Kony Fabric

Kony Fabric QuickStart Guide Series

Getting Started with Kony Fabric

Release V8

Revision History

Date	Document Version	Description of Modifications/Release
09/19/2017	1.0	Document published for V8 GA

1. Overview

Kony Fabric provides enterprise security and complex system integration services and allows developers to focus on building app experiences. This is accomplished by providing a powerful set of services to handle identity, integration, objects, orchestration, data sync, and engagement services. When these services are configured within Kony Fabric, they can easily be incorporated into a mobile application using any third-party app development tool using our SDKs or direct REST API interface.

Kony Fabric has multiple features that can be used - Identity, Integration, Objects, Orchestration, Sync , and Engagement. These features can be accessed via a common, centralized console.

For successful authentication with users, and to access centralized features of Kony Fabric, Kony recommends that you install the following Kony Fabric features for on-premises:

- Kony Fabric Identity and Console
- Kony Fabric Server
- Kony Fabric Engagement Services
- Kony Fabric Sync

The following are the five major services offered by Kony Fabric:

- **Identity**: Authenticate and authorize your app users including Salesforce, Active Directory, SAP, or other third-party identity providers that support Security Assertion Markup Language (SAML.)
- **Integration**: Securely connect your app to any back-end data using a variety of connectors for standard services such as REST, SOAP, and JSON end points and for enterprise connectors such as Salesforce and SAP. You can also build custom connectors using Java code to handle any atypical integration requirement.
- **Orchestration**: Optimize app performance or create new services by building server-side composite services and workflows including the ability to execute custom business logic.

- **Sync**: Enable apps to work offline by keeping a copy of relational data structures on the device. Securely synchronize changes between end-user devices and enterprise databases or web service-enabled systems.
- **Engagement Services**: Engage with your users over cross-platform push notifications, SMS, and email. This service includes the ability to track the effectiveness of messaging campaigns. You can also collect user information and behavior analytics to enable you to better target messaging based on user segmentation rules and location defined by geo-boundaries or iBeacons.

This Quick Start guide helps you through creating a basic set of back-end services for authenticating a user and then accessing a simple integration and orchestration service.

> ***Note:*** cURL - a command line tool for getting or sending files using URL syntax. This guide uses the cURL command to represent a mobile device making HTTPS API calls to a Kony Fabric environment. cURL is typically pre-installed on Linux and Mac systems.
> For Windows, go to http://curl.haxx.se/download.html, download cURL, and the SSL libraries required to connect to HTTPS URLs.
>
> For cURL commands and documentation, refer to http://curl.haxx.se/docs/

2. Accessing Kony Fabric Console

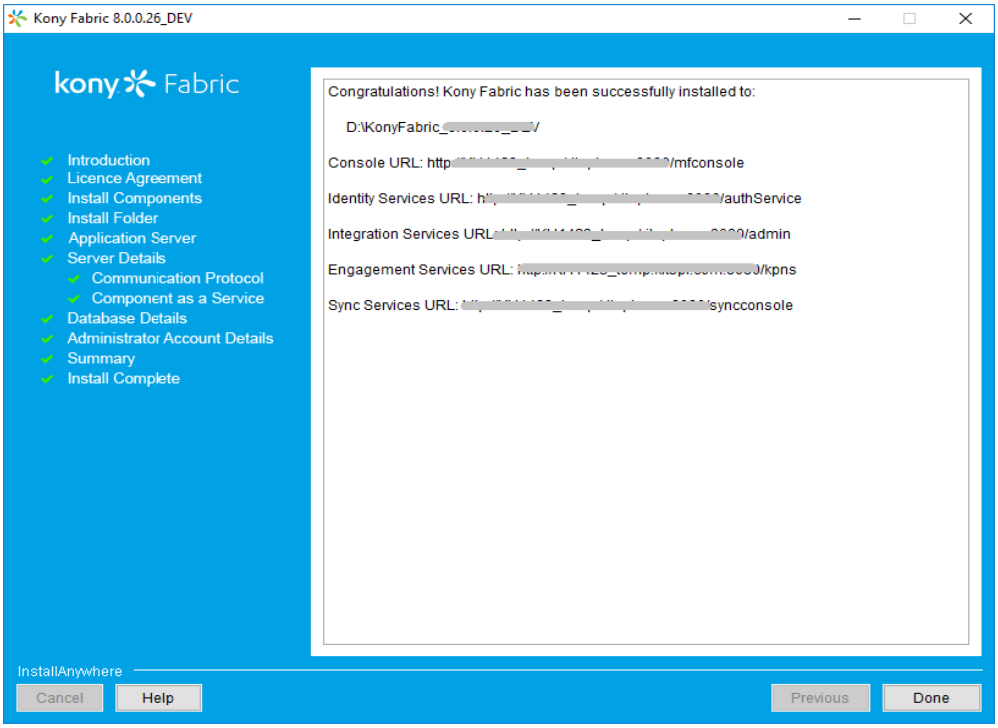
Before you use various Kony Fabric services, you must create a superuser.

To accessing Kony Fabric, follow these steps:

1. How to Get Started with Kony Fabric Console
2. How to Log In to Kony Fabric Console

2.1 How to Get Started With Kony Fabric Console

After installation, you need to configure identity services and create your administrator account. Based on your Kony Fabric installation, you will see the a list of URLs in the **Install Complete** window, shown below:

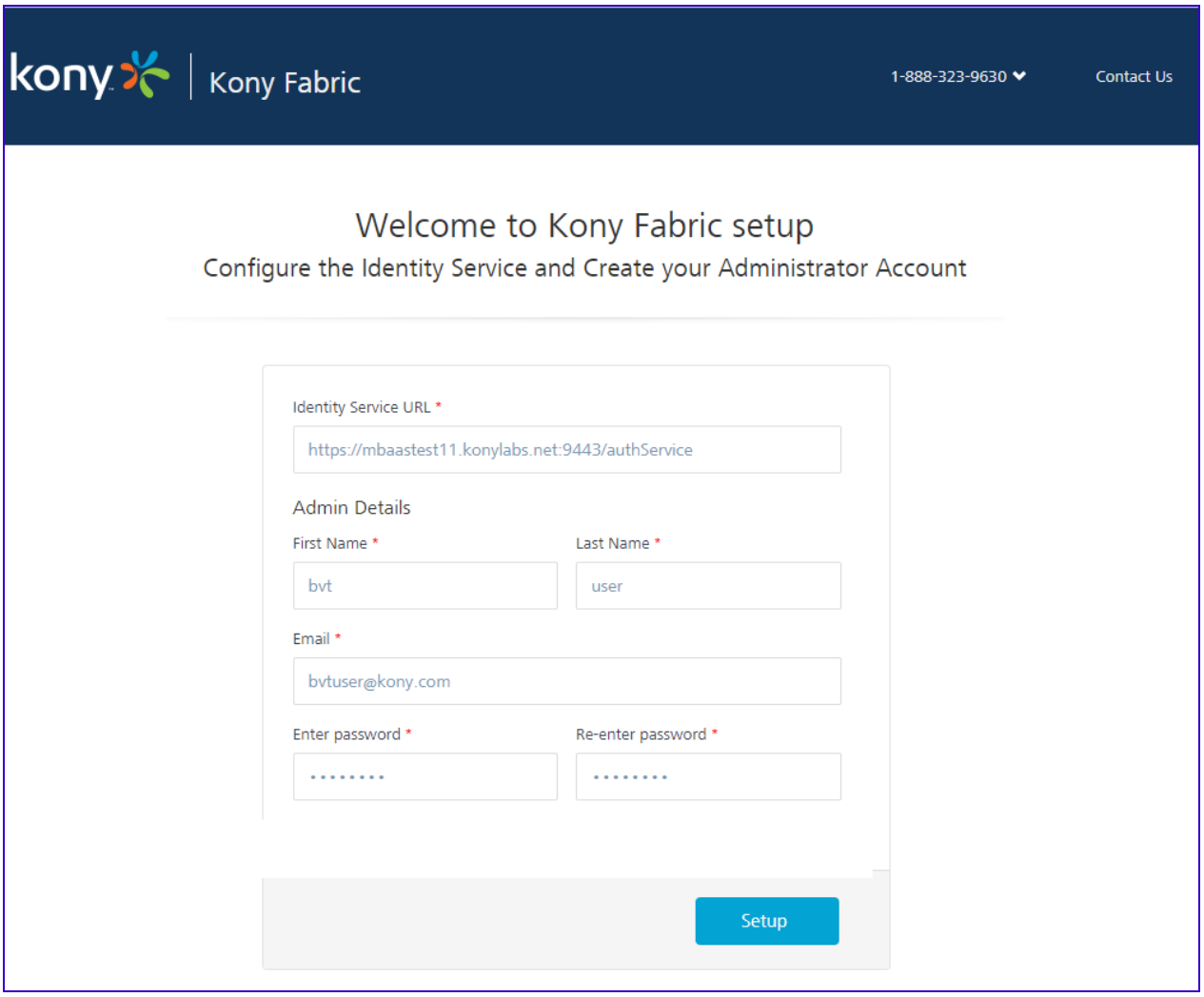


To launch Kony Fabric console, follow these steps:

1. From the **Install Complete** window, copy the URL from **Kony Fabric Console URL**, and then go the URL in your web browser.

> ***Note:*** To remember the URL of this portal, bookmark the URL by adding it to your favorites.

The **Welcome to Kony Fabric setup** page appears only if you have not already configured your identity services.



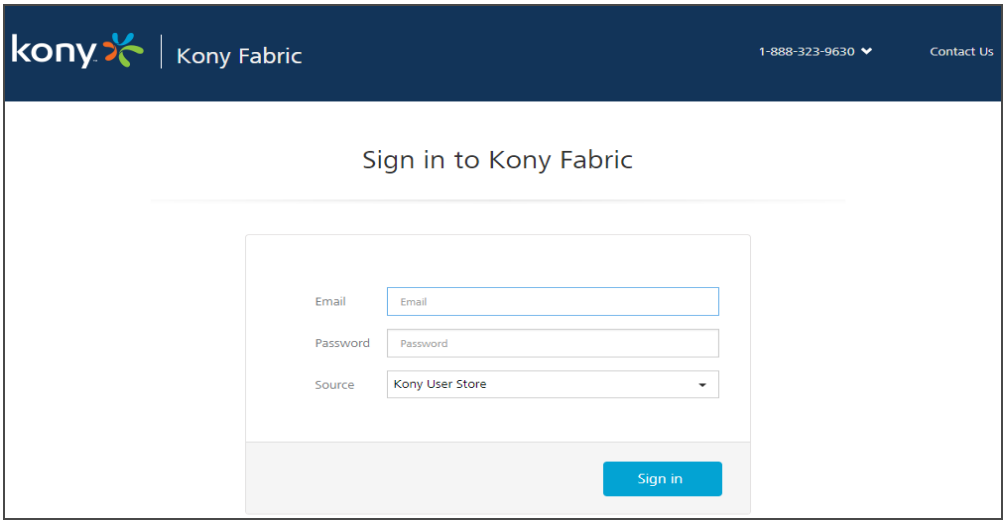
> ***Note:*** Fields marked with an asterisk are mandatory.

2. In **Kony Identity Service URL** text box, enter Kony Identity Service URL from the **Install Complete** page.
3. Under the **Kony Fabric Console Admin Details**, enter the following details:
    - **First Name**: Enter the first name of the user.
    - **Last Name**: Enter the last name of the user.
    - **Email**: Enter the email address of the user. It can include alphanumeric and special characters that follow standard email address form.
    - **Enter password**: Enter the password for the user. This is a string of characters that allows access to a system. It can be a combination of alphanumeric and special characters.
    - **Re-enter password**: Retype the password to ensure the user's identity.
4. Click **Setup**.
   Once the details are validated for one-time configuration, the system will:
    - Associate your credentials with Kony Fabric identity services and authorization services.
    - Display the **Sign in to your Kony Account** page.

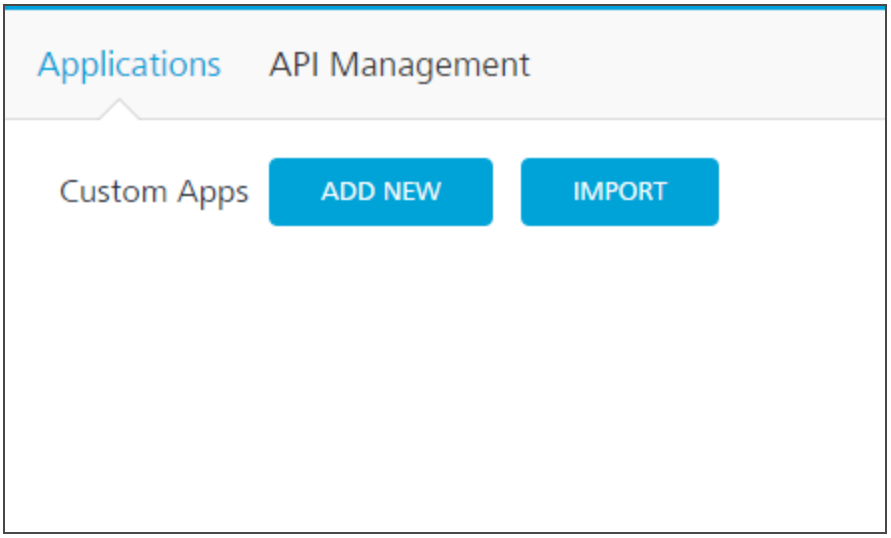
2.2 How to Log In to Kony Fabric Console

If you have configured identity services and created your administrator account (Kony Fabric superuser account), you can log in to the Kony Fabric console. A superuser will have owner permissions by default.

1. Go to **Kony Fabric Console URL** that you bookmarked in the previous section. The **Sign in to Kony Fabric** page appears.



2. Provide your Kony administrator account log-in credentials that you have created, and click **Sign in**.
   After validating your credentials, you are directed to your Kony Fabric account. By default, the **Apps** page appears.



From this page, you can navigate to consoles (app services, sync services, engagement services), applications, environments, and settings.

3. Environments

You need to create an environment to publish your apps. Environments can include at least one server or a combination of all such as Kony Fabric Server, Kony Fabric Engagement Services, Kony Fabric Sync, and Kony Fabric Management.

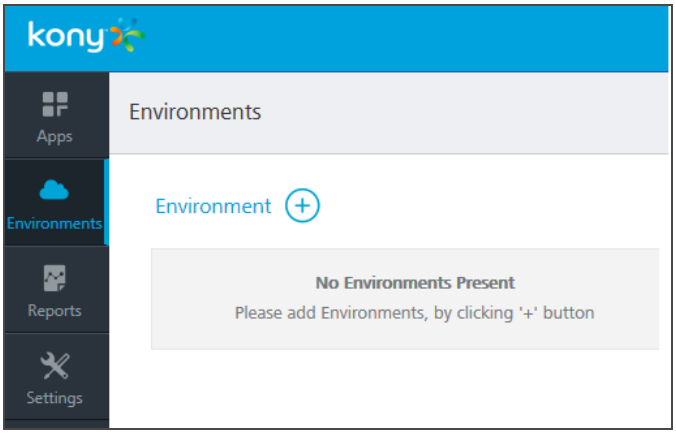
> *Important:* As a user, you must be an admin or owner to access the Environments page and perform different tasks based on the role.
>
> Ensure that your environments include all required servers that are part of an app.
>
> For example, if your environment contains only Kony Fabric Sync, and you try to publish an app with Kony Fabric Engagement Services, the system throws an error.

3.1 How to Add an Environment

You can add as many environments with different combinations of servers.

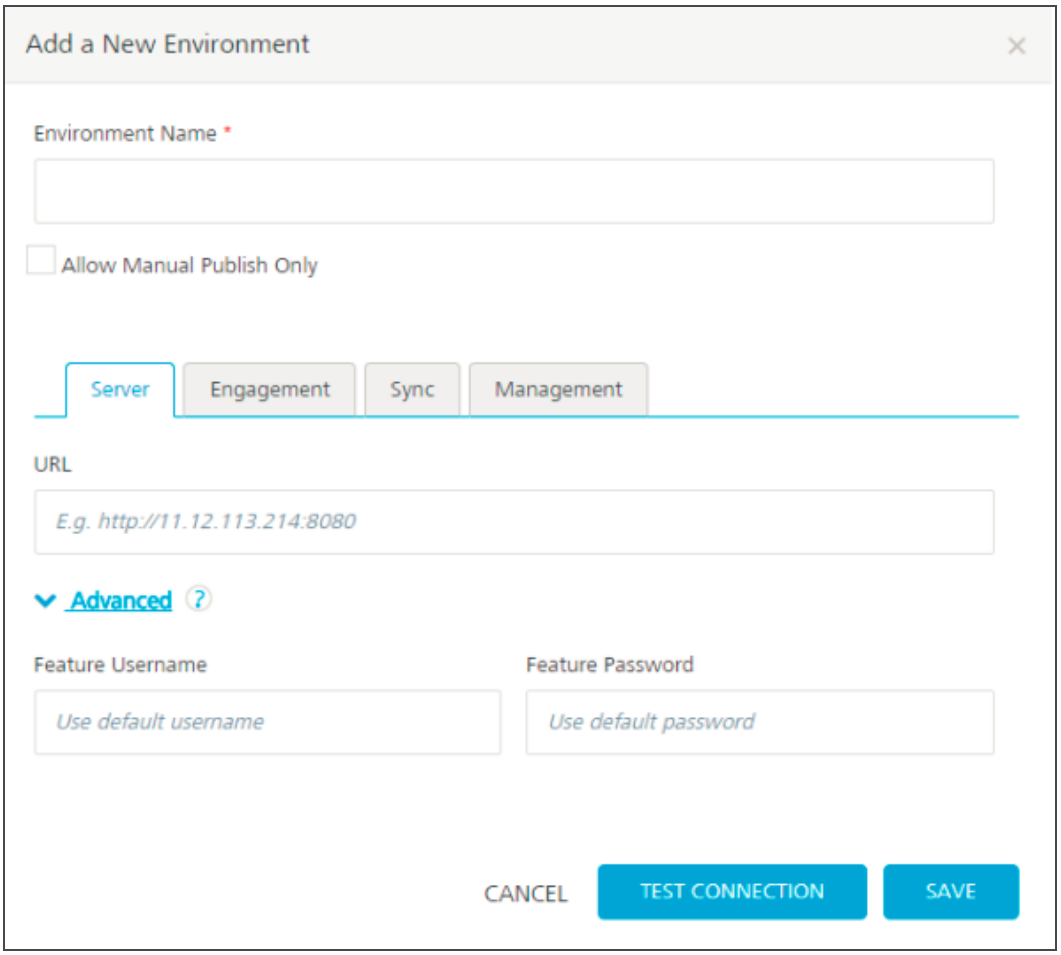
To add an environment, follow these steps:

1. In your Kony Fabric account, click **Environments**. The **Environments** page appears.



2. Click the **Add a New Environment** button.

3. In the **Add a New Environment**, enter an environment name.



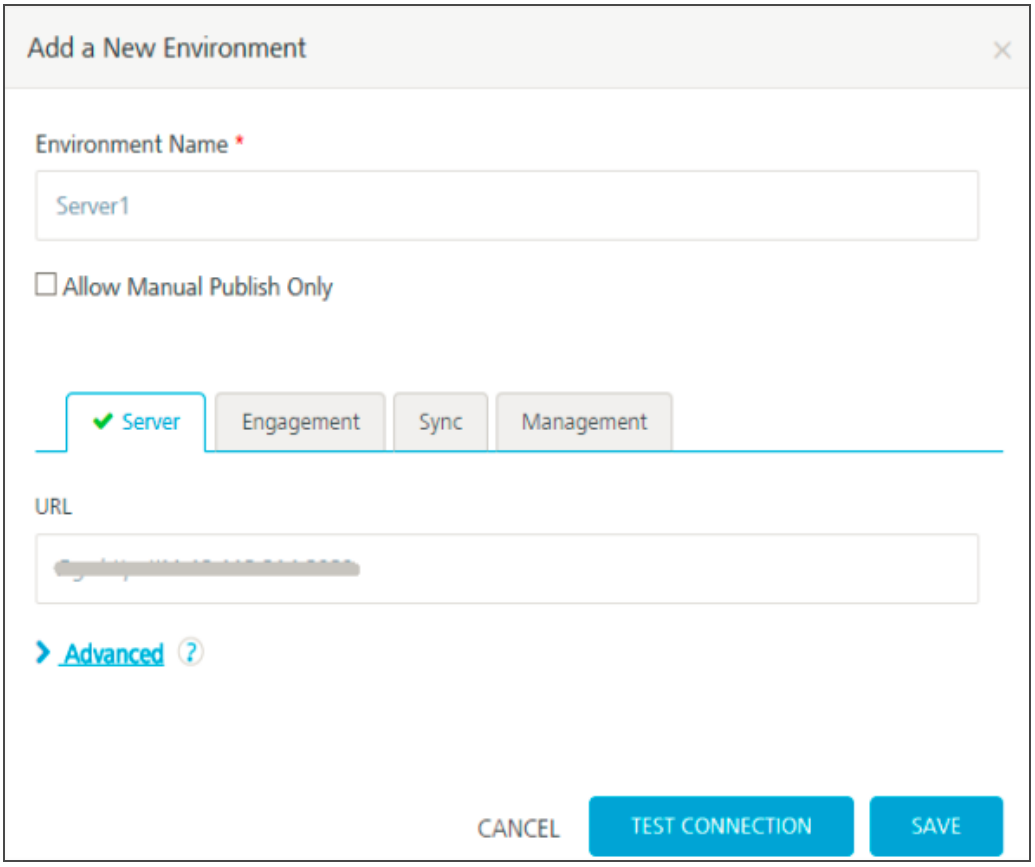
4. Select the **Allow Manual Publish Only** check box to confirm this environment to be a manual publish environment. By default, the **Allow Manual Publish Only** check box is cleared.

> ***Important:*** If you create an environment by selecting the **Allow Manual Publish Only** check box, in the **Publish** tab, the **Manual Publish** icon appears for the environment. The Manual Publish icon denotes that the environment is configured for manual publish. For more details about how to use manual publish, refer to the Publish the App section.

5. In the **Server** tab, provide the following details:
    - **URL**: Enter the URL for your Kony Fabric Server.
    - Under **Advanced**, do the following:
        - **Feature Username**: By default, this field shows the default username of Kony Fabric Server. You can modify if required.

          > ***Note:*** You need to modify the username and password only if these credentials are changed via the Kony Fabric Server console.

        - **Feature Password**: By default, this field shows the default password of Kony Fabric Server. You can modify if required.
6. To configure Kony Fabric Engagement Services or Kony Fabric Sync or Kony Fabric Management, click the respective tabs and enter details.
7. Once you enter details, click **Test Connection**. If the server details are correct, the system displays a check mark next to a service, shown below:



8. Click **Save** to apply the environment capabilities. The environment is created in the **Environments** page.

4. Creating Your Kony Fabric App

Adding a Kony Fabric app to your account creates a container or a logical wrapper around all the services you want to provide for your mobile app. Once your services are published, you will receive an App Key App Secret, and Service URL, which are used within your client app development tool to securely connect to your back-end Kony Fabric services. The App key, App secret, and Service URL are initialized through SDKs.

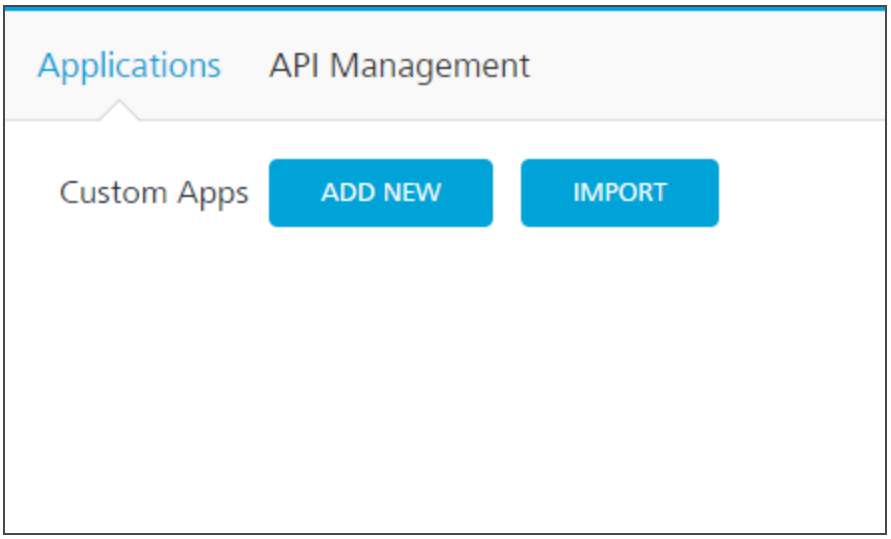
To create your Kony Fabric app, follow these steps:

1. Go to the **Kony Fabric Console URL** that you bookmarked in the How to Access Kony Fabric Console section.
2. In the Sign in to Kony Fabric page that appears, provide your Kony administrator account log-in credentials that you have created, and click **Sign in**.

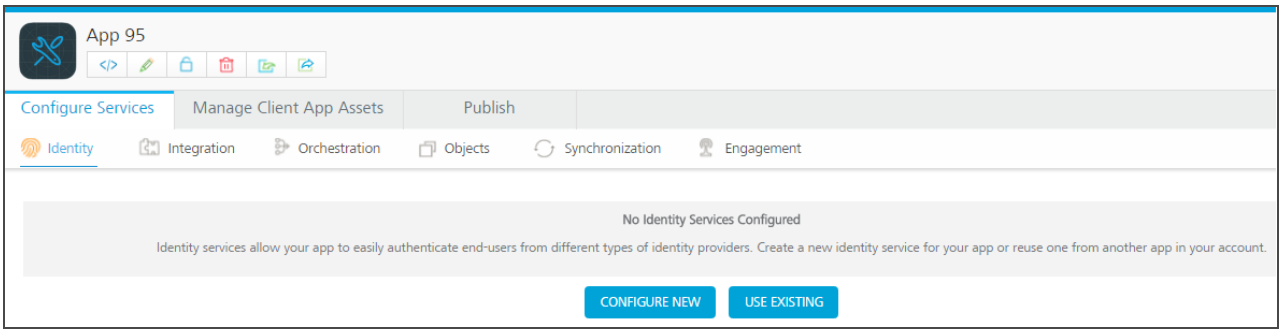
   > ***Note:*** For more details about how to get started and log in to console, refer to How to Access Kony Fabric Console.

   After validating your credentials, you are directed to your Kony Fabric account. By default, the Apps page appears.
3. Click **Apps** menu from the left pane.

4. Click **ADD NEW**.



5. Rename the app and change your app icon, if required.



5. Creating an Identity Service

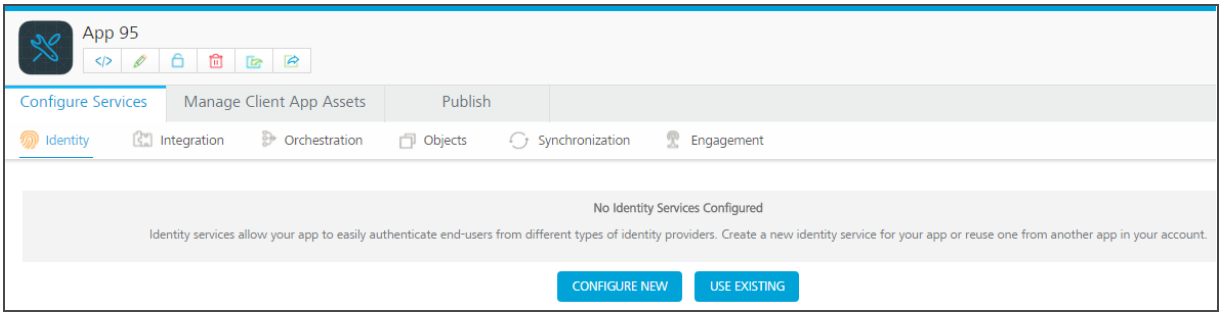
The Identity Service allows you to add a simple authentication and authorization method to your mobile app. This service can integrate with various back-end identity providers (IDP) such as Salesforce, SAP, Active Directory (direct or by Active Directory Federation Services (AD FS)) or any SAML 2.0 enabled end-point. After successfully authenticating, the back-end IDP returns a security token that is held by Kony Fabric. This token can be used in subsequent calls to integration or orchestration services automatically. This helps remove the burden of single sign-on token management within the client app.

For this Quick Start guide, we will use the built-in Kony User Repository provided by Kony Fabric as our identity provider. For more information on integrating with other back-end IDPs, please refer to our tutorial for integrating a sample CRM app with Salesforce.

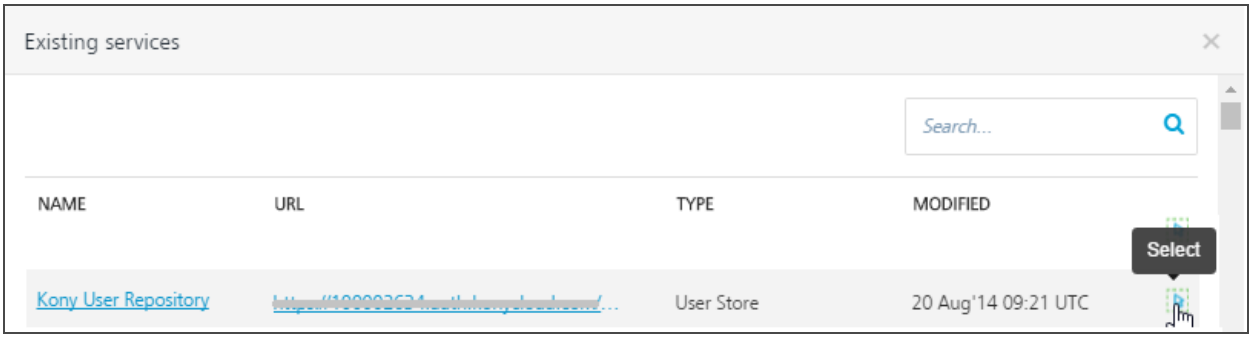
5.1 Configuring the Service

To configure an Identity service, follow these steps:

1. Under **Configure Services** > **Identity** tab click **USE EXISTING**.

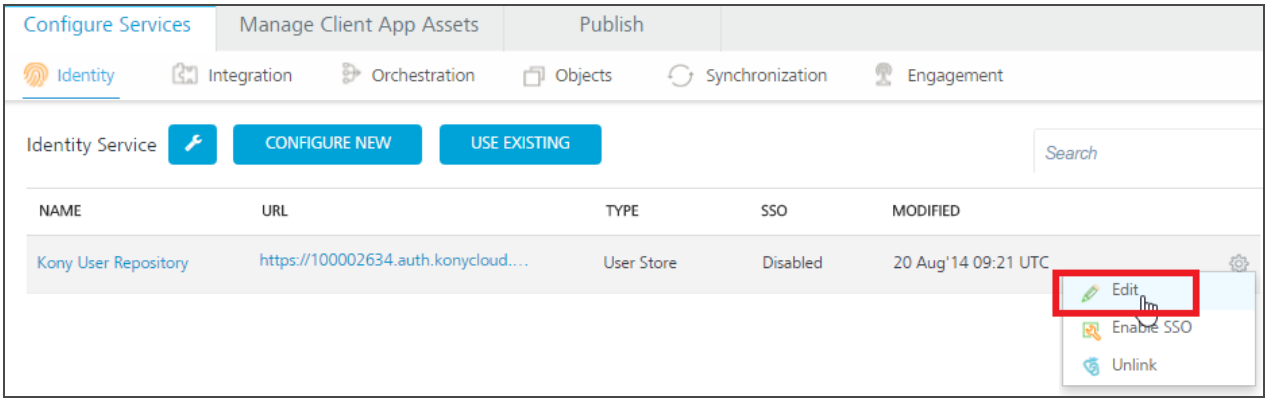


2. In the **Existing services** page, over your cursor over the **Kony User Repository** and click **Select**. The user store is added to your app.



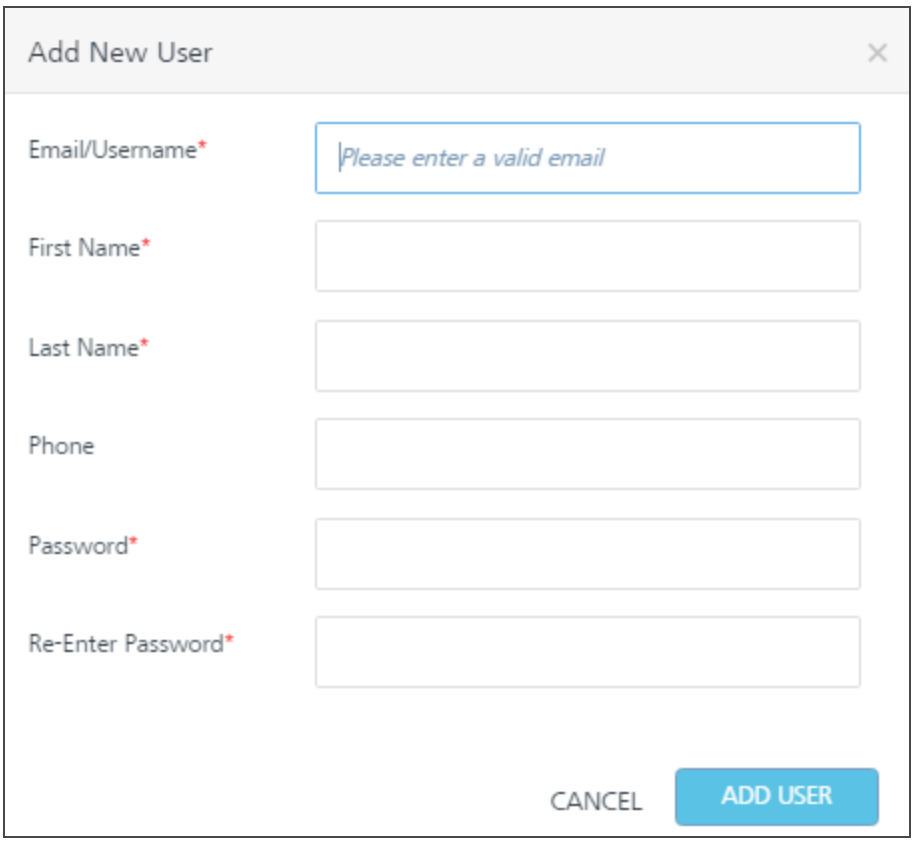
The identity service for the Kony User Repository is now available for use.

3. Click the settings icon and then click **Edit**.



4. Click **ADD NEW USER**. The **Add New User** window appears.

5. Provide the required details, and then click **Add User**.



6. Creating an Integration Service

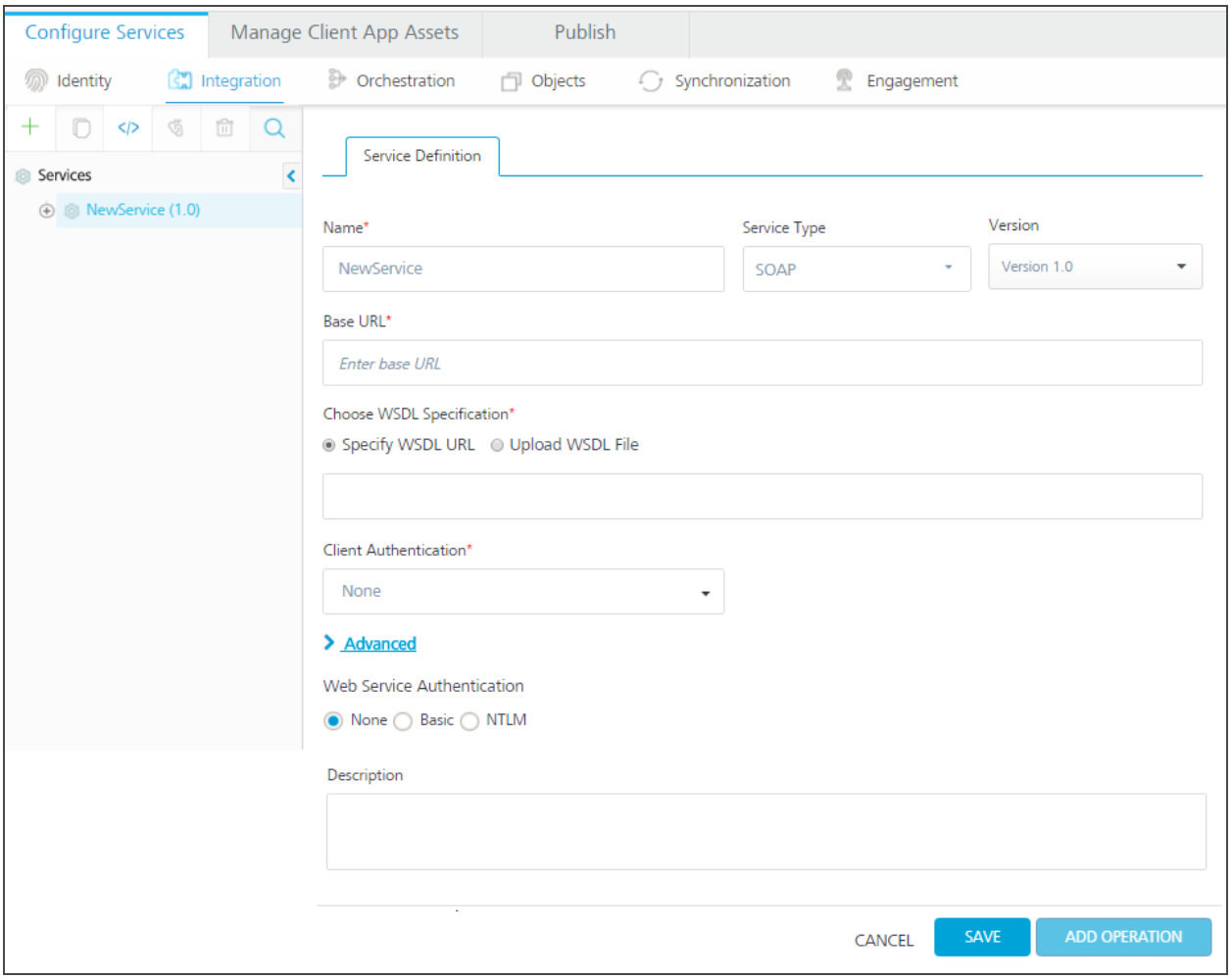
Now that we can authenticate our users, we need an easy way to retrieve data from an existing back-end system. In many cases, the back-end system does not return the data in the exact format we want, and/or it returns more data than our app needs.

The Kony Fabric Integration Services can consume data from any back- end system. You can use our standard technology connectors for REST, JSON, or SOAP web services. You can also use our enterprise business connectors that make it easy to connect to enterprise back-end systems like Salesforce or SAP, and browse for the data objects and services you want to expose to your app.

For this example, we will use a publicly available SOAP web service for getting weather information. To get the current weather and the weather forecast for a ZIP code, we will have to call two separate services.

To call the weather services, follow these steps:

1. Under the **Configure Services** tab, Click the **Integration** tab.
2. Click **CONFIGURE NEW.**



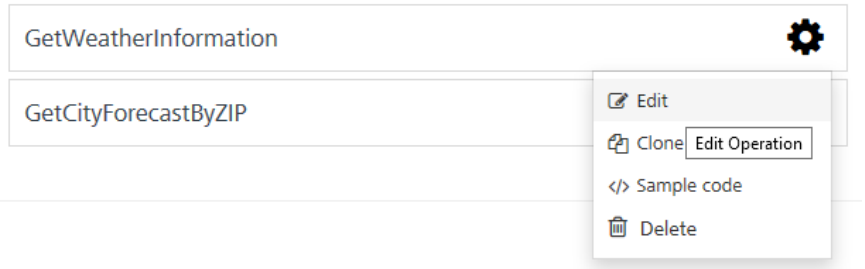
3. Name your new service **Weather** and choose *SOAP* as the **Endpoint Type**.
4. Then enter the following URLs to complete the service definition:
   - In the **Base URL** box, type: http://wsf.cdyne.com/WeatherWS/Weather.asmx
   - In the **WSDL URL** box, type: http://wsf.cdyne.com/WeatherWS/Weather.asmx?wsdl
5. In the **Choose WSDL URL**, select the option to specify the WSDL URL or upload the WSDL

file.

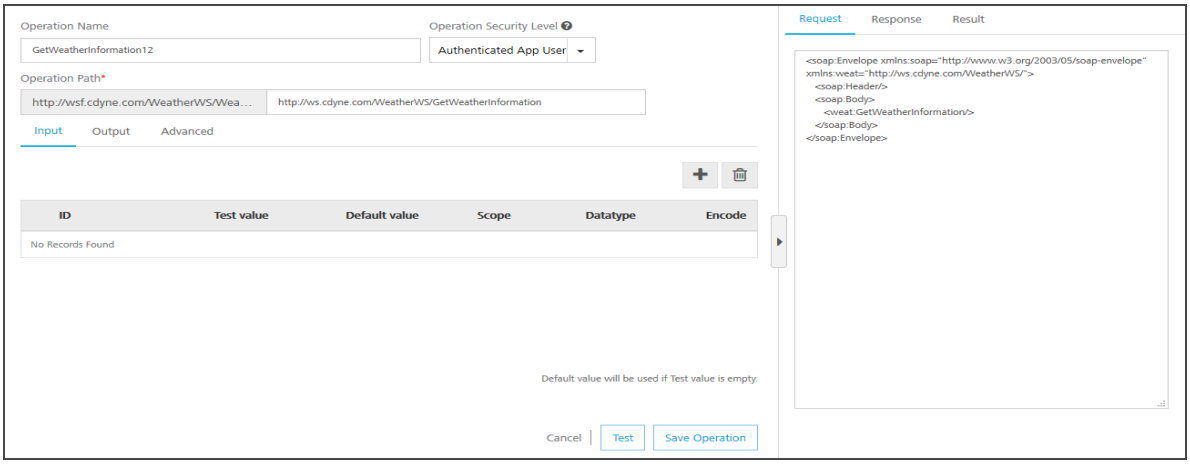
- If you click **Specify WSDL URL**, the system displays URL text box. Enter the WSDL URL.
- If you click **Upload WSDL File**, the system allows you to upload the WSDL file. Click the **Upload WSDL File** button to navigate to the WSDL file from your local system, and then click **Open**. The system uploads your WSDL file.

6. In the **Client Authentication** field, select an identity provider from the drop-down list. This drop-down list shows identity providers only if you have created identity providers for OAuth 2.0 in the Identity page.
7. Under the **Web Service Authentication**, select one of the following modes:
   a. **None**: Select this option if you do not want to provide any authentication for the service.
   b. **Basic**: Provide User ID and Password if the external Web service requires form or basic authentication.
   c. **NTLM**: Your service follows the NT LAN Manager authentication process. You are required to provide the User ID, Password, NTLM Host, and NTLM Domain.
   d. To enable the proxy, select the **Use proxy from settings** check box. By default, the check box is cleared.
8. Click **SAVE** to retrieve the WSDL. Each of the available operations are listed in a drop-down box. Select the *GetCityForecastByZip* and *GetCityWeatherByZip*. Click **Add Operation**. This will create two operations under your Weather service that maps to the SOAP web service methods.

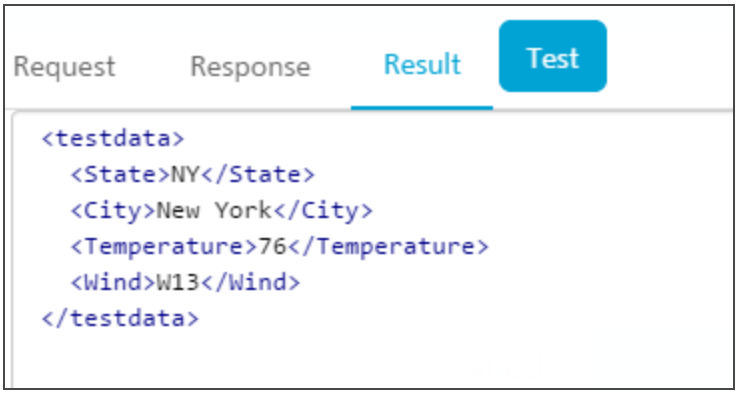
9. To test and edit the *GetCityWeatherByZip*, click the settings icon and choose **Edit**.



10. The operation details window opens. A sample web service request is provided showing a placeholder for any input parameters. For the GetCityWeatherByZip, the ZIP is the only input parameter displayed as `<ns1:ZIP>?XXX?</ns1:ZIP>` in the sample request. At this point, we could hard code a value, but since we want our app to provide the zip code, we need to provide an input variable name: `<ns1:ZIP>$zip</ns1:ZIP>`. We then need to define that variable under the input tab including a test value of *10036*.



11. You can then test the service and see the SOAP web service response.

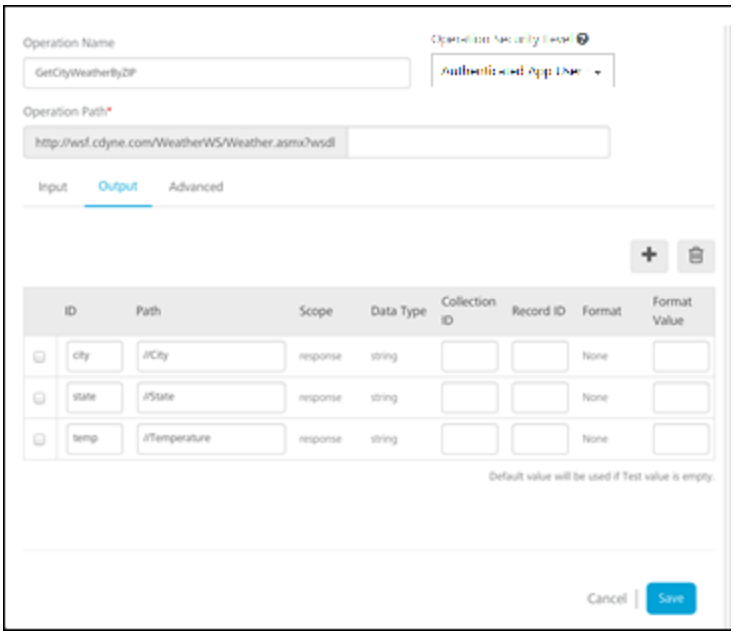


12. On the **Output** tab, enter the following parameters and path.

    city //City

    state //State

    temp //Temperature



13. Click the **Test** button again and the result will be displayed as XML.

The result will be converted to a JSON before being sent to the device.

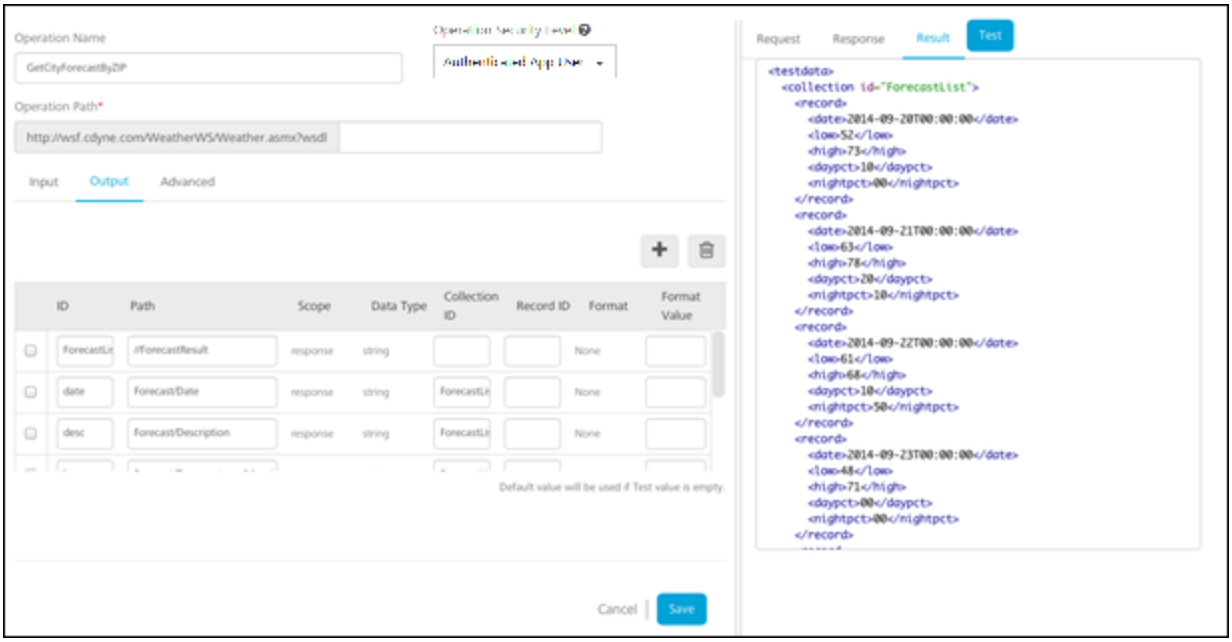
> ***Note:*** This is a simple example, but it shows the power and flexibility the Kony Fabric Integration Service provides to retrieve data and process it before returning an optimized JSON string to the device. You can also configure additional processing under the advanced tab including deploying custom code that executes before and after the service invocation.

14. Edit the *GetCityForecastByZip* in the same way. This service returns a repeating data structure for each day providing that day's weather forecast. This requires the use of the collection ID under the output tab to create a repeating set of JSON objects. After creating the **ZIP** input parameter the same way as the previous service, enter the following output parameters:

ID	xPath	CollectionID
ForecastList	//ForecastResult/Forecast	
date	Forecast/Date	ForecastList
desc	Forecast/Description	ForecastList
low	Forecast/Temperatures/MorningLow	ForecastList

ID	xPath	CollectionID
high	Forecast/Temperatures/DaytimeHigh	ForecastList
daypct	Forecast/ProbabilityOfPrecipiation/Daytime	ForecastList
nightpct	Forecast/ProbabilityOfPrecipiation/Nighttime	ForecastList

Test your service and you will see the resulting XML showing the repeating collections of forecasts.



7. Creating an Orchestration Service

The following types of Orchestration Services are supported by Kony Fabric:

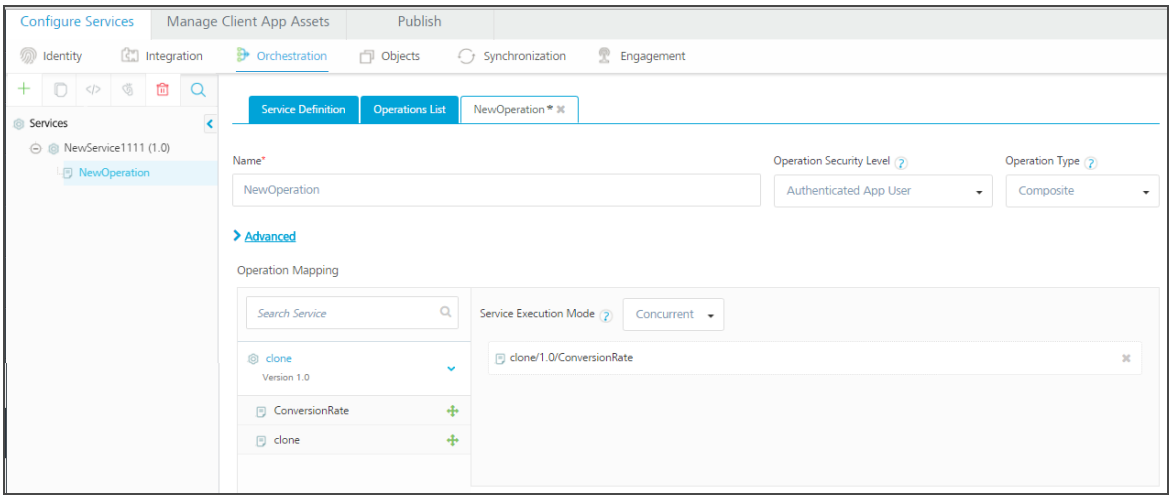
- **Composite Services** include:
    - **Concurrent Service**: All specified integration services are called in parallel.
    - **Sequential Service**: The output of one service can be used as the input of a subsequent service. Each integration service in the chain will be executed sequentially.
- **Looping Service**: Allows you to call the same service in a loop using the same input values until you reach a break condition or you can send in a delimited set of input values and the service will loop through the inputs until it reaches the end.

For this example, we want to return the current weather and the forecast in one service call. Therefore, we want to create a concurrent composite Orchestration Service using our *GetCityWeatherByZip* and our *GetCityForecastByZip*. This allows our app to call one Orchestration Service using the ZIP Code and getting back all the data we need.

To execute an Orchestration Service, follow these steps:

1. On the **Orchestration** tab, click **CONFIGURE NEW.**
2. Enter a name for the service as **GetCityWeatherAndForecastByZip** and click **SAVE**.
3. Click **Operation List** tab, and click **ADD OPERATION**. t

4. Enter the *GetCityWeatherByZip* and the *GetCityForecastByZip* operations.



5. From the **Operation Type** drop-down list, click **Composite**.

6. In the pane that lists integration services and orchestration services, select an integration service or orchestration service, and expand the service. Then drag an operation to the panel under **Service Execution Mode**.

7. Service Execution Mode drop-down list, click **Concurrent**.

8. Click **SAVE OPERATION**.

8. Creating an Object Service

Click here for more details.

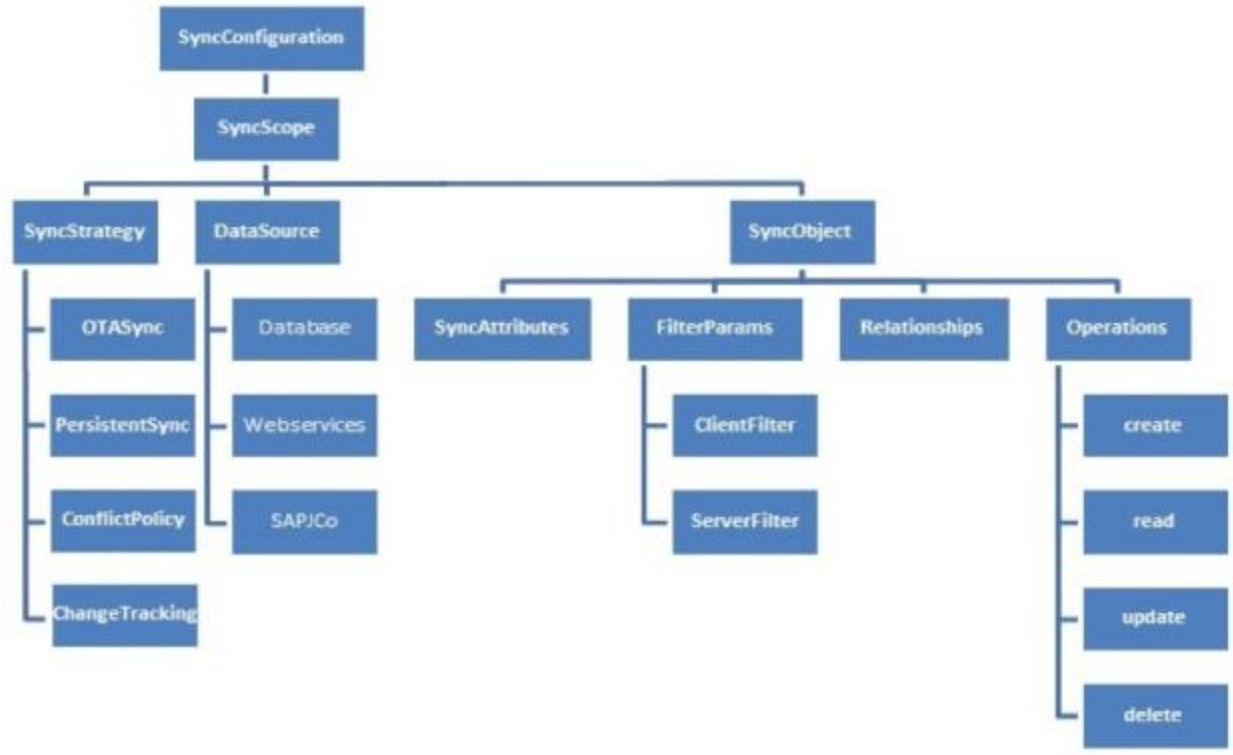
9. Synchronization

Kony Synchronization is a comprehensive data synchronization platform that enables developers to add synchronization capabilities to mobile applications. Fundamental to Sync Framework is the ability to support offline and collaboration of data between devices and the backend systems.

To enable synchronization capability for an app, you need to define a Sync Configuration file.

9.1 Sync Configuration file

A Sync Configuration captures details of the data synchronization characteristics of an application. These details are captured in a file typically referred to SyncConfig.xml (the name really does not matter) adhering to the SyncConfig.xsd schema. A SyncConfig.xml represents the below structure.



The two most important elements of this schema are:

- Sync Scope
- Sync Object

9.1.1 Sync Scope

A Sync Scope groups together the Sync Objects that share common synchronization characteristics like Sync Strategy, Datasource and so on.

A Sync Configuration can have multiple Sync Scopes. It is not possible to define relationships between Sync Objects belonging to different Sync Scopes.

9.1.2 Sync Object

Conceptually, you can consider a Sync Object as a business object that has some public attributes and some methods. The public attributes correspond to the fields visible to client devices, and they are used for synchronization. The methods correspond to the CRUD operations that map to the backend services exposed for the object. The parameter values methods /operations based on both public attribute values.

A Sync Object is meta-data:

- Defining the business object model of an application.
- Defining the way data is exchanged between mobile devices and backend.

A Sync Object is data:

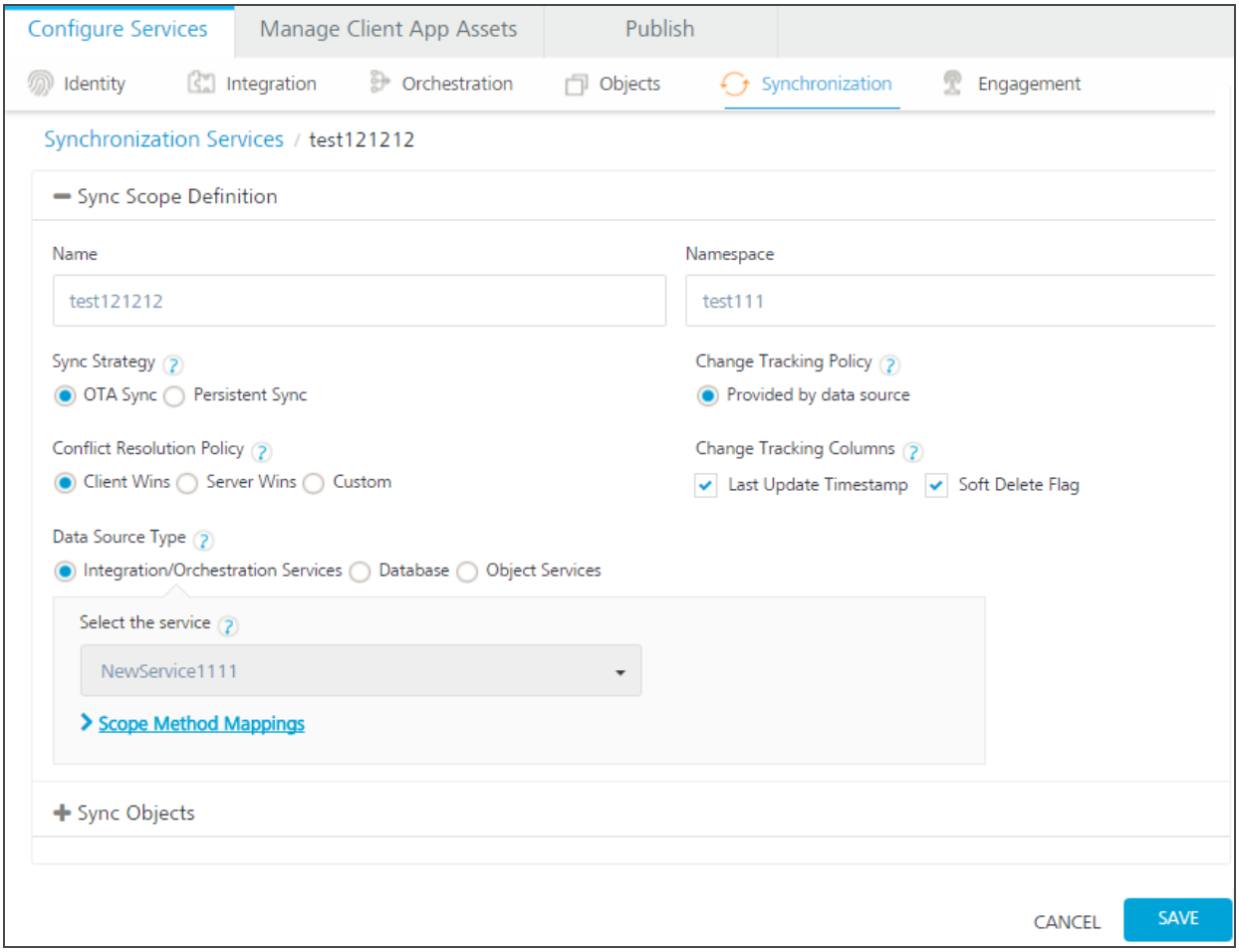
Sync Object data is a business object instance exchanged between client and server.

9.2 Adding a New Synchronization Scope

> ***Note:*** The following section explains setting up a Sync scope for Salesforce account.

To add a new Synchronization scope, follow these steps:

1. From the **Synchronization** page, click **CONFIGURE NEW**.
2. Under **Sync Scope Definition**, provide the following details:



   a. Provide a name for the new Sync scope. (For example, *FSSync*)

   b. Specify a **Namespace** for the Sync scope. The Namespace should follow a prescribed format such as *com.kony*.

   c. Select the required service from the **Integration Service** list.

d. Select a **Sync Strategy**. The available options are **OTA Sync** and **Persistent Sync**.

> ***Note:*** To understand which strategy to use for your sync scope, refer section Appendix - Sync Strategy.

e. Select a Change Tracking Policy (CTP) if you want to track the changes happening in the server database. Select Provided by data source, if you have a provision to track changes in the data source. For database this would be like a timestamp column which updates for any changes made to the row. Set CTP as Kony Sync Server, if you want SyncServer to track the changes. This option will be available only if you had selected Persistent Sync as Sync Strategy.

f. In case of conflicts between the data at the client and server end, specify any of the following under **Conflict Resolution Policy**:

- Client Wins: The changes on the client side take precedent over the changes on the server side.
- Server Wins: The changes on the server side take precedent over the changes on the client side.
- Custom: Enables you to upload an Interceptor class, which comprises the logic or policy for conflict resolution.

g. In the **Change Tracking Columns**:

i. Select the **Last Updated Timestamp** check box when you have column that represents the latest edited values.

ii. Select the **Soft Delete Flag** check box when the database has the column that represents soft deletes. Soft delete field in a record represents that a particular record is deleted by changing the status to deleted. This record will exist in the

database. Thus by selecting this field Kony Sync server does not sync records whose status is set as deleted.

h. Under **Data Source Type**, select one of the following:

- Integration/Orchestration Services: If you select a service that does not have an identity service, set the scope method mappings for the Sync Scope. If you select a service that has an Identity service, specify the user ID and password.

  To use an Integration service or Orchestration service as the data source, follow these steps:

  Click in the Select the service field. A drop-down menu appears. Select the service from the menu.

- **Database**: Use this option if you want the Synchronization service to connect directly with the data source without going through an Integration service. This option is typically used for a persistent sync strategy.

  To use a database as the data source, specify the following connection details of the backend database:

  - Database Type
  - Database Connection URL
  - User ID
  - Password

Click **Test Connection** to verify the connection to the database.

- **Object Services**: This is a Sync scope mapped to an object service. An object service has all the information to auto-generate the Sync scope, including objects, relationships, change tracking, and lifecycle methods. You need only provide the scope specific data, such as sync strategy and filters; the rest of the Sync scope is

inferred. If the object service changes, the scope is refactored to incorporate those changes.

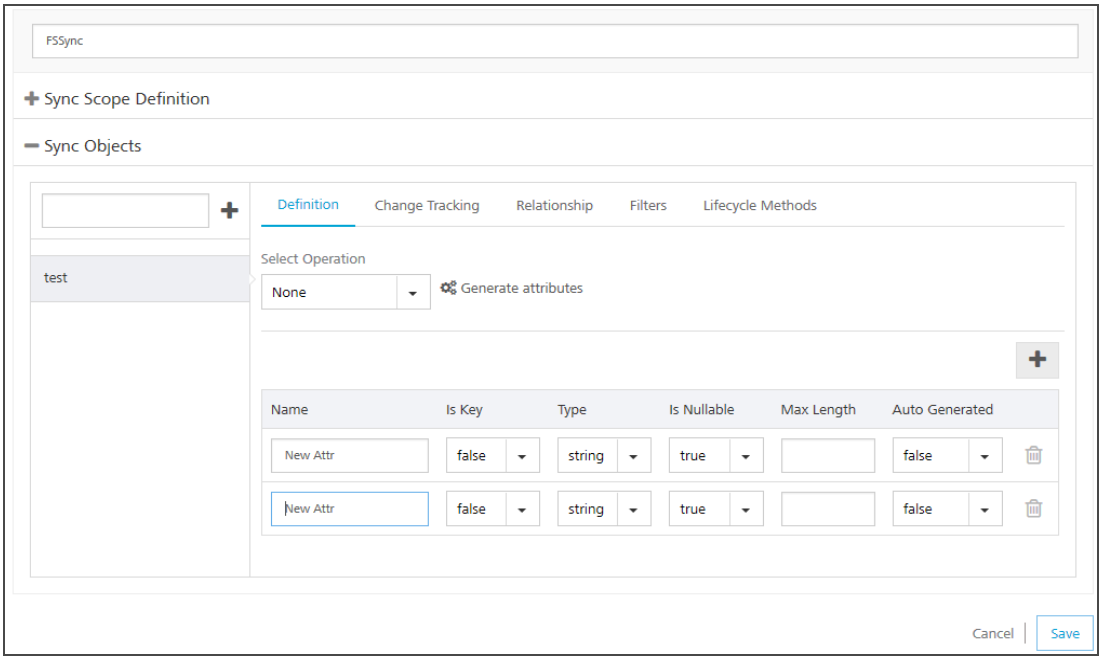
Note that a persistent sync strategy is not supported for a Sync scope that uses an object service as the data source type.

To use an object service as the data source:

- Click in the Select the service field. A drop-down menu appears. Select the object service from the menu.

3. Expand **Sync Objects**.
4. Under **Sync Objects**, provide the following details:
   a. On the left pane, provide a name for your Sync object, and then click the **Plus** button.
   b. On the **Definition** tab of the new Sync object, select an operation from the **Select Operation** list, and click **Generate attributes**.

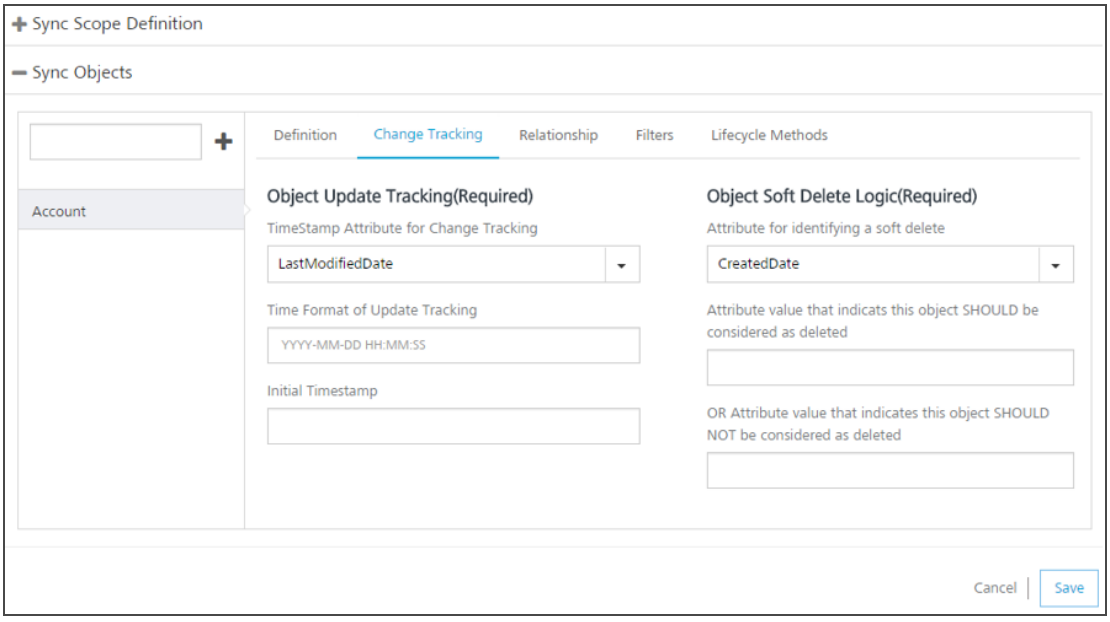
> ***Note:*** The list of operations available for a new Sync object depends on the Integration Service selected in the Sync Scope.



5. On the **Change Tracking** tab, do the following:
    a. From the **TimeStamp Attribute for Change Tracking** list, select an attribute that denotes a particular record is modified.
    b. From the **Attribute for Identifying a soft deleted** list, select an attribute that denotes a soft delete.

> ***Note:*** You need to select **TimeStamp Attribute for Change Tracking**, only if you have selected **Last Update Timestamp** check box under the **Change Tracking Columns** respectively.

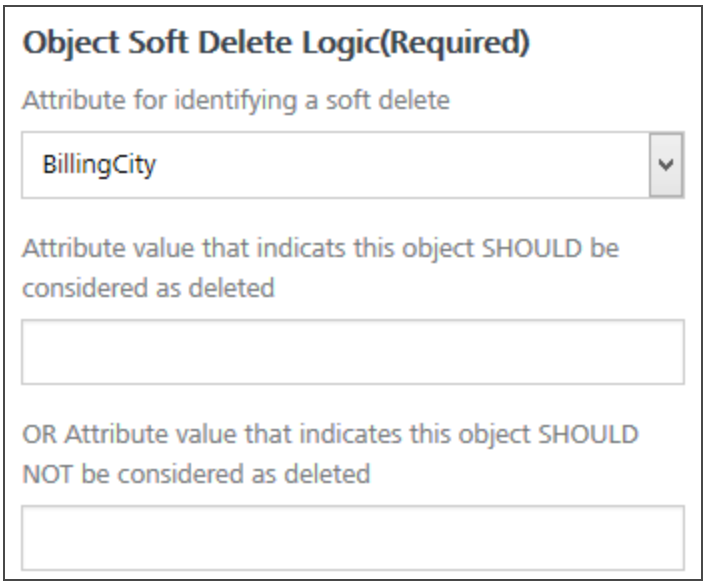
> ***Note:*** You need to select **Attribute for Identifying a soft delete** only if you have selected **Soft Delete Flag** check box under the **Change Tracking Columns**.



For non Boolean attributes, enter additional values that will be considered for soft deleting. For example, from the list if you select **BillingCity**, the system displays the following fields.

- **Attribute value that indicates this object SHOULD be considered as deleted**: if this value matches with the main attribute, the system deletes this attribute.
- **OR Attribute value that indicates this object SHOULD NOT be considered as deleted**: if this value matches with the main attribute, the system does not delete

this attribute.

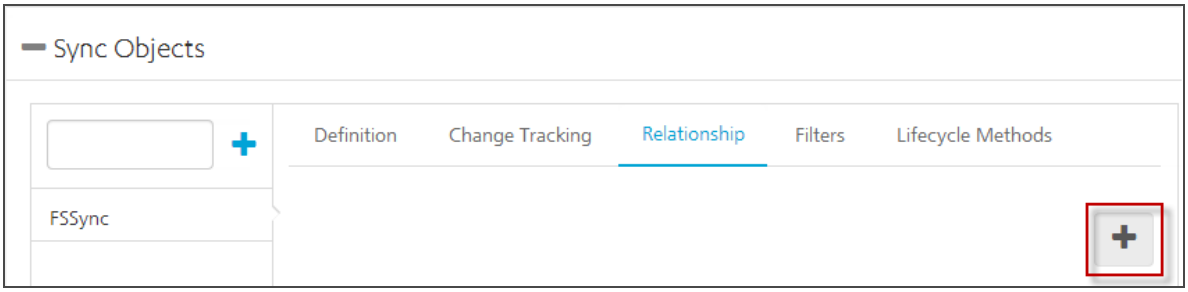


c. Change **Time Format of Update Tracking**, if required. By default, Salesforce time format is *YYYY-MM-DD HH:MM:SS*.

d. In **Initial Timestamp** box, enter the date from which the records are to fetched.

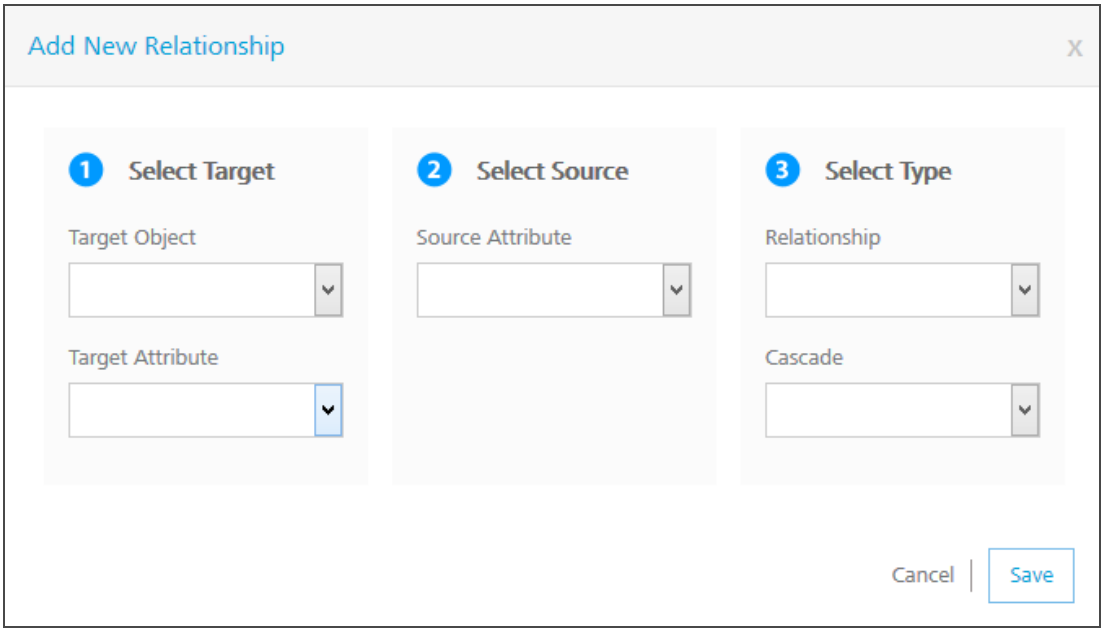
e. Click **Save**.

6. On the **Relationship** tab



Click the **Plus** button to open **Add New Relationship** dialog.

a. Provide the following details:



i. Select the required object from the **Target Object** list.

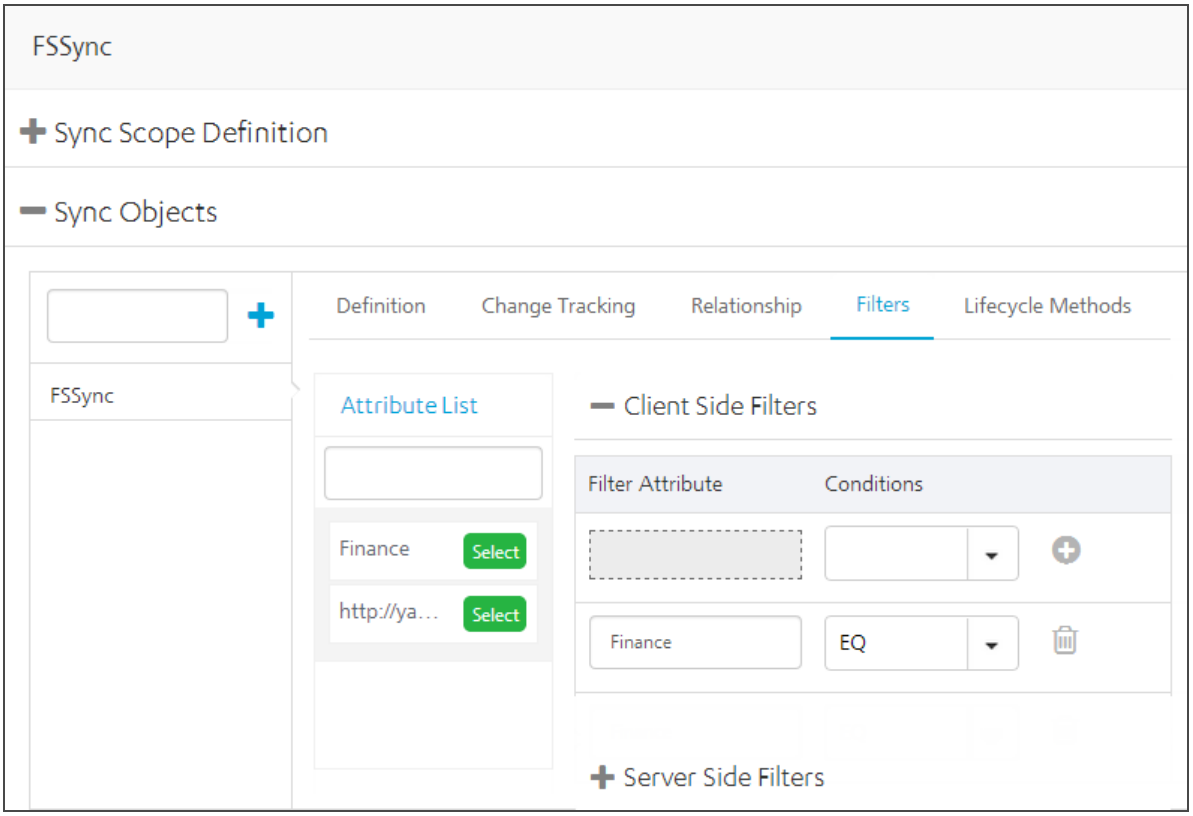
ii. Select the required attribute from the **Target Attribute** list.

iii. Select the required attribute from the **Source Attribute** list.

iv. Select the type of relation between Source attribute and target attribute from the **Relationship** list.

v. Select *True* from the **Cascade** list if you want to delete a record in the parent table and its child tables.

7. On the **Filters** tab, provide the following details:



   a. In the **Client Side Filters**, from the **Attribute List**, select an attribute.

   b. For the selected attribute, provide a condition.

   c. To save the current filter and add another filter, click the **Plus** button.

   d. In the **Server Side Filters**, from the **Attribute List**, select an attribute.

   e. For the selected attribute, provide a condition.

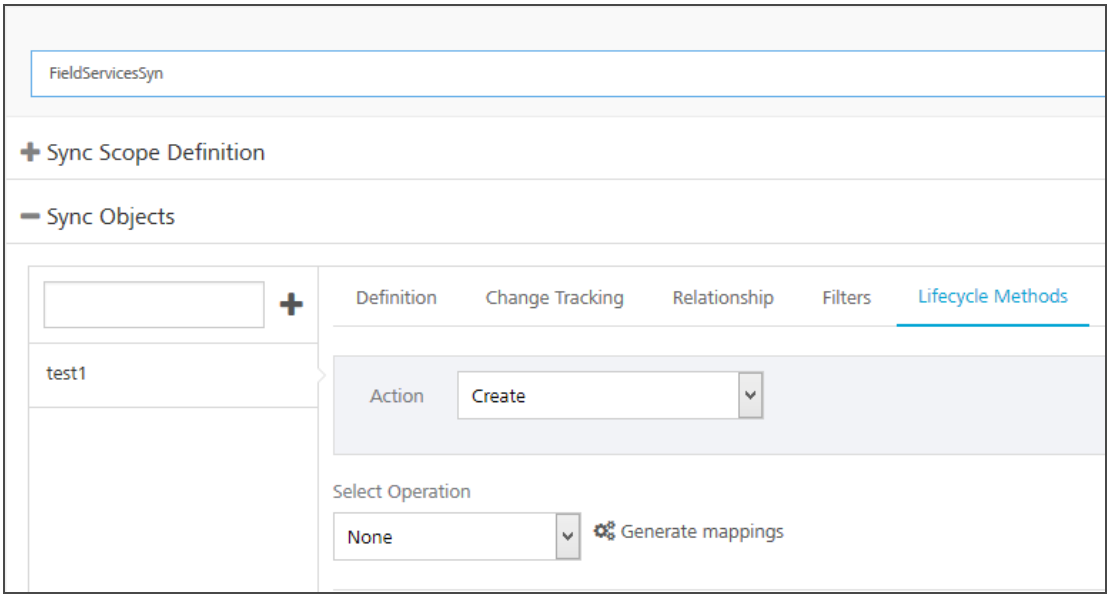
   f. To save the current filter and add another filter, click the **Plus** button.

8. On the **Lifecycle Methods** tab, provide the following details:

   a. From the **Action** list, select an action.

   b. From the **Select Operation** list, select an operation.

c. Click **Generate Mappings**.



> ***Note:*** Input mapping is generated only for *Create*, *Update* and *Delete* operations.

> ***Note:*** Output mapping is generated for all the operations: *Create*, *Update*, *Delete*, *get*, *getUpdated*, *getDeleted* and *getBatch*.

> ***Note:*** Header Mapping needs to be added manually.

d. Add Input parameters from the **Input Mapping** by clicking the **Plus** button. Provide the following details:

   a. From the **Source Type** list, select the type of the source.

   b. From the **Source Value** list, select a value.

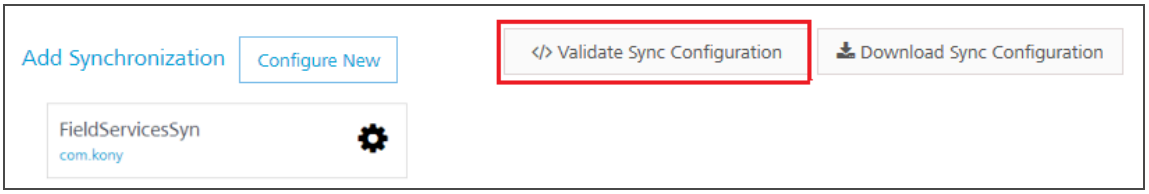
   c. From the **Service Input Param** list, select an input parameter.

   d. Click **Save**.

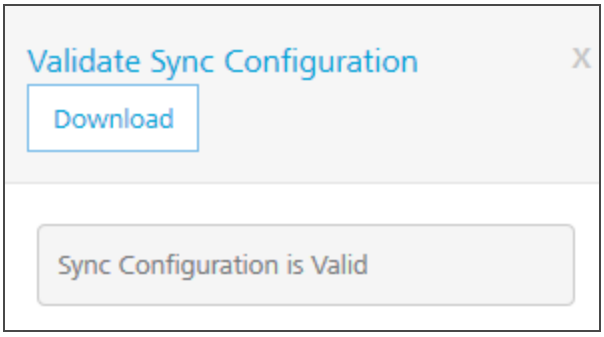
9.3 Validate Sync Configuration

Kony Fabric allows you to validate the Sync configuration before you can utilize the scope in your application.

To validate the your Sync configuration, on the **Synchronization** page, click **Validate Sync Configuration**.



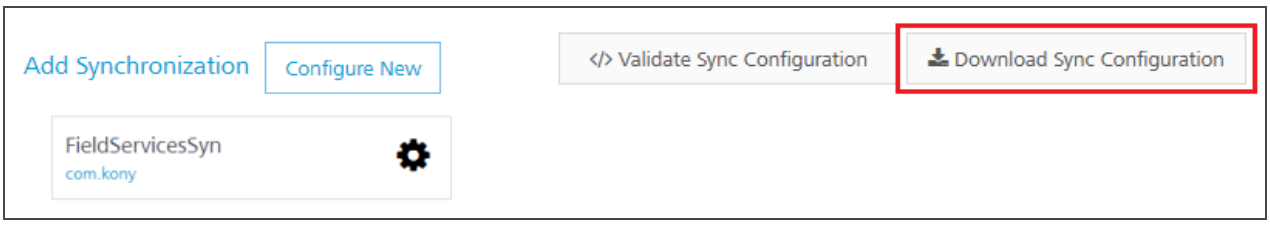
You receive the following message if your scope is valid:



To download the file, click **Download**. This file is useful when the Sync Scope is invalid, and you wanted to know the details of the errors encountered while validating the Sync Scope.

9.4 Download the Sync Configuration

Click **Download Sync Configuration** to download the Sync configuration file *Syncconfig.xml* file on your computer.

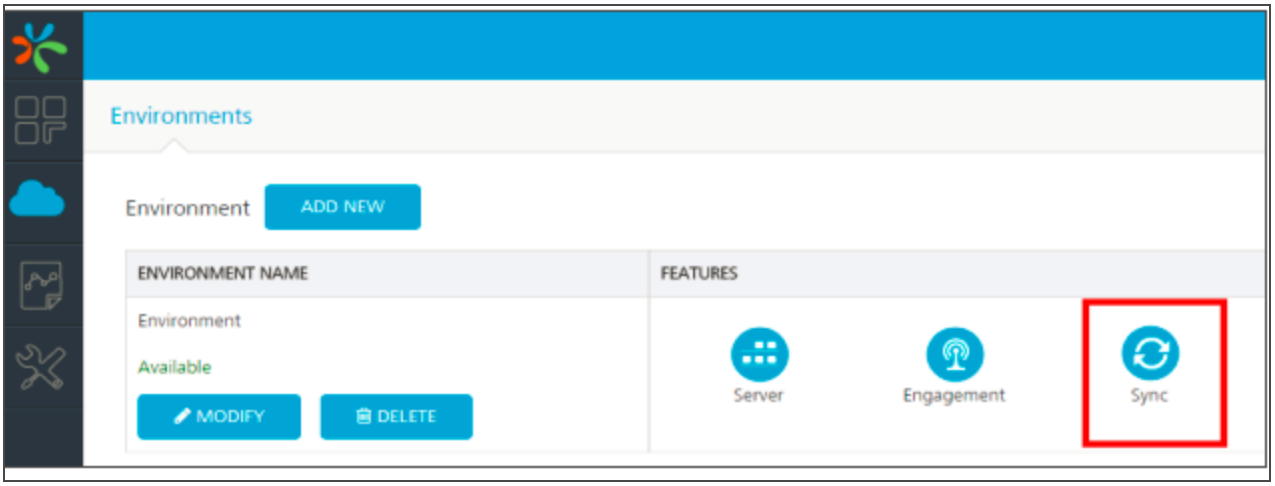


9.5 Sync Console

> ***Note:*** The details of your sync scope will be available in Sync Services after you *publish* the app.

Kony Sync Management Console provides a single point of control for monitoring and configuring the Kony sync console creation process.

To view your Sync Console, click **Sync Services** from your cloud account.



For more details on Sync Console, refer to the following document:
http://docs.kony.com/konylibrary/sync/kony_sync_console_user_guide/Default.htm

10. Engagement

Engagement Services allows you to upload push certificates for iOS, Android, BlackBerry, and WNS (Windows) platforms.

For sending messages, follow these steps:

1. Add Push Certificates
2. Access Messaging Console
3. Send a Push Message

10.1 Add Push Certificates

Kony Fabric Engagement Services supports the following platforms:

1. iOS
2. Android
3. BlackBerry
4. WNS

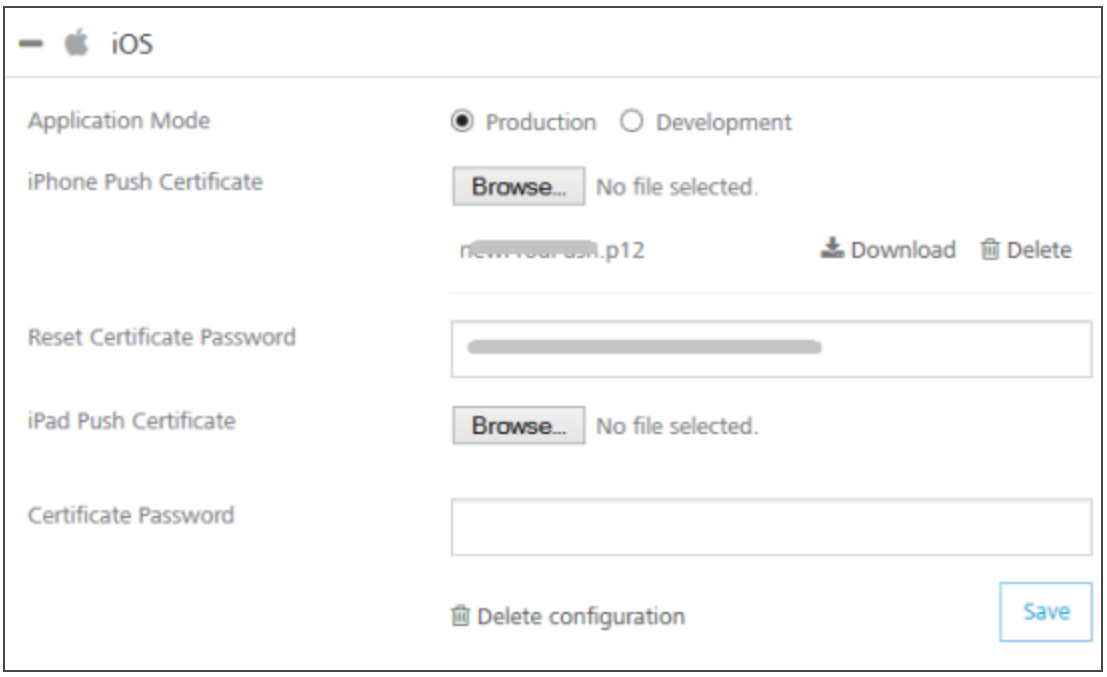
This section details the process for adding push certificates to your application.

10.1.1 iOS

> ***Note:*** Refer to the following section for creating a push certificate: Engagement Services Console User Guide > Applications

To add iOS Push Certificates for your app, follow these steps:

1. Expand **iOS**. A list of configurable items appear.



2. **Application Mode**: An appropriate application mode.
    - Production mode: When selected, production certificates and associated password details are entered while sending push notifications. Push notifications are delivered in real-time.
    - Development mode: When selected, you can still send push message notifications, but delivery of push notifications are not real-time.
3. **iPhone Push Certificate**: From here, you can upload, download, or delete a certificate.
    - Click **Browse** to upload an iPhone certificate.
    - Click **Download** to download an iPhone certificate.
    - Click **Delete** to delete an iPhone certificate.
4. **Certificate Password**: Enter the password for iPhone, and then click Save to complete the configuration process.

5. **iPad Push Certificate**: From here, you can upload, download, or delete a certificate.
    - Click **Browse** to upload an iPhone certificate.
    - Click **Download** to download an iPhone certificate.
    - Click **Delete** to delete an iPhone certificate.
6. Click **Save** to complete the configuration process for iOS platform.

10.1.2 Android

> ***Note:*** Refer to the following section for creating a push certificate: Engagement Services Console User Guide > Applications

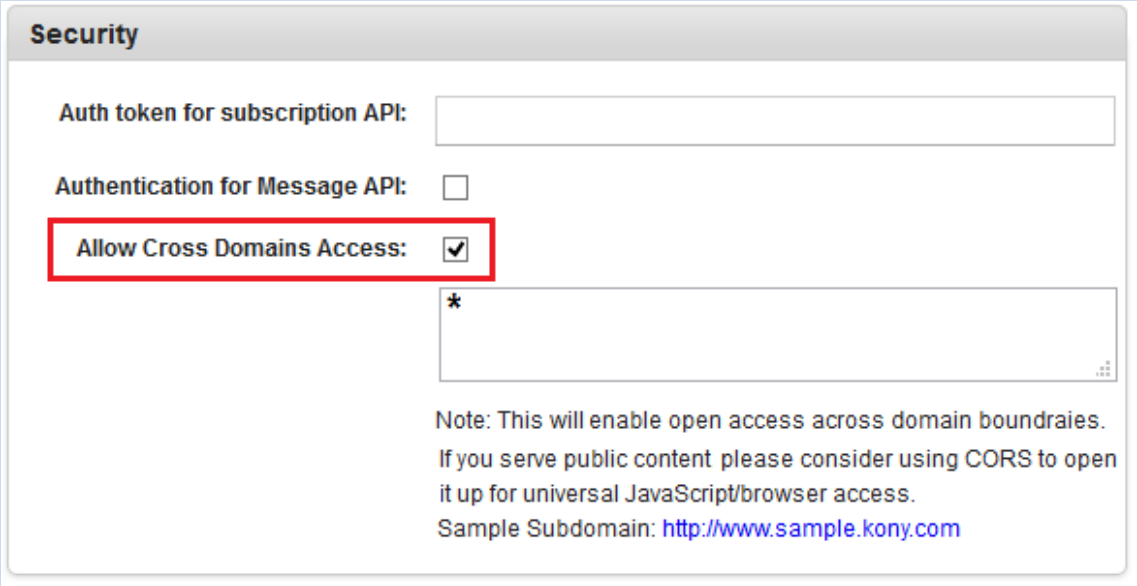
To add Android Push Certificates for your app, follow these steps:

1. Expand **Android**. A list of configurable items appear.

2. Enter the GCM authorization key, and then click **Save** to complete the configuration process.

> ***Note:*** Google Cloud Messaging for Android (GCM) is a service that helps you to send data from servers to Android applications on Android devices. This can be a lightweight message telling the Android application that there is new data to be fetched from the server (for example, a movie uploaded by a friend), or it can be a message containing up to 4kb of payload data (so apps like instant messaging can consume the message directly). The GCM service handles all aspects of queuing of messages and delivery to the target Android application running on the target device.

> ***Important:*** From PhoneGap application, to use messaging services (subscription, push messages and fetch messages), you must enable cross-origin resource sharing (CORS) in KMS console.
>
> To enable CORS, in **Kony Fabric Engagement Console > General > Settings > Security**, select the **Allow Cross Domains Access** check box. In Kony Fabric Engagement Console, by default the check box is cleared.
>
> For more details, refer to Kony Fabric Messaging Console > General > Settings > Security section.

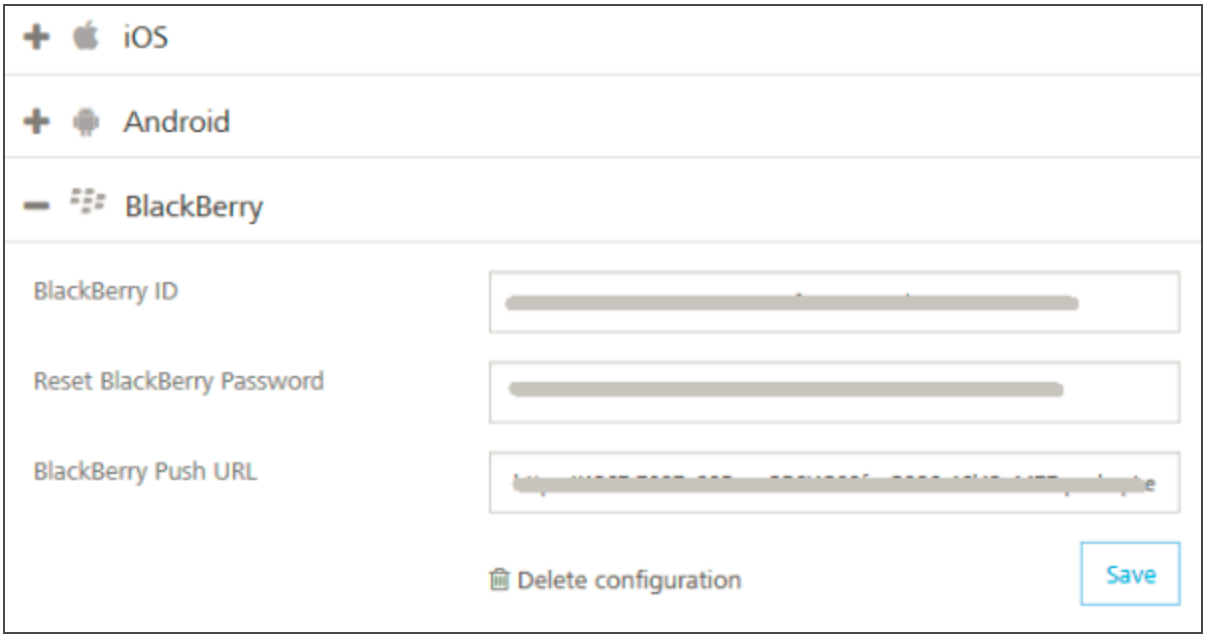


10.1.3 BlackBerry

> ***Note:*** Refer to the following section for creating a push certificate: Engagement Services Console User Guide > Applications

To add BlackBerry Push Certificates for your app, follow these steps:

1. Expand **BlackBerry**. A list of configurable items appear.



2. **BlackBerry ID**: Enter the ID.

> ***Note:*** BlackBerry Identity is a single, master key for BlackBerry products, sites, services, and applications, offering: Simplified access, privacy and security controls, a personalized and customizable experience.

3. **BlackBerry Password**: Enter the password.
4. **BlackBerry Push URL**: Enter the web address.

5. Click **Save** to complete the configuration process.
6. To delete configuration for BlackBerry, click **Delete Configuration**.

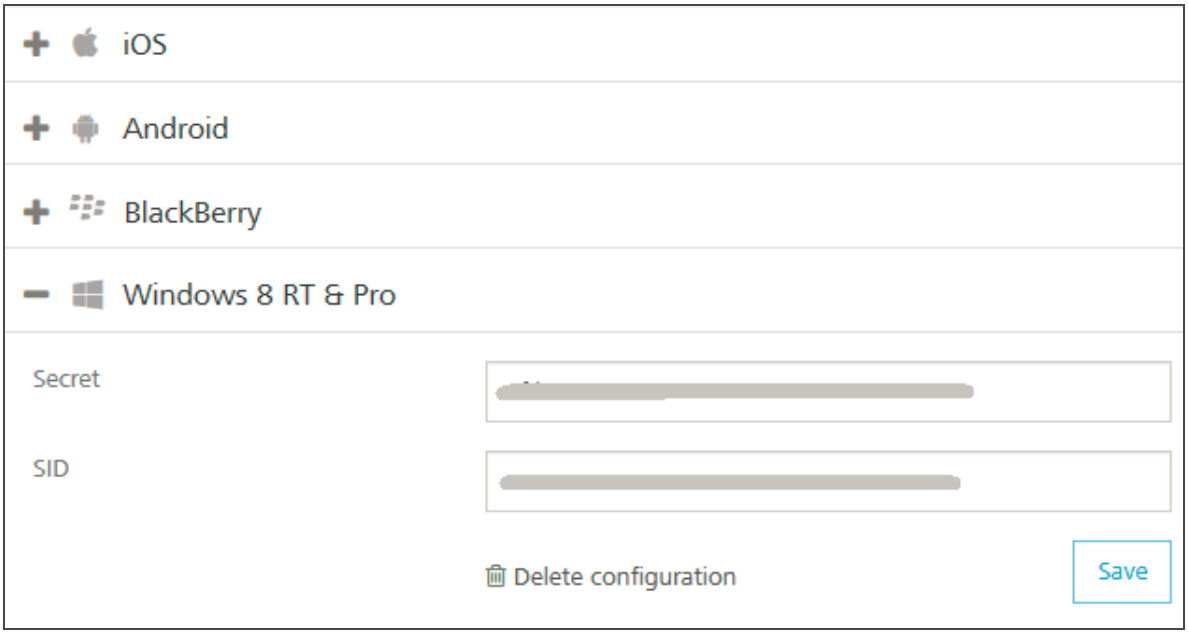
10.1.4 WNS (Windows)

> ***Note:*** Refer to the following section for creating a push certificate: Engagement Services Console User Guide > Applications

> ***Note:*** Windows push certificate is a purchased SSL certificate that is converted to correct format for uploading to Kony Fabric.

To add Windows Push Certificates for your app, follow these steps:

1. Expand **WINDOWS 8 RT** and **PRO**. A list of configurable items appear.



2. **Secret**: Enter the secret key details.

> ***Note:*** Windows Secret is an associated secret key that contains strings used in authentication with KMS APIs. It is used in authentication on the client side during registration.

3. **SID**: Enter the SID details, and then click Save to complete the configuration process.

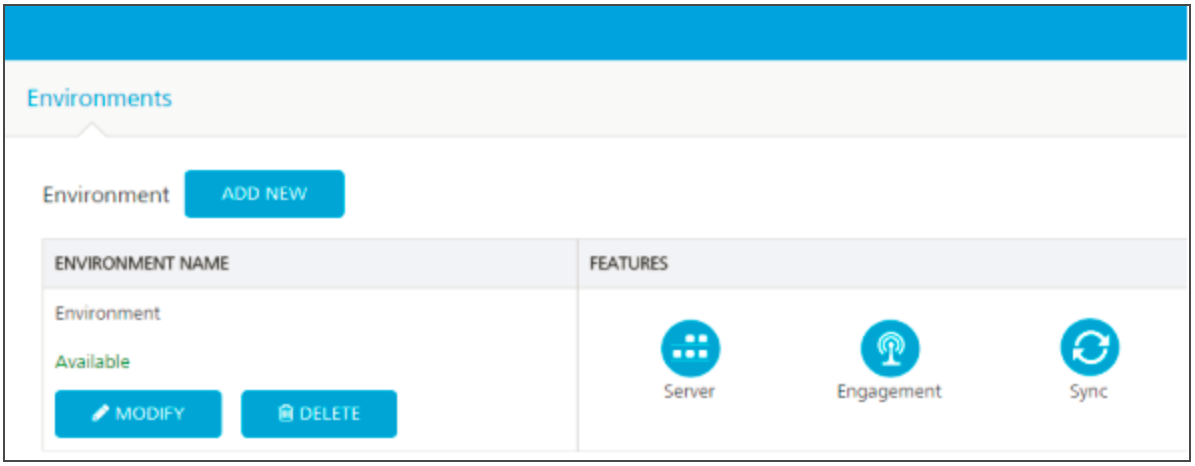
> ***Note:*** Windows SID is a security identifier that is a unique, immutable identifier of a user, user group or other security principal. A security principal has a single SID for life, and all properties of the principal, including its name, are associated with the SID. This design allows a principal to be renamed (for example, from "John" to "Jane") without affecting the security attributes of objects that refer to the principal.

4. To delete push configuration for Windows, click **Delete Configuration**.

10.2 Accessing Engagement Services Console

The Engagement Services Console allows you to add and manage applications, view the stored certificates, and manage a subscribers list.

You can access Engagement Services console from your Kony Fabric cloud account by clicking the **Engagement Service** in the your cloud dashboard.



Note: For more information on Engagement Services Console, refer to the following guide: http://docs.kony.com/konylibrary/messaging/kms_console_user_guide/Default.htm.

11. Publishing the App

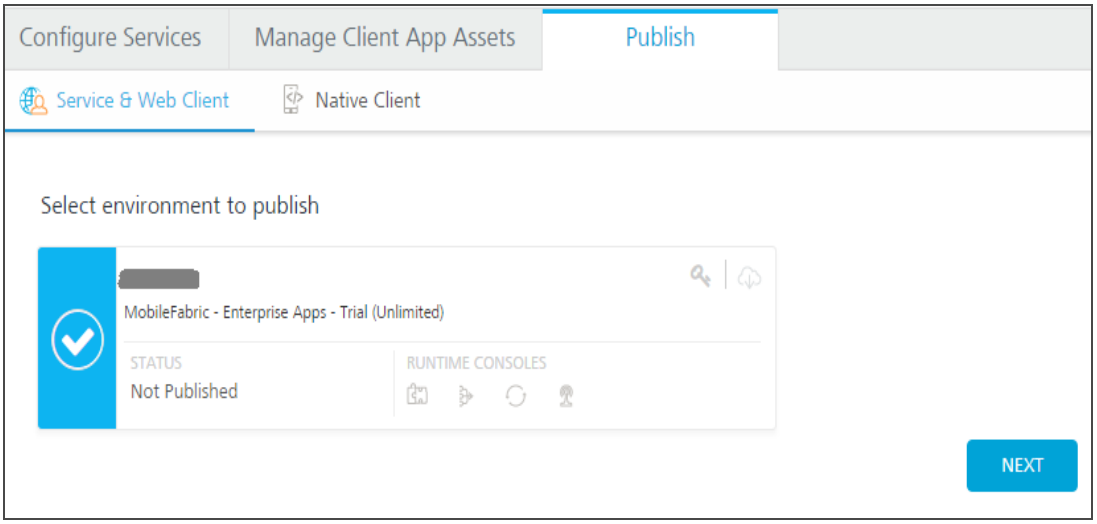
Once you have configured your demo app to use Kony User Repository identity service, you need to publish the app.

Based on environments created, Kony Fabric Console allows you to publish apps by using automated publish or manual publish.

- With automated publish, your apps are published to clouds or environments.
- Manual Publish is required only because of some limitations with publishing custom code associated with integration services.

To publish a service, follow these steps:

1. Click the **Publish** tab to view your available environments.
2. Select your target environment, and then click **Publish**.

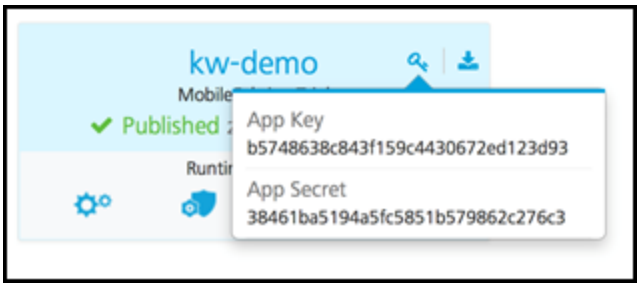


11.1 Testing the Service

Now that the identity service for our app has been published, we can test the service by trying to authenticate as our demo user. To do this, we need the app key, app secret, and the identity service URL of our runtime environment.

For testing the service, follow these steps:

1. From the **Publish** tab, click the key icon of our runtime environment.

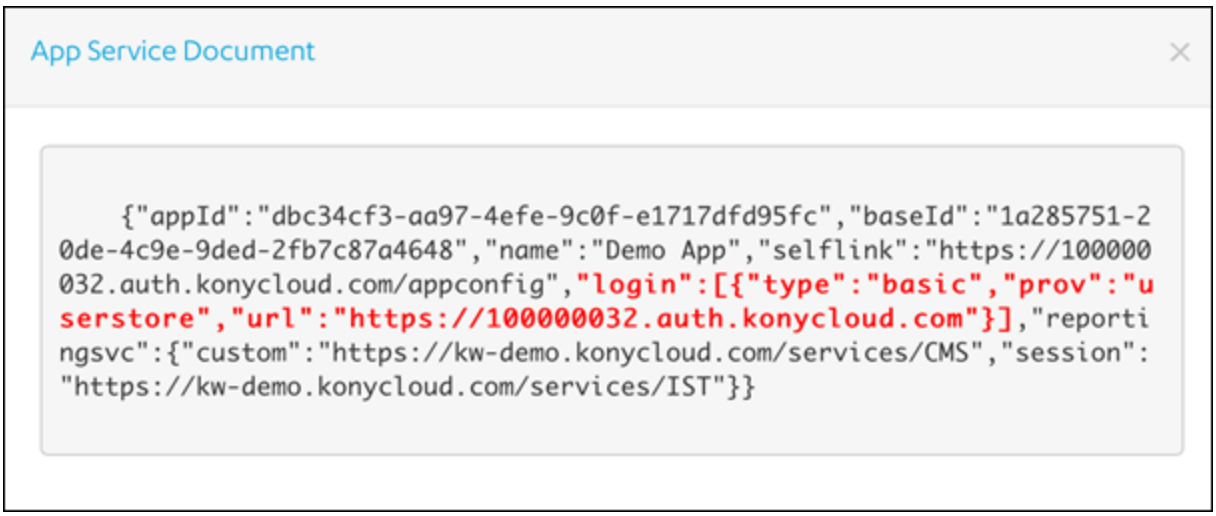


   The app key and app secret are displayed.

   The App key, App secret, and Service URL are used to initialize a client app to use Kony Fabric services.

> ***Note:*** App Key is unique to each environment.

2. Click the download icon, and then click **App Service Document**.



This will display a configuration JSON used by the client app to discover what services are available to this app in this environment. The configuration also contains the **login URL** to the user store (highlighted in red).

3. Test the service using the following cURL command for authenticating a user.

> ***Note:*** cURL - a command line tool for getting or sending files using URL syntax. This guide uses the cURL command to represent a mobile device making HTTPS API calls to a Kony Fabric environment. cURL is typically pre-installed on Linux and Mac systems.
> For Windows, go to http://curl.haxx.se/download.html, download cURL, and the SSL libraries required to connect to HTTPS URLs.
>
> For cURL commands and documentation, refer to http://curl.haxx.se/docs/

```
curl -X POST -H "X-Kony-App-Key:
24662f8e60c8a5cd2b2117e37d22fe32" -H "X-Kony-App-Secret:
75aa0fe163ace8f5c4a92245b97d95c6" -H "Accept: application/json" -
H "Content-Type: application/x-www-form-urlencoded" -d
'userid=demo%40kony.com&password=Pass1234'
'https://100000032.auth.konycloud.com/login?provider=userstore'
```

4. The JSON response contains the following elements:

    a. **profile**: Includes user profile information. In this case, it is the user profile attributes from Kony User Repository. If this identity services were connected to an enterprise identity service provider, this would include user profile information from that system.

    b. **provider token**: This is the security token returned from the external identity service provider such as Active Directory or Salesforce. In this case, it is the token returned from the Kony User Repository.

    c. **refresh token**: The refresh token has a longer timeout than the provider token. The refresh token can be used to get a new provider token, but it requires the use of the app key and app secret to request a new provider token.

    d. **claims token**: This is a Kony Fabric claims token that will be used for any subsequent calls to Integration, Objects, Orchestration, Sync, or Engagement Services.

The token values are formatted as JWT tokens and are digitally signed by the server so they can be validated by the server on subsequent calls. They can be decoded using a JWT decoder such as https://developers.google.com/wallet/digital/docs/jwtdecoder to view the data it includes.

The following is a sample JSON response from the cURL command:

```
{
    "profile": {
        "email": "demo@kony.com",
        "userid": "demo@kony.com",
        "firstname": "Demo",
        "lastname": "User"
    },
    "provider_token": {
       "exp": 1412190752000,
       "value":
```

```
"eyAiYWxnIjogIk5PTkUiLCAidHlwIjogImp3cyIgfQ.eyAiX2FjcyI6ICIxMDA
w
MDAwMzIiLCAiZXhwIjogMTQxMjE5MDc1MiwgIl9pc3NtZXRhIjogIi9hcGkvdjE
v
bWV0YWRhdGEvVXl3M0pDdVU4XzVnUEZFNzdCM3ZGdz09IiwgIl92ZXIiOiAidjE
u
MSIsICJfcHJvdl91c2VyaWQiOiAiZGVtb0Brb255LmNvbSIsICJfaWRwIjogInV
z
ZXJzdG9yZSIsICJpc3MiOiAiaHR0cHM6Ly8xMDAwMDAwMzIuYXV0aC5rb255Y2x
v
dWQuY29tIiwgIl9lbWFpbCI6ICJkZW1vQGtvbnkuY29tIiwgImp0aSI6ICJlMDU
w
MmFiNS05OTY4LTQzNzctOWRkNC04ZWI4OWJhMGVhMjEiLCAiaWF0IjogMTQxMjE
4
NzE1MiB9.MCwCFAa5lgjc8PKc3lZwXydRviPtrJXjAhRWSssiS86n4oWyuCZEsc
Z
wkn7aHw",
    "provider": "userstore",
    "params": {}
    },
    "refresh_token":

"eyAiYWxnIjogIk5PTkUiLCAidHlwIjogImp3cyIgfQ.eyAiX3Njb3BlIjogImc
i
LCAiX2FjcyI6ICIxMDAwMDAwMzIiLCAiZXhwIjogMTQxMjI3MzU1MiwgIl9pc3N
t
ZXRhIjogIi9hcGkvdjEvbWV0YWRhdGEvVXl3M0pDdVU4XzVnUEZFNzdCM3ZGdz0
9
IiwgIl92ZXIiOiAidjEuMSIsICJfcHJvdl91c2VyaWQiOiAiZGVtb0Brb255LmN
v
bSIsICJfaWRwIjogInVzZXJzdG9yZSIsICJfYXBwIjogImRlZjljNzM4LTAxNjM
t
```

```
NDgzZS05NzdmLTM1MDIxMjVjMTk4YyIsICJpc3MiOiAiaHR0cHM6Ly8xMDAwMDA
w
MzIuYXV0aC5rb255Y2xvdWQuY29tIiwgIl9lbWFpbCI6ICJkZW1vQGtvbnkuY29
t
IiwgImp0aSI6ICI0MTI1ZmE5Yy1lZDlmLTRjMTItYTYzNC02OGJkOTAwYTNhMTg
i
LCAiaWF0IjogMTQxMjE4NzE1MiwgIl9wdWlkIjogMjgwODI0NjA0OTc5NDU1MDg
2
IH0.MCwCFACJQFUW0C4pYFV2GIvOB0erHrENAhQQ3-Dvfe9ytvCzu-tbJZ_
630lu
XA",
    "claims_token": {
        "value":

"eyAiYWxnIjogIk5PTkUiLCAidHlwIjogImp3cyIgfQ.eyAiX3Njb3BlIjogImc
i
LCAiX2FjcyI6ICIxMDAwMDAwMzIiLCAiX3ZlciI6ICJ2MS4xIiwgIl9pZHAiOiA
i
dXNlcnN0b3JlIiwgIl9hcHAiOiAiZGVmOWM3MzgtMDE2My00ODNlLTk3N2YtMzU
w
MjEyNWMxOThjIiwgImlzcyI6ICJodHRwczovLzEwMDAwMDAzMi5hdXRoLmtvbnl
j
bG91ZC5jb20iLCAiX2VtYWlsIjogImRlbW9Aa29ueS5jb20iLCAiaWF0IjogMTQ
x
MjE4NzE1MiwgImV4cCI6IDE0MTIxOTA3NTIsICJfaXNzbWV0YSI6ICIvYXBpL3Y
x
L21ldGFkYXRhL1V5dzNKQ3VVOF81Z1BGRTc3QjN2Rnc9PSIsICJfcHJvdl91c2V
y
aWQiOiAiZGVtb0Brb255LmNvbSIsICJqdGkiOiAiY2M4MGFkNGEtNGQ0NS00MmF
k
LTk2ZjUtZTY0NzYwZWViZjI2IiwgIl9hdXRoeiI6ICJleUp3WlhKdGFYTnphVzl
1
```

```
Y3lJNmUzMHNJbkp2YkdWeklqcGJYWDAiLCAiX3B1aWQiOiAyODA4MjQ2MDQ5Nzk
0
NTUwODYgfQ.MC0CFQCP_1JSQe9stMYjr8P4vrgKYuTn5gIUSx6j_
R9dbjFFCcTCL
AiD6AOdqh0"
,
        "exp": 1412190752000
    }
}
```

12. Settings

Using **Settings**, a superuser can manage tasks such as adding new users, assigning roles to users, deleting users, configuring proxy server, and configuring reports server.

Settings includes the following sections:

- Users
- Proxy
- Studio
- Reports

12.1 Users

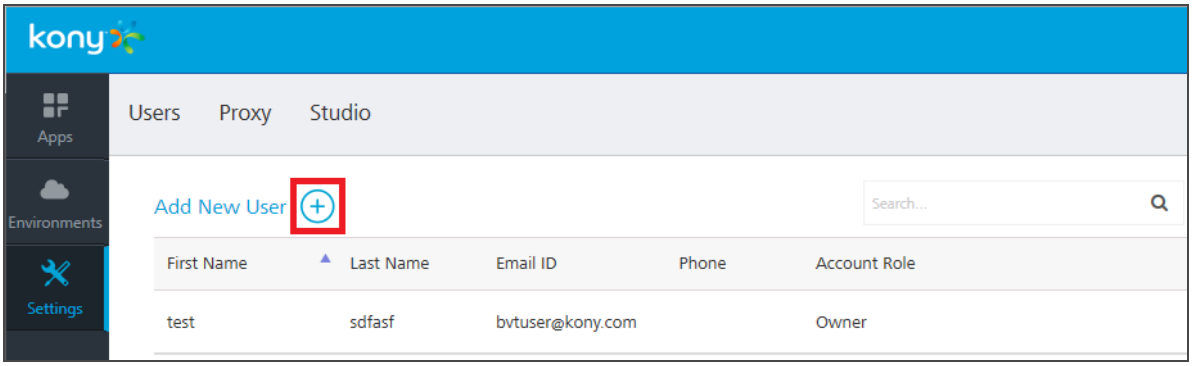
A user is an individual person. Each user needs an account to access the Kony Fabric console. A superuser creates user accounts for owners, admins, and members who use the Kony Fabric console.

> ***Important:*** As a user, you must be an admin or owner to access the Users page and perform different tasks based on the role.

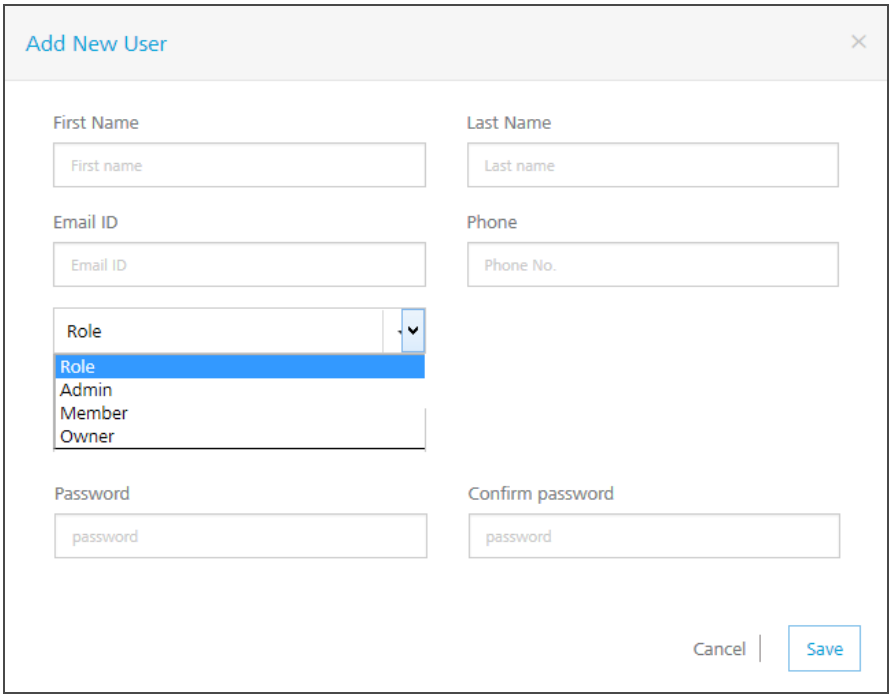
12.1.1 How to Add a User

To add a user, follow these steps:

1. In your Kony Fabric account, click **Settings**. By default, the **Users** page appears. The **Users** tab is visible to only users who are owners or admins. The page lists all owners, admins, and members of the account.



2. In the **Users** page, click **Add New User** button. The **Add New User** page appears.



> ***Note:*** All these fields are mandatory except the **Phone** number field.

3. Enter the details as required.

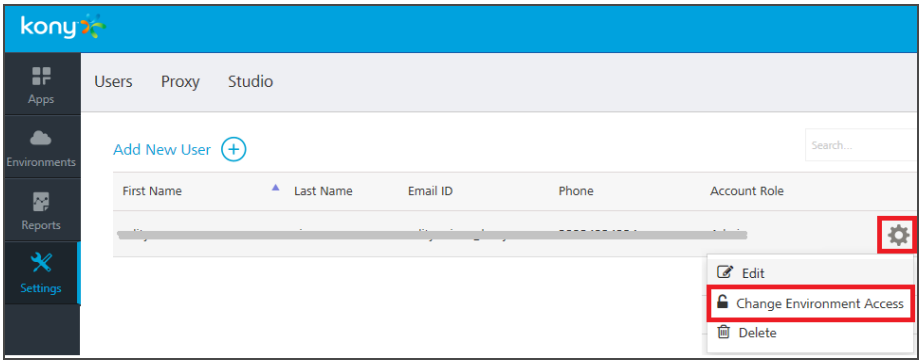
4. Click **Save** to save the user details. The system will add the new user in the grid.

12.1.2 How to Change Environment Access to a User

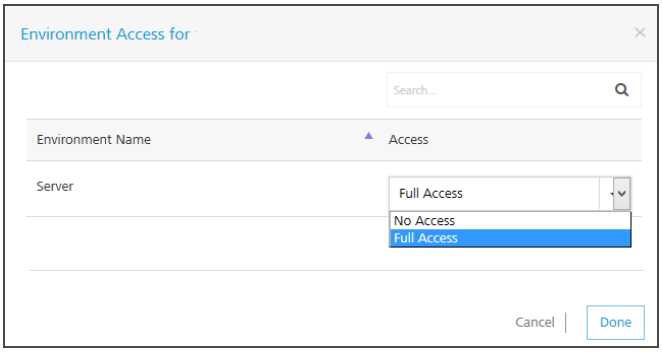
Users can be provided full access or no access to configured environments. An environment can contain all three servers such as Integration, Engagement and Sync Services together or in different combinations. You can change the access for each user separately.

To change an environment access, follow these steps:

1. In the **Settings > Users** page, hover your cursor over the required user from the list, click the **Settings** button, and then click **Change Environment Access**.



   The **Environment Access** page appears with all configured environments.



2. For an environment, from the **Access** drop-down list, select the option.
   - **No Access**: indicates that users cannot access an environment.
   - **Full Access**: indicates that users can access an environment.

3. Click **Done** to close the page.

12.2 Proxy

With proxy, you can enable more security to your apps. Typically, you use the proxy server to filter web content and monitor uploads and downloads when surfing the Internet. When connecting to the Internet through proxies, the IP address of your machine will not be shown. However, the IP of the proxy server will be shown.

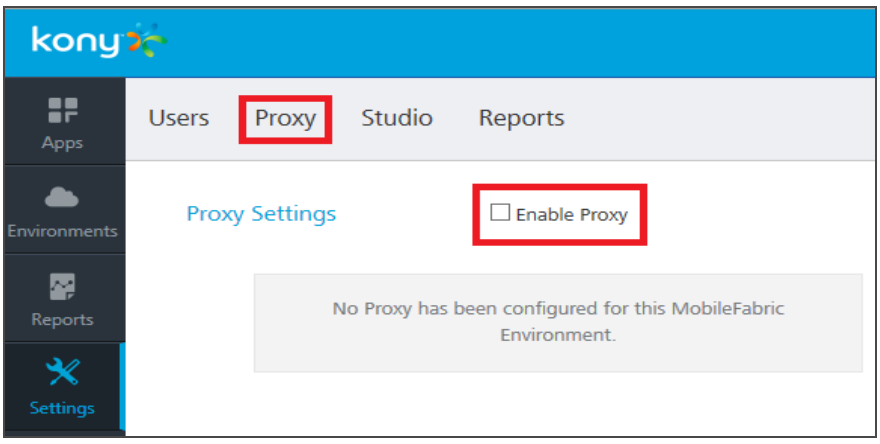
> ***Important:*** As a user, you must be an admin or owner to access the **Proxy** page and perform different tasks based on the role.

12.2.1 How to Configure a Proxy

You can configure only one proxy server. A proxy server can be basic or NT LAN Manager (NTLM) authentication.

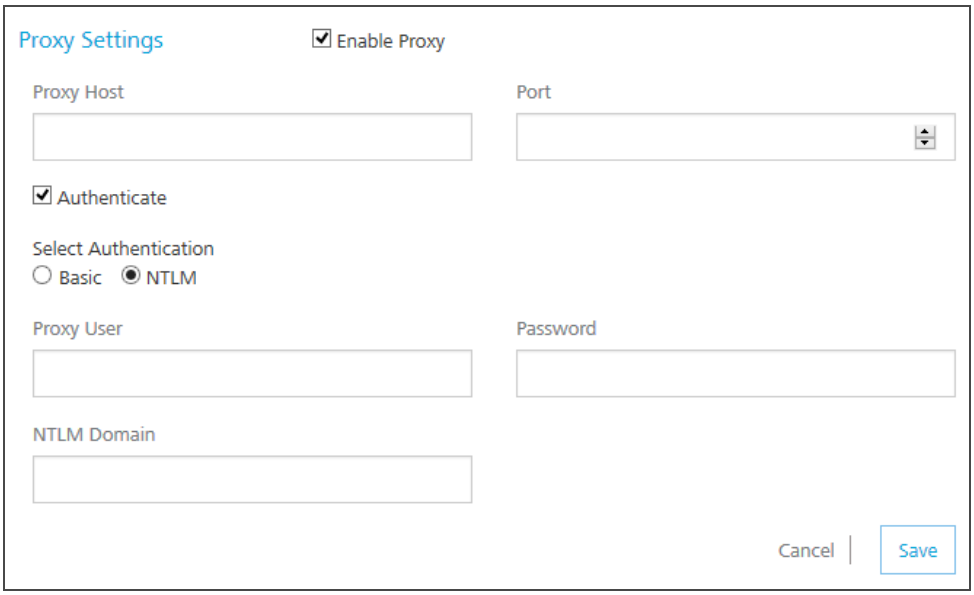
To configure a basic or NTLM proxy, follow these steps:

1. In your Kony Fabric account, click **Settings > Proxy**. The **Proxy Settings** page appears.



2. Select the **Enable Proxy** check box.

3. In the **Proxy Host** text box, enter the IP of the server.



4. From the **Port** text box, enter the port number. The **Port** text box supports port numbers from 1 to 65535.

5. To enable authentication for your proxy, select the **Authenticate** check box, and follow these steps. Otherwise skip to Step 6.

    a. Under **Select Authentication**, select **Basic** or **NTLM**.

    For NTLM authentication, you need to add the following configurations for Kony Studio. Follow these steps:

    - In the **Proxy User** text box, enter the user for the proxy.
    - In the **Password** text box, enter the password for the proxy.
    - In the **NTLM Domain** text box, enter the domain for the proxy.

6. Click **Save** to the save the proxy. The confirmation message appears.

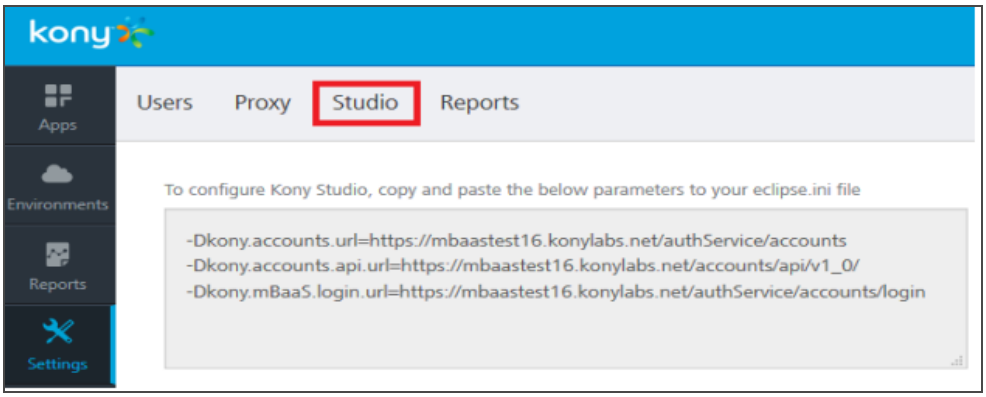
12.2.2 How to Enable a Proxy to an Integration Service

Once a proxy is configured, you can enable the proxy for an integration service. For more details, refer to Creating an Integration Service.

12.3 Studio

The Studio tab lists -D parameters that you need to log in to Kony Studio (IDE.) The parameters are generated during Kony Fabric installation.

To configure Kony Studio, copy and paste the following parameters in the `eclipse.ini` file located in your Kony Studio install folder - for example, `<C:\Program Files\Kony_6.0.3QA\Kony_Studio>eclipse.ini`.



12.3.1 How to Configure -D parameters in Kony Studio

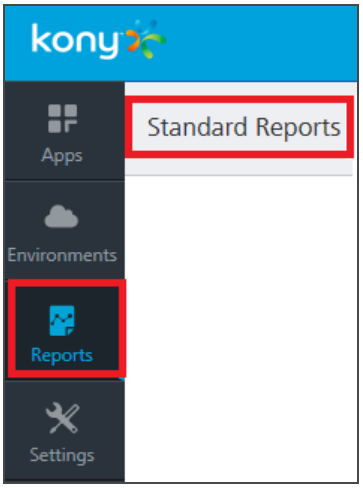
To configure -D parameters in Kony Studio (IDE), follow these steps:

> ***Important:*** If you use secured services (HTTPS), configure Java Runtime Environment (JRE) associated with Kony Studio with CA certificates. If your CA certificate is not configured, the login to Kony Studio fails.
>
> For details, refer to Kony Fabric Install Guide > Troubleshoot with SSL Certificate Issues.

1. Open the `eclipse.ini` file located in your Kony Studio install folder - for example, `<C:\Program Files\Kony_6.0.1GA\Kony_Studio>eclipse.ini`.
2. Copy the **-D parameters** from the **Studio** tab and paste them in the `eclipse.ini` file.
3. Save the `eclipse.ini` file and restart Kony Studio.

12.4 Reports

Under the **Settings**, the **Reports** tab allows you to configure the JasperReports Server. Once you complete JasperReports Server configuration, the **Reports** page (shown below) displays data (reports) from the JasperReports Server.



Currently, the **Reports** page displays only **Standard Reports**. To view standard reports, click the report. For more details on standard reports, refer to Kony Reporting and Analytics - Standard Reports.

12.4.1 How to Configure JasperReports Server

Before configuring the JasperReports Server in the **Reports** tab, ensure that you have installed the JasperReports Server and configured Kony Fabric Console in the JasperReports Server.

1. In your Kony Fabric account, click **Settings** > **Reports**. The **Reports** page appears.
2. In the **Jasper URL** text box, enter the JasperReports Server URL.
3. In the **Username** text box, type jasperadmin.

   > ***Note:*** Note: Enter credentials for jasperadmin. The default credentials for jasperadmin:
   > username = jasperadmin
   > password = jasperadmin

4. In the **Password** box, type `jasperadmin`.
5. Click **Save** to the save the JasperReports Server. The confirmation message appears.

   After you configured JasperReports Server successfully, you can access the standard reports from **Reports** > **Standard Reports** page.