Kony Fabric

Roles and Access Control Guide

Release V8

Document Relevance and Accuracy

This document is considered relevant to the Release stated on this title page and the document version stated on the Revision History page. Remember to always view and download the latest document version relevant to the software release you are using.

September, 2017

Revision History

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

Table of Contents

1. Preface

Kony Fabric is a Mobile Back-end as a Service (MBaaS) provider that helps developers build native and web apps for mobile. Various back-end services are easily integrated with the application irrespective of whether the application is built using JavaScript, PhoneGap, iOS, or Android frameworks.

Kony Fabric allows you to define the back-end to build native mobile apps for iOS, Android, and HTML5-based apps for modern browsers. Kony Fabric ensures that developers build mobile applications quickly by focusing on core areas and obtaining secured back-end services instantly. Kony Fabric has multiple features that can be used - Identity, Integration, Orchestration, Objects, Sync, and Engagement Services. These features can be accessed through a common, centralized console.

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

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

Kony Fabric supports the following back-end services for your applications:

- Identity: This feature allows you to define the type of authentication used for granting access to your application. Kony Fabric supports the following authentication services: Microsoft Active Directory, Salesforce, Security Assertion Markup Language (SAML), Kony SAP Gateway, Kony Facebook, and Kony User Repository.
- Integration: This feature allows you to define various back-end services for your application. You can define the service in XML, SOAP, JSON, Java, Salesforce, and Kony SAP Gateway.

- Orchestration: This feature allows you to create two types of orchestration services. They are:
    - Composite: Allows you to run two or more services concurrently or sequentially.
    - Looping: Allows you to run a single service in a loop until the loop ends or an exit criteria is met.
- Synchronization: This feature allows you to define the synchronization services for your application. Sync supports only Web Services, except SAP Sky.
- Engagement Services: This feature allows you to define and configure push messaging services for your application.

1.1 Purpose

The document helps you familiarize with the Kony Fabric and provide procedural information to perform various tasks required to build your application.

1.2 Intended Audience

This document is intended for developers who would like to turn their applications into an enterprise-grade applications using Kony back-end services.

1.3 Formatting Conventions Used in This Guide

The following formatting conventions are used throughout the document:

Conventions	Explanation
`Monospace`	• User input text, system prompts, and responses • File path • Commands • Program code • File names
Italic	• Emphasis • Names of books and documents • New terminology
Bold	• Windows • Menus • Buttons • Icons • Fields • Tabs • Folders
URL	Active link to a URL.
Note:	Provides helpful hints or additional information.
Important:	Highlights actions or information that might cause problems to systems or data

1.4 Related Documents

Document	Purpose
Kony Fabric Installation Guide Windows	This document explains how to install Kony Fabric and additional software on your Windows computer.
Kony Fabric Installation Guide Linux	This document explains how to install Kony Fabric and additional software on your Linux.

1.5 Contact Us

We welcome your feedback on our documentation. Write to us at techpubs@kony.com. For technical questions, suggestions, and comments, or to report problems on Kony's product line, contact support@kony.com.

2. Console Access Control

Kony Fabric supports access controls for Kony Fabric applications and services. Kony Fabric users who have the permission to create Kony Fabric apps and services can control the access to the applications and services.

For example, an owner invites a new user to the Kony Fabric account. The new user can create a Kony Fabric application and services, and can then control the access by other users to the application. The role of a user determines the access the user has to applications and services, the access control the user can set, and the access control that other users can set for that user. For example, a user who has a member role can create an app and then give full access to the app to specific member users, while setting read-only access for all other member users. Users who have an owner or admin role always have full access to all Kony Fabric apps and services.

2.1 Use Case

The following describes a use case for access control of Kony Fabric applications and services. The scenarios in the use case help you understand how users can control access to applications and services. The use case also shows how the role of a user determines the level of access the user can control, and the user's level of access that other users can control.

Account Owner

1. A user creates a new Kony Fabric account. The user who created the account is the first user and is assigned the Owner role. The user is referred to as the AccountOwner.

   An owner of a Kony Fabric account has full access rights to all Kony Fabric apps that are created on the account. The owner also has permissions to perform create, retrieve, update, and delete (CRUD) operations in all the services in all the apps.

2. The AccountOwner invites AppUser1 and AppUser2 to the Kony Fabric account as members.

   By default, AppUser1 and AppUser2 have the rights to create new apps and services, and have full access to existing apps and services.

Create Applications

1. AppUser1 creates App A that has a Weather Service and a News Service.
2. AppUser2 creates App B that has a GeoLocation Service and ATM Locator Service.

   By default, the applications and services that users create have global read-write access for all users of the account.

Control Access to Applications

1. AppUser2 decides that he needs to protect his App B.
2. From the apps page, AppUser2 selects *Console Access Control* from the App menu.
3. AppUser2 removes general access for all users and adds himself as a specific access user.

   AppUser3 logs in and can no longer see App B in the console. If AppUser2 had set read-only for All Users, then AppUser3 could see the application, but not modify its configuration (for example, add or remove services).

Control Access to Services

1. AppUser2 decides that he needs to control access to a service in his App B from other users.

   Identity, Integration and Orchestration services are shared components. AppUser3 can still go and modify any of those services that would affect the functionality of App B. If AppUser2 wants to completely lock down App B, he would also have to change the access control of all the services associated with the app.
2. AppUser2 opens App A and selects *Console Access Control* from the Settings menu for a service.
3. AppUser2 adds himself as a specific-access user to the service just as he did for App B.
4. AppUser2 downgrades general access for all users to Read Only.

AppUser2 cannot completely remove access for all users to the service. AppUser2 can only downgrade all users from Full Access to Read Only. This is because other users have access to an app, but they do not have access to all the associated services.

Full Access to App and Full Access to Service

In the case where a user has full access to the app and full access to the service:

- The user can add and create new services, unlink the services, switch between versions of a service, delete a version of a service, and save a service as a new version.
- The user can switch between the versions of a service, but cannot save the service or unlink the service regardless of whether the user has read only or full access to the service.

Full Access to App and Read Only Access to Service

In the case where a user has full access to the app and read only access to the service:

- The user can use the Use Existing option to add a service. If the user has full access rights on the service added, the user can modify the service.
- The user can clone a read-only service and gain full access to the new service.
- The user can configure a new service and unlink a read-only service.
- The user cannot edit a read-only service in the app, but the user can save it (clone it) as a new service.
- The user can change the version of the read-only service within the app.
- The user can switch between the versions of the service within the app, as he is configuring the app and not the service. The user can also unlink the same service. However, the user cannot create a new version of the service or delete a version because the user does not have full access to the service.

Read-Only Access to App and Full Access to Service

In the case where a user has read-only access to the app and full access to the service:

- The user cannot modify the configuration of the app, and the Use Existing and Clone services are disabled.
- The user cannot unlink a service or configure new service to the app.
- The user can modify the service, but cannot save it as a new service within the app, because the user does not have full-access rights to modify the app.
- The user cannot change the version of the service within the app.

Read-Only Access to App and Read-Only Access to Service

In the case where a user has read-only access to both the app and service:

- The user cannot modify the configuration of the app, and the Use Existing and Clone services are disabled.
- The user cannot unlink a service or configure a new service to the app.
- The user cannot edit the service and save it as a new service from within the app.

2.2 How to Use Access Control

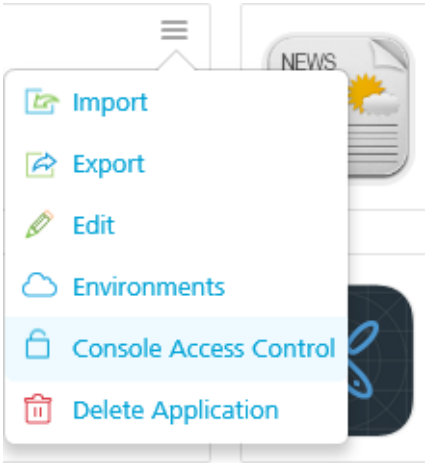
You can configure access control for Kony Fabric applications and services. By default, all users have full access rights to create and access apps and services. Use the Apps Console Access Control page to control access to an applications. Use the Services Console Access Control page to control access to a service.

2.2.1 How to Use Access Control for Applications

You can access the Apps Console Access Control page from the Applications page or from within an app.

To set access control from the Applications page, do the following:

1. From Kony Fabric Console, click **Apps** to display the Applications page.
2. In the **Applications** page, hover your cursor over the **App menu** button of an app.



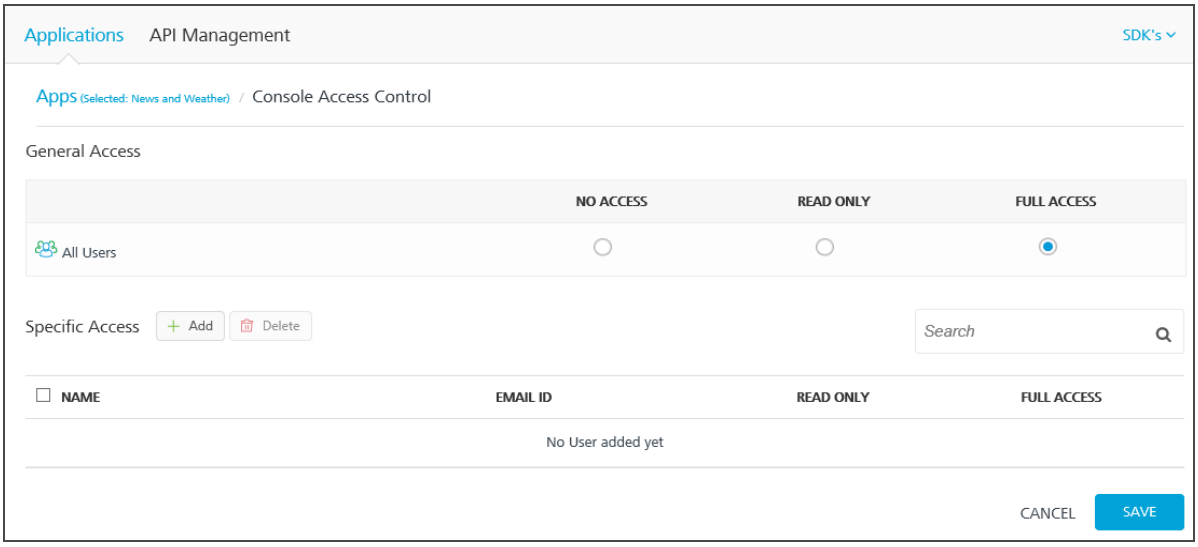
3. Click **Console Access Control**.

   The Apps Console Access Control page appears.

To set access control from an app, do the following:

1. From Kony Fabric Console, click **Apps** to display the Applications page.
2. In the **Applications** page, select an app.
3. Click the Console Access Control button (the lock icon).

   The Apps Console Access Control page appears.



To set general access to an app for all users, do the following:

- In the **General Access** area, for **All Users**, select an access control option.

  By default, all users have full access rights to create and access apps. If you want to block access to any of the other members on the account, select No Access. Users with no access permissions cannot access the app, and the app does not appear on the Applications page.

  Before you select No Access on the General Access level, add yourself or another user on the Specific Access level.

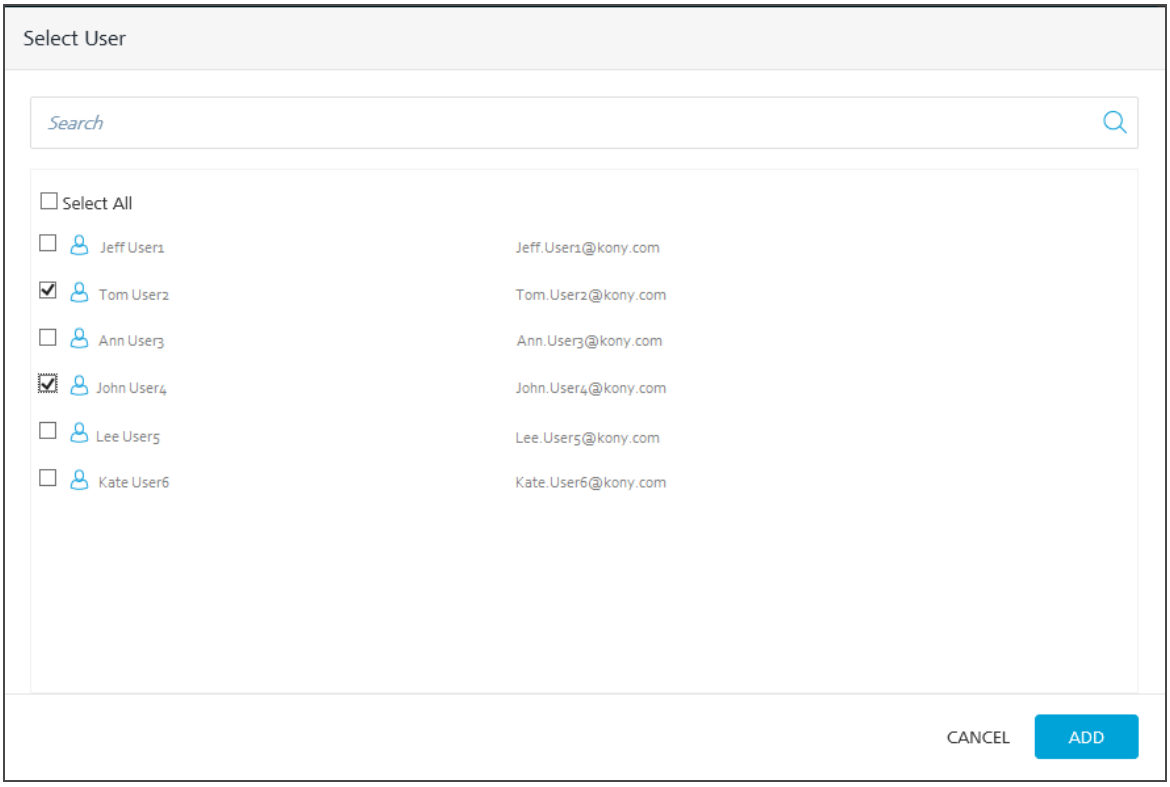
To set specific access to users for an app, do the following:

1. In the **Specific Access** area, click **Add**.

   The Select User windows appears. All the owners and admins might not be shown in the list of Specific Access users.

2. Select the users that you want to add to the Specific Access list.

   The Select User window appears.



3. Click **Add**.

   The users that you selected are added to the Specific Access list.

4. Select the access control option.

   Note that the read-only option for a user is disabled if the general access permission is set to full access. You cannot set access control for specific access at a setting lower than the general access setting.

5. Click **Save**.

If a member user gives a second member user Full Access permission for an app, both member users have the same permissions for the app.

To remove specific access to users for an app, do the following:

1. In Specific Access, select the users that you want to remove.
2. Click the **Delete** button.

   You can hover your cursor over a user, and then click the Delete icon.

What Full Access Permission for an App Means

- A user with full access can link or unlink any services to the app. The user can publish the app if the user has permissions to publish for that environment.
- A user with full access has permission to configure and change the control access list.

What Read-Only Permission for an App Means

- A user with read-only access cannot link or unlink any services to the app.
- A user with read-only access cannot configure or change the control access list for the app.

2.2.2 How to Use Access Control for Services

You access the Services Console Access Control page from within an application or from API Management.

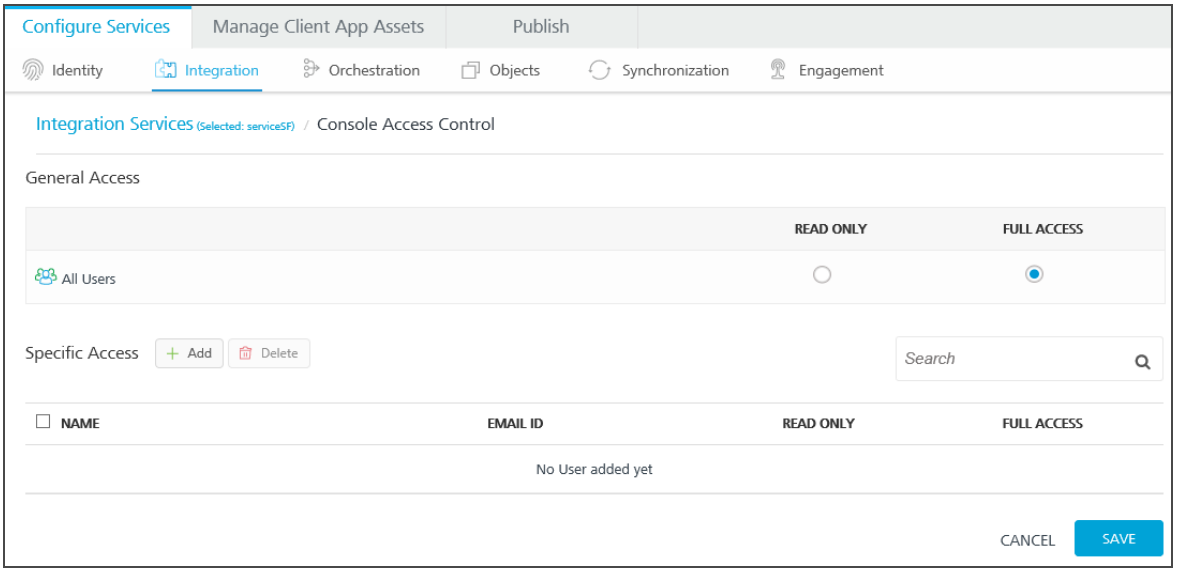
By default, all the services created have Full Access for all users. You can control access to integration services, orchestration services, and object services by setting the access control for the service. For example, UserA decides to give read-only access to all users for an integration service (General Access), and give full access to the service to UserB (Specific Access).

To set access control for a service from an app, do the following:

1. From Kony Fabric Console, click **Apps** to display the Applications page.
2. In the **Applications** page, open an app.
3. In the **Configure Services** tab, click the Integration, Orchestration, or Objects service tab.

4. Hover your cursor over the required service, click the **Settings** menu. Click Console Access Control.

   The Services Console Access Control page appears.



To set access control for a service from API Management, do the following:

1. From Kony Fabric Console, click **Apps** to display the Applications page.
2. In the **Applications** page, click **API Management**.
3. Click the Integration or Orchestration service tab.
4. Hover your cursor over the required service, click the **Settings** menu.Click **Console Access Control**.

   The Services Console Access Control page appears.

To set general access to a service for all users, do the following:

- In the **General Access** area, for **All Users**, select an access control option.

  By default, all users have full access rights to create and access services. Before setting the general access to read-only for all users, give specific access to at least one user. For example, UserA adds UserB to the Specific Access user list and gives UserB full access. Then UserA sets Read Only for General Access. UserB now has full access to the weather services but another member user, User3, has read-only access.

To give specific access to users for an app, do the following:

1. In the **Specific Access** area, click **Add**.

   The Select User windows appears. All the owners and admins might not be shown in the list of Specific Access users.

2. Select the users that you want to add to the Specific Access list.

   The Select User window appears.

3. Click **Add**.

   The users that you selected are added to the Specific Access list.

4. Select the access control option.

   Note that the read-only option for a user is disabled if the general-access permission is set to full access. You cannot set access control for specific access at a setting lower than general access setting.

5. Click **Save**.

3. Index