Proficy Authentication 2023

User Guide

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. Overview

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.

When a user is created or deleted in a product that uses Proficy Authentication, the associated user account is created or deleted in the UAA 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 UAA, or it can reuse an existing instance of UAA which was previously installed by another Proficy product. When more than one product uses the same instance of Proficy Authentication, this is called a shared or common UAA.

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

Proficy 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.

Install and Components

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

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

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

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

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

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

Note:
Proficy Authentication supports UAA version 4.30.0 or later.

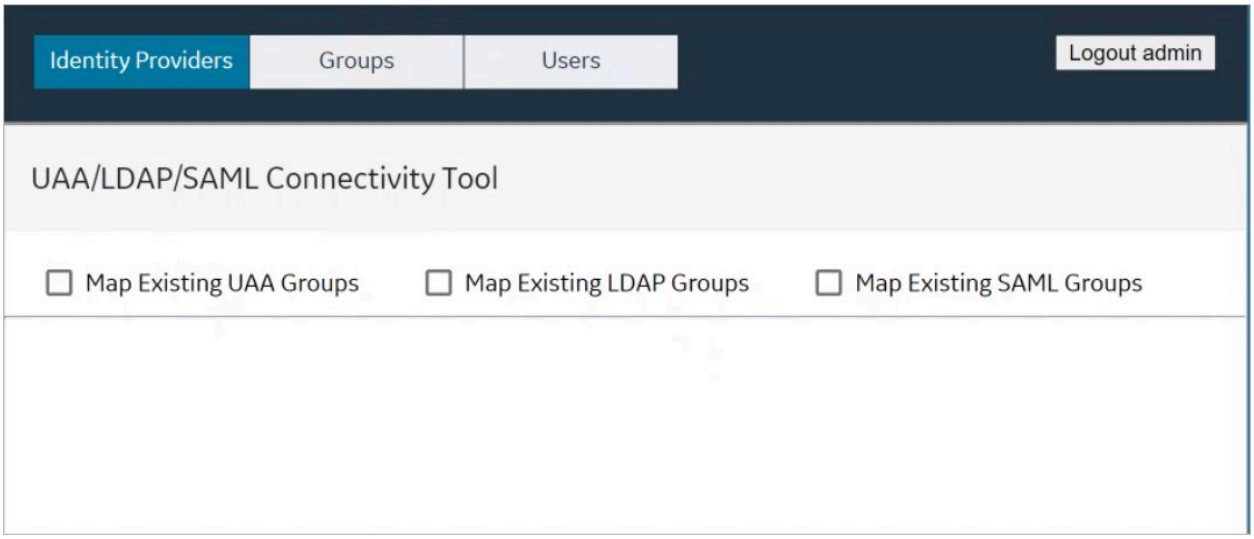
Log in to Proficy Authentication

The Proficy Authentication application is used to perform UAA configuration tasks.

1. In a web browser, enter the `server name/securityadministrationapp`. Alternatively, you can use the Proficy Authentication shortcut  to launch the application.
2. Log in with the client ID and client secret that you specified when you installed your Proficy product. Alternatively, you can provide the username and password of a user with sufficient privileges.

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

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


Identity Providers
Groups
Users
Logout admin
UAA/LDAP/SAML Connectivity Tool
Map Existing UAA Groups
Map Existing LDAP Groups
Map Existing SAML Groups

Chapter 2. Connectivity

Service Providers and Identity Providers

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

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

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

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

IDP integration can be configured in the Connectivity section of the Proficy Authentication.

Group Mappings

Group Mappings

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

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

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

- **External IDP group to Proficy Authentication group:** In the case of external IDP integration, users in the external IDP may be granted access to a Proficy product by mapping the IDPs groups to the product's Proficy Authentication groups. One example of this is mapping LDAP groups to Operations Hub groups.

Group mapping and membership can be configured in the Connectivity section of the Proficy Authentication.

Map Existing UAA Groups With Proficy Authentication

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

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

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

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

5. Select **Test**.
   If connection to the UAA server is established, a message appears, confirming the same.
6. Select **Continue**.
   In the **UAA Mapping** section, the drop-down list box contains a list of groups in Proficy Authentication. In the **Filter** box, a list of groups in the existing UAA instance appear.
7. In the drop-down list box, select the Proficy Authentication group to which you want to map the existing UAA groups.
8. In the **Filter** box, select the check boxes corresponding to the existing UAA groups that you want to map.

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

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

9. Select **Map Members**.
   A message appears, confirming that the Proficy Authentication group is mapped to the existing UAA groups that you have selected.
10. Repeat steps 7-9 for all the Proficy Authentication groups that you want to map.

The existing UAA groups are mapped with the Proficy Authentication groups.

Map LDAP Groups With Proficy Authentication

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

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

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

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

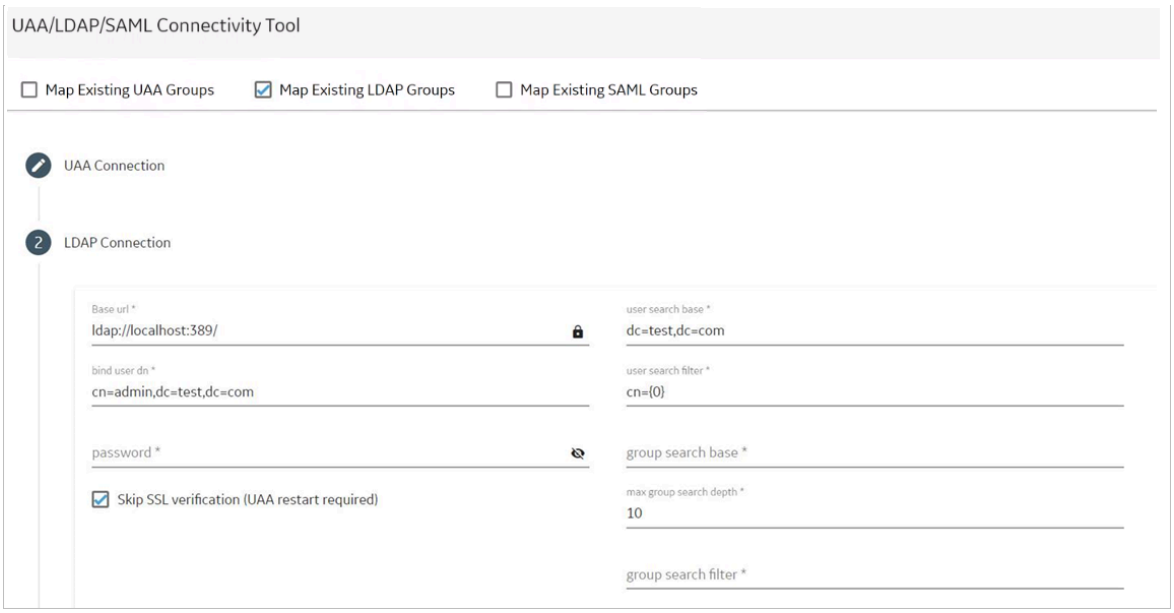
5. Select **Test**.
   If connection to the Proficy Authentication server is established, a message appears, confirming the same.

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

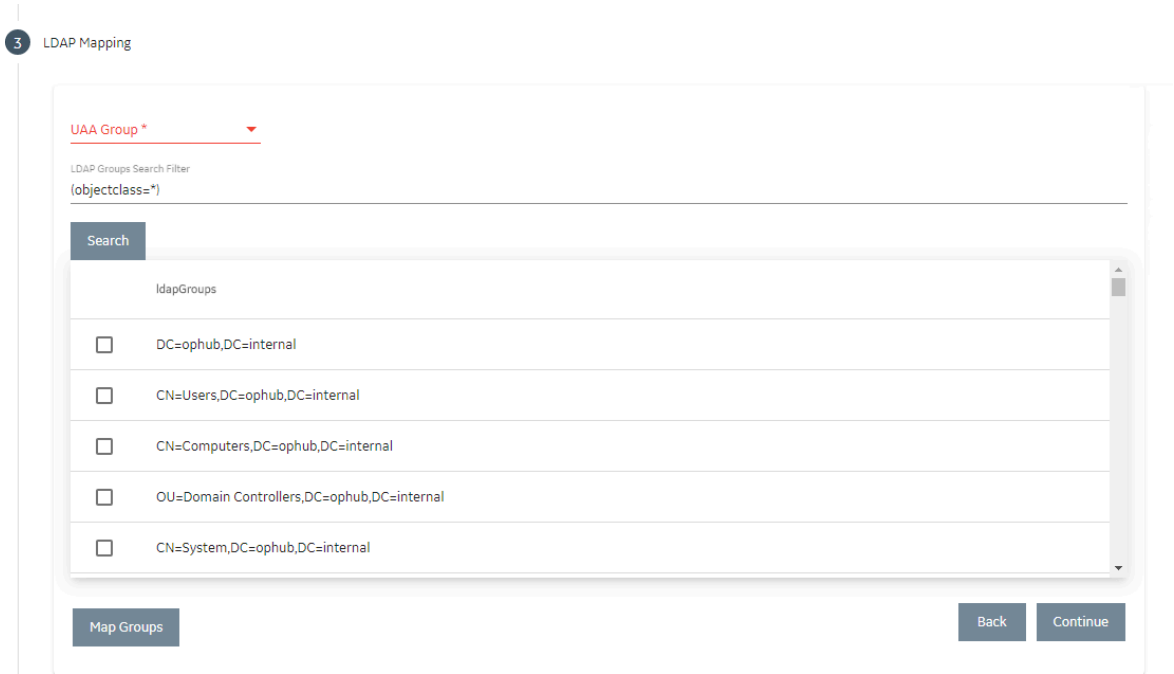
6. In the **LDAP Connection** section, provide values as specified in the following table.

Field	Description
URL	Enter the base URL of the LDAP server (for example, https://localhost).
Bind User DN	Enter the distinguished name of the bind user (for example, `cn=admin,ou=Users,dc=test,dc=com`).
Password	Enter the password for the LDAP user ID that searches the LDAP tree for user information.
Skip SSL Verification	Select this check box if you do not have the certificate to access the LDAP server. Messages are still encrypted, but the certificate is not verified for correctness. Do not select this option if you are not confident of the direct connection to the LDAP server; it could result in redirected traffic outside of your controlled network.
User Search Filter	◦ `cn={0}`: Allows the LDAP user (active directory user) to login with their display name. ◦ `sAMAccountName={0}`: Allows the LDAP user (active directory user) to login with their account name (Windows login name).
User Search Base	Enter the starting point for the LDAP user search in the directory tree (for example, `dc=developers,dc=com`). If you use only `DC=pa,DC=com`, timeout may occur due to slow system response. Use the exact `OU` to avoid timeout.
Group Search Base	Enter the starting point for the LDAP group search in the directory tree (for example, `ou=scopes,dc=developers,dc=com`). If you use only `DC=Ge,DC=com`, timeout may occur due to slow system response. Use the exact `OU` to avoid timeout.
Max Group	Enter a value to define the maximum depth for searching LDAP groups. (This may impact performance for very large systems.) By default this value is `10`.

Field	Description
Search Depth	
Group Search Filter	Enter the subdirectories to include in the search (for example, `member={0}` retrieves the `memberOf` attribute values for the specific user).



7. Select **Test**, and then select **Submit**.
   If connection to the LDAP server is established, a message appears, confirming the same.
8. Select **Test** again, and then select **Continue**.
   In the **LDAP Mapping** section, the drop-down list box contains a list of groups in Proficy Authentication.
9. In the drop-down list box, select the Proficy Authentication group to which you want to map LDAP groups. You can also search for a group in the **LDAP Groups Search Filter** box. When searching, be sure to use the standard LDAP query language for your search.



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

10. Select **Map Groups**.
    A message appears, confirming that the LDAP groups are mapped to the Proficy Authentication group.
11. Repeat steps 8-10 for all the Proficy Authentication groups that you want to map.

The LDAP groups are mapped with the Proficy Authentication groups.

Map SAML Groups With Proficy Authentication

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

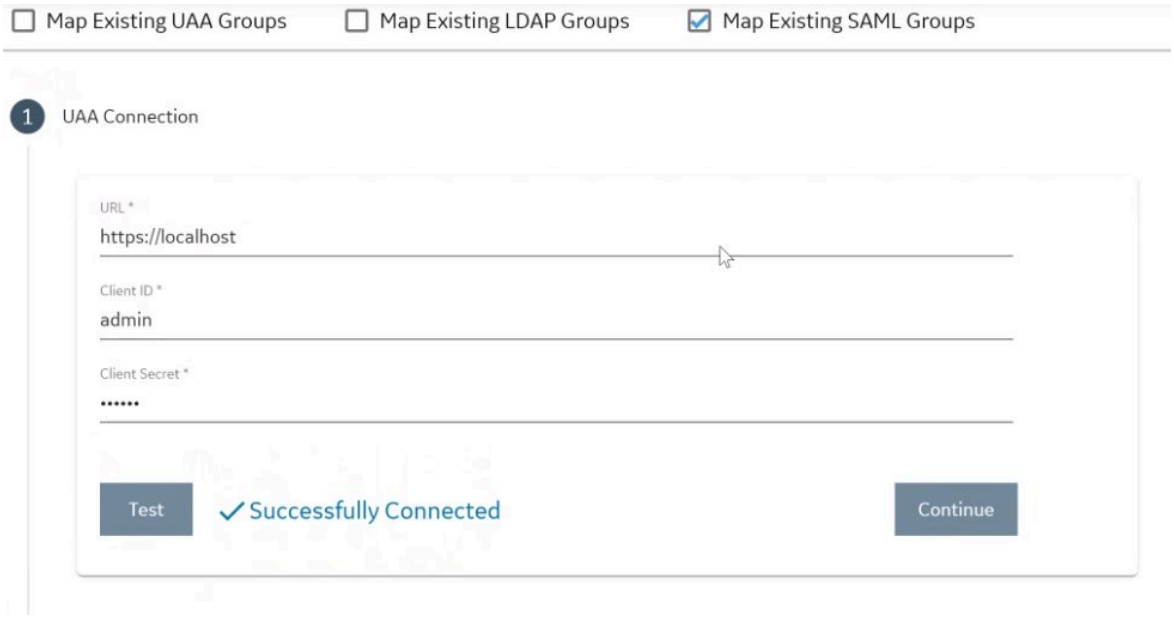
1. Double-click  on your desktop.
   The icon appears on your desktop after you install Proficy Authentication.
2. Select the **Identity Providers** tab.
   The **Proficy Authentication/LDAP/SAML Connectivity Tool** appears.
3. Select the **Map Existing SAML Groups** check box.

4. In the **UAA Connection** section, provide values as specified in the following table.

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

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

5. Select **Test**.

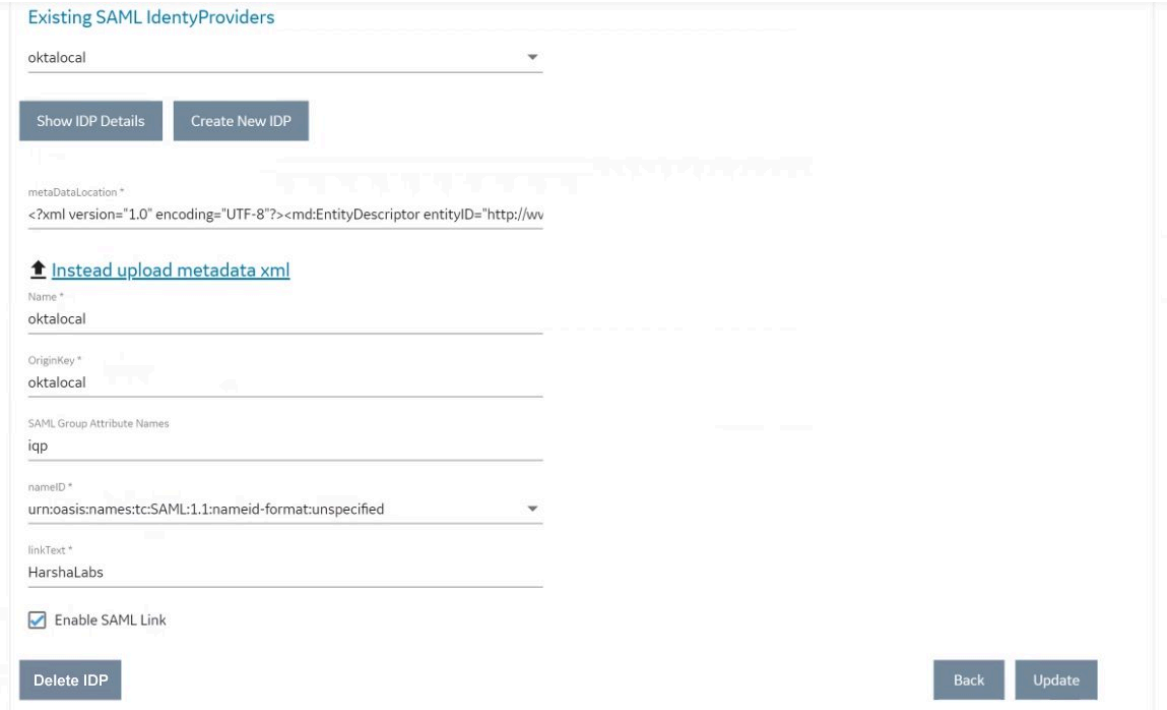


If connection to the Proficy Authentication server is established, a message appears, confirming the same.

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

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

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



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

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

The **SAML Mapping** screen appears.

9. In the drop-down list box, select the Proficy Authentication group to which you want to map SAML groups.
10. Enter a **SAML Group** and click **Add Group**. Repeat this step for each SAML group you want to add.

11. When finished adding SAML groups, click **Map Groups**.
12. Next, select **Continue** to complete.

    A message appears, confirming that the SAML groups are mapped to the Proficy Authentication group.

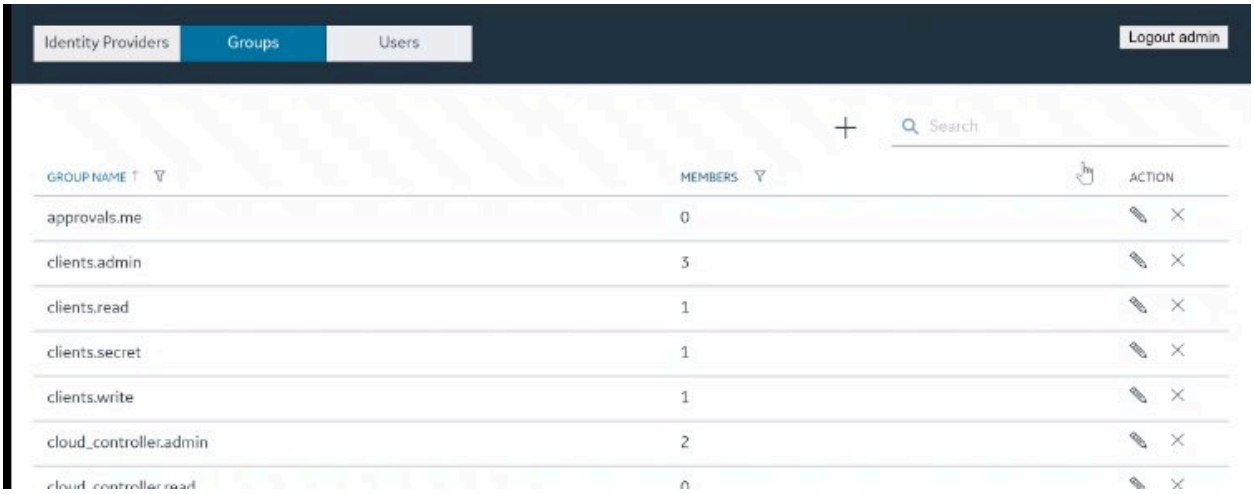
Chapter 3. Manage Proficy Authentication Groups

About Groups

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

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

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



Create Groups

As an administrator, you can create new groups based on your requirement.

Log in to Proficy Authentication 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`.

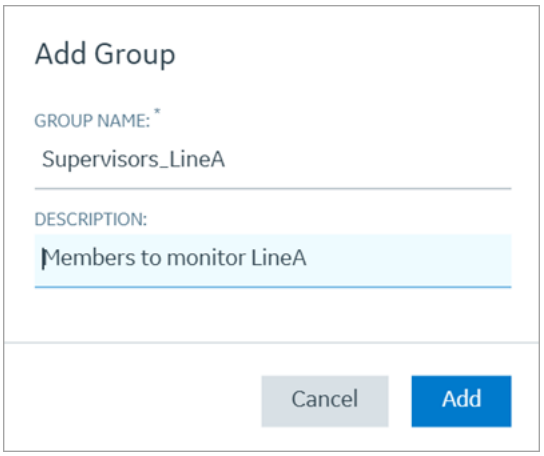
1. Select the **Groups** tab.
   The existing list of Proficy Authentication groups appear.

2. Select +

   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.
DESCRIPTION	A brief description of the group.

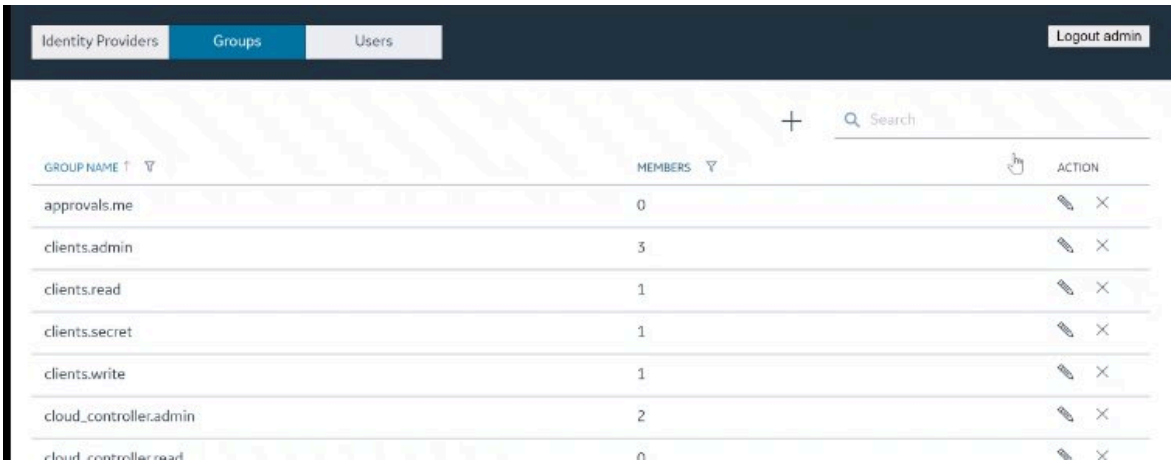
4. Select **Add**.



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

Delete Groups

1. Select **Groups**.



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

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

Add or Remove Members from Groups

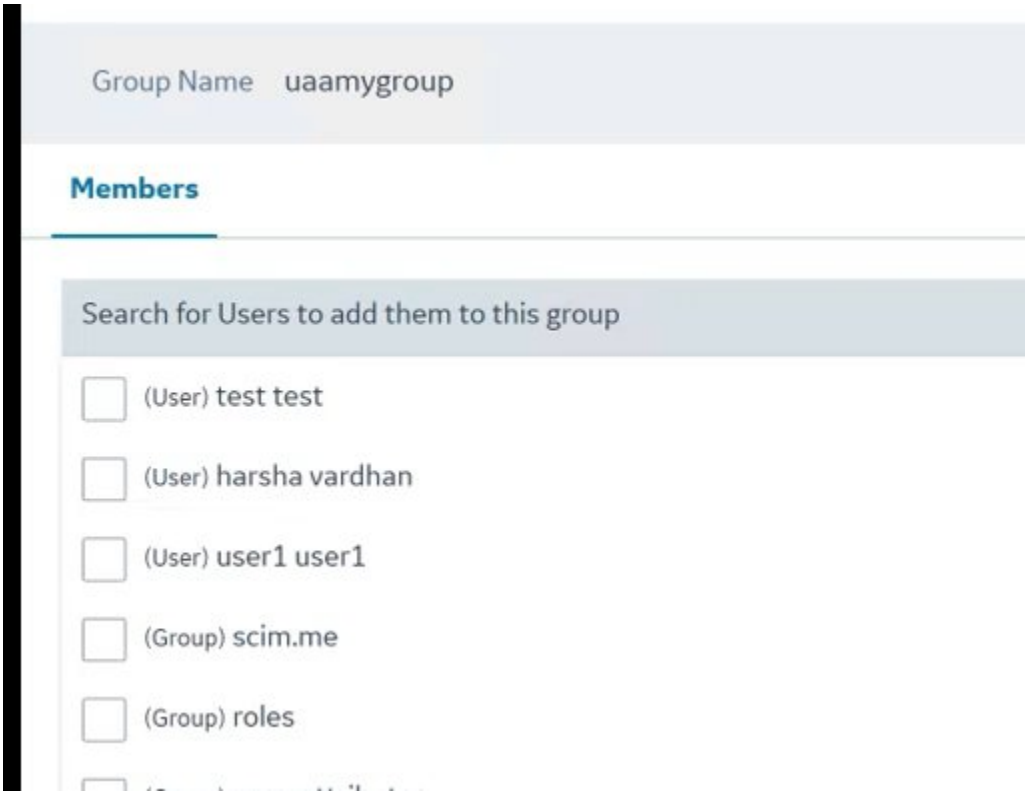
1. Select **Groups**.

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

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

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

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



The list of available users and groups appears.

4. Select the check box next to each user or group that you want to add.
5. To add the members to the group, select +.
   The members (users or groups) are added to the group. The count of the total members of the group is updated.
6. To delete a member from the group, select × in the row containing the member you want to delete.
   The member is deleted from the group. The count of the total members of the group is updated.

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

Chapter 4. Manage Proficy Authentication Users

About Users

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

You can create users locally within this application for authentication and assign them to the required Proficy Authentication groups.

Users are added to Proficy Authentication in two ways:

- Directly adding users: You can create a new user using this application, or using any user interface provided by a product that uses the Proficy Authentication application plugin.
- Mapping existing user groups: If you have user groups in an existing Proficy Authentication instance, LDAP service, or SAML service, you can map these groups with the Proficy Authentication group. The users of these groups can then use the Proficy Authentication application.

You can directly add users to Proficy Authentication ly accessing the Users section.

Create Users

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

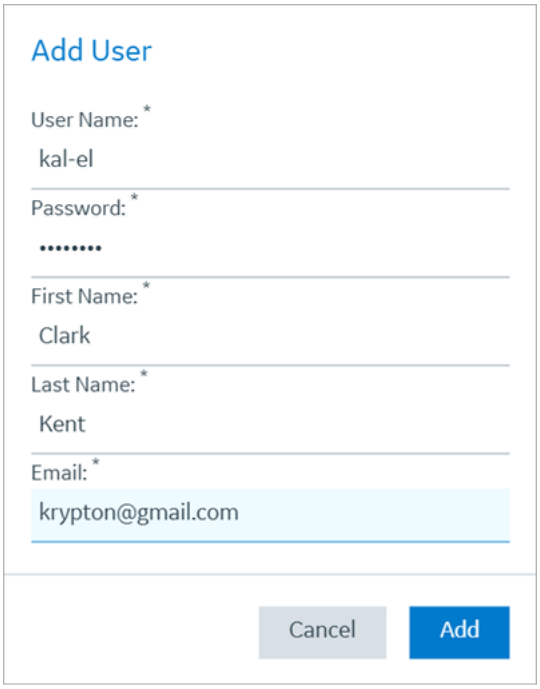
Log in to Proficy Authentication as an administrator.

1. Select the **Users** tab.
   The existing list of Proficy Authentication user accounts appear.
2. Select +
   The **Add User** screen appears.
3. Enter the following details for the new user account.

Field	Description
User Name	The user name to log in to Proficy Authentication.
Password	The password to log in to Proficy Authentication.
First Name	User's first name
Last Name	User's last name

Field	Description
Email	User's email address

4. Select **Add**.



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

For user accounts originating from LDAP or SAML, refer to Add LDAP/SAML Users *(on page 24)*.

Add LDAP/SAML Users

Log in as LDAP or SAML user to create a 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.

Modify or Delete Users

1. Select the **Users** tab.
   The existing list of Proficy Authentication user accounts appear.
2. Select for the user you want to modify, and enter your changes.
3. To delete a user, select for the user you want to delete.
   The user is deleted from the group. The count of the total members of the users is updated. The count of the total members of users is updated.

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

Change Password

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

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

1. Log in to Proficy Authentication on a web browser.
2. Go to your **Account Settings** screen.
3. Select **Change Password**.
4. Provide the following information:

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

5. Select **CHANGE PASSWORD**.

The password is changed successfully.

Reset Password for a User

Administrators can reset the password for Proficy Authentication users.

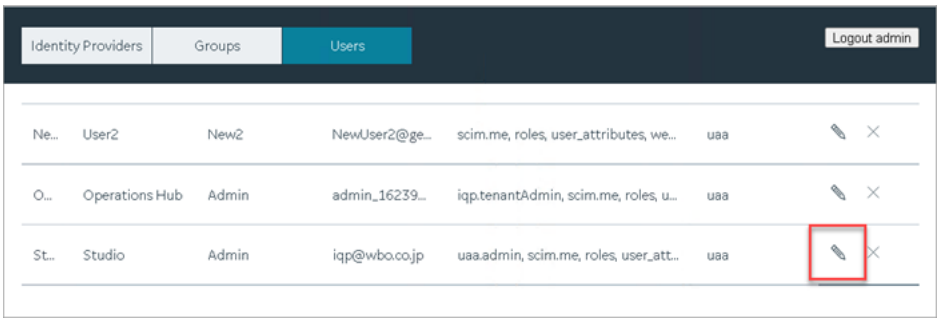
You must have administrator access to log in to the application.

1. Double-click  on your desktop.

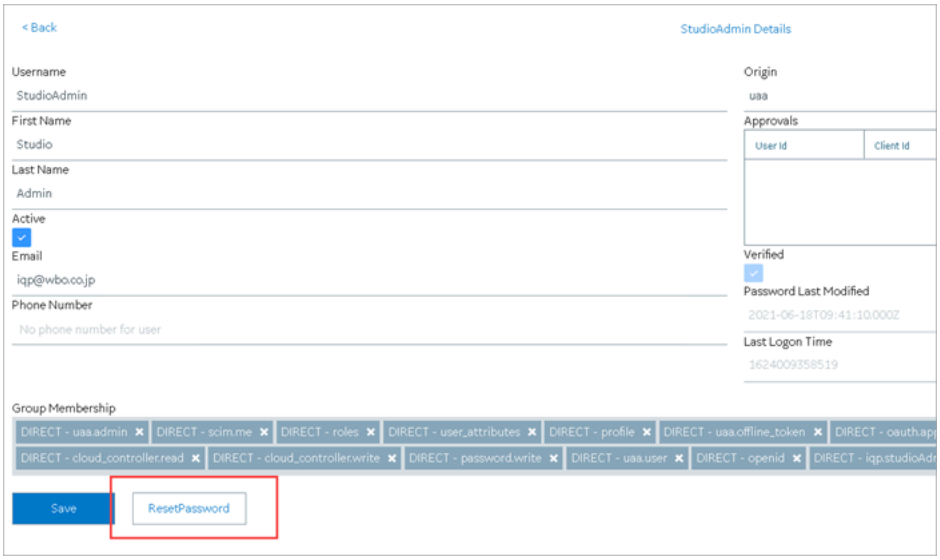
   The icon appears on your desktop after you install Proficy Authentication.
2. Log in to Proficy Authentication using `admin` account.
3. Select the **Users** tab.

   The list of all Proficy Authentication users appears.
4. Select  for the username you want to reset the password.

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

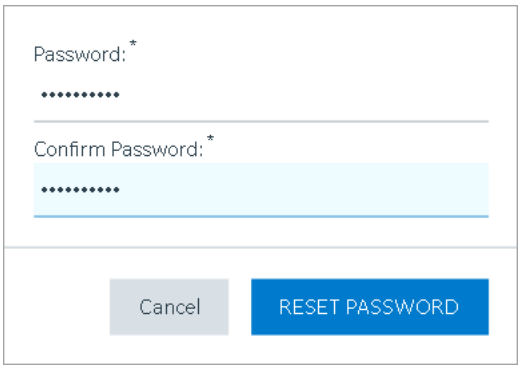


5. Select **Reset Password**.



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

7. Select **RESET PASSWORD**.



The password for the user is reset successfully.

Chapter 5. Windows Integrated Authentication / Auto-login

Windows Integrated Authentication is a new capability added to Proficy Authentication Service from version 2.5.

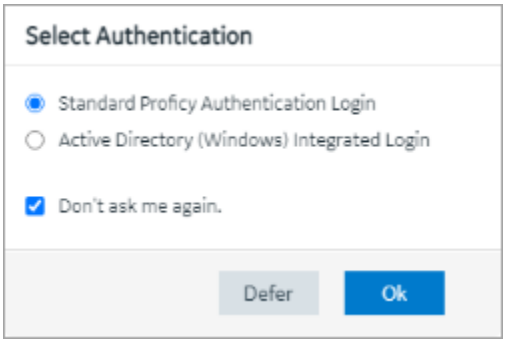
When Windows Integrated Authentication or Auto-login is enabled, users logged into any Windows machine in a domain are able to access Operations Hub and/or hosted Proficy applications without the need to type in their Windows credentials again. The same Windows logged-in user context is used for authenticating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

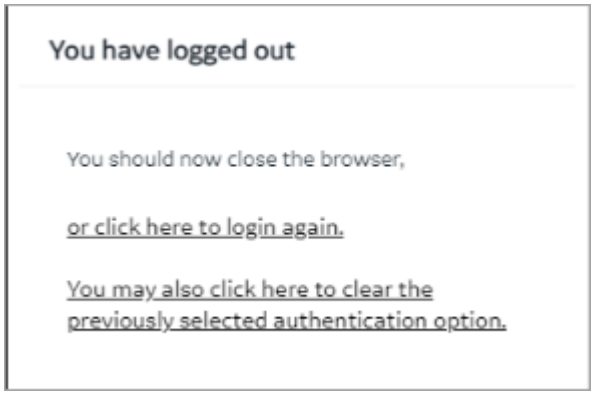
This document describes the steps to configure the 'Windows Integrated Authentication' functionality in an instance of Proficy Authentication service. After configuring auto-login, when you attempt to log into Operations Hub / hosted Proficy applications, the **Select Authentication** screen appears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

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

Note:

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



Standard Proficy Authentication Login	Choose this option if you want to use the standard login (username/password or SAML). This is a regular login, which is based on username/password, including LDAP, or SAML.
Active Directory (Windows) Integrated Login	This option appears only if Windows auto-login is configured. This allows to automatically log into Operations Hub using the user's domain 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. With **Don’t ask me again** enabled, you can clear the last selected authentication only during logout.  Select **You may also click here to clear the previously selected authentication option** to clear the saved selection. Once cleared, the clearing option is hidden from the logout screen.

	Select **click here to login again** to return to the login page.
Defer	Select to dismiss this screen, and skip selecting an authentication. You have the choice to select authentication next time you login.

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.

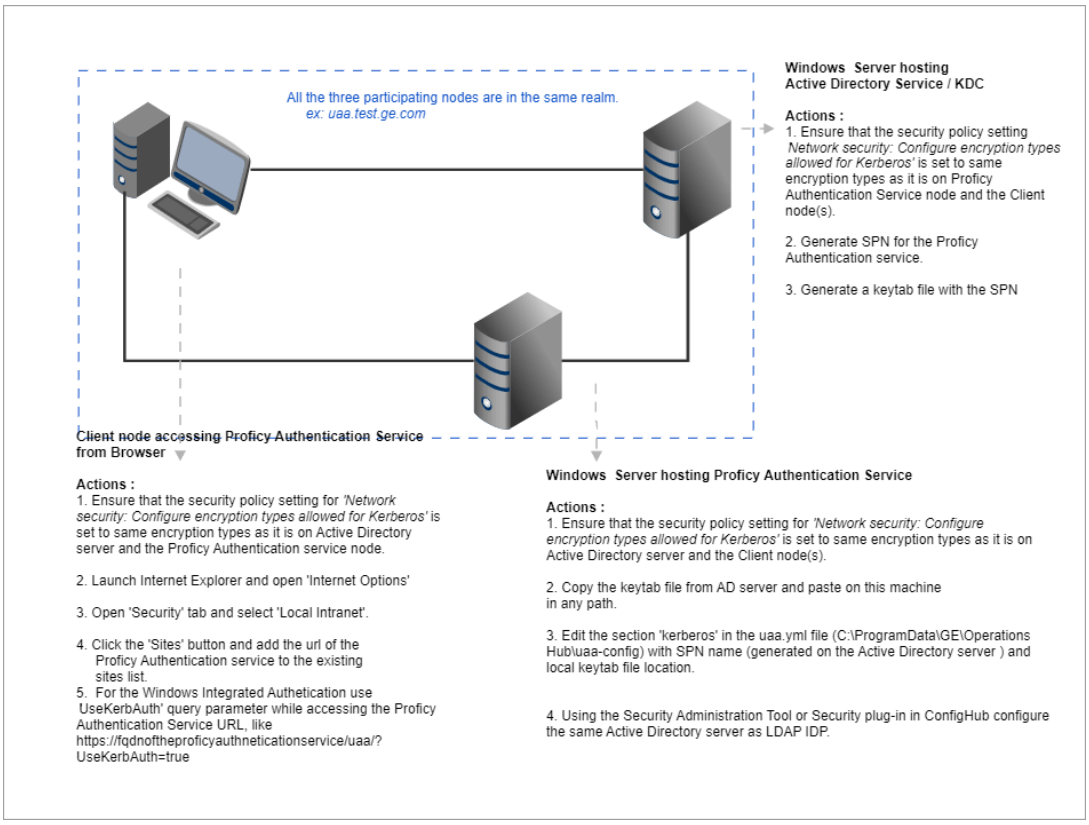
1. Configure Security Policy *(on page 31)*.
2. Create a service principal for your user account *(on page 32)*.
3. Generate the Kerberos keytab file *(on page 35)*.
4. Update the Proficy Authentication .yml file *(on page 38)*.
5. Add LDAP Identity Provider *(on page)* for the Active Directory service 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 39)*.

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



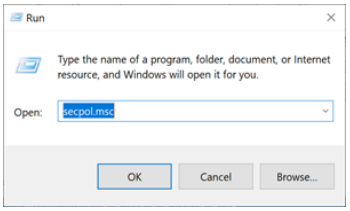
Configure Security Policy

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

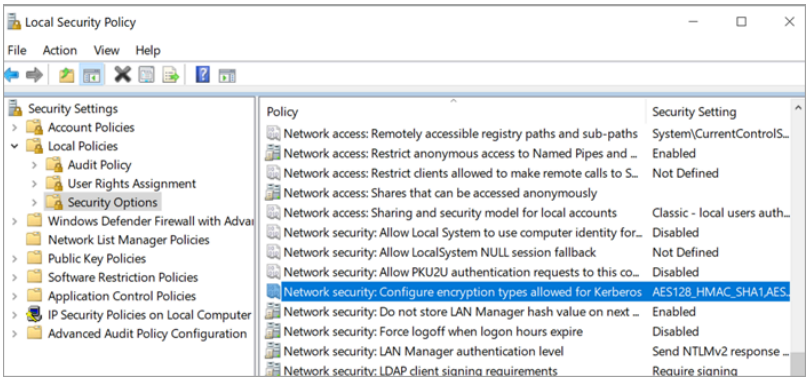
It is possible that you may not have access to your computer's local security policy settings, if it is governed by a group policy (controlled by your domain administrator). In any case, make sure that these security options are enabled for your computer.

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

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

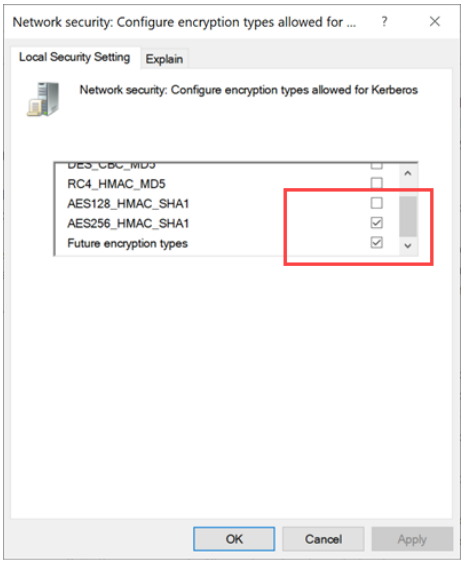


2. Navigate to **Security Settings > Local Policies > Security Options**.



3. Double-click and open `Network security: Configure encryption types allowed for Kerberos` security policy setting.
4. Select the valid encryption types that you want to use as shown in the figure. Ensure that the selection is same across all the participating nodes.

   You can select either `AES128_HMAC_SHA1` or `AES256_HMAC_SHA1` as the encryption type. Also select the `Future encryption types` option.



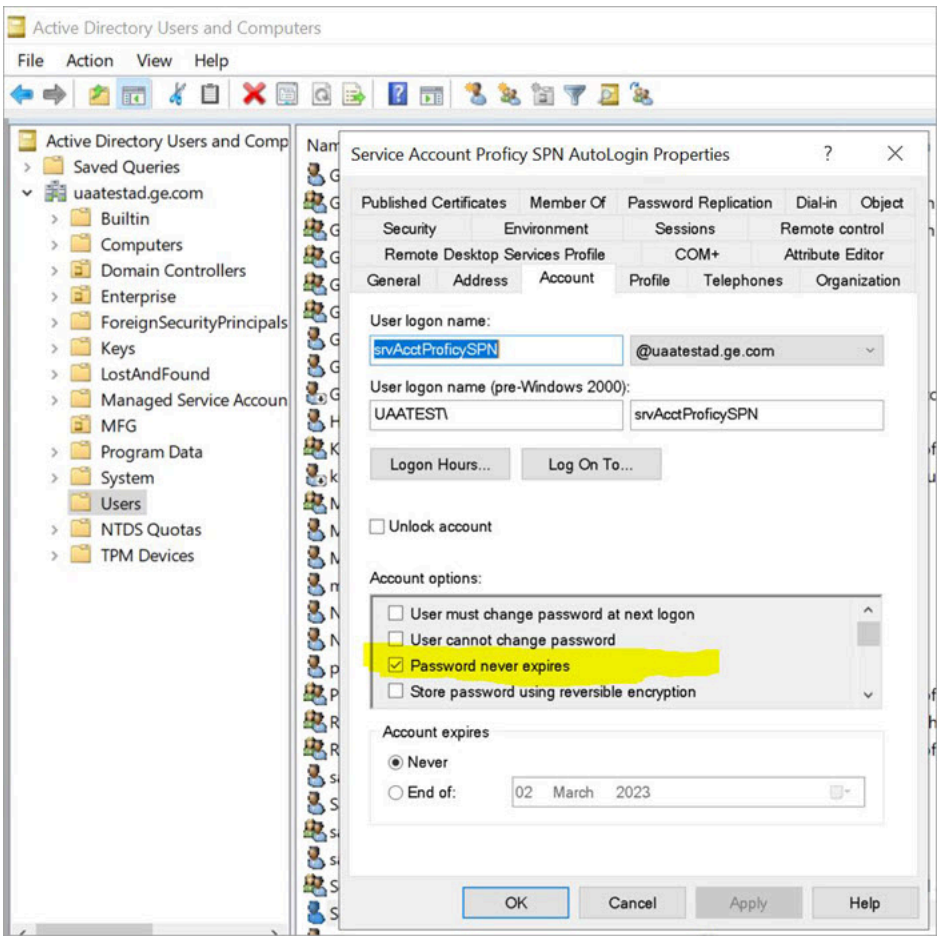
> **Note:**
> In our current documentation, we use `AES256_HMAC_SHA1` encryption type in our example code to generate the keytab file *(on page 35)*.

For more information refer to Microsoft documentation on security policy settings.

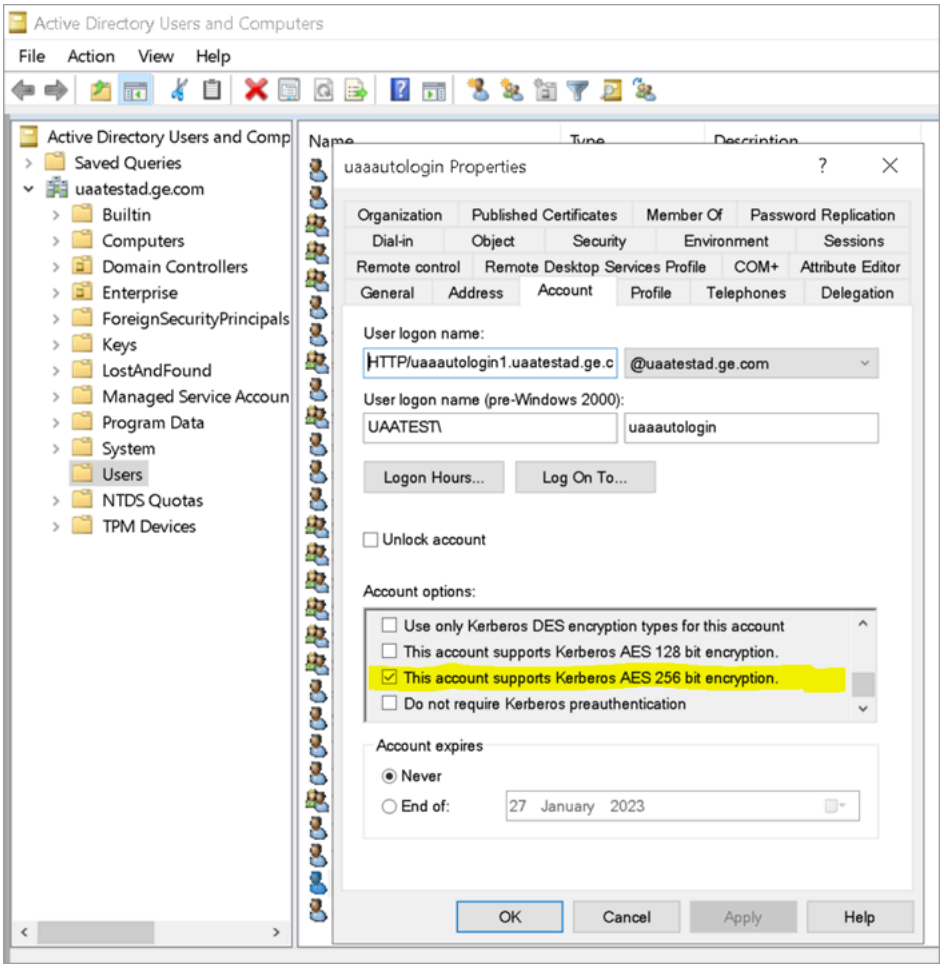
Create Service Principal Name

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 31)*



Note:
Delete existing SPNs, if any. Refer to Useful SPN commands *(on page 44)*.

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 account>`

Code	Replace With
`<FQDN>`	Fully Qualified Domain Name (FQDN) of the server on which Proficy Authentication service is running.

Code	Replace With
	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>`	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 35)*

Generate Keytab File

Generate the Kerberos keytab file.

Create Service Principal Name *(on page 32)*

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 AES256-SHA1 -pType KRB5_NT_PRINCIPAL`

Code	Replace With
`<filename>`	Name of the keytab file.

Code	Replace With
	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 pincipal name>`	Enter the service principal name that was created in the following format: `HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD.GE-.COM`
`<User account>`	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 existing user account, (or) rename the **logon name** in the user account.
`<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 Gei321itc -crypto
 AES256-SHA1 -pType KRB5_NT_PRINCIPAL
Targeting domain controller: uaatestad.uaatestad.ge.com
Using legacy password setting method
```

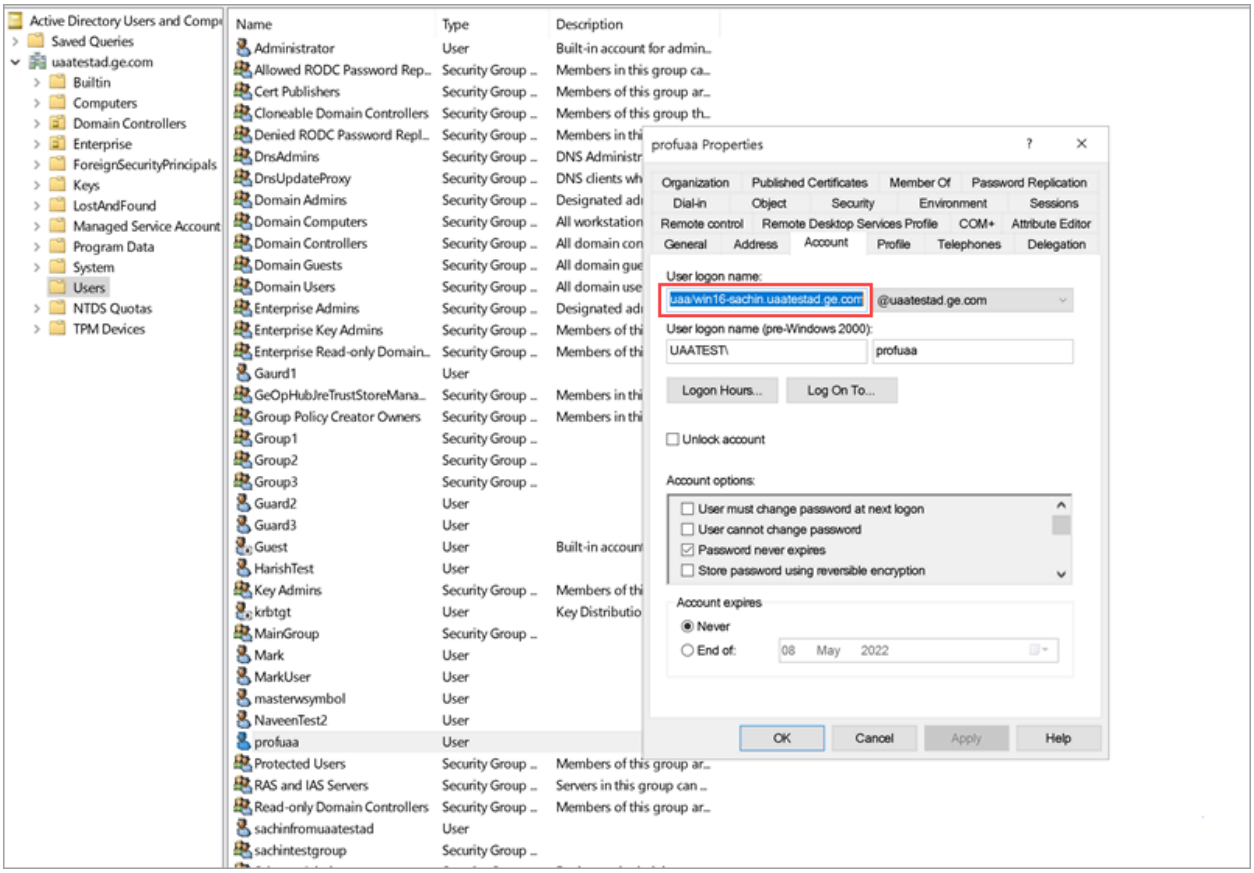
```
Successfully mapped HTTP/SACHINJOHUB21VM.uaatestad.ge.com to Mark.

Key created.

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

Keytab version: 0x502

keysize 105 HTTP/SACHINJOHUB21VM.uaatestad.ge.com@UAATESTAD.GE.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x12

 (AES256-SHA1) keylength 32 (0x3fb2a2824864a6b3617bfa4a6458af83534efdb8a3eac08b02316cce9c4ee7fc)
```

Example of a failed log:

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

 HTTP/win16-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.



- Copy the keytab file on the machine, where Proficy Authentication is installed.
- Update the Proficy Authentication uaa.yml file *(on page 38)*.

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 35)*.
- Copy the keytab file from the Active Directory server, and paste it anywhere on the Proficy Authentication machine.
- Make a note of the keytab file location on the Proficy Authentication machine.

You must be an administrator to perform this task.

1. Log in to the computer machine where Proficy Authentication is installed.
2. Access the `uaa.yml` file.
   The file is located at `C:\ProgramData\Proficy\Operations Hub\uaa-config\uaa.yml`
3. To modify, open `uaa.yml` in any text editor.
   Example: Notepad++
4. Search for `kerberos` and enter values for the following keys:

service-principal	Enter the service principal name. For more information, refer to Create Service Principal Name *(on page 32)*.
keytab-location	Enter the location path where you copied the keytab file on this machine.

   For example:

```
kerberos:
    service-principal: HTTP/win16-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.

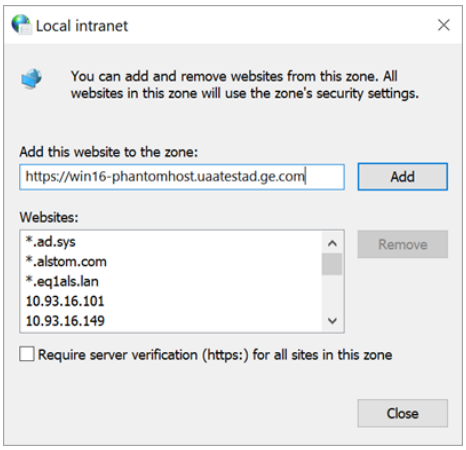
Windows Auto-login works if the following tasks are accomplished.

- Create Service Principal Name *(on page 32)*
- Generate Keytab File *(on page 35)*
- Proficy Authentication Service Configuration *(on page 38)*

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

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

1. Go to **Control Panel > Internet Options**
   The **Internet Properties** dialog appears.
2. On the **Security** tab, select **Local intranet > Sites**.
   The **Local intranet** window appears.
3. Select **Advanced**.
4. In **Add this website to the zone**, enter the URL of the Proficy Authentication service, and then select **Add**.



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

Kerberos supported SPNEGO authentication is enabled on your IE browser.

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

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.

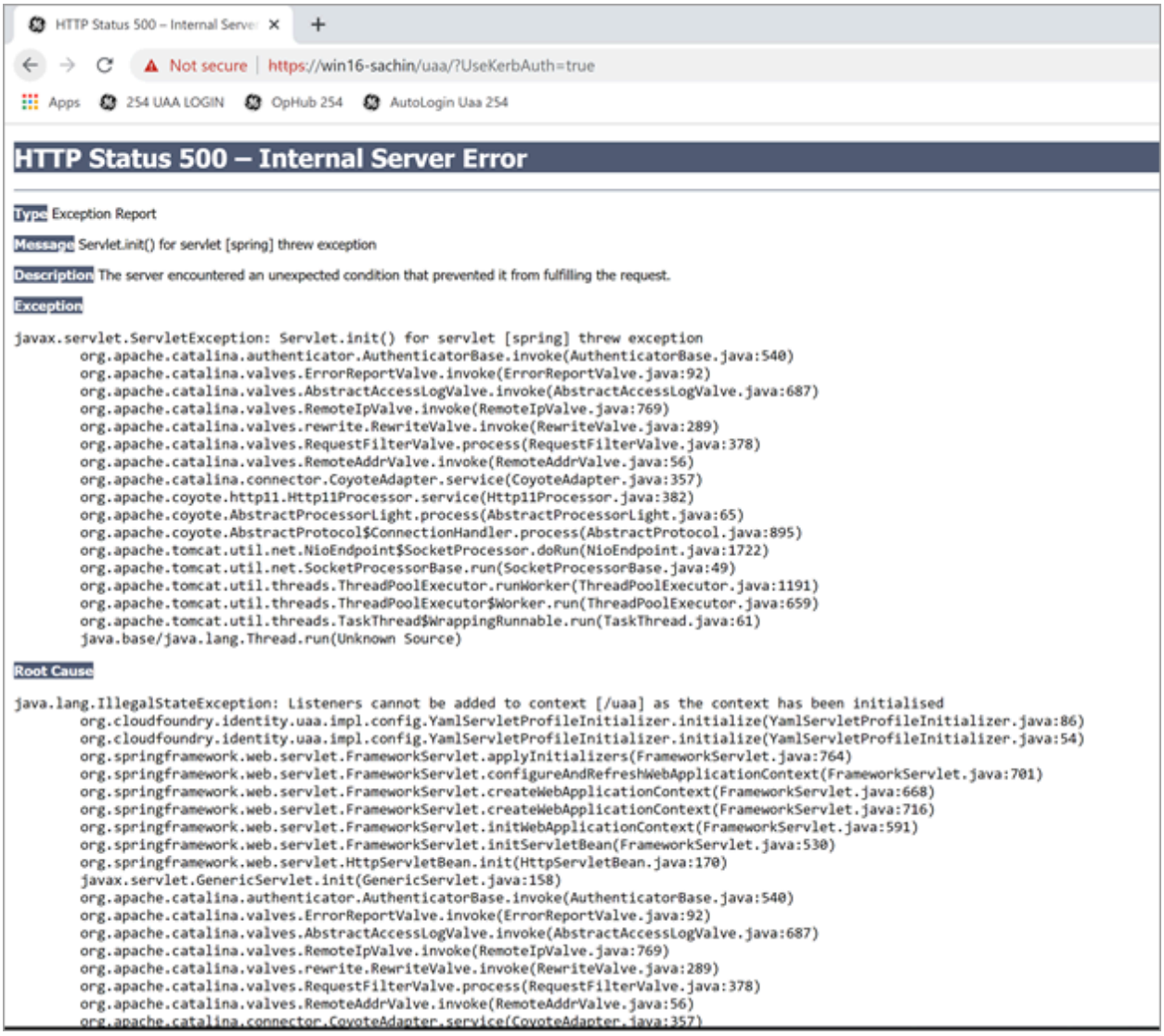
Exception

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

Root Cause

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

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



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
 TlRMTVNTUAABAAAAl4II4gAAAAAAAAAAAAAAAAAAAAAAKADk4AAAADw==
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-nio-9480-exec-9] .... ERROR ---
 DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Failure unspecified at GSS-API
 level (Mechanism level: Clock skew too great (37))
[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
 DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Clock skew too great (37)
[2022-02-19 13:14:55.556] cloudfoundry-identity-server - 14532 [http-nio-9480-exec-9] .... ERROR ---
 DynamicKerberosAuthenticationManager: Root cause for Kerberos validation failure : Clock skew too great (37)
```

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

Useful SPN commands

To view existing SPNs	`setspn -F -Q HTTP/<FQDN>` Example: `setspn -F -Q HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD-.GE.COM`
To delete SPN	`setspn -D HTTP/<FQDN> <user account>` Example: `setspn -D HTTP/win16-phantomhost.uaatestad.ge.com@UAATESTAD.GE-.COM ghost1`