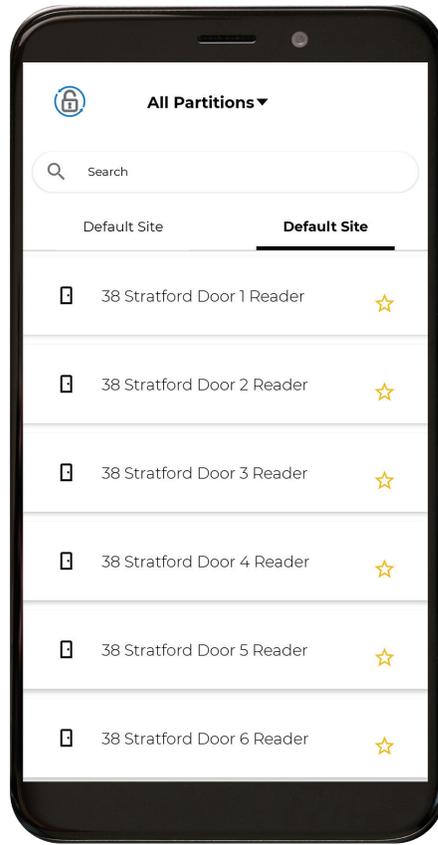


AC SERIES

AC Key Programming Guide



Introduction

This is a guide to setting up AC Key for the AC Series access control system. AC Key is a mobile app available for Apple® iOS and Google Android™ that allows users to unlock connected doors and issue temporary passes to visitors. Both AC Key and visitor pass activity is recorded in AC Nio™, allowing administrators to keep track of site traffic.

This guide assumes that the AC Nio™ software is fully configured and operational. If that is not the case, refer to the AC Series - Quick Start Guide available at <https://www.aiphone.com/ACSeriesQuickStartGuide> before continuing.

AC Nio™ Configuration

Before the AC Key apps can be added to the system, AC Nio™ will need to be configured to allow the connection.

Configuring AC Nio™ for Remote Access

Log in to AC Nio™ using a web browser. Navigate to **Administration**, System Settings.



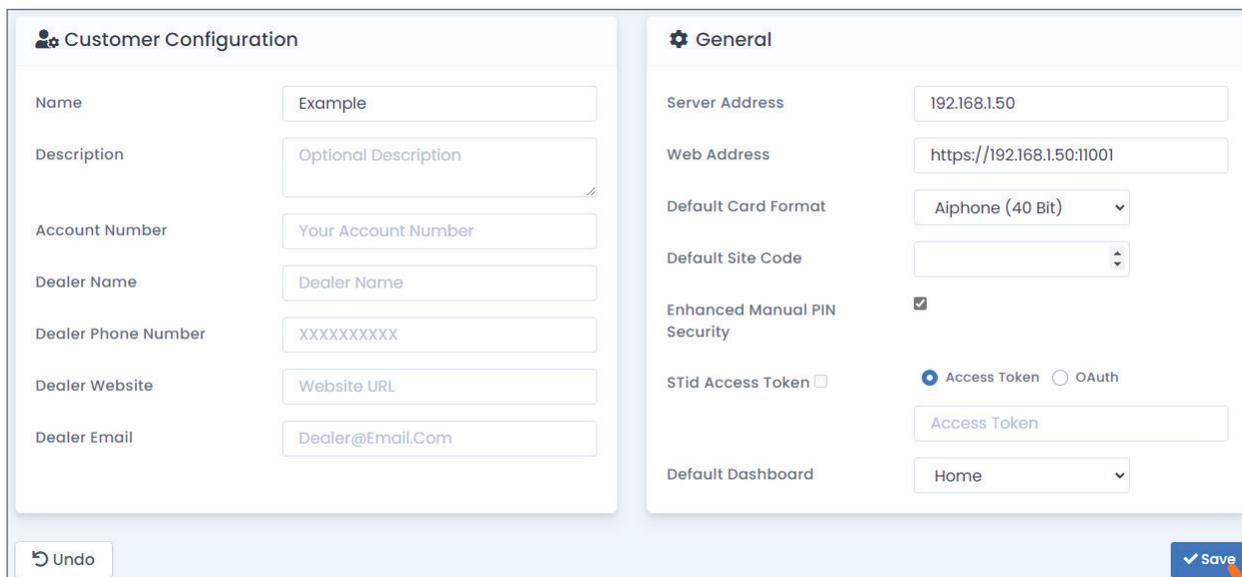
AC Key can be configured for on-site or for off-site use. On-site use allows users to operate AC Key while connected to the local WiFi network. There will need to be routing in place between the subnet the AC Key users will be on and the AC Nio™ host to facilitate the connection.

Off-site use allows the mobile device to operate AC Key while connected to any WiFi or cellular connection. A VPN is recommended for remote usage. However, port forwarding using the connection port for AC Nio™ would allow access via public IP. Consult the network administrator as needed.

Select **General Configuration**. Under Web Address, enter the hostname or IP address with the connection port of the PC or host running AC Nio™.

Example: <https://192.168.1.50:11001>

Click **Save**.

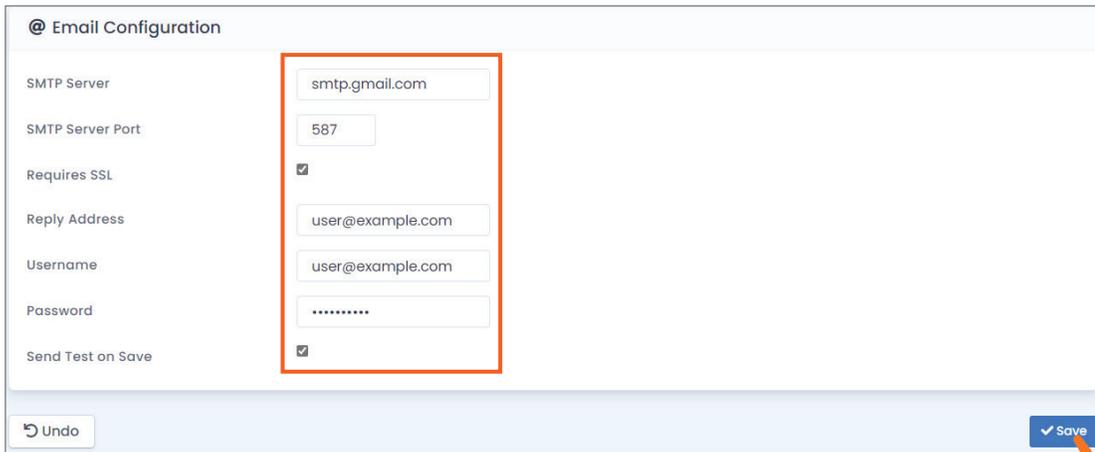
A screenshot of the AC Nio™ General Configuration page. The page is divided into two columns. The left column is titled 'Customer Configuration' and contains fields for Name (Example), Description (Optional Description), Account Number (Your Account Number), Dealer Name (Dealer Name), Dealer Phone Number (XXXXXXXXXX), Dealer Website (Website URL), and Dealer Email (Dealer@Email.Com). The right column is titled 'General' and contains fields for Server Address (192.168.1.50), Web Address (https://192.168.1.50:11001), Default Card Format (Aiphone (40 Bit)), Default Site Code (empty), Enhanced Manual PIN Security (checked), STid Access Token (unchecked), Access Token (radio button selected), OAuth (radio button unselected), and Default Dashboard (Home). At the bottom right, there is a blue 'Save' button with a checkmark, which is pointed to by an orange hand icon.

Configuring Email

An email account is required to send user credentials. Navigate to **Administration**, System Settings. Select **Email Configuration**.



Enter the SMTP and account information for the desired email account. The settings shown in the screenshot are only an example; consult with the network administrator for the proper settings. It is recommended to select Send Test on Save to confirm that the information is properly configured. Click **Save** and ensure that the confirmation email has arrived.



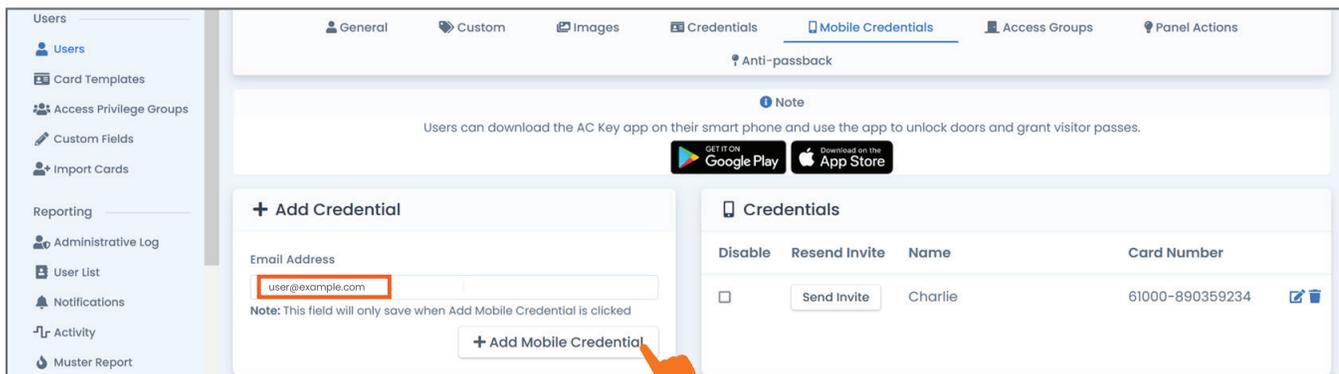
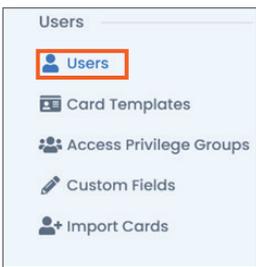
A screenshot of the Email Configuration form. The form fields are: SMTP Server (smtp.gmail.com), SMTP Server Port (587), Requires SSL (checked), Reply Address (user@example.com), Username (user@example.com), Password (masked with dots), and Send Test on Save (checked). The fields are highlighted with a red box. At the bottom right, there is a blue Save button with a checkmark, which is pointed to by an orange hand icon.

i The SMTP settings shown in the screenshot are only an example. Consult with the network administrator for the proper settings.

Creating Mobile Credentials

Before AC Key can be configured, the user needs to be created in AC Nio™. The steps for adding users are including in the AC Series Quick Start Guide linked on page 2 of this guide. Once the user exists, they can be assigned a mobile credential.

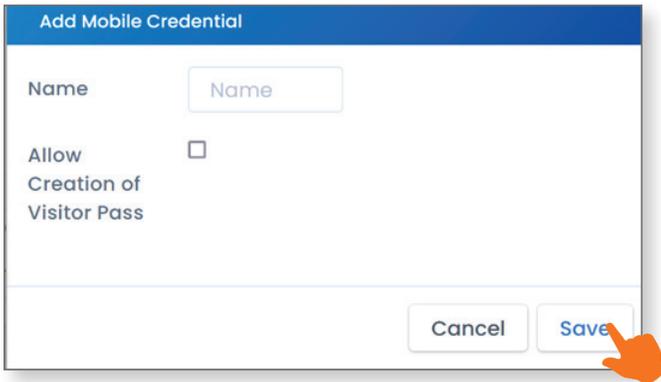
Navigate to Users. Select **Mobile Credentials**. Enter the user's email. Click **Add Mobile Credential**.



A screenshot of the Mobile Credentials page. The page has a navigation bar with tabs: General, Custom, Images, Credentials, Mobile Credentials (selected), Access Groups, and Panel Actions. Below the navigation bar, there is a note about downloading the AC Key app. The main content area has two sections: "Add Credential" and "Credentials". The "Add Credential" section has an "Email Address" field with "user@example.com" entered, which is highlighted with a red box. Below the field is a "Note: This field will only save when Add Mobile Credential is clicked" and a "+ Add Mobile Credential" button, which is pointed to by an orange hand icon. The "Credentials" section has a table with columns: Disable, Resend Invite, Name, and Card Number. The table contains one row with "Charlie" as the name and "61000-890359234" as the card number.

Creating Mobile Credentials *(continued)*

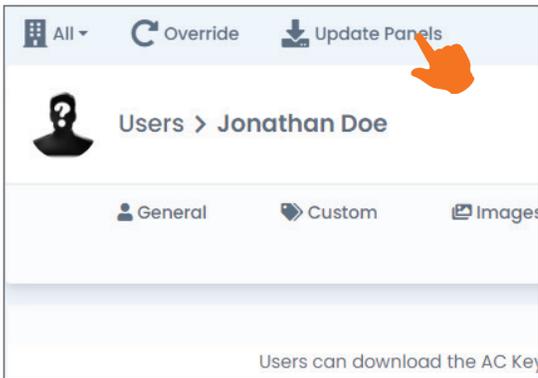
A popup window will appear. Enter a name for the Mobile Credential. If the user needs the ability to grant visitor passes, select the checkbox for **Allow Creation of Visitor Pass**. Click **Save**.



This will add an entry in the Credentials section to the right. If the invitation email was not received, click **Send Invite** under Resend Invite to send it again.

Updating Settings

To finish adding the credential to AC Nio™, click **Update Panels**.



AC Key Registration

Once AC Nio™ is prepared for AC Key access, users' mobile apps will need to be registered. AC Key can be installed on a variety of compatible phones and tablets. For simplicity, the term mobile device is used going forward.

AC Key requires iOS® version 13.4 or higher, or Android™ 5.1 or higher on a mobile device with Google Play™ support, and is available in the Apple® App Store® and Google Play for Android.

Installing AC Key

Search the mobile device's app store on the mobile device for AC Key and install the app. If the app does not show up in the search, the mobile device may not meet the requirements to run AC Key.

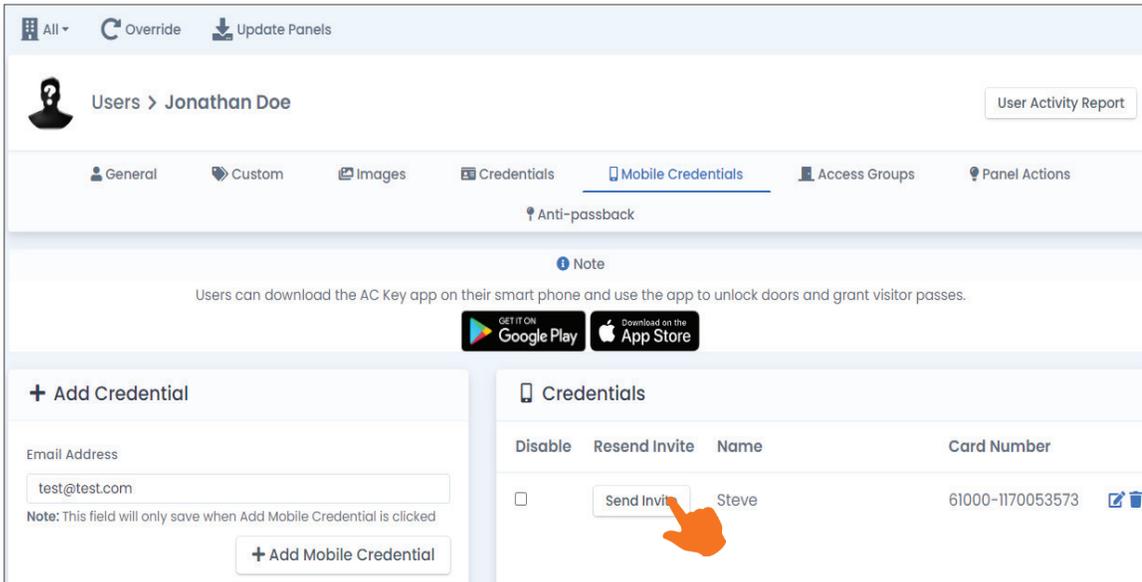
Verifying Connection

If a user will only use AC Key while on site, make sure that the mobile device is connected to the same WiFi network as the PC or other host running AC Nio™. While in operation, the mobile device will need to either have a reserved IP address in the same range as the AC Nio™ host, or routing will need to be configured. Consult the network administrator as needed.

If AC Key will be used remotely, the mobile device can access the system from any cellular or WiFi connection. However, port forwarding will need to be configured on the AC Nio™ host's network to allow access. Consult IT as needed.

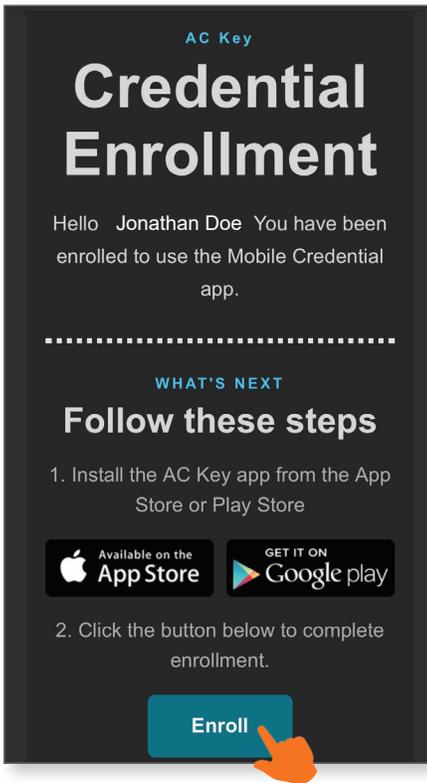
Activating AC Key

If the new user has not received an email notification yet, return to AC Nio™ and navigate to Users. Click the gear box next to the user's name. Select **Mobile Credentials** and click **Send Invite** to resend the email. If the email has still not arrived at that point, check the junk or spam folder on the new user's email account.



The screenshot shows the AC Nio user management interface. At the top, there are navigation options: All, Override, and Update Panels. Below that, the user profile for Jonathan Doe is shown, with a User Activity Report button. The main navigation bar includes General, Custom, Images, Credentials, Mobile Credentials (selected), Access Groups, and Panel Actions. Under Mobile Credentials, there is an Anti-passback section and a Note stating: "Users can download the AC Key app on their smart phone and use the app to unlock doors and grant visitor passes." Below the note are links to download the app on Google Play and the App Store. The main content area is split into two panels. The left panel is titled "+ Add Credential" and contains an "Email Address" field with "test@test.com" and a "+ Add Mobile Credential" button. The right panel is titled "Credentials" and contains a table with columns: Disable, Resend Invite, Name, and Card Number. The table has one row for a credential named "Steve" with card number "61000-1170053573". An orange hand icon points to the "Send Invite" button in the "Resend Invite" column for the "Steve" credential.

Once the email is received, open the email on the new user's mobile device and tap **Enroll**. This will open AC Key. Depending on the operating system version and settings on the mobile device, the link may open directly in AC Key or via a web browser with a prompt that opens AC Key. This will automatically import the necessary information. Once the information has been imported, proceed to **Agreeing to the Privacy Policy** on the next page.

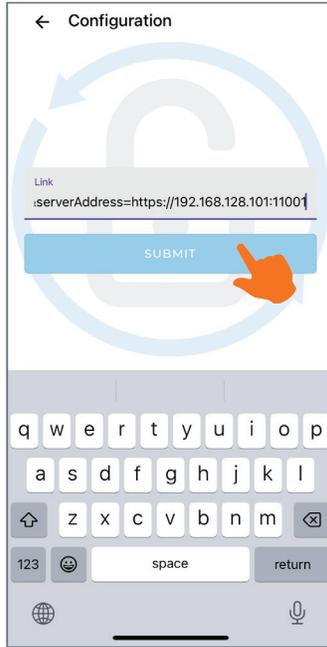
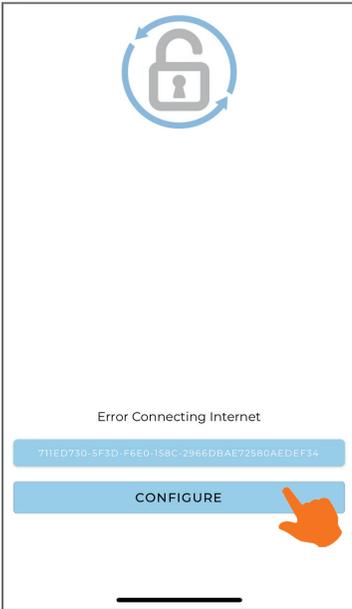


The screenshot shows the AC Key mobile enrollment screen. At the top, it says "AC Key" and "Credential Enrollment". Below that, it says "Hello Jonathan Doe You have been enrolled to use the Mobile Credential app." There is a dashed line separator. Below that, it says "WHAT'S NEXT" and "Follow these steps". Step 1 is "1. Install the AC Key app from the App Store or Play Store". Below step 1 are buttons for "Available on the App Store" and "GET IT ON Google play". Step 2 is "2. Click the button below to complete enrollment." Below step 2 is a blue "Enroll" button with an orange hand icon pointing to it.

Resolving AC Key Activation Errors

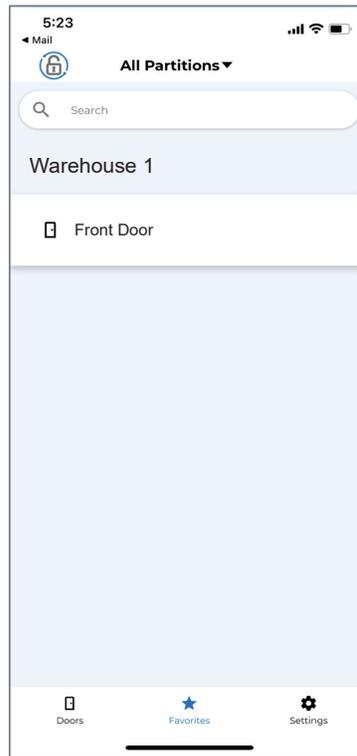
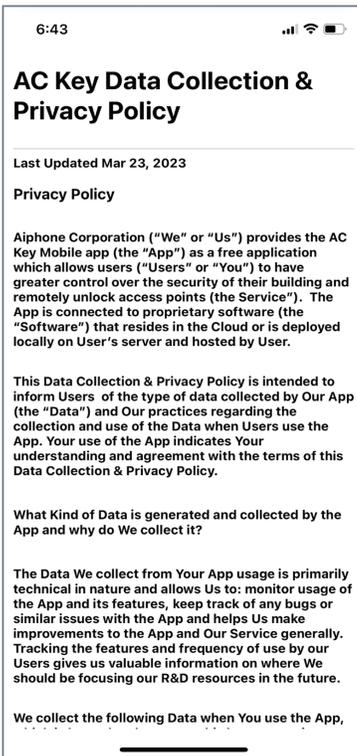
If the information was not imported successfully, an error message, "Error Connecting Internet," will appear. To resolve the error, navigate back to the email and copy the email link by performing a long press on **Enroll** and choosing the **Copy** prompt. Open AC Key. The "Error Connecting Internet" message will appear again. Tap **Configure**.

Enter the link by performing a long press in the **Link** box and choosing the **Paste** prompt. Tap **Submit** to proceed with the activation.



Agreeing to the Privacy Policy

A privacy policy page will open. Scroll to the bottom and agree to the privacy policy. Once this is done, AC Key registration is complete, and the app will be available to use on the phone.



For more details about the features and information above, please contact Technical Support.