

Proficy Authentication 2023 User Guide



Proprietary Notice

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

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

© 2023, General Electric Company. All rights reserved.

Trademark Notices

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

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

All other trademarks are the property of their respective owners.

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

doc@ge.com

Proficy Authentication

Contents

Chapter 1. Proficy Authentication	4
About Proficy Authentication	4
Set up Proficy Authentication	4
Application Overview	10
Manage Identity Providers	12
Add LDAP Identity Provider	12
Enable SAML	15
Add SAML Identity Provider	26
Enable Multi-Factor Authentication	
Modify LDAP Identity Provider	31
Modify SAML Identity Provider	34
Delete Identity Provider	
Manage Groups	35
Overview of iFIX Groups in Proficy Authentication	
Overview of Historian Groups in Proficy Authentication	36
Create Groups	
Modify Groups	
Map Groups	39
Add/Remove Users in a Group	42
Add/Remove Sub-Groups in a Group	43
Delete Group	44
Manage Users	45
Create Users	45
Create Users Add/Remove Groups for a User	45 47
Create Users Add/Remove Groups for a User Reset User Password	45 47 49
Create Users Add/Remove Groups for a User Reset User Password Delete User	45 47 49 50

Con	figure Security Policy	54
Crea	ate Service Principal Name	56
Gen	erate Keytab File	59
Prof	ficy Authentication Service Configuration	62
Con	figure Browser	63
Trou	ubleshooting Error Logs	64
High Ava	ailability	70
Con	figure High Availability for Proficy Authentication	70
Con	figure iSCSI Target	71
Con	figure iSCSI Initiator	72
Crea	ate a Virtual Disk	74
Initia	alize a Virtual Disk	76
Crea	ate a Cluster	78
Con	figure Role	82
Con	figure Proficy Authentication Installation	87
Prer	requisites for Installing Operations Hub with External Proficy Authentication	92
Customi	ze Login Screen	97

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. You can configure Proficy Authentication from Configuration Hub.

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

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

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

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

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.

Configuration Hub Login	Ø,
Authentication Source not configured Click setup below to configure	
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: confighubadmin
Client Secret	The client secret provided during installing Con- figuration Hub.

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

4. Select Verify.

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

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

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

Field	Description
Server Name (Fully Qualified Name)	The host name of the machine where Proficy Authentication is installed. Enter a fully qualified domain name. For exam- ple, 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 443.
	The server connection is automatically tested on entering the port. You can also select Test to test the connection.
Use Configuration Hub Administration creden- tials for Proficy Authentication	Select this check box to populate the same lo- gin credentails you entered for Configuration Hub Admin account.
	If you want to use unique login credentials for Proficy Authentication, clear the check box and enter CLIENT ID and CLIENT SECRET .
Proficy Authentication Client ID	The administrator client identifier that has per- mission (authority) to log in to Proficy Authenti- cation.
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
lssuer	CN=SACHINAUTHGUARD Root CA 202112241544, OU=Operations Hub Site,
	O=GE Customer
Valid From	2021-12-24 00:00:00 GMT
Valid To	2026-12-23 00:00:00 GMT

7. Select Trust.

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

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 Authenti- cation.

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

Application Overview

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

You can perform the following tasks in Proficy Authentication:

- Configure UAA/LDAP/SAML identity providers
- Create new user accounts
- · Create new group accounts and add users/other groups as members
- Perform UAA/LDAP/SAML group mapping

Displaying Data Columns

You can show or hide columns within the Proficy Authentication application.

- 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.

Sorting Data

The sorting option appears when you select a data column.

- Select 1 to sort data in an ascending order.
- Select ↓ to sort data in a descending order.

Filtering Data

The filtering option appears next to each data column.

- 1. Select 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.

Searching Data

Use the search option to search for existing accounts in Proficy Authentication. You can also filter account details using search keywords.

Manage Identity Providers

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.

curity-Proficy Authentication \propto			
dentity Provider Groups Users			
Q Search		+ 50	53
Identity Providers †	Туре	Action	11.
Okta Login Station	saml		-
1122	uaa		_

The LDAP Identity Provider screen appears.

3. Enter the following details:

Field	Description
Name	A unique name to help identify your LDAP con- nection.
URL	The URL of the LDAP server. The trailing slash (/) must be included at the end of the URL.
	thentication in the following format: • Insecure port:
	ldap://100.100.100.2:389/ • Secure port: ldaps://100.100.100.2:636/
	You can also use a fully qualified domain name instead of an IP address.

Field	Description
	For a secure port, provide user credentials.
Bind User Distinguished Name	Distinguished LDAP user name.
	Describes the part of the hierarchy the user belongs to on the active directory network.
	CN=Common Name. DC=Domain Component. OU= Organization Unit Name.
	CN and DC are typically required, while OU is optional.
	Example: CN=John Smith,OU=Factory,DC=Compa- ny,DC=COM
Password	The password to log in to the LDAP server if you choose secure authentication.
Test	Tests the connection to the LDAP server. If the URL and login details are correct, you will re- ceive 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 estab- lishing a secure connection between client and server for exchanging LDAP data.
	Clear the check box to allow SSL verification. Refer to step 4.

LDAP Identity Provider		
Name* DSFREE50KFORUM		
URL*		
ldap://10.181.215.2:389/		_
Bind User Distinguished Name *		
CN=spcuser1,CN=Users,DC=pa,DC=com		
Password *		
		8
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.

Certificate cannot be retrieved Please use the browse button below	to select the sen	ver certificat	e
Browse			
			Close
			Close

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

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

The LDAP identity provider is created.

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 26)* 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 26)* 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 16)
- Configure Azure AD as SAML IDP (on page 22)

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.

Create App Integration	Browse Ap	o Catalog	
			Assign Users to App More V
Q Search			
STATUS		0	Okta Admin Console
ACTIVE	0		
INACTIVE	0	3	Okta Browser Plugin
ACTIVE	0	0	Okta Browser Plugin

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 [2	0	OIDC - OpenID Connect Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
	0	SAML 2.0 XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
	0	SWA - Secure Web Authentication Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
	0	API Services Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.
		Cancel Next

The Create SAML Integration screen appears.

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

1 General Settings	2 Configure SAML
1 General Settings	
App name	Multiverse Paradigm
App logo (optional)	E Contraction of the second se
App visibility	 Do not display application icon to users
Cancel	Next

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

Single sign on URL	Use the dowloaded Proficy Authentication
	metadata me (on page 15) sami-sp.xml to
	get the URL for this field. It should look some-
	thing like this:
	<pre><md:assertionconsumerservice Location = https://ghildz593e.logon.ds.ge.com/uaa/saml/SSO/alias/ophubSamlSp* Binding="urn:oasis:names:tc:SAML:2.0.bindings:HTTP-POST" isDefault="true" index="0"/> <md:assertionconsumerservice Location="https://ghildz593e.logon.ds.ge.com/uaa/oauth/token/alias/ophubSamlSp* Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI" index="1"/></md:assertionconsumerservice </md:assertionconsumerservice </pre>
Audience URI (SP Entity ID)	Refer to saml-sp.xml to get the logout URL. It
	should look something like this:
	<pre><?xml version="1.0" encoding="UTF-8">> - <md:entitydescriptor entityid="https://ghidz593e.logon.ds.ge.com/uaa/saml/metadata" id="https://ghidz593e.logon.ds.ge.com_uaa_saml_metadata" xmlns:md="urn:coasis:names:tc:SAML:2.0::metadata"></md:entitydescriptor></pre>
Enable Single Logout	a. Select Show Advanced Settings.
	b. Select the check box for Allow applica-
	tion to initiate Single Logout.

	c. Enter Single Logout URL . Refer to sp.xml to get the logout URL. It s look something like this: (md:keybecryter (md:keybecryter) (md:keyb	O saml – :hould allas/ophubSamlSp ⁻
Attribute Statements (optional)	Add user attribute statements such as first name, and last name as shown her	email, re:
	Name Name format (optional) Value email Unspecified * user.email first name Unspecified * user.firstName last name Unspecified * user.lastName Add Another Add Another Item (Content of the content o	• • × • ×
Group Attribute Statements (optional)	Add group attribute statements such as and groupB as shown here: Group Attribute Statements (optional) Name Name format Filter (optional) groupA Unspecified * Contains * manager groupB Unspecified * Contains * operator Add Another	s groupA

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	
Once you have a working SAML integration, submit it for Okta review	to publish in the OAN.
General Sign On Import Assignments	
Settings	Edit
Sign on methods	
The sign-on method determines how a user signs into and manages their creater application. Some sign-on methods require additional configuration in the 3 rd Application username is determined by the user profile mapping. Configure	edentials for an ^d party application. profile mapping
SAML 2.0	
Default Relay State	
SAML 2.0 is not configured until you complete the setup instruct	ions.
View Setup Instructions Identity Provider metadata is available if this application supports	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 26)* 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 SAML configuration with Azure AD (Active Directory).

- 1. Visit https://azure.microsoft.com/en-us/free/ and create an account.
- 2. Add an enterprise application. For more information, refer to Microsoft Azure documentation. Ops Hub Dev is the example enterprise application used in the procedural steps (refer to the figure in step 2).
- 3. Create at least one user and group.

The following steps include:

- Creating a SAML app in Azure (steps 1-5).
- Configuring Azure metadata xml in Proficy Authentication (steps 6-7).
- 1. Download Proficy Authentication sam1-sp.xml metadata file. Refer to Enable SAML (on page 15) on how to download the file.
- 2. Sign in to the Azure portal, and upload saml-sp.xml.
 - a. From left menu, select Manage > Single sign-on.
 - b. Select Upload metadata file.

				/			
 Dashboard > Ops Hub Dev > Ops Hub Dev SAML Entryrise Application Overview Deployment Plan Manage Properties Ouners Roles and administrators Users and groups 	-based « T u Set u An SSO implemmore. Read 1	Desced Sign-on Change single sign-on mode Test this application Confeedbackt Set up Single Sign-On with SAML An 550 implement. Choose SAM, single sign-on whenever possible for existing applications that do not use OpenID Connect or more. Read the configuration guide of for help integrating Ops Hub Dev. Basic SAML Configuration					
 Single sign-on Provisioning Application proxy Self-service Custom security attributes (preview) 	0	Attributes & Claims	https://www.www.ami/SSO/aka/k phu5amtip Optionof Optionof Https://www.ami/SSO/aka/k https://www.ami/SingleLogo ut/aka/ophubSamtSp				
Security Conditional Access A Permissions Token encryption Activity	0	givenname sumame emailaddress name Unique User Identifier	user.givenname user.sumame user.mail user.userprincipalname user.userprincipalname	2 tot			
	Ops Hub Dev SAML Interview Application Conversion Properties Convers Convers Convers Convers Convers Convers Convers Conver	Ops Hub Dev SAML-based Interprise Application III: Overview III: Single sign-on III: Provisioning III: Application proxy III: Security III: Conditional Access III: Previsions III: Token encryption Activity III: Sign-in logs	Ops Hub Dev SAML-based Sign-on Interprise Application Image Image	Ops Hub Dev SAML-based Sign-on Interprise Application Interprise Application prove Interpr			

3. Perform user and group attribute mapping in Azure.

- Attributes & Claims
 Edit

 givenname
 user.givenname

 surname
 user.surname

 emailaddress
 user.mail

 name
 user.userprincipalname

 Unique User Identifier
 user.groups
- a. Under the User Attributes & Claims section, select Edit and add claims.

b. Select Add new claim and save entered details to set up claims.

Dashboard > paintcorp > Enterprise applications > Ops Hub De	ev > SAML-based Sign-on >	
Attributes & Claims		
+ Add new claim + Add a group claim III Columns 🖉	Got feedback?	
Required claim		
Claim name	Value	
Unique User Identifier (Name ID)	user.userprincipalname [nameid-formatemailAddress]	
Additional claims		
Claim name	Value	
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups [SecurityGroup]	••••
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd	user.mail	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.sumame	

Note:

Make a note of the claim name value (for example user.groups). You need to provide this value in the **Attribute Name** field when adding a SAML identity provider in step 6a *(on page 25)*.

c. Select Add a group claim and set up group claims.

Dashboard > mintorp > Enterprise applications > Ops Hub D Attributes & Claims	ev > SAML-based Sign-on >		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 🖗	Got feedback?		This page includes previews available for your evaluation in the 'Advanced options' section.	
Required claim Claim name Unique User Identifier (Name ID) Additional claims	Value user.userprincipalname (nameid-form	natiemailAddress] ••••	Which groups associated with the user should be returned in the claim? None All groups Security groups Directory roles	
Claim name	Value		Groups assigned to the application	
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.groups [SecurityGroup] user.mail user.givenname user.userprincipalname user.surname		Source attribute * Group ID V Advanced options	~

4. Under the SAML Signing Certificate section, download the Federation Metadata XML file.

Activity		
Sign-in logs	SAML Signing Certificate	0 tot
Usage & insights Audit logs Provisioning logs Access reviews	Status Thumbprint Expiration Notification Email App Federation Metadata Url Certificate (Base64)	Active 53C100005 00000000000000000000000000000000
	Federation Metadata XML	Download
	Set up Ops Hub Dev You'll need to configure the applicatio	in to link with Azure AD.
	Login URL	https://ogin.microsoftonline.com/bit/s504-6442_
	Azure AD Identifier	https://stb.windows.net/b344736_6442-4/5a-9622_
	Looper Life	have the international states of the state of the

5. Perform user group mapping in Azure.

DEVELOPERGROUP1 Group	Members			
	< + Add members 🗙 Remove 💆 Refred	h 🗋 Bulk operations 🗸 💷 Columns 🕂 Got !	wdbadk?	
Overview				
X Diagnose and solve problems	Some groups can't be managed in the Azure po	ortel: Learn where to manape these, provide C		
Manage	Direct members All members			
T Properties				
Members	P Search by name	Add filters		
A Owners	Name	T; Type	(mail	User type
Roles and administrators	🗆 😹 Settiner	User	Testürsen@idomain.ge.com	Member
Administrative units	🗌 🚾 Viter'i LastName	User	Voerbillmicrosoft.com	Member
Group memberships	E Konthame Voer2	User	Use/3@domain.ge.com	Member
Applications	- two -	User	User Olympical com	Member
🔓 Licenses				
Azure role assignments				
Activity				
E Access reviews				
Audit logs				
👃 Bulk operation results				
Troubleshooting + Support				
New support request				

- 6. Log in to Proficy Authentication and do the following:
 - a. Upload the **Federation Metadata XML** file downloaded from the Azure portal in step 4 (on page 24).

For step-by-step instructions, refer to Add SAML Identity Provider (on page 26).

b. Add and map SAML groups.

For step-by-step instructions, refer to Map Groups (on page 39).

7. To test SAML authentication, visit Operations Hub login page, and select Sign In With Azure.



 You should login successfully. In Azure portal, you can access the logs to verify successful logins:

Test User1	Sign-	in logs 👒	-												2
	< ± 0	writed 🖂 🔘 (Export D	lata Settings 🕺 Tros	biesh	oot 🕐 Refresh 🕴 🛙	Co	umns 🔗 Got feed	fback?						
K Diagnose and solve problems Manage	0	fart to switch back t	to the de	elauit sign-ins asperiencel	Cirk	here to leave the preview.	•								
👗 Inolie	Det	Last 24 hours	(p	how dates as Local	ų	ser contains 14		and the part of th	P.	Trans Add filters					
 Custom security attributes (preview) 	User	ign-ins (Interactiv	ve) (User sign-ins (non-inte	nich	4)									
Assigned roles	Date		÷.,	Request ID	τ_{k}	User	τ_k	Application	τ_{\pm}	Status	IP address	τ_k	Location	Conditional Access	Authentication require
Administrative units	5/4/	1022, 7:54:40 AM		2053530-c711-4o4c-8e	ų	Test User1		Ops Hub Dev		Success	0.0.0.0		USA	Success	Single-factor authentication

 If login access is denied, then verify the group attribute name and group name from SAML Azure (see troubleshooting below). Clear the cache and login again.

Troubleshooting: For troubleshooting, add SAML-tracer extension to Chrome.

- 1. Open SAML-tracer from your browser extensions.
- 2. Log in to Operations Hub to reproduce the SSO login issue.
- 3. In SAML-tracer, look for POST messages, and select the Summary tab.

In the following screenshot, incorrect SAML group attribute names were detected, and replaced with the correct ones to fix the login issue.

-SK SAN	1L-tracer	
×Clear	Il Pause ± Autoscroll ♥ Filter resources O Colorize & Export &	Import
POST POST GET POST	https://login.microsoftonline.com/b5da5f35-6442-4f5a-9622-92ec6a53512 https://login.wicrosoft.com/OneCollector/1.0/?cors=true&c https://login.microsoftonline.com/Kmsi	17/login ontent-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.uk.p.enc.corp/uaa/oauth/authorize?client_id=kp-dev https://www.uk.p.enc.corp/kp/ https://www.uk.p.enc.corp/kp/ https://www.uk.p.enc.corp/kp/ https://www.uk.p.enc.corp/kp/ https://www.uk.p.enc.corp/kp/st/st/ontige_fonts/Primary-Font- https://www.uk.p.enc.corp/kp/st/st/ontige_fonts/Primary-Font- https://www.uk.p.enc.corp/kp/st/st/ontige_fonts/Primary-Font- https://www.uk.p.enc.corp/kp/st/st/st/ontige_fonts/Primary-Font- https://www.uk.p.enc.corp/kp/st/st/st/st/st/st/st/st/st/st/st/st/st/	Gredrect_uri=https://www.computetogin&response_type=code&state=evj/www. h Inspira-Sans/GEInspiraSans-Regular-v02.ttf
HTTP	Parameters SAML Summary	
http:/ http:/ http:/ http:/ http:/ http:/ http:/ http:/ http:/ http:/	Schemas.microsoft.com/identity/claims/objectidentifier /schemas.microsoft.com/identity/claims/displayname /schemas.microsoft.com/iss/2008/06/identity/claims/groups /schemas.microsoft.com/iss/2008/06/identity/claims/groups /schemas.microsoft.com/iss/2008/06/identity/claims/groups /schemas.microsoft.com/iss/2008/06/identity/claims/groups /schemas.microsoft.com/iss/2008/06/identity/claims/groups /schemas.microsoft.com/iss/2008/06/identity/claims/groups /schemas.microsoft.com/iss/2008/06/identity/claims/groups /schemas.microsoft.com/iss/2008/06/identity/claims/groups /schemas.microsoft.com/identity/claims/groups /schemas.microsoft.com/identity/claims/groups	10770936CTLCTL0975-ferrormed14 Kengen A Teeters Figures ContractorGroups AT grees Compared Contractors Compared Contractors Compared Contractors HPTLTENES https://sts.windows.net/b5d85f35-6442-4f5a-9622-92ec68355127/ bttp://stbms.windows.net/b5d85f35-6442-4f5a-9622-92ec68355127/ bttp://stbms.windows.net/b5d85f35-6442-4f5a-9622-92ec68355127/ bttp://stbms.windows.net/b5d85f35-6442-4f5a-9622-92ec68355127/ bttp://stbms.windows.net/b5d85f35-6442-4f5a-9622-92ec68355127/
http://	<pre>>scenes.macrosoft.com/claims/autnimethoosrefefences /schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname /schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</pre>	<pre>nccp://schemes.microsoft.com/ws/2000/06/loentity/authenticationMethod/password ** Kenedit Teeters</pre>

Add SAML Identity Provider

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

Enable a SAML identity provider (on page 15). 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 \propto			
Identity Provider Groups Users			
Q Search			+ 🖏
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 16).

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. Enter the URL in the text field, and select Load . The data from the URL appears in a text box,
Name	and is read-only. 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.

OIE: All fields are mai	ndatory		
) Upload XML File	Provide File Location		
https://dev-38020232	2.okta.com/app/exk2uugkc5PUxlfaa5d7	7/sso/saml/meta	Load
xml version="1.0" e<br entityID="http://www umbound="urpoposic	ncoding="UTF-8"?> <md:entitydescript .okta.com/exk2uugkc5PUxlfaa5d7"</md:entitydescript 	OF	*
lame* okta_123			
lame* okta_123 ttribute Name*			
lame* okta_123 ttribute Name* email			
lame* okta_123 ttribute Name* email lame ID*			
lame* okta_123 ttribute Name* email lame ID* urn:oasis:names:tc:SA	ML:1.1:nameid-format:emailAddress		× •

5. Select Save.

The SAML identity provider is created.

Enable Multi-Factor Authentication

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

Install the Google Authenticator app on your mobile device.

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

Note:

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

- 1. Log in to Configuration Hub as an administrator.
- 2. Go to Proficy Authentication > Security > Identity Provider.

The existing list of identity providers appear.

3. Select the UAA record for which you want to enable the multi-factor authentication.

The option to enable MFA appears on the **DETAILS** panel under the **MFA** section.

4. Enable the toggle switch for MFA.

By default, MFA is disabled.

	FIELD	VALUE
~	ADMINISTRATOR	CREDENTIALS
	Client ID	admin
~	GENERAL	
	URL	https://deskto
/	MFA	
	Disabled	O.D.
	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.

Modify LDAP Identity Provider

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

Add LDAP Identity Provider (on page 12)

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

DE	TAILS	×
CV	VARIRSSVR2K19	
Q	Search	
	Field	Value
~	GENERAL	(ľ
	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 grou	
	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.		
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.		
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.		
Group Filter	member={0}	Retrieves the memberof attribute values for the specific user. This is field is populated by default.		

Search Criteria	Example Value	Description	
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.	

Modify SAML Identity Provider

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

Add SAML Identity Provider (on page 26)

- 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 display the details in a pop-up screen.

DETAILS			\times		
Ok	Okta Login Station				
Q	λ 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.

Delete Identity Provider

This topic describes how to delete identity providers.
Add SAML Identity Provider (on page 26)

- 1. Log in to Configuration Hub as an administrator.
- 2. Go to Proficy Authentication > Security > Identity Provider.

The existing list of identity providers appear.

3. Select the identity provider you want to delete.

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

4. Select **Doo**, then **Delete**.

Security-Proficy Authentication	×	DE
Identity Provider Groups	Users	O
		م
Q Search		+ 🐵
Identity Providers 1	Туре 🝸	Action
Okta Login Station	saml	ose Man Groupe
uaa	uaa	Poloto
		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 iFIX Groups in Proficy Authentication

Proficy Authentication provides access to the following security groups for iFIX access:

scada.fix_shared_IFIX_PROFICY_AUTH_ADMIN,scada.fix.shared.APPLICATION_DESIGNER,

scada.fix.shared.OPERATORS, scada.fix.shared.SUPERVISORS, **and** scada.proficy.admin.

The following descriptions explain the access provided for iFIX groups in Proficy Authentication.

• scada.fix_shared_IFIX_PROFICY_AUTH_ADMIN: This group allows access to all iFIX application features. Any Proficy Authentication user who is a member of this group will have privileges similar to a native iFIX ADMIN user (except the access to security areas). Proficy Authentication users who want to directly log in to iFIX can use this group.

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: This group allows a user to access Configuration Hub and provides use of iFIX features such as iFIX connection, database, and model management.

Important:

Be aware that the scada.fix.shared.APPLICATION_DESIGNER group 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 Manager
- Database Reload
- Database Save
- Security Configuration
- System Configuration

To create a new group or modify an existing group, use the iFIX Security Configuration application.

- scada.fix.shared.OPERATORS: This group provides run mode only access for a user in iFIX.
- scada.fix.shared.SUPERVISORS: This group provides 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: This group allows the Proficy Authentication user access to the iFIX Projects panel and to the Deploy operations from Configuration Hub. This group is for Proficy Authentication only; this group is not linked to any iFIX group and has no permissions in iFIX.

Overview of Historian Groups in Proficy Authentication

Proficy Authentication provides access to the following security groups for Historian access:

historian_enterprise.admin, historian_enterprise.user,historian_rest_api.admin,

historian_rest_api.read, historian_rest_api.write, historian_visualization.admin,

historian_visualization.user, ih_archive_admins, ih_audited_writers, ih_collector_admins, ih_readers, ih_security_admins, ih_tag_admins, ih_unaudited_logins, **and** ih_unaudited_writers.

The following descriptions explain the access provided for Historian groups in Proficy Authentication:

- historian_enterprise.admin: Provides read/write access to Configuration Hub APIs.
- historian_enterprise.user: Allows access to Configuration Hub APIs.
- historian_rest_api.admin: Provides read/write access to public REST API.
- historian_rest_api.read: Provides read access to public REST API.

- historian_rest_api.write: Provides write access to public REST API.
- historian_visualization.admin: Provides access to Trend Client and the Web Admin console.
- historian_visualization.user: Allows access to Trend Client.
- ih_archive_admins, ih_audited_writers, ih_collector_admins, ih_readers, ih_security_admins, ih_tag_admins, ih_unaudited_logins, ih_unaudited_writers: Provides access to tables for the Historian OLE DB provider.

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 +

curity-Proficy Authentication $~~ imes~~ imes~~ imes~$		
Identity Provider Groups Users		
Q Search		+®
Group Name T	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, <pre>supervisors_LineA</pre>

Field	Description
Description	A brief description of the group.

Add Group		
Group Name* Supervisors_LineA		
Description		
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 42)
- Add/Remove Sub-Groups in a Group (on page 43)
- Map Groups (on page 39)
- 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 **200**, then **Edit**.

The group opens in a new tab.

Security-Proficy Aut 🗙 confighub.acc	ess-Proficy Authentication $- imes$			
Group				
confighub.access	•			
Member(Users) Mapping Member(O	Groups)			
O. Guart				~
Q Search			+	<u>{</u> 0}
User Name † 🝸	Origin T	Emails T		
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 42)</i> .
Mapping	Displays the list of mapped groups for this group. You can add/ remove mapped groups <i>(on page 39)</i> .
Member (Groups)	Displays the list of sub-groups added to this group. Add/Re- move Sub-Groups in a Group <i>(on page 43)</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	
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 \overline{V} .

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=*)		Y			
Groups					Mapped Gro	pups
	DN					DN
	CN=HelpLibra	ryUpdaters,CN=User	s,DC=p			CN=SQLServer2005SQLBrowserUser\$C
 Image: A start of the start of	CN=WSS_ADM	MIN_WPG,CN=Users,[DC=pa,	←		CN=SQLServerMSASUser\$CWARIRSSVR2
\checkmark	CN=Administr	rators,CN=Builtin,DC=	pa,DC			CN=WSS_WPG,CN=Users,DC=pa,DC=com
	CN=Guests,CI	N=Builtin,DC=pa,DC=	com	\rightarrow		CN=Users,CN=Builtin,DC=pa,DC=com
	CN=Print Ope	rators,CN=Builtin,DC	=pa,DC			
	CN=Backup O	perators,CN=Builtin,[DC=pa,			
	CN=Replicato	r,CN=Builtin,DC=pa,D	C=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**.

Group	
cloud_controller.admin 👻	
Member(Users) Mapping Member(Groups)	
Identity Provider	
Okta Login Station 👻	
Add SAML Group	
	+
Groups	Mapped Groups
Group Name	Group Name
✓ corp_group	secure_sys_group
✓ action_group	←
cloud_group	
	\rightarrow

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 38) 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 1	
\checkmark	ch_admin	
~	kal_el	
	mandrake_01	
\checkmark	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 38) 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				
∽ search				
	GROUPNAME T			
	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 **Doo**, then **Delete**.

Identity Provide Groups Jsers		
Q Search		+ 🐵
Group Name	Members	T Action
clients.admin	0	
clients.read	1	000
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 Authentica- tion.
Password	The password to log in to Proficy Authentica- tion.
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

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.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 client secret.		
password.write This admin scope enables to change password.		
	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 47).

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 45)

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

DE	TAILS		\times
ch,	admin		
Q	Search		- 1
	Field	Value	
>	GENERAL		
\sim	GROUP MEMBERS	SHIP	
	uaa.admin		
	scim.write		

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 Membership Q Search			
	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 $aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa$				DETAILS	×
Identity Provider Groups Users				phantom	
				Q Search	
Q Search			+ 💿	Eald	Value
				Field	value
User Name 1 Y	Email 🍸	Origin	Action	> GENERAL	
ch_admin	ch_admin@test.org	uaa		> GROUP MEMBER	SHIP 🖸
kal_el	krypton@gmail.com	uaa		V PASSWORD	
mandrake_01	magician@gmail.com	uaa		 Inst Medified 	04/04/2022 2
phantom	devilwolf@gmail.com	uaa	向	Last Modified	04/01/2022, 2
				Last Logon	
				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*		8
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 2.5.

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 12).



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 54).
- 2. Create a service principal for your user account (on page 56).
- 3. Generate the Kerberos keytab file (on page 59).
- 4. Update the Proficy Authentication .yml file (on page 62).
- 5. Add LDAP Identity Provider (on page 12) 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 63).





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 <u>AES256_HMAC_SHA1</u> encryption type in our example code to generate the keytab file *(on page 59)*.

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 dummy 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 54)





Note:

Delete existing SPNs, if any. Refer to Useful SPN commands (on page 69).

You must be an administrator to perform this task.

- 1. Log in to your Active Directory machine.
- 2. Open the Windows Command Prompt application.

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

account>

Code	Replace With
<fqdn></fqdn>	Fully Qualified Domain Name (FQDN) of the server on which Proficy
	Authentication service is running.
	For example, HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD-
	.GE.COM
	Note:
	These should be in capital letters:
	• HTTP
	• uaatestad.ge.com (the domain name that follows @)
<user account=""></user>	Dedicated dummy user account created for Proficy Authentication
	service.
	For example, ghost1.

Based on the above examples, your code should look like this: setspn -S HTTP/win16-

phantomhost.uaatestad.ge.com@UAATESTAD.GE.COM ghost1

The service principal name (SPN) is created.

Generate Keytab File (on page 59)

Generate Keytab File

Generate the Kerberos keytab file.

Create Service Principal Name (on page 56)

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 to specify an absolute path for file creation. For example, -out c: \Documents\myskullcave.keytab.			
<service name="" pincipal=""></service>	Enter the service principal name that was created in the following format: <pre>http:/win16-phantomhost.uaatestad.ge.com@UAATESTAD.GEcom</pre>			
<user account=""></user>	Enter the same dummy user account that was used during 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 dummy 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 Gei32litc -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/winl6-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/win16-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/win16-sachin.uaatestad.ge.com@UAATESTAD.GE.COM on CN=John, CN=Users, DC=uaatestad, DC=ge, DC=com. kinits to 'HTTP/win16-sachin.uaatestad.ge.com@UAATESTAD.GE.COM' will fail. Successfully mapped HTTP/win16-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/win16-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 dummy 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 | 62

Active Directory Users and Compl	Name	Туре	Description						
> Saved Queries	🛃 Administrator	User	Built-in account for a	admin					
 Image: State of the state of th	Allowed RODC Password Rep	Security Group	Members in this gro	oup ca					
> Buitin	A Cert Publishers	Security Group	Members of this gro	oup ar_					
> Computers	Real Cloneable Domain Controllers	Security Group	Members of this gro	oup th					
Entermice	Benied RODC Password Repl.	Security Group	Members in thi	fun Deposition				2 ×	
 Enterprise EcreignSecurit/Principals 	A DrsAdmins	Security Group	DNS Administr	oruaa Properties				1 ^	
> Kes	Register Drs. UpdateProxy	Security Group	DNS clients wh	Organization Pub	blished Certificates	Member Of	Passwo	d Replication	
> CostAndFound	😤 Domain Admins	Security Group	Designated ad	Dial-In Obi	lect Securit	v Enviror	nment	Sessions	
> Managed Service Account	A Domain Computers	Security Group	All workstation Re	ternote control R	Remote Desktop Se	arvices Profile	COM+ A	Attribute Editor	
> Program Data	A Domain Controllers	Security Group	All domain con G	General Addres	ss Account	Profile Tel	ephones	Delegation	
> Svstem	A Domain Guests	Security Group	All domain gue						
C Users	A Domain Users	Security Group	All domain use	User logon name:		1			
> Intervention NTDS Quotas	Enterprise Admins	Security Group	Designated ad	uaa/win16-sachin.u	uaatestad.ge.com	@uaatestad.g	e.com	~	
> 📔 TPM Devices	Enterprise Key Admins	Security Group	Members of thi	User logon name (p	pre-Windows 2000)):			
	Enterprise Read-only Domain	Security Group	Members of thi	UAATEST		profuaa			
	Sourd1	User							
	ReOpHubJreTrustStoreMana_	Security Group	Members in thi	Logon Hours	Log On To.				
	Roup Policy Creator Owners	Security Group	Members in thi						
	Sroup1	Security Group		Unlock account					
	Sroup2	Security Group							
	Sroup3	Security Group	A	Account options:					
	Guard2	User	r	User must chu	to browned as	next logge		^	
	Guard3	User		User cannot o	chance password	Indiat Rogert			
	Suest .	User	Built-in account	Password new	ver expires				
	HarishTest	User		Store passwo	and using reversible	encryption			
	A Key Admins	Security Group	Members of thi			,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		•	
	2 krbtgt	User	Key Distributio	Account expires					
	A MainGroup	Security Group	,	Never					
	A Mark	User		O End of:	08 May 2	022			
	AmarkUser	User							
	anasterwsymbol	User							
	NaveenTest2	User							
	s profuaa	User			OK Ca	ancel	Apply	Help	
	Reprotected Users	Security Group	Members of this aro	oup ar					1
	RAS and IAS Servers	Security Group	Servers in this group	p can					
	Read-only Domain Controllers	Security Group	Members of this aro	oup ar_					
	& sachinfromuaatestad	User							
	A sachintestgroup	Security Group							
	A								

- Copy the keytab file on the machine, where Proficy Authentication is installed.
- Update the Proficy Authentication uaa.yml file (on page 62).

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 59).
- 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\GE\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 56)</i> .
keytab-location	Enter the location path where you copied the keytab file on this ma- chine.

For example:

kerberos:

service-principal: HTTP/winl6-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 56)
- Generate Keytab File (on page 59)
- Proficy Authentication Service Configuration (on page 62)

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 Loc	al intranet	×		
4	You can add and remove websites from this z websites in this zone will use the zone's securi	one. All ty settings.		
Add th	nis website to the zone:			
https	://win16-phantomhost.uaatestad.ge.com	Add		
Websi	tes:			
*.ad.	sys ^	Remove		
*.alst	om.com			
*.eq1	lais.lan			
10.93	3.16.149			
Require server verification (https:) for all sites in this zone Close				

- 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/usa/?UseKerbAuth=true

Troubleshooting 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:5 org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92) org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.jav org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769) org.apache.catalina.valves.rewrite.RewriteValve.invoke(RemoteIpValve.java:289) org.apache.catalina.valves.RequestFilterValve.invoke(RemoteAddrValve.java:378) org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:36) org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:357) org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:357) org.apache.coyote.http11.Http11Processor.service(Http11Processor.java:382) org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65) org.apache.coyote.AbstractProtocol\$ConnectionHandler.process(AbstractProtocol.java: org.apache.tomcat.util.net.NoEndpoint\$SocketProcessor.doRun(NioEndpoint.java:1722) org.apache.tomcat.util.net.SocketProcessorBase.invu(SocketProcessorBase.java:49) org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java org.apache.tomcat.util.threads.ThreadPoolExecutor.favariang.apache.tomcat.util.threads.ThreadPoolExecutor.favariang.java.base/java.lang.Thread.run(Unknown Source)</pre>
<pre>Root Cause java.lang.IllegalStateException: Listeners cannot be added to context [/uaa] as the context org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(org.springframework.web.servlet.FrameworkServlet.applyInitializers(FrameworkServlet org.springframework.web.servlet.FrameworkServlet.configureAndRefreshWebApplicationC org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(Framew org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(Framew org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(Framew org.springframework.web.servlet.FrameworkServlet.initServletBean(FrameworkServlet.j org.springframework.web.servlet.FrameworkServlet.initServletBean(FrameworkServlet.j org.springframework.web.servlet.HttpServletBean.init(HttpServletBean.java:170) javax.servlet.GenericServlet.init(GenericServlet.java:158) org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:5 org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92)</pre>

org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.jav org.apache.catalina.valves.RemoteIpValve.invoke(RemoteIpValve.java:769) org.apache.catalina.valves.rewrite.RewriteValve.invoke(RewriteValve.java:289) org.apache.catalina.valves.RequestFilterValve.process(RequestFilterValve.java:378)

org.apache.catalina.valves.RemoteAddrValve.invoke(RemoteAddrValve.java:56)

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

A MITE Carbon S00 - Internal Science X
W HITP Status 500 - Internal server X T
← → C A Not secure https://win16-sachin/uaa/?UseKerbAuth=true
👬 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.
Evention
<pre>javax.servlet.ServletException: Servlet.init() for servlet [spring] threw exception org.apache.catalina.walves.ErrorReportValve.invoke(ErrorReportValve.java:92) org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:92) org.apache.catalina.valves.RemotEJValve.invoke(RemotEJValve.java:769) org.apache.catalina.valves.RemotEJValve.invoke(RemotEJValve.java:289) org.apache.catalina.valves.RemotEJValve.invoke(RemotEJValve.java:378) org.apache.catalina.valves.RemotEAddrValve.invoke(RemotEAddrValve.java:378) org.apache.catalina.valves.RemotEAddrValve.invoke(RemotEAddrValve.java:356) org.apache.catalina.valves.RemotEAddrValve.invoke(RemotEAddrValve.java:357) org.apache.catalina.valves.RemotEAddrValve.invoke(RemotEAddrValve.java:357) org.apache.covote.http11.Http11Processor.service(Http11Processor.java:382) org.apache.covote.AbstractProcessorlight.process(AbstractProcessorlight.java:65) org.apache.covote.AbstractProcesSorlight.process(AbstractProcessorlight.java:65) org.apache.tomcat.util.net.NoEndpointSocketProcessor.dkun(NieEndpoint.java:1722) org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49) org.apache.tomcat.util.threads.ThreadPoolExecutor.juNorker(ThreadPoolExecutor.java:1191) org.apache.tomcat.util.threads.ThreadPoolExecutor.java:659) org.apache.tomcat.util.threads.ThreadPoolExecutor.java:191) org.apache.tomcat.util.threads.ThreadPoolExecutor.java:659) org.apache.tomcat.util.threads.ThreadPoolExecutor.java:659) org.apache.tomcat.util.threads.ThreadPoolExecutor.java:659) org.apache.tomcat.util.threads.TastThread\$WrappingRunnable.run(TastThread.java:61) java.base/java.lang.Thread.run(Uknown Source)</pre>
Root Cause
<pre>java.lang.IllegalStateException: Listeners cannot be added to context [/uaa] as the context has been initialised org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(YamlServletProfileInitializer.java:86) org.cloudfoundry.identity.uaa.impl.config.YamlServletProfileInitializer.initialize(YamlServletProfileInitializer.java:86) org.springframework.web.servlet.FrameworkServlet.apylpinitializers(FrameworkServlet.java:764) org.springframework.web.servlet.FrameworkServlet.configureAndRefreshWebApplicationContext(FrameworkServlet.java:771) org.springframework.web.servlet.FrameworkServlet.createWebApplicationContext(FrameworkServlet.java:786) org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(FrameworkServlet.java:736) org.springframework.web.servlet.FrameworkServlet.initWebApplicationContext(FrameworkServlet.java:591) org.springframework.web.servlet.FrameworkServlet.initServletBean.java:170) javax.servlet.GenericServlet.init(GenericServlet.java:158) org.apache.catalina.authenticator.AuthenticatorBase.invoke(AuthenticatorBase.java:540) org.apache.catalina.valves.ErrorReportValve.invoke(ArterorReportValve.java:92) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:769) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:769) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:789) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:789) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:789) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:789) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:789) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:789) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:789) org.apache.catalina.valves.RemotefValve.invoke(RemotefValve.java:378) org.apache.catalina.valves.RemotefValve.jave:378) org.apache.catalina.valves.RemotefValve.jave:378)</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

[2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] ERROR ----DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null [2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] ERROR ----DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Defective token detected (Mechanism level: GSSHeader did not find the right tag) [2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] ERROR ----DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Defective token detected (Mechanism level: GSSHeader did not find the right tag) [2022-02-21 19:09:21.839] cloudfoundry-identity-server - 13956 [http-nio-9480-exec-8] WaRN --- SpnegoAuthenticationProcessingFilter: Negotiate Header was invalid: Negotiate T1RMTVNTUAABAAAl4I14gAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA e= org.springframework.security.authentication.BadCredentialsException: Bad Credentials excpetion. It could be due to keytab file and the SPN configuration.

Crypto Mismatch

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

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

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

Clock skew between client and server

The following errors appear in uaa.log.

[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] ERROR
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null
[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] ERROR
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : null
[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] ERROR
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
level (Mechanism level: Clock skew too great (37))
[2022-02-19 13:14:55 556] cloudfoundry-identity-server - 14532 [http-min-9480-exec-9] FREOR
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API level (Mechanism level: Clock skew too great (37))
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API level (Mechanism level: Clock skew too great (37)) [2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] ERROR
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API level (Mechanism level: Clock skew too great (37)) [2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] ERROR DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Clock skew too great (37)
DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API level (Mechanism level: Clock skew too great (37)) [2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] ERROR DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Clock skew too great (37) [2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] ERROR

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/win16-phantomhost.uaatestad.ge.com@UAATESTAD-
	.GE.COM
To delete SPN	setspn -D HTTP/ <fqdn> <user account=""></user></fqdn>
	Example: setspn -D HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD.GE-
	.COM ghost1

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 71)
 - b. Create a Virtual Disk (on page 74)
- 2. Set up the iSCSI initiators: Node1 and Node2.
 - a. Configure iSCSI Initiator (on page 72)
 - b. Initialize a Virtual Disk (on page 76)
- 3. Open Failover Cluster Manager on any of the iSCSI initiator nodes in a cluster (Node1 or Node2), and create a cluster (on page 78).
- 4. Create and configure a role for the failover cluster. See Configure Role (on page 82).
- 5. Install Proficy Authentication on both the nodes.

See Configure Proficy Authentication Installation (on page 87).

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 92)*.

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:	

Section	What To Do	
	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 74).

Configure iSCSI Initiator

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

Configure iSCSI Target (on page 71).

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:	

Section	What To Do
	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 Local Server All Servers File and Storage Services ▶	WELCOME TO SERVER MANAGER O Configure this local server	Component Services Computer Management Defnagment and Optimize Drives Disk Cleanup Event Viewer
	OUTCR START 2 Add roles and features 3 Add other servers to manage WHAT'S NEW 4 Create a server group 5 Connect this server to cloud services	ISCS Initiator Local Security Policy Microsoft Asure Services ODEC Data Sources (37-bit) ODEC Data Sources (64-bit) Performance Monitor Print Management Recovery Drive Recipient, Effect
	Roles AND Server Groups Roles 1 Servers total: 1 File and Storage 1 Services 1 Manageability Events Events 1 Services 1 Manageability Events Services 1 Services Services Burdomance Deformance	Resource Monitor Services System Configuration System Information Insk Scheduler Windows Defender Finwall with Advanced Security Windows Nemory Diagnostic Windows PowerShell Windows PowerShell (diff) Windows PowerShell ISE

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:

Tweet	O side Compare	
iayer.	Quo currec	rver
Discovered targets	Qui	ck Connect
	to each target individually. Connections made here will be added to restore them will be made every to Discovered targets	to the list of Favorite Targets and an a me this computer restarts.
	Name	Status
To connect using advanced options, sel dick Connect. To completely disconnect a target, selec then dick Disconnect. For target properties, including configur opticit the turoust and dick Disconting.		
To connect using advanced options, sel dick Connect. To completely disconnect a target, select then dick Disconnect. For target properties, including configur select the target and cick Properties.	Progress report	

- 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 76)

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 71).

- 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- tion	The iSCSI target server and volume details are displayed.
iSCSI Virtual Disk Name	Enter a name for the virtual disk. For example, $_{\tt sharedDisk}$
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 access 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: 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 74).

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 24.28 GB Online	UaalSCSI (G:) 24.28 GB NTFS Healthy (Primary Partition)
O Disk 2	
Jnknown	
10.00 GB Offline 🚺	Online
	Properties
-	Lists.

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

Disk 1	
Basic	UaalSCSI (G:)
24.28 GB Online	24.28 GB NTFS
Unknown 10.00 G	Initialize Disk
A Read Read of the	
Not Init	Offline
CD	Offline Properties

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)	
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**.

	i	New Simple Volume
Disk 1 Basic 24.28 GB Online	UaalSCSI (G:) 24.28 GB NTFS Healthy (Primary Partition)	New Spanned Volume New Striped Volume New Mirrored Volume New RAID-5 Volume
— Disk 2		Properties
Basic 9.98 GB Online	9.98 GB Unallocated	- Help
CD-ROM 0		

The New Simple Volume Wizard screen appears.

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

You need to:

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

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

Create a Cluster

This topic describes how to create a failover cluster.

Install Failover Cluster Manager on the iSCSI initiator nodes. Refer to steps 1-4 in Configure iSCSI Initiator (on page 72).

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

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

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

4. Complete Validate a Configuration Wizard with these options:

Section	What To Do
Before You Begin	Skip to the next section.
Select Servers or a Clus- ter	Browse and locate the servers you want to add to the cluster. Refer to Add Server Nodes for Validation <i>(on page 79)</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.

Section	What To Do
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 .

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

The Select Computers screen appears.

2. Select Advanced.

Select Computers	×
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 Compute	ers		×
Select this object	t type:		
Computers		Object	Types
From this locatio	n:		
cluster.ge.com		Locat	ions
Common Que	ries		
Name:	Starts with $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$		<u>C</u> olumns
Description:	Starts with ~	1.50	Find Now
Disabled a	occounts		Stop
Non expiri	ng password		
Days since la	ist logon: V		/ //
		~	Quant
Search results:		OK	Cancel
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**.

Select	Computers			\times
Select	this object type: uters		Object Types	
Even	his location:			_
du	Windows Security		×	
c	Enter network credentia	ls		L
	Enter your credentials for an acco cluster.ge.com.	unt with permissi	ons for	,
	For example user, user@example. name	microsoft.com, or	domain\user	F
1	User name			
See	Password			b
Nam	Domain: CLUSTER			
	ОК	Cano	el	
	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		Loca	tions
Common Queries			
			Colores
Name: Starts with	1 ×		Courns
Description: Starts with	1 ×		Find Now
			Cana
Disabled accounts			oloh
Non expend password	1		
Deys since last logon:			/ /
Days since last logon:	×		۶۶
Days since last logon:	Ψ.		#
Days since last logon:	v	OK	Second 1
Days since last logon: Search results:		ОК	Servel Cancel
Deys since last logon: Search results: Name	- In Folder	СК	Cancel
Deys since last logon: Search results: Name	In Folder cluster.ge.comD	ок	Cancel
Deys eince last logon: Search results: Name RAMIKORRA10	in Folder cluster ge.com/D cluster ge.com/C	ок	Served ^
Deys since lest logon: Search results: Name RAMIKORRA10 & Rolat SACHINAUTHQUARD	In Folder duster ge.com/D duster ge.com/C	OK	Cancel
Deys since lest logon: Search results: Name Rolkic/RRA10 Role1 SACHINAUTHGUARD SELVA-GE2	In Folder cluster.ge.com/D cluster.ge.com/C cluster.ge.com/C	ок	Cancel
Deys since last logon: Search results: Name RAVIKORRA10 Role 1 SACHINAUTHOUARD SEL VA-GE2 Sefs	In Folder cluster.ge.com/D cluster.ge.com/C cluster.ge.com/C cluster.ge.com/C cluster.ge.com/C	CK	Cancel
Deys since last logon: Search results: Name RAVIKORRA10 Role1 SALVAGE2 Sofs useocluster useocluster	In Folder duster ge.com/D duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C	OK	Cancel
Deys since lest logon: Search results: Name RAVINORRA10 Role1 SACHINAUTHOUARD SELVAGE2 Sofs useconfig UsaMcClaster UsaMcClaster	In Folder duster ge.com/D duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C	OK	Canoel
Deys since lest logon: Search results: Name Relation Rolet SACHINAUTHOUARD Set VA-GE2 Sofs Usacouter Usacouter Usacouter Usacouter Usacouter	In Folder duster ge.com/D duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/C duster ge.com/D	ок	Canoel

6. Select **OK** to exit.

		\times
	9	bject Types
cluster ge.com		
¢		
	5	heck Names
	ок	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.
- 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 78).
- 4. Right-click **Disks** and select **Add Disk**.

The Add Disks to a Cluster screen appears.

- 5. Select the disk you want to add, and select **OK**.
- 6. In Failover Cluster Manager, expand your cluster name and select Roles.
- 7. Right-click Roles and select Create Empty Role.

The newly created role appears in the Roles pane with the name New Role.

8. Right-click New Role and select Properties.

The New Role Properties screen appears.

9. Enter a name for the new role, and select Apply.

You can assign the role to multiple node servers and set an order of preference.

For example, the new name is Demo Role.

New Role	Properties	×
General	Failover	
3	New Role	
Name:		
Demo F	Role	
Prefer Select to list at the	red Owners t the <u>preferred owners</u> for this clustered role. Use the buttons them in order from most preferred at the top to least preferred bottom.	
	aahanode1 Up	
	Down	
Priority:	Medium	
Status:	Running	
Node:	uaahanode1	
	OK Cancel Apply	
	43	

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. Co	mplete	New	Resource	Wizard with	n 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 87)</i> . For ex- ample, hauaacluster.cluster.ge.com wherein cluster.ge.com is the 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 config- ured for high availability.		
Configure Client Access Point	Verifies the validity of the client access point settings and creates a new resource.		
Summary	Select Finish.		

Salover Ouster Manager								- 0	×
File Action View Help									
🗢 🔶 🙇 📷 🖬 📷									
Relover Ouster Manager	Roles (1)							Actions	_
UserleOuter.duiter.ge.com Roles Nodes	Dearth Dearter → Lat ▼ Lat ▼ Lat ▼ Lat ▼ Lat ▼ Lat				Roles				
	Name	Salue	Type	Owner Node	Proty	Information		🕸 Configure Role.	_
> 🛃 Storage	Case role	Reving	Other	usahanode1	Medum			What Machines.	•
Networks								Create Empty Role	
Conservers.								Vew	•
	<u>K</u>						>	S Refresh	
	w 🔚 Una min					Parlament Charterny 13	er Setiers	📔 ныр	_
								Uas role	
	Name			Satur	Information			G Start Role	
	Pieles			0.44				G Stop Role	
	B GE PHONY ANY	entication Tomost Web S	erver	(Board				Add File Share	
	Summer Sectors	recebor rospectat, ce	180.000	0.044				2 Move	•
	# JE Outer Die 1			(i) Orige				S Ounge Startup Priority	•
	Server Name							18 Information Details.	
	II P Name hausach	dar.		Online				Show Ortical Events	
	ET P Address	10 181 250 202		Online				Add Storage	
								Add Resource	•
								More Actions	•
								X Remove	_
								Properties	
	<						×	🖬 Help	_
< >	Summary Resources								

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.

Fallover Cluster Manager									- a ×	
File Action View Help										
💠 🔿 🙍 🔯 🛅										
Railover Cluster Manager	Roles (1)								Actions	
UaaHaCluster.duster.ge.com Roles Nodes	Search			₽ Queries ▼			🔎 Queries 🔻 🔛	Roles		
	Name	Satur	Type	Owner Node	Prorty	Information			No Configure Role	
> 🛃 Storage	Usa role	Running	Other	usahanode2	Medum				Virtual Machines_	
Networks									Create Empty Role	
El como creno									View 🕨	
									G Refresh	
									P Help	
	¢							>	GE Proficy Authentication PostgreSQL.	
									Bring Online	
	Vaa role						Preferred Owners: A	ty node	Take Offline	
	Name			Status	Information			^	🔞 Information Details	
	B .B Ouster Disk 1			(Online				10	Show Critical Events	
	UsalSCS	a (F)		0					More Actions	
	NTFS 24	1 GB free of 24.3 GB							X Remove	
	Roles								Properties	
	🗃 🗟 GE Proficy Au	thentication Tomcat Web S	ever	Online					Help	
	IP Address	s: 10.181.251.217		Online						
	GE Proficy Authentication PostgreSQL Database			Online						
	Server Name									
	😑 🥦 Name: hauaac	duster		Online						
	IP Address	s: 10.181.251.217		Online				¥.		
< >	Summary Resources								I	

The properties screen for that service appears.

c. Select the Dependencies tab, and select Insert.

GE Pr	GE Proficy Authentication PostgreSQL Database Properties $\qquad imes$						
	Advanced P	olicies	Registry Replication				
	General	Depende	encies	Policies			
Spe	ecify the resource brought online:	es that must be brou	ght online bef	ore this res	ource can		
	AND/OR	Resource					
	Click here to a	dd a dependency					
					-		
			Insert		Delete		
No	dependencies.						
		OK	Ca	ncel	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 Re	gistry Replication		
	General	Dependencies	Policies		
Spec be br	cify the resource rought online:	es that must be brought online l	before this resource can		
	AND/OR	Resource			
		Cluster Disk 1			
	AND	: IP Address: 10.181.251.217			
•	AND	Name: hauaacluster	~		
	Click here to add a dependency				
		add a dependency			
		add a dependency	ert Delete		
		add a dependency	ert Delete		
Clus	ter Disk 1 AND aacluster	Ins DIP Address: 10.181.251.217 A	ert Delete ND Name:		

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 $\ensuremath{\textbf{Select Node}}$.
 - 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 87).

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.
- After installing Proficy Authentication on both the nodes, copy the DATABASE_PASSWORD registry key from the last installed node to overwrite the registry key in the first installed node.
 For example, in the following scenario:
 - a. First Proficy Authentication is installed successfully on the Node1 machine.
 - b. Next Proficy Authentication is installed successfully on the Node2 machine.

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

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

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

Image: Share View Image: Bit Mome Share View Image: Share Image: Share View							
	Name	Date modified	Туре	Size			
	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 KB 54 KB 49 KB			

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\GE\Proficy Authentication\httpd\conf\cert

📕 🗹 📕 🖛 🛛 🛛	ert				- 0	
File Home	Share	View				~
← → × ↑ 🛛	- GE :	Proficy Authentication > httpd > conf >	cert ~	ບ Search cert		
🖈 Quick access	^	Name	Date modified	Туре	Size	
Desktop		Iocalhost.ot	24-06-2022 18:59	Security Certificate	5	KB
Develop		localhost.key	24-06-2022 18:59	KEY File	- 4	K8
 Downloads 		server.at	24-06-2022 18:59	Security Certificate	5	KB
Documents		server.key	24-06-2022 18:59	KEY File	- 4	KB
Pictures	*					_
and a						

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	-		\times
Server Certificate External Trust Messages			
On this page, you can view and update the certificate chain used by the ma 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 for does not contain the private key, then you must provide a standalone key fil	mat. If the le in PEM fo	certificate 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 70)*.

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			×
General Details Certifica	tion Path		
Show: <al></al>	~		
Field Version Ser al number Signature algorithm Signature hash alg Sisuer Valid from Subject Public key	Value V3 404c24e3fafe870e sha256RSA sha256 GE Customer, Oper 05 June 2022 05:30 05 June 2027 05:30 GE Customer, Oper RSA (4096 Bits)	~	
	Edit Dranart as	Carau ba Fila	
	Eait Properties	Copy to File	

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.

<i>Ş</i> (Certificate Export Wizard		
	Completing the Certificate E	xport Wizard	
	You have successfully completed the Certificat	e Export wizard.	
	You have specified the following settings:		
	File Name Export Keys Include all certificates in the certification path File Format	C:\Users\Administrator\Do No No Base64 Encoded X.509 (*.	ownloads\(Jaa_(cer)
	<		>
		Fir	nish 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		

Proficy Authentication	Service	
Configure a built-in or externa	al Proficy Authentication instand	re
Proficy Authentication Base URL:	https://hauaacluster.cluster.ge.com/u:	Test
Admin Client ID:	admin	
Admin Client Secret:	•••••	
Proficy Authentication certificate file:	C:\Users\Administrator\Downloads\or	Browse View
Notes: Administrator of the Proficy Aut above. If you specify an issuer certifica the inputs before proceeding.	hentication service should provide you th te above, view and confirm. Use the Test I	e information button to validate

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 > White Labelling**. 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 company logo. 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. 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.

% G đ						@ ■~ ≙~
NAVIGATION ×	Security-Proficy Aut_ \times White Labelling Proficy Authentication \rightarrow	×			DETAILS	×
 Proficy Authentication 	Company Name* GE			*	UAA Login Preview	
Security					2 GE	×
White Labelling	Company Logo" Allowed Image Extensions: one aux. log load 1 Maximum Ela tipa Linih 3 M	•				
	Anowes mage bitersons and, and, and, and, and are been units a new second and a new second se					Digital
	sevectimage image Available ×				Welcor	me!
	Square Logo Altransferman Detendorer zone auer for fans Haufmann Elle State				User Identi	ifier
	Select Image				Password	
	Footer Legal Text			SIGN		
	cooperation from			or sign in a	with:	
					of This is a	
				factor link – Sec label	and faster	
	Footer Links		+			
	Label* T	URL*	Action			
	Second footer label	https://www.ge.com/digital/	Đ			
	This is a footer link	https://www.ge.com/	ē			
			Reset	+		

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