate Management Tool	-		×
Server Certificate External Trust Messages			
On this page, you can view and update the certificate chain used by the mai You can use a locally generated server certificate, or import one issued by a	in web serv third party.	er.	
Local Certificate			
View Renew			
Imported Certificate			
View Remove			
Certificate to Import			
Certificate File: C:\Users\Administrator\Desktop\server.pem	Select	View	
Key File: C:\Users\Administrator\Desktop\server.key	Select	Clear	
Password: (Only for PFX/P12 File)		Import]
You can import a certificate (chain) file in either PEM format or PFX/P12 form does not contain the private key, then you must provide a standalone key file	nat. If the o le in PEM fo	certificate f ormat.	file
O Use Local Certificate Use Imported Certificate		Apply	
		Close	

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.

💼 Certificate	\times
General Details Certification Path	
Certification path	
UAAHANODE2 Root CA 202206062043	
View Certificate	
Certificate status:	
This certificate is OK.	
OK	

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

💼 Certif cate			\times
General Details Certifica	tion Path		
Show: <al></al>	~		
Field Version Ser al number Signature algorithm Signature hash alg Valid from Valid from Subject Public key	Value V3 454c24e3fafe870e sha256RSA sha256 GE Customer, Oper 05 June 2022 05:30 05 June 2027 05:30 GE Customer, Oper RSA (4095 Bits)		*
	Edit Propert es	Copy to File	
		OK	

The Certificate Export Wizard appears.

7. Select Next.

Ş	Certificate Export Wizard
	Welcome to the Certificate Export Wizard
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
	To continue, click Next.
	Next Cancel

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

(rt File Format Certificates can be exported in a variety of file formats.
	Select the format you want to use:
_	ODER encoded binary X.509 (.CER)
	Base-64 encoded X.509 (.CER)
	Oryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	O Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Enable certificate privacy
	Microsoft Serialized Certificate Store (.SST)

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



10. Select Finish.

Certificate Export Wizard	
Completing the Certificate	Export Wizard
You have successfully completed the Certific	tate Export wizard.
You have specified the following settings:	
File Name Export Keys Include all certificates in the certification pa File Format	C:\Users\Administrator\Downloads\Uaa_(No ath No Base64 Encoded X.509 (*.cer)
<	>
	Finish Cancel

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

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

GE Operations Hub 2022.4	4.1	
Proficy Authentication	Service	
Configure a built-in or extern	al Proficy Authentication instar	ice
Use External Proficy Authentication:	2	
Proficy Authentication Base URL:	https://hauaacluster.cluster.ge.com/ua	Test
Admin Client ID:	ədmin	
Admin Client Secret:	•••••	
Proficy Authentication certificate file:	C:\Users\Administrator\Downloads\op	Browse View
Notes: Administrator of the Proficy Aul above. If you specify an issuer certifica the inputs before proceeding.	thentication service should provide you t ite above, view and confirm. Use the Test	he information button to validate
Cancel		Previous Next

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	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.	
	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.	
	Select $ imes$ to remove an existing image.	
Square Logo	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.	
	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.	
	Select $ imes$ to remove an existing image.	
Footer Legal Text	Use this space to enter any legal information.	
Footer Links	 To add hyperlinks, create a label and provide a URL to connect. a. Select + to add a row. b. Enter a label name. c. Enter a URL for the label name. Select to delete existing labels. 	

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.

% ଲି		? ◧▾ ◬▾
NAVIGATION \times	Custom labels-Proficy Authentication $~\times~$ Security-Proficy Aut $~\times~$	DETAILS
✓ ► Proficy Authentication	Company Name* GE	UAA Login Preview
Security		0.02
🕲 Custom labels	Company Logo* Allowed Image Extensions: .png, .jpg, .jpeg, I Maximum File Size Limit: 1 MB	GE Digital
	Select Im Image Available ×	Welcome!
	Square Logo	User Identifier
	Allowed Image Extensions: .png, .jpg, .jpeg. Maximum File Size Limit: 1 MB	Password
	Select Im	
	Footer Legal Text	SIGN IN
	copyright year	or sign in with:
		Okta
		copyright year This is a footer link
	Footer Links	
	Label* † URL* Action	
	This is a footer link https://www.ge.com/ 🔟	
	Reset Save	

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/Fold- er Name	Default Location	Target Folder
data-v13	C:\ProgramData\GE\Proficy Authenti- cation\uaa-postgres	PROFICY_AUTHENTICATION_BKP_YYYYM- MDD-HHMMSS\uaa-postgres
uaa.yml	C:\ProgramData\GE\Proficy Authenti- cation\uaa-config	PROFICY_AUTHENTICATION_BKP_YYYYM- MDD-HHMMSS\uaa-config
uaa-httpd.conf	C:\Program Files\GE\Proficy Authen- tication\httpd\conf\app-specific.d	PROFICY_AUTHENTICATION_BKP_YYYYM- MDD-HHMMSS\uaa-config
server.xml	C:\Program Files\GE\Proficy Authen- tication\uaa-tomcat\conf	PROFICY_AUTHENTICATION_BKP_YYYYM- MDD-HHMMSS\uaa-config
Certificate(if exist)	C:\ProgramData\GE\Proficy Authenti- cation\cert-manager\extraca\ldap SecAdminSrv	PROFICY_AUTHENTICATION_BKP_YYYYM- MDD-HHMMSS\uaa-config
keytab file(if exist)	C:\ProgramData\GE\Proficy Authenti- cation\uaa-config	PROFICY_AUTHENTICATION_BKP_YYYYM- MDD-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.psl 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

<pre>javax.servlet.ServletException: Servlet.init() for servlet [spring] threw exception org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92) org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.j org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769) org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIVvalve.java:289) org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:378 org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:350) org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:350) 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.jav org.apache.tomcat.util.net.NioEndpoint\$SocketProcessor.doRun(NioEndpoint.java:172 org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49) org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.ja org.apache.tomcat.util.threads.Thread\$WrappingRunnable.run(TaskThread.java:61 java.base/java.lang.Thread.run(Unknown Source)</pre>	:5 1v) 2) va av
Root Cause java.lang.IllegalStateException: Listeners cannot be added to context [/uaa] as the conte org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initializ org.springframework.web.servlet.FrameworkServlet.applyInitializers(FrameworkServl org.springframework.web.servlet.FrameworkServlet.configureAndRefreshWebApplication org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(Frame org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(Frame org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(Frame org.springframework.web.servlet.FrameworkServlet.initServletBean(FrameworkServlet org.springframework.web.servlet.FrameworkServlet.initServletBean(FrameworkServlet org.springframework.web.servlet.HttpServletBean.init(HttpServletBean.java:170) javax.servlet.GenericServlet.init(GenericServlet.java:158) org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java org.apache.catalina.valves.FrorReportValve.invoke(ErrorReportValve.java:92) org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769) org.apache.catalina.valves.rewite.RewiteValve.invoke(RewiteValve.java:269) org.apache.catalina.valves.rewite.RewiteValve.invoke(RewiteValve.java:289)	kt(et et ew ew or .j

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 Serve: × +
← → C A Not secure https://win16-sachin/uaa/?UseKerbAuth=true
III Apps 🕲 254 UAA LOGIN 🕲 OpHub 254 🕲 AutoLogin Uaa 254
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
<pre>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(RemiteValve.java:289) org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:378) org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56) org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:55) org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:357) org.apache.coyote.http11.Http11Processor.service(Ittp11Processor.java:382) 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.SocketProcessor.doRun(NioEndpoint.java:1722) org.apache.tomcat.util.httpads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:191) org.apache.tomcat.util.threads.ThreadPoolExecutor.vun(ThreadPoolExecutor.java:659) org.apache.tomcat.util.threads.ThreadPoolExecutor.SWorker.run(ThreadPoolExecutor.java:659) org.apache.tomcat.util.threads.ThreadPoolExecutorSWorker.run(TaskThread.java:61) java.base/java.lang.Thread.run(Unknown Source)</pre>
<pre>isoblecture 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.springframework.web.servlet.FrameworkServlet.applyInitializers(FrameworkServlet.java:764) org.springframework.web.servlet.FrameworkServlet.context(FrameworkServlet.java:764) org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(FrameworkServlet.java:781) org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(FrameworkServlet.java:786) org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(FrameworkServlet.java:781) org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(FrameworkServlet.java:780) org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(FrameworkServlet.java:591) org.springframework.web.servlet.FrameworkServlet.java:158) org.springframework.web.servlet.init(GenericServlet.java:158) org.apache.catalina.valves.FrorReportValve.java:158) org.apache.catalina.valves.FrorReportValve.invoke(ErrorReportValve.java:540) org.apache.catalina.valves.AbstractAccesslogValve.invoke(AbstractAccesslogValve.java:687) org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769) org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:376) org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIVValve.java:378) org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIVValve.java:378) org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIVValve.java:378) org.apache.catalina.valves.RemoteAddrValve.jivves(RemoteAddrValve.java:370)</pre>

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

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
[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)
<pre>[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</pre>

Note:

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

Useful SPN commands

To view existing SPNs	setspn -F -Q HTTP/ <fqdn></fqdn>
	Example: setspn -F -Q HTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM

	Command Prompt
	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!
To delete SPN	setspn -D HTTP/ <fqdn> <user account=""></user></fqdn>
	Example: setspn -D HTTP/phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM
	ghostl

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.

Step 1: Delete Any Oth- er SPN (if exists)	Run the command setspn -D HTTP/thenameyougavetothespn spnUserName Replace:					
	 thenameyougavetothespn with the SPN you want to unregister spnUserName with the user who created the SPN being un-registered. 					
	Select Command Prompt -					
Optional step: Verify Un-Registration	Run the command setspn -F -Q HTTP/thenameyougavetothespn*					
Step 2: Update Logon Name in Active Direc- tory	 Go to Active Directory. Open the properties of the existing spnUserName. 					

spnUserSrvAcctAutoLogin2 Properties ? × Organization Published Certificates Member Of Pessword Replication Dial-in Object Security Environment Sessions Remote control Remote Desktop Services Profile COM+ Attribute Editor General Address Account Profile Telephones Delegation User logon name: HTTP/useasutologin2 usatestad ge.com User logon name: User logon name: User logon name (pre-Windows 2000; Replace with UAATESTADOI Logon Hours Log On To User cannot change password at next logon Organization Published certificates Member Of Pessword Repl User logon name (pre-Windows 2000; SpnUserAutoLogin2 Logon Hours Log On To Unlock account Account options: Organization Published personnel at next logon Organization Published certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword Repl Dial-in Object Security Environment Sessions Remote control Remote Desktop Services Profile COM+ Attribute SpnUser/AutoLogin2 User logon name: UAATESTADOI SpnUser/AutoLogin2 User cannot change password at next logon Organization Published certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published Certificates Member Of Pessword at next logon Organization Published					,
Organization Published Certificates Member Of Pessword Replication Dial-in Object Security Envisionment Sessions Remote control Remote Desktop Services Profile COM+ Attribute Editor General Address Address Account HTTP/uaeautologin2 uaatestad ge.com Dial-in Object Security User logon name:	spnUserSrvAcctAutoLogin2 Properties	?	\times		
Ceneral Address Account Profile Telephones Delegation User logon name: HTTP/Laasudologn2_Laatestad.ge com User logon name (pre-Windows 2000; "Ceptace with UAATESTADO1 spnUserAutoLogin2 Logon Hours Log On To Uhick account user logon name (pre-Windows 2000); Uhick account user logon name (pre-Windows 2000); Ukart ESTADO1 spnUserAutoLogin2 User logon name (pre-Windows 2000); user logon name; Indication of the provide memory and	Organization Published Certificates M Dial-in Object Security Remote control Remote Desktop Service	Member Of Password R Environment S es Profile COM+ Attrib	Replication Sessions bute Editor	spnUserSrvAcctAutoLogin2 Prope	erties ?
User logon name: HTTP/usaautologin2 usatestad ge.com User logon name (pre-Windows 2000; Reface with UAATESTADO1 spnUserAutoLogin2 Lagon Hours Log On To User logon name (pre-Windows 2000): UAATESTADO1 User logon name (pre-Windows 2000): UAATESTADO1 User logon name: User logon name (pre-Windows 2000): UAATESTADO1 User logon name (pre-Windows 2000): User const thange password at next logon Ouser const thange password at next logon Ouser const thange password using reversible encryption Cocount expires Never End of: 16 December 2023	General Address Account Pro	ofile Telephones D	Delegation	Dial-in Object Sec	urity Environment Ses
HTP/baaautologin2 vaatestad ge Quaatestad ge com User logon name (pre-Windows 2000 Profile Telephones Dale UAATESTAD0 spnUserAutoLogin2 Logon Hours Log On To Unlock account Quaatestad ge.com User logon name (pre-Windows 2000): Quaatestad ge.com User cannot change password Logon Hours Log On To Account express Store password at next logon Quaatestad ge.com Store password using reversible encryption Varcount change password Quaatestad ge.com Varcount express Never Store password at next logon Quaatestad ge.com On for intep	User logon name:	1 N 24		Remote control Remote Desktop	Services Profile COM+ Attribute
User logon name (pre-Windows 2000): tebsde win UAATESTADO. ppnUserAutoLogin2 Logon Hours Log On To Unlock account Unlock account Account options: User must change password at next logon Password never expires Store password using reversible encryption Account expires Never End of: 16 December 2023	HTTP/uaaautologin2.uaatestad.ge.c @u	uaatestad.ge.com	~	General Address Account	Profile Telephones Dele
UNAR Est ALLOR spinUserAutoLogin2 Logon Hours Log On To Unlock account User logon name (pre-Windows 2000): UATESTADO spilUserAutoLogin2 Logon Hours Log On To Unlock account User must change password at next logon User cannot change password User sound express Store password using reversible encryption User must change password Account express User must change password Never User cannot change password End of: 16 December 2023	User logon name (pre-Windows 2000) Kepla	lace with		User logon name:	
Logon Hours Log On To User logon name (pre-Windows 2000): UATESTADON Account options: User cannot change password at next logon User saword never exples User annot change password at next logon Store password using reversible encryption User cannot change password at next logon Account exples User annot change password at next logon Never Desmote cannot change password at next logon End of: 16 December 2023	Sph	nOserAutoLogin2	>	spnUserAutoLogin2	@uaatestad.ge.com
UNIdok account Image password at next logon Account options: Unidok account User must change password at next logon Image password at next logon Password never expires User must change password at next logon Store password using reversible encryption User must change password at next logon Veser cannot change password Image password at next logon Store password using reversible encryption User must change password at next logon Veser cannot change password Password never expires Store password using reversible encryption Password never expires Never 16 December 2023	Logon Hours Log On To			User logon name (pre-Windows 20	00):
 User must change password at next logon User cannot change password Password never expires Nover End of: 16 December 2023 User cannot change password at next logon User cannot change password Password never expires Store password using reversible encryption 	Unlock account			Logon Hours Log On	spnUserAutoLogin2
 ✓ User cannot change password ✓ Password never expires Store password using revensible encryption ✓ Account expires ← Never ← End of: 16 December 2023 ✓ Count expires ● Never <	User must change password at next	logon	^	Unlock account	
Password never expires Store password using reversible encryption Account expires Never Child of: 16 December 2023 Child of: 16 December 2023 Child of: 16 December 2023	✓ User cannot change password			Account options:	
Store password using reversible encryption Image: Store password using reversible encryption Account expires Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption Image: Store password using reversible encryption	Password never expires				at payt legan
Account expires Account expires Account expires Account expires Account expires Store password using reversible encryption Account expires Account expires Brud of: 16 December 2023 Frud of: 16 December	Store password using reversible encry	ryption	~	User cannot change password	rd
Never If December 2023 Account expires Never Dend of: 16 December 2023	Account expires			Password never expires	
○ End of: 16 December 2023 □ - Account expires ④ Never ○ End of: 16 December 2023 □ -	Never			Store password using reversit	ble encryption
(e) Never (c) End of: 16 December 2023	O End of: 16 December 2023		3-	Account expires	
				Never End of: 16 Decembe	r 2023 🔲-

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:

Update HTTPD Configu-	1. Visit the location C:\Program Files\GE\Proficy Authentication\httpd			
ration File	\conf\app-specific.d\uaa-httpd.conf and open uaa-httpd.conf in a			
	text editor.			
	2. Add the following code:			
	#SPNEGO authentication HTTP request header size			
	LimitRequestFieldSize 16384			
	3. Save and close the httpd configuration file.			



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 'multidomain 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 Usecase: 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.