



GroupID
by imanami

Version 10.0



GroupID
Authenticate



GroupID
Automate



GroupID
Self-Service



GroupID
Synchronize



GroupID
Password Center



GroupID
Insights



GroupID
Mobile App



GroupID
Reports

Configuration Guide

GroupID for ServiceNow

This publication applies to Imanami GroupID Version 10.0 and subsequent releases until otherwise indicated in new editions.

© **Copyright Imanami Corporation 2020.** Trademarks are the property of their respective owners.

Contents

Chapter 1 - GroupID for ServiceNow: An

Introduction.....1

Chapter 2 - Server Configurations3

View the service endpoint name 3

View the ServiceNow service URL 4

View the physical path to the service folder 5

Change the IIS site for the ServiceNow service... 5

View the IIS server URL 6

Manage file logging..... 6

Associate an identity store with the application.. 7

Set identity store priority..... 8

Manage third-party configurations.....10

View the Application ID and keys10

Enforce IP restrictions11

Map attribute for auto login12

Allow users to authenticate on external applications.....12

Chapter 3 - Design Configurations 14

Customize the search forms.....14

Edit a field on a search form or results page.....15

Add a field to a search form or results page 17

Remove a field18

Customize Object Properties pages.....19

Add a new tab (category).....19

Change the name of a tab (category)21

Remove a tab from an object's properties page.....21

Add a field to a tab21

Edit a field23

Remove a field23

Customize the Toolbars 24

Modify the properties of a toolbar button ... 24

Chapter 4 - Configure the GroupID application in ServiceNow 27

Install the GroupID application..... 27

Configure the GroupID application in ServiceNow 28

Provide the ServiceNow Service URL 28

Manual versus auto login..... 30

The GroupID application in ServiceNow 33

Style sheet customization 35

User authentication controls 35

Chapter 1 - GroupID for ServiceNow: An Introduction

You can integrate the Imanami GroupID application into your ServiceNow instance.

In this way, ServiceNow users can enjoy a unified experience while using the GroupID application within the ServiceNow interface, without having to switch applications.

The GroupID application for ServiceNow offers limited functionality, enabling users to:

- Search the directory
- View the groups that the user owns
- Expire and renew groups that the user owns
- View the groups that the user is a member of
- Join and leave semi-private and public groups
- Approve or deny workflow requests

GroupID administrators maintain complete control over the GroupID application in ServiceNow, since they can configure what users can view and do using the application. Administrators can specify both [server-end](#) and [design-level](#) configurations for the application using GroupID Management Console.



In this guide, the term 'GroupID application' or 'application' refers to the GroupID app that is developed specifically for deployment on the ServiceNow platform and published on the ServiceNow store.

The term 'GroupID' refers to the main GroupID application that comprises of GroupID Management Console, portals, schedules, services, and more.

Prerequisites

Consider the following before deploying the GroupID application on the ServiceNow platform:

- The GroupID ServiceNow service should be hosted on a website in IIS (Internet Information Server) and exposed over the internet for the GroupID application to work in ServiceNow.

This service enables communication between the GroupID application in ServiceNow and the GroupID server.

- The GroupID Security service must be up and running. This service is required to authenticate and authorize users on the GroupID application in ServiceNow.
- The ServiceNow service and the Security service must be accessible over the Internet with a trusted security certificate.

Installation and Configuration

The GroupID application for ServiceNow is published on the ServiceNow store under the name, Imanami GroupID. To install and configure it, see Chapter 4 - Configure the GroupID application in ServiceNow.

Application logs

Actions performed in the GroupID application in ServiceNow are logged in GroupID. The GroupID administrator can view these logs by clicking the History Summary node in GroupID Management Console.

Moreover, a text file containing event logs for the ServiceNow service is also created at the location:

```
[GroupID 10 installation  
directory]\ExternalApplications\ServiceNow\Inetpub\ServiceNow\Web\Logs\Ser  
viceNow.log
```

See Manage file logging on page 6 for details.

Chapter 2 - Server Configurations

The ServiceNow service is a service in GroupID that enables the GroupID application to function in ServiceNow. This service is hosted on a website in IIS and exposed over the internet, so that the GroupID application can connect to it.

In GroupID Management Console, you can:

- View the name of the ServiceNow service endpoint and the service URL. This URL is required to configure the GroupID application on the ServiceNow platform.
- Move the ServiceNow service under a different website on IIS.
- Set file logging for the ServiceNow service.
- Associate and disassociate identity stores with the application.
- Specify third-party configurations, required for configuring the GroupID application in ServiceNow and controlling access.
- Enable the *external application authentication* permission for security roles in GroupID.

View the service endpoint name

You can view the endpoint name of the ServiceNow service.

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. Click the **General** tab.

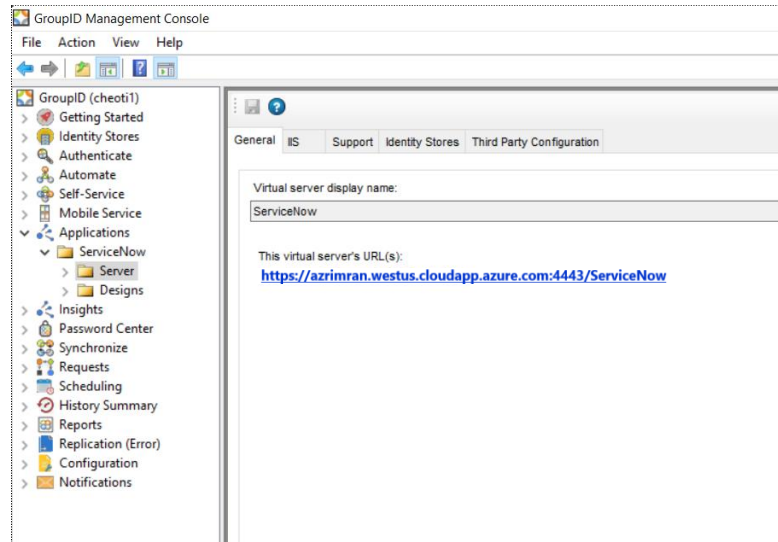


Figure 1: General tab

The **Virtual server display name** box displays the name of the ServiceNow service endpoint.

View the ServiceNow service URL

The URL for the ServiceNow service enables you to configure the service endpoint for the GroupID application in ServiceNow.

This URL must be accessible over the Internet with a trusted security certificate. Copy it and provide to the user responsible for configuring the GroupID application on the ServiceNow platform.

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. Click the **General** tab (Figure 1).
The URL for configuring the GroupID application in ServiceNow is displayed under **This virtual server's URL(s)**.

This URL must be entered in the **GroupID Configurations** page (Figure 18) to connect the GroupID application to the GroupID server.

View the physical path to the service folder

You can view the physical path to the ServiceNow service folder on disk.

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. Click the **IIS** tab.

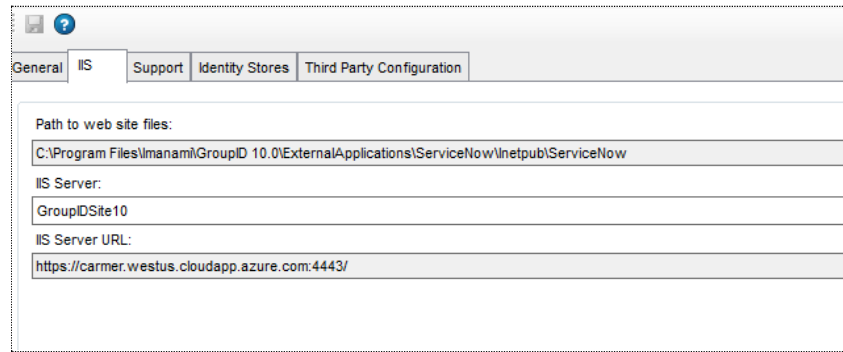


Figure 2: IIS tab

The **Path to web site files** box displays the path to the directory where the ServiceNow service files are located on disk. This field is read-only.

Change the IIS site for the ServiceNow service

The ServiceNow service for the GroupID application is hosted on a website in IIS on the GroupID server machine.

On the **IIS** tab, you can move the ServiceNow service under a different site in IIS. In such an instance, the URL of the service also changes. You must reconfigure the GroupID application on the ServiceNow platform with the new URL. The URL is displayed on the **General** tab (Figure 1).

To change the IIS site:

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. Click the **IIS** tab (Figure 2).
The **IIS Server** box displays the IIS site that hosts the ServiceNow service for the GroupID application.
3. You can select a different site from the **IIS Server** list to move the service directory under it.

The list displays the websites defined on the IIS server.

4. On the toolbar, click **Save** .

View the IIS server URL

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. Click the **IIS** tab (Figure 2).
The **IIS Server URL** box displays the URL of the IIS web server that hosts the ServiceNow service for the GroupID application.

Manage file logging

GroupID employs file logging to monitor events from the ServiceNow service, that may help in tracking events from the GroupID application in ServiceNow. You can specify the kind of information to be tracked by setting the logging level.

File Logging records the ServiceNow service events in log files that are created at the following location:

[GroupID 10 installation
directory]\ExternalApplications\ServiceNow\Inetpub\ServiceNow\Web\Logs\

File Logging uses the Rollover Logging mechanism to log events. This mechanism logs events in a text file named **ServiceNow**. When the file size reaches 100 MB, the rollover archives the log file in the same directory by replacing the file extension with the suffix .Log.X and then creating a new text file named **ServiceNow**. X in .Log.X is a number from 1 to 10 representing the archiving order; the lower the number, the more recently the file was archived.

File Logging groups events into six levels, depending on the type of information being captured. These levels are:

Level	Information Captured
1-All	Every event involving the ServiceNow service; this is the highest logging level.
2-Debug	Fine-grained event information that is most useful for debugging the service.
3-Info	Successful operations of a functionality.
4-Warn	Events that are not necessarily significant, but that could potentially cause a future problem.
5-Error	Errors that might still allow the service to continue running.
6-Fatal	Severe errors that will presumably cause an operation to abort.
Off	No events captured; turn off file logging.

Table 1: File logging levels

To set the logging level:

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. Click the **Support** tab.

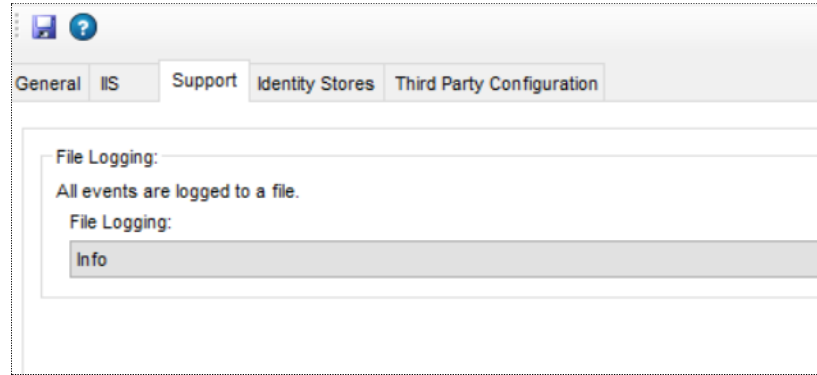


Figure 3: Support tab

3. From the **File Logging** list, select the required logging level for the ServiceNow service.

Select *Off* to turn off file logging.

4. On the toolbar, click **Save** .

Associate an identity store with the application

You must associate one or more identity stores with the GroupID application. While logging into the application, users must choose an identity store from the available list to connect the application to.

By default, the application is associated with all identity stores that existed when GroupID was installed. You can associate more identity stores with the application or remove a previously associated one.

To associate an identity store:

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. Click the **Identity Stores** tab.

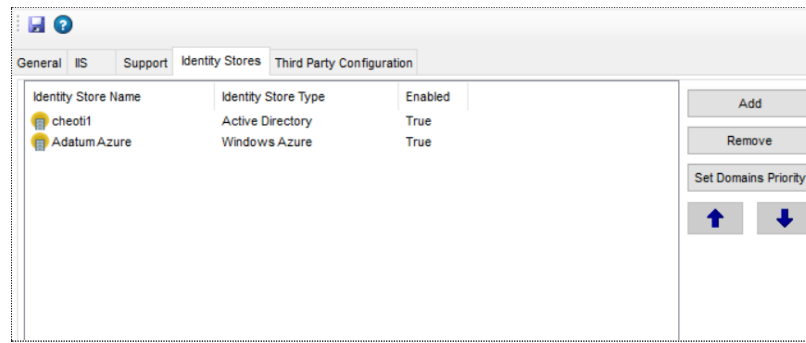



Figure 4: Identity Stores tab

3. Click **Add**; the **Add Identity Store(s) in Server** dialog box is displayed.
4. Select the check box for an identity store to associate it with the application and click **OK**.

The selected identity store(s) are displayed on the **Identity Stores** tab. Users can connect the GroupID application in ServiceNow to these identity stores.

5. On the toolbar, click **Save** .

To remove an identity store

1. On the **Identity Stores** tab, select an identity store and click **Remove**. Users will not be able to connect the GroupID application to this identity store.
2. On the toolbar, click **Save** .

Set identity store priority

Identity stores listed on the **Identity Stores** tab (Figure 4) are assigned a priority in the order of listing, with the topmost identity store having the highest priority.


The GroupID application in ServiceNow supports manual login and auto login, with the identity store priority being essential to auto login. When multiple identity stores are associated with the GroupID application, auto login requires that users be auto authenticated and logged into the identity store with the highest priority. See Auto login for details.

When an identity store has multiple child domains, the GroupID application picks the child domain with the highest priority for auto login.

To change identity store priority:

1. On the **Identity Stores** tab (Figure 4), select an identity store and use the up and down arrows to move it up or down the identity store list, thereby changing its priority.

For example, in Figure 4, cheoti1 has a higher priority than the Adatum Azure identity store. You can move Adatum Azure up the list to change the priority of both identity stores.

2. On the toolbar, click **Save** .

Set domain priority

In a multi domain identity store, a user may exist in multiple child domains. In such an instance, child domain priority determines the domain for auto login.

In auto login, users are authenticated in the child domain with the highest priority and logged into the GroupID application.

1. On the **Identity Stores** tab (Figure 4), select an identity store and click the **Set Domain Policy** button.

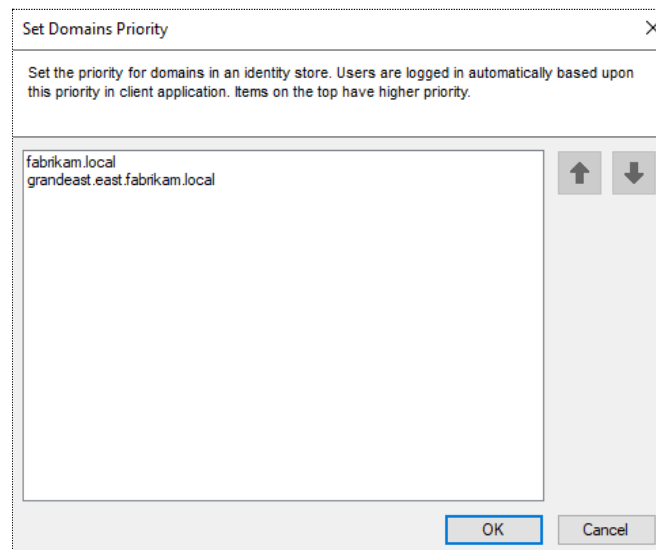



Figure 5: Set Domain Policy dialog box

This dialog box lists the child domains, if the identity store has any. Domain priority is determined in the order of listing, with the domain on the top having the highest priority.

2. Select a child domain and use the up and down arrows to move it up or down the list, thereby changing its priority.
3. Click **OK**.
4. On the toolbar, click **Save** .

Manage third-party configurations

Third-party configurations relate to the information and controls required to set up the GroupID application in ServiceNow. You can:

- View and copy the application ID and public key for the GroupID application.
- Restrict users to access the GroupID application in ServiceNow from specific IP addresses.
- Specify an attribute for value matching, to be used when users auto log into the GroupID application.

View the Application ID and keys

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. Click the **Third-Party Configuration** tab.

The screenshot displays the 'Third Party Configuration' tab in the GroupID Management Console. The interface includes the following elements:

- Application ID:** A text box containing the value `Bb44c5fd-7af3-4010-807d-147fef48eedf`.
- Private Key:** A text area containing a long alphanumeric string: `PFJTQutleVZhHVPjXNb2R1bHVzPREMKV6c y9qcS9EcUnyZHrUnk2MUGVdDEZUJITDFN NXBDYj2MVMNQ3IEVXBPRy9pRIN2U0RUxh 0eUpOTVEMGV4TKN1MnFHWkdcVxvSXBZ 2hRD4d1NWT2RlWkNUdR3Q1k4a2hqVTIRV RYkRTQk4ydG81YIMvVUtoT0pSSmdpNnpzT URZbCUVHpkdJVCVTB5MzYwcVFPYVdRbl Y1YxHxZRBMD08L01vZHVsdXOM`.
- Public Key:** A text area containing the same alphanumeric string as the Private Key.
- Generate Keys:** A button located to the right of the Public Key field.
- IP Addresses:** A large empty text area for listing IP addresses.
- Add IP Address:** A button located to the right of the IP Addresses field.
- Remove IP Address:** A button located below the Add IP Address button.
- Enable IP Address Validation:** A checkbox that is currently unchecked.
- Attribute Mapping:** A dropdown menu with `EmailAddress` selected.

Figure 6: Third-Party Configuration tab

3. The application ID, public key, and private key required to set up the GroupID application in ServiceNow, are displayed in the respective boxes.

Copy them as needed and provide them in the **GroupID Configurations** page in ServiceNow (Figure 19).

4. In case the keys are compromised, you can regenerate them. Click the **Generate Keys** button. This will overwrite the existing keys with new keys.

You must also update the public key in GroupID configurations in ServiceNow (Figure 19).

5. On the toolbar, click **Save** (📁) to save the new keys.

Enforce IP restrictions

You can specify the IP addresses from which users can log in and access the GroupID application in ServiceNow.

When IP address restrictions are defined and a login originates from an unknown IP address, the GroupID application does not allow it.

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. On the **Third-Party Configuration** tab (Figure 6), select the **Enable IP Address Validation** check box.

This enables the **Add IP Address** and **Remove IP Address** buttons next to the **IP Addresses** box.

3. Click **Add IP Address** to specify an IP address.

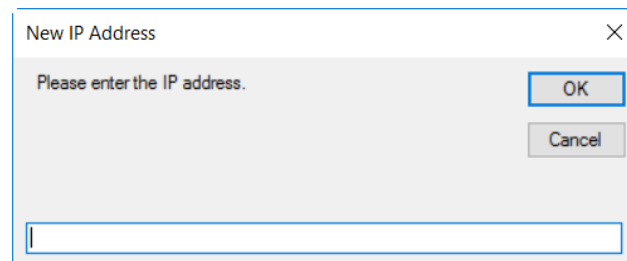


Figure 7: New IP Address dialog box

4. Enter an IP address in the **New IP Address** dialog box and click **OK**.

The IP is displayed in the **IP Addresses** box. Only users from these IP addresses can log into the GroupID application in ServiceNow.

To remove an IP address, select it and click **Remove IP Address**.


5. On the toolbar, click **Save** (📁).

Map attribute for auto login

Attribute mapping is required for auto logging ServiceNow users into the GroupID application.

While configuring the GroupID application in ServiceNow, the administrator must specify an attribute, say Email (Figure 19). As its counterpart, you must specify an attribute, say Email, in third-party configurations (Figure 6).

When a user, who is logged into ServiceNow, accesses the GroupID application, the system looks up the values of these attributes in the ServiceNow database and an identity store (say, IS-A) respectively, thereby authenticating the user when the values match. The application connects to IS-A and the user is logged in.

1. In GroupID Management Console, select **Applications > ServiceNow > Server**.
2. On the **Third-Party Configuration** tab (Figure 6), select an attribute from the **Attribute Mapping** list.
3. On the toolbar, click **Save** .

Allow users to authenticate on external applications

You must grant the external application authentication permission to security roles in an identity store in order to enable role members to log into the GroupID application on ServiceNow.

Simply put, only users with this permission in an identity store (IS-A) can connect the GroupID application to IS-A and log in.

This implies that the external application authentication permission must be granted to the required security role(s) in each identity store that the GroupID application can connect to.

1. In GroupID Management Console, click the **Identity Stores** node.
2. On the **Identity Stores** tab, double-click an identity store to open its properties.
3. On the **Security Roles** tab, select a role to grant the external application authentication permission to it, and click **Edit**.
4. On the Role Properties window, click the **Permissions** tab.

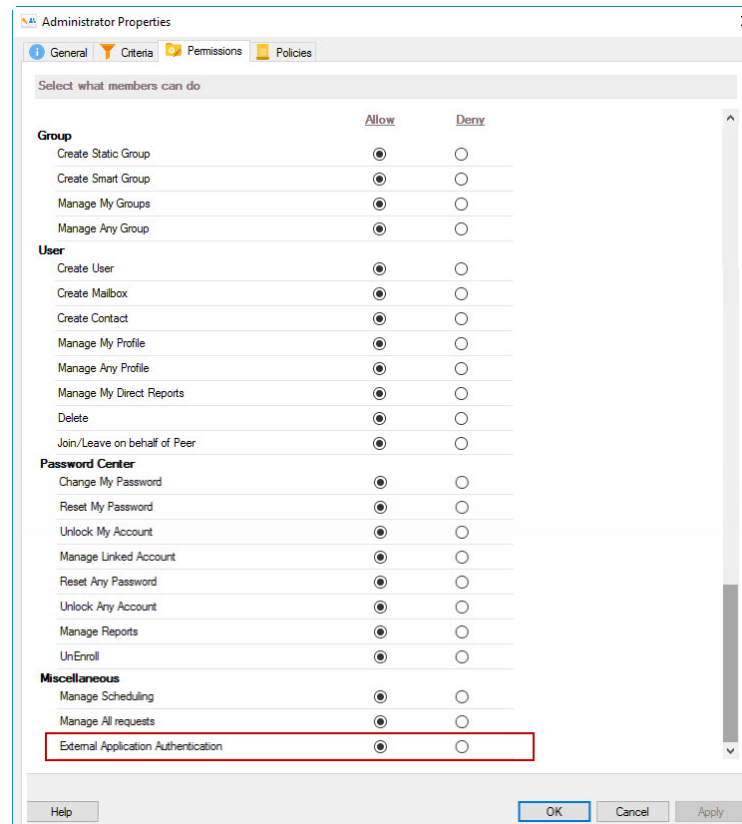


Figure 8: Role Properties window – Permissions tab

5. Select the **Allow** option button for the **External Application Authentication** permission to assign it to the role.

Users with this permission will be able to authenticate on external applications; such as ServiceNow.

6. Click **OK**.

Chapter 3 - Design Configurations

The GroupID application in ServiceNow comes with a default design template, where a few web pages and fields are predefined. However, you can customize the application pages by adding and removing fields.

When multiple identity stores are associated with the GroupID application, you can customize the design template for each identity store. In this way, the application comes with a different design for each of the associated identity stores.

You can customize the following design features:

- Directory search: specify the fields to be displayed on the search forms and search result pages in the application.
- Object properties: control what properties of directory objects (user, mailbox, contact, group, computer) you want to display in the application.
- Toolbars: customize the buttons on the application toolbars.



The *Computers* and *Contact* object types are not supported in a Microsoft Azure-based identity store.

Customize the search forms

In the GroupID application in ServiceNow, users can search for directory objects in the connected identity store.

You can customize the search forms and corresponding search result pages displayed in the application by:

- Adding new fields
- Editing existing fields
- Removing fields
- Changing the arrangement of fields on a page

You can only customize existing pages; you cannot add new ones.

The following table lists the search form/result pages that you can customize:

Search form	Description
Default	The search form is used to search for user, contact, mailbox, and computer objects while the results page displays results for this search.
Group	The search form is used to search for groups (static groups and Smart groups) while the results page displays results for this search.

Table 2: Search forms in the GroupID application

Edit a field on a search form or results page

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it. All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. Click the **Search Forms** tab.

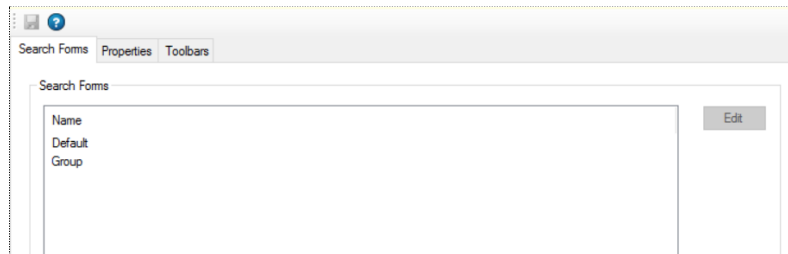


Figure 9: Search Forms tab

4. The **Search Forms** area lists the search forms available in the GroupID application. To modify a form, select it and click **Edit**.

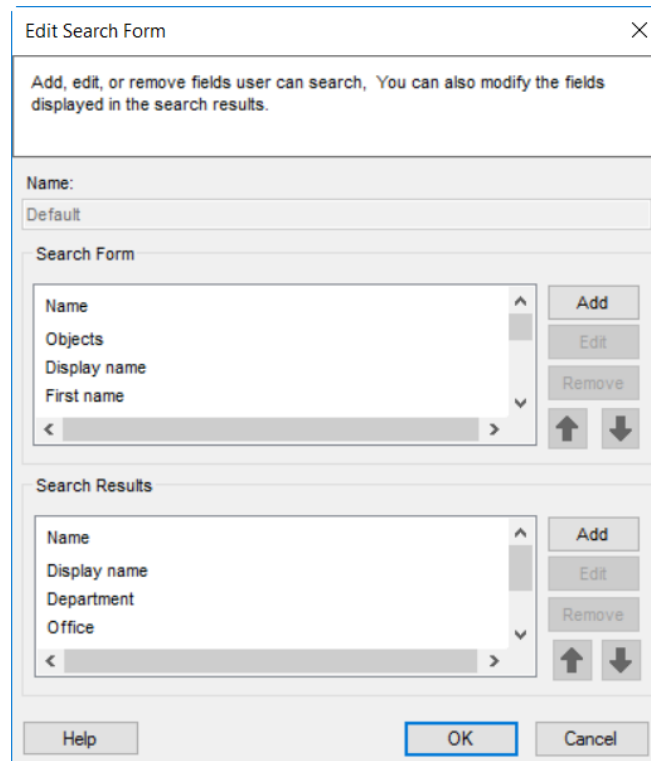




Figure 10: Edit Search Form dialog box

The **Search Form** and **Search Results** areas list the fields currently available on the search form and the search results pages of the selected search form.

Select a field and click  or  to rearrange the order of fields on the application page.

5. Select a field to modify it and click **Edit** in the respective area.

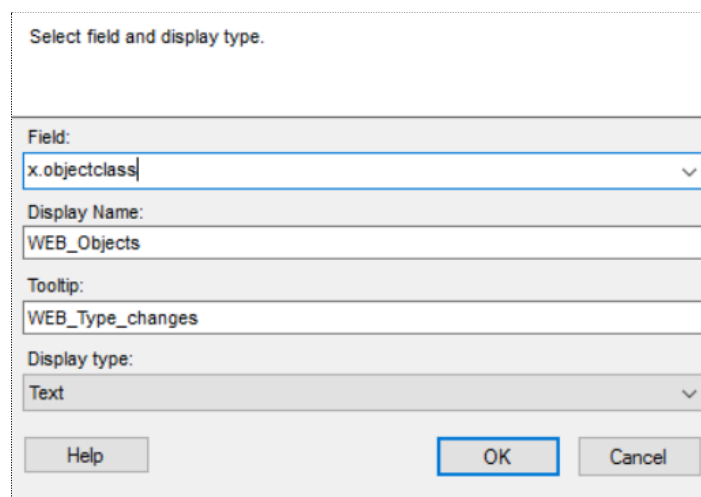



Figure 11: Edit Field dialog box



6. Modify the information as required and click **OK**:
 - **Field** – The schema attribute linked to the field.
 - For the search form, the search string that a user enters in this field is matched to the attribute's values in the identity store for retrieving search results.
 - For the search results page, the field displays the value of this attribute.
 - **Display Name** - The field's label displayed in the GroupID application.
 - **ToolTip** – The text that is displayed when a user hovers the pointer over the field.
 - **Display type** – The display type used to render the field in the application.
7. Click **OK** to close the **Edit Search Form** dialog box (Figure 10).
8. On the toolbar, click **Save** .


Add a field to a search form or results page

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it. All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. Click the **Search Forms** tab (Figure 9).
4. In the **Search Forms** area, select a search form to add field(s) to it and click **Edit**.
5. On the **Edit Search Form** dialog box (Figure 10), click **Add** in the **Search Form** or **Search Results** area to add a field to the respective page.


The **Add Field** dialog box is displayed, which is similar to the **Edit Field** dialog box (Figure 11).
6. From the **Field** list, select a schema attribute to link to the field.
 - For the search form, the search string that a user enters in this field is matched to the attribute's values in the identity store for retrieving search results.
 - For the search results page, the field displays the value of this attribute.

7. In the **Display Name** box, type a display name for the field. This name is the field's label on the search form or search results page.
8. In the **Tooltip** box, type the text to be displayed when a user hovers the pointer over the field.
9. From the **Display type** list, select the display type to use for rendering this field on the application.
10. Click **OK** to close the dialog box.
The new field is displayed in the respective area on the **Edit Search Form** dialog box (Figure 10).

Select a field and click  or  to rearrange the order of fields on the application page.

11. Click **OK**.
12. On the toolbar, click **Save** .

Remove a field

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it.
All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. Click the **Search Forms** tab (Figure 9).
4. In the **Search Forms** area, select a search form to remove a field from it and click **Edit**.
5. On the **Edit Search Form** dialog box (Figure 10), select a field in the **Search Form** or **Search Results** area to remove it and click **Remove**.
6. Click **OK**.
7. On the toolbar, click **Save** .

Customize Object Properties pages

Users can view basic information (properties) of the following directory objects in the GroupID application in ServiceNow:

- User
- Contact
- Mailbox
- Static group
- Smart group
- Computer

In the GroupID application, the property page of an object has multiple tabs, where each tab groups similar attributes. These tabs are referred to as categories.

Customization of an object's property page includes:

- **At the category level:**
 - [Adding a new tab \(referred to as a category\) to a properties page](#)
 - [Modifying an existing tab](#)
 - [Removing a tab from a properties page](#)
- **At the field level:**
 - [Adding a field to a tab](#)
 - [Modifying a field on a tab](#)
 - [Removing a field from a tab](#)

Add a new tab (category)

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it. All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. Click the **Properties** tab.

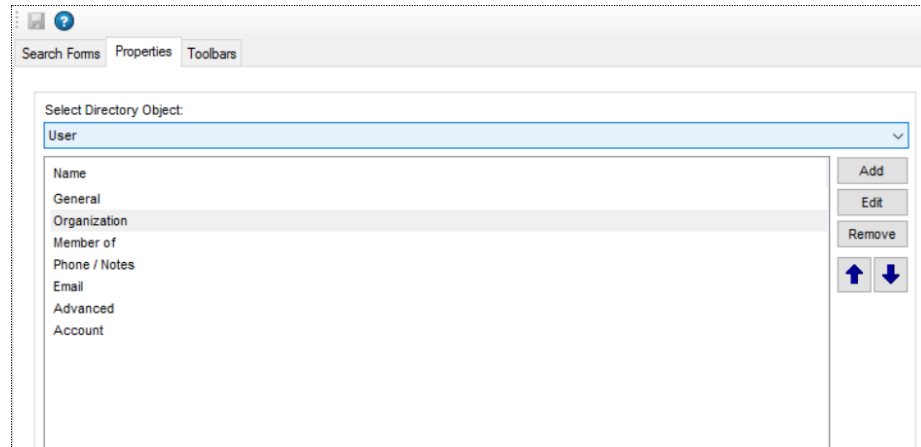


Figure 12: Properties tab

4. From the **Select Directory Object** list, select a directory object to add a tab to its properties page.

The **Name** list shows the tabs (categories) currently available on the object's properties page.

5. Click **Add**. The **Add Category** dialog box is displayed.

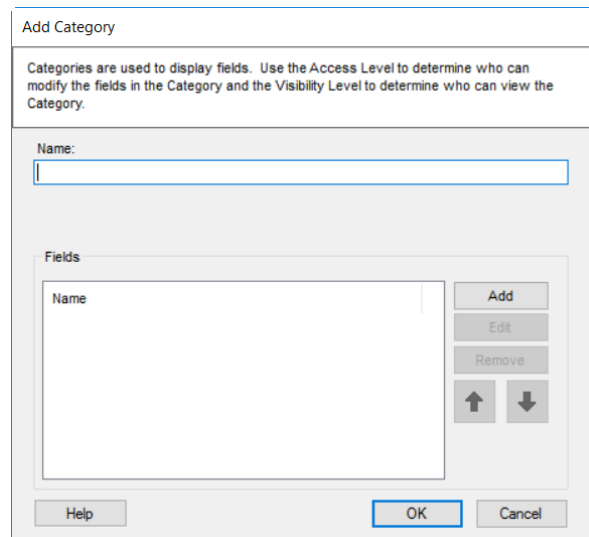




Figure 13: Add Category dialog box

6. In the **Name** box, type a name for the category. The tab will be displayed on the properties page with this name.
7. To add fields to the tab, see Add a field to a tab on page 21.
8. Click **OK** to close the **Add Tab/Category** dialog box.
9. On the toolbar, click **Save** .

Change the name of a tab (category)

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it.
All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. On the **Properties** tab (Figure 12), select the required directory object and then the tab to be modified.
4. Click **Edit**.
5. The **Edit Tab/Category** dialog box is displayed, which is similar to the **Add Tab/Category** dialog box (Figure 13). Refer to the instructions under the figure to edit the properties page.

Remove a tab from an object's properties page

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it.
All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. On the **Properties** tab (Figure 12), select the required directory object and then the tab to be removed.
4. Click **Remove**.
5. On the toolbar, click **Save** .

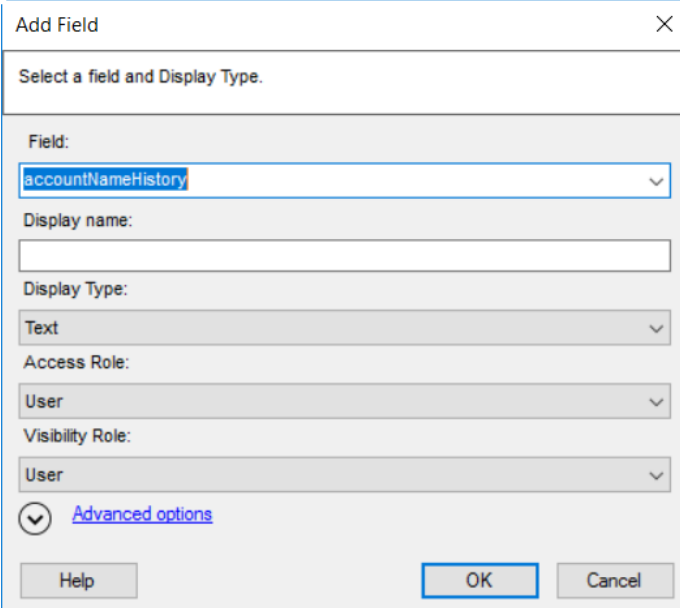
Add a field to a tab

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it.
All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. Click the **Properties** tab (Figure 12).
4. From the **Select Directory Object** list, select a directory object to add a new field on its properties page.

5. In the **Name** list, select the object's property page to add a field to, and click **Edit**.

The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 13).

6. On the **Edit Category** dialog box, the **Fields** area displays the fields available on the properties page. Click **Add**.



The image shows a dialog box titled "Add Field" with a close button (X) in the top right corner. Below the title bar is a label "Select a field and Display Type." followed by a horizontal line. The main area contains several fields: "Field:" with a dropdown menu showing "accountNameHistory"; "Display name:" with an empty text box; "Display Type:" with a dropdown menu showing "Text"; "Access Role:" with a dropdown menu showing "User"; and "Visibility Role:" with a dropdown menu showing "User". At the bottom left, there is a collapsed section icon (a circle with a downward arrow) and the text "Advanced options" in blue. At the bottom right, there are three buttons: "Help", "OK", and "Cancel".

Figure 14: Add Field dialog box

7. From the **Field** list, select a schema attribute to link to this field.
8. In the **Display Name** box, type a display name for the field. This name is the field's label on the properties page.
9. From the **Display Type** drop-down list, select a display type for rendering this field on the tab.
10. From the **Visibility Role** drop-down list, select a security role. The field would be visible to users of the selected role and to roles with a priority value higher than the selected role.


Select **Never** to hide the field from all users.


The visibility level determines the security roles whose members can view the field on the tab. The **Visibility Role** list contains all security roles defined for the identity store.



The Access Role, Max Length, Is Required, Is Read Only, and Filter Bad Words options do not apply.

11. Click **OK** to close the **Add Field** dialog box.

The field is displayed in the **Fields** area on the **Add Category/Edit Category** dialog box (Figure 13). You can rearrange the fields using the up and down arrows () , modify a field, and even remove a field from the tab.

12. Click **OK**.
13. On the toolbar, click **Save** .

Edit a field

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it. All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. Click the **Properties** tab (Figure 12).
4. From the **Select Directory Object** list, select a directory object to edit a field on its properties page.
5. Select the object's property page in the **Name** list and click **Edit**.

The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 13).

6. The **Fields** area displays the fields available on the properties page. Select a field and click **Edit**.


The **Edit Field** dialog box is displayed, which is similar to the **Add Field** dialog box (Figure 14). Follow the steps under the figure to edit the field details and save the changes.

Remove a field

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it. All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. Click the **Properties** tab (Figure 12).

4. From the **Select Directory Object** list, select a directory object to remove a field from its properties page.
5. Select the object's property page in the **Name** list and click **Edit**.

The **Edit Category** dialog box is displayed, which is similar to the **Add Category** dialog box (Figure 13).

6. In the **Fields** area, select the field you want to remove and click **Remove**.
7. Click **OK** to close the **Edit Category** dialog box.
8. On the toolbar, click **Save** .

Customize the Toolbars

Toolbars are available on different pages of the GroupID application in ServiceNow. GroupID enables you to customize the following toolbars:

- **Group:** Available on the group properties page.
- **Default Search:** Available on the search results pages.

The buttons available on these toolbars are predefined. You cannot add or remove a button; you can only edit a few details for each button, such as the button text and tooltip text.

Modify the properties of a toolbar button

1. In GroupID Management Console, select **Applications > ServiceNow > Designs**.
2. Select an identity store to customize the application design for it. All identity stores associated with the GroupID application are listed under **Designs**. You can design a different application for each of these.
3. Click the **Toolbars** tab.

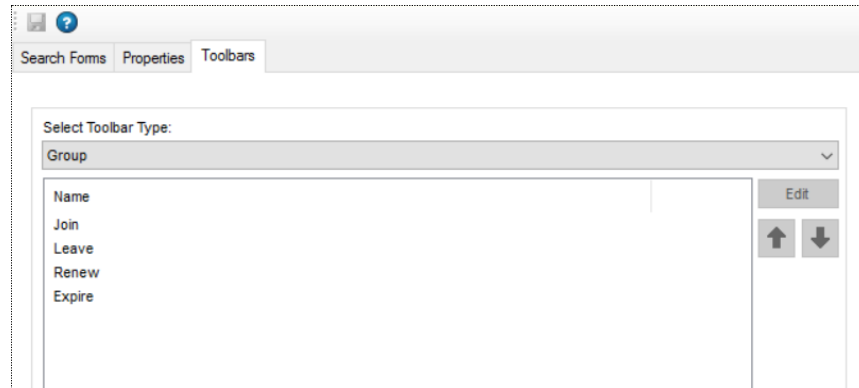


Figure 15: Toolbars tab

4. From the **Select Toolbar Type** drop-down list, select the toolbar you want to modify.

The **Name** area lists all buttons on this toolbar.

5. Select a button to modify it and click **Edit**.

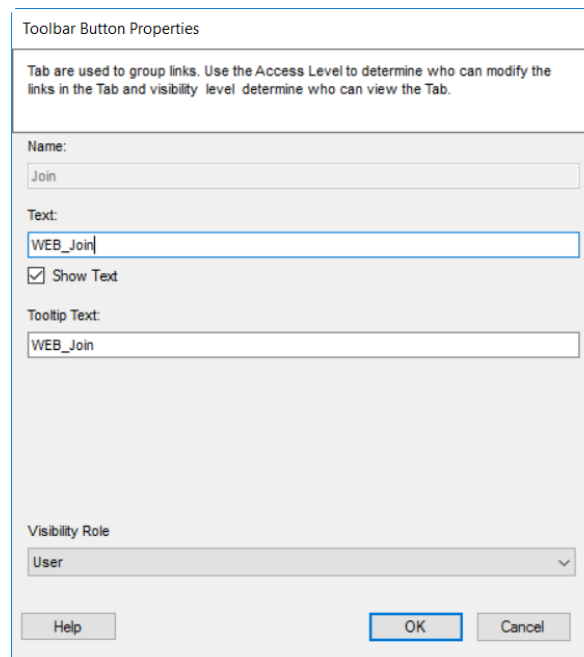





Figure 16: Toolbar Button Properties dialog box

6. Modify the following information as required:
 - a. **Name** – The name of the toolbar button. It is non-editable.
 - b. **Text** – The text that would be displayed on the button as its name.

- c. **Show Text** – Select this check box to display the text on the button; else the button would be displayed without the text.
- d. **Tooltip Text** - The text to appear when a user hovers the pointer over the button.
- e. **Visibility Role** – Select a security role. The toolbar button would be visible to users with the selected role and to roles with a [priority value](#) higher than the selected role.

Select **Never** to hide the button from all users.

The visibility level determines the security role(s) whose members can view the button on the toolbar. The **Visibility Role** list contains all security roles defined for the identity store.

- 7. Click **OK** on the **Toolbar Button Properties** dialog box.
- 8. You can rearrange the order of buttons on a toolbar.
On the **Toolbars** tab (Figure 15), select a toolbar and use  and  to rearrange its buttons.
- 9. On the toolbar, click **Save** .

Chapter 4 - Configure the GroupID application in ServiceNow

To integrate the GroupID application into your ServiceNow instance, do the following:

- Install the Imanami GroupID application into your ServiceNow instance.
- Configure the application by connecting it to the GroupID application server.

Complete these simple steps to enable your ServiceNow users to use the GroupID application from within your ServiceNow instance.

Install the GroupID application

Install the Imanami GroupID application from the ServiceNow store.

1. On the ServiceNow Store, search for **Imanami GroupID** and install the application.
2. On logging into your ServiceNow instance, the dashboard is displayed:

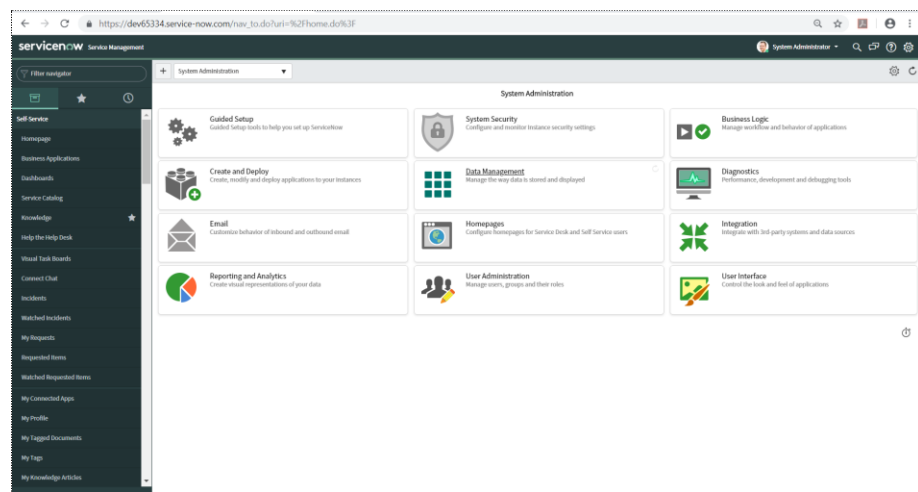


Figure 17: ServiceNow instance – Dashboard

The left pane lists the applications available in your ServiceNow instance. Locate Imanami GroupID and configure it.

Configure the GroupID application in ServiceNow

The ServiceNow service for the GroupID application is hosted on the IIS server running on the GroupID machine. To connect the GroupID application deployed on the ServiceNow platform to the server, you must register the ServiceNow service URL with the application. This done, you must also:

- Specify whether ServiceNow users should log into the GroupID application manually or automatically.
- Map an attribute to authenticate the users for auto login.
- Assign a role to the GroupID application users in ServiceNow.

Provide the ServiceNow Service URL

To connect the GroupID application to the IIS web server that hosts the ServiceNow service, you must manually enter the ServiceNow service URL in the GroupID application on the ServiceNow instance.

1. Log into your ServiceNow instance.
2. Search for **Imanami GroupID** in the left pane and then click **GroupID Configurations**.

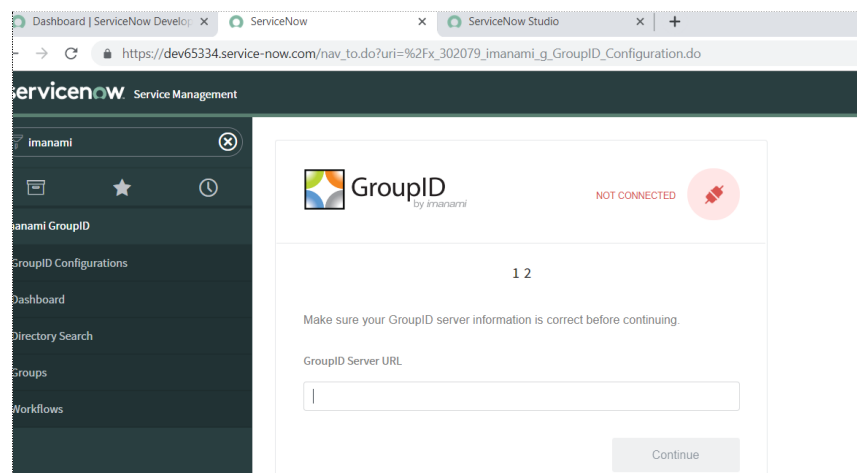


Figure 18: GroupID Configurations page

3. In the **GroupID Server URL** box, provide the URL of the IIS web server that hosts the ServiceNow service for GroupID application.

Copy this URL from under the **This virtual server's URL(s)** label on the **General** tab (Figure 1).

An example of the URL is:

<https://azrimran.westus.cloudapp.azure.com:4443/ServiceNow>

This URL should meet the following conditions:

- It must be publicly accessible over the internet.
- A security certificate from a trusted certificate authority must be configured for the IIS site that hosts the ServiceNow service.

4. Click **Continue**.

The system validates the URL while the status changes from 'Not Connected' to 'Connecting' and then 'Connected'.

More fields are displayed as follows:

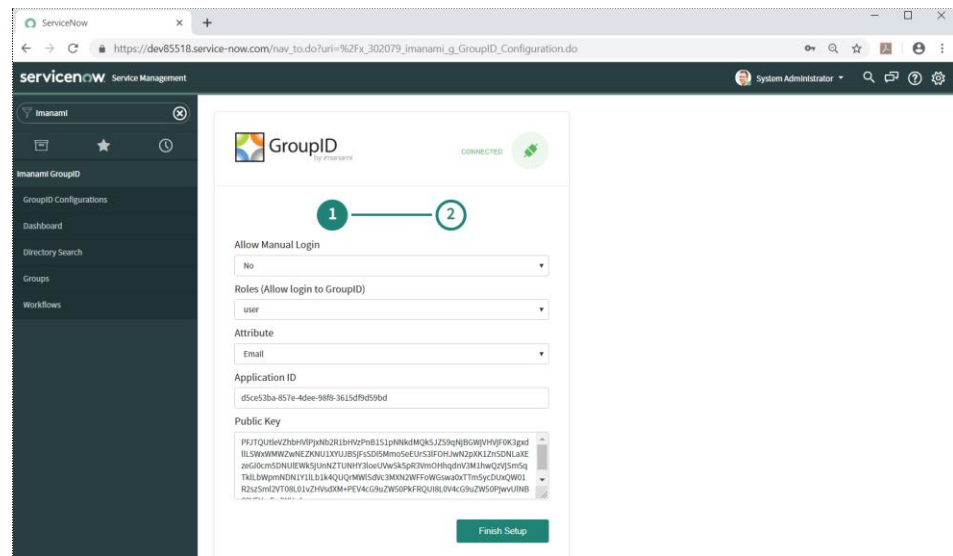


Figure 19: GroupID Configurations page (2)

5. From the **Allow Manual Login** list, select

- **Yes:** to provide both the auto login and manual login options to users that are logged into ServiceNow, for access to the GroupID application.
In manual login, users must provide their GroupID credentials to log into the GroupID application in ServiceNow.
- **No:** to enable users logged into ServiceNow to access the GroupID application without having to log in with their GroupID credentials.

See Manual versus auto login on page 30.

6. From the **Roles (Allow login to GroupID)** list, select a role that would be assigned to users on the GroupID application in the ServiceNow context. Options are:
 - **Admin** - Enables users to manage the GroupID application in ServiceNow. The GroupID Configuration node (Figure 18) is visible to such users.
 - **User** – This role can use the GroupID application in ServiceNow but does not have the privilege to configure the application.

The actions that a user can perform in the GroupID application are controlled by the identity store permissions granted to the security role assigned to the user in GroupID.

7. Select an attribute from the **Attribute** list to support auto login. This attribute is mapped to the attribute selected on the **Third Party Configuration** tab (Figure 6). When the values of these attributes match, a ServiceNow user will be auto logged into the GroupID application.

See Auto login for details.

8. Copy the GroupID application ID and public key from the **Application ID** and **Public Key** boxes on the **Third Party Configuration** tab (Figure 6) and provide them in the respective boxes on the **Configure GroupID Application** page (Figure 19).
9. Click **Finish Setup**.

Manual versus auto login

While configuring the GroupID application in ServiceNow, the administrator can enable manual or auto login for ServiceNow users who want to access the GroupID application in ServiceNow.

Manual login

When a user, who is already logged into ServiceNow, accesses the GroupID application, he or she is directed to the **Dashboard** page for signing in.

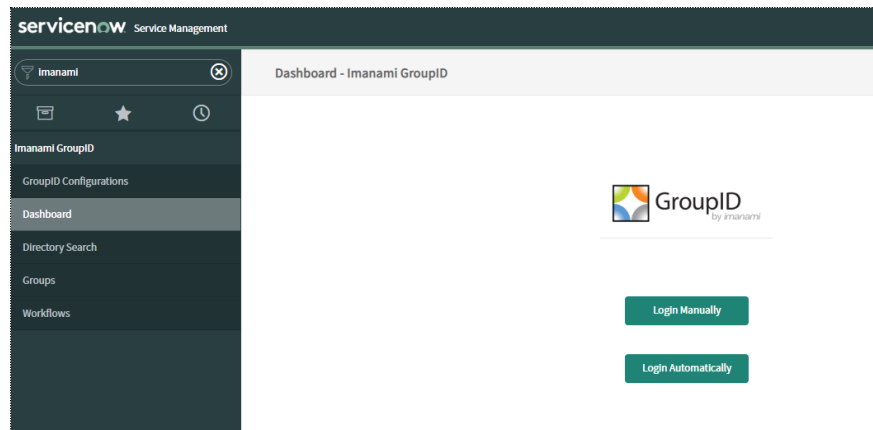


Figure 20: Dashboard

The user is presented with two options:

- **Login Manually**
On selecting this, the **GroupID Authenticate** dialog box is displayed, where the user has to select an identity store to connect to, and provide his or her identity store credentials to log into the GroupID application in ServiceNow.

When a single identity store is associated with the GroupID application, it is the default selection.

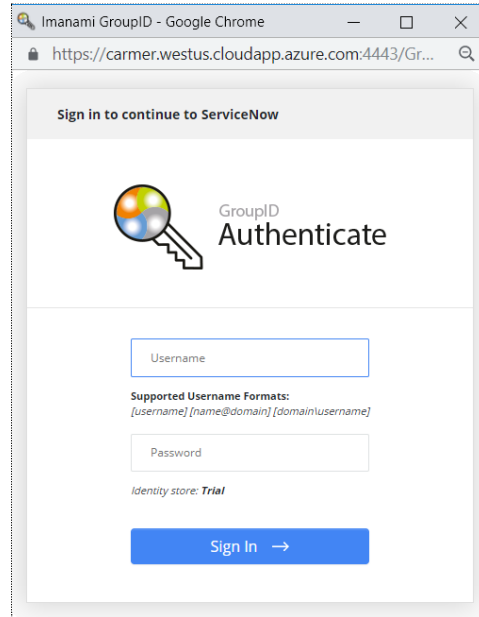


Figure 21: GroupID Authenticate dialog box

- **Login Automatically**
On selecting this, the user is automatically logged into the GroupID application. The process is the same as discussed under Auto login.

Auto login

When a user, who is already logged into ServiceNow, accesses the GroupID application, he or she is auto logged in.

Auto login works by taking the following into consideration:

- **Attribute mapping**

While configuring the GroupID application in ServiceNow, the administrator must specify an attribute, say Email (Figure 19). Similarly, in the GroupID application settings in GroupID, the administrator must specify an attribute, say Email (Figure 6).

To log a ServiceNow user into the GroupID application, the system looks up the values of these attributes in the ServiceNow database and an identity store (say, IS-A) respectively, thereby authenticating the user when the values match. The application connects to IS-A and the user is logged in.

- **Identity store selection**

With one identity store

When a single identity store (IS-A) is associated with the GroupID application, the system reads the attributes specified for value mapping, performs user authentication based on value matching, and connects the application to IS-A.

With multiple identity stores

When multiple identity stores (IS-A and IS-B) are associated with the GroupID application, the application connects to the identity store with the highest priority. The order in which identity stores are listed on the **Identity Stores** tab (Figure 4) determines their priority, with the identity store at the top having the highest priority.

Suppose the identity stores are listed in the order:

IS-A
IS-B
IS-C

IS-A has the highest priority while IS-C has the lowest.

For auto login, the system attempts to authenticate a user in the identity store with the highest priority. It reads the attributes specified for value mapping, performs user authentication based on value matching, and connects the application to IS-A.

However, if the attributes' values do not match in IS-A (indicating that the user does not exist in IS-A), the system takes the next identity store in the priority line (IS-B) and attempts to authenticate the user on the basis of the attributes specified for value mapping, and connects the application to IS-B.

If the attributes' values do not match in IS-B, the same process is repeated with IS-C.

Once a user auto-logs into the GroupID application, he or she has the option to select another identity store and connect the application to it.

With a multi domain identity store

An identity store may have multiple domains, in which case a user is authenticated in the domain with the highest priority.

See Set domain priority for details.



For both manual and auto login, a user must fall in a security role that has the **External Application Authentication** permission set to 'Allow' in the respective identity store.

The GroupID application in ServiceNow

The Imanami GroupID application comprises of the following pages:

- **GroupID Configurations** (Figure 18)
Enables administrators to set up the GroupID application in ServiceNow.
- **Dashboard** (Figure 20)
Use this page to sign into the GroupID application (in case of manual login). For a logged-in user, it displays the user's profile, the number of workflow requests pending for action, and the number of expiring groups.

- **Directory Search**

Enables users to search the directory for user, group, contact, mailbox, and computer objects.

Figure 22: Directory Search page

Click an object displayed in the search results to view its properties.

Users can join and leave groups.

- **Groups**

Users can view the groups they own, be they active, expiring, expired, or deleted groups. Users can also view the groups they are a member of.

Type	Display Name	Description	Owner	Email	Expiration Date	Security
Deleted_AutoGroup	Deleted_AutoGroup	AutoGroup	AutoGroup			Private
Deleted_MailGroups	Deleted_MailGroups	MailGroups	AutoGroup	MailGroup@imanamitoken.com		Private
Expired_Deleted_Workflow Group	Expired_Deleted_Workflow Group	Workflow Group	AutoGroup			Private
Expired_Expired_Expired_Expired_Expired_my_group_1	my_group_1		AutoGroup			Private
Expired_Expired_Group 1	A public group		AutoGroup			Private
Expired_Expired_Group 2	A read private group		AutoGroup			Private

Figure 23: Groups page

Click a group to view its properties. Users can also expire and renew their groups.

- **Workflows**

Enables users to approve and deny workflow requests. The requests come from GroupID and the workflow rules, as specified in GroupID, apply to them.

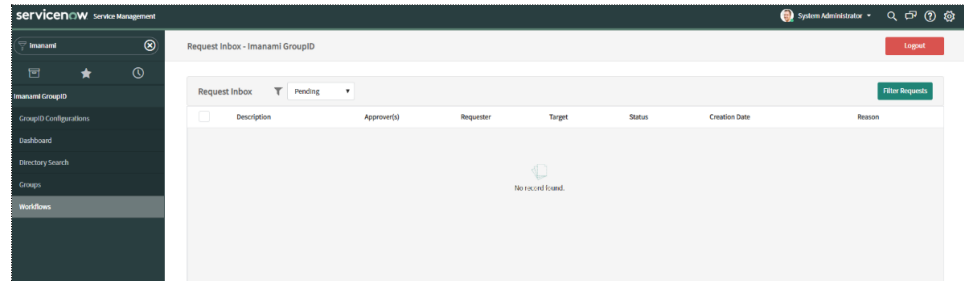


Figure 24: Workflows page



Users can perform actions in the GroupID application according to the permissions granted to their respective security roles in the connected identity store.

Style sheet customization

The GroupID application is published on the ServiceNow store and must be installed on a ServiceNow instance from there.

The style sheet for the GroupID application in ServiceNow is not customizable, since the administrator does not have access to the application's source code.

User authentication controls

For a user to authenticate on the GroupID application in ServiceNow, the following checks apply:

- The [External Application Authentication permission](#) must be enabled for the user's security role in an identity store. This should essentially be the identity store the GroupID application is being connected to.
- (For auto login) The values of the [mapped attributes](#) must match for the user in ServiceNow and in the identity store that the GroupID application is being connected to.
- If the administrator has specified [IP address\(es\)](#), the user can only access the GroupID application in ServiceNow from a machine having one of the listed IP addresses.



GroupID
by imanami

Imanami Corporation

2301 Armstrong Street
Livermore, CA 94551
United States

<https://www.imanami.com/>

Support: (925) 371-3000, Opt. 3
support@imanami.com

Sales: (925) 371-3000, Opt. 1
sales@imanami.com

Toll-Free: (800) 684-8515
Phone: (925) 371-3000
Fax: (925) 371-3001