# GroupID
by *imanami* | NOW PART OF netwrix

Version 10

GroupID
Authenticate

GroupID
Automate

GroupID
Self-Service

GroupID
Synchronize

GroupID
Password Center

GroupID
Insights

GroupID
Mobile App

GroupID
Reports

# User Guide
## GroupID Mobile Service

GroupID
by *imanami* | NOW PART OF netwrix

# Contents

# Chapter 1 – GroupID Mobile Service: An Introduction

GroupID Mobile Service lets you quickly configure the GroupID app for smartphones.

The GroupID app provides a mobile interface to an identity store. Using it, users can do the following on their phones:

- Search the directory

- Validate their directory profiles

- Enroll their identity store accounts

- Join or leave a semi-private or public group

- View the groups that the user owns as well as groups the user is a member of

- Approve or deny workflow requests

- Make a phone call or send email to a user or contact

- Change account password

- Reset account password

- Unlock an account

To secure access to the app, the administrator can enable the following layers of security:

- Multifactor Authentication

- Second Factor Authentication

Administrators maintain complete control over the app, since they can configure what users can view and do using the app. Administrators can specify both server-end and design-level configurations for the app.

The Android, Windows, and iOS versions of the GroupID app have been published on Google Play, Windows Store, and App Store respectively. To install and configure it, see  Chapter 4 - Set up the Mobile app on a Smartphone.

## App logs

Actions performed in the GroupID app 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 GroupID Mobile Service is also created at the location:

[GroupID 10 installation directory]:\GroupIDMobileService\Templates\Web\Logs\

See Manage file logging on page 6 for details.

# Chapter 2 – Server Configurations

The GroupID Mobile service is a web service that is hosted on a site in IIS. It allows the GroupID app to connect to the GroupID server, enabling it to work on your smartphone.

> **NOTE** The GroupID app can connect with GroupID Mobile service over HTTP and HTTPS. For HTTPS, a security certificate from a trusted certification authority is required.

In GroupID Management Console, you can:

- View the name of the GroupID Mobile service endpoint and the service URL. This URL is used to configure the app on users' phones.

- Move the GroupID Mobile service under a different website in IIS.

- Set file logging for the GroupID Mobile service.

- Associate and dissociate identity stores with the app.

## View the mobile service endpoint name

You can view the name of the GroupID Mobile service endpoint.

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Server**.

2. On the **General** tab, the **Virtual server display name** box displays the name of the GroupID Mobile service endpoint.
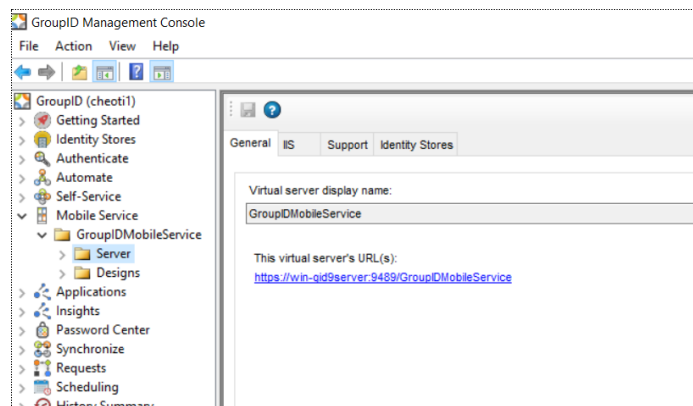


Figure 1: General tab

# View the GroupID Mobile Service URL

The URL for the GroupID Mobile service enables you to configure the service endpoint in the mobile app.

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Server.**

2. Click the **General** tab (Figure 1).
   The GroupID Mobile service URL is displayed under **This virtual server's URL(s)**.

   This URL launches the GroupIDMobileService page in a web browser, which displays a QR code. Users can configure the GroupID app on their phones by scanning the QR code. See Scan the QR code.

# View the physical path to the service folder

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

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Server**.
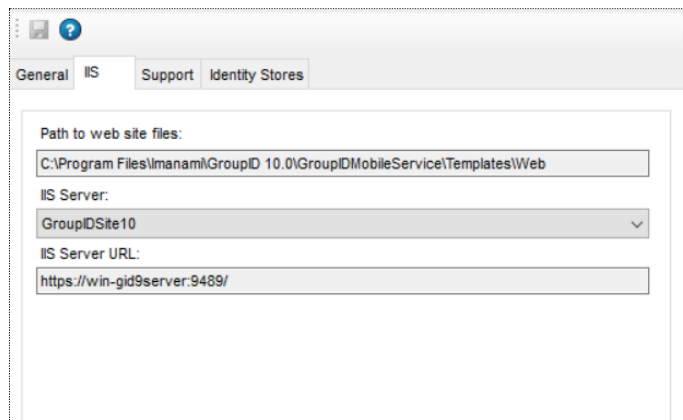
2. Click the **IIS** tab.



Figure 2: IIS tab

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

# Change the IIS site for the GroupID Mobile service

The GroupID Mobile service for the GroupID app is hosted on a website in IIS on the GroupID server machine.

On the **IIS** tab, you can move the GroupID Mobile service under a different site in IIS. In such an instance, the service URL and the IIS server URL also change. These URLs are used to configure the GroupID app on users' phones. You must provide the new URLs to your GroupID app users, so they can re-configure the app.

**To change the IIS site:**

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Server**.

2. Click the **IIS** tab (Figure 2).
   The **IIS Server** box displays the IIS site that hosts the GroupID Mobile service for the GroupID app.

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

The URL for IIS server that hosts the GroupID Mobile Service enables users to configure the GroupID app on a smartphone.

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Server**.

2. Click the **IIS** tab (Figure 2).
   The **IIS Server URL** box displays the URL of the IIS web server that hosts the GroupID Mobile service for the GroupID app.

   Users must enter this URL in the **Enter Server URL** page of the app (Figure 17) to connect the GroupID app to the server.

# Manage file logging

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

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

 [GroupID 10 installation directory]:\GroupIDMobileService\Templates\Web\Logs\

File Logging uses the Rollover Logging mechanism to log events. This mechanism logs events in a text file named GroupID10-Mobile-Service. 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 GroupID10-Mobile-Service. 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 GroupID Mobile 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 **Mobile Service > GroupIDMobileService > Server**.

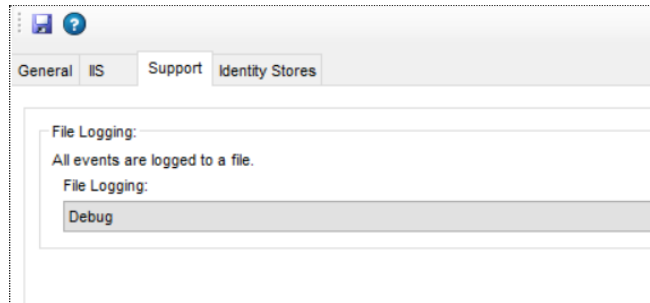2. Click the **Support** tab.

Figure 3: Support tab

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

   Select *Off* to turn off file logging.

4. On the toolbar, click **Save** 🖫.

# Associate an identity store with the app

You must associate one or more identity stores with the mobile app. While logging into the app, users must select an identity store from the available list to connect the app to.

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

**To associate an identity store with the mobile app:**

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Server**.
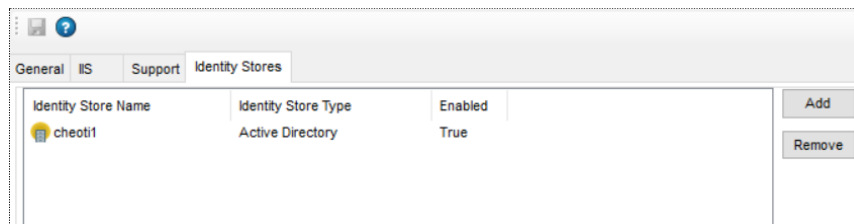
2. Click the **Identity Stores** tab.


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 app and click **OK**.

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

5.  On the toolbar, click **Save** 💾.

**To remove an identity store**

1.  On the **Identity Stores** tab, select the identity store you want to remove and click **Remove**. Users will not be able to connect to this identity store using the app.

2.  On the toolbar, click **Save** 💾.

# Chapter 3 – Design Configurations

The GroupID mobile app comes with a default design template, where a few fields are available on the app's pages. However, you can customize the pages by adding and removing fields.

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

You can customize the following design features:

- Directory Search: specify the schema attributes on which directory search can be performed in the app. You can also control the fields to be displayed on the search results pages in the app.

- Object Properties: control what properties of directory objects (user, group) you want to display in the app.

- Functionality: grant permissions on different features of the app to security roles in an identity store.

- Property Validation: manage the fields (schema attributes) that users must review and update while validating their profiles using the app.

## Customize the search feature

In the GroupID mobile app, users can search for directory objects (groups, users, contacts) in the connected identity store. You can specify the schema attributes users can perform search on.

You can also customize the search results pages for user/contact and group search by adding and removing fields. However, you cannot add new pages.

The contact object type is not supported in a Microsoft Azure based identity store.

## Customize directory search in the app

In the GroupID mobile app, users can search for directory objects (groups, users, contacts) in an identity store.

You can specify the schema attributes users can perform search on. When a user enters a search string, the values of all specified attributes would be matched to return the results.

You can also specify a search operator that determines what part of the attribute value should match the search string.

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2. Select an identity store to customize the app design for it.
   All identity stores associated with the app are listed under **Designs**. You can design a different app for each of these.

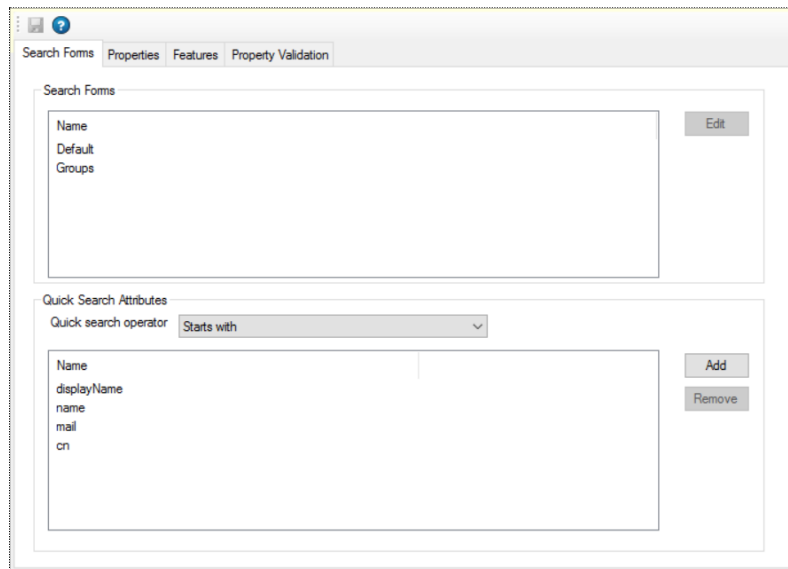3. Click the **Search Forms** tab.



Figure 5: Search Forms tab

In the **Quick Search Attributes** area, the **Name** column lists the schema attributes whose values will be matched when a user enters a search string in the app's directory search box.

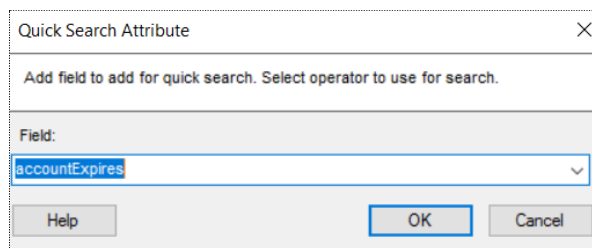4. Click **Add** to add a new attribute to this list.



Figure 6: Quick Search Attributes dialog box

5. On the **Quick Search Attribute** dialog box, select a schema attribute from the **Field** drop-down list and click **OK**.

   The attribute is displayed in the **Name** column in the **Quick Search Attributes** area.

   To remove an attribute from the list, select it and click **Remove**.

6. From the **Quick search operator** drop-down list, select an option.

   - **Equal** - looks up the values of all attributes listed in the *Name* column and returns records that have a value exactly matching the search string.

   - **Contains** - looks up the values of all attributes listed in the *Name* column and returns records that have a value that contains the search string. In other words, the search string is contained anywhere in the value.

   - **Starts with** - looks up the values of all attributes listed in the *Name* column and returns records with values starting with the search string.

   - **Ends with** - looks up the values of all attributes listed in the Name column and returns records with values ending with the search string.

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

## Edit a field on a search results page

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs.**

2. Select an identity store to customize the app design for it.
   All identity stores associated with the app are listed under **Designs**. You can design a different app for each of these.

3. Click the **Search Forms** tab (Figure 5).

4. In the **Search Forms** area, these search results pages are listed for customization:

   - For group search, the **Groups** page displays the search results.

   - For user and contact search, the **Default** page displays the search results.

   Select a search results page to modify its field(s) and click **Edit**.
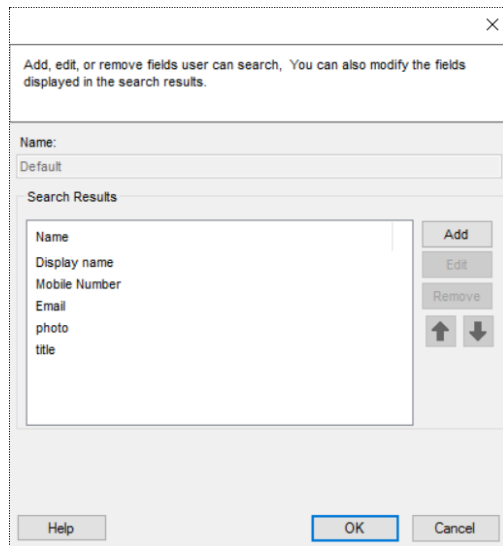
Figure 7: Edit Search Forms dialog box

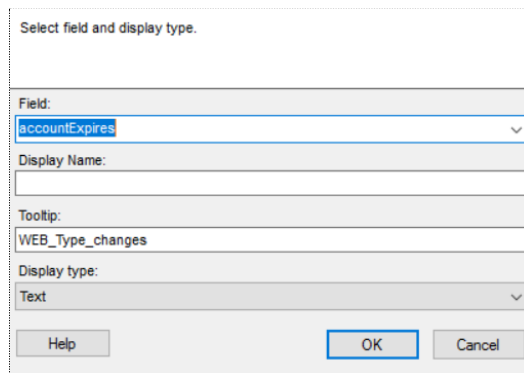5. On the dialog box, select a field to modify it and click **Edit**.



Figure 8: Edit Field dialog box

6. Modify the information as required and click **OK**:

- **Field** – The schema attribute linked to the selected field. The field displays the value of this attribute.

- **Display Name** - The field's label displayed in the app.

- **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 app.

7. Click **OK** to close the **Edit Search Forms** dialog box (Figure 7).

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

# Add a field to a search results page

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2. Select an identity store to customize the app design for it.
   All identity stores associated with the app are listed under **Designs**. You can design a different app for each of these.

3. Click the **Search Forms** tab (Figure 5).

4. In the **Search Forms** area, select a search results page to add field(s) to it and click **Edit**.

5. On the **Edit Search Forms** dialog box (Figure 7), click **Add**.
   The **Add Field** dialog box is displayed, which is similar to the **Edit Field** dialog box (Figure 8).

6. Provide the following information for the new field and click **OK**:

   - **Field** – Select a schema attribute to link to this field. The field will display the value of this attribute.

   - **Display Name** – Type a label for the field. This label is displayed as the name of the field in the app.

   - **ToolTip** - Type the text to be displayed when a user hovers the pointer over the field.

   - **Display type** – Select a display type to render the field in the app.

7. Repeat steps 5 and 6 for each new field to be added to the search results page.

8. Click **OK** to close the **Edit Search Forms** dialog box (Figure 7).

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

# Remove a field from a search results page

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2. Select an identity store to customize the app design for it.
   All identity stores associated with the app are listed under **Designs**. You can design a different app for each of these.

3. Click the **Search Forms** tab (Figure 5).

4. In the **Search Forms** area, select a search results page to remove a field from it and click **Edit**.

5. On the **Edit Search Forms** dialog box (Figure 7), select a field and click **Remove**.

6. Click **OK** to close the **Edit Search Forms** dialog box (Figure 7).

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

# Customize Object Properties pages

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

- Users/Contacts

- Groups

You can customize the property page for an object by specifying the fields (attributes) to display for that object in the app.

The contact object type is not supported in a Microsoft Azure based identity store.

# Add a new field

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2. Select an identity store to customize the app design for it.
All identity stores associated with the app are listed under **Designs**. You can design a different app for each of these.
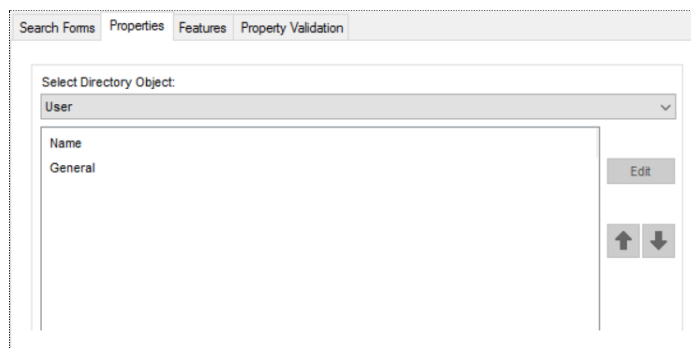
3. Click the **Properties** tab.



Figure 9: Properties tab

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**.

Edit Design Category

Categories are used to display fields.  Use the Access Level to determine who can modify the fields in the Category and the Visibility Level to determine who can view the Category.

Name:

WEB_General

Fields

Name
First name
Initials
Last name
Title
Company
City
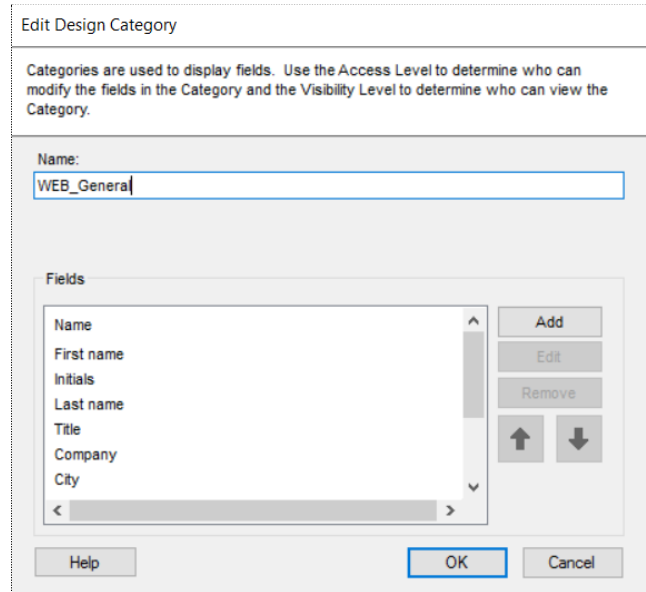
Add
Edit
Remove

Help     OK     Cancel

Figure 10: Edit Design Category dialog box

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

Add Field     ✕

Select a field and Display Type.

Field:

accountExpires

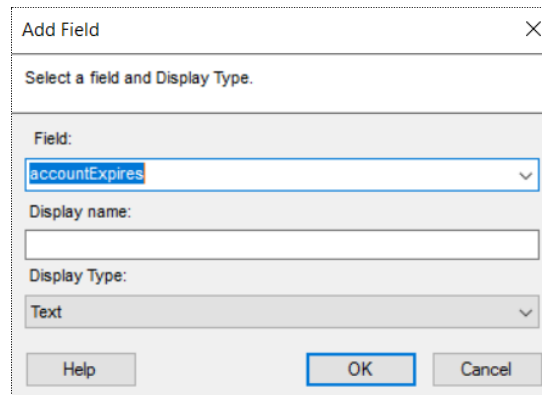Display name:

Display Type:

Text

Help     OK     Cancel

Figure 11: Add Field dialog box

7. On the **Add Field** dialog box, provide the following information for the new field and click **OK**:

- **Field** – Select a schema attribute to link to the field. The field will display the value of this attribute.

- **Display Name** - Type a label for the field. This label is displayed as the name of the field in the app.

- **Display Type** – Select a display type that would be used to render the field in the app.

8. Repeat steps 6 and 7 for each new field to be added to the properties page.

9. Click **OK** to close the **Edit Design Category** dialog box (Figure 10).

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

# Edit a field

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2. Select an identity store to customize the app design for it.
   All identity stores associated with the app are listed under **Designs**. You can design a different app for each of these.

3. Click the **Properties** tab (Figure 9).

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**.

6. On the **Edit Design Category** dialog box (Figure 10), the **Fields** area displays the fields available on the properties page. Select the field you want to edit and click **Edit**.

   The **Edit Field** dialog box is displayed, which is similar to the **Add Field** dialog box (Figure 11).

7. Modify the required information for the selected field and click **OK**:

   - **Field** – The schema attribute linked to the field. The field displays the value of this attribute.

   - **Display Name** - The field's label displayed in the app.

   - **Display Type** – The display type used to render the field in the app.

8. Click **OK** to close the **Edit Design Category** dialog box (Figure 10).

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

# Remove a field

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2. Select an identity store to customize the app design for it.
   All identity stores associated with the app are listed under **Designs**. You can design a different app for each of these.

3. Click the **Properties** tab (Figure 9).

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**.

6. On the **Edit Design Category** dialog box (Figure 10), the **Fields** area displays the fields available on the properties page. Select a field and click **Remove**.

7. Click **OK** to close the **Edit Design Category** dialog box (Figure 10).

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

# Grant permissions to user roles on the app

For each identity store in GroupID, three user roles are defined by default, namely, Administrator, Helpdesk, and User.
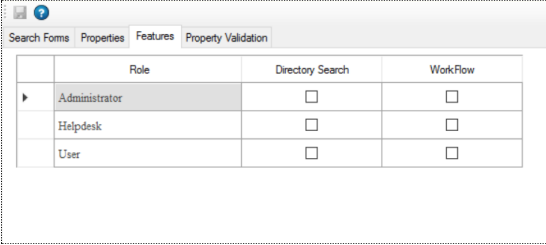
In a Microsoft Azure based identity store, the Administrator and User roles are available by default.

You can grant permissions on the GroupID app to each user role within an identity store, so that role members can access the permitted features only.

**To grant permissions to user roles:**

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2. Select an identity store to grant permissions to its user roles on the app.
   All identity stores associated with the app are listed under **Designs**. You can grant permissions on the app for each of these.

3. Click the **Features** tab.

Figure 12: Features tab

All user roles defined in the identity store are listed in the **Role** column. You can grant permissions to a role on the following app features:

- **Directory Search**: Enables role members to search the directory.

- **Workflow**: Enables role members to view the workflow requests.

4. To grant permission to a role on a function, select the check box for that function.
   To deny permission to a role on a function, clear the check box for that function.

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

# Manage Property Validation

Use the **Property Validation** tab to manage the fields that are displayed on the **Validate Profile Properties** page of the GroupID mobile app. App users can validate and update their directory profile information on this page.

On the **Property Validation** tab, a few fields for profile validation are specified by default. You can add more fields, edit the existing fields, and even remove them. However, the *My Direct Reports* field cannot be edited or removed.

# Add a new field

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2. Select an identity store to manage the profile validation fields available in the app.
   All identity stores associated with the app are listed under **Designs**. You can manage profile validation fields for each of these.

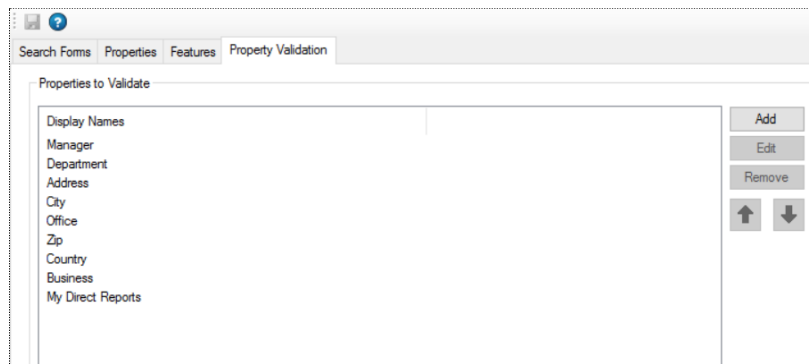3. Click the **Property Validation** tab.



Figure 13: Property Validation tab

All fields currently available on the Validate Profile Properties page of the GroupID mobile app are listed under **Display Name**.

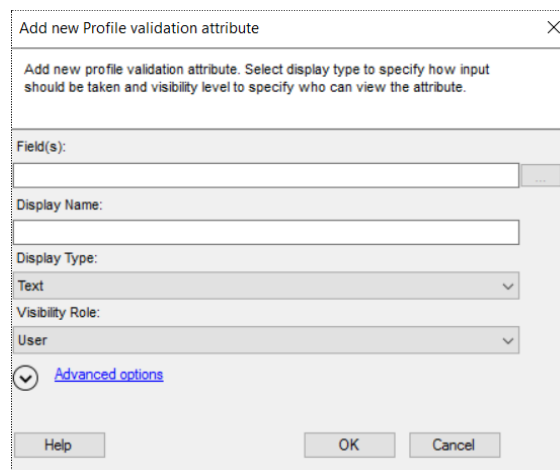4. Click **Add** to add a new field.



Figure 14: Add new Profile Validation Attribute dialog box

5. Click the ellipsis button next to the **Field(s)** box to launch the **Select Profile Validation Attributes** dialog box, where you can select one or more schema

attributes. For each of these attributes, a separate field would be displayed on the **Validate Profile Properties** page in the mobile app.
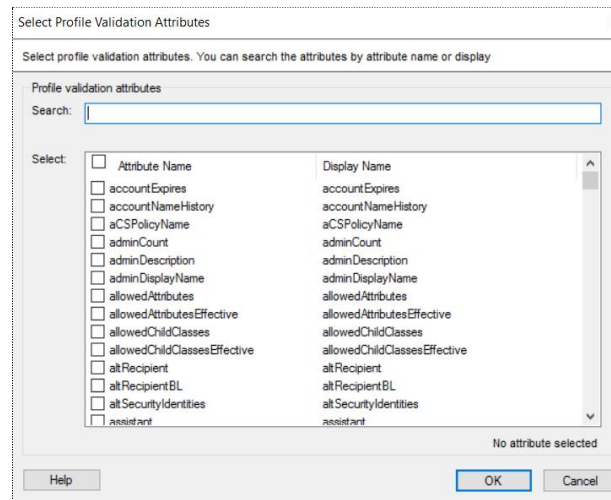


Figure 15: Select Profile Validation Attributes dialog box

- Use the **Search** box to filter the schema attributes listed in the **Select** area.

- Select the check boxes for the attributes you want to display in the app for profile validation.

- Click **OK**.

6.  In the **Display Name** box, specify a name to display for the field in the app. This box is not available when you select multiple attributes in the **Field(s)** box.

7.  From the **Display Type** drop-down list, select the display type to use for rendering the field(s) in the app.
    When multiple attributes are selected in the **Field(s)** box, this display type applies to each of them.

8.  From the **Visibility Role** drop-down list, select a security role. The field(s) 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(s) from all users.

- Select **Manager and Owner** to make the field(s) visible only to the user's manager. They would not even be visible to the user.
  For example, if the *Manager and Owner* role is selected for the *Manager* field on the *Validate Profile Properties* page, the field would be visible to user managers for their respective direct reports.

- Select **Self** to make the field(s) visible only to the logged-in user. It would not be visible to any other user, such as the user's manager or a role with a higher priority value.

The visibility role determines the roles whose members can view the field(s) in the app. The **Visibility Role** list contains all security roles defined for the identity store along with two hard-coded roles: **Manager and Owner** and **Self**.

NOTE Each security role in an identity store is assigned a priority value in the 1-99 range, where 1 is the highest and 99 is the lowest value. Role priority is unique for each role in an identity store, and determines which role is higher than the other.

9. Click **Advanced options** to enter further details for the field(s).

10. As mentioned for **Visibility Role**, the field(s) are visible to members of the selected role and roles having a priority value higher than the selected role.

    Use the *Exclude Role* option to exclude a higher priority role or roles from getting visibility on the field.

    In the **Exclude Role** area, select the check boxes for the roles you want to deny visibility on the field(s).

11. In the **ToolTip Text** box, type the help text that would appear when a user hovers the mouse over the field.
    This box is not available if you select multiple attributes in the **Field(s)** box.

12. In the **Max Length** box, enter a number that represents the maximum number of characters that can be entered as value for each of the selected field(s).
    Entering *0* indicates it can accept an unlimited number of characters as value.

13. Select the **Is Read Only** check box if the field(s) are meant to be read-only.

14. Select the **Is Required** check box to force the user to provide a value for the field(s).

15. Click **OK** to close the **Add new profile validation attribute** dialog box.

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

## Edit a field

1. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2.  Select an identity store to manage the fields that would be available in the app for user profile validation.
    All identity stores associated with the app are listed under **Designs**. You can manage profile validation fields for each of these.

3.  Click the **Property Validation** tab (Figure 13).
    All fields currently available on the Validate Profile Properties page of the GroupID mobile app are listed under **Display Name**.

4.  Select a field to edit it and click **Edit**.

5.  The **Edit Profile Validation Attribute** dialog box is displayed, which is similar to the **Add new Profile Validation Attribute** dialog box (Figure 14). Modify the required information and click **OK**:

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

NOTE    You cannot edit the *My Direct Reports* field.

# Remove a field

1.  In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Designs**.

2.  Select an identity store to manage the fields that would be available in the app for user profile validation.
    All identity stores associated with the app are listed under **Designs**. You can manage profile validation fields for each of these.

3.  Click the **Property Validation** tab (Figure 13).
    All fields currently available on the Validate Profile Properties page of the GroupID mobile app are listed under **Display Name**.

4.  Select the required field and click **Remove**; then click **Yes** on the confirmation dialog box.

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

NOTE    You cannot remove the *My Direct Reports* field.

# Chapter 4 – Set up the Mobile app on a Smartphone

To use the GroupID mobile app, a user must do the following:

- Install the Imanami GroupID app on a smartphone.

- Configure the app by connecting it to the GroupID server.

Complete these simple steps and start using the app.

## Install the GroupID app

The Android, Windows, and iOS versions of the GroupID Mobile app are available on Google Play, Windows Store, and App Store respectively.

1. Go to the relevant store on your smartphone and search for **Imanami GroupID**.
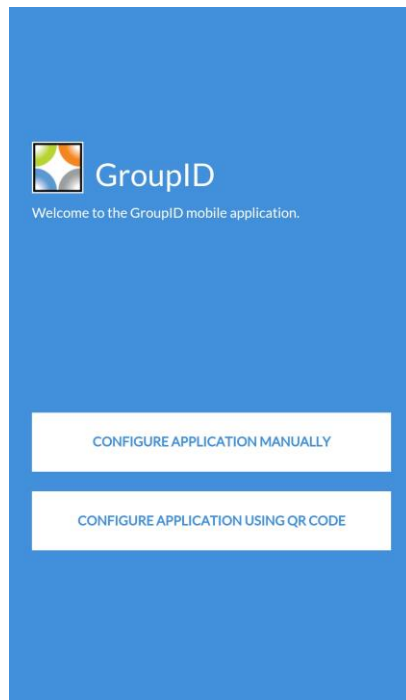
2. Install the app and launch it on your phone.



Figure 16: GroupID Mobile app - Welcome page

# Configure the app

The GroupID Mobile service for the GroupID app is hosted on the IIS server running on the GroupID machine. To connect the mobile app on a smartphone to the server, you must register the IIS server URL with the app. Choose any of the following methods to do so:

- Enter the web server URL manually in the app, or

- Scan a QR code with your phone.

## Manually provide the IIS server URL

To connect the GroupID app to the IIS web server that hosts the service for the app, you can manually enter the server URL in the app.

1. Launch the GroupID Mobile app on your smartphone and tap **Configure Application Manually** on the **Welcome** page (Figure 16).

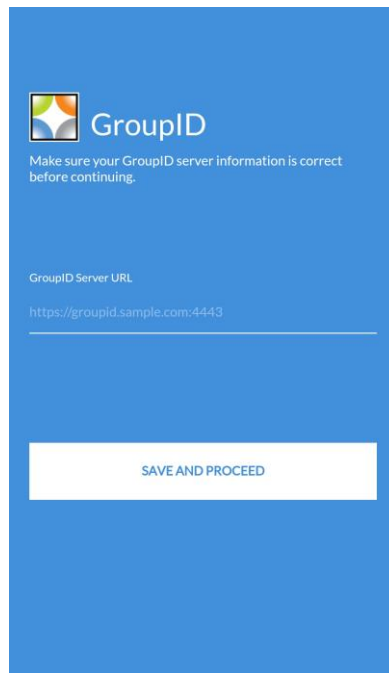   The following page is displayed:

   

Figure 17: Enter server URL page

2. In the **GroupID Server URL** box, provide the URL of the IIS web server that hosts the service for GroupID mobile app.

This URL is displayed in the **IIS Server URL** box on the **IIS** tab (Figure 2), so provide it to your users for configuration purpose.

3. Tap **Save and Proceed**.
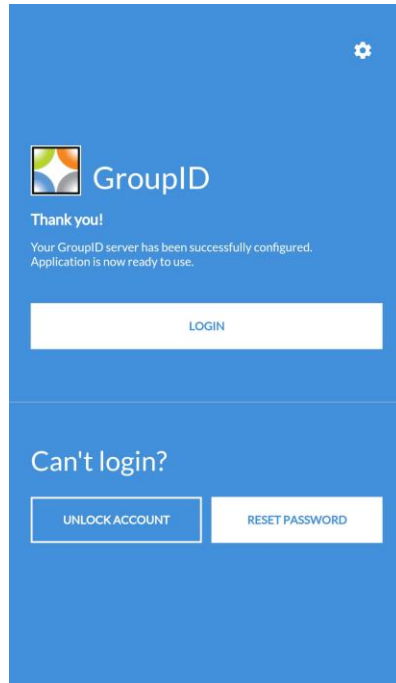The app validates the URL and on success, the **Login** page is displayed.



Figure 18: Login page

Log into the app and start using it.

## Scan the QR code

The QR code is an easy way to configure the GroupID app. Simply open the GroupIDMobileService page containing the QR code in a web browser and scan this code with your smartphone.

4. In GroupID Management Console, select **Mobile Service > GroupIDMobileService > Server**.

5. On the **General** tab (Figure 1), click the URL displayed under **This virtual server's URL(s)**. or provide it to your users, so they can use it to launch the GroupIDMobileService page in a web browser.
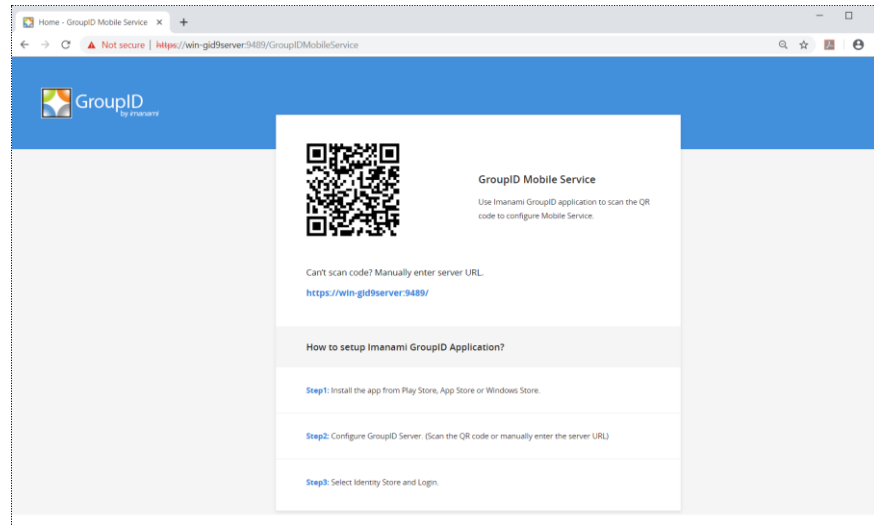
Figure 19: GroupIDMobileService page

6. Now launch the GroupID Mobile app on your smartphone and tap **Configure Application using QR Code** on the **Welcome** page (Figure 16).

7. Scan the QR code with your smartphone.
   On successful configuration, the **Login** page (Figure 18) is displayed.

Log into the app and start using it.

**Imanami | Now part of Netwrix**

6160 Warren Parkway, Suite 100,
Frisco, TX 75034,
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