Collins Aerospace
An RTX Business

Izon Connected Platform

Setup Guide

ARINCDIRECT, a part of Collins Aerospace
2551, Riva Road
Annapolis, MD 21401-7435
USA
CAGE CODE: 83S81

We try to supply publications that are free of errors, but some can occur. If a problem is found with this publication, you can send the necessary data to Collins Aerospace. When you report a specified problem, give short instructions. Include the publication part number, the paragraph or figure number, and the page number.

To send data to Collins Aerospace about this manual:

Address: Collins Aerospace
2551 Riva Road, M/S 291-100
Annapolis, MD 21401-7435
USA
Email: ATDS@collins.com

For technical support, please contact:

Email: flightops@arinc.com
Phone: 1.410.266.2266

PUBLICATION COPYRIGHT HISTORY

Revision History		
Date	**Revision**	**Description**
07-Oct-2021	0.0	Initial Issue.
12-Jul-2022	1.0	Template and branding template.
16-Jan-2023	2.0	Added Multi-Factor Authentication.
30-Oct 2023	3.0	Updated branding and support email address.
5-Dec 2023	4.0	Updated user profile format and session timeout length.

Table of Contents

List of Figures

List of Tables

No table of figures entries found.

1 Purpose

This document provides guidance on how to register and configure an account on Izon, the Collins Connected Platform. Direction is also given on how to navigate the Izon Store and how to provide feedback.

2 Registration

To access the **Izon** platform, all customers need to create an **Izon** account. Please visit www.collinsizon.com to create your account. One of the first initiatives delivered with the **Izon** platform is the ability to enable Single Sign-On capabilities for customers to access all their Business Aviation features and services.

When creating an **Izon** account, it's important to remember the registered account email and password as this is the primary identity that ties all the customer's Business Aviation applications together. There are no requirements on email usage for setup, however, password requirements are displayed during the registration process.

Once registered with an email address and password, the registered account is required to be authenticated. Customers will need to check the email address used during registration to verify identity. The customer should receive an email from do-not-reply@collinsizon.com.

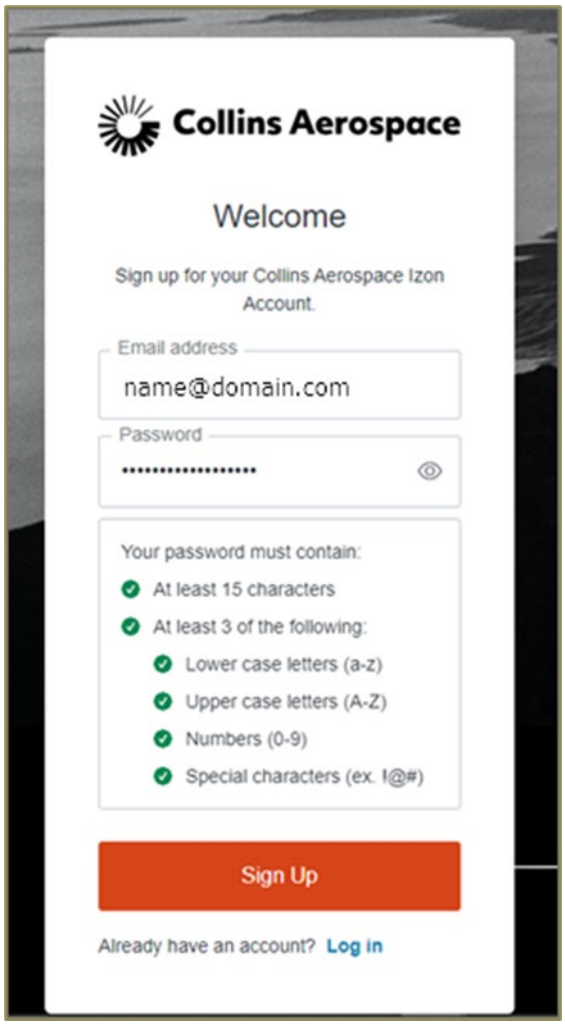

Figure 2-1: Izon Account Registration

If the account is not authenticated *within one hour* of receiving the email, customers will need to login to Izon using their credentials and they will be taken to the "Check Your Email" page where customers can request another verification email. After the account has been verified, please proceed with the onboarding process.

***Note:** It is possible that emails are sent to a junk or spam folder. Therefore, it is recommended to check these folders if an email does not appear in the Inbox within a few minutes.*

To access Izon, it is a requirement to review and accept the Terms and Conditions, as well as acknowledge the Cookie Consent, prior to creating a profile.

3 Creating Your Account

3.1 Linking Of Accounts

You've made it. Welcome to Izon! Now it's time to link existing flight planning account(s) from ARINCDirect. Fill in your ARINCDirect credentials when prompted after the email authentication.

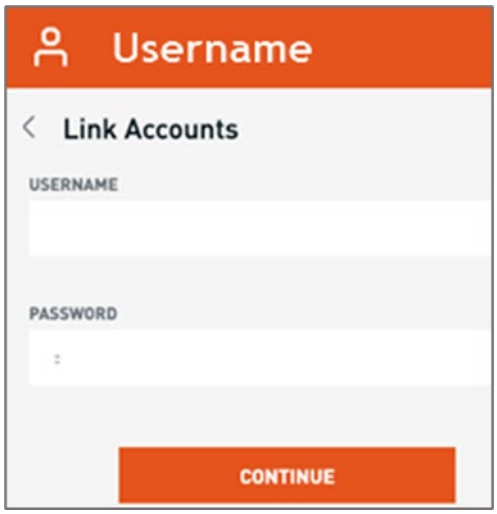

Figure 3-1: Create Account - Link Accounts

***CAUTION:** When signing up for an **Izon** login, if an ARINCDirect account is not linked within 30 days **Izon** will delete the newly created account.*

Linking more than one account will give access to the **Izon Dashboard** and enable the ability to switch between accounts effortlessly. If connecting multiple accounts, navigate to the upper right-hand corner of the **Izon Dashboard**. See Account Management – Section 3.2 for instructions on linking additional accounts.

3.2 Account Management

At any point in the **Izon** journey, the ability to link existing ARINCDirect account(s) is available. Navigate to the **Account Management** corner, click on the Context Menu and **Linked Accounts.**

Figure 3-2: Create Account - Account Management

A window will open from the side of the page, with the ability to **Link Another Account**.

Click **Link Another Account** and enter the username and password credentials to authenticate the linking of the account.

Within this management window, an account may also be removed.

At any point during your **Izon** journey, transitioning between linked ARINCDirect accounts is seamless. Navigate to **Account Management** (upper right-hand corner), select the Context Menu and the **Active Account** bar dropdown menu and select a different account.

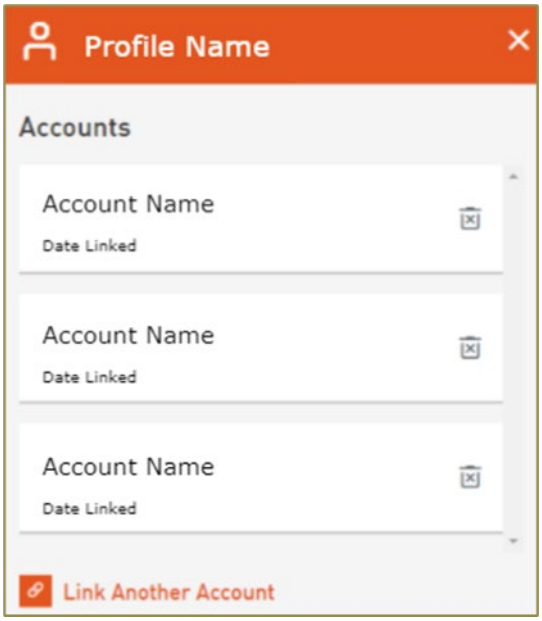

Figure 3-3: Account Management - Profile Name

After transition to a different account within the **Account Management** window, remember that any opened applications within the initial ARINCDirect account will be signed out as part of the Single Sign-On functionality.

When choosing to work in Izon applications after switching accounts in the **Account Management** window, relaunch of the applications from your **Izon Dashboard** is required. Because of **Izon's imbedded security design**, this workflow is in place to mitigate any account confusion while working in open applications launched from the platform.

4 Izon Dashboard

4.1 Application Toolbar

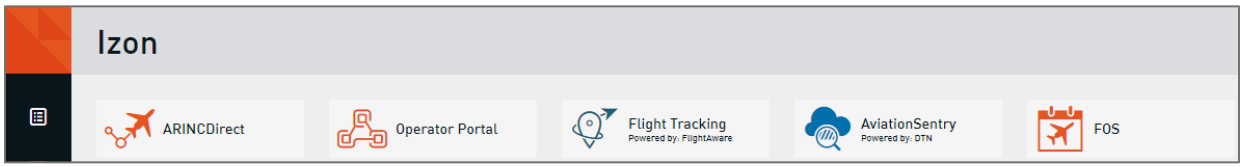

Figure 4-1: Izon Dashboard - Application Toolbar

When launching the Izon Dashboard, an **Application Toolbar (AT)** is displayed at the top of the **Dashboard**. The **AT** is a space dedicated for applications frequently visited and consists of several applications. The ability to reorder, add, and remove applications is available on the menu located on the right-hand side by clicking on the three dots.

5 Session Timeout/Logout

A session timeout will occur for **Izon** after 55 minutes of inactivity. After 55 minutes, the customer will be presented with a **Session Timeout** notification warning the customer they have five (5) minutes to refresh their activity and remain logged into **Izon**. If no activity is taken place in that additional five minutes, the customer is safely logged out of **Izon**. The ARINCDirect applications, will continue to have a timeout of approximately 60 minutes applied for inactivity.

When ready to logout out of Izon, navigate to the **Account Management** section and click the three dots to logout. When logging out of **Izon**, the ARINCDirect and Operator Portal applications will also be logged out.

6 Feedback

The **Feedback** interface is the most important feature of the new **Izon** platform as customer evaluation will be critical to ARINCDirect's success and dictate how the platform is shaped and built. A user's credentials will auto-populate when submitting feedback for ease of use.

6.1 How to Report an Issue or Send Feedback on a Desktop

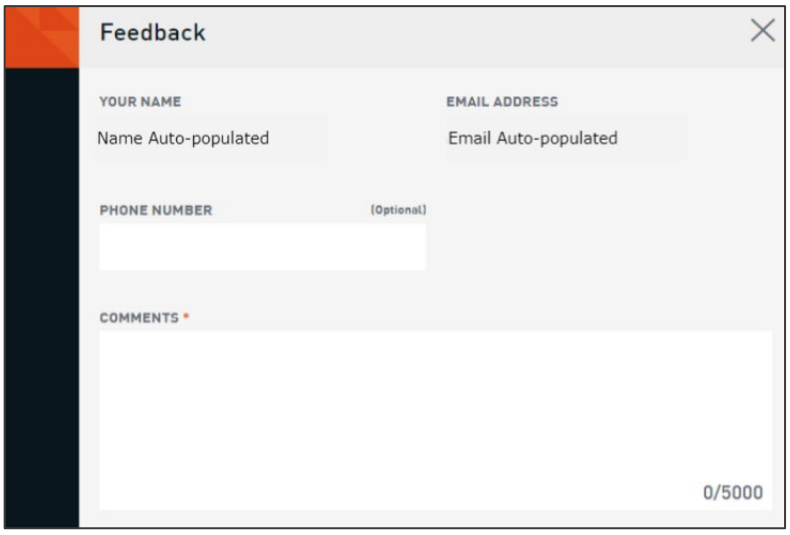

Figure 6-1: Feedback

1. Open the **Izon** Dashboard on desktop.
2. Navigate to the **Navigation Rail Bar** on the far left-hand side.
3. Click on the **Feedback** icon located on the bottom of the **Navigation Rail Bar.**
4. Submit feedback in the open form.

6.2 How to Report an Issue or Send Feedback on a Mobile/Tablet Device

1. Open the **Izon Dashboard** on the mobile device.
2. Click the "hamburger" icon in the top left of the screen to open the **Navigation Rail Bar.**
3. On the Navigation Rail Bar, click on **Feedback.**
4. Submit feedback in the open form.

The **Send Feedback** function will forward the information to a support team that will address the issue promptly.

Figure 6-2: Send Feedback

7 Multi-Factor Authentication

Enhanced security measures are available that provides extra protection for individual accounts. Multi-Factor Authentication (MFA) is available for all Izon customers.

7.1 What is MFA?

Multi-Factor Authentication (MFA) is a verification method that requires more than one type of customer verification. MFA reduces the chance of cybersecurity attacks as MFA provides added layers of security to protect customers and their data. In addition, this additional security protocol can help meet regulatory requirements.

7.2 How does MFA work?

MFA requires an additional authentication method beyond just username and password. Customers will need to provide further proof of identity to access Izon and Izon's applications. There are several MFA methods available for Izon customers. See details below.

7.3 Available MFA Methods

7.3.1 Push Notification

Push notifications are sent to a customer's device, typically a mobile device or tablet, from which a customer can instantaneously enable or deny account access via the simple press of a button. Push notifications can only be enabled with the Auth0 Guardian Application.

7.3.2 One-Time Passcode

A customer can generate a one-time passcode that changes over time to validate access to their Izon account. One-Time Passcodes can be enabled with any authenticator of the customer's choice.

7.3.3 SMS/Text Message

If the customer prefers to not install additional applications/authenticators to their device, there is a Text Message option that can be enabled for MFA. This option enables the customer to send a one-time passcode over SMS which the customer is prompted to enter into Izon before a customer has access to their account. This method of authentication is not the most reliable option as it's the least secure of the three. Note: Standard message and data rates may apply when using this method.

7.4 Navigating to MFA within Izon

When launching an Izon session and upon landing on the Dashboard page, navigate to the context menu (three dots) within the User Profile window in the upper right-hand corner.

Clicking these dots will display a profile window with the option "Security Settings". Click on the "Configure Multi-Factor Authentication" option to display available MFA methods of your choice.

7.5 Configuring MFA

The Secure Your Account window will display different options for MFA within Izon.

7.5.1 Push Notification

1. Push Notifications can only be enabled within the Auth0 Guardian App. To implement this MFA method, download the Auth0 Guardian App either from the App Store on an Apple device, or Google Play for an Android device.
2. Once the third-party app is installed, continue to the next page to scan the QR code to register a device.
3. Open the Authenticator app on your device and click “+” to install a new authentication.
4. If successfully registered, the next screen displays a recovery code. This recovery code is to be used in the event the registered device has been misplaced or cannot authenticate. To finish enrollment, the customer must acknowledge the code by checking the box next to “I have safely recorded this code.”
5. Congratulations, you’re enrolled!

7.5.2 One-Time Passcode

1. One-Time Passcodes can be enabled with any authenticator of the customer’s choice. To begin, download the authenticator of choice to proceed (Google Authenticator, Microsoft Authenticator, Cisco Duo Mobile, etc.).
2. Once the third-party app is installed, please continue to the next page to scan the QR code to register the device.
3. Follow the instructions on the authenticator app to set up a new MFA account.
4. Scan the QR code within the Izon MFA enrollment process. Upon successfully scanning of the QR Code, a 6-digit code is provided in the authenticator application. Enter the 6-digit code as displayed in the authenticator application with no special characters, spaces, or hyphenations. Note: Please be aware that codes may change every few seconds as instructed by each authenticator application.
5. If successfully registered, the next screen displays a recovery code. This recovery code is to be used in the event a registered device has been misplaced or cannot authenticate. To finish enrollment, the customer must acknowledge the code by checking the box next to “I have safely recorded this code.”
6. Congratulations, you’re enrolled!

7.5.3 SMS/Text Message

1. To begin, a valid phone number and mobile device is required.
2. The first screen upon SMS enrollment will request the customer to choose their Country Code of choice.
3. The phone number must only contain valid numbers, with no special characters, spaces, or hyphenations. Once a valid phone number with ten digits is provided, click continue.
4. The next screen will ask for a 6-digit code that is sent to the mobile device number that was provided. Enter the 6-digit code as displayed in the SMS message with no special characters, spaces, or hyphenations. Note: The text message with the 6-digit code has an expiration time of three (3) minutes. After that, a request to resend another code is required.
5. If successfully registered, the next screen displays a recovery code. This recovery code is to be used in the event a registered device has been misplaced or cannot authenticate. To finish enrollment, the customer must acknowledge the code by checking the box next to “I have safely recorded this code.”
6. Congratulations, you’re enrolled!

7.6 Deleting MFA Methods

To remove an MFA method, take the following steps.

1. Navigate to the Multi-Factor Authentication enrollment window.
2. Click on the drop-down arrow for the selected MFA method to be removed.
3. Click the trash-can icon.
4. The selected MFA method will be removed as well as the device.

8 Izon Store

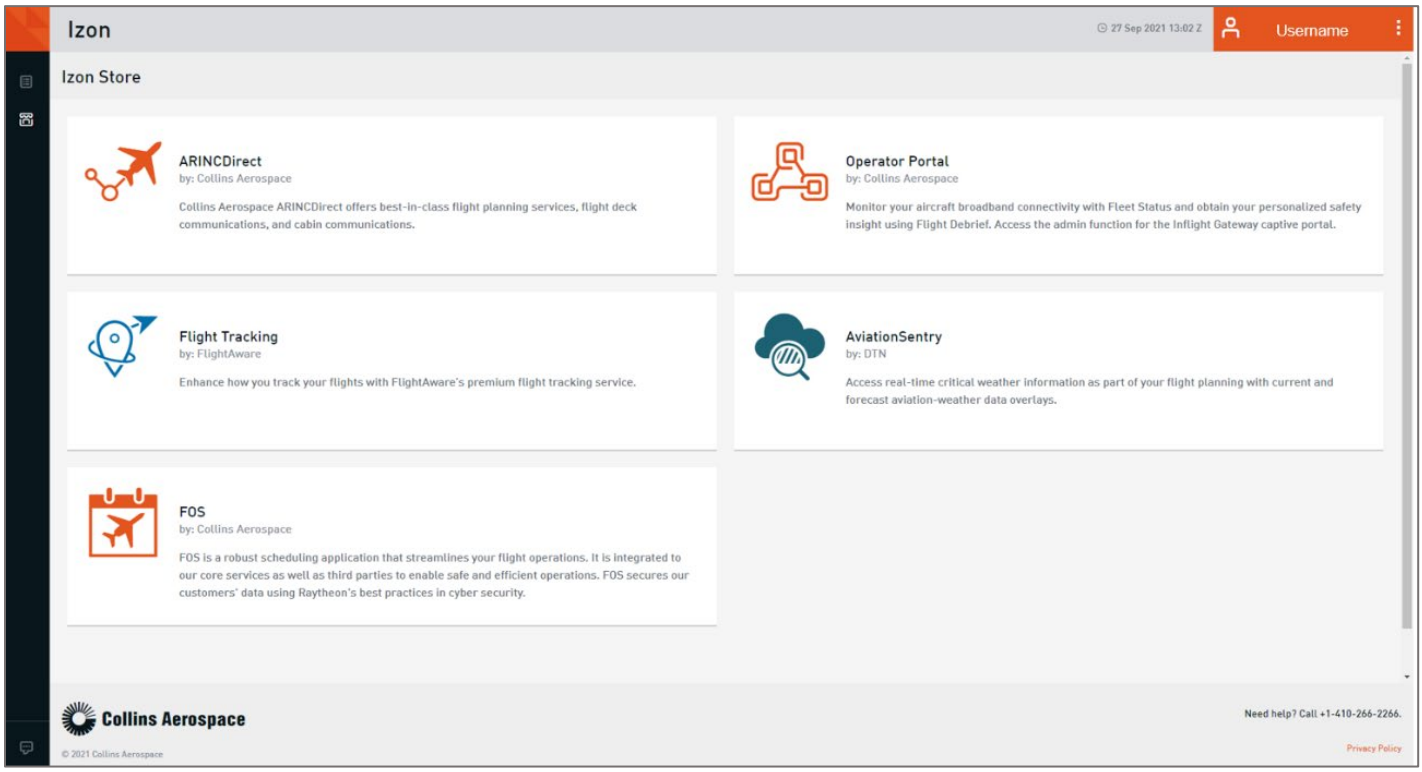

Figure 7-1: Izon Store

The **Izon Store** is designed to deliver ARINCDirect's long-term strategy of technology enabling third-party applications and services hosted on the Izon platform and engineered with future single sign-on capability. Several applications are available for use in the **Izon Store**, and more applications are slated in forthcoming enhancements.

9 Support

For additional support please submit feedback with your question, comment, or concern, or email our support team at flightops@arinc.com.

Appendix A Acronym List

Term	Definition
AT	Application Toolbar
MFA	Multi-Factor Authentication