

Predict | Protect | Prevent

ARCON | PAM

ARCON Authenticator Guide

Table of Contents

1. Overview	3
2. Pre-Requisite	3
3. Enabling Multi Factor Authentication - Mobile OTP	3
4. ARCON PAM Mobile OTP - Self Registration	3
4.1 Download and Install ARCON PAM Authenticator	3
4.2 Self-Registration	5
5. Post Mobile OTP Registration	7
6. Mobile OTP Registration for Multiple Instances	9

1. Overview

One-time Passwords or OTP considered as a secure way of dual factor authentication. Mobile one time password (OTP) configuration is one of the dual factor authentication. It is used by mobile users by implementing the application on mobile, in order to securely login into ARCON PAM. The users will have to download and install **ARCON Authenticator** App from **Google Play Store** to the mobile device to configure mobile OTP dual factor authentication.

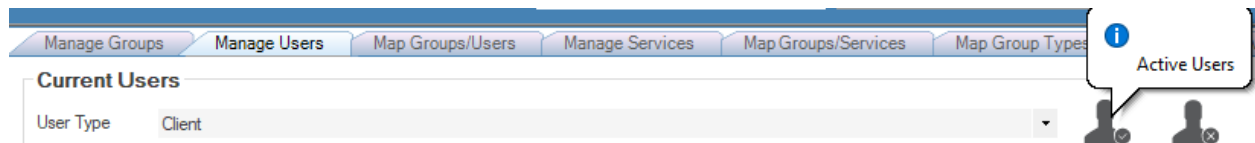
2. Pre-Requisite

- ARCON Authenticator shall be compatible only with ARCON PAM 4.8.5.0_U3 and above.

3. Enabling Multi Factor Authentication - Mobile OTP

In order to enable Mobile OTP use following path:

1. Server Manager → Manage User → Click Active User

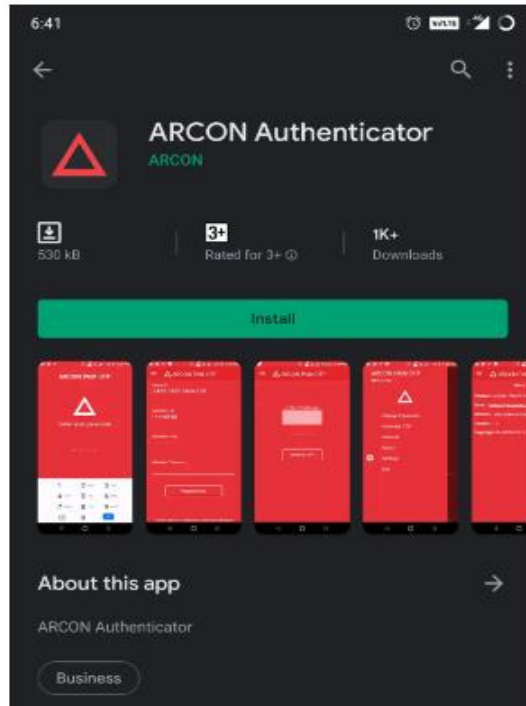


2. Select the User from the Active User List
3. Right Click on User → Edit User Setting
4. Select the Dual Factor Authentication Type as Mobile OTP and click Enable Dual Factor Type checkbox and Click Enforce Self Registration.

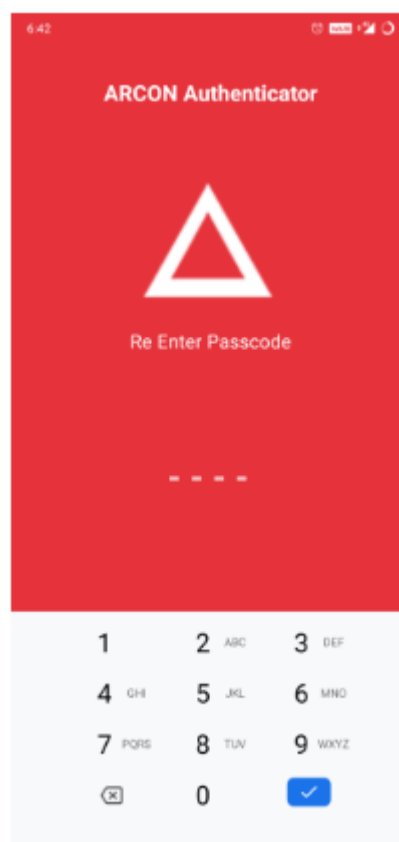
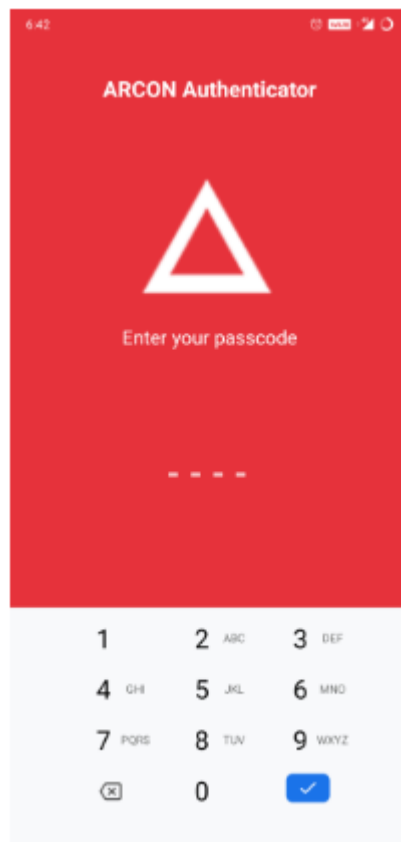
4. ARCON PAM Mobile OTP - Self Registration

4.1 Download and Install ARCON PAM Authenticator

1. You need to download and install ARCON Authenticator App from Google Play Store on your mobile to configure mobile OTP dual factor authentication.

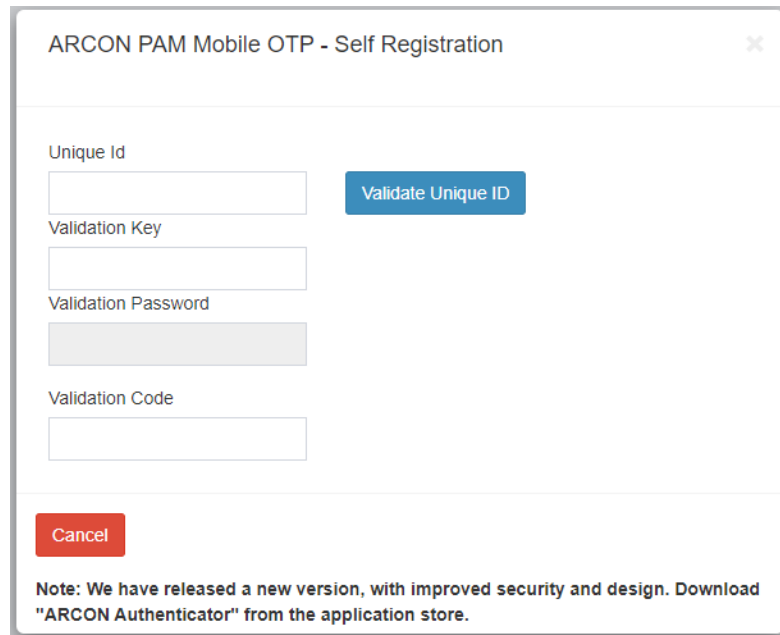


2. Enter a Pass code for first login attempt and re-enter pass code to confirm.



4.2 Self-Registration

1. Launch the PAM URL and Login using your AD credentials. Below screen will be shown:



The image shows a self-registration dialog box titled "ARCON PAM Mobile OTP - Self Registration". It contains four input fields: "Unique Id", "Validation Key", "Validation Password", and "Validation Code". A blue button labeled "Validate Unique ID" is positioned to the right of the "Unique Id" field. A red "Cancel" button is located at the bottom left. A note at the bottom states: "Note: We have released a new version, with improved security and design. Download 'ARCON Authenticator' from the application store."

ARCON PAM Mobile OTP - Self Registration

Unique Id

Validation Key

Validation Password

Validation Code

Validate Unique ID

Cancel

Note: We have released a new version, with improved security and design. Download "ARCON Authenticator" from the application store.

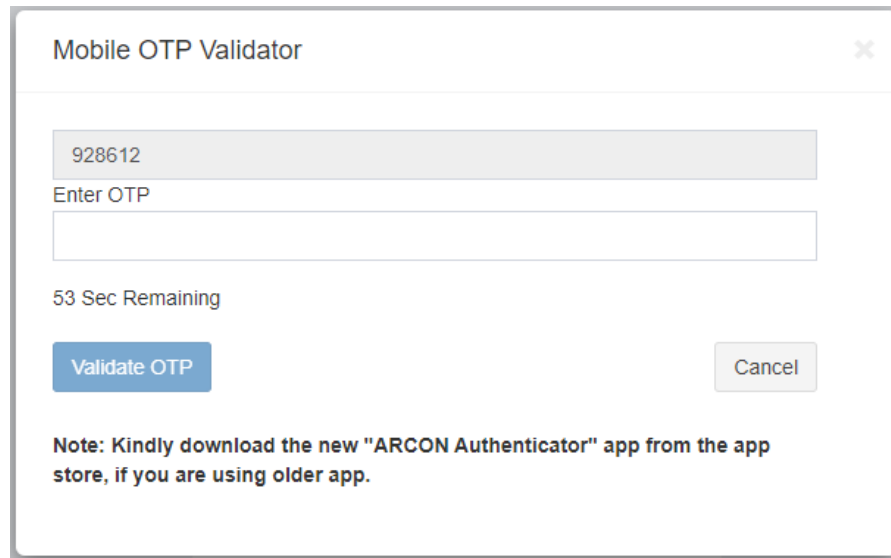
2. Enter the **Instance Name** (Instance Name will help to distinguish between multiple instance of OTP configured)

The screenshot shows the ARCON Authenticator app interface. At the top, the status bar displays the time 7:21, a battery icon, and a signal strength indicator. The app's header is red with a white menu icon on the left and the 'Authenticator' logo on the right. Below the header, the 'Instance Name' field contains 'Instance Name_1'. The 'Unique ID' field displays '2702 2203 4608 482'. The 'Validation Key' field displays '99733779'. The 'Validation Code' field displays '8014656'. The 'Validation Password' field is empty. Below these fields is a checkbox labeled 'Mark as default'. At the bottom, there is a red 'Update' button. A note at the very bottom states: '*Kindly note your validation code after validation.'

3. Enter the unique number generated on ARCON Authenticator App in the **Unique ID** field on the Self Registration screen.
4. Click on **Validate Unique ID** button next to Unique ID field.
5. Enter the **Validation Key** number generated on ARCON Authenticator App in **Validation Key** field on the Self Registration screen.
6. Click on generate **Validation Password** button next to **Validation Key** field. It will generate the Validation password in **Validation Password** field.
7. Enter the generated validation password in **Validated Password** field on ARCON Authenticator App. Post entering password, Click on **Validate Phone**. This will generate validation code on App.
8. Enter the generated code into Validation Code field on Self Registration screen.
9. Click Validate Code button. User will get **"Mobile OTP Registration Successfully Completed"** message. Click on OK.

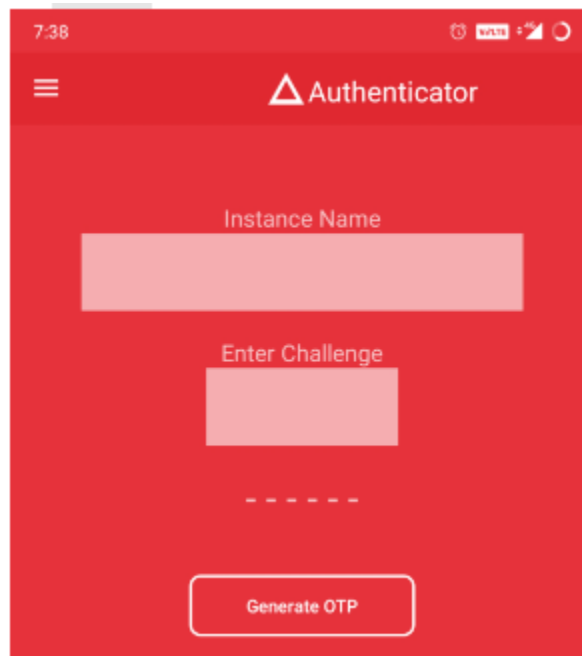
5. Post Mobile OTP Registration

1. Re-Login into PAM using AD credential. Below Mobile OTP Validator Screen will appear.



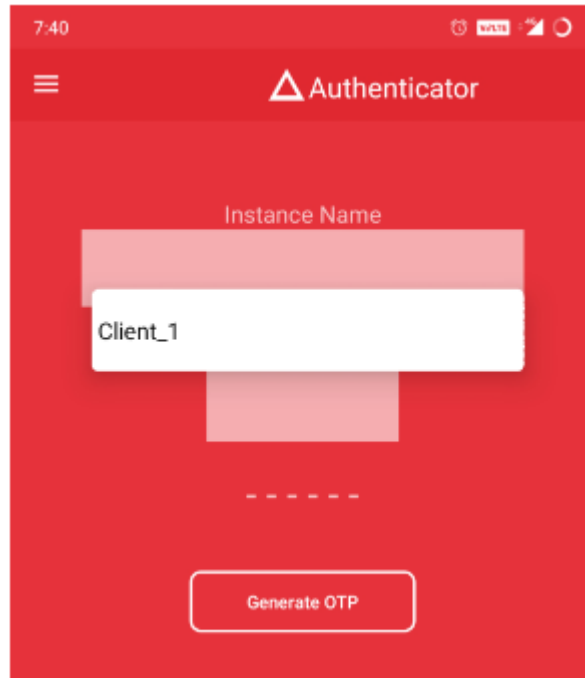
A screenshot of a 'Mobile OTP Validator' dialog box. At the top, it says 'Mobile OTP Validator' with a close button (X) on the right. Below this, there is a text input field containing '928612'. Underneath the input field is the label 'Enter OTP' and another empty text input field. Below the input fields, it says '53 Sec Remaining'. At the bottom left is a blue button labeled 'Validate OTP', and at the bottom right is a grey button labeled 'Cancel'. At the very bottom, there is a note: 'Note: Kindly download the new "ARCON Authenticator" app from the app store, if you are using older app.'

2. Go to App → Left Top Menu Button  → Generate OTP. Below Screen will appear.

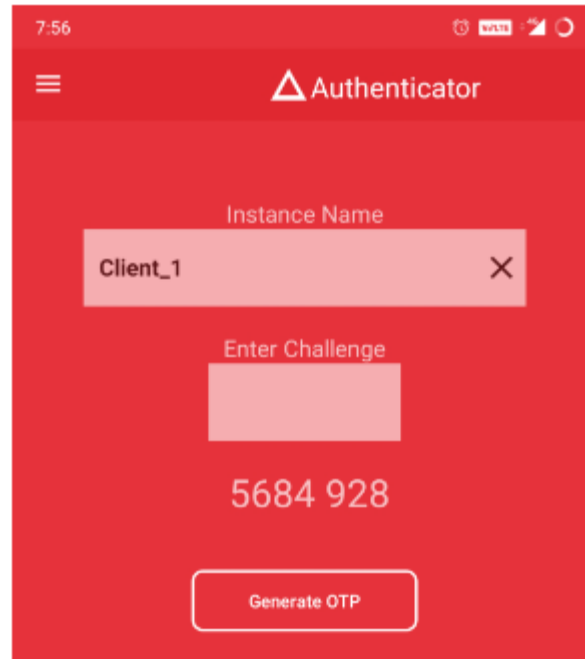


A screenshot of the ARCON Authenticator app interface. The background is red. At the top, the status bar shows the time '7:38' and various icons. Below the status bar, there is a white menu icon (three horizontal lines) on the left and the app name 'Authenticator' in white text on the right. In the center, there is a white text input field labeled 'Instance Name'. Below this, there is another white text input field labeled 'Enter Challenge'. Underneath the 'Enter Challenge' field, there are five white dashes '-----'. At the bottom center, there is a white rounded rectangular button labeled 'Generate OTP'.

3. Tap the Instance Name field on App. It will list down the instance Name as shown below:



4. Select the Instance Name as per the client instance you want to login.
5. Tap Enter Challenge field and enter the 6 digit pin generated on the screen.
6. Post entering challenge PIN, click on generate OTP. OTP will be generated as shown below

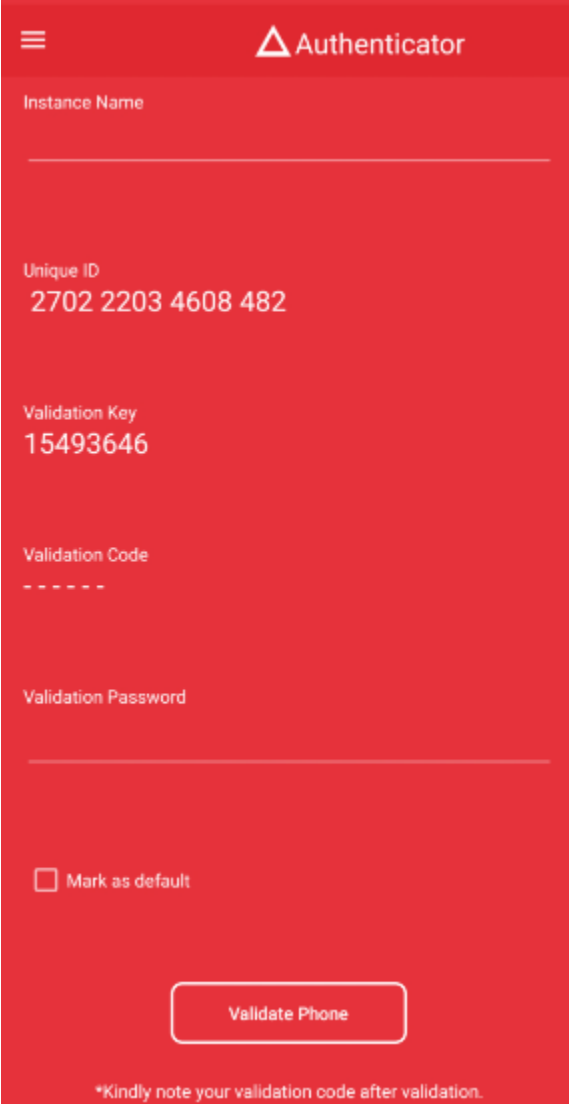


Step 8: Enter the generated OTP generated OTP Validator screen. Click OK

6. Mobile OTP Registration for Multiple Instances

There are scenario where users are working on multiple instance of ARCON PAM having Mobile OTP as multiple factor authentication. In this case, user will have to follow below steps for multiple registration of Mobile OTP.

1. Go to ARCON Authenticator App → Click on Menu button on Top Left → Click on Create Instance.

The screenshot shows the ARCON Authenticator app interface. At the top, there is a red header with a white menu icon on the left and the text "Authenticator" on the right. Below the header, the form is divided into several sections. The first section is labeled "Instance Name" and has a white text input field. The second section is labeled "Unique ID" and displays the number "2702 2203 4608 482" in white. The third section is labeled "Validation Key" and displays the number "15493646" in white. The fourth section is labeled "Validation Code" and has a white text input field with six dashes "-----" as a placeholder. The fifth section is labeled "Validation Password" and has a white text input field. Below these fields, there is a checkbox labeled "Mark as default". At the bottom of the form, there is a white button with the text "Validate Phone". At the very bottom, there is a small white text note: "*Kindly note your validation code after validation."

Step 2: Enter the New Instance Name.

Step 3: Follow the same steps mentioned in section 2.2