CipherLab

Reference Manual

Applock

For Android Mobile Computer

RS30
RS31
RS35
RS36
RS50
RS51
HERA51
RK25
RK26
RK95
9700A

Version 1.10

Copyright © 2023 CIPHERLAB CO., LTD.
All rights reserved

The software contains proprietary information of its owner; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development, this information may change without notice. The information and intellectual property contained herein is confidential between the owner and the client and remains the exclusive property of the owner. If having any problems in the documentation, please report them to us in writing. The owner does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of the owner.

For product consultancy and technical support, please contact the local sales representative. Also, visit our website for more information.

All brand, logo, product and service, and trademark names are the property of their registered owners.

Google, Google Play, Android and other marks are trademarks of Google Inc.

The editorial use of these names is for identification as well as to the benefit of the owners, with no intention of infringement.

CIPHERLAB logo is a registered trademark of CIPHERLAB CO., LTD. All other brands, products and services, and trademark names are the property of their registered owners. The editorial use of these names is for identification as well as to the benefit of the owners, with no intention of infringement.

CIPHERLAB CO., LTD.
Website: http://www.CipherLab.com

RELEASE NOTES

Version	Date	Notes
1.10	Sep. 08, 2023	Add the new supported device models
1.09	April 20, 2021	Update all figures. Section 1.2 “Use AppLock for the 1st Time”: Update the description about the password for Admin Mode. Add the description about “WMDS Agent” to Section 1.2 “Use AppLock for the 1st Time”. Revise “Reset Chrome blacklist policy” to Section 3.3.3 “Site Protection”. Remove “Enable Screen Pinning When Lock Screen Is Not Set as "None" or "Swipe".” from 3.3.3 “Screen Pinning”. Add description about notifications of ADCClient and OEMConfig to Section4.2.3 “Show filtered notifications”. Add new section “Launch Button Assignment” to Chapter 5: “Other Functions (Administrator Only)”.
1.08	Oct. 5, 2020	RS35 Mobile Computer is supported. Section 3.1.1 “Add Application”: Add the description about more option menu on the Available Applications page. Update Section 3.3.1 “Hide Icon on AppLock Desktop”. Add “Reset Chrome blacklist policy” to Section 3.3.3 “Site Protection”. Add new section 3.3.4 “Chrome Shortcut”. Update section 3.4 “Recent Apps Whitelist”. Update Section 4.4 “Security”. Section 4.5 “Assist app”: Add the note about the access to “assist app” for all supported models. Update section 4.7 “USB Connection Allowed”. Update the releated figures.
1.07	August 18, 2019	Add new section 2.2.2 “Admin Menu in Android Safe Mode”. Add new section 3.2.4 “Adjust Auto start delay”. Update the related figures.
1.06	April 30, 2019	Update all figures RS51 Mobile Computer is supported Add “Home screen text color” to section 4.3 “Display” Add “Monitoring App Installation” to section 4.4 “Security”

Version	Date	Notes
1.05	Dec. 28, 2018	Update section 3.1.1 “Add application” & 3.1.2 “Add Shortcut” Add new section 3.1.3 “Add Package Naming Rule” Update section 3.1.5 “Clear All Applications and Shortcuts” Add “Enable Log” to section 4.4 “Security” Update the related figures.
1.04	June 15, 2018	Update Section 3.1.2 “Add Shortcut” Add new section 3.3.4 “Rearrange the Sorting Order of the Apps/Shortcuts on Desktop” Update the related figures
1.03	May 10, 2018	RK25 Mobile Computer is supported Change Section 2.6 to Chapter 3 “Applications Management (Administrator only)” Add note to Section 3.1.2 Add Section 3.3.1 “Hide icon on AppLock Desktop” Add Section 3.3.3 “Site Protection” Change Section 2.8 to Chapter 4 “Option (Administrator only)” Revise Section 4.2.2 “Enable Notification Bar” Add Section 4.2.3 “Show filtered notifications” Change Section 2.9 to Chapter 5 “Other Functions (Administrator only)” Revise Section 5.5 “Exit” Update the related figures.
1.02	Dec. 7, 2017	Revise “Set AppLock as Home App” of Section 1.1 Add “Heads-up Notifications” to Section 2.8.1 Add “Remove Lockscreen Icons” to Section 2.8.5 Update the related figures.
1.01	Oct. 16, 2017	Support Android 6.0 & Android 7.0 Update all figures Revise “Delete Applications or Shortcuts” of Section 2.6.1 Revise “Notification bar” of Section 2.8 Add “Assist app” & “USB Connection Allowed” to Section 2.8 Add Section 2.6.3 “Screen Pinning”
1.00	Apr 27, 2017	Initial release

CONTENTS

RELEASE NOTES 3
INTRODUCTION 7
Features 8
CHAPTER 1. SETUP 9
1.1 Launch AppLock 10
1.1.1 Launch AppLock from Normal Operation Mode 10
1.1.2 Set AppLock as Home App 11
1.2 Use AppLock for the 1st Time 12
CHAPTER 2. USE APPLOCK 14
2.1 Access Levels 15
2.2 Menu 16
2.2.1 Open Menu 16
2.2.2 Admin Menu in Android Safe Mode 17
2.3 Toolbar (Administrator Only) 19
2.4 Working Views 21
2.4.1 Allowed Apps View 21
2.4.2 Auto Start APPS View (Administrator Only) 21
2.5 Admin Mode (Administrator Only) 22
2.5.1 Admin Mode 22
2.5.2 User Mode 23
2.6 Manage System Settings (Administrator Only) 24
2.6.1 Export 25
2.6.2 Import 26
CHAPTER 3. APPLICATIONS MANAGEMENT (ADMINISTRATOR ONLY) 27
3.1 Allowed Apps View 28
3.1.1 Add Application 28
3.1.2 Add Shortcut 30
3.1.3 Add Package Naming Rule 33
3.1.4 Delete Applications or Shortcuts 41
3.1.5 Clear All Applications and Shortcuts 42
3.1.6 Rename Applications or Shortcuts 47
3.2 Auto Start APPs View 48
3.2.1 Set Application as Auto Start APPS 48
3.2.2 Remove Application 49
3.2.3 Clear All Applications 49
3.2.4 Adjust Auto start delay 50

3.3 More Application Settings for Allowed Apps View....52
3.3.1 Hide Icon on AppLock Desktop....52
3.3.2 Screen Pinning....55
3.3.3 Site Protection....61
3.3.4 Chrome Shortcut....71
3.3.5 Rearrange the Sorting Order of the Apps/shortcuts on Desktop....80
3.4 Recent Apps Whitelist....81
CHAPTER 4. OPTION (ADMINISTRATOR ONLY)....83
4.1 Options Menu (Administrator Only)....84
4.2 Notification Bar....85
4.2.1 Show Notification Bar....85
4.2.2 Enable Notification Bar....86
4.2.3 Show filtered notifications....87
4.2.4 Heads-up notifications....89
4.3 Display....90
4.3.1 Wallpaper....90
4.3.2 Logo....90
4.3.3 Home screen text color....91
4.4 Security....92
4.5 Assist app....95
4.6 Remove Lockscreen Icons....98
4.7 USB Connection Allowed....99
CHAPTER 5. OTHER FUNCTIONS (ADMINISTRATOR ONLY)....100
5.1 Launch Button Assignment....101
5.2 Launch System Settings....101
5.3 Reset to Default....102
5.4 Clear Recent Apps....102
5.5 About....102
5.6 Exit....103

INTRODUCTION

Developed for Android mobile computers, **AppLock** controls the interface provided to users. It dominates over the O.S. and limits the system resources made available to users. Properly tuned, AppLock gives way to ordinary working applications while locking out those that are not so productive.

If you have a collection of mobile computers, you can apply a uniform user environment to the entire group without the need of great time and effort. This can be done easily by reduplicating a copy of master settings to your entire set of mobile computers.

This manual covers usage of AppLock. We recommend that you read this document thoroughly before starting, and keep a copy of this manual at hand for quick reference.

FEATURES

- Supports CipherLab Android mobile computers:
  - Android 4.4 KitKat (RS30)
  - Android 6.0 Marshmallow (9700A, RS31 & RS50)
  - Android 7.0 Nougat (RS31 & RK25)
  - Android 8.0 Oreo (RS51 & HERA51)
  - Android 9.0 Pie (RK25 & RK95)
  - Android 10 (RS35)
  - Android 11(RK25, RS35, RS51 & HERA51)
  - Android 12 (RK26, RK95 & RS36)

- Full control over system services
- Limits the accesses to crucial system settings
- Locks out unproductive applications
- Auto-launched productive applications upon system startup
- Superuser mode for administration of operating system
- Supports importing and exporting settings to configuration files

Chapter 1

SETUP

This chapter guides to the launch of AppLock.

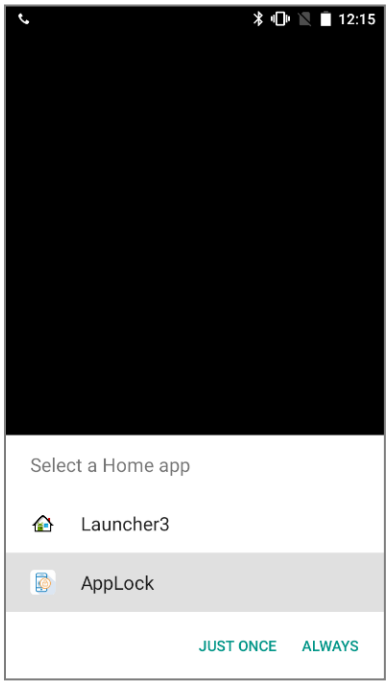
This chapter also covers the 1st launch of the application.

IN THIS CHAPTER

1.1 Launch AppLock..... 10
1.2 Use AppLock for the 1st Time..... 12

1.1 LAUNCH APPLOCK

AppLock is a built-in app and will be automatically executed when you turn on the device. After the flash screen, you may be prompted to select a Home app. By selecting APPLock mode, you will enter launch AppLock program.



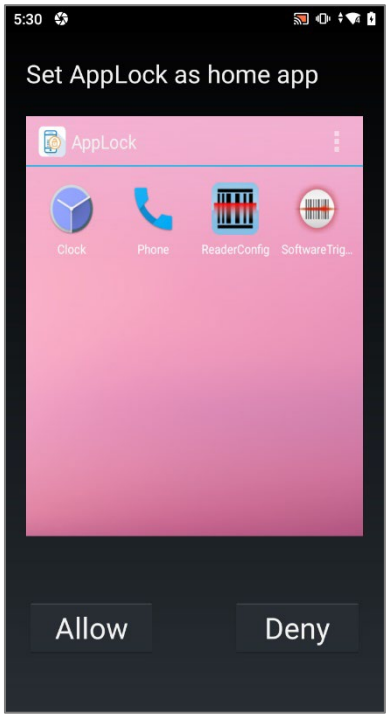
1.1.1 LAUNCH APPLOCK FROM NORMAL OPERATION MODE

To launch AppLock from normal operation mode:

1) Go to App Drawer (All Applications), and then tap on AppLock icon .

2) AppLock opens showing "**Set AppLock as home app**" screen. Tap on "**Allow"** to continue; tap "**Deny**" to leave this page.

   Please refer to Set AppLock as Home App for details.

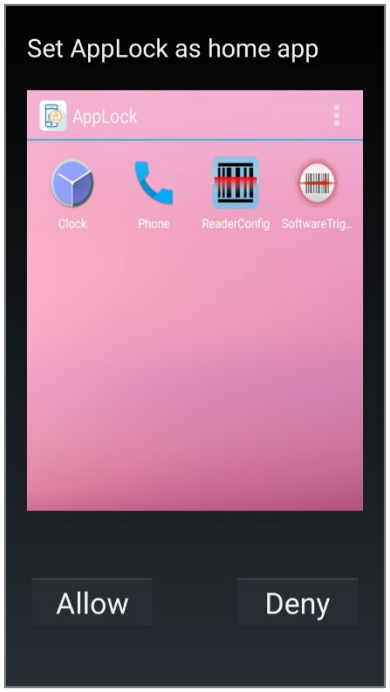


1.1.2 SET APPLOCK AS HOME APP

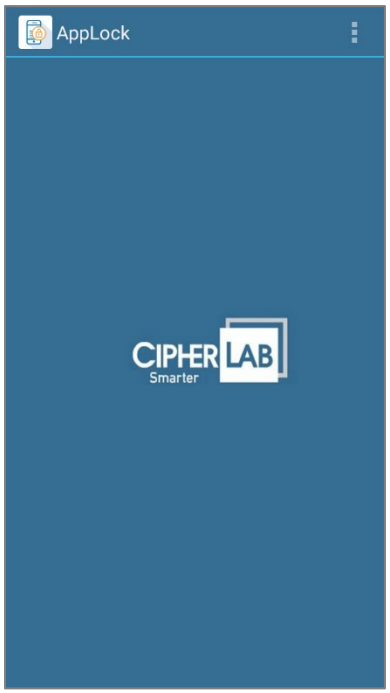
You may decide whether to set AppLock as the home application. If AppLock is set as the home application, when the **Home** button is pressed, AppLock's **Allowed Apps** view will show on the screen.

1) The first time AppLock launches, the notification screen "**Set AppLock as home app**" shows.

   Tap **Allow** to proceed, or tap "**Deny**" to return to the previous page.



2) AppLock opens showing the user level main screen.



1.2 USE APPLOCK FOR THE 1ST TIME

AppLock adopts user levels that set limits to AppLock's advanced functions. See Access Levels for more details.

When launched for the 1st time, AppLock doesn't require password for administrator mode (the superior access level). The full functionality is open to everyone who operates it as long as you log in to AppLock.

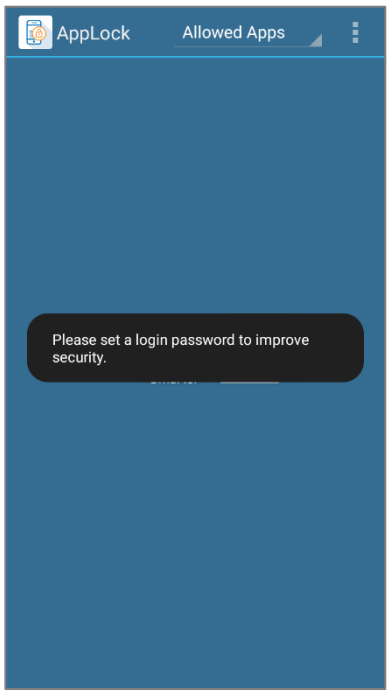
Log in to AppLock to set up an administrative control:

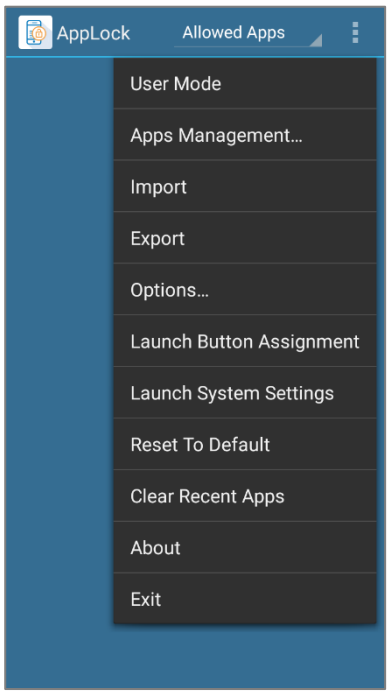
1) Launch the application as described in Launch AppLock.

2) Tap the menu button ⋮ in the top right corner to open the drop-down menu.

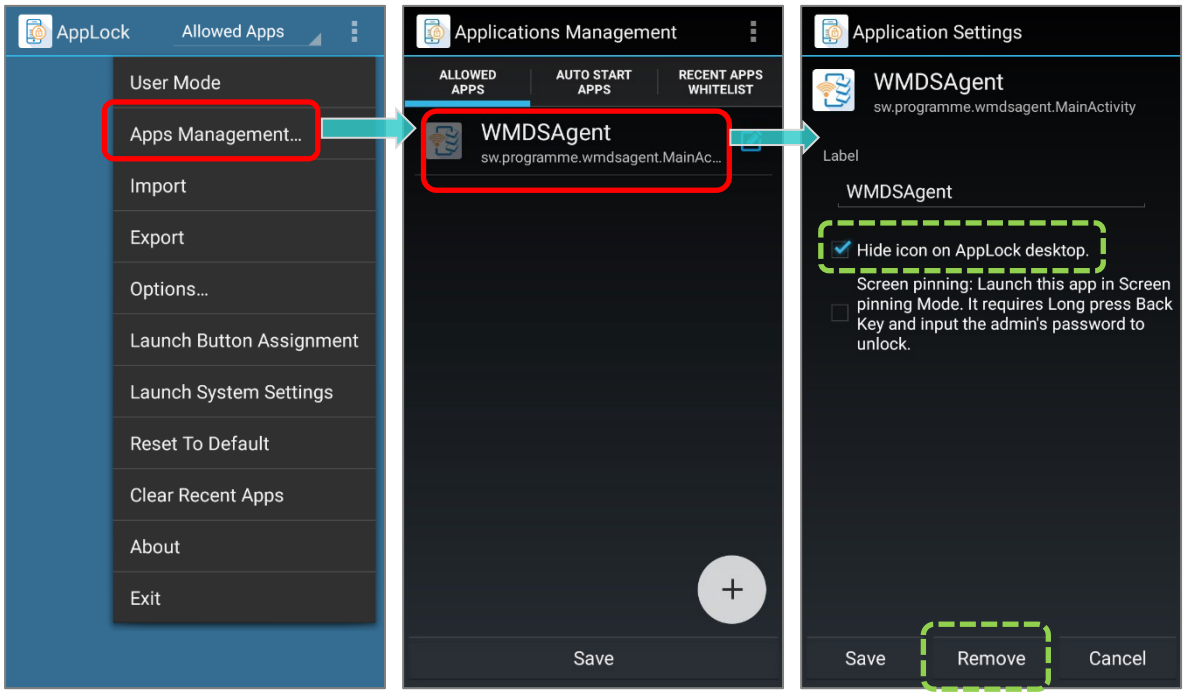
3) Tap on "**Admin Mode**".
   For the first time to login "**Admin Mode**", no password is required because it is not set yet.
   Please do remember to set a new password for administrator in Security.

4) You will be logged in as an administrator. Tap the menu button ⋮ in the top right corner, and the administrator level toolbar becomes available. See Security for details on setting up login password.



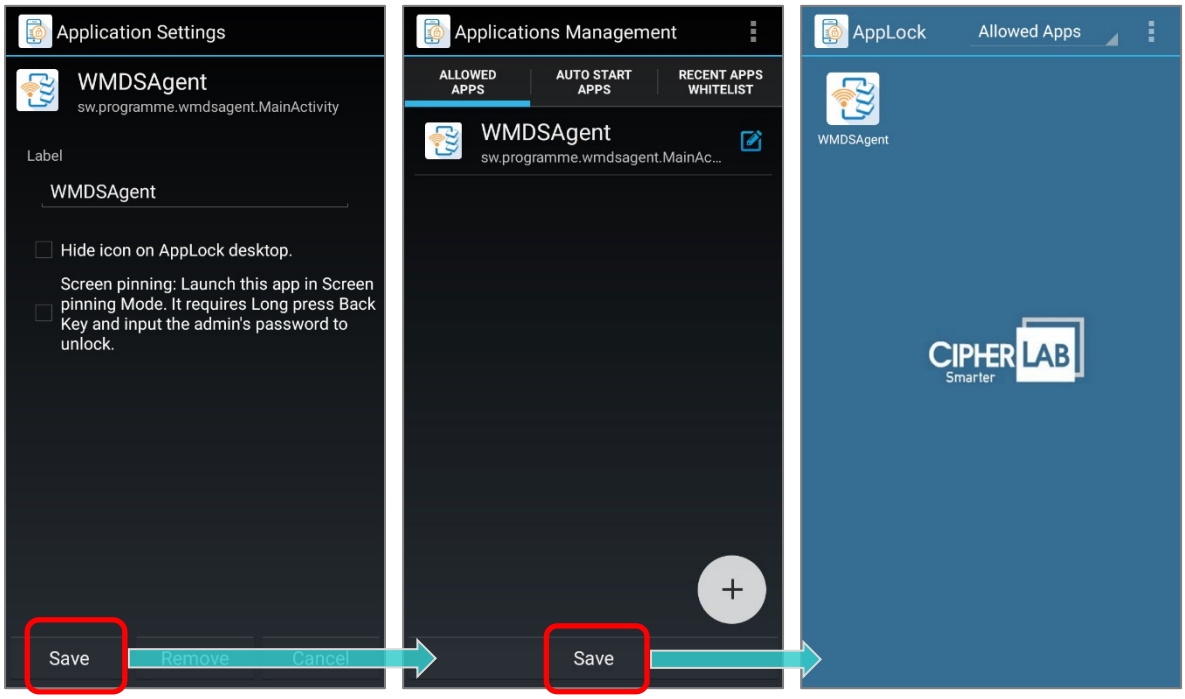


Enter "**Application Management**" of "**Admin Mode**" after AppLock is launched for the 1st time or after AppLock is "**Reset To Default**", you will find the hidden default application "**WMDS Agent**" (Wireless Mobile Deployment System for Android is a windows-based server program that can deploy the configuration projects to Android devices through wireless network).



To display the application "**WMDS Agent**" on AppLock main screen, please uncheck "**Hide icon on AppLock desktop**"; to remove this app, please tap on "**Remove**" button.

Make sure to save before leaving every current page.



Chapter 2

USE APPLOCK

This chapter will walk you through the application's menu, toolbar and main working views. A few sections are also included herein to describe the access levels applied. Also, cloning application settings to a group of mobile computers is also mentioned.

IN THIS CHAPTER

2.1 Access Levels 15
2.2 Menu 16
2.3 Toolbar (Administrator Only) 19
2.4 Working Views 21
2.5 Admin Mode (Administrator Only) 22
2.6 Manage System Settings (Administrator Only) 24

2.1 ACCESS LEVELS

AppLock's offers two access levels for usage:

User

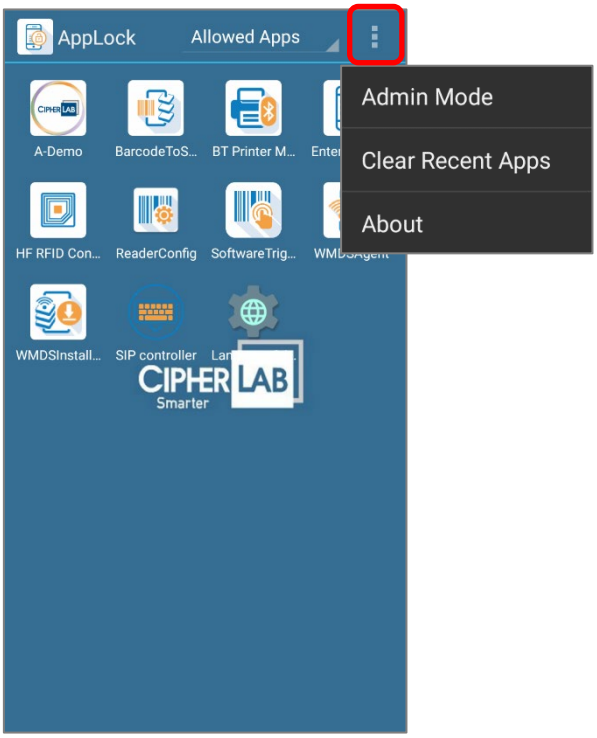
An ordinary user that uses the operating system for their day-to-day tasks. Users are generally warded off from some system settings and relatively unproductive applications.

Administrator

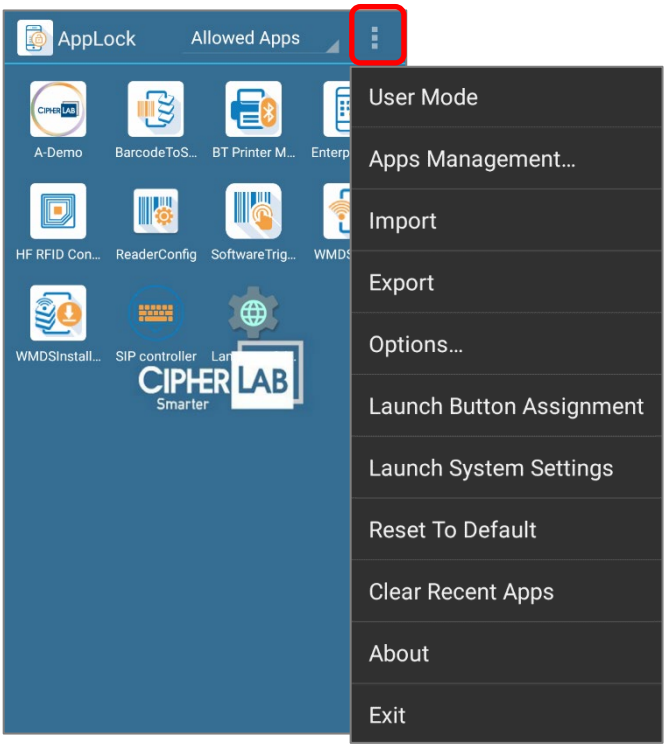
A super user mode with administrative privileges over the operating system. An administrator (most of all) doesn't use the operating system for daily tasks but manages it and prepares it for other users. The administrator is able to tailor which applications and which system settings are available to users.

These two access levels are implemented through menu completeness, which relies on switching between **User Mode** and **Admin Mode**, as detailed in the following section.

User



Administrator



2.2 MENU

Same as most software products, AppLock features a command menu to receive instructions and thus take actions.

2.2.1 OPEN MENU

To open the AppLock menu:

1) Launch the application as described in Launch AppLock.
2) Tap the menu button ⋮. The settings menu opens reflecting the current access level.

User level:

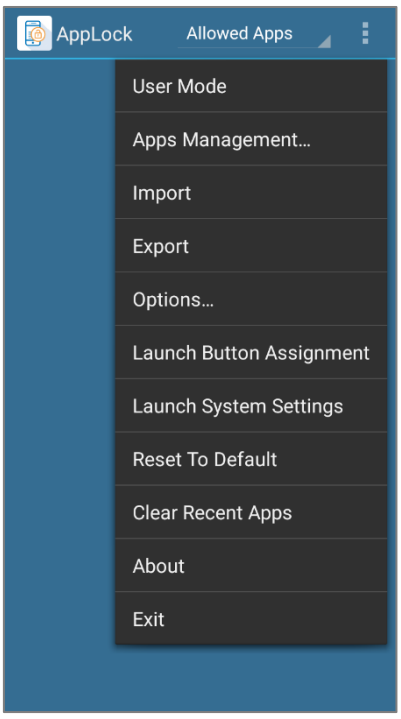
Before logging in to AppLock, AppLock provides users with a pared-down menu. Users can only access the applications on the **Allowed Apps** view, erase the record of recently used applications, or view version information.

Administrator level:

After logging in to AppLock, AppLock provides the administrator with a completely functional menu plus a toolbar. The administrator thus has full access and full control of AppLock's services.

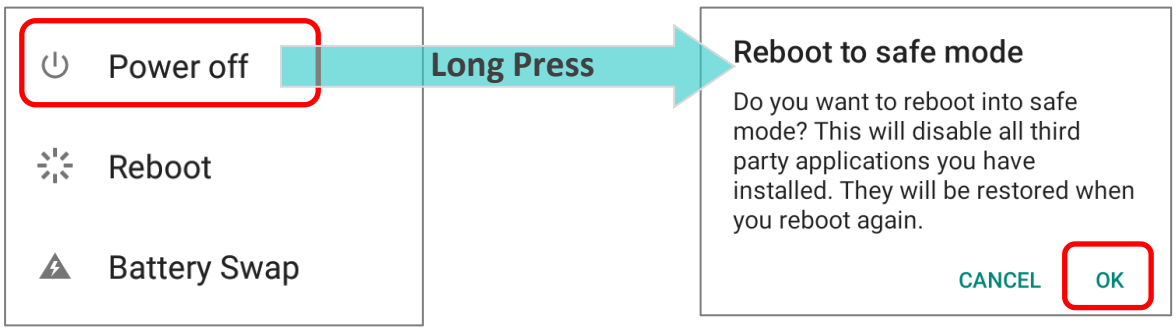
User Level Menu

Administrator Level Menu



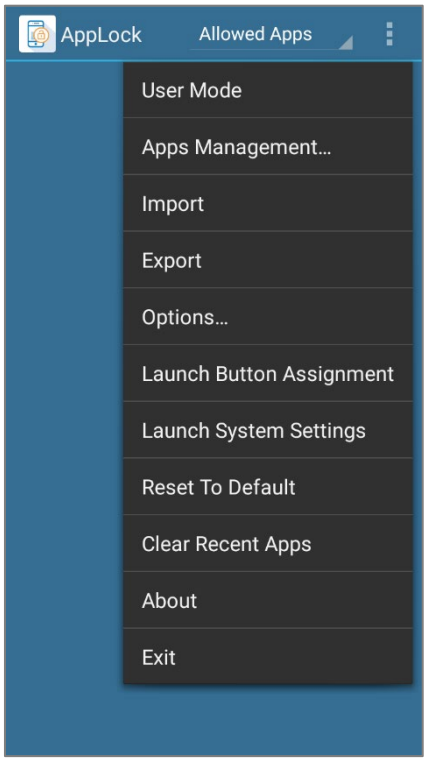
2.2.2 ADMIN MENU IN ANDROID SAFE MODE

By long pressing "**Power off**" on the power menu, a prompt appears for confirming whether to enter "**safe mode**" after rebooting the device. Tap on "**OK**" and the device will reboot automatically.



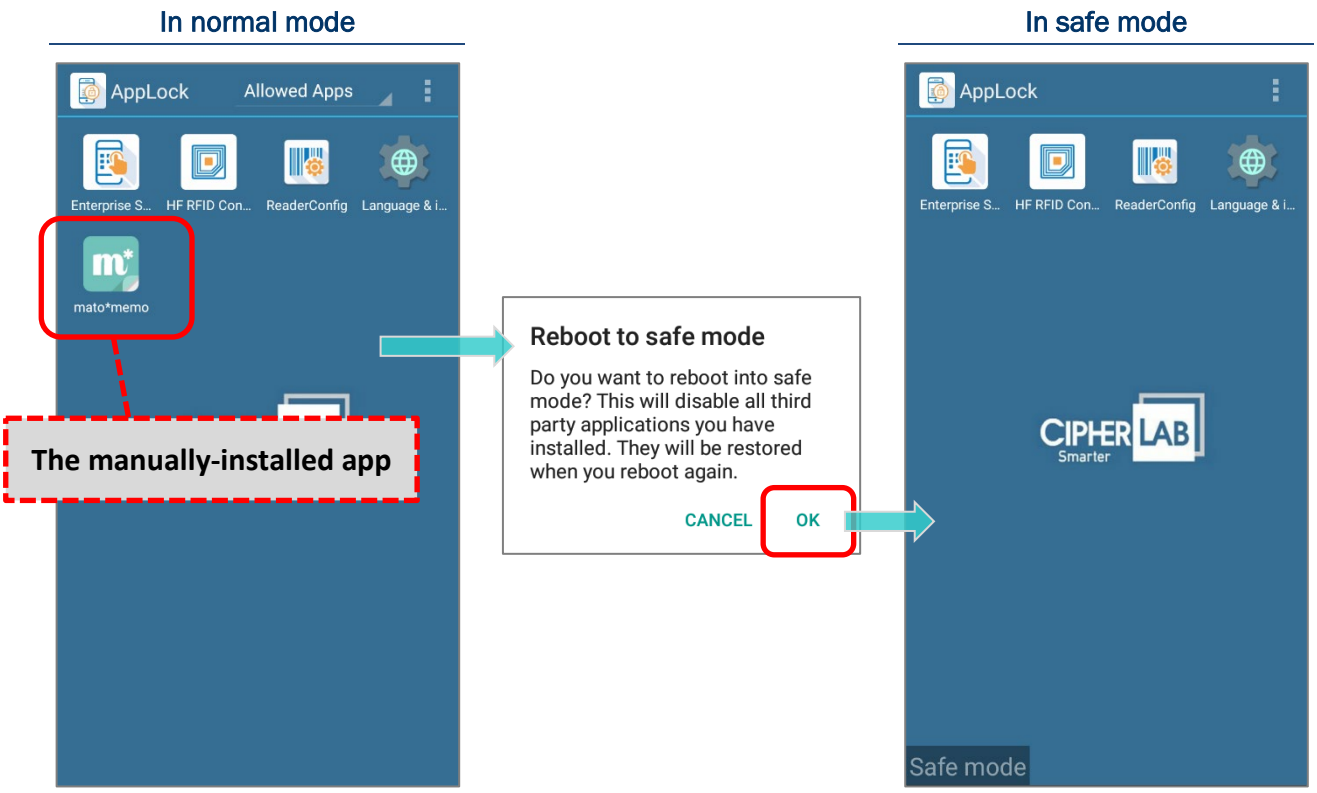
AppLock is not configurable in safe mode. Most functions on the admin menu is hidden.

Admin Menu in Normal Mode



Admin Menu in Android Safe Mode

In safe mode, those apps which is manually installed by the user(s) will be hidden as well. Once you reboot the device to return to normal mode, those manually-installed apps will be shown on AppLock main screen.

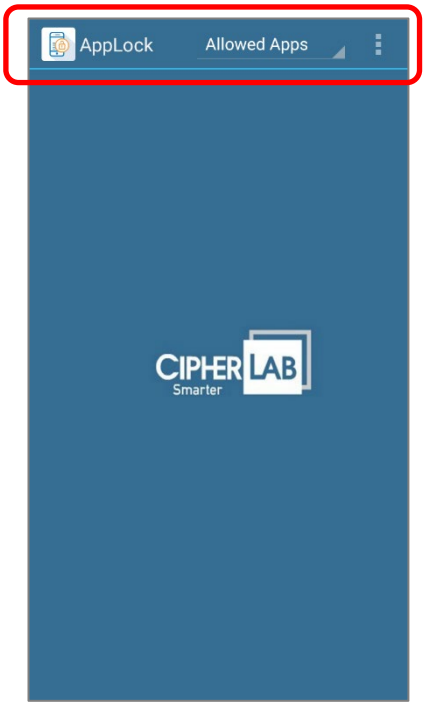


The manually-installed app is shown on AppLock main screen in normal mode.

The manually-installed app is hidden on AppLock main screen in safe mode.

2.3 TOOLBAR (ADMINISTRATOR ONLY)

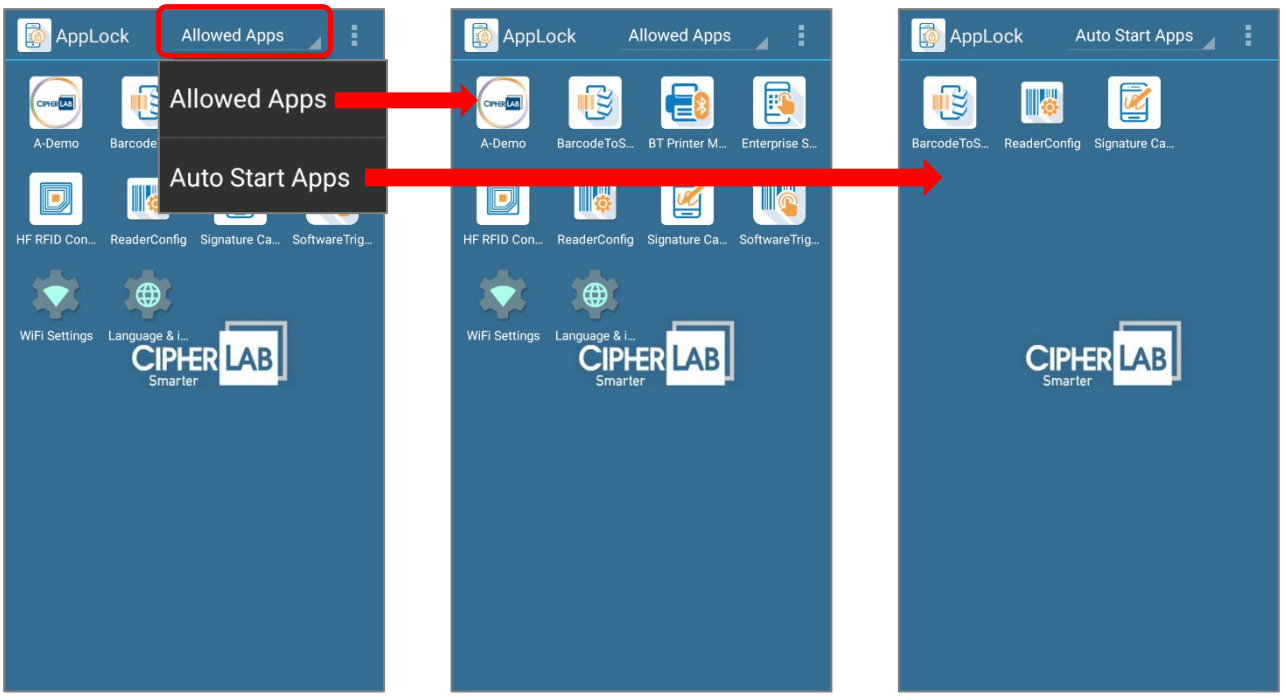
If you are logged in as an administrator, AppLock also features a toolbar at the top to switch working views and access full functions in the settings menu.



WORKING VIEW MENU

The working view menu is for tapping to switch between **Allowed Apps** and **Auto Start Apps**.

Select the Working View | Allowed Apps View | Auto Start Apps View



MENU BUTTON

Tap on the menu button to open the **Access Levels Menu** so instructions can be given to AppLock to invoke actions.

AppLock's offers two access levels for usage:

User:

An ordinary user that uses the operating system for their day-to-day tasks. Users are generally warded off from some system settings and relatively unproductive applications.

Administrator:

A super user mode with administrative privileges over the operating system. An administrator (most of all) doesn't use the operating system for daily tasks but manages it and prepares it for other users. The administrator is able to tailor which applications and which system settings are available to users.

These two access levels are implemented through menu completeness, which relies on switching between **User Mode** and **Admin Mode**, as detailed in the following section.

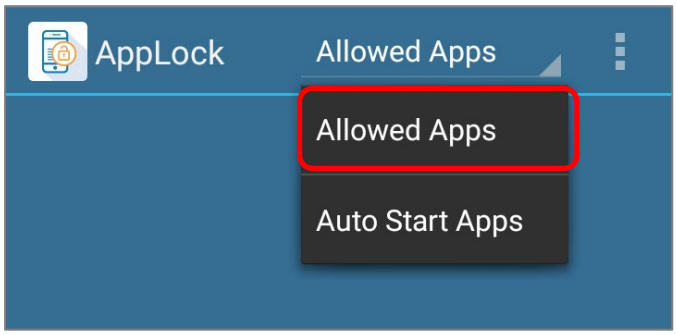
2.4 WORKING VIEWS

AppLock relies on **Allowed Apps** view and **Auto Start Apps** view to deliver its key performance. **Allowed Apps** view lists applications available for usage. This page is accessible for both users and the administrator, but only the administrator is able to edit its settings. **Auto Start Apps** view is only viewable and editable by the administrator.

2.4.1 ALLOWED APPS VIEW

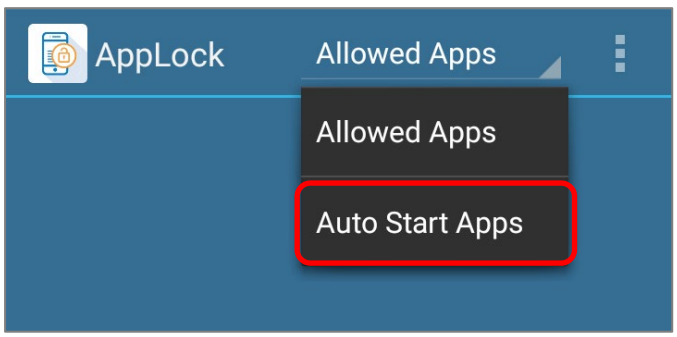
Allowed Apps view delivers available applications to users. Administrators may add or remove applications and shortcuts to this working view, or restore it to default state.

Allowed Apps view is the default screen for users. If you are an administrator, you may tap the working view button on the toolbar to switch between **Allowed Apps** view and **Auto Start Apps** view.



2.4.2 AUTO START APPS VIEW (ADMINISTRATOR ONLY)

Auto Start Apps view is available to the administrator only. It delivers the applications and system settings set to automatically open the next time AppLock is launched.



After applications or system settings are added to this page, the next time AppLock is launched on the mobile computer, the desired applications and/or settings will open. When the specified application(s) or settings(s) are closed, the mobile computer will then proceed to show AppLock on its screen.

2.5 ADMIN MODE (ADMINISTRATOR ONLY)

Log in to AppLock for administration over the operating system to manage and prepare system services for the user. An administrator is able to determine which applications and system settings are accessible to the user.

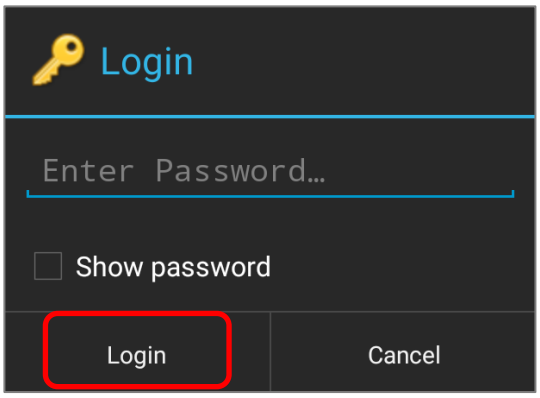
2.5.1 ADMIN MODE

To login to Admin Mode:

1) Tap menu icon ⋮ on the toolbar.

2) Tap on "**Admin Mode"**.

3) Enter the login password and tap on "Login" to confirm.



Upon logging in, the menu and toolbar become fully available for use.

To set up a password, see Security for details.

Or just tap **Login** to enter the **Admin Mode** without entering password (the default password is none).

2.5.2 USER MODE

To logout from Admin Mode and enter User Mode:

1) Tap menu icon on the toolbar.

2) Tap on "**User Mode"**.

   The access level will return to user level, and the menu and toolbar will deliver only restricted functions.

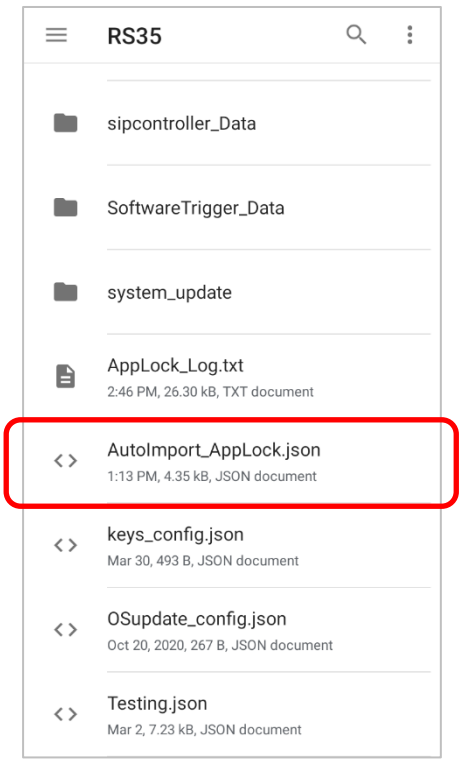
Note:

When you logout from Admin mode and enter User Mode, based on the current Recent Apps Whitelist, AppLock will automatically Clear Recent Apps.

For more information, see Recent Apps Whitelist and Clear Recent Apps.

2.6 MANAGE SYSTEM SETTINGS (ADMINISTRATOR ONLY)

An AppLock application configuration file containing **Apps Management** and **Options settings**, named **AutoImport_AppLock.json**, is kept in the device's internal storage. It is also accessible from a PC through a mobile deployment system, allowing the administrator to deploy a customized config file to multiple devices within just a few clicks. At the first start-up of AppLock after the device boots up, this application will locate this file and load the settings; if this file is missing, a new AutoImport_AppLock.json file will be automatically generated using the current AppLock settings. Any change made to the application settings under Administrator mode will be immediately saved to this file. On the other hand, to maintain the consistency and make sure user behavior is not affecting the configuration, under User mode, AppLock will automatically check if this file has been modified as the user returned to Allowed Apps view from other applications or setting pages. If so, AppLock will load the original version of AutoImport_AppLock.json to overwrite the current one.



Note:

Do not rename this file.

2.6.1 EXPORT

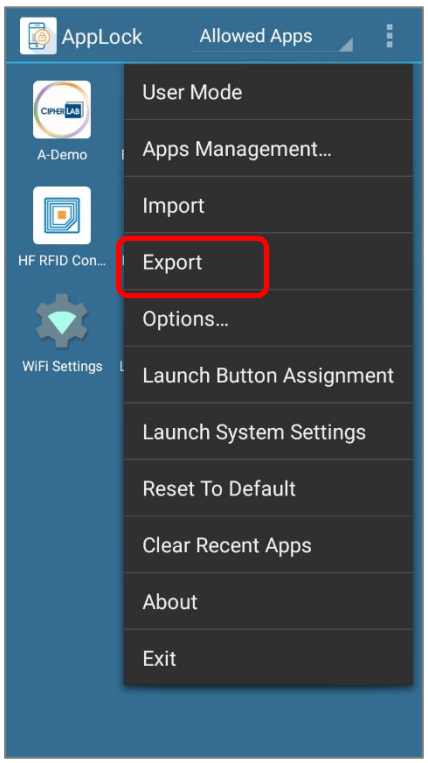
By exporting and importing these configuration files, you can easily share a copy of AppLock's settings among a group of mobile computers.

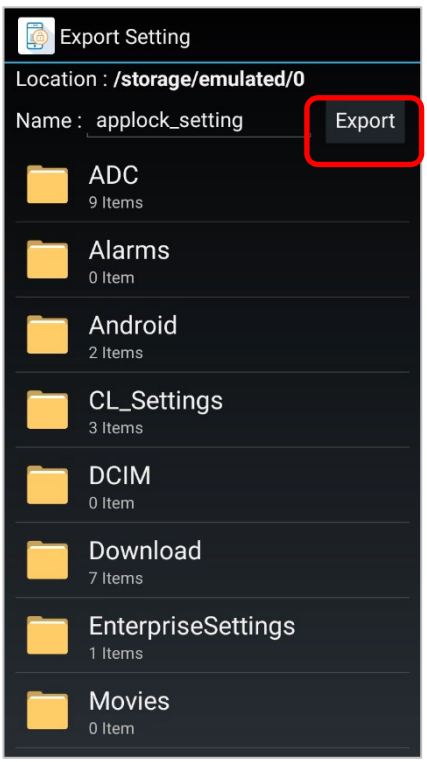
To export the settings file:

1) Tap the menu button .

2) Tap on "**Export**".

3) Enter the name of the settings file, and tap to select a path to store the file.





4) Tap on "**Export**". The settings file will be exported to the specified path.

Note:

1. The default exported file name is ***applock_setting.json***.
2. To avoid confusion, do not name an exported setting file as that of the system config files - ***AutoImport_AppLock.json***.

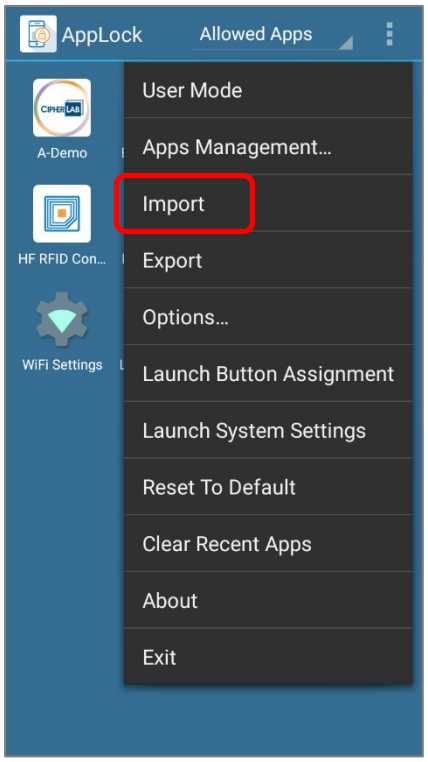
2.6.2 IMPORT

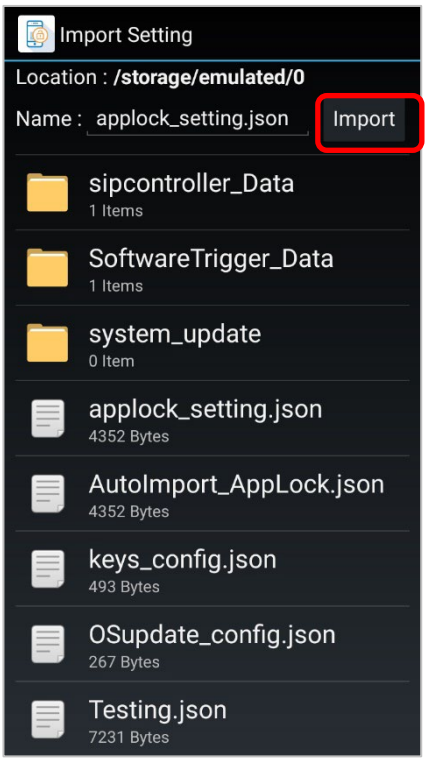
To import the settings file:

1) Tap the menu button ⋮ .

2) Tap on “**Import**”.

3) Tap to select the path where the settings file (.json) is stored.





4) Tap on “**Import**”.

The selected file will be imported into the AppLock and the new settings will be immediately applied.

Chapter 3

APPLICATIONS MANAGEMENT (ADMINISTRATOR ONLY)

This chapter introduces the functions in "**Applications Management**" page for administraror. Administrators are allowed to edit the applications shown on **Allowed Apps** view, **Auto Start Apps** view and **Recent Apps Whitelist** to limit the accesses for users.

IN THIS CHAPTER

3.1 Allowed Apps View 28
3.2 Auto Start APPs View 48
3.3 More Application Settings for Allowed Apps View 52
3.4 Recent Apps Whitelist 81

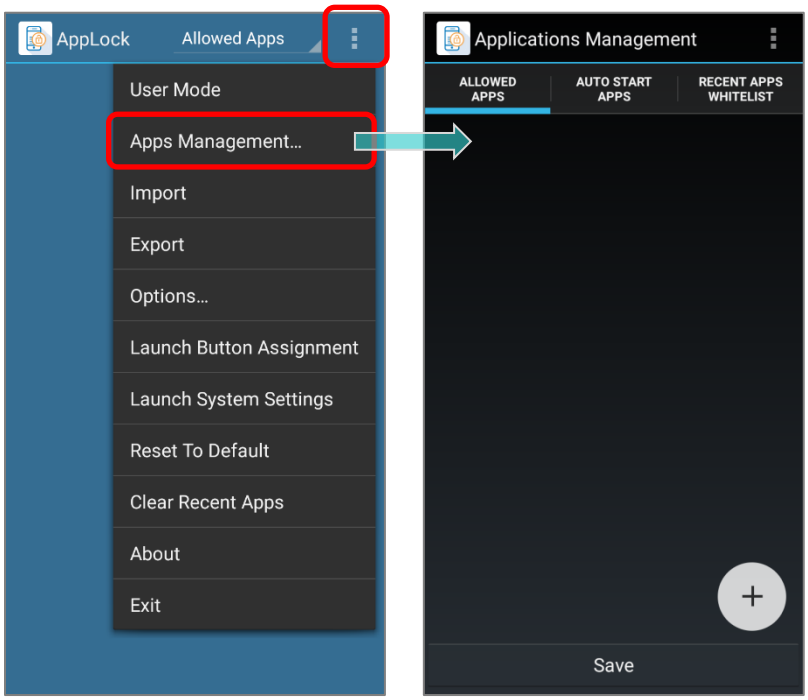
3.1 ALLOWED APPS VIEW

3.1.1 ADD APPLICATION

To add an application to **Allowed Apps** view:

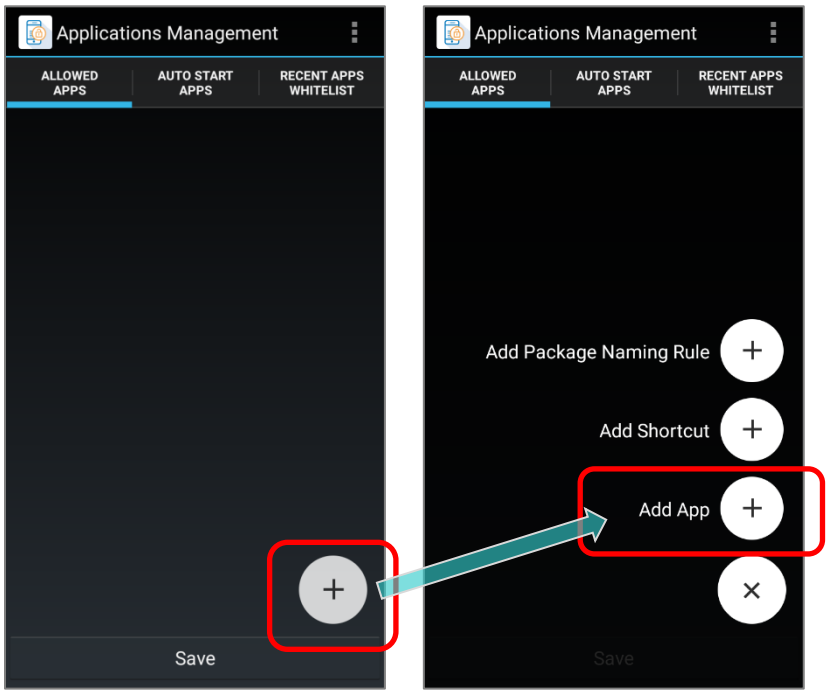
1) Tap menu button ⋮ on the toolbar.

2) Tap "**Apps Management…**" to enter **Applications Management** screen.



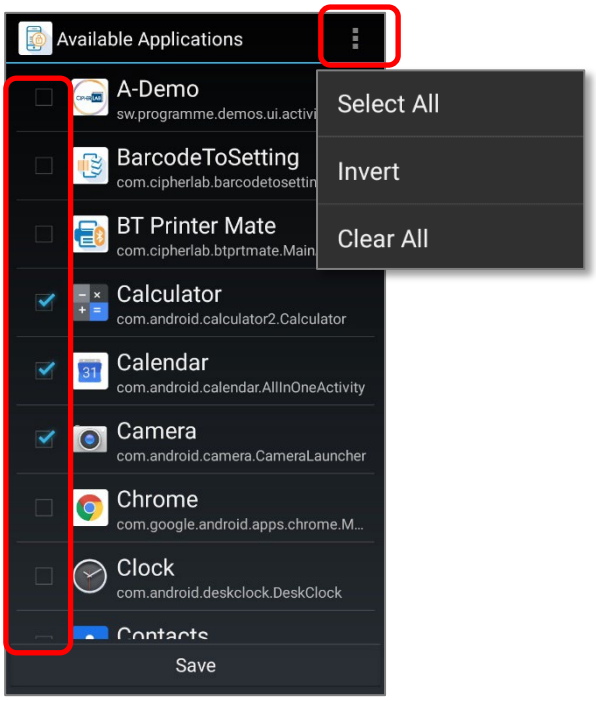
3) Tap on the "**Add**" button ⊕ to expand more option, and then tap on "**Add App**".

The screen shows a list of applications available on the device.



4) Select the applications you would like to make available on the **Allowed Apps** view.

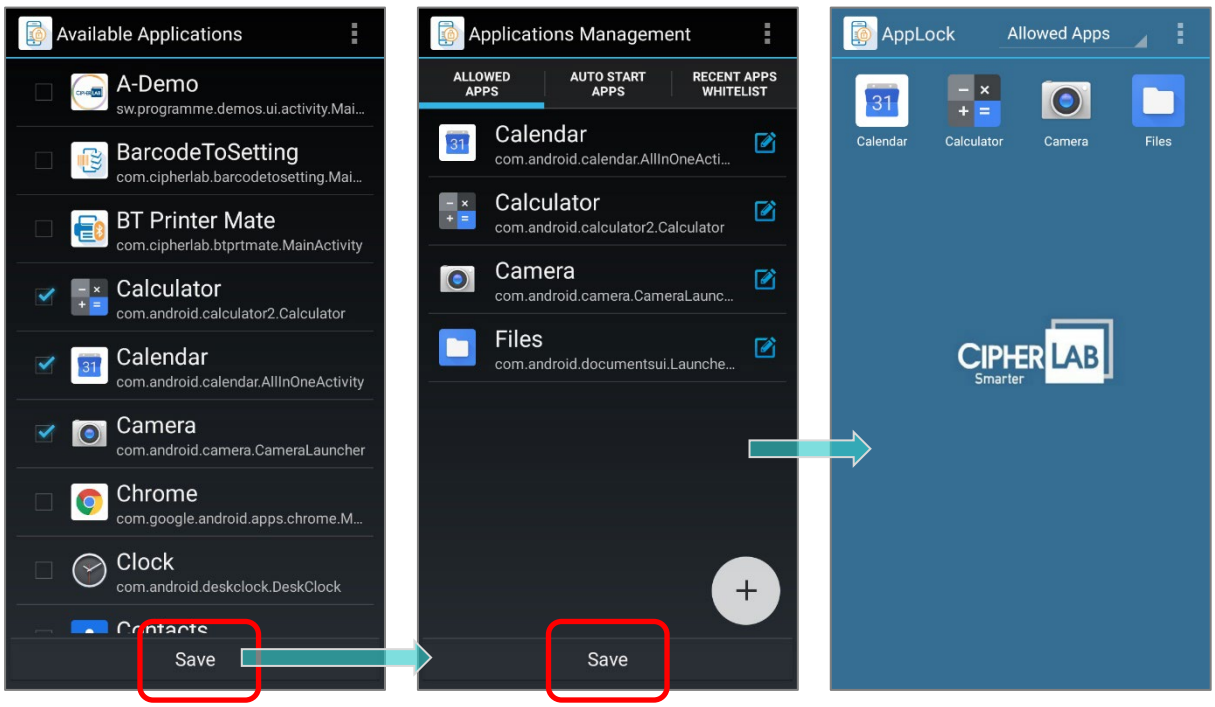
   You can also tap "**More**" button ⋮ on the action bar to open a menu for more options:



Item	Description
Select All	Tick all the applications listed on the **Available Application** list.
Invert	Uncheck the selected applications and check all the unselected ones.
Clear All	Uncheck all the selected applications.

5) Tap on "**Save**". The **Allowed Apps** screen shows the applications (and shortcuts) you assigned to the **Allowed Apps** view.

6) Tap on "**Save**" to save the settings made to the working view.

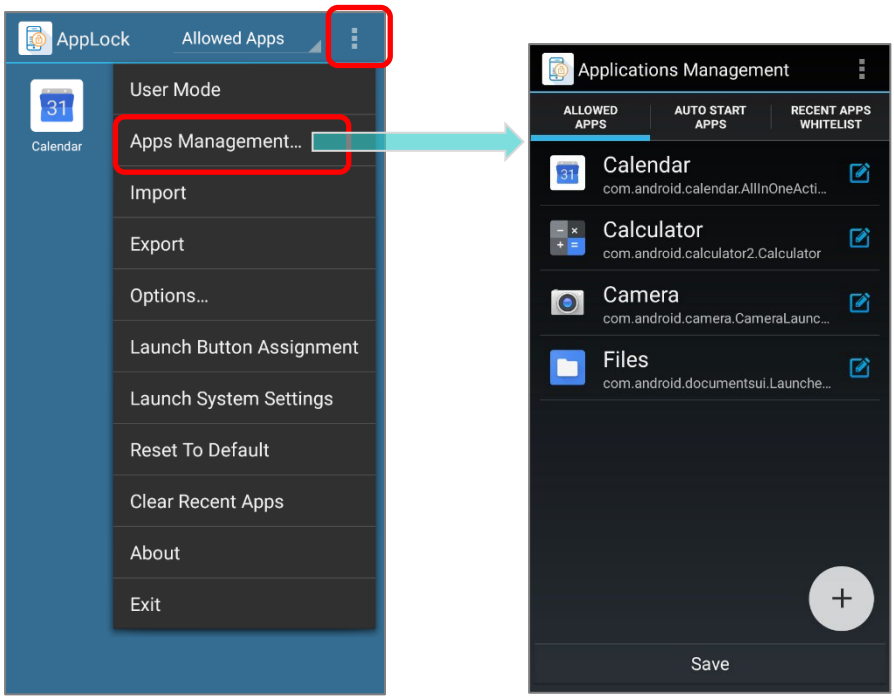


3.1.2 ADD SHORTCUT

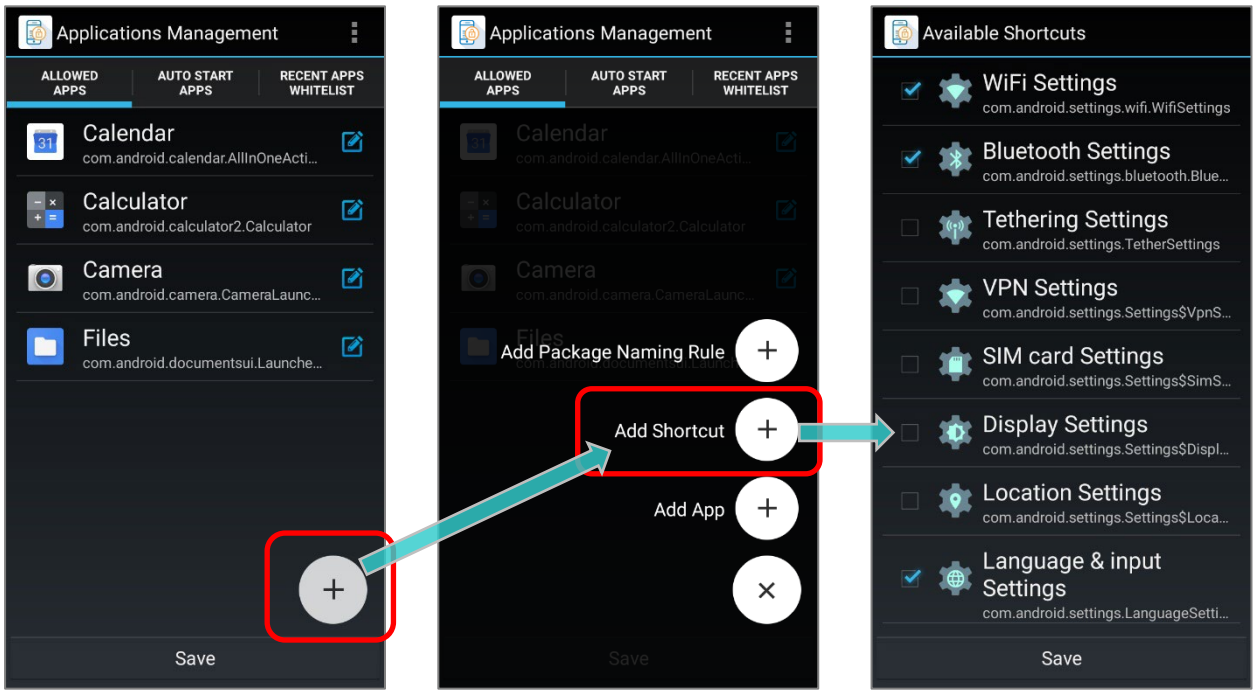
To add a shortcut to **Allowed Apps** view:

1) Tap menu button ⋮ on the toolbar.

2) Tap "**Apps Management…**" to enter Applications Management screen.

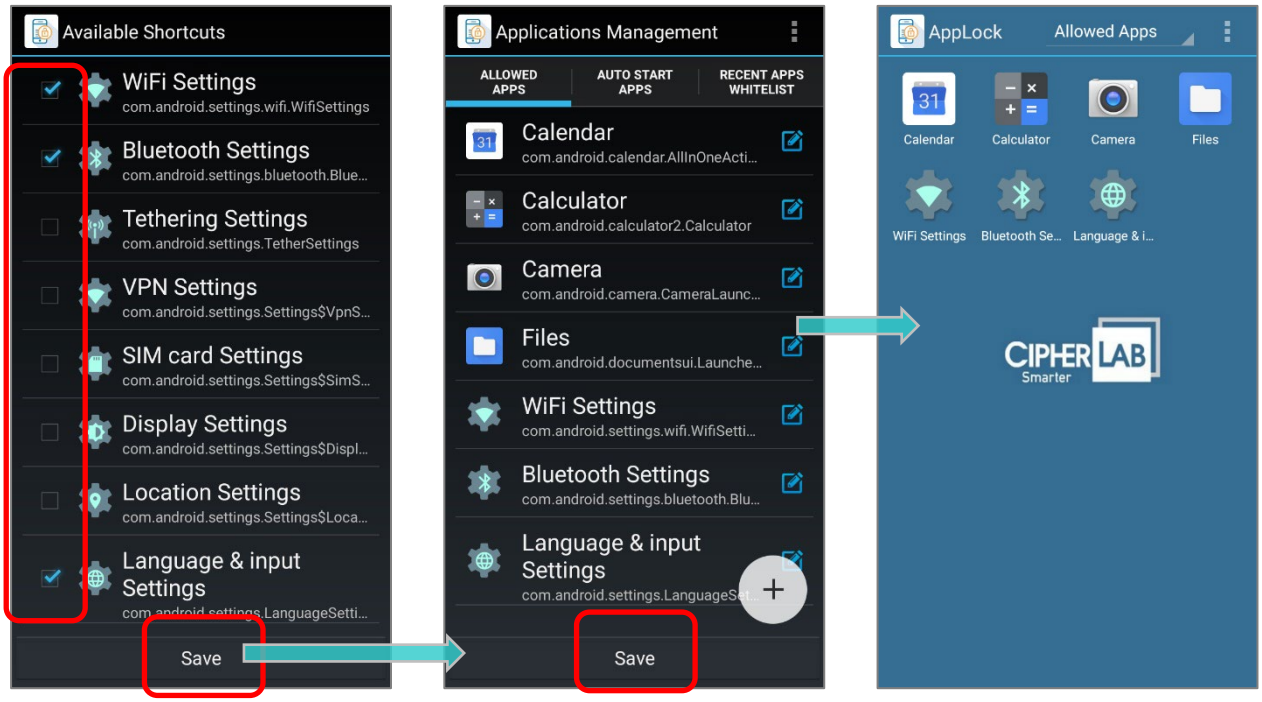


3) Tap on the "**Add**" button ⊕, and then "**Add Shortcut**".
The "**Available Shortcuts**" screen shows up, listing the shortcuts from system settings



4) Select the shortcuts you would like to make available on the **Allowed Apps** view, and tap on "**Save"**.

5) The **Allowed Apps** tab page shows the shortcuts (and applications) you assigned to **Allowed Apps** view. Tap on "**Save"** to save the settings.

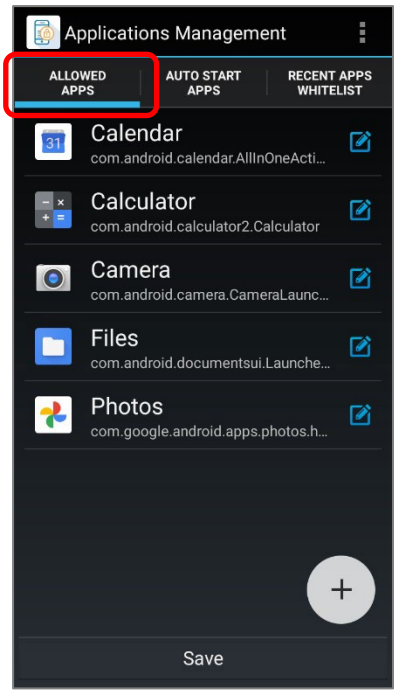


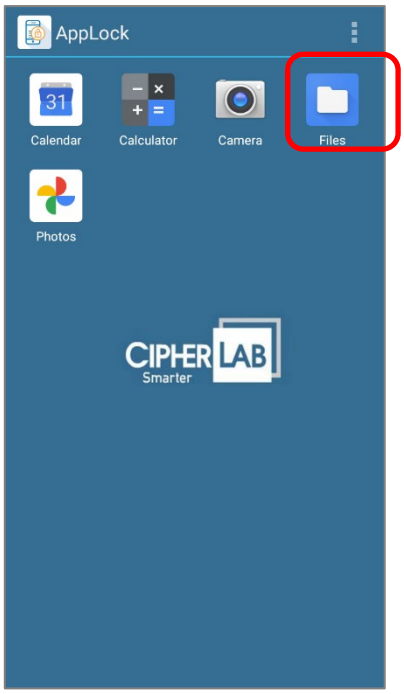
Note:

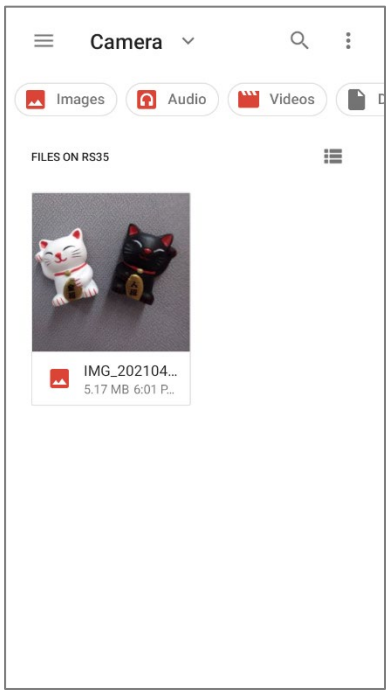
The shortcuts listed on **"Available Shortcuts"** screen depends on your device system setting.

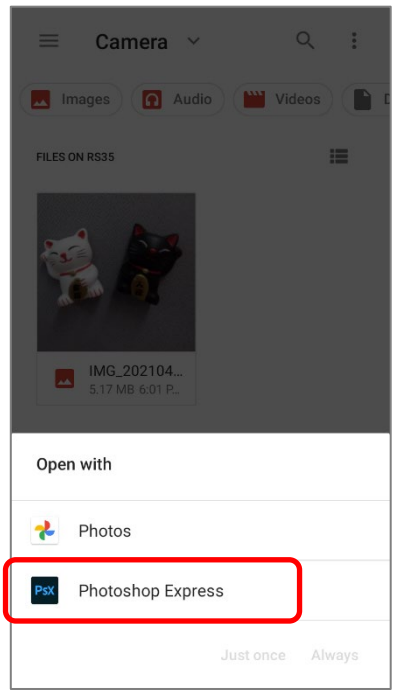
Note:

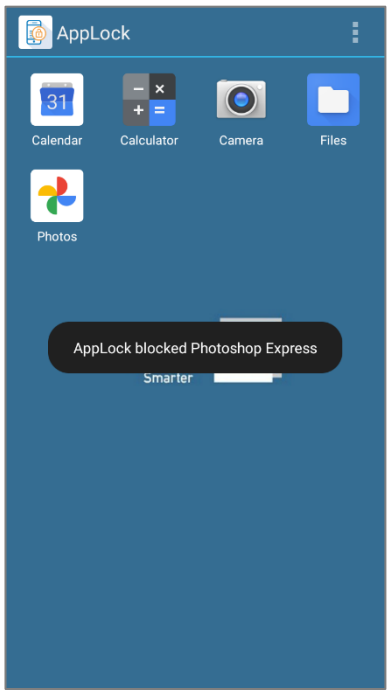
In **Applications Management** screen, administrators arrange which applications and shortcuts to be added to "**Allowed Apps**" list for users to access on **AppLock Main Screen**. Applications excluded from Allowed Apps list can be launched only by administrators. Thus, if users try to open a file by File Manager with an unallowed application in User Mode, AppLock will block the unallowed applications.





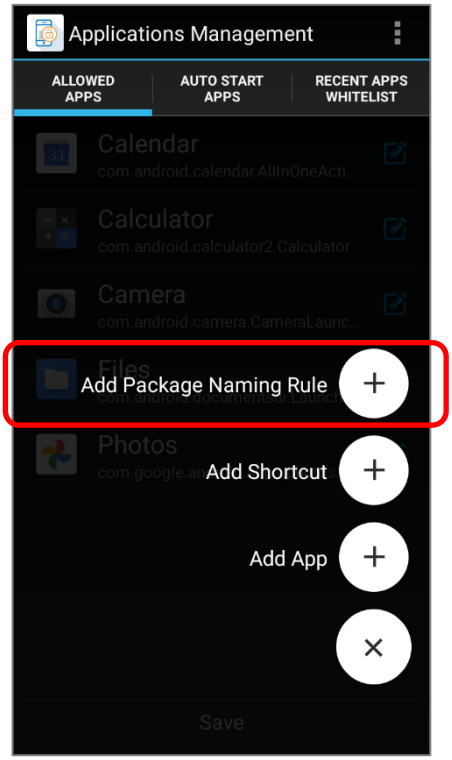






3.1.3 ADD PACKAGE NAMING RULE

Users are forbiddon from installing any apk (Android application package) which is not listed on "**Allowed apps list**", however, administrator can permit users installing apk by setting "**Add Package Naming Rule**".

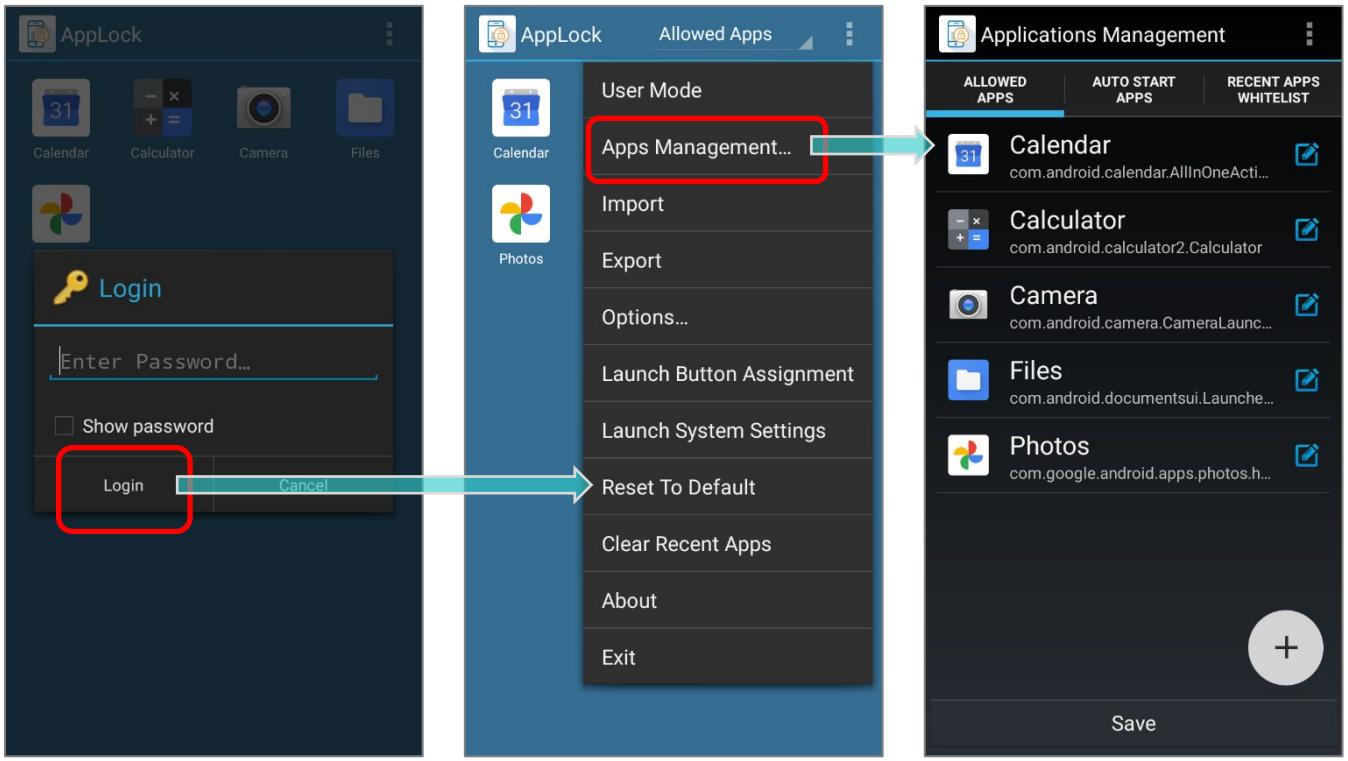


"**Add Package Naming Rule**" is for administrator to set the naming rule to prescribe which apk (Android application package) can be manually installed by users and automatically added to "**Allowed apps list**" after installation.

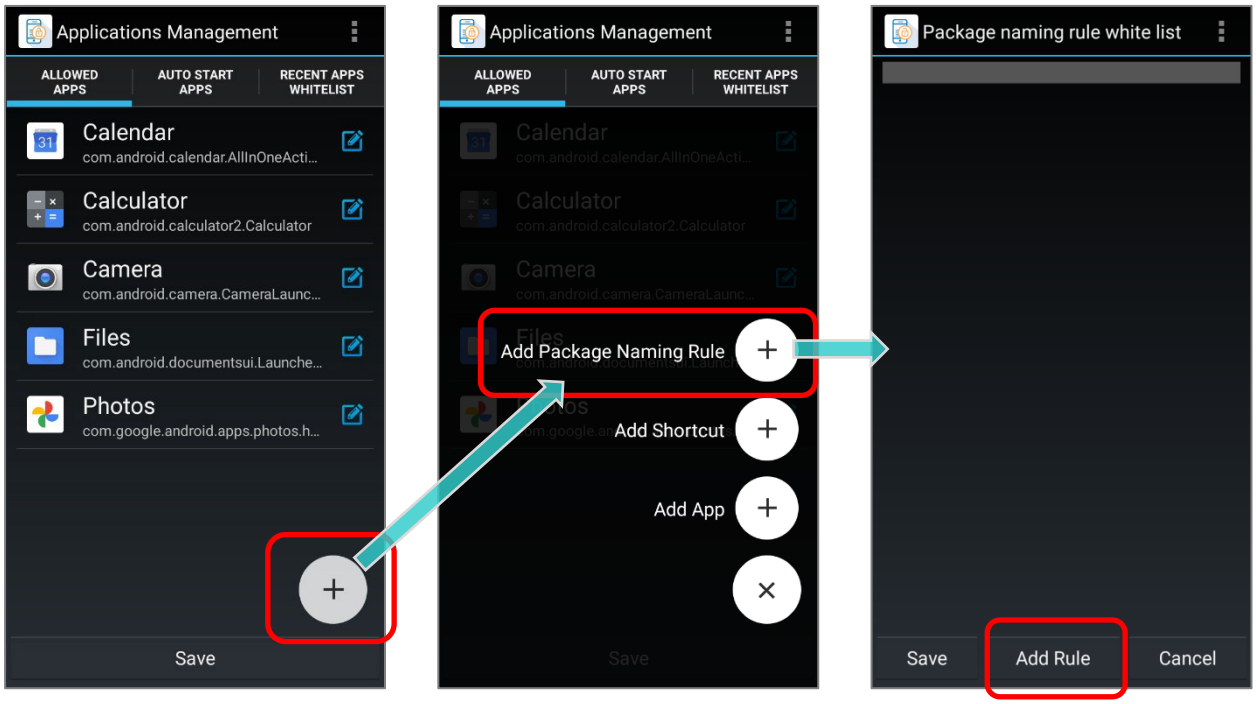
By adding your package naming rule, if users try to install the apk which doesn't match the rule, it will be blocked.

ADD RULE TO PACKAGE NAMING RULE WHITE LIST

To add package naming rule, please login as admin and enter Applications Management screen.

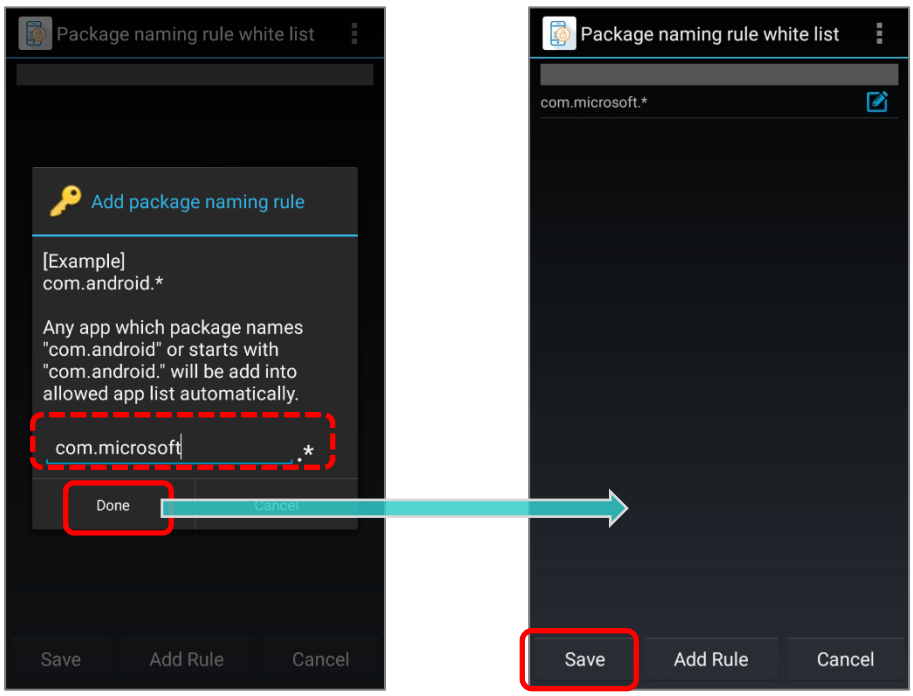


Tap on the “**Add**” button , and then “**Add Package Naming Rule**”. The “**Package naming rule white list**” screen shows up.



Tap “**Add Rule**” and enter your rule in the pop-up window, and then tap on “**Done**” to add your rule to “**Package naming rule white list**”.

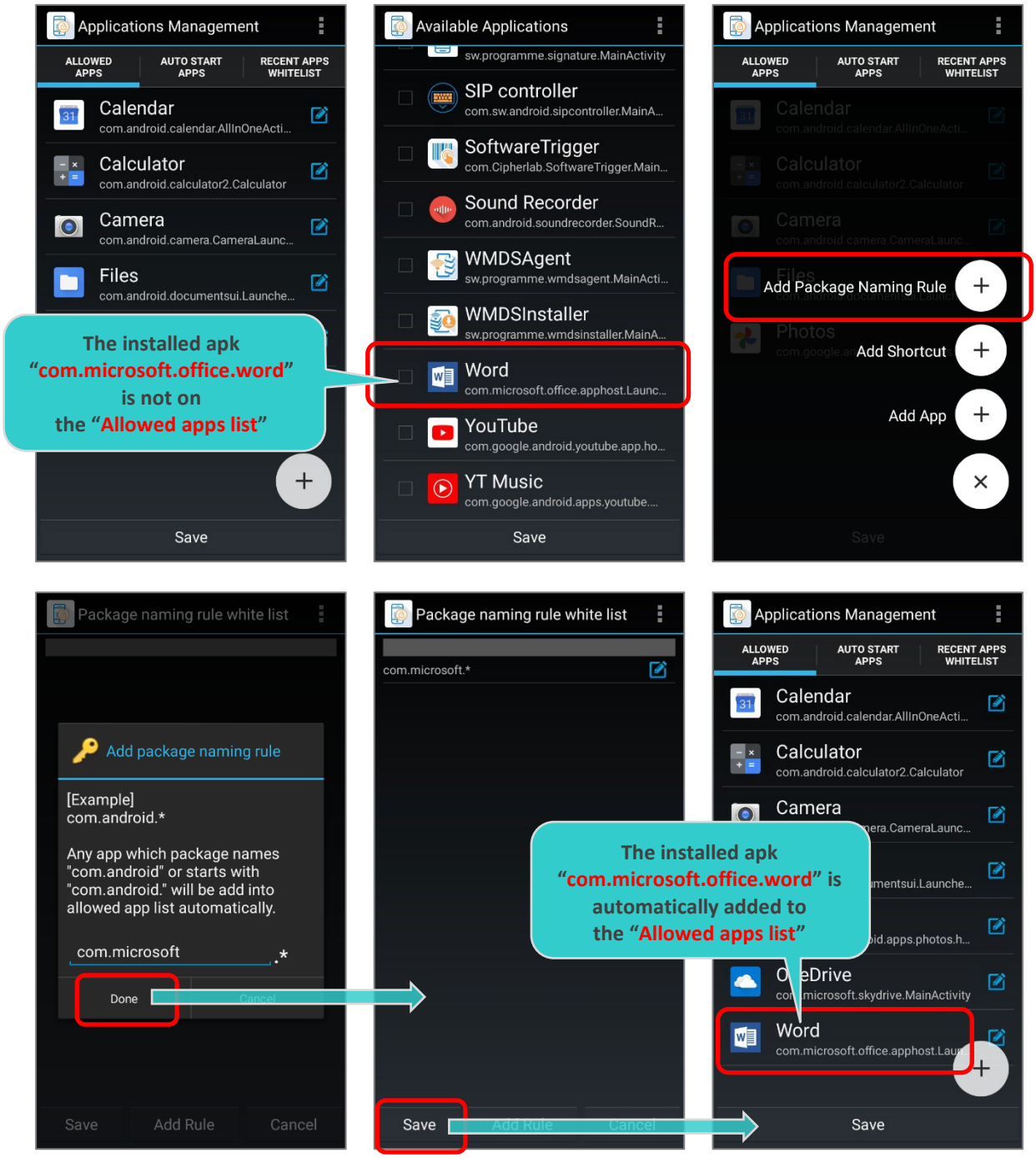
The following example is adding “**com.microsoft**” as the package naming rule. To make your packaging naming rule take effect, make sure to tap on “**Save**” in every page before returning to the main screen.



THE INSTALLED APK MATCHES THE NEWLY-ADDED PACKAGE NAMING RULE

Before the package naming rule(s) is set, any installed apk will not be displayed if it is not selected to be shown on “Allowed apps list”. Once administrator add the rule(s) to “**Package naming rule white list**”, the installed apk which matches the rule(s) will be added to “Allowed apps list” automatically.

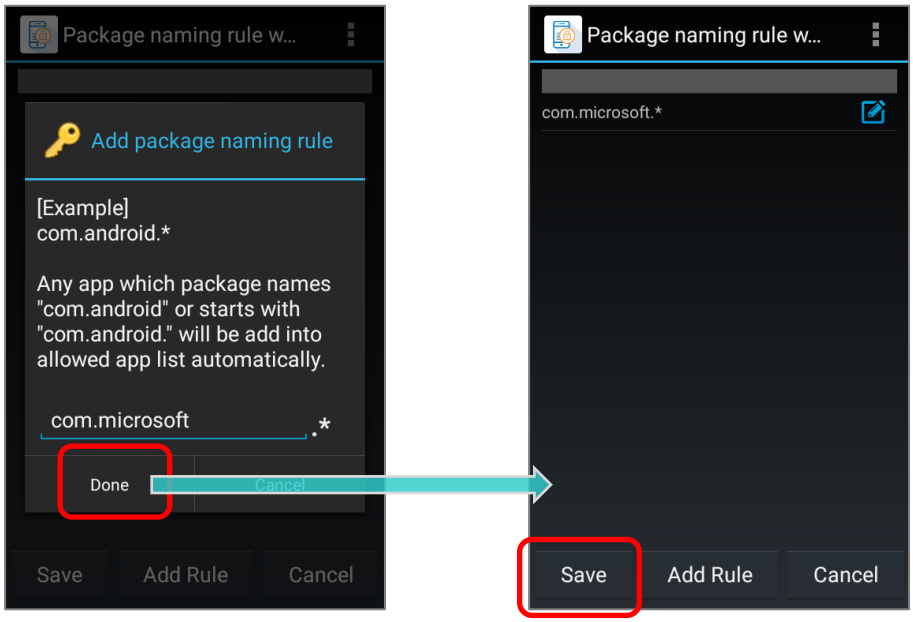
For example, the installed apk “**com.microsoft.office.word**” is not on the “**Allowed apps list**”. After setting “**com.microsoft**” as the package naming rule, the installed apk “**com.microsoft.office.word**” is automatically added to “**Allowed apps list**”.



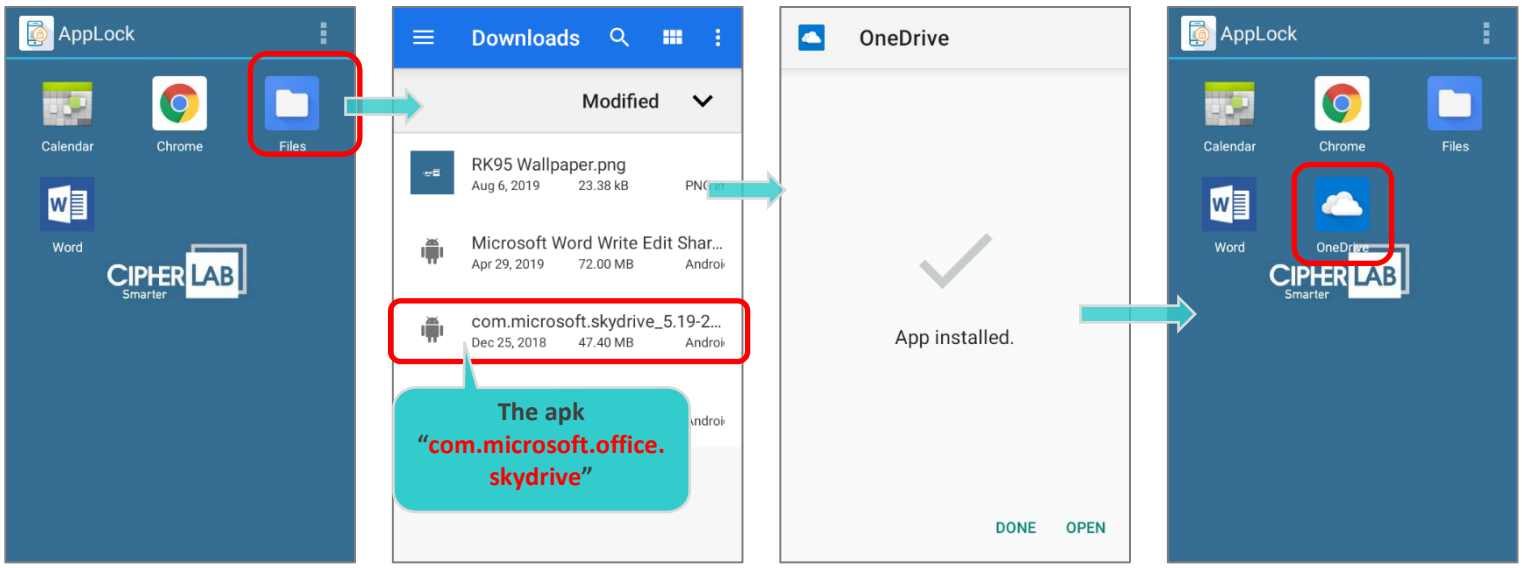
INSTALLING APK AFTER SETTING PACKAGE NAMING RULE

Once administrator add the rule(s) to "**Package naming rule white list**", users can manually install the apk which match the rules. The following example is adding "**com.microsoft**" as the package naming rule:

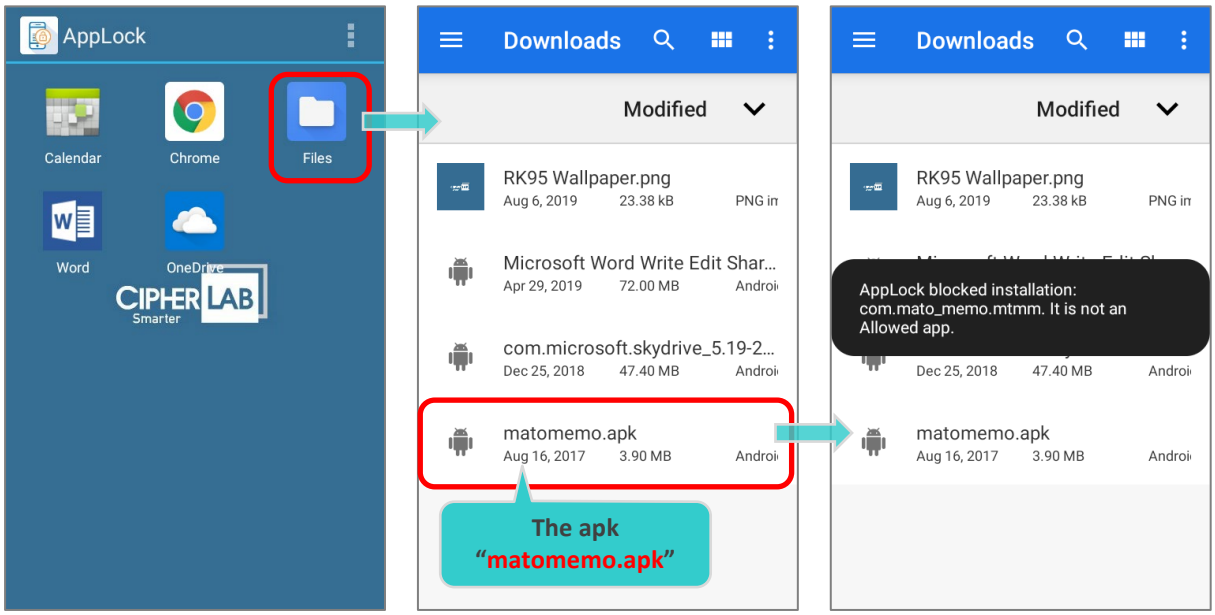
1) In admin mode, setting "**com.microsoft**" as the package naming rule.



2) In user mode, manually installing the apk "com.microsoft.skydrive" which matches the package naming rule "**com.microsoft**", and the apk "com.microsoft.skydrive" is successfully installed.



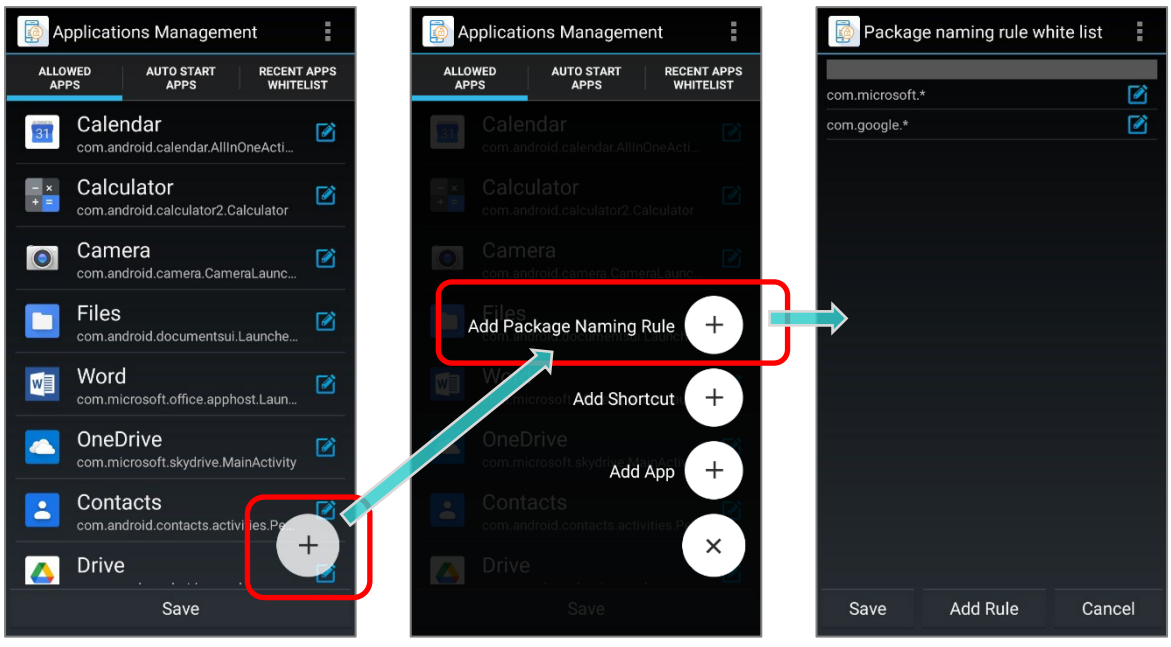
3) In user mode, manually installing the apk “matomemo.apk” which doesn’t match any rules on “**Package naming rule white list**”, and it is blocked.



Note: To restrict the installation of the apk which doesn’t meet the “**package naming rule**”, “**Monitor App Installation**” should be enabled in advanced.

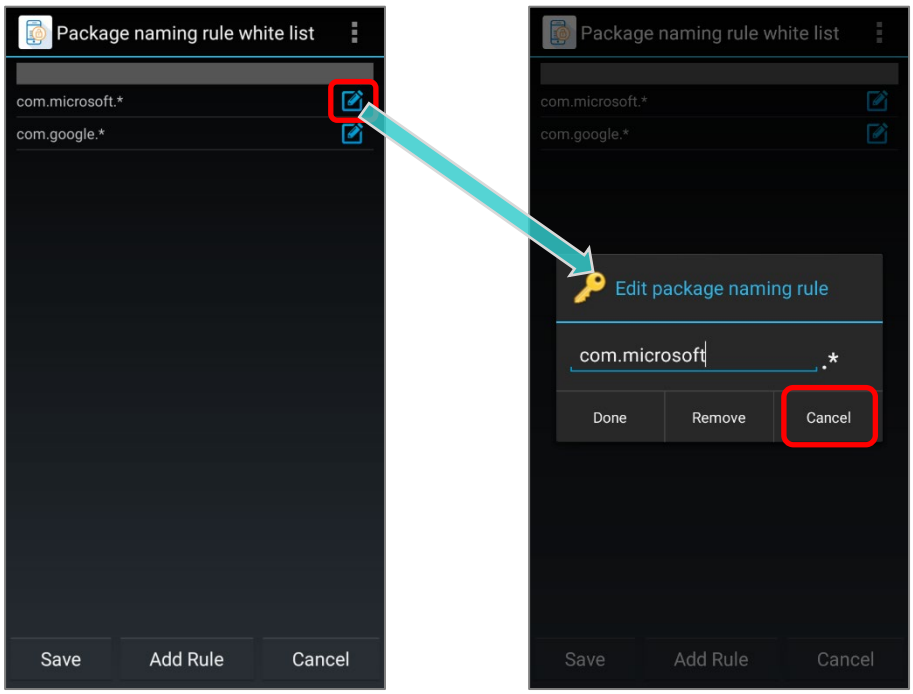
DELETE PACKAGE NAMING RULE(S)

Please log in as admin and access Applications Management → “**Add**” button (+) → “**Add Package Naming Rule**”, and follow the steps to delete the package naming rules:



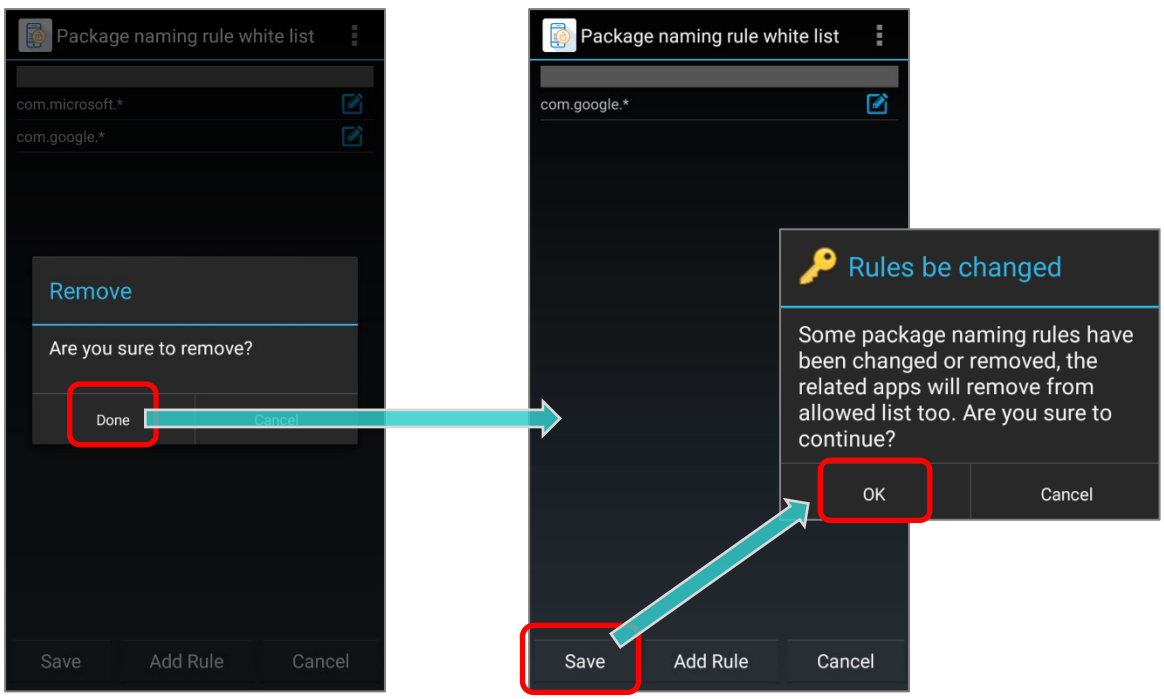
TO DELETE A SINGLE RULE

1) In “**Package naming rule white list**” page, tap on “**Edit**” button on the right side of the rule you would like to remove to open its “**Edit package naming rule**” pop-up window.



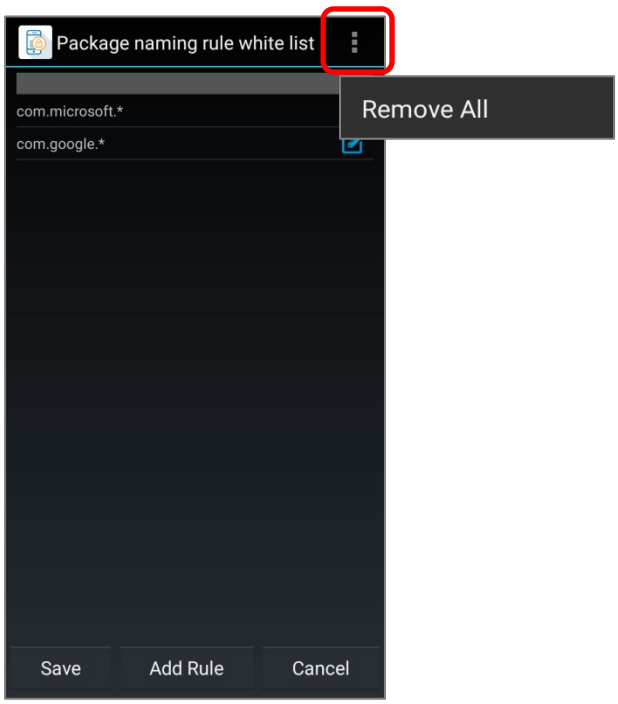
2) Tap on “**Remove**” to delete this rule, and confirm by tapping on “**Done**”

3) The rule is now removed. Make sure to tap on “**Save**” in every page before returning to the main screen to make your settings take effect.



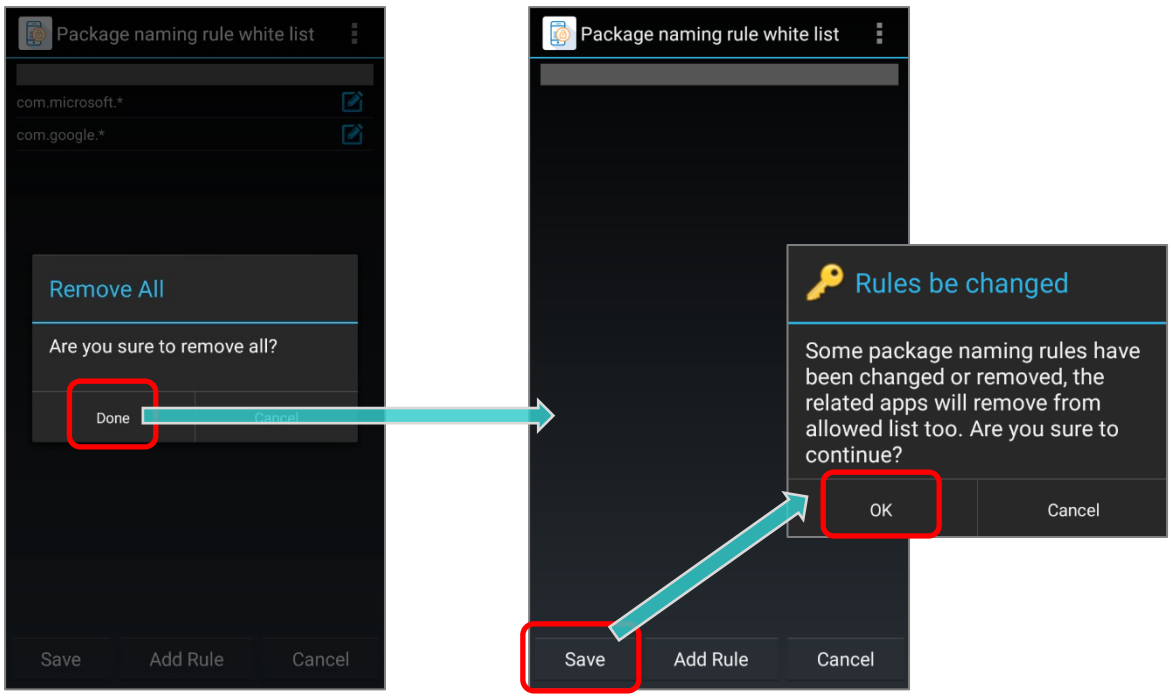
TO DELETE ALL RULES

1) In "**Package naming rule white list**" page, tap on "**More**" button ⋮ on the action bar.



2) Tap on "**Remove All**" and confirm by tapping on "**Done**".

3) All rules are removed. Make sure to tap on "**Save**" in every page before returning to the main screen to make your settings take effect.



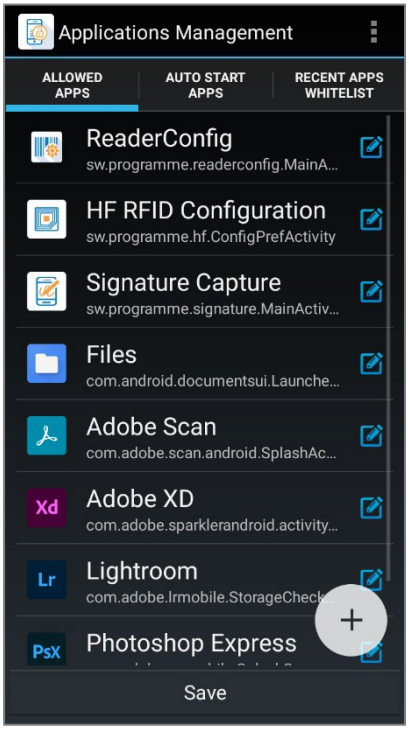
Note:

Remove "**package naming rule**" will delete the relative apps at the same time.

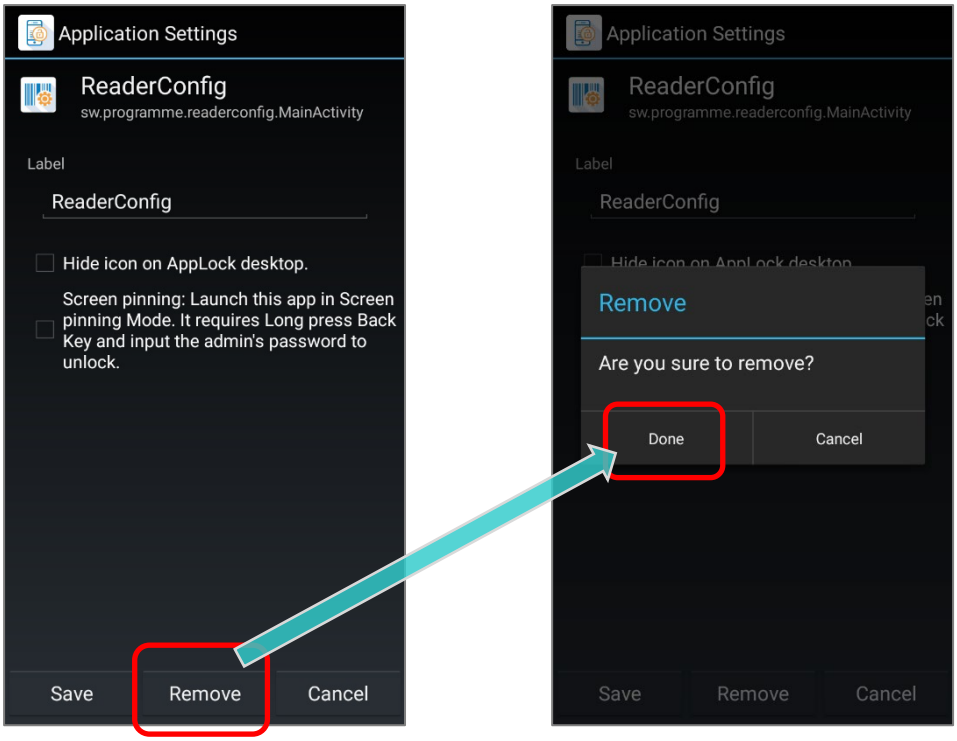
3.1.4 DELETE APPLICATIONS OR SHORTCUTS

To delete an application or shortcut:

1) In the **Allowed Apps** tab page under **Applications Management** screen, tap the application or shortcut to edit.



2) Tap on "**Remove**" in the bottom, and confirm by tapping on "**Done**".



3.1.5 CLEAR ALL APPLICATIONS AND SHORTCUTS

You may clear all applications and shortcuts made available to the **Allowed Apps** view. The steps to clear all applications differs base on the scenario as following:

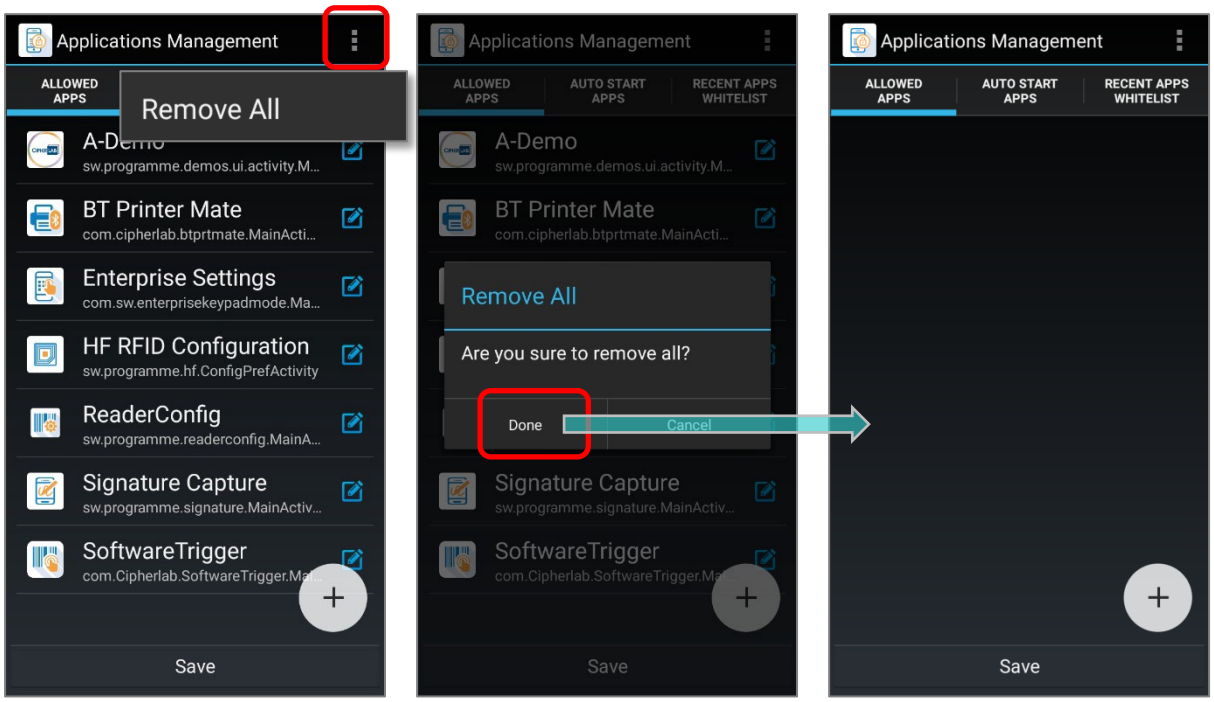
NO APPS ON ALLOWED APPS LIST ARE AUTOMATICALLY ADDED BY PACKAGE NAMING RULE

If all the apps and shortcuts on the "**Allowed Apps list**" are all manually added by administor, all apps can be deleted at one time:

1) In the **Applications Management** screen, tap on "**Allowed Apps**".

2) Tap the **More** button ⋮ on the action bar.

3) Tap on "**Remove All**" and confirm by tapping on "**Done**". All the applications and shortcuts on the **Allowed Apps** view will be cleared.



4) Make sure to save your changed settings before leaving **Application Management** page.

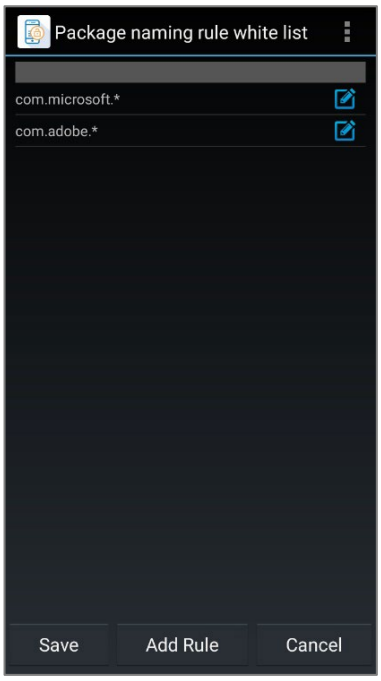
ALL APPS ON ALLOWED APPS LIST ARE AUTOMATICALLY ADDED BY PACKAGE NAMING RULE

If there are only apps added by "**Package Naming Rule**" on the "**Allowed Apps list**", you can delete all of them by:

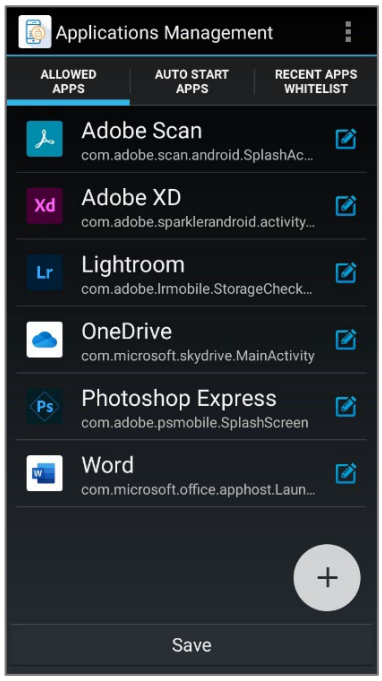
1) In the **Applications Management** screen, tap on "**Allowed Apps**".

2) Tap the **More** button ⋮ on the action bar.

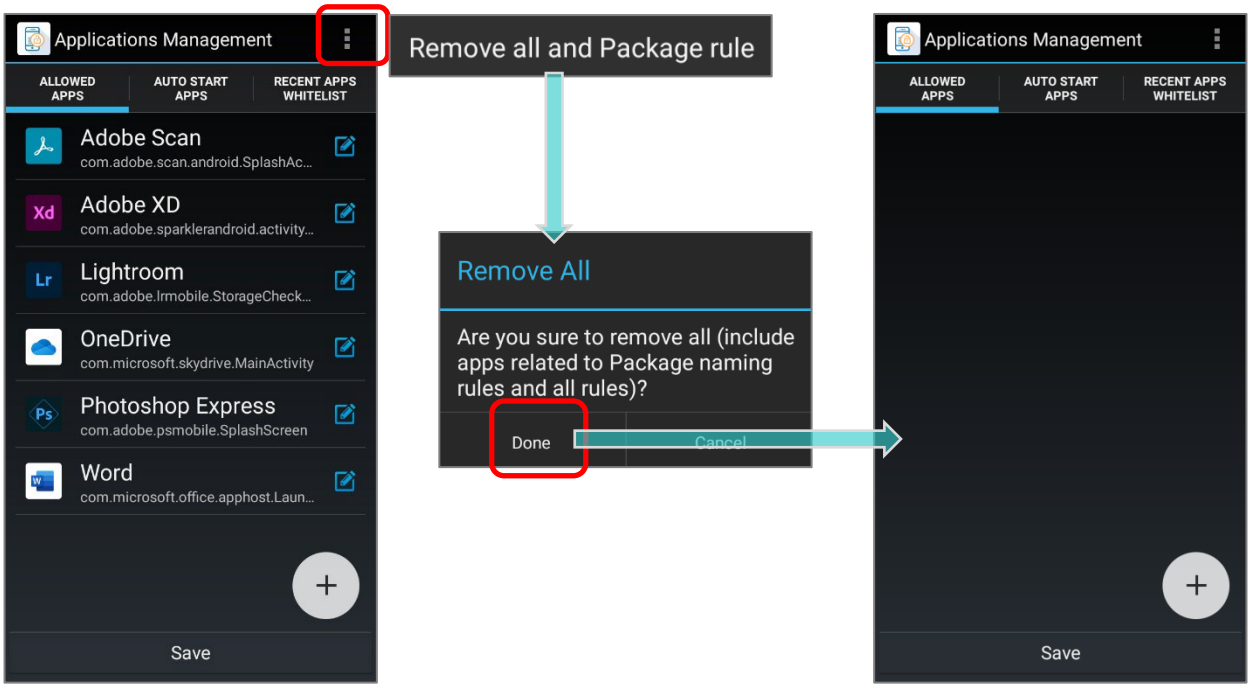
The Package Naming Rule



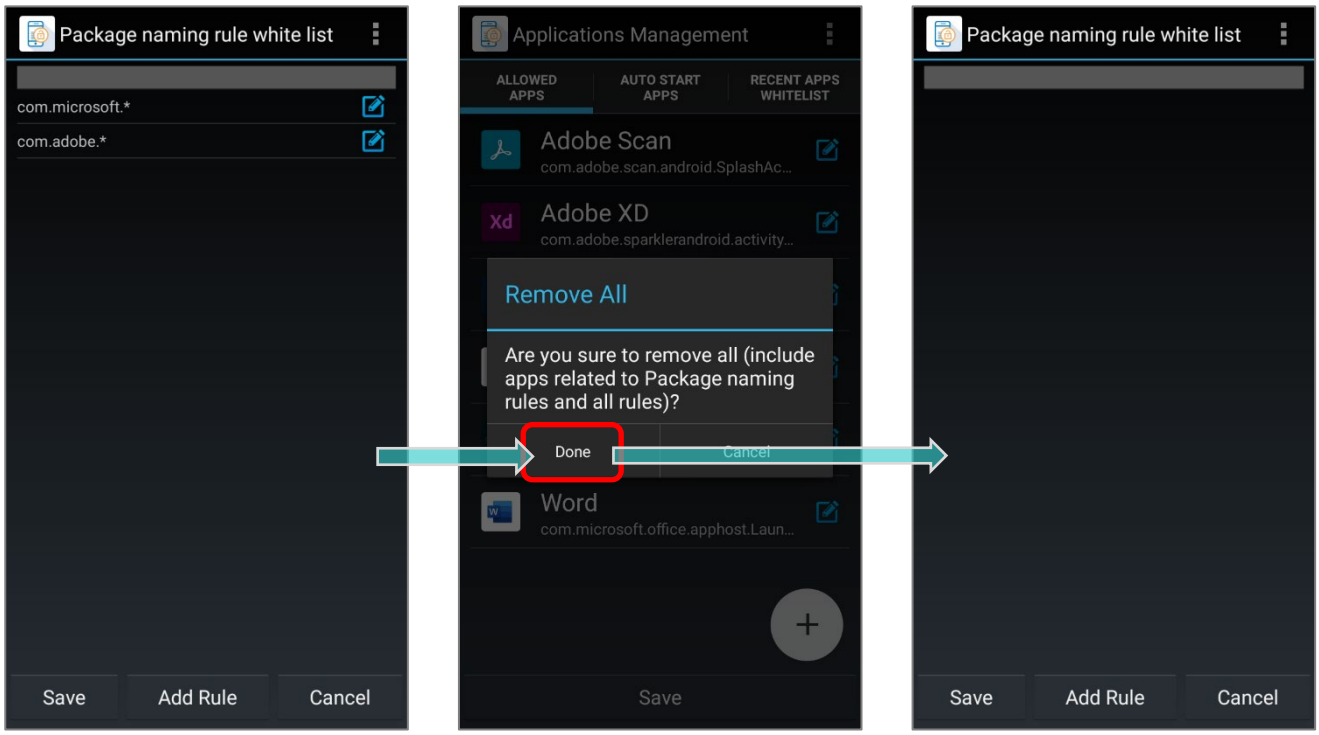
The Allowed Apps List



3) Tap on "**Remove All and Package rule**" and confirm by "**Done**". All the applications on the Allowed Apps view will be cleared.



Please note that deleting all apps by “**Remove All and Package rule**”, your “**Package Naming Rule**” on “**Package naming rule white list**” will be all removed at the same time.



The Package Naming Rule (original)

Delete all apps on Allowed Apps list by “Remove All and Package rule”

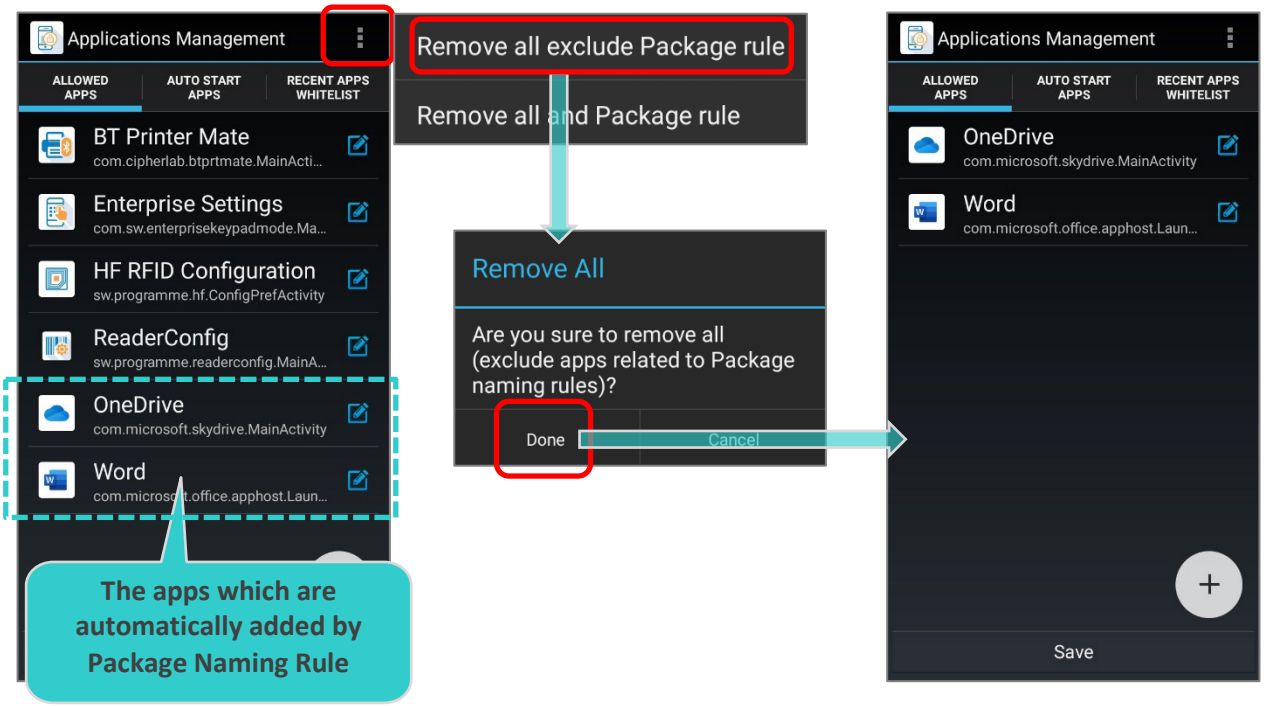
The Package Naming Rule (after performing “Remove All and Package rule”)

ALLOWED APPS LIST CONTAINS BOTH MANUALLY-ADDED APPS & APPS AUTOMATICALLY ADDED BY PACKAGE NAMING RULE

If manually-added apps, shortcuts, and apps automatically added by Package Naming Rule are all listed on "**Allowed Apps list**", you may delete them by:

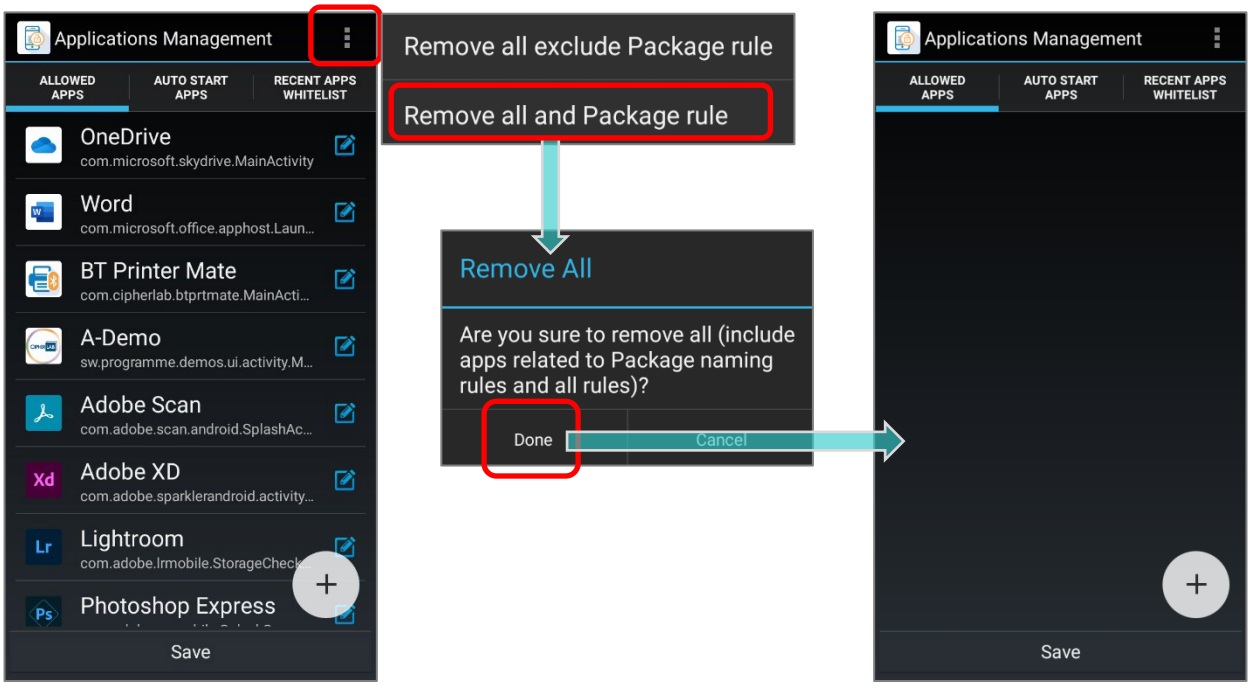
REMOVE ALL EXCLUDE PACKAGE RULE

1) In the Applications Management screen, tap on "**Allowed Apps**".
2) Tap the **More** button ⋮ on the action bar.
3) Select "**Remove all exclude Package rule**", and all the manually-added apps & shortcuts will be removed while apps automatically added by **Package Naming Rule** remain on "**Allowed Apps list**".

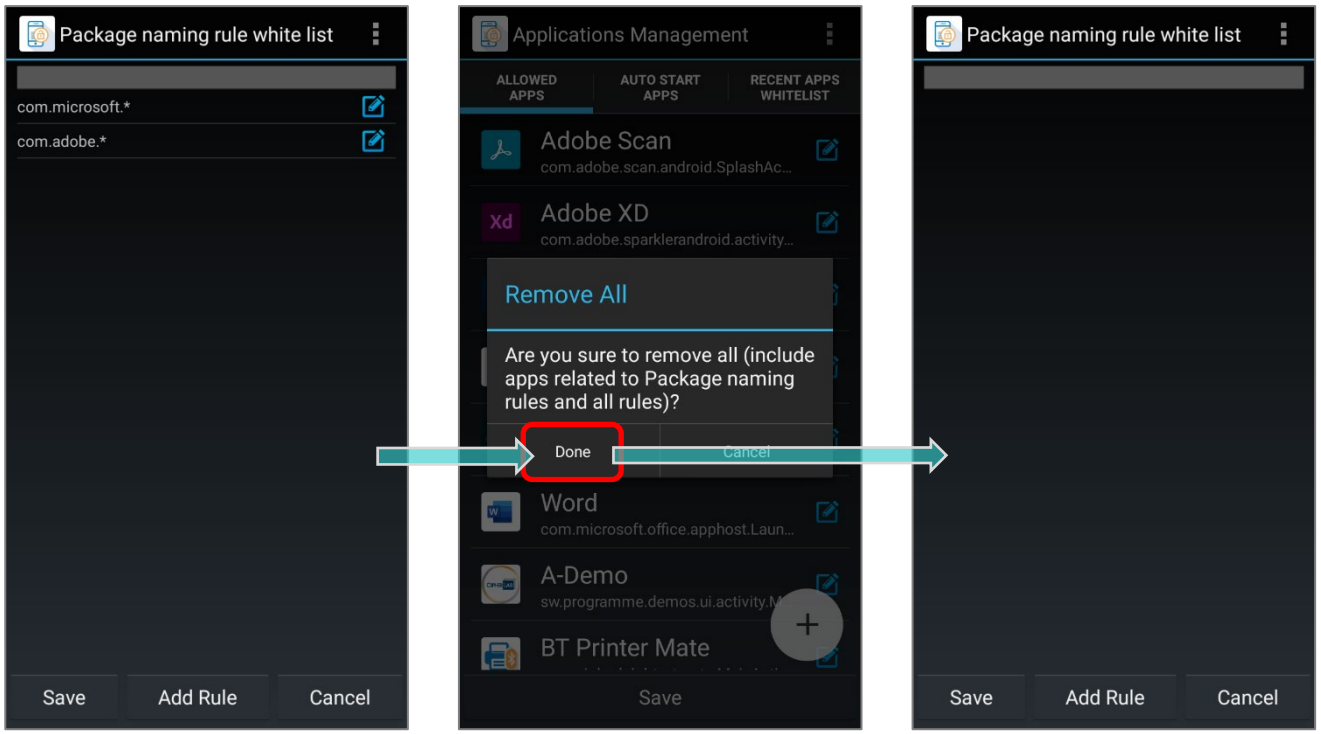


REMOVE ALL AND PACKAGE RULE

To remove all the apps and shortcuts including manually-added apps and apps added by Package Naming Rule at one time, please tap on "**Allowed Apps**" tab page → the **More** button ⋮ on the action bar → "**Remove all and Package rule**".



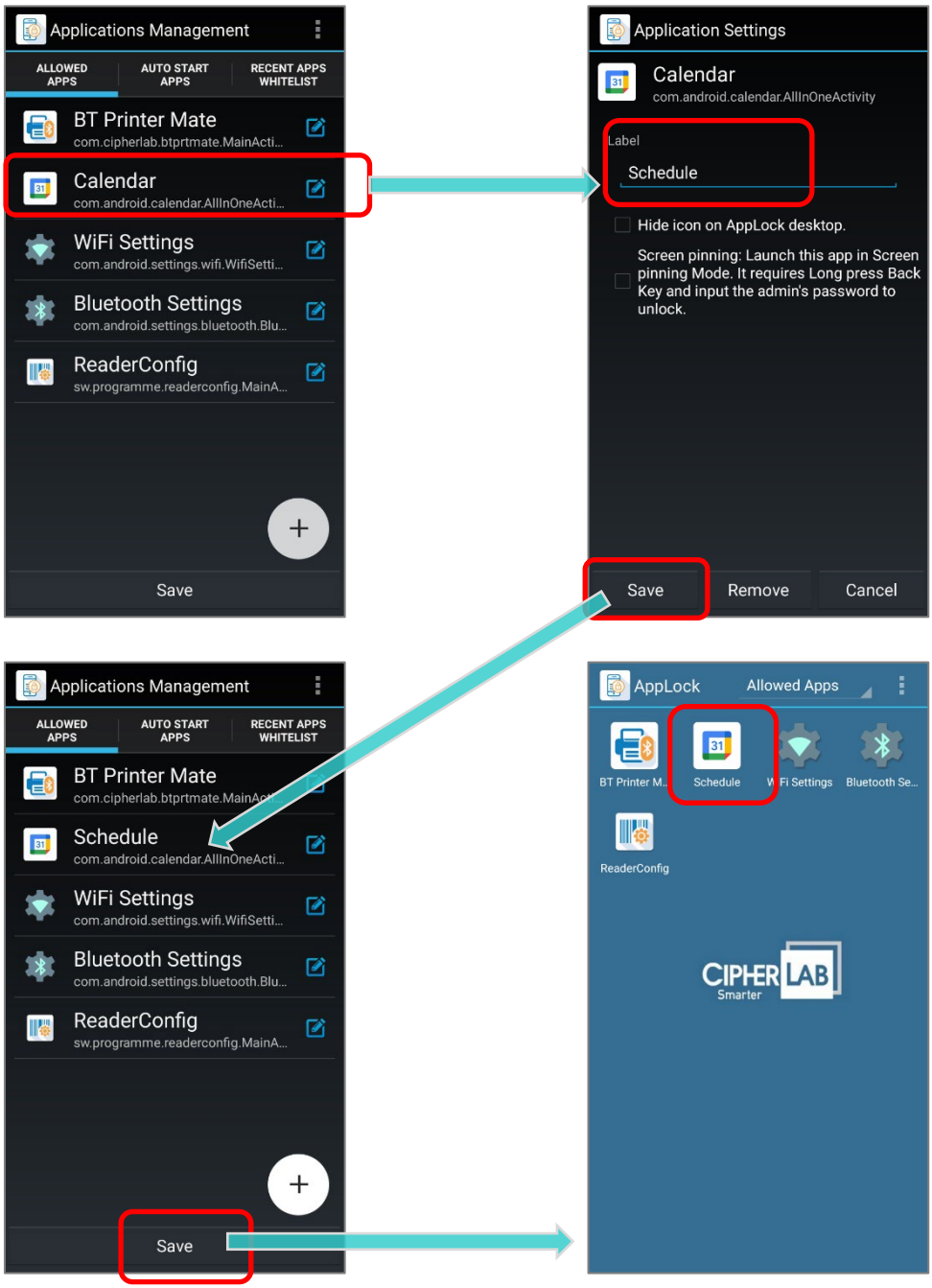
By selecting "**Remove All and Package rule**", your "**Package Naming Rule**" on "**Package naming rule white list**" will be all removed at the same time.



3.1.6 RENAME APPLICATIONS OR SHORTCUTS

To rename an application or shortcut:

1) In the **Applications Management** screen, tap on "**Allowed Apps**".
2) Tap an application you would like to rename.
3) Edit its new name in the blank under **Label**, and confirm the word you enter.
4) Tap on "**Save**" to save the name.
5) The new name will show on the **Allowed Apps** view, tap on "**Save**" to save this setting.



3.2 AUTO START APPS VIEW

3.2.1 SET APPLICATION AS AUTO START APPS

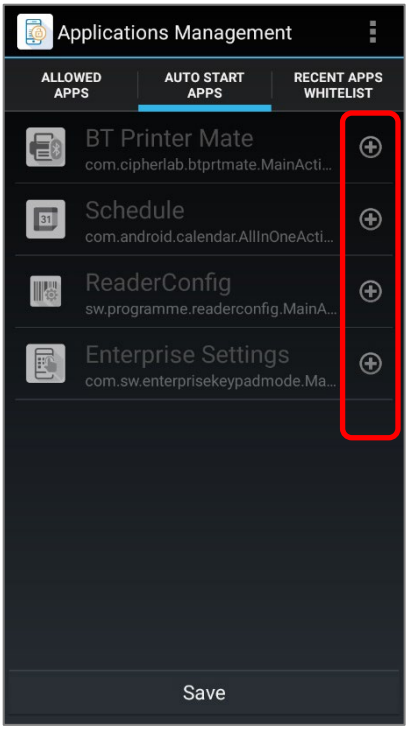
To set an application to auto start once AppLock launches:

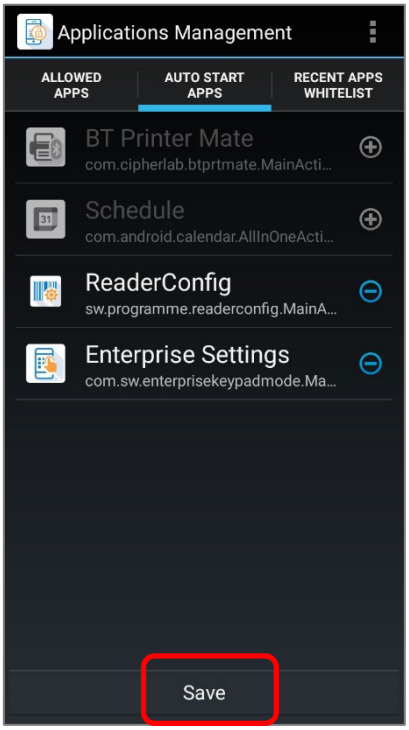
1) In the Applications Management screen, tap **Auto Start Apps**.

2) Tap on the right of the application to add it to **Auto Start Apps**.

3) The application will be added to the **Auto Start Apps** view.

4) Tap **Save** to save the setting.





Note:

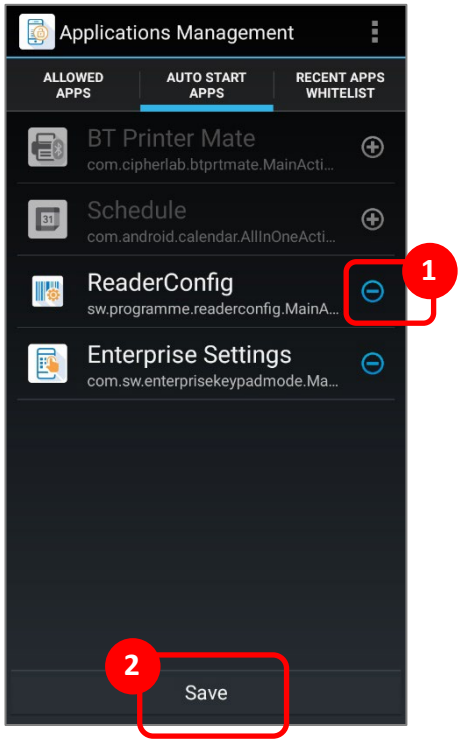
You may add more than one application to the **Auto Start Apps** view.

3.2.2 REMOVE APPLICATION

To cancel auto start of the application:

1) On **Auto Start Apps** view, tap on on the right of the application.

2) Tap on "**Save**".



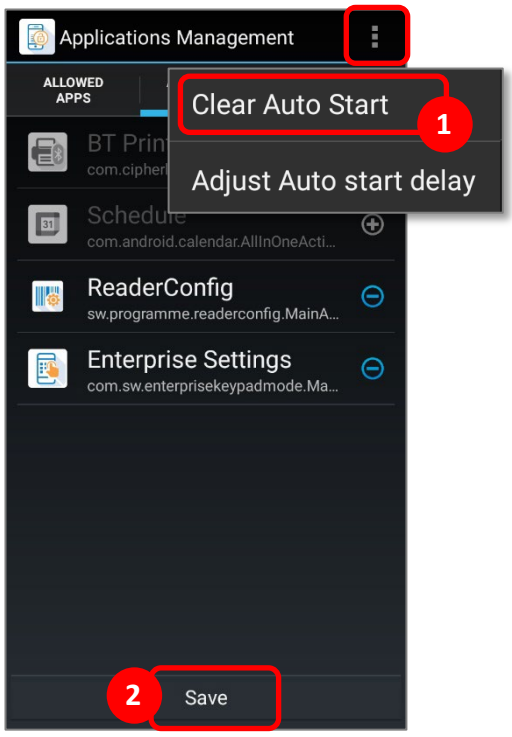
3.2.3 CLEAR ALL APPLICATIONS

You may clear all applications made available to the **Auto Start** Apps view.

1) In the **Applications Management** screen, tap on "**Auto Start Apps"**.

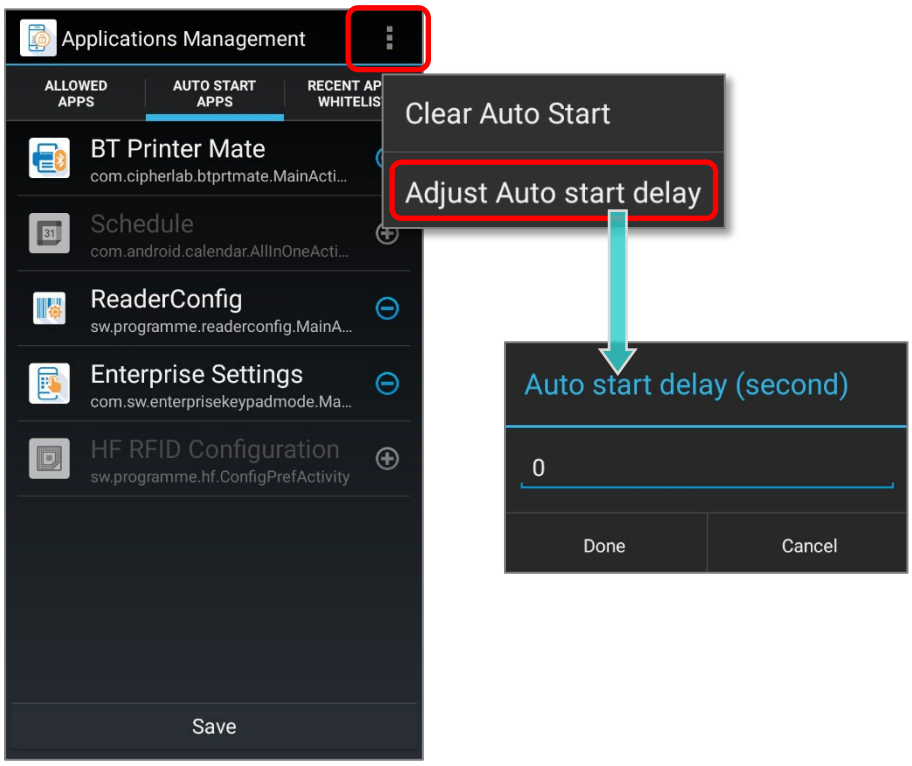
2) Tap the **More** button on the action bar.

3) Tap on "**Clear Auto Start**" in the drop-down menu. The applications on the **Auto Start Apps** view will be cleared.



3.2.4 ADJUST AUTO START DELAY

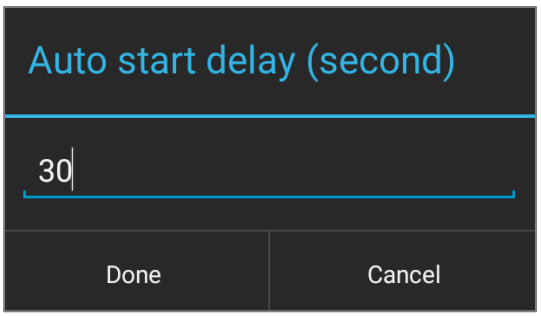
"**Adjust Auto Start Delay**" is to specify a certain amount of time to delay launching the Auto Start Apps at AppLock startup. The default setting is **0** (second).



To configure the delay time:

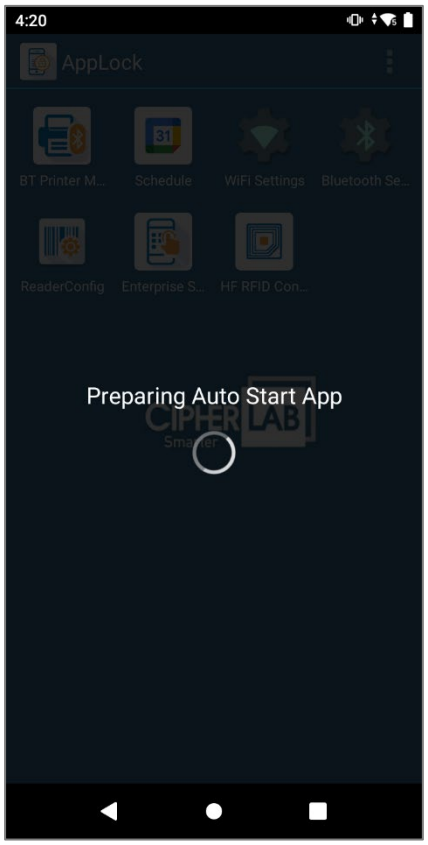
1) In the **Applications Management** screen, tap on "**Auto Start Apps**", and then tap on the **More** button ⋮ on the action bar. Select "**Adjust Auto start delay**" in drop-down menu.

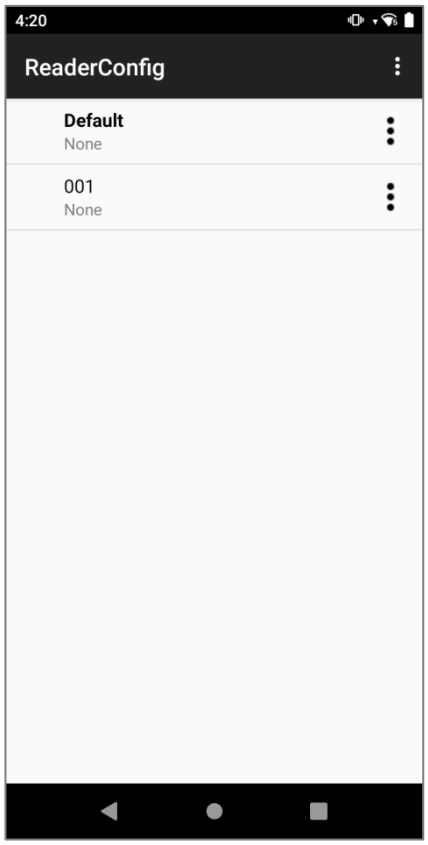
2) Input the delay time (the maximum is 30 seconds) in the pop-up window and then tap on "**DONE**" to save the setting.



3) Make sure to tap on "**Save**" in every page before returning to the main screen.

Once the delay time is set, everytime you launch AppLock or boot up the mobile computer whose home app is set to be AppLock, those "**Auto Start Apps**" will be launched after the delay time. During the delay time, the prompt "**Preparing Auto Start App**" is displayed on screen.



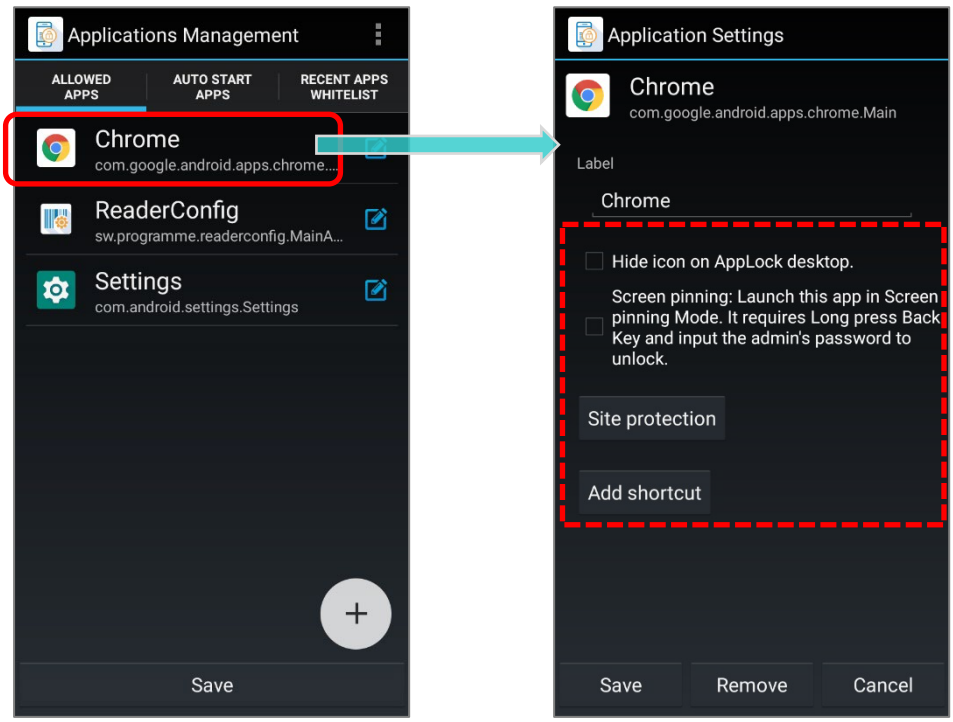


Note:

If the mobile computer (whose home app is AppLock) is booted up or rebooted, the "**Preparing Auto Start App**" screen shows up during the preiod before the system booting is completed, thus, it may take few more seconds to wait for "**Auto Start Apps**" to show up even the delay time is set to be 0 second.

3.3 MORE APPLICATION SETTINGS FOR ALLOWED APPS VIEW

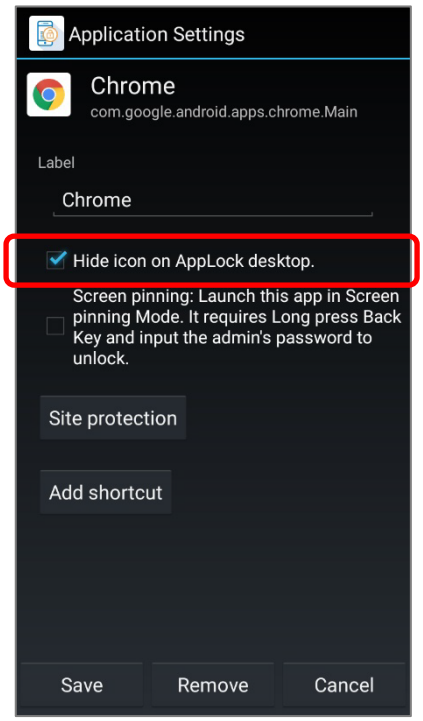
Except of the basic settings, such as add or delete applications and rename applications, **Allowed Apps Views** offers more applications settings for administrator to further control the interface provided to users.



3.3.1 HIDE ICON ON APPLOCK DESKTOP

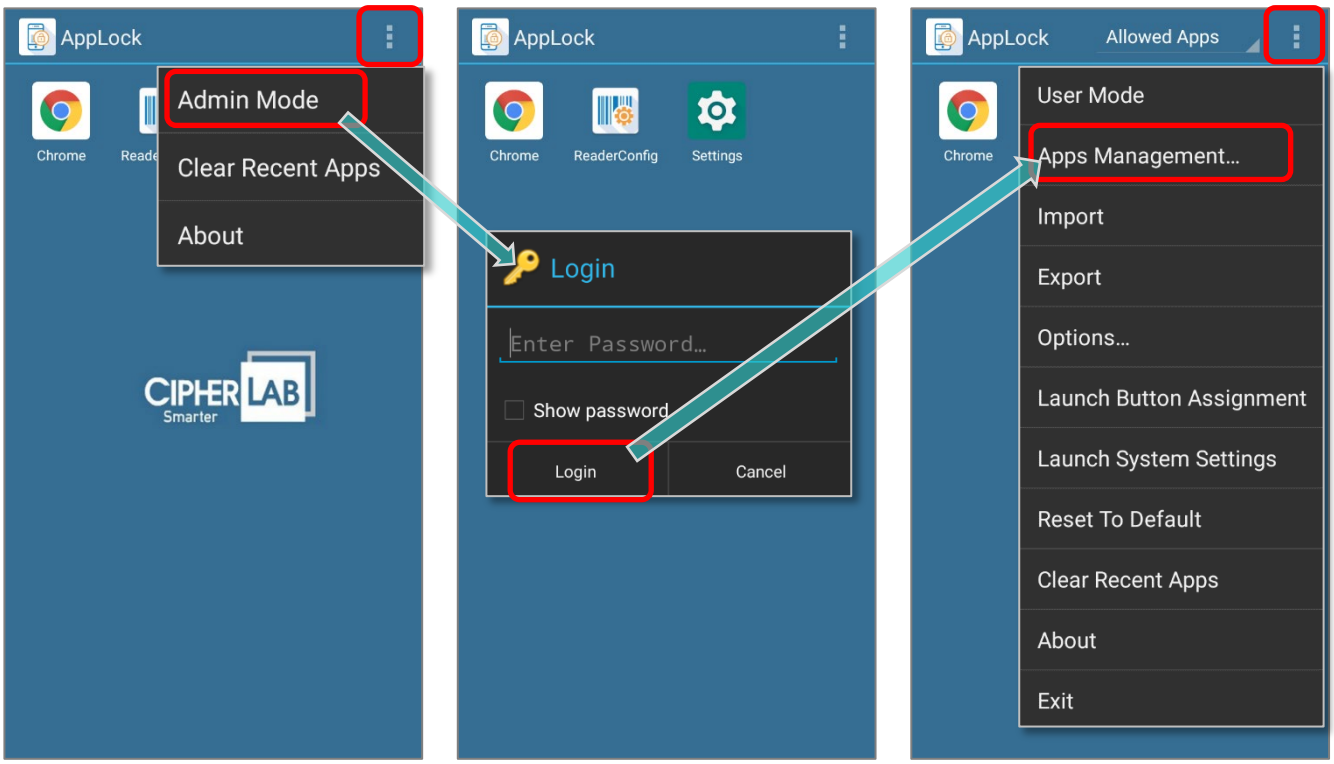
"**Hide icon on AppLock desktop**" is the function for the administrator to determine whether an app/ shortcut on Allowed Apps list is visiable in Allow Apps view of the main screen.

With "**Hide icon on AppLock desktop**" enabled, the app/ shortcut will not be shown in **Allow Apps view** no matter in **Admin Mode** or **User Mode**, but it is still operational as other apps displayed on Allow Apps view.

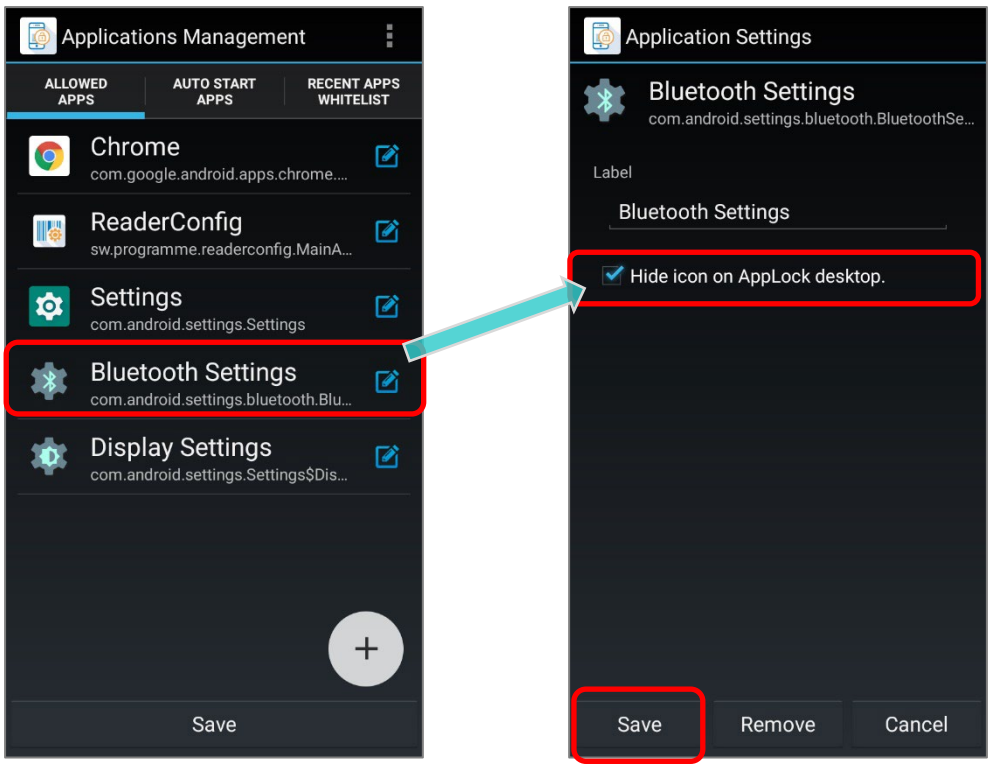


To enable "**Hide icon on AppLock desktop**", please:

1) Login to **Admin** Mode, and enter **Applications** Management screen.

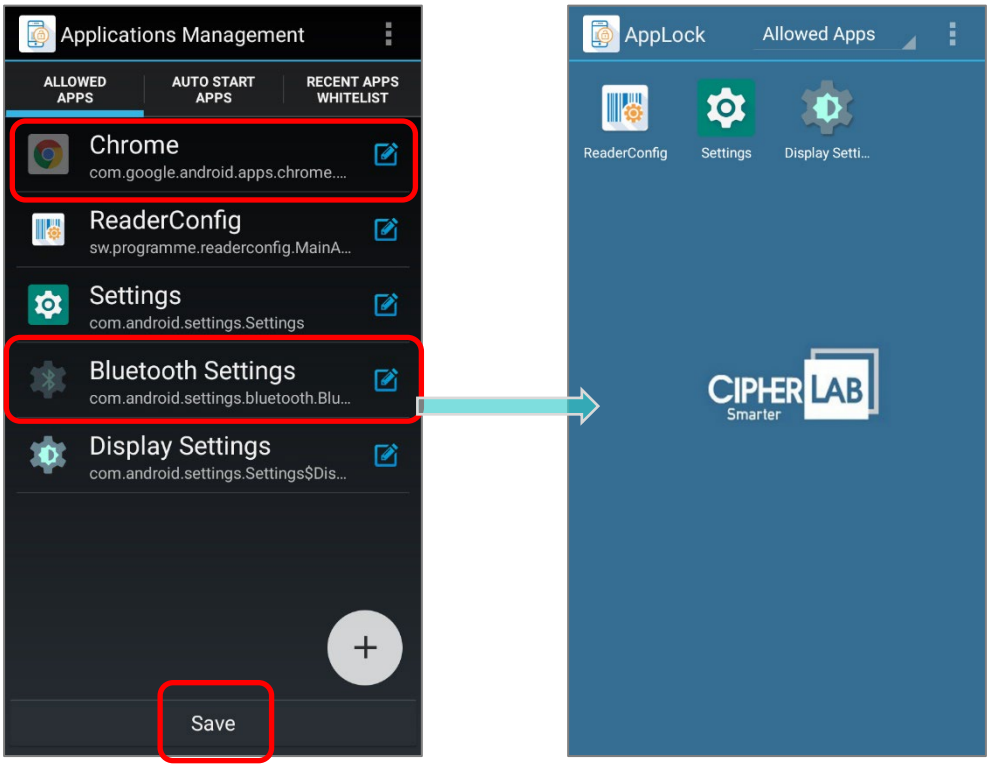


2) In Application Management page, tap the application or shortcut on Allowed Apps list to enter its "**Application Settings**" page. Tick "**Hide icon on AppLock desktop**" and tap "**Save**".



3) This app/ shortcut icon on Allowed Apps list is now darker than those apps without "**Hide icon on AppLock desktop**" enabled.

   Make sure to save before leaving Application Management screen.



3.3.2 SCREEN PINNING

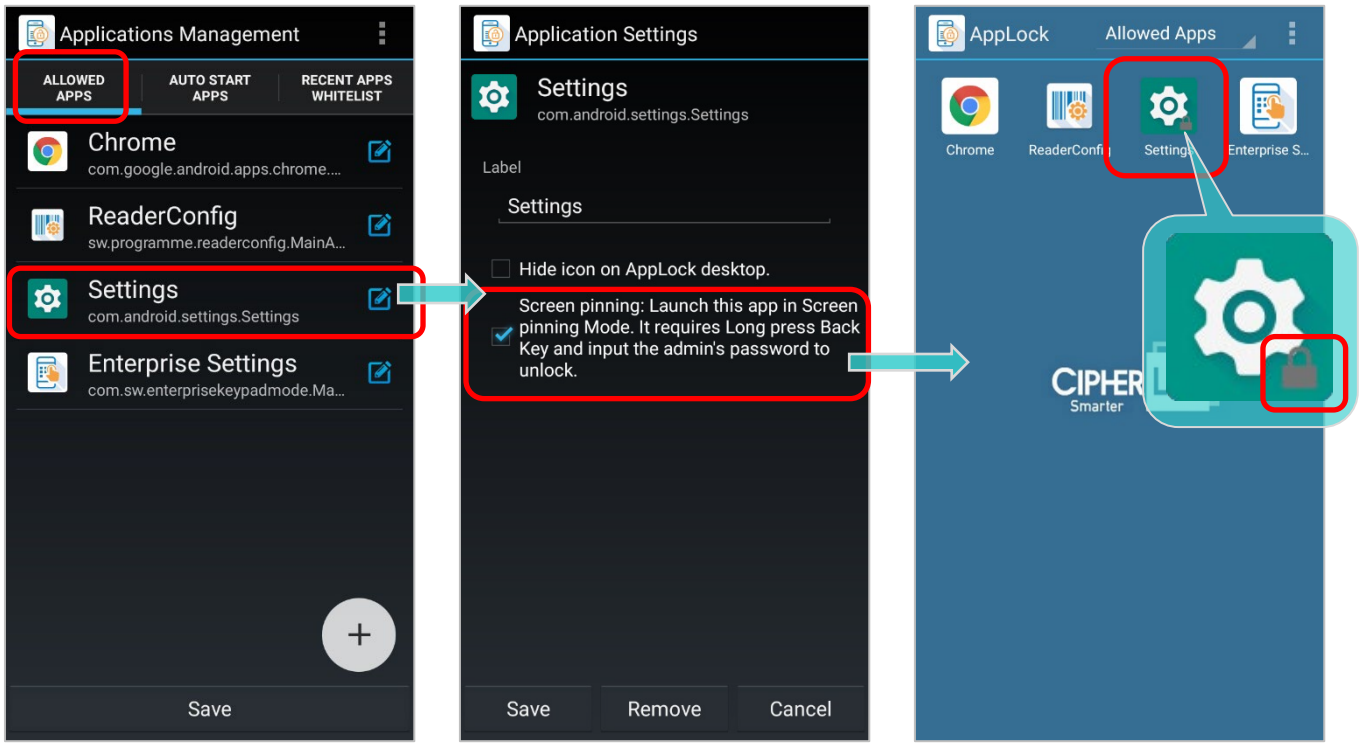
Applications with "**Screen Pinning**" function enabled could not be exited or closed by tapping any hardware buttons or by any means, even if the application itself offers the quit/exit/leave function. The only way to unpin the screen-pinned application is to long press **Back** button and then input the admin password in the "**Unpin Application**" pop-up window.

Once the application is unpinned, click **Back** button again to exit it.

ENABLE SCREEN PINNING FUNCTION FOR AN APPLICATION

To enable "**Screen Pinning**" function for a certain application, please:

1) Enter Application Management → Allowed Apps tab page
2) Click the application to be enabled "**Screen Pinning**", and tick the screen pinning function in its Application Settings page.
3) Save the settings. The screen-pinned application is now with a lock icon in the lower-right corner.

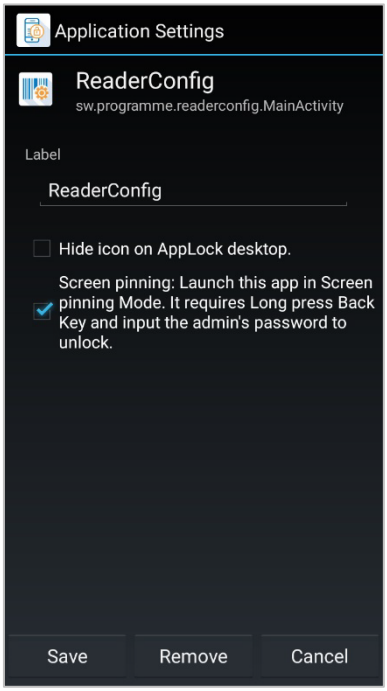


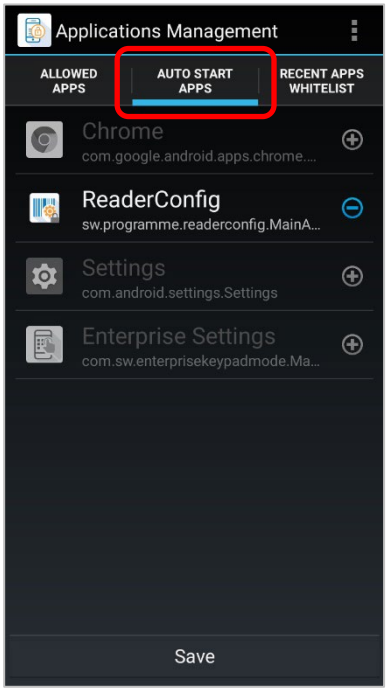
Note: Only the device with Android version 6.0 or later supports **Screen Pinning** function.

AUTO START APP WITH SCREEN PINNING ENABLED

To set a screen-pinned application to be auto started, follow the steps of Set Application as Auto Start Apps.

Please note that **ONLY ONE** application with "**Screen Pinning**" function enabled could be set to be auto started.

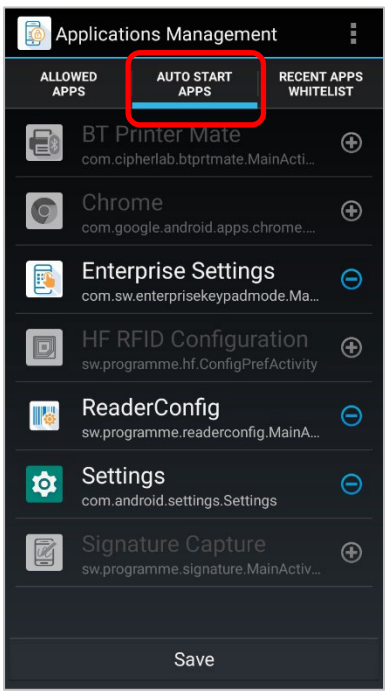


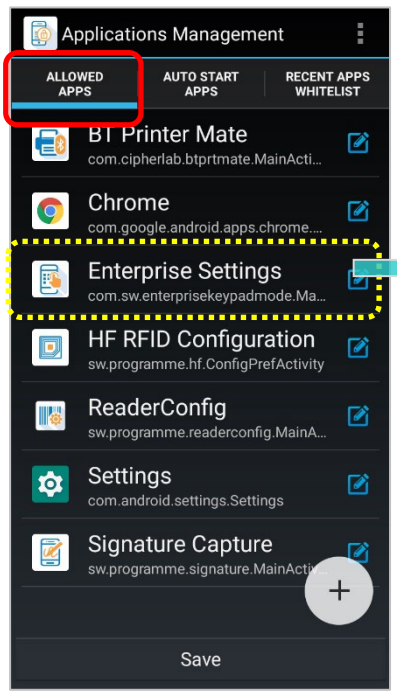


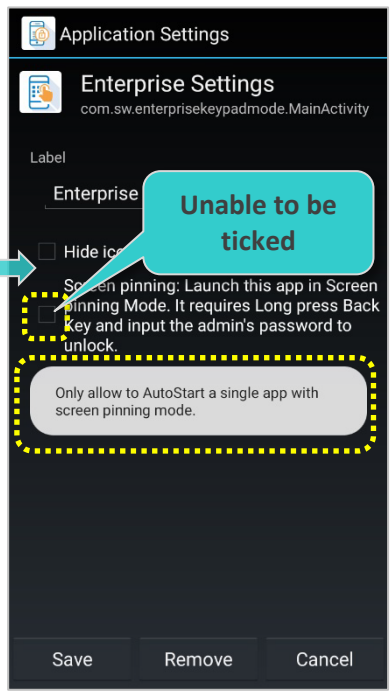
Under the circumstances listed below, no screen-pinned application could be set as Auto Start App:

WHEN THERE'S MORE THAN 1 AUTO START APP AND NO SCREEN-PINNED APPS:

No Auto Start Apps could be set to be screen-pinned application until all the Auto Start Apps are cleared, or to remain only one Auto Start App to be enabled screen pinning.

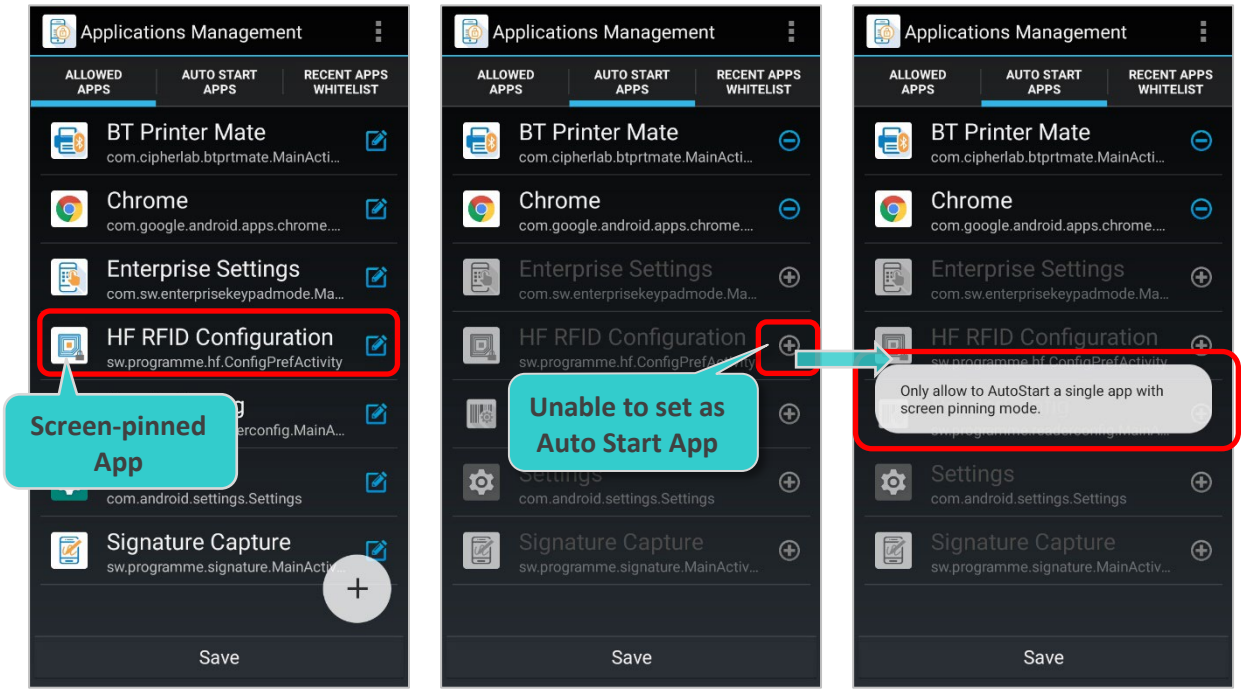






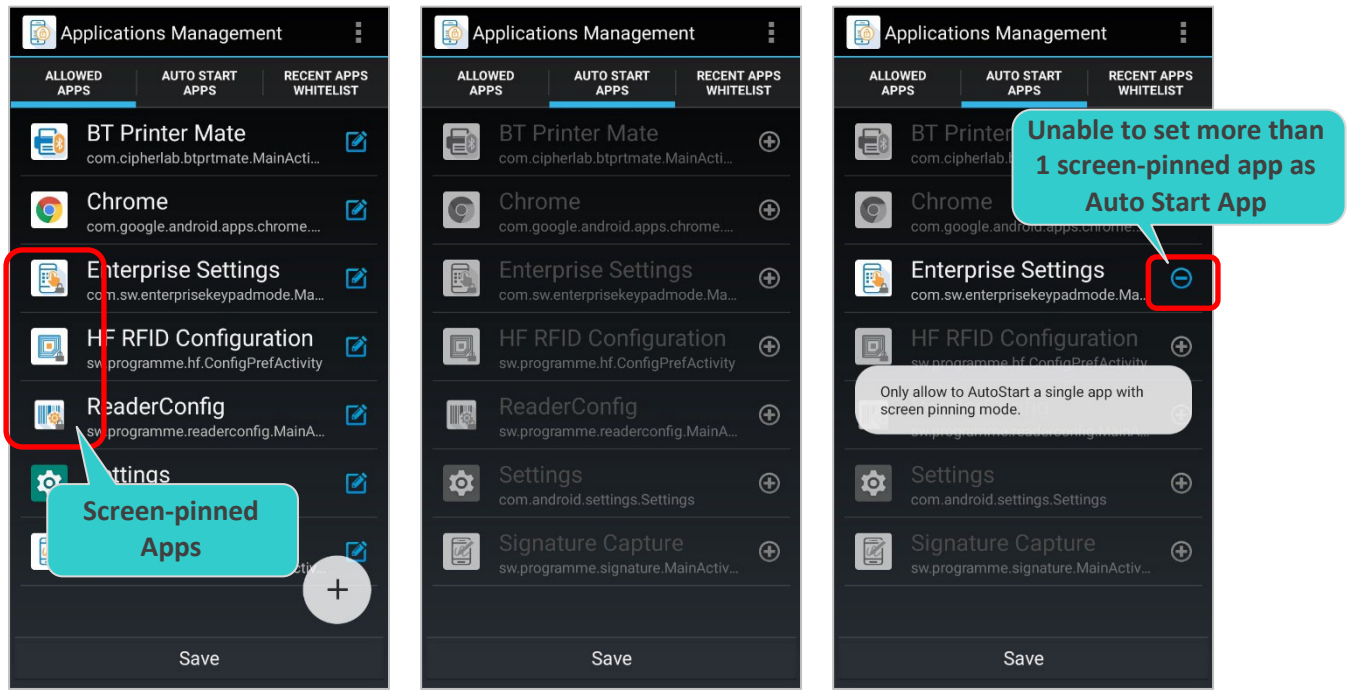
WHEN THERE'S AUTO START APP(S) WITHOUT SCREEN PINNING FUNCTION ENABLED:

No screen-pinned Apps could be set as Auto Start App until all the Auto Start Apps are cleared.



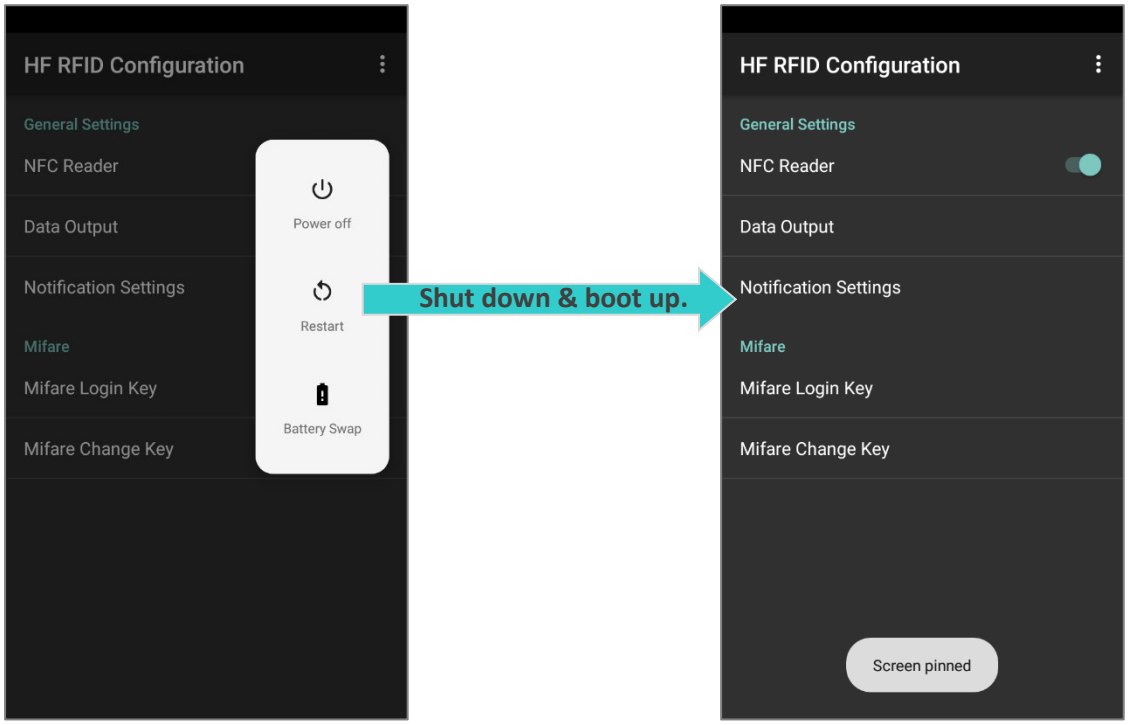
WHEN THERE'S MORE THAN 1 SCREEN-PINNED APP AND NO AUTO START APPS:

Only one screen-pinned App could be set as Auto Start App.



SHUT DOWN WHILE STAYING IN A SCREEN-PINNED APPLICATION

If the mobile computer is shut down while the screen stay in a screen-pinned application, next time the mobile computer is booted up, the screen will restore to the screen-pinned application even this screen-pinned application is not the Auto Stat App.

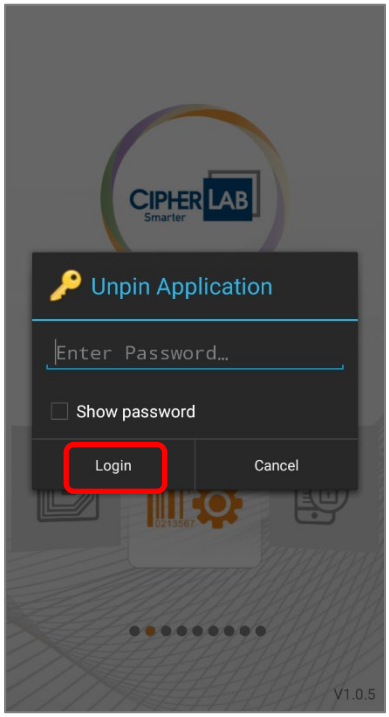


UNPIN AN APPLICATION

To unpin an application with **Screen Pinning** function enabled:

1) Long press **Back** button till a pop-up window appears.

2) Input the admin password in "**Unpin Application**" pop-up window, and tap "**Login**".



3) The application is now unpinned. Click **Back** button again to exit the application.

DISABLE THE SCREEN PINNING FUNCTION FOR AN APPLICATION

To disable "**Screen Pinning**" function for an application, please:

1) Enter Application Management → Allowed Apps tab page.

2) Click the screen-pinned application to enter its **Application Settings** page to untick the screen pinning function.

3) Save the settings.

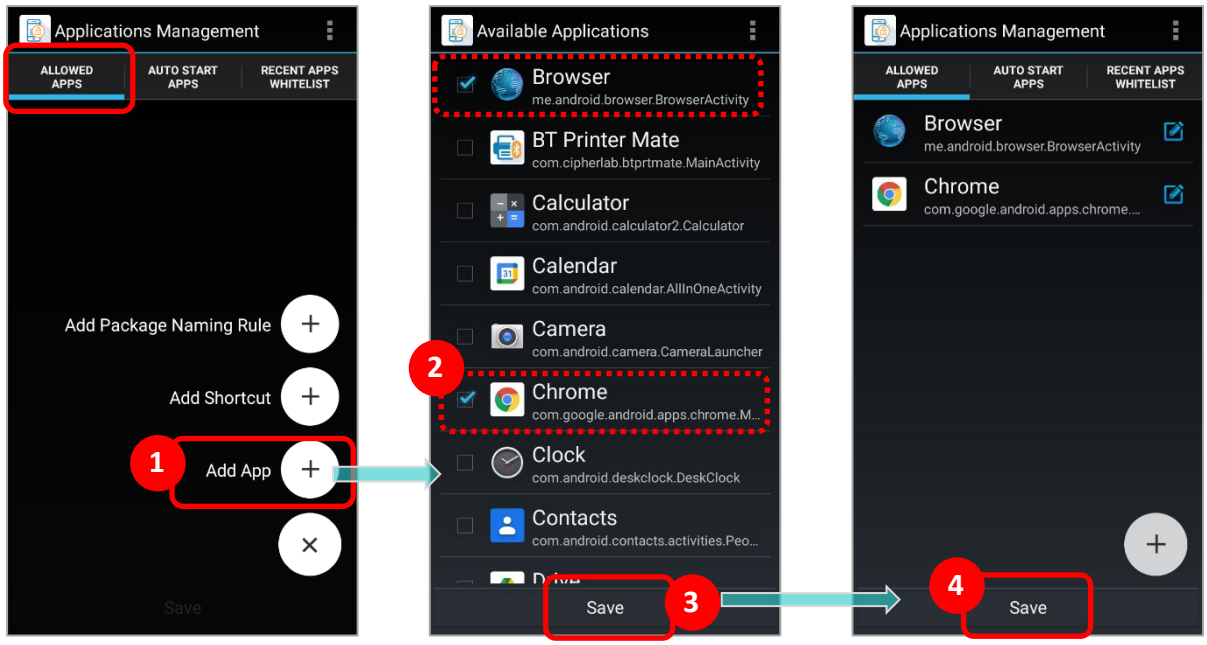
3.3.3 SITE PROTECTION

For **Android default browser** and **Chrome**, AppLock supports the function "**Site protection**" which could set certain sites as blacklist or whitelist for up to 32 URLs.

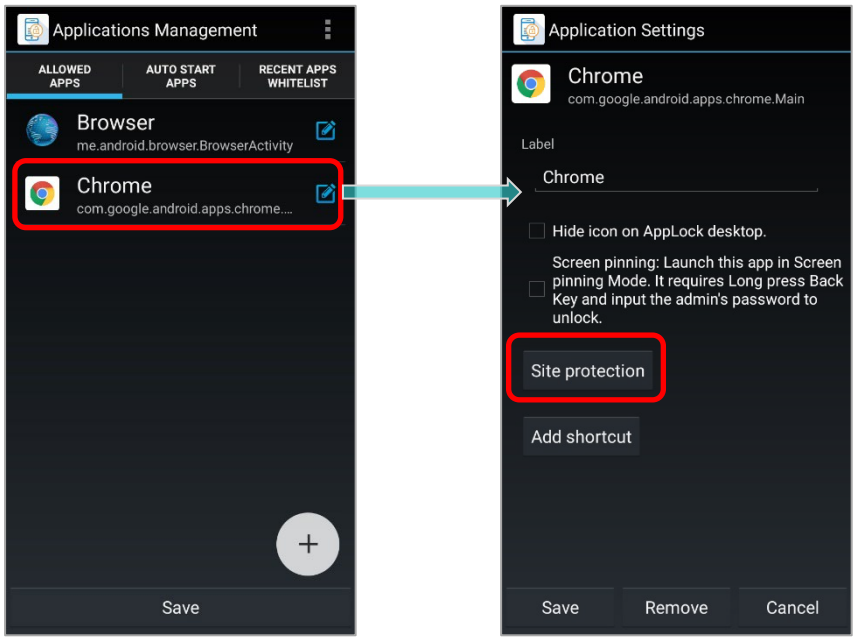
ENABLE SITE PROTECTION

To enable "**site protection**", please:

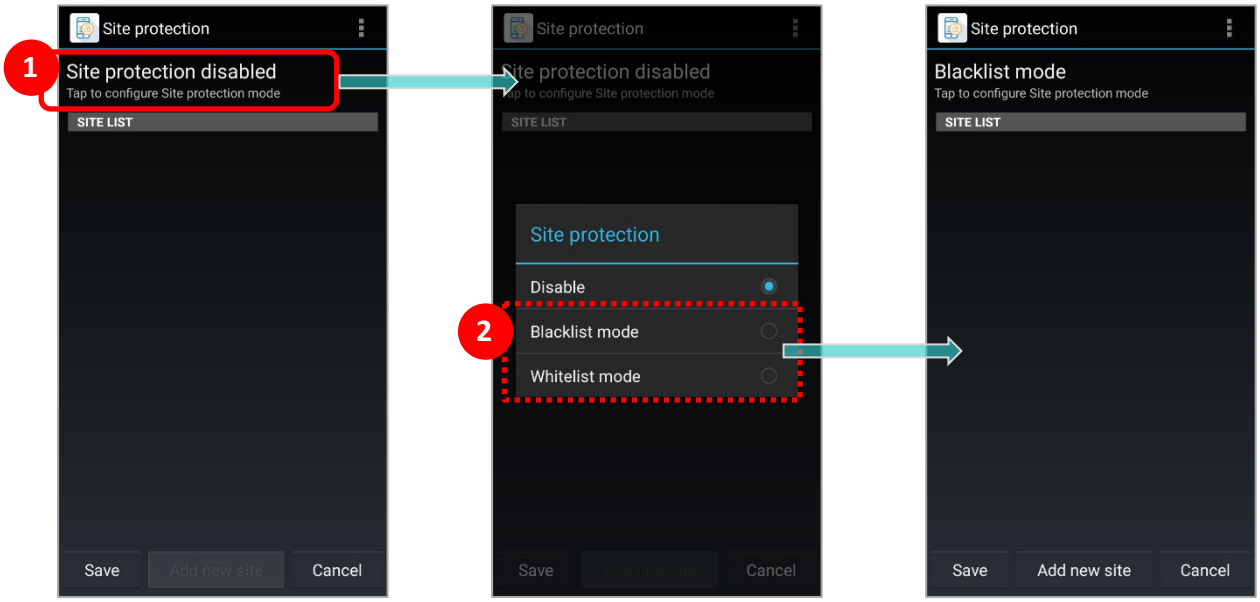
1) Login "**Admin Mode**" to enter **Applications Management** page. Tap "**Add App**" to add Android default browser/ Chrome to **Allowed Apps** list.



2) In "**Allowed Apps**" tab page of Applications Management, tap Android default browser/ Chrome to enter its **Application Settings** page, and then tap "**Site protection**".

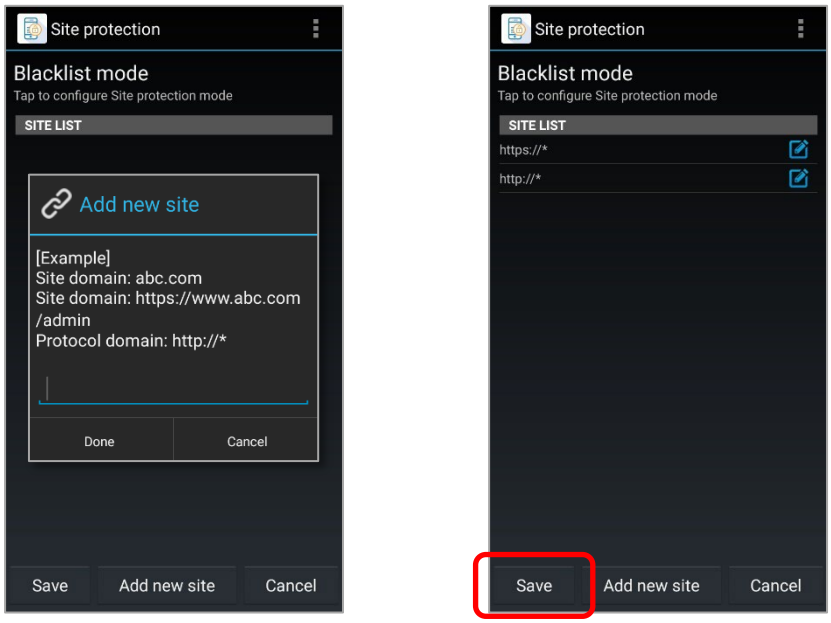


3) The default setting of **Site protection** is disabled. To enable site protection, tap "**Site protection disabled**" and select "**Blacklist mode**" or "**Whitelist mode**" in the popup window.



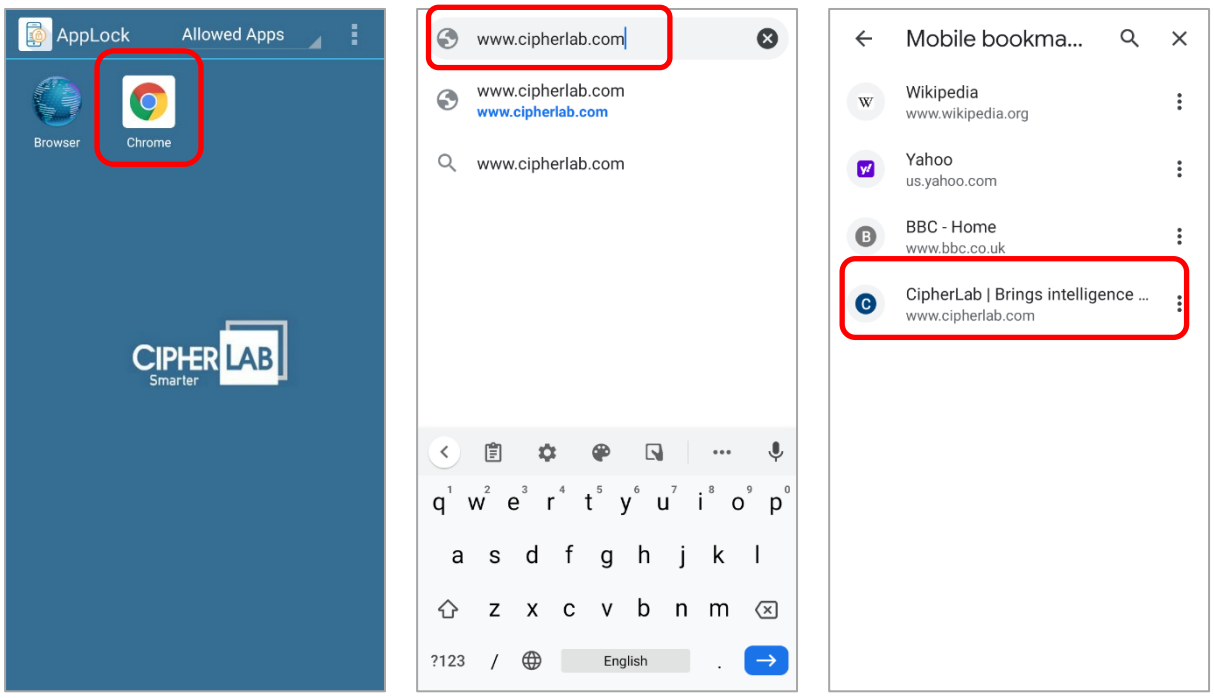
Setting	Description
Disable	The function "**Site protection**" is not enabled.
Blacklist mode	Those URLs on **Site List** are prohibited to be visited.
Whitelist mode	Only those URLs on **Site List** are permitted to be visited.

4) Tap "**Add new site**" in the bottom of the screen to enter URL as blacklist or whitelist. Make sure to "**Save**" before leaving **Site protection** and other previous pages to make the settings take effect.



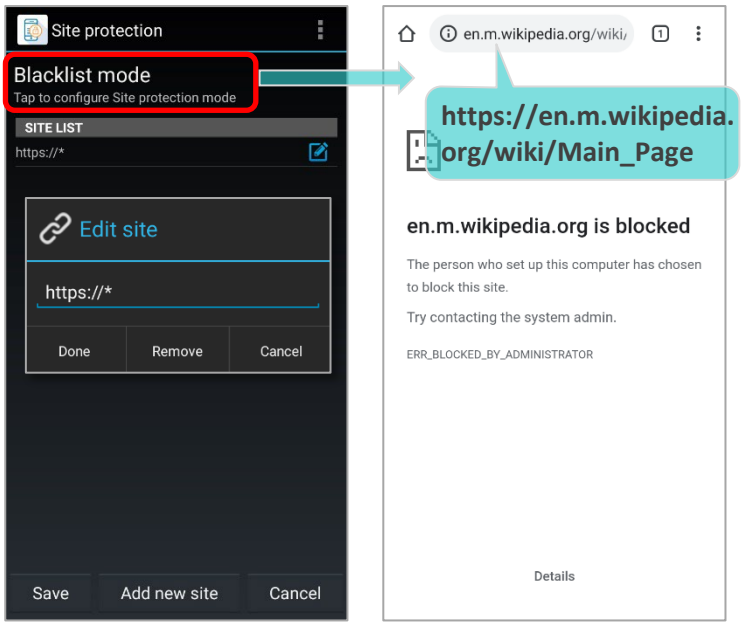
LAUNCH ANDROID DEFAULT BROWSER/ CHROME WITH SITE PEOTECTION ENABLED

On AppLock main screen (no matter in Admin mode or User mode), tap Android default browser or Chrome to launch it, and input the web address directly or select the website from your bookmark.

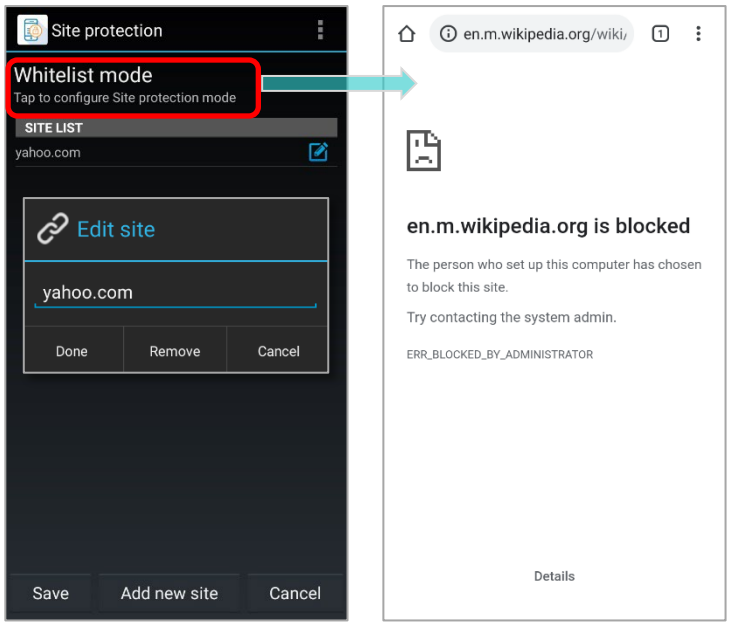


The webpage is blocked if it is on **Site List** in **Blacklist mode**, or if it is excluded from **Site List** in the **Whitelist mode**.

Blacklist Mode



Whitelist Mode

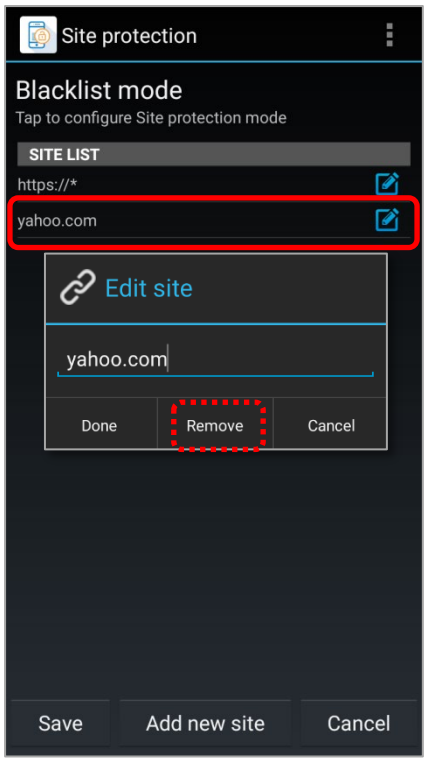


REMOVE URL FROM SITE LIST

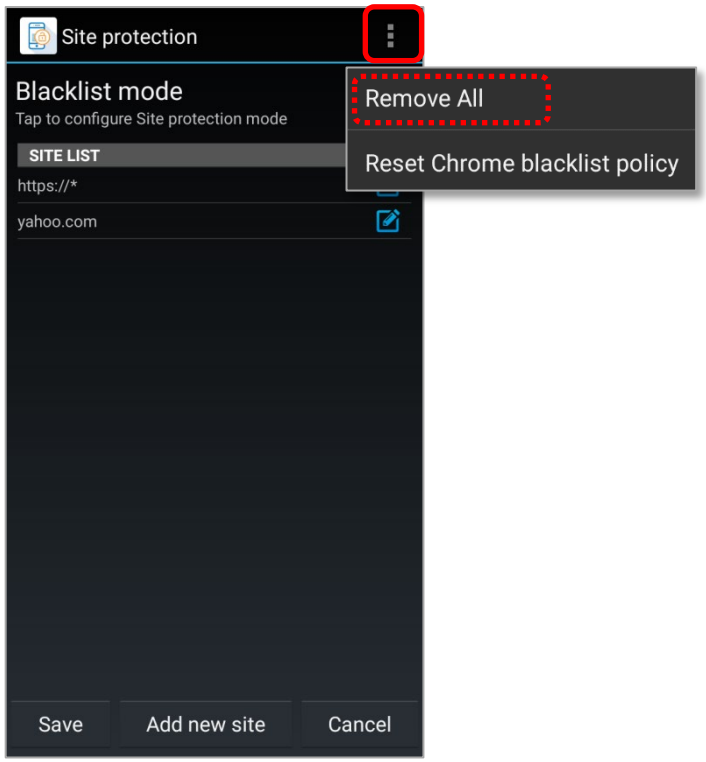
To move a certain URL from Site List, please tap on the Edit icon or the URL directly in **Site protection** page to open the "**Edit site**" window and select "**Remove**".

To remove all URLs on **Site List** at once, please tap the menu icon at the top right corner of Site protection page, and tap "**Remove All**".

Remove one URL



Remove All URL



Be sure to "**Save**" before leaving **Site protection** and other previous pages.

ADD NEW SITE

Administrator can add up to 32 URLs to "**Site List**", and all the URLs listed on **Site List** will be either on **Blacklist** or **Whitelist** depending on the mode you select for **Site protection**.

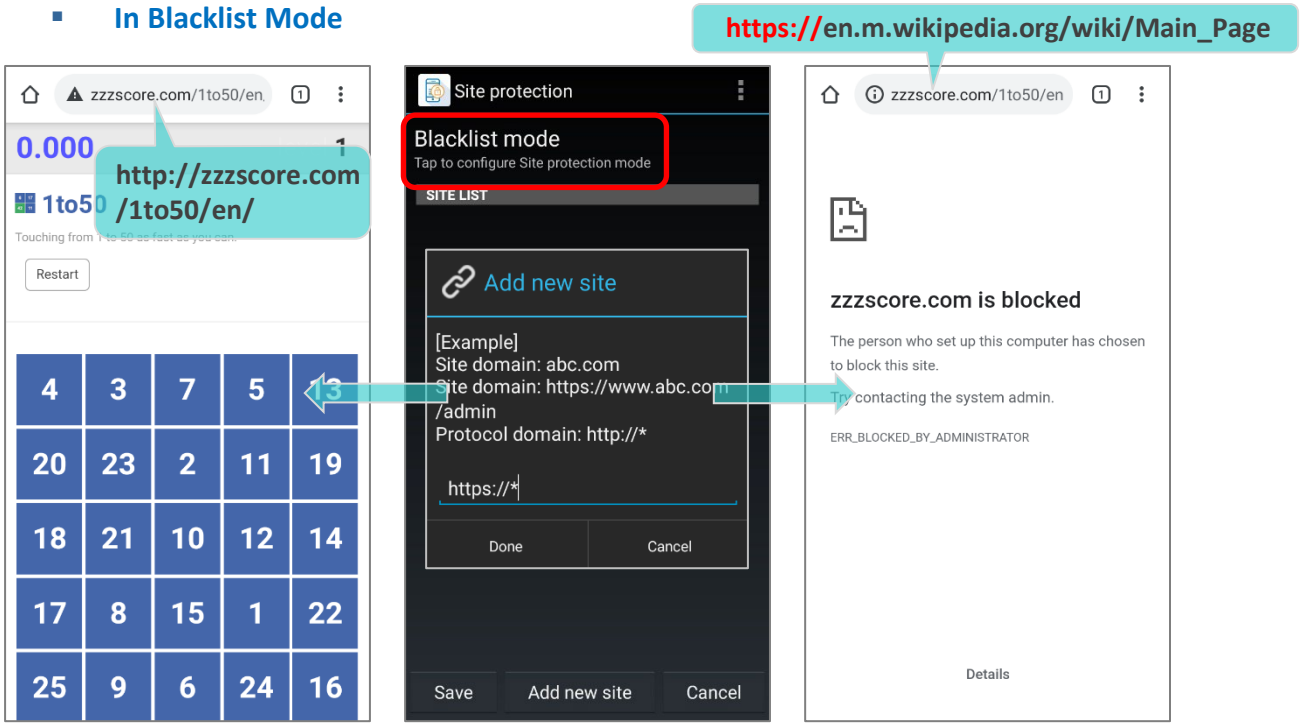
In Site protection page, tap "**Add new site**" and input URL in the popup window. Tap **Done** and then "**Save**" in every page before returning back to the main page.

The examples of the valid URL to be added are as below:

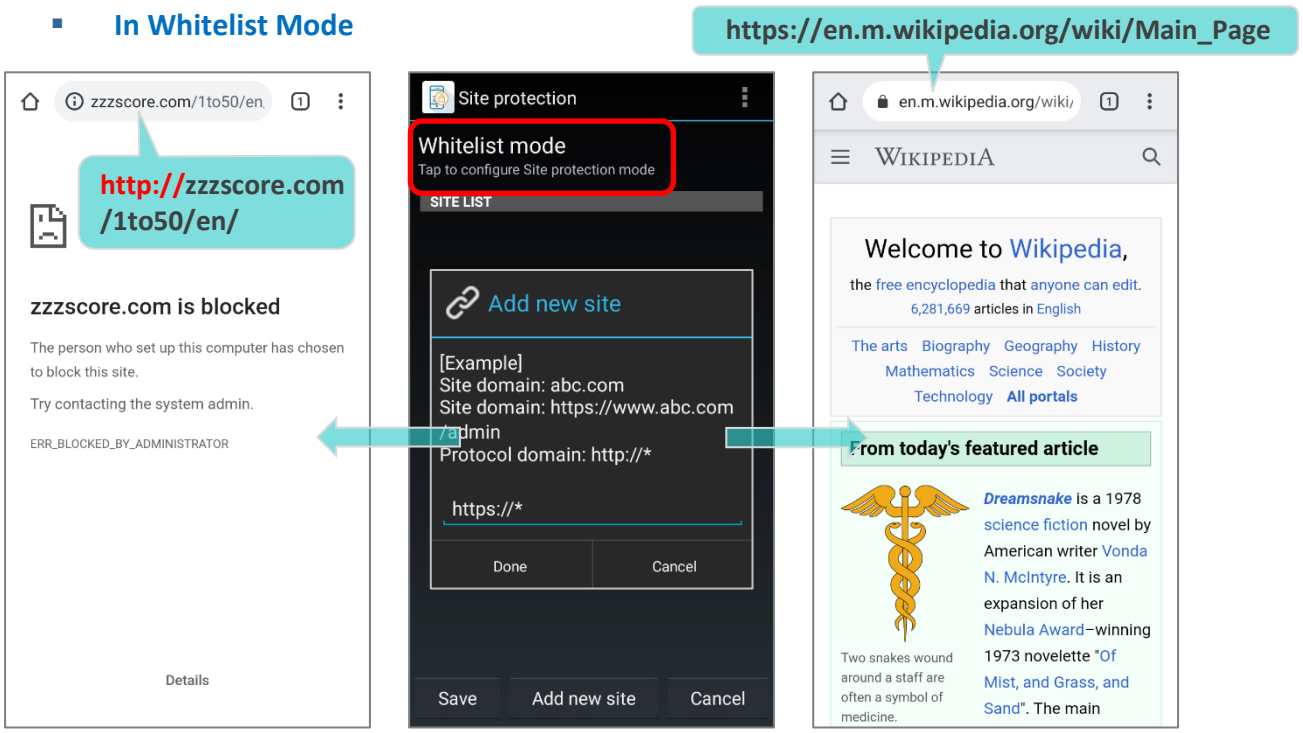
1) Input the protocol and an asterisk, e.g. http://* or https://*

   All the webpages start with protocol "**http://**" or "**https://**"would never be visited in **Blacklist** mode whereas no webpage could be visited except of those starts with "**http://**" or "**https://**" in **Whitelist** mode.

- **In Blacklist Mode**



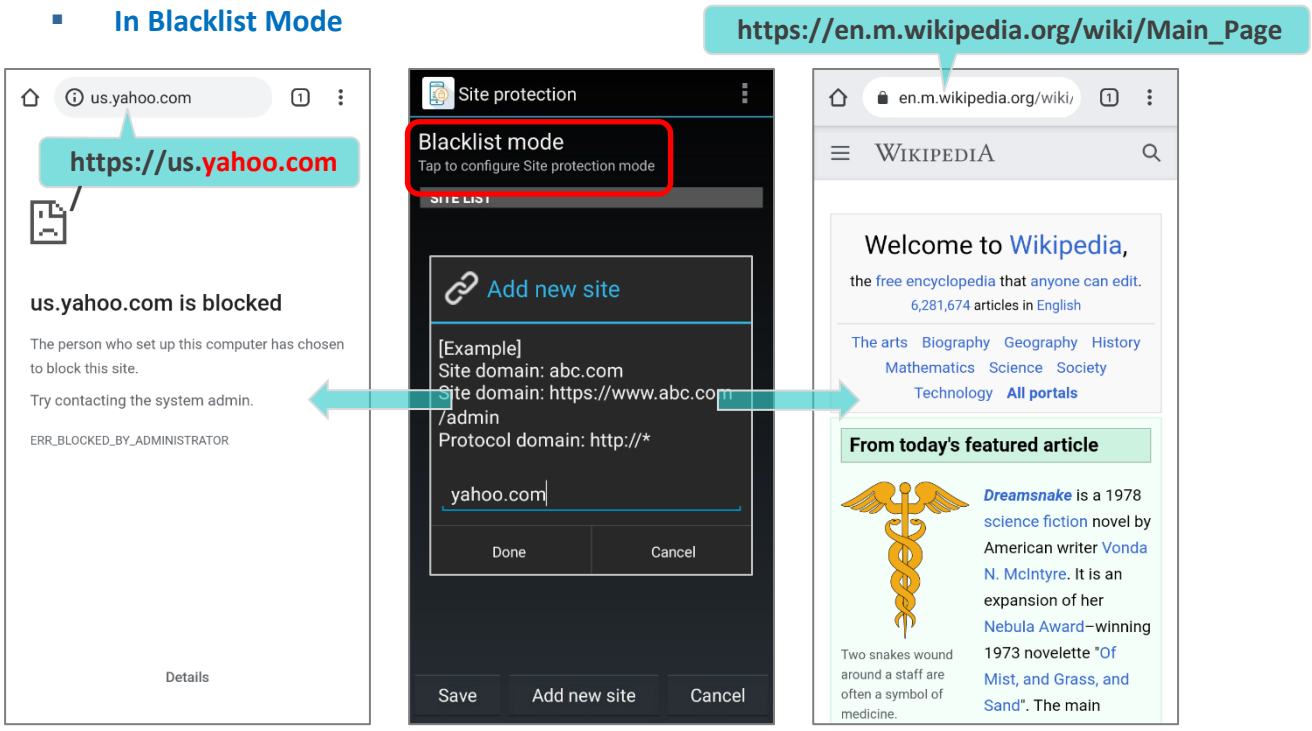
- **In Whitelist Mode**



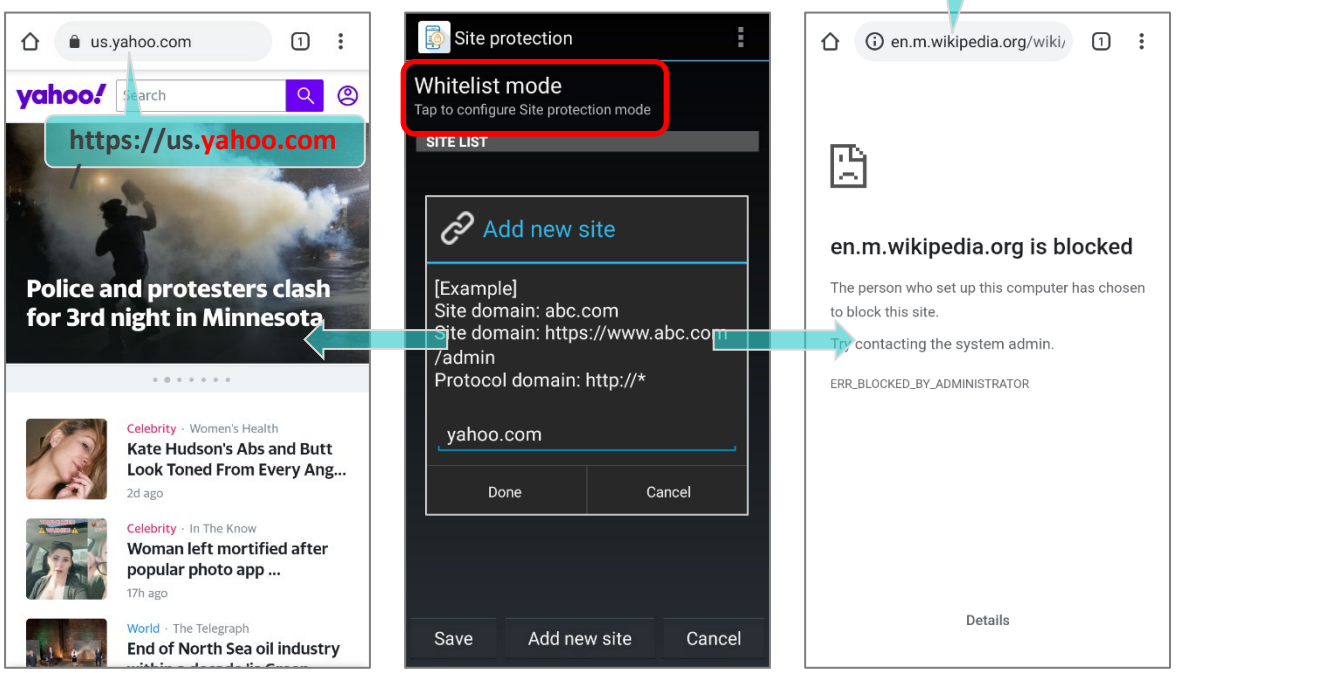
2) Input the domain name, e.g. yahoo.com

All the webpages with the domain name "**yahoo.com**" would never be visited in **Blacklist** mode whereas no webpage could be visited except of those with the domain name "**yahoo.com**" in **Whitelist** mode.

- **In Blacklist Mode**



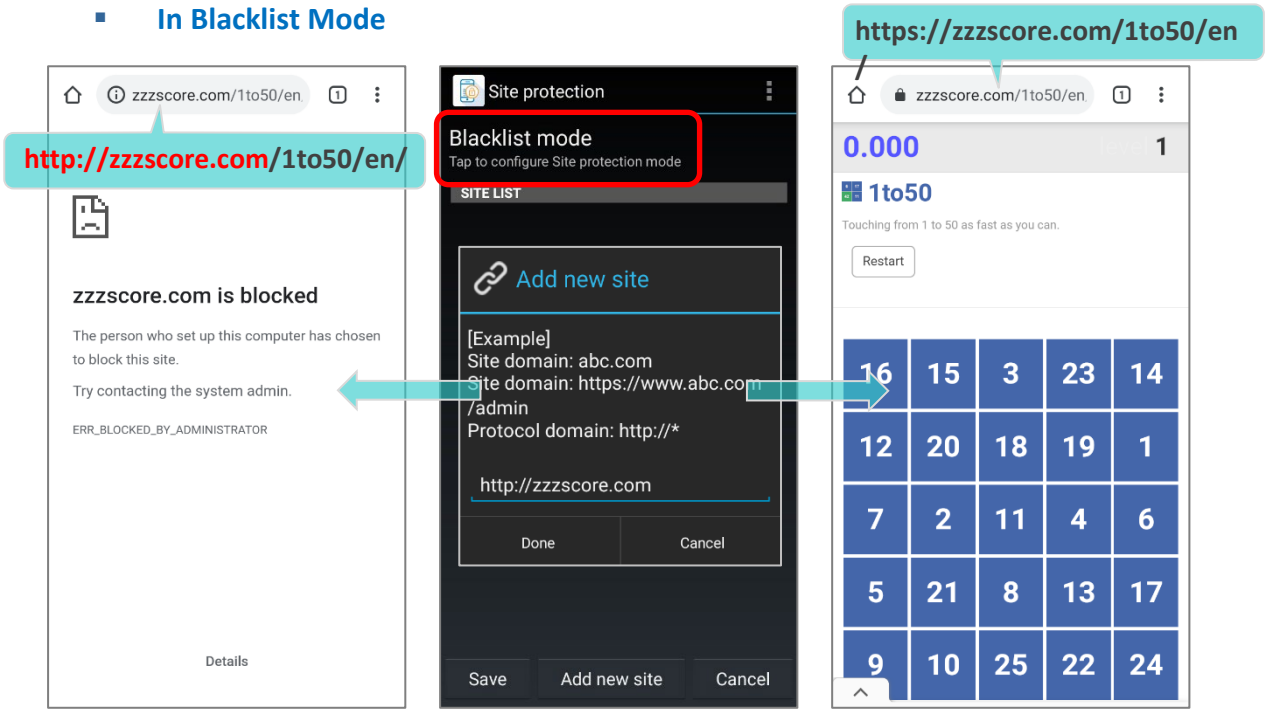
- **In Whitelist Mode**



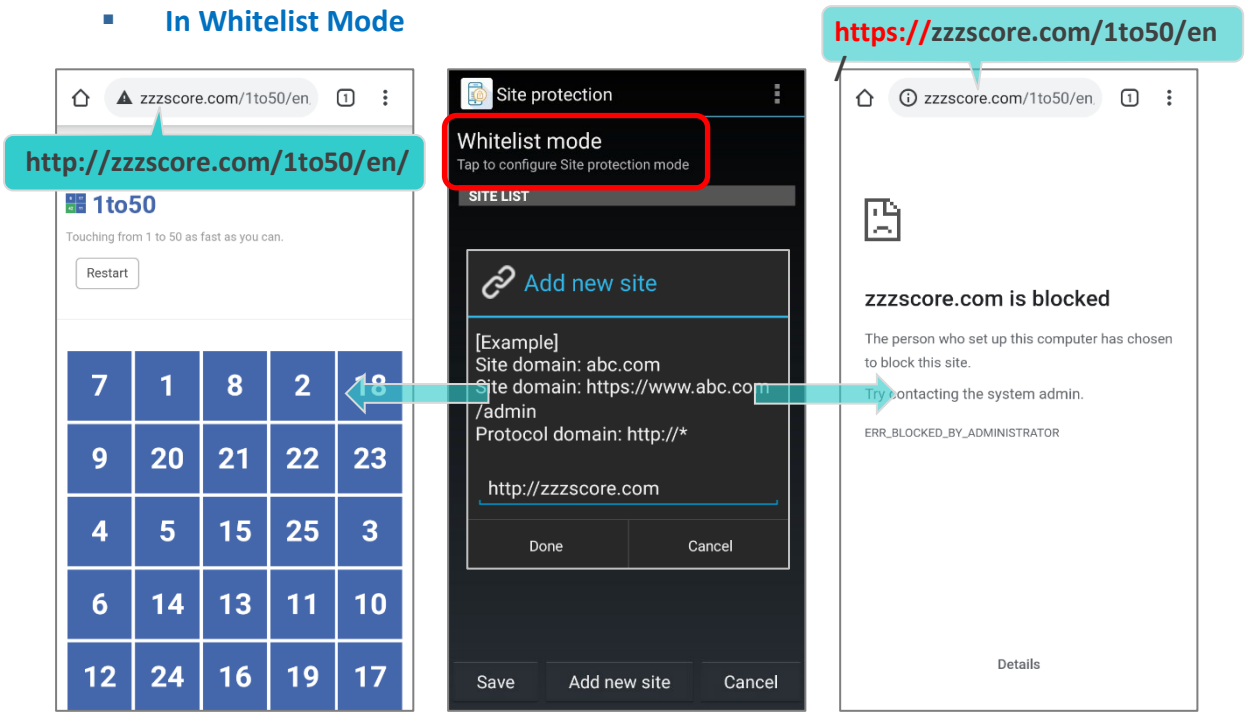
3) Input the protocol and the domain name , e.g. http://zzzscore.com

All the webpages with both the protocol "**http://**" and the domain name "**zzzscore.com**" would never be visited in **Blacklist** mode whereas no webpage could be visited except of those with both the protocol "**http://**" and the domain name "**zzzscore.com**" in **Whitelist** mode.

- **In Blacklist Mode**



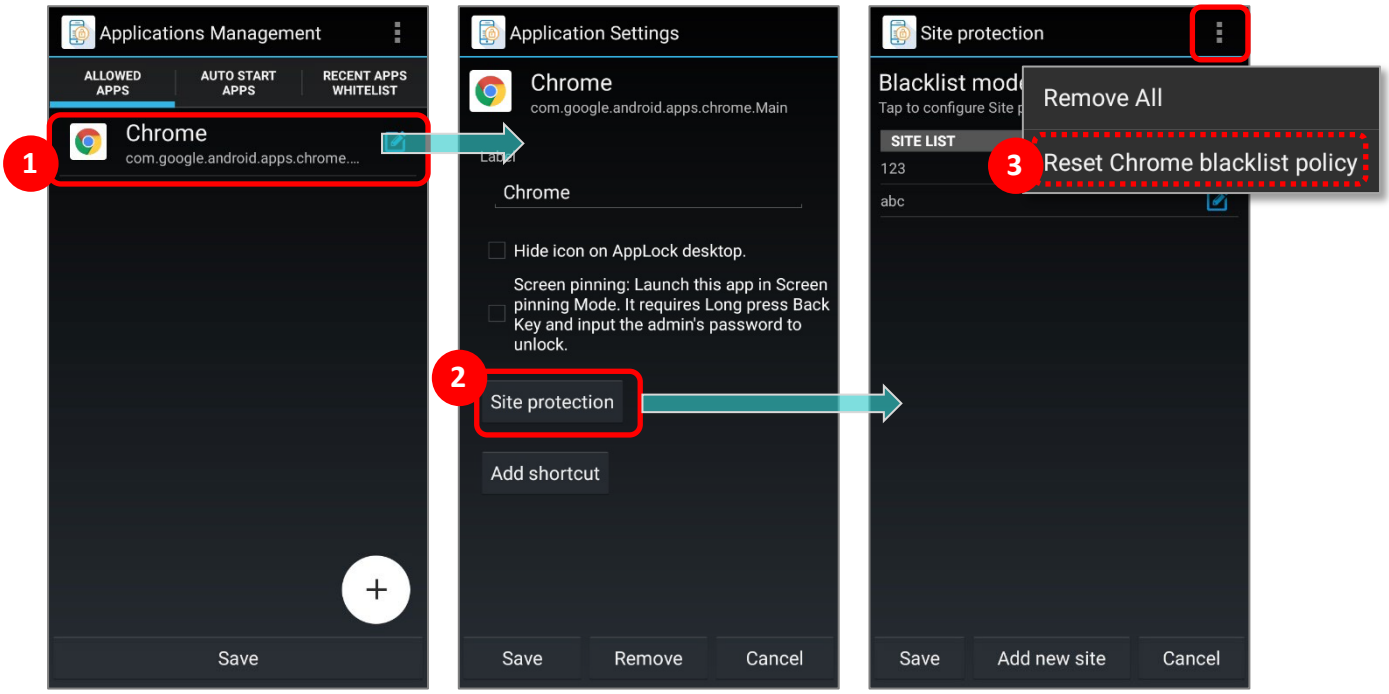
- **In Whitelist Mode**



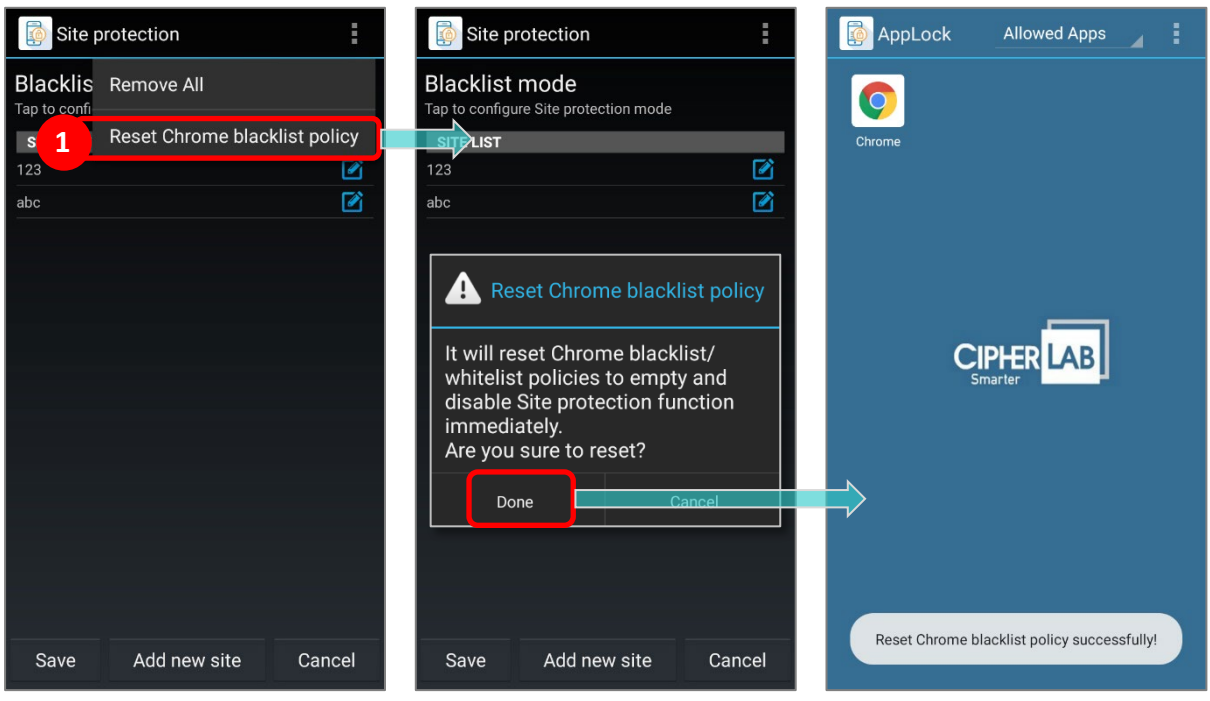
Note: If both **Android default browser** and **Chrome** are installed in the device, the setting of **Site protection** and **Site List** works for both of them.

RESET CHROME BLACKLIST POLICY

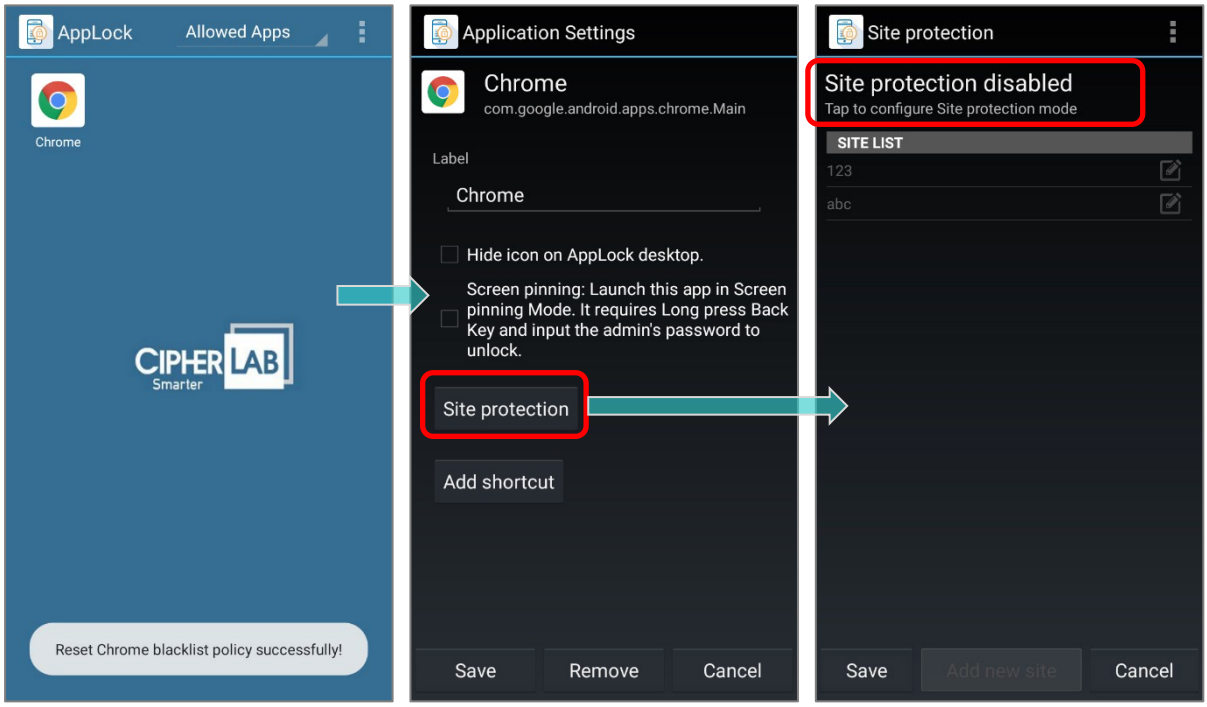
"**Reset Chrome blacklist policy**" is to disable "**Site protection**" and clear the **URLBlacklist/ URLWhitelist** of Chrome Ploicies to avoid the inconsistent policy settings between **AppLock** and **Chrome**.



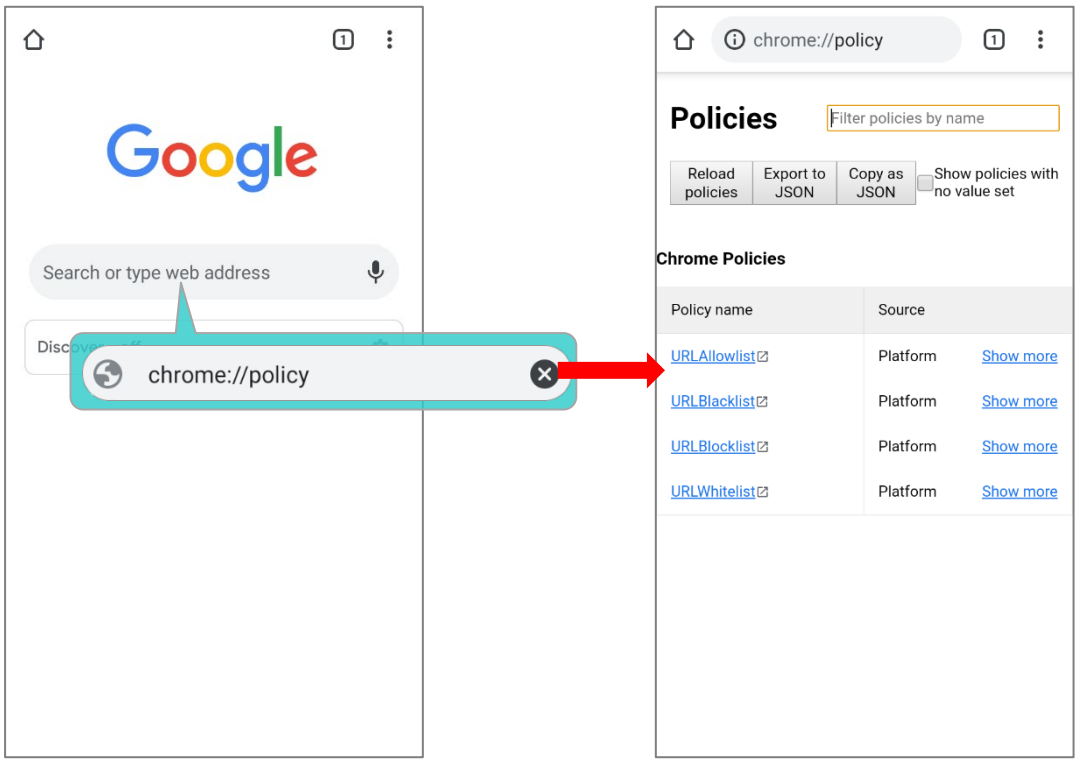
Please tap on the menu icon ⋮ at the top right corner of **Site protection** page, and select "**Reset Chrome blacklist policy**". Confirm deleting by tapping on "**Done**", and you will jump to AppLock main screen with a toast message "**Reset Chrome blacklist policy successfully!**" shown on it.



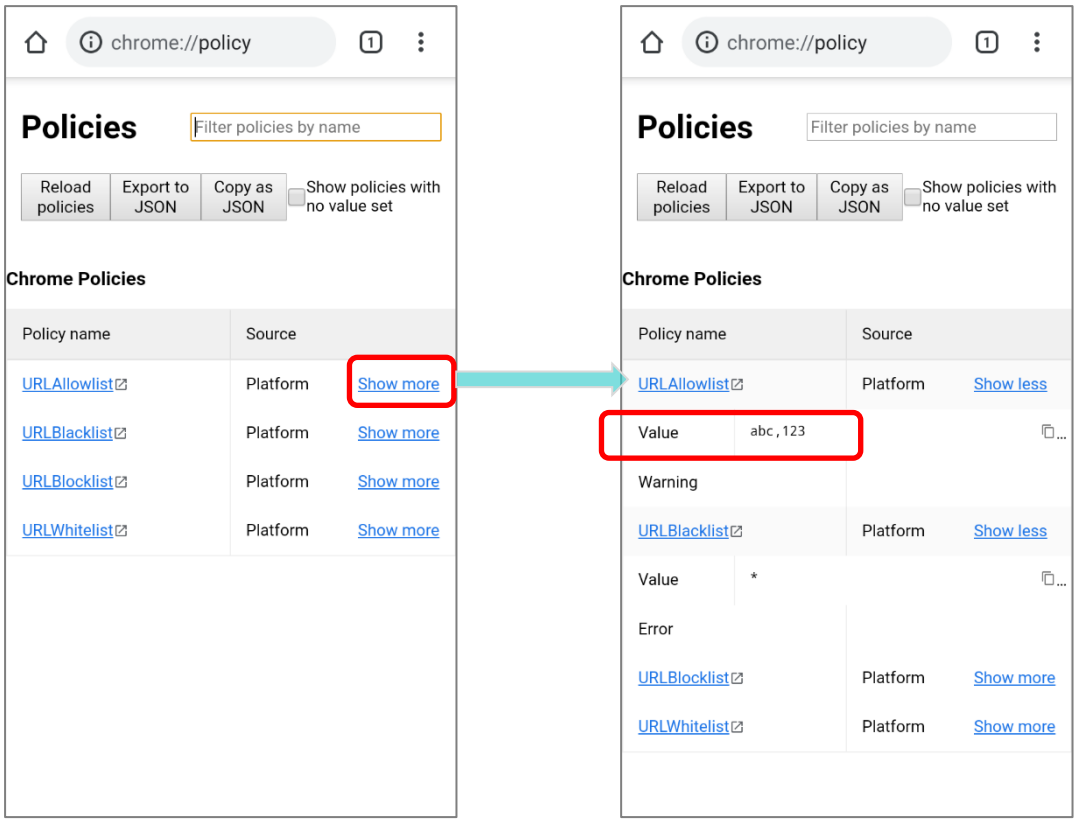
"**Site protection**" is now disable. Meanwhile, **URLBlacklist/ URLWhitelist** of Chrome Ploicies are cleared as well.



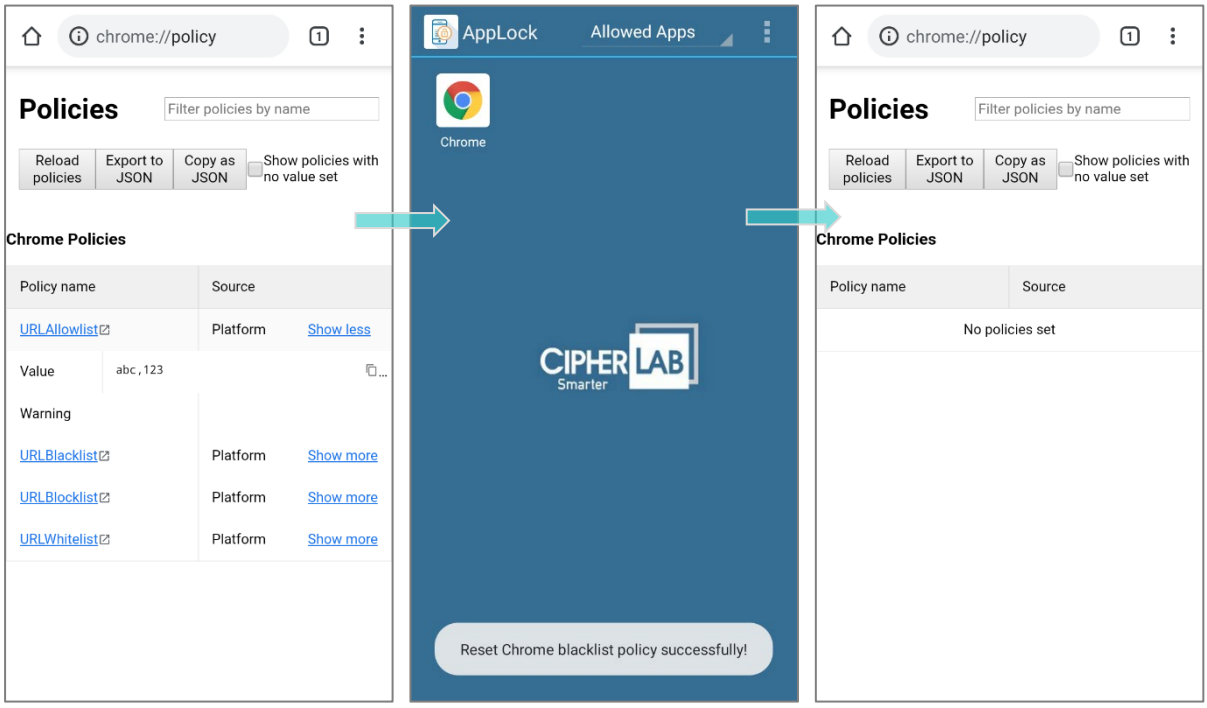
To check Chrome policy, please launch the app "**Chrome**" and input "**Chrome://policy**" into URL bar to enter **Policies** page to check your Chrome Policies.



Tap on “**Show more**” to check “**Value**” which shows the policies (URLs) you set on “**Site List**”.



Chrome policies are cleared after “**Reset Chrome blacklist policy**” is executed.

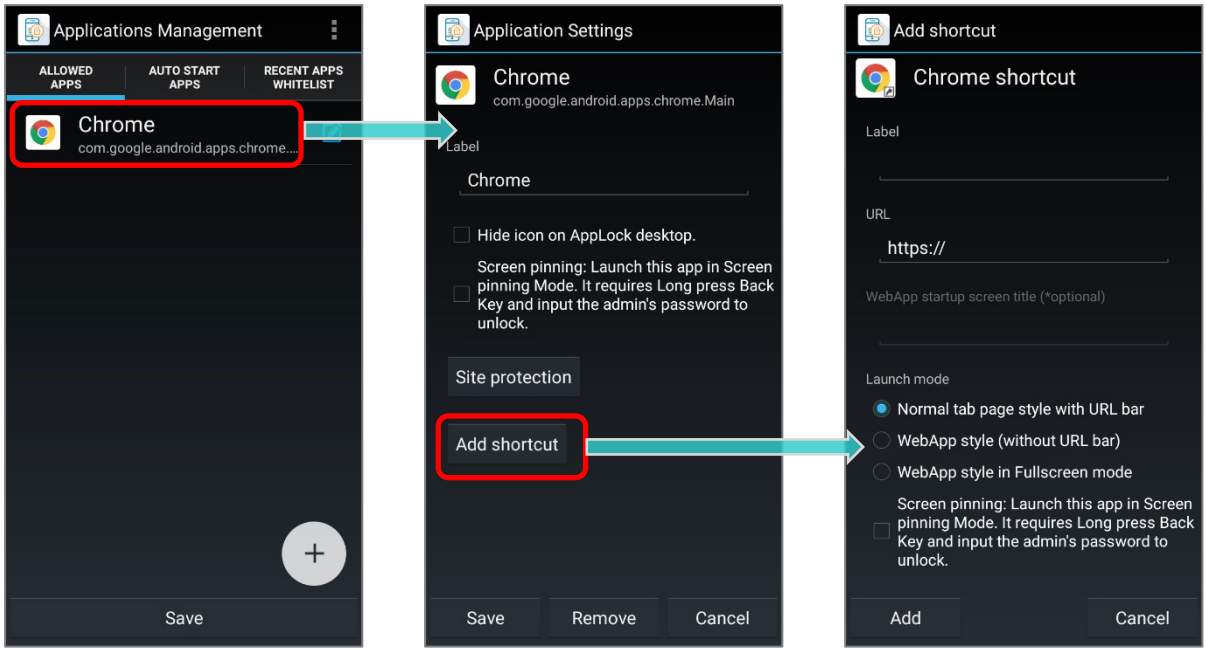


3.3.4 CHROME SHORTCUT

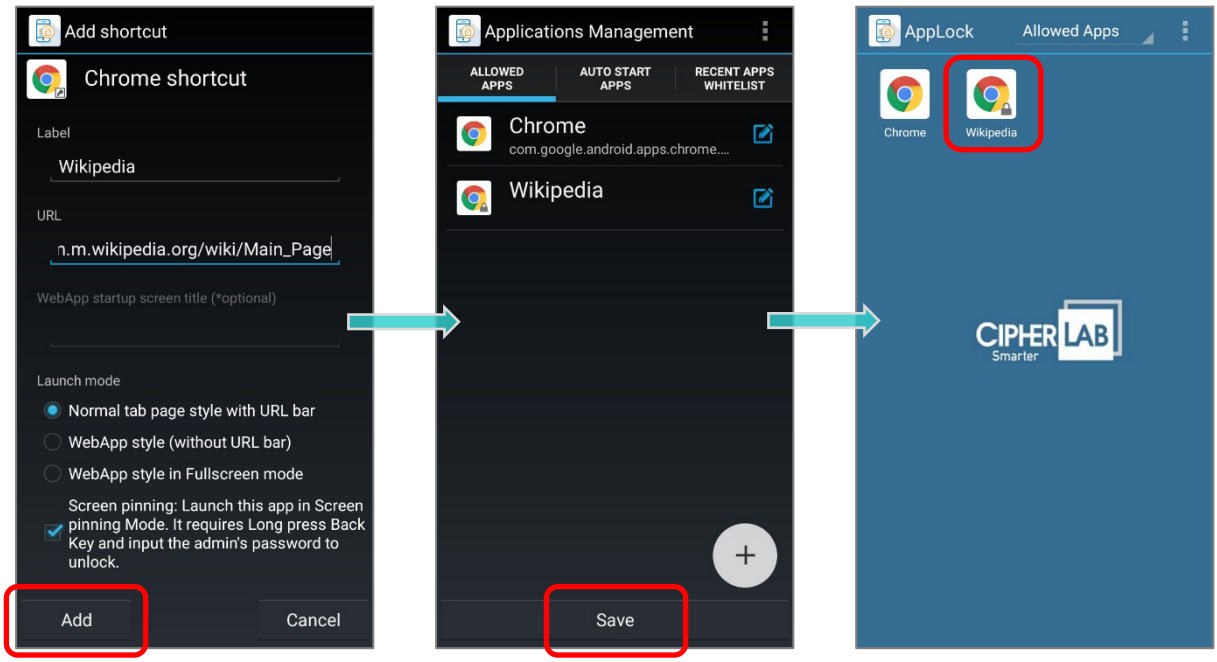
For the application "**Chrome**", you can add website shortcut to the main screen by "**Add shortcut**". To add website shortcut to the main screen:

1) Add Chrome to **Allowed Apps** list as the steps in "Add Application" describes.

2) On "**Allowed Apps**" list, tap on "**Chrome**" to enter its Application Settings page, and then tap on "**Add shortcut**" .



3) Fill in the necessaey fileds, select the "**Launch Mode**", decide whether to enable screen pinning for this Chrome shortcut, and finally tap on "**Add**" button.
Make sure to save your changed settings before leaving Application Management page.



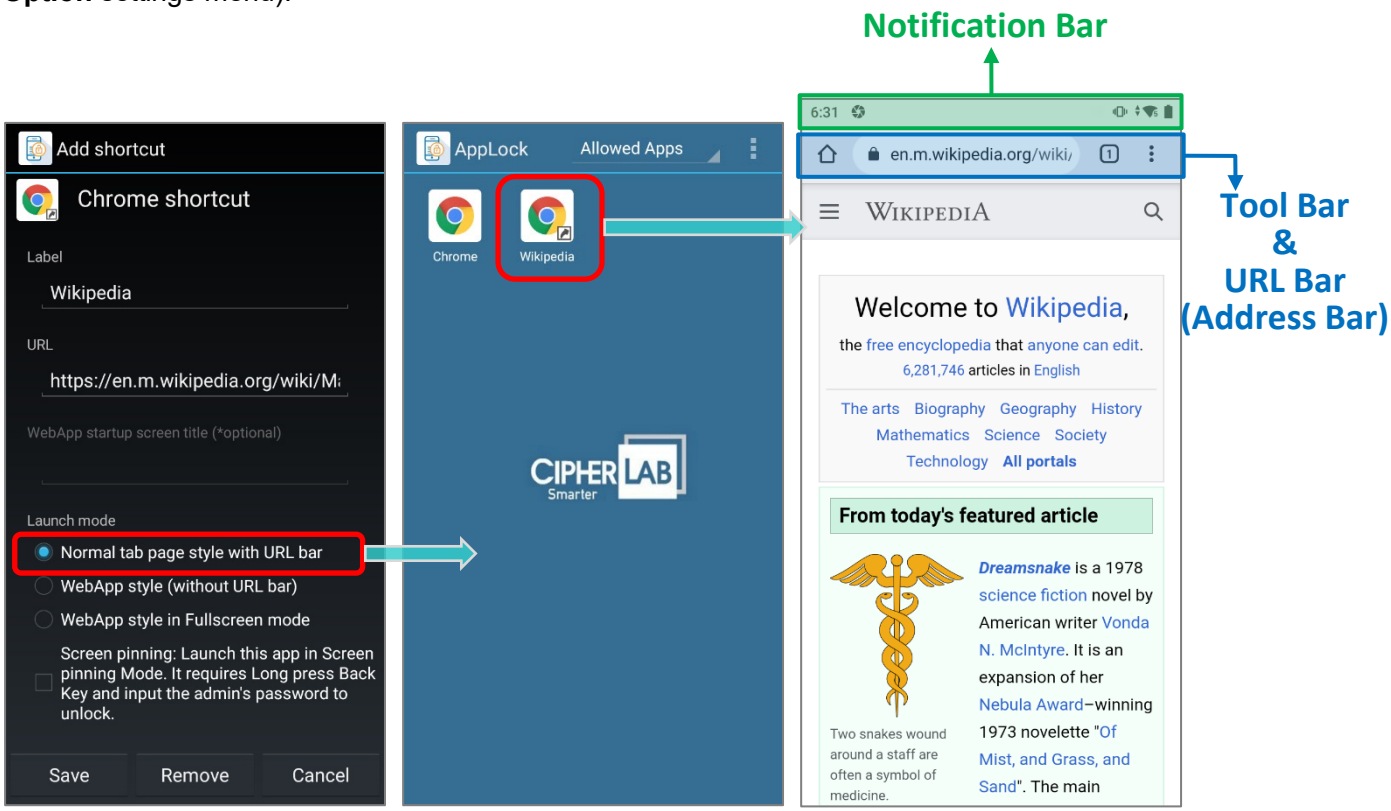
Item	Description
Label	The title you would like to name for this webpage, and it will be displayed below this Chrome shorcut icon on AppLock main screen.
URL	The address of the webpage to be set as a shortcut.
WebApp startup screen title	By selecting "**WebApp Style (without URL bar)**" or "**WebApp Style in Fullscreen mode**", you can further set WebApp startup screen title which will be shown on the startup screen when you launch this Chrome shortcut. Please refer to "WebApp startup screen title" for details.
Launch Mode	The mode of the webpage to be displayed.
Screen pinning	Once screen pinning is enabled, users have to enter the login password to exit this Chrome shortcut.

LAUNCH MODE

Launch Mode is to set the way the webpage appears. The available modes to be set are:

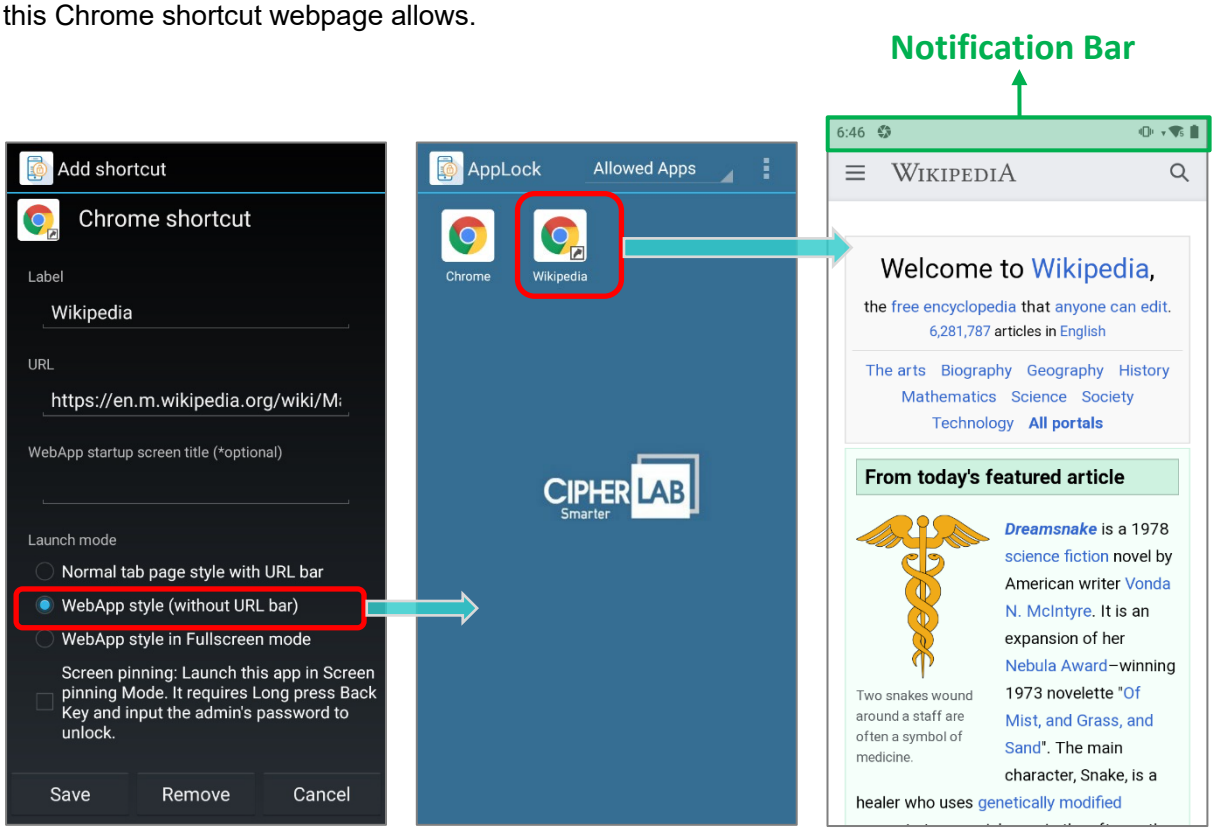
NORMAL TAB PAGE STYLE WITH URL BAR

The Chrome shortcut webpage is displayed as a default Chrome tab page which allows **tool bar**, **URL bar**, and **notification bar** to be shown (even you disable "**Show Notification Bar**" from **Option** settings menu).



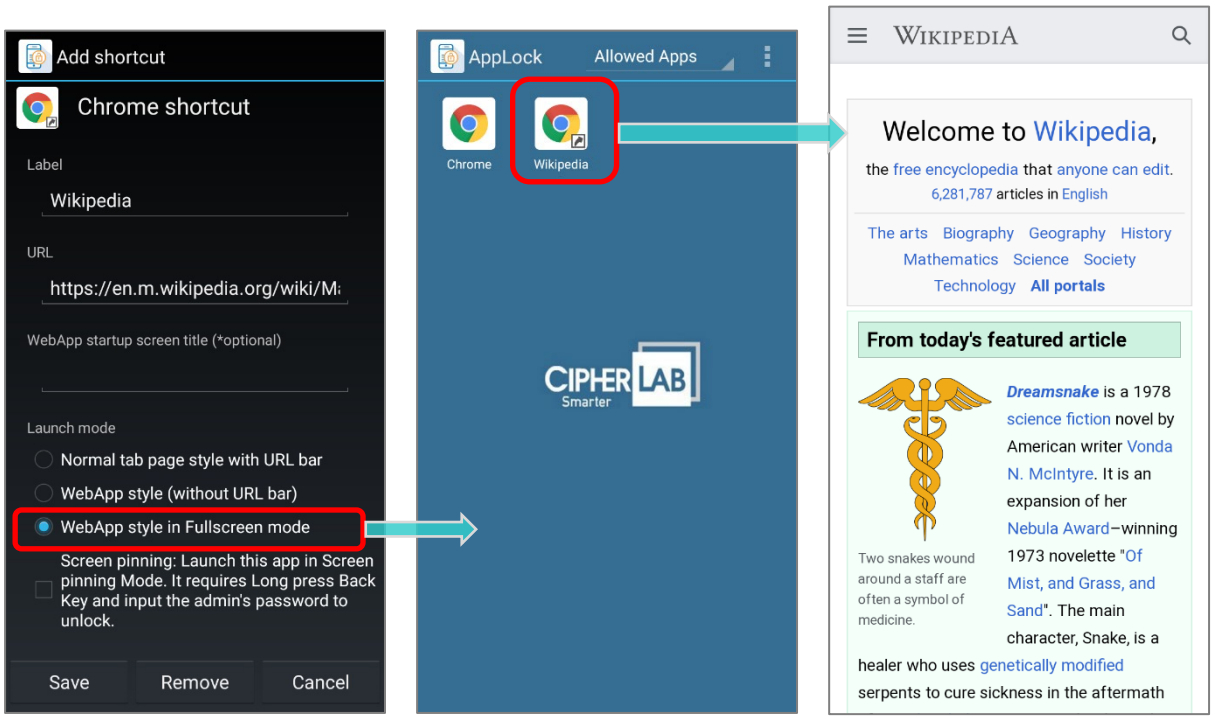
WEBAPP STYLE (WITHOUT URL BAR)

Only notification bar is displayed (even "**Show Notification Bar**" is disabled), and there's no URL bar for users to manually input web address. Thus users cannot access other websites other than this Chrome shortcut webpage allows.



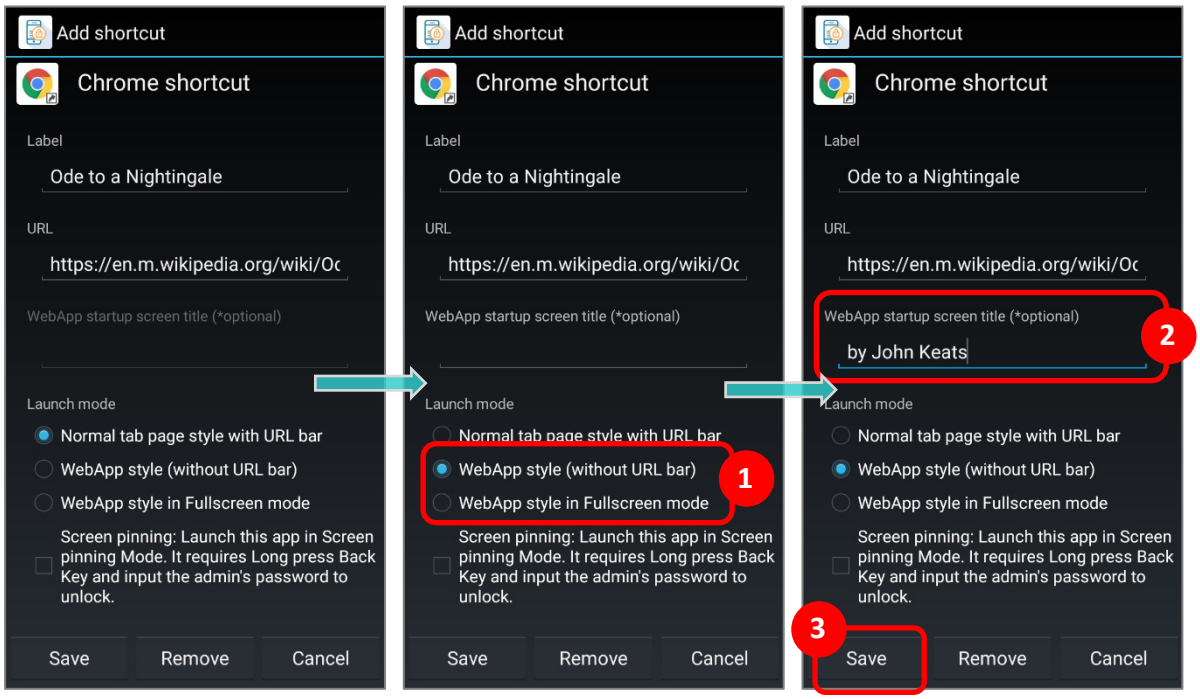
WEBAPP STYLE IN FULLSCREEN MODE

Neither notification bar nor toolbar & URL bar are displayed.

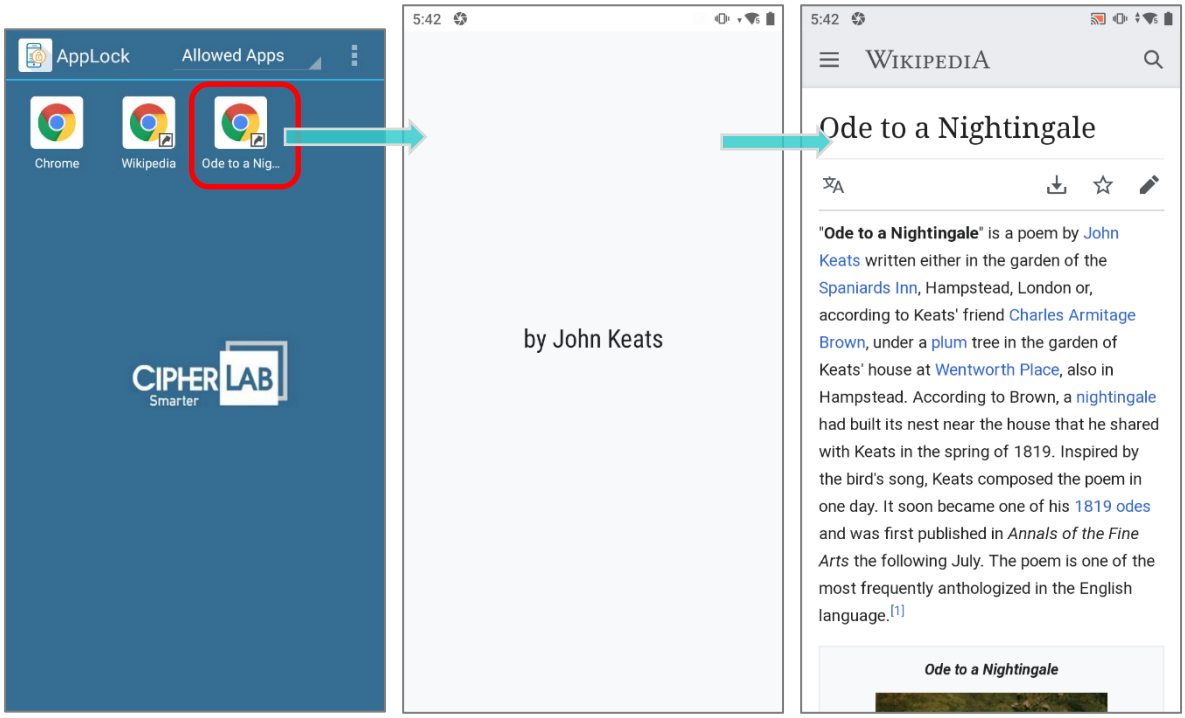


WEBAPP STARTUP SCREEN TITLE

"**WebApp startup screen screen title**" is only available when **Launch Mode** is set to be "**WebApp Style (without URL bar)**" or "**WebApp Style in Fullscreen mode**".

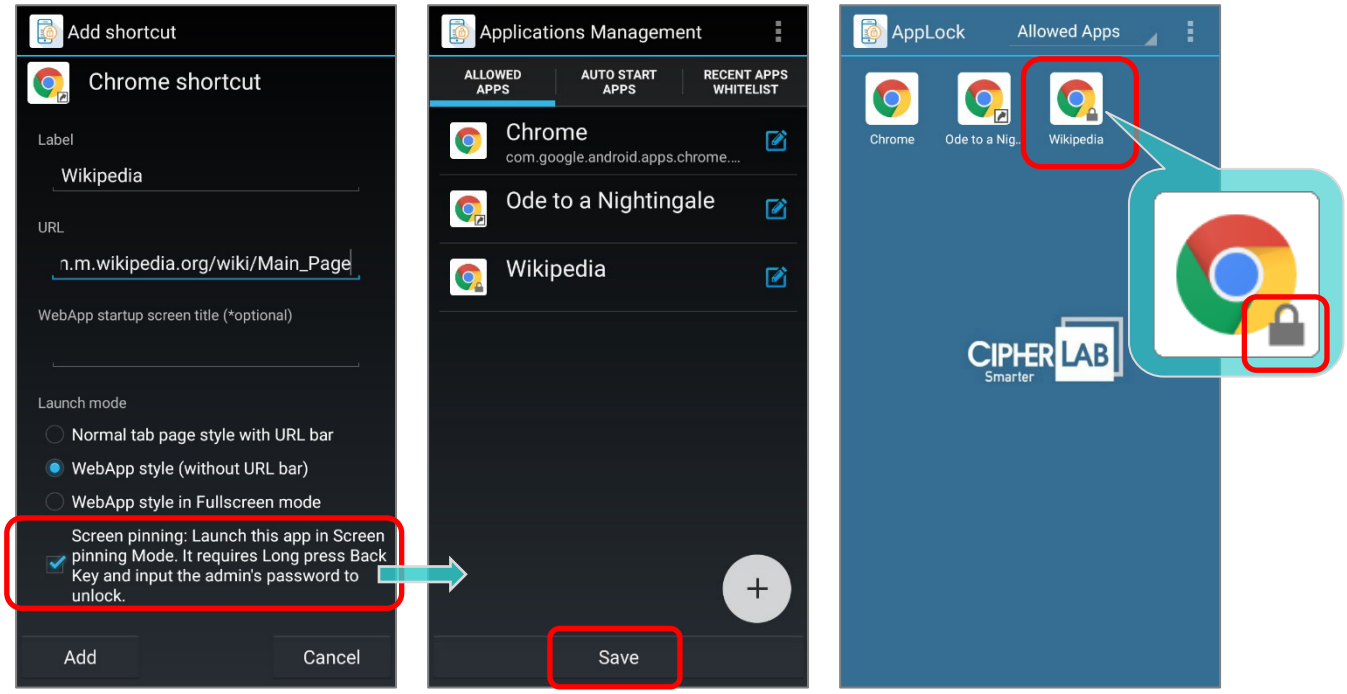


Once this Chrome shortcut is launched, the content you input into "**WebApp startup screen screen title**" field will be displayed on the on the startup screen before entering the webpage.

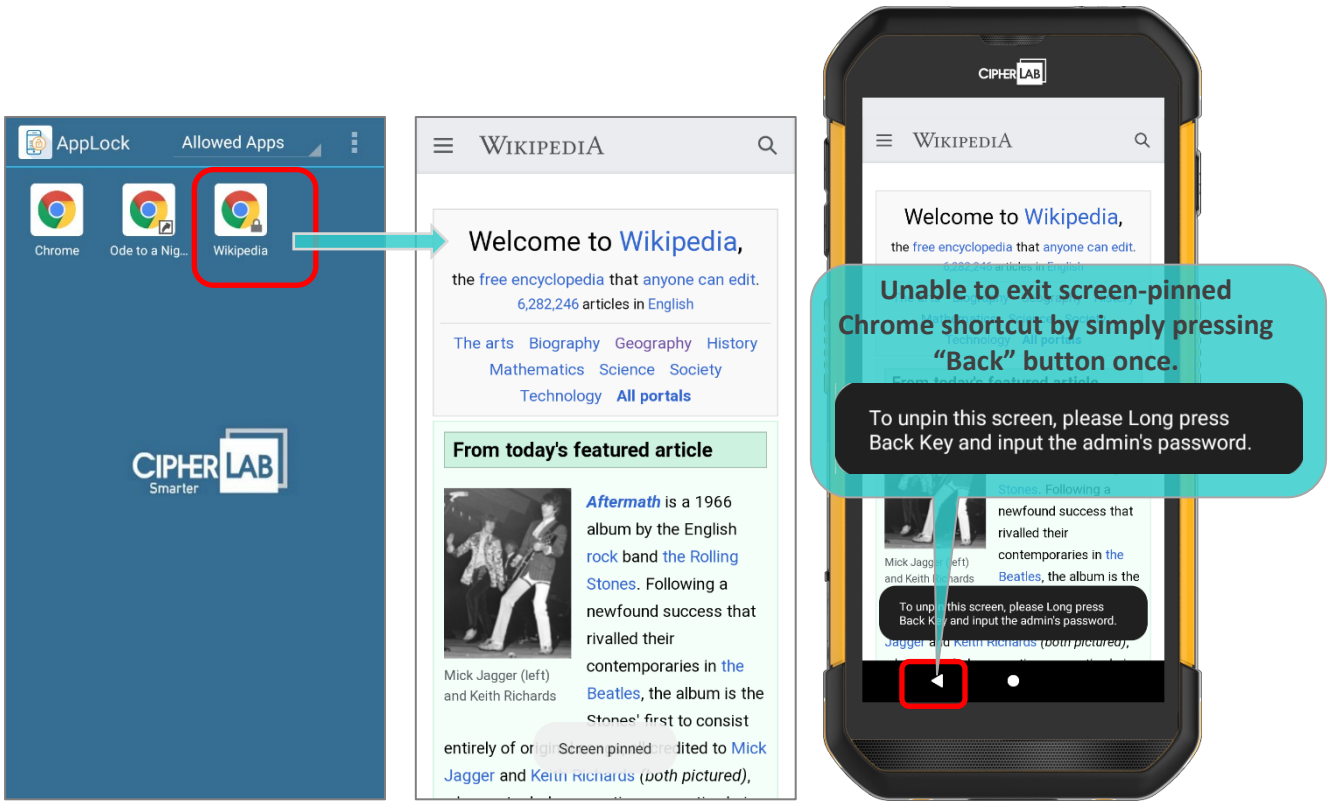


SCREEN PINNING

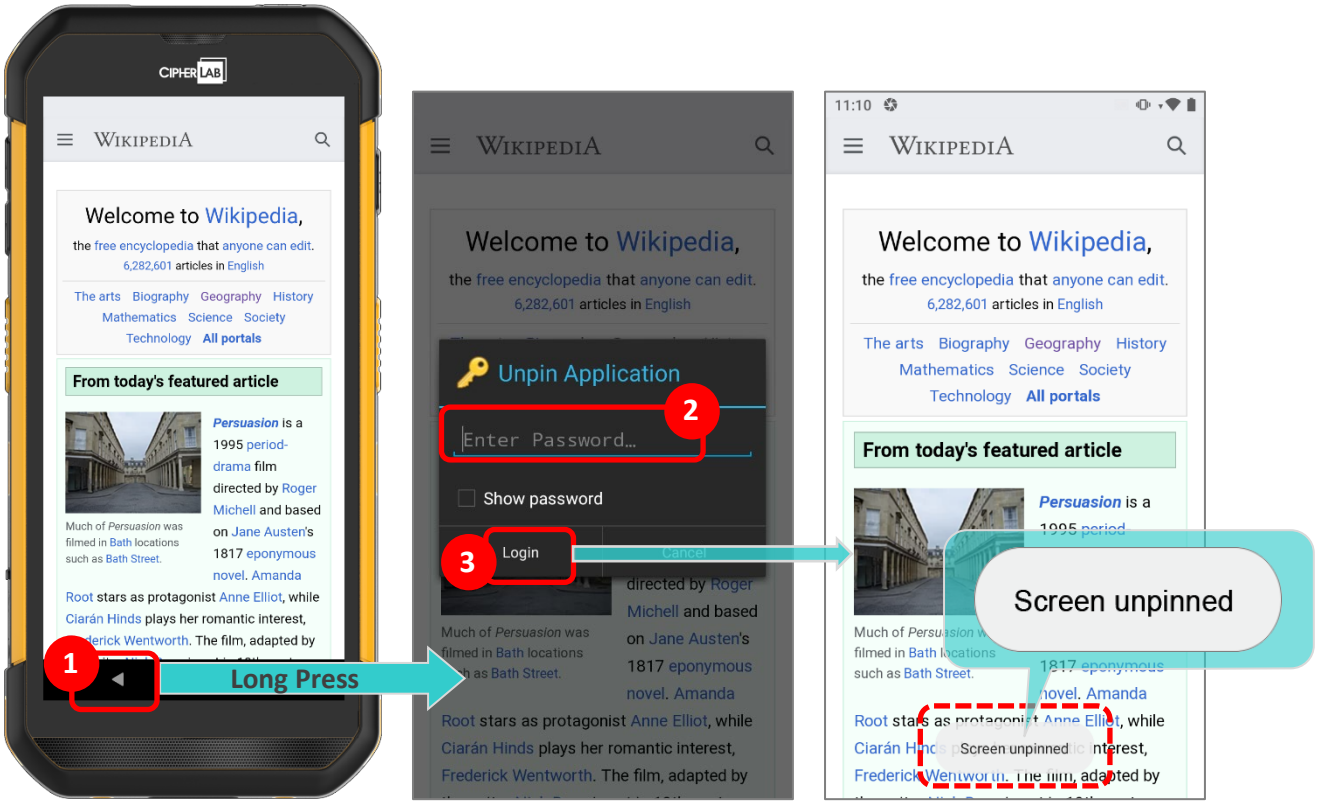
"**Screen Pinning**" for Chrome shortcut is to pin the webpage on screen after this Chrome shortcut is launched. By enabling "**Screen Pinning**" for Chrome shortcut, a lock icon is shown on the lower-right corner of the screen-pinned Chrome shortcut.



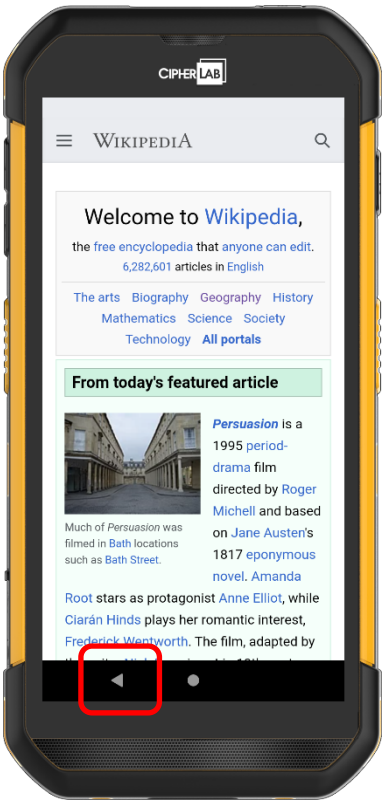
Once the screen-pinned Chrome shortcut is launched, users cannot exit it by pressing **Back** button once untill [the admin password] is entered.



To unpin the screen-pinned Chrome shortcut, please long press **Back** button and then input the admin password in the "**Unpin Application**" pop-up window.



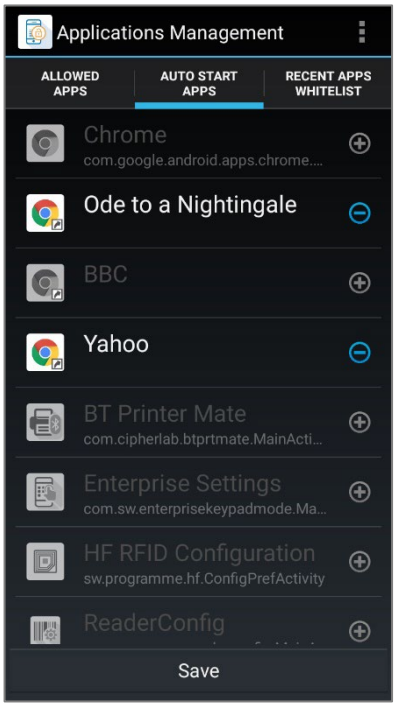
After unpinning the Chrome shortcut, click **Back** button again to exit it.



SET CHROME SHORTCUT AS AUTO START APP

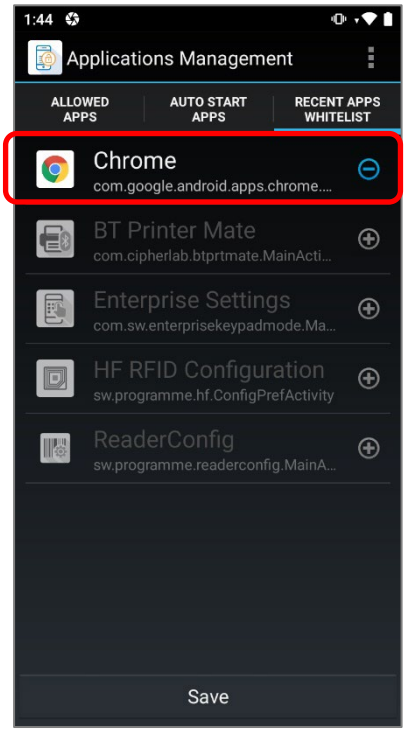
Chrome shortcut(s) can be set as **Auto Start App** by tapping on ⊕ of the **Chrome shortcut** you'd like to add on "**Auto Start App**" tab page of Applications Management.

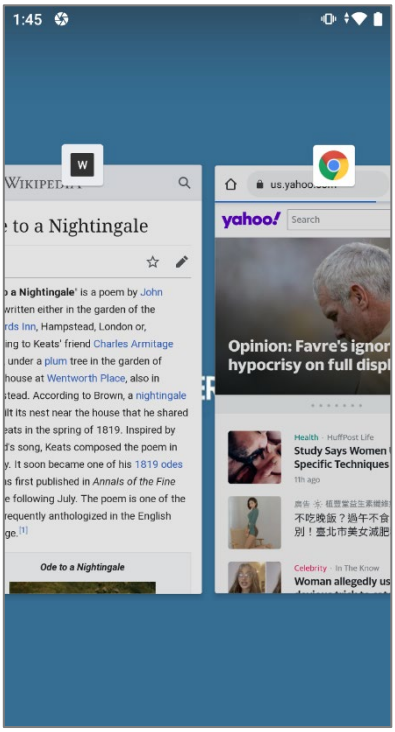
Please refer to Auto Start APPs View for details and Auto Start App with Screen Pinning Enabled for how set a screen-pinned Chrome shortcut to be auto started app.



RECENT APPS WHITELIST

Chrome shortcut(s) is not displayed on "Recent Apps Whitelist" for users to select. To make your Chrome shortcut(s) available to recently used applications list, please add the application "**Chrome**" by tapping on its ⊕ button on **Recent Apps Whitelist** tab page of **Applications Management**. All your Chrome shortcuts will be kept on the record list of recently used applications.



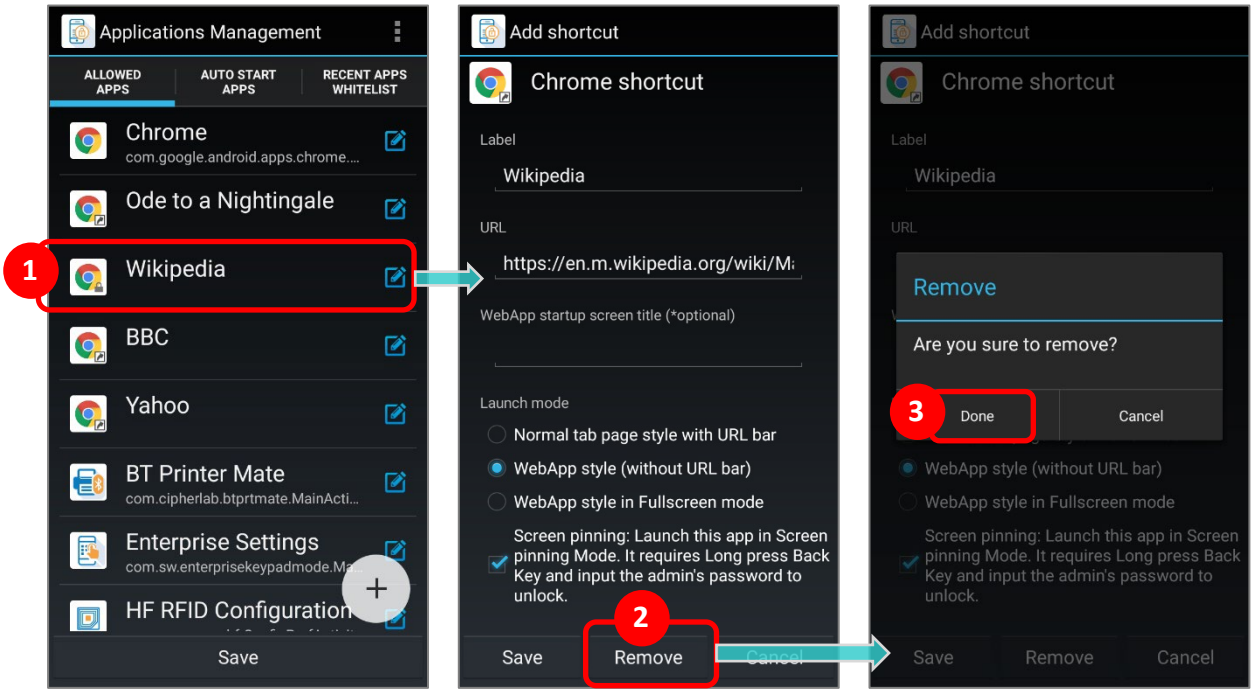


REMOVE CHROME SHORTCUT

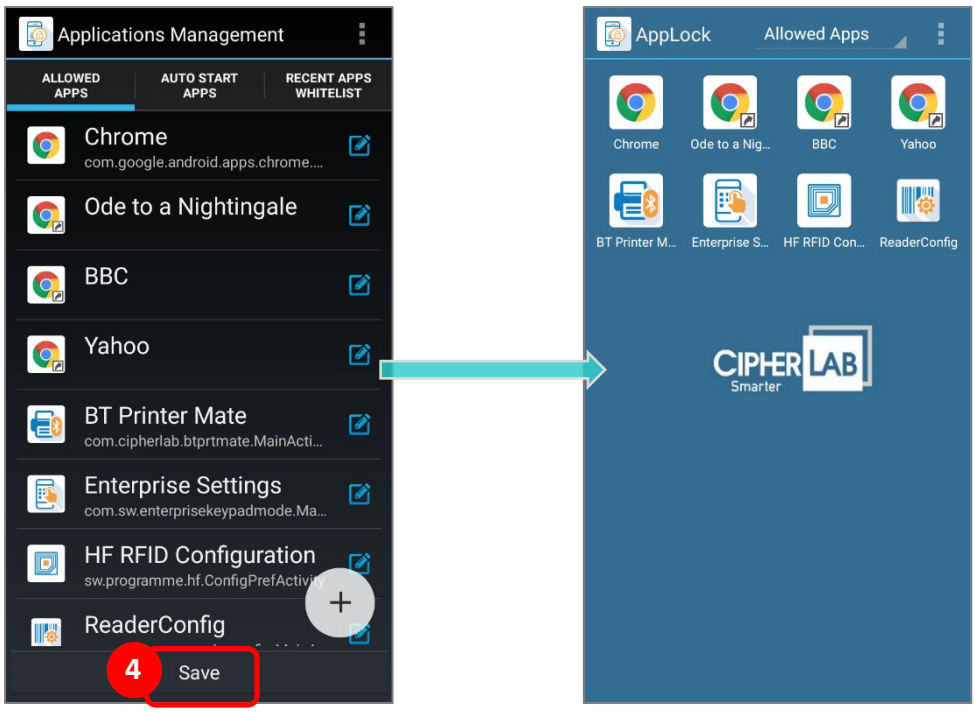
You may remove your Chrome shortcut by the following steps:

1) On **Applicaation Management** page, tap on the Chrome shortcut to be removed to enter its detailed page.

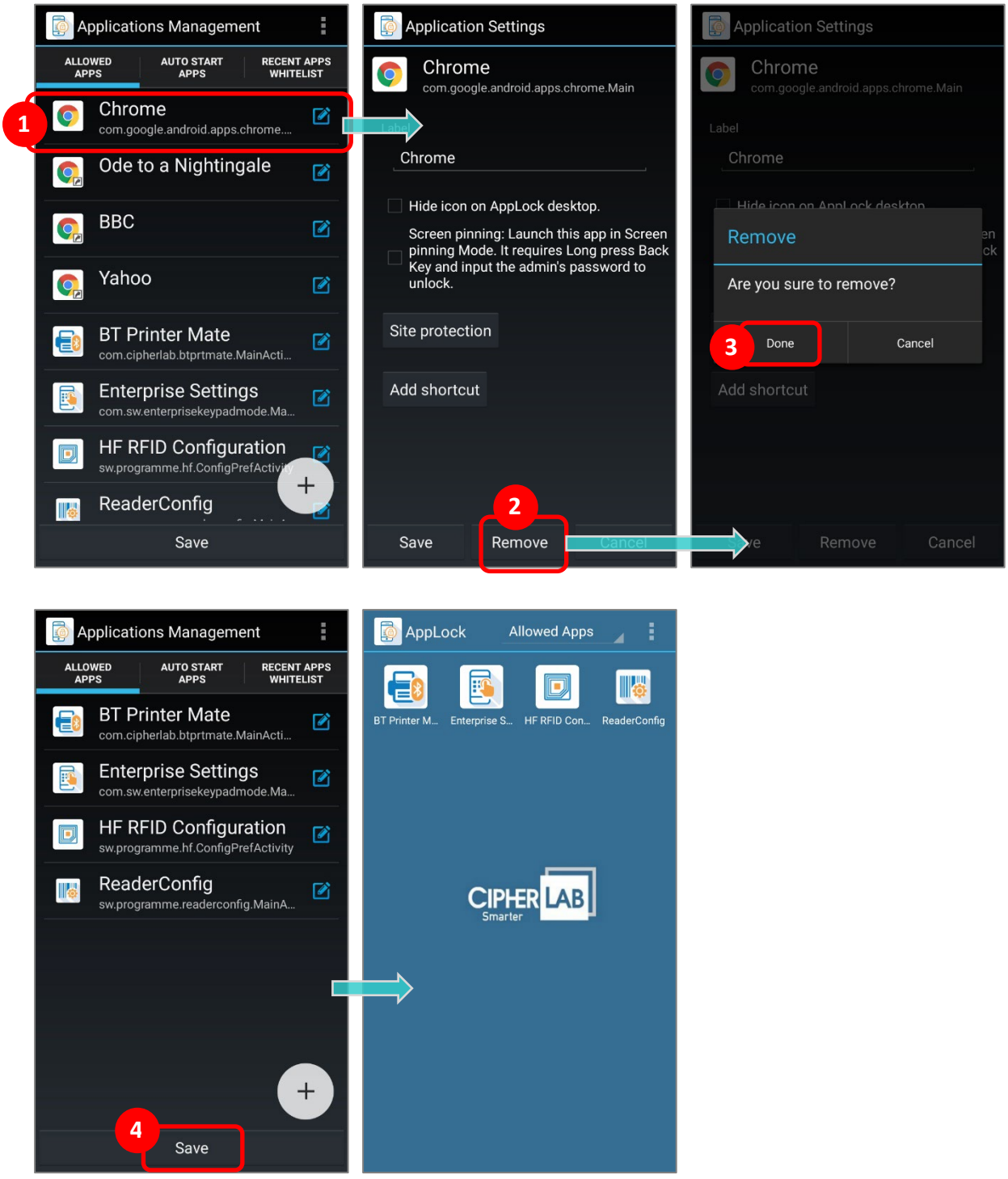
2) Tap on "**Remove**" and confirm this action by "**Done**".



3) Make sure to "**Save**" before leaving Applicaation Management.



Please note that by removing the application "**Chrome**", all your Chrome shortcut(s) will be removed as well.



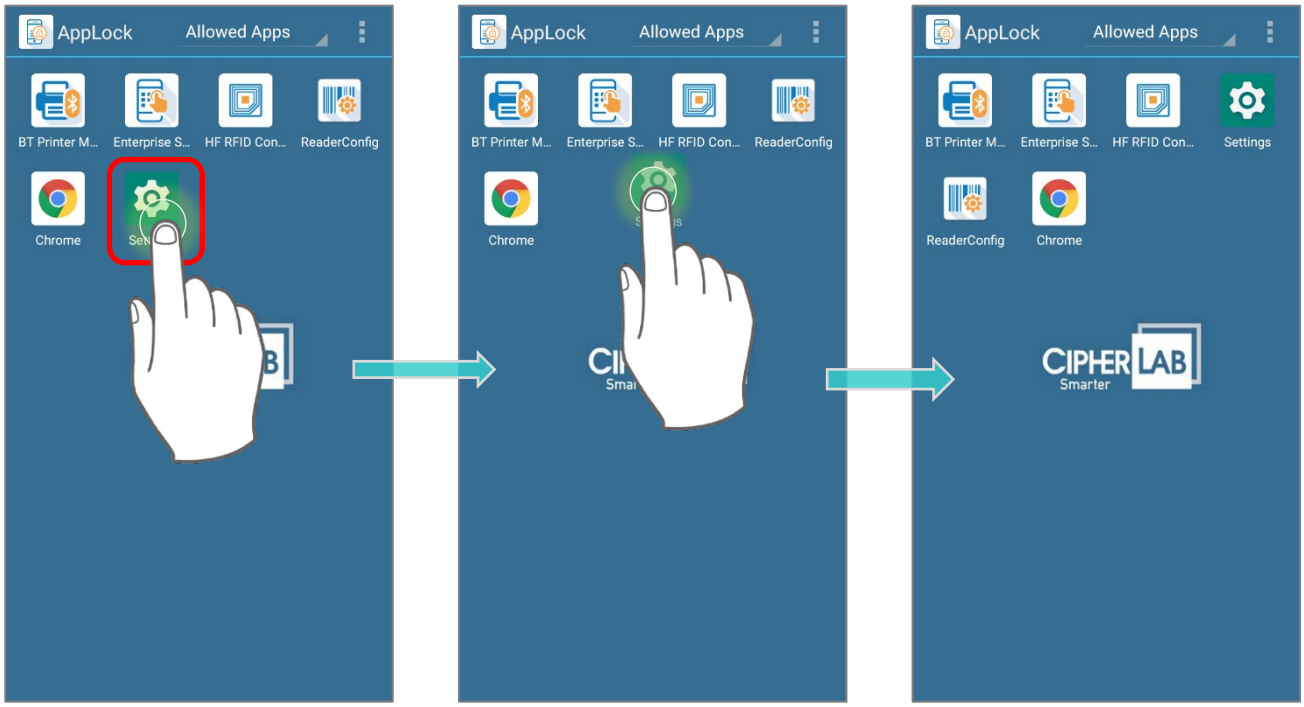
3.3.5 REARRANGE THE SORTING ORDER OF THE APPS/SHORTCUTS ON DESKTOP

Administractor can rearrange the sorting order of the apps/shortcuts shown on AppLock main screen by dragging:

1) On "**Allowed Apps**" view of AppLock main screen, long press the app/shortcut icon you would like to change its sorting order. Once the app/shortcut icon becomes translucent, you can move it by dragging.

2) Keep pressing and holding the app/shortcut icon, and drag it to change its position. Release the icon to have it placed.

- Step 1:
  Long press the app/shortcut.
- Step 2:
  Hold and drag the app/shortcut to the preference place.
- Step 3:
  Release the app/shortcut.

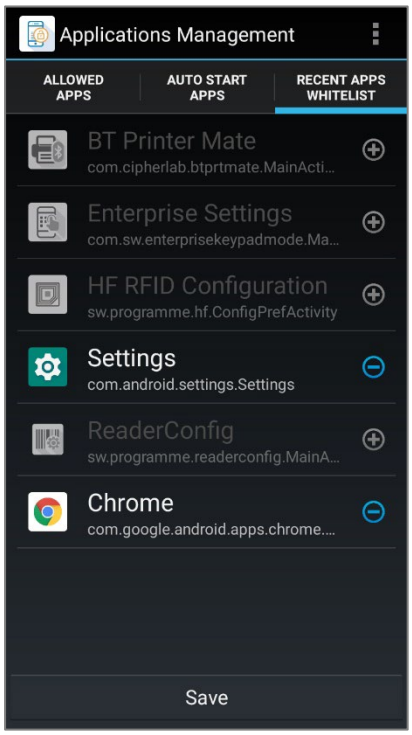


Note:

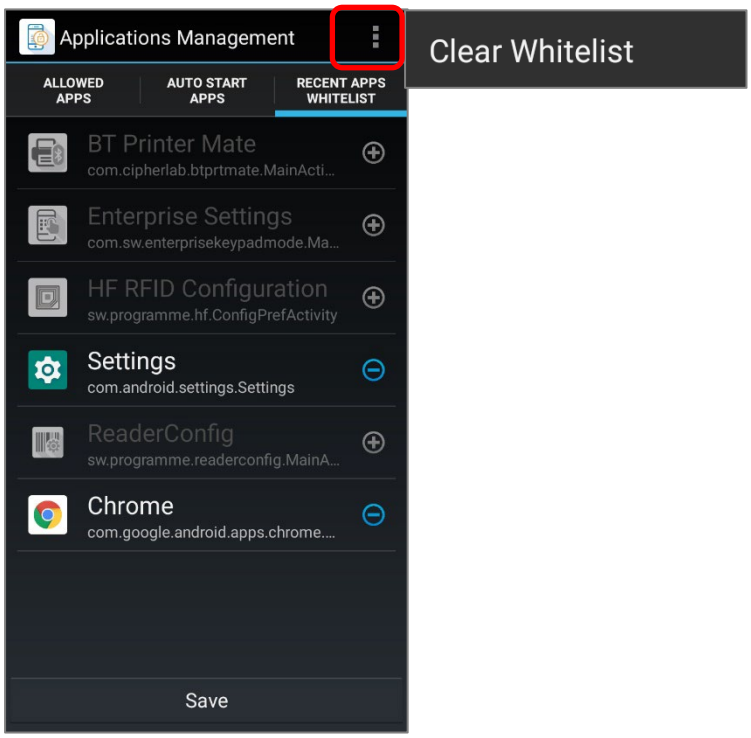
You can only rearrange the apps and shortcuts' sorting order, but not drop them to the blank space on AppLock main screen.

3.4 RECENT APPS WHITELIST

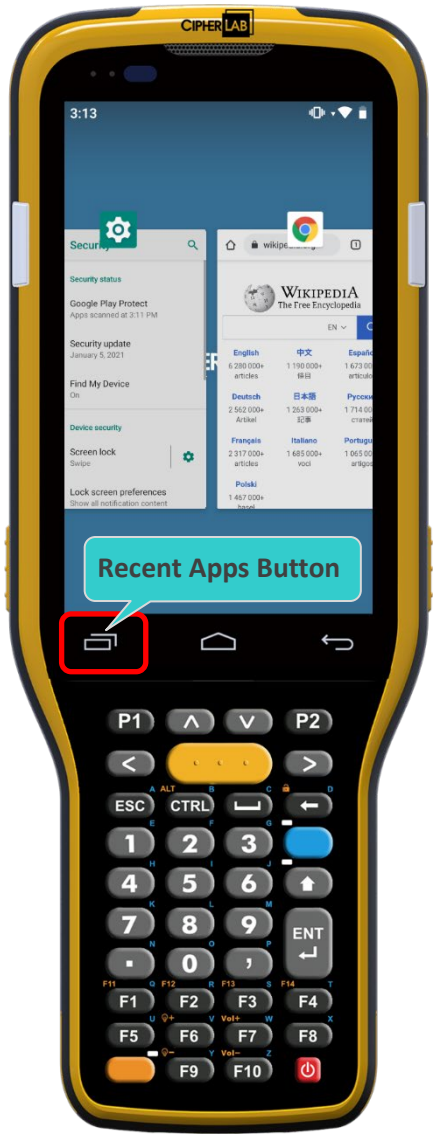
In the **Applications Management** screen, tap **Recent Apps Whitelist** to select the applications to retain in the recent apps list by tapping on ⊕ button.

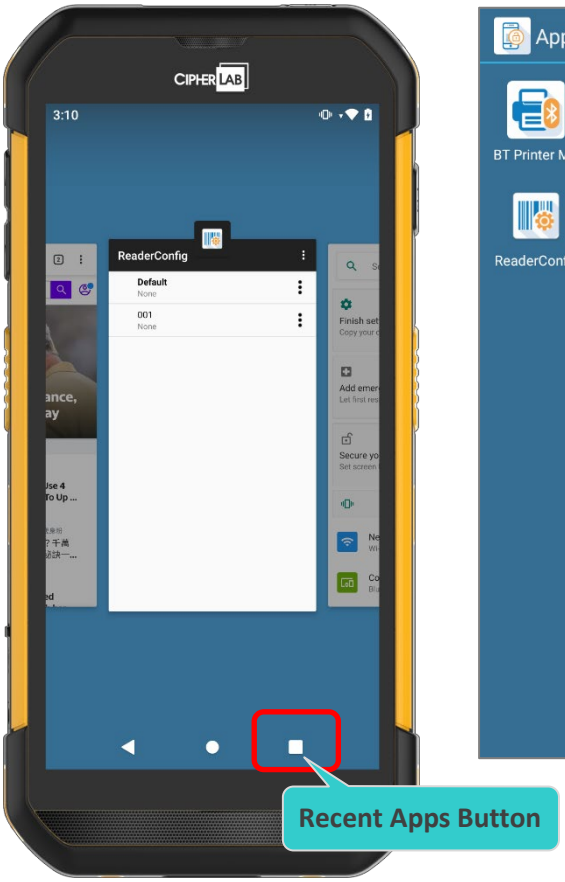


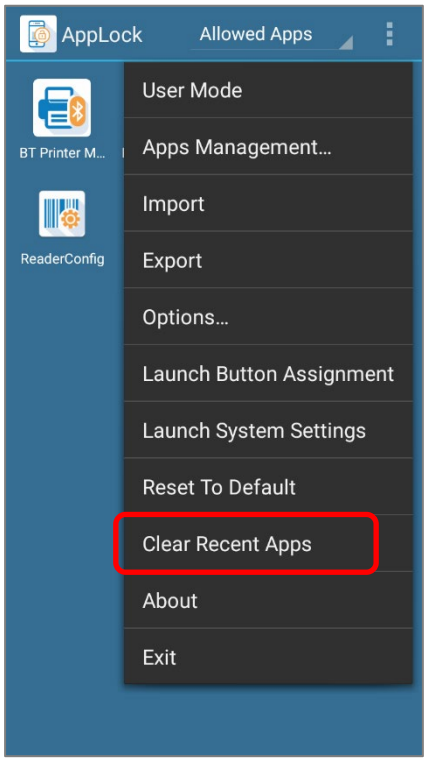
To remove the application from **Recent Apps Whitelist**, you can tap menu button ⋮ on the action bar and tap on "**Clear Whitelist**" to remove all the applications, or tap on ⊖ button of the application to be removed.



Pressing “**Recent Apps**” button will dislay the record of recently used applications. The record can be cleared by “**Clear Recent Apps**”, but the selected application(s) on **Recent Apps Whitelist** will be kept.







Chapter 4

OPTION (ADMINISTRATOR ONLY)

This chapter specifies the **Options** menu which is an administrator-only setting group that controls how AppLock acts each time it is used.

IN THIS CHAPTER

4.1 Options Menu (Administrator Only) 84
4.2 Notification Bar 85
4.3 Display 90
4.4 Security 92
4.5 Assist app 95
4.6 Remove Lockscreen Icons 98
4.7 USB Connection Allowed 99

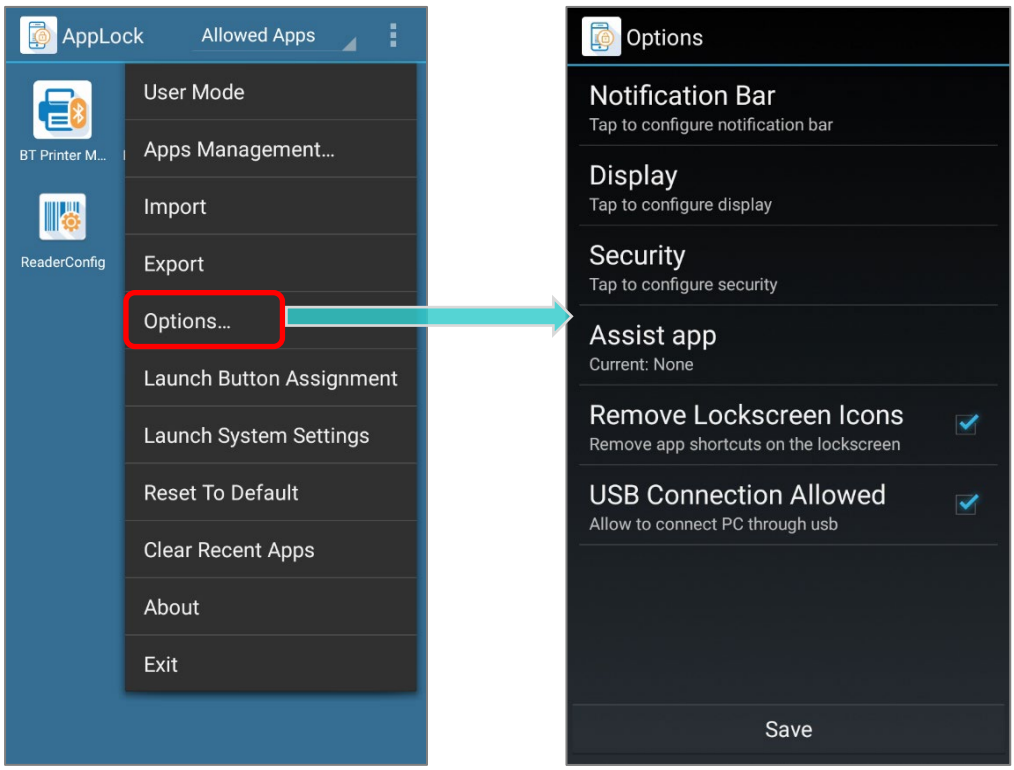
4.1 OPTIONS MENU (ADMINISTRATOR ONLY)

To open the Options menu:

1) Tap the menu button ⋮ .
2) Tap on "**Options….**"

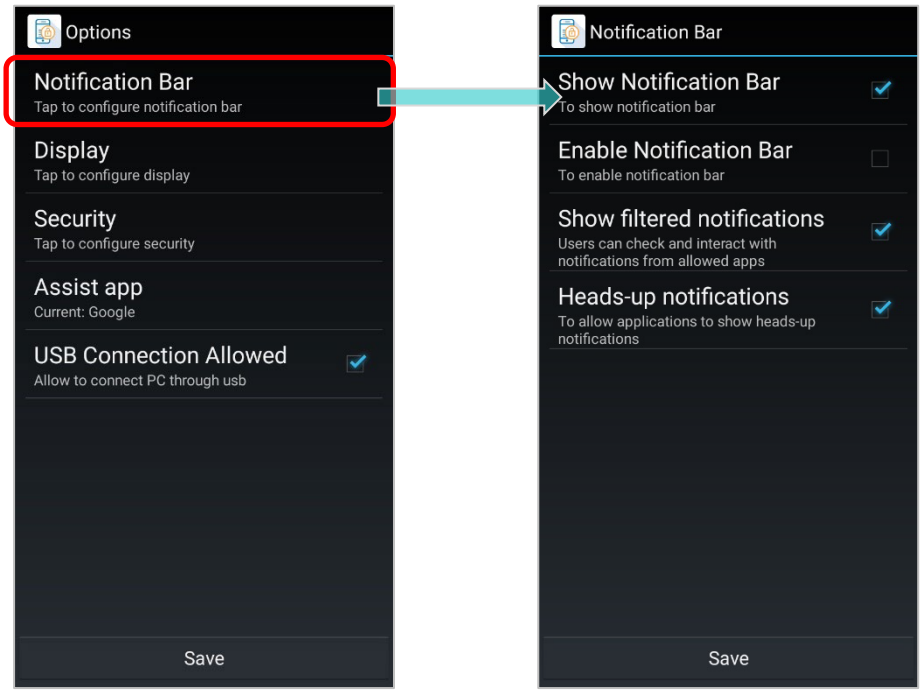
Options menu features the following functions:

- Notification Bar
- Display
- Security
- Assist app
- Remove Lockscreen Icons
- USB Connection Allowed



4.2 NOTIFICATION BAR

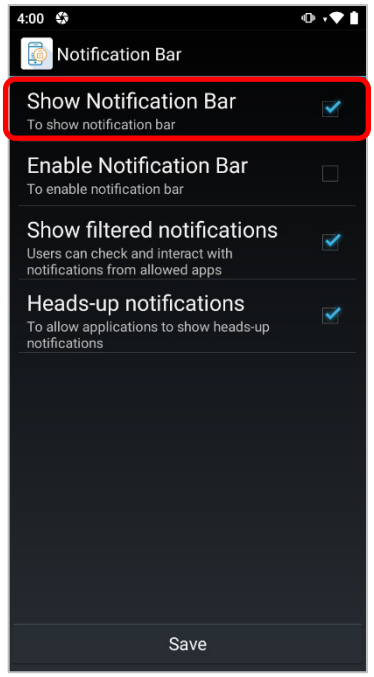
Tap **Notification Bar** to open settings for the system notification bar.



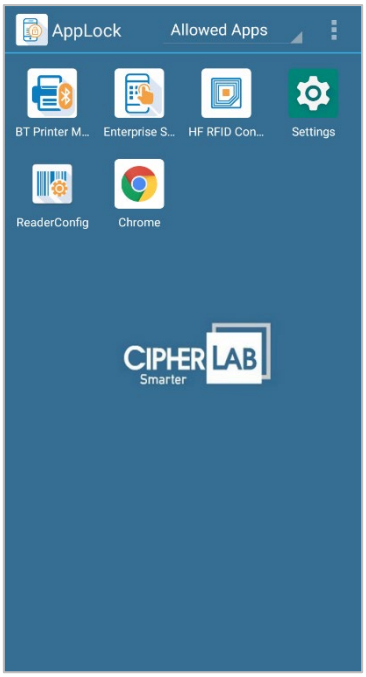
4.2.1 SHOW NOTIFICATION BAR

"**Show Notification Bar**" is the function to shows the notification bar on the top of the screen. Use the notification bar to check battery status, wireless connection status, and system notifications.

Enable "Show Notification Bar"



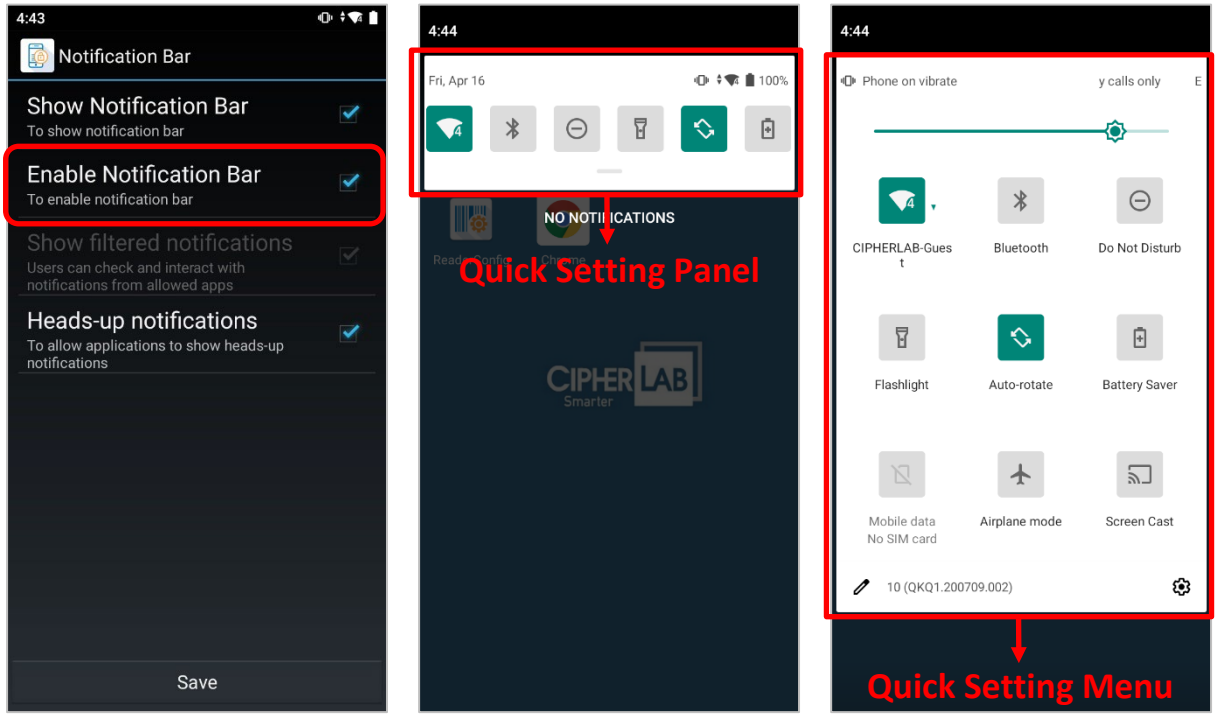
Disable "Show Notification Bar"



4.2.2 ENABLE NOTIFICATION BAR

The default setting of "**Enable Notification Bar**" is unticked. Tick the checkbox to enables the notification bar.

By enabling the function "**Enable Notification Bar**", the notification bar could be slid down to check & manage system notifications and open **Quick Setting Panel** and **Quick Setting Menu**. Also, all the notifications on the lock screen will be shown.

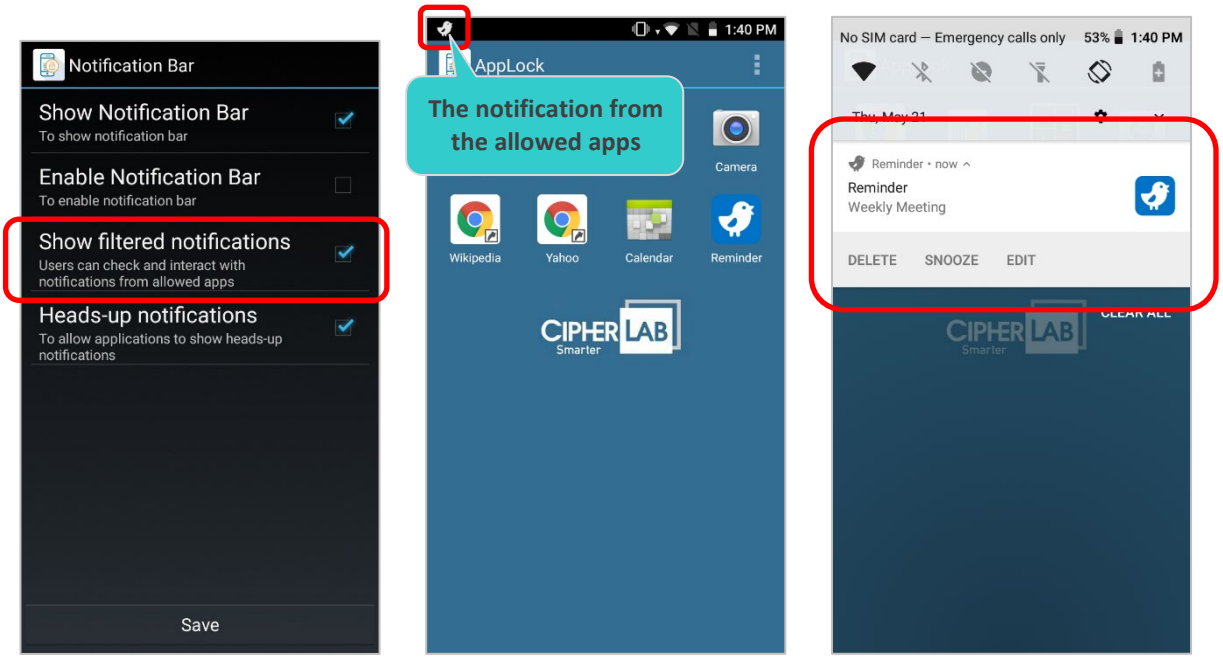


If "**Enable Notification Bar**"is disable, the setting of "**Show filtered notifications**" takes control whether to block the notification bar and to show the notifications on the lock screen:

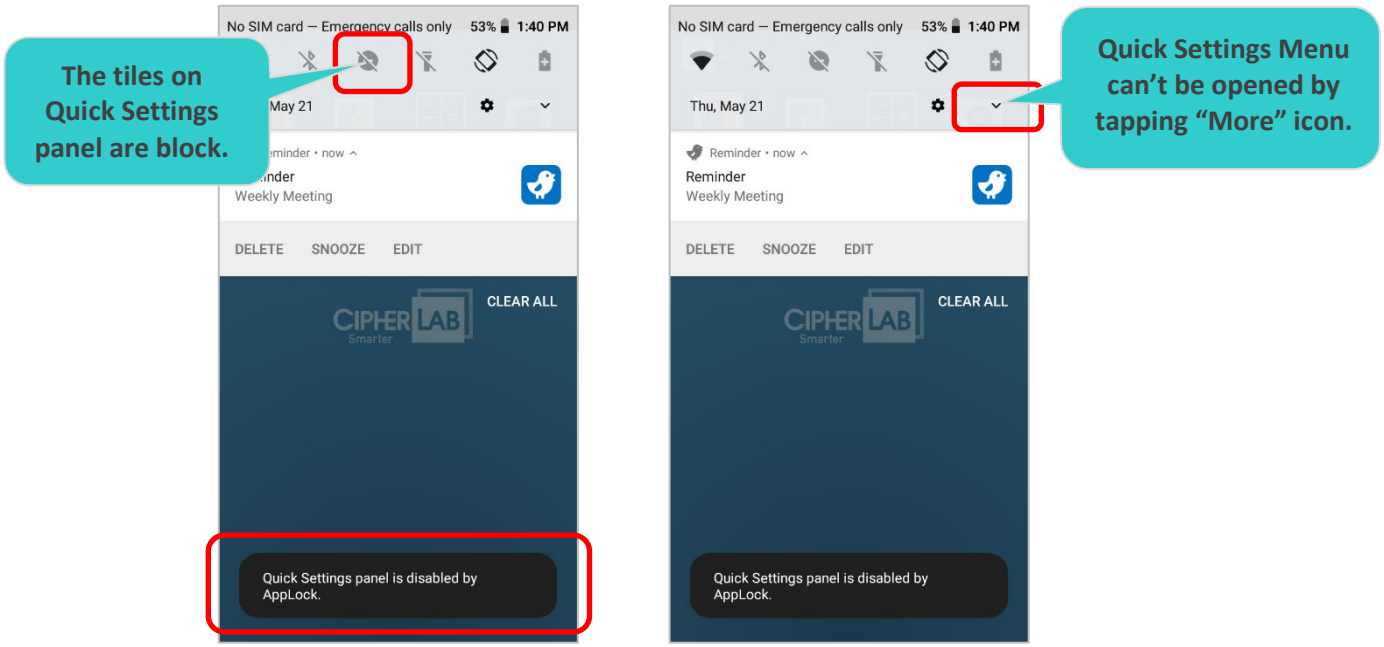
	Enable Notification Bar **ON**	Enable Notification Bar **OFF**	
		Show filtered notifications **ON**	Show filtered notifications **OFF**
Notification Bar	Notification bar can be slid down.	Notification bar could be slid down to reveal notification drawer.	Unable to slide down the notification bar.
Lock Screen	All notifications on the lock screen will be shown.	Only the notifications from Allowed apps will be shown.	No notifications will be shown on lock screen.

4.2.3 SHOW FILTERED NOTIFICATIONS

"**Show filtered notifications**" is for administrators to determine whether showing the notifications of allowed apps to users. The default setting is enabled, however, this function doesn't work when "**Enable Notification Bar**" is ticked. To make the setting of "**Show filtered notifications**" take effect, please disable "**Enable Notification Bar**" beforehand.

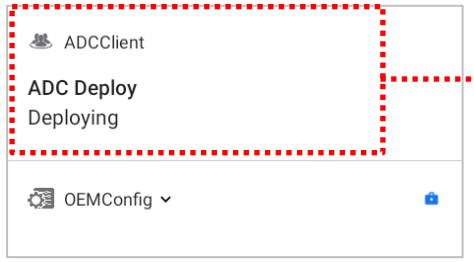


When "**Show filtered notifications**" is enabled, the status bar could be slid down to reveal notification drawer for checking the notifications from allowed apps only. The quick settings panel is unavailable as well as the quick setting tiles on it.



Note:

By default, the notifications from ADCClient and OEMConfig are always shown when the device works with ADC (Android Deployment Configurator) or ReMoCloud even they are not on the allow app list or even "**Heads-up notifications**" is disabled.



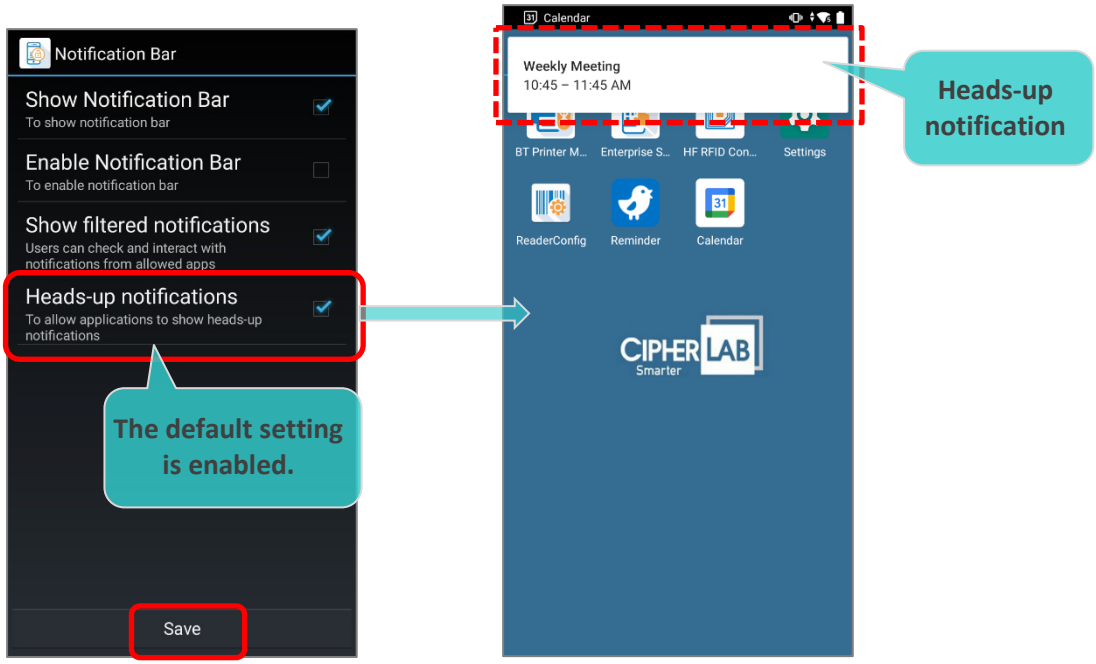
The notification is available when the device works with ADC.

The notification is available when the device works with ReMoCloud.

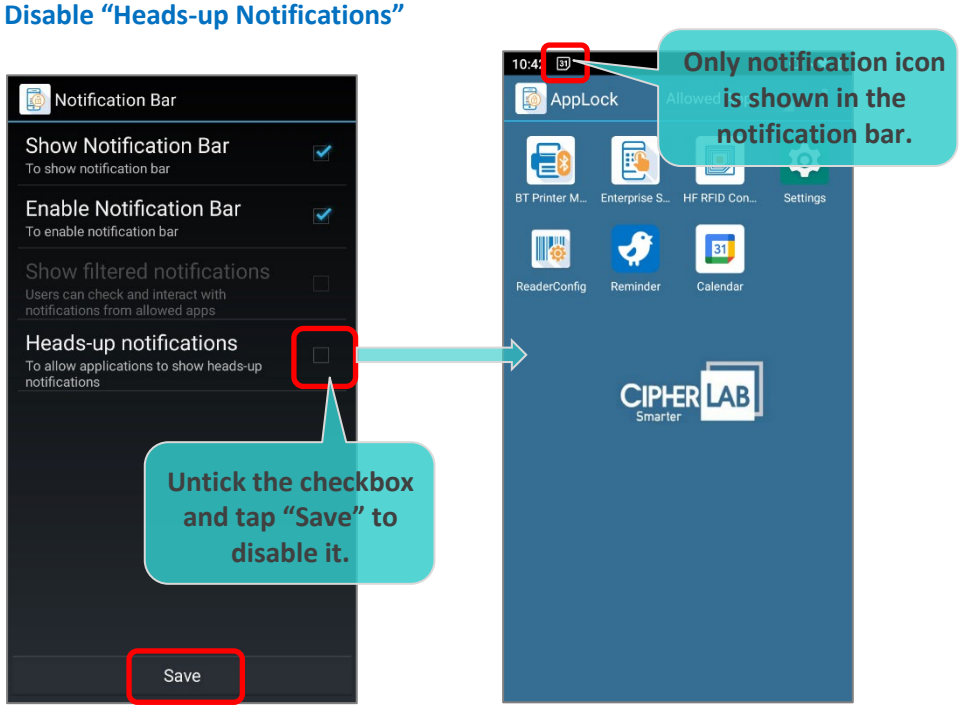
4.2.4 HEADS-UP NOTIFICATIONS

The default setting is to enable "**Heads-up notifications**". Untick the checkbox to disable the head-up notifications to pop-up.

Enable "Heads-up Notifications"



Disable "Heads-up Notifications"



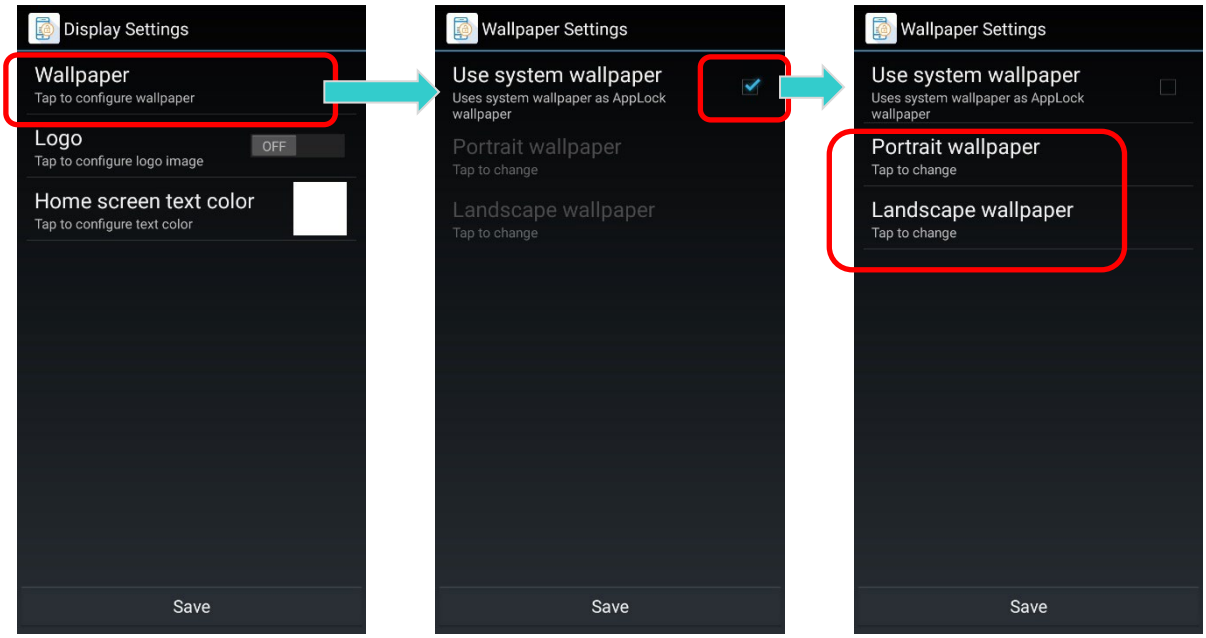
Note: The function "**Heads-up notifications**" is not supported for RS30 mobile computer.

4.3 DISPLAY

Tap on **Display** to open settings for the wallpaper and the logo seated right below the toolbar.

4.3.1 WALLPAPER

"**Wallpaper**" is to set the wallpaper for the main screen, you can select to use the system wallpaper. To use a custom wallpaper for portrait view or landscape view, please deselect "**Use system Wallpaper**" first, and then tap "**Portrait wallpaper**" or "**Landscape wallpaper**" to select image files. After finish setting, please tap on "**Save**" to confirm the settings.

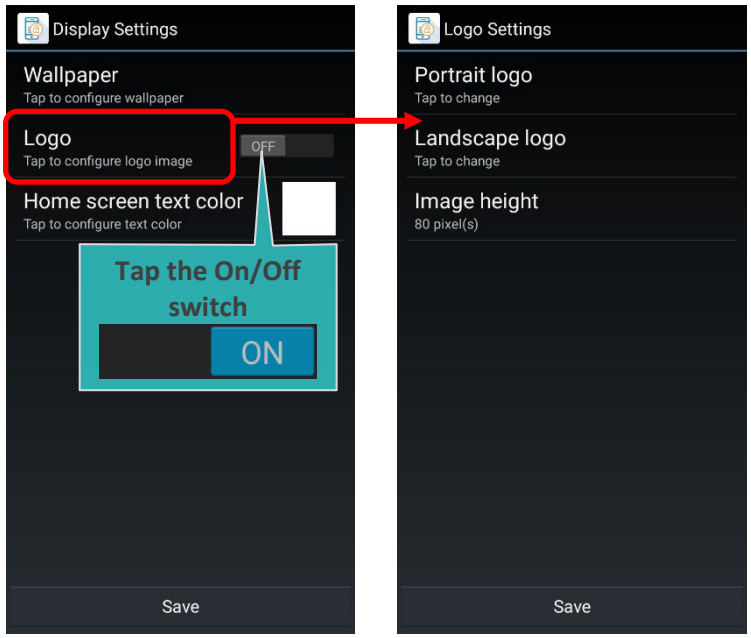


4.3.2 LOGO

Tap the On/Off switch to enable displaying a logo at the top of the main screen.

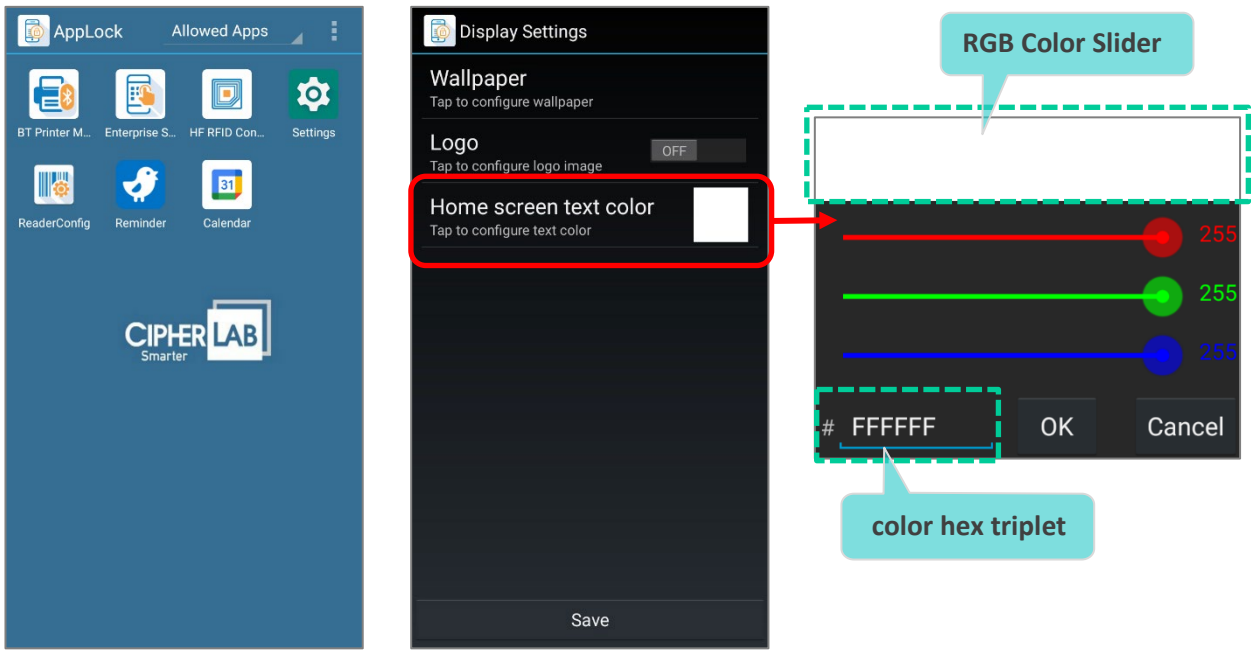
Tap the Logo label to select a logo for portrait view or landscape view, and set the image height (1~270 pixels).

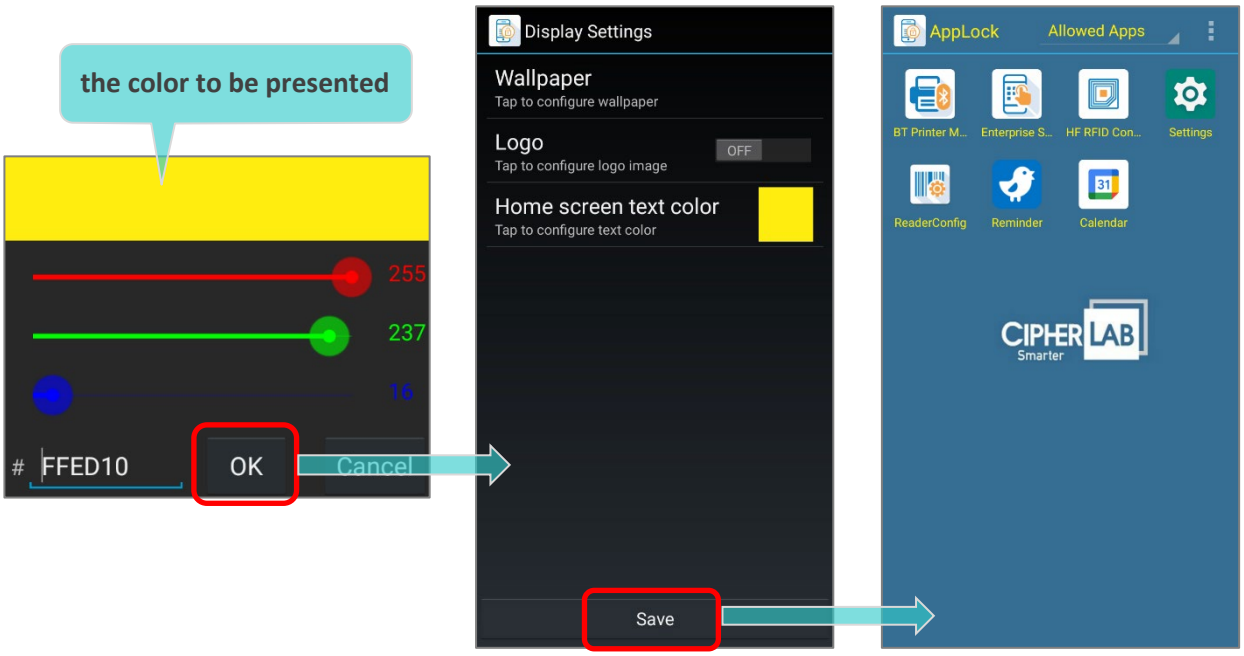
Tap on "**Save**" to confirm the settings.



4.3.3 HOME SCREEN TEXT COLOR

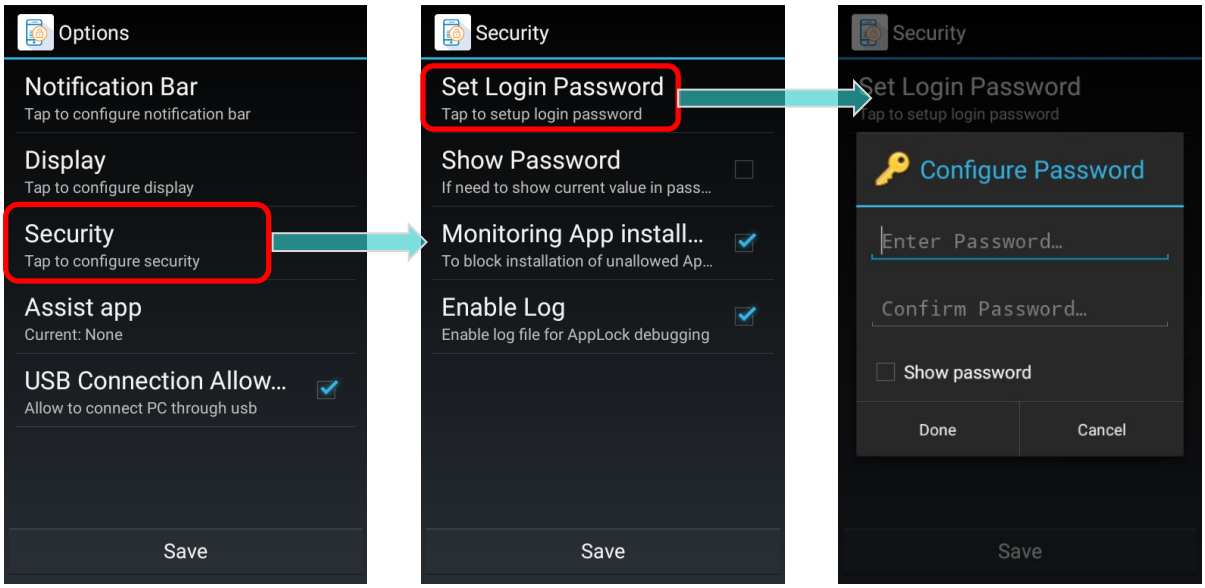
The default text color displayed on home screen is white whose RGB color is (255,255,255) and the color hex is #FFFFFF. You can change the text color on home screen by dragging the RGB color sliders or directly input the color hex triplet (hexcode) to designate your home screen text color.





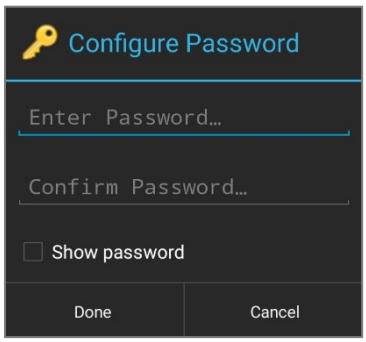
Make sure to tap on "**Save**" in every page before returning to the main screen.

4.4 SECURITY

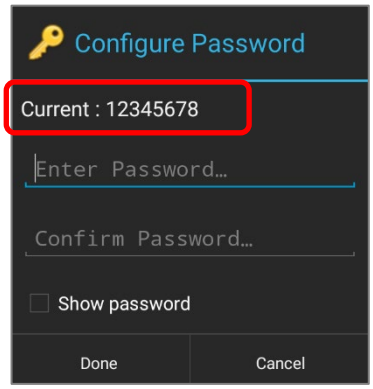


SET LOGIN PASSWORD

"**Set Login Password**" is to set the login password for the administrator access level. To display the current password, please enable "**Show Password**" on **Security** page.

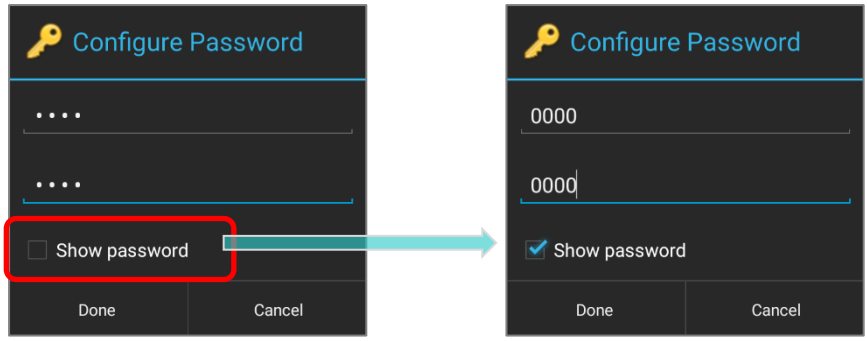


Current password is hidden.



Current password is shown.

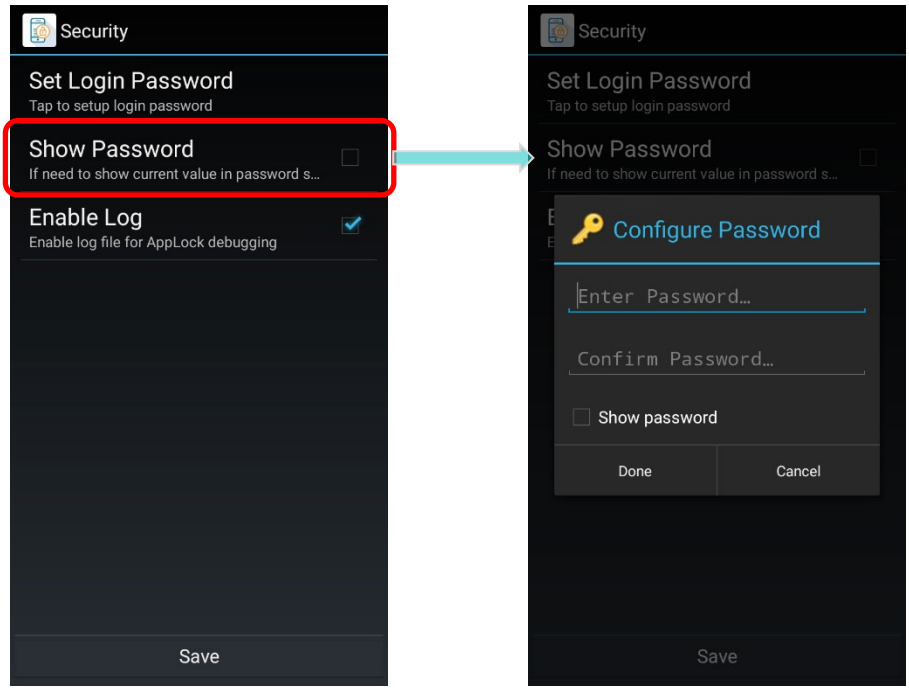
If "**Show password**" on "**Configure Password**" popup dialog is ticked, the new password you enter and confirm will be shown.



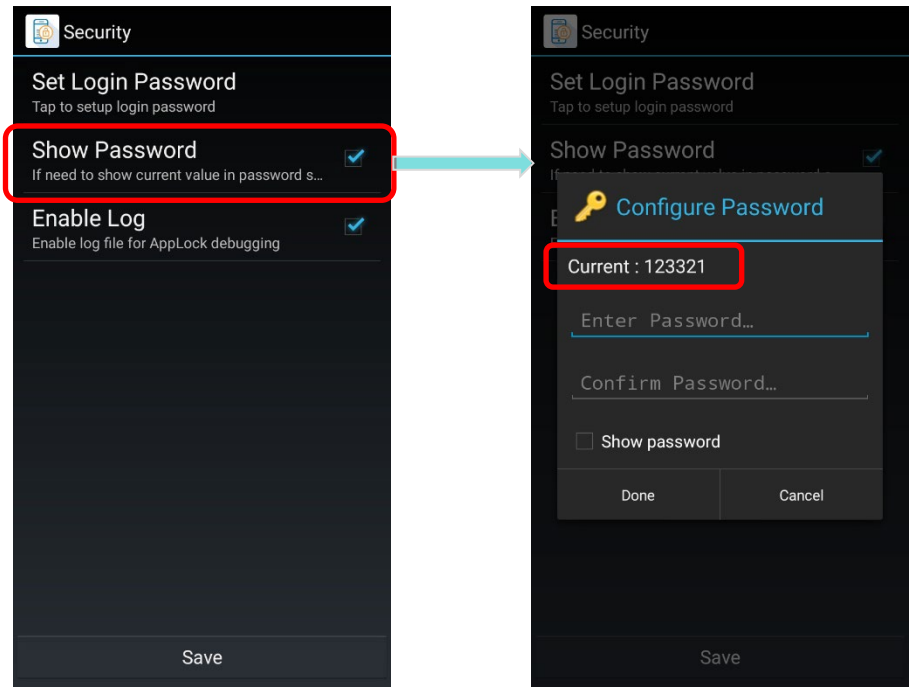
SHOW PASSWORD

By ticking the checkbox of "**Show Password**" on **Security** page, the current password is shown during setup of a new password.

Disable "Show Password"

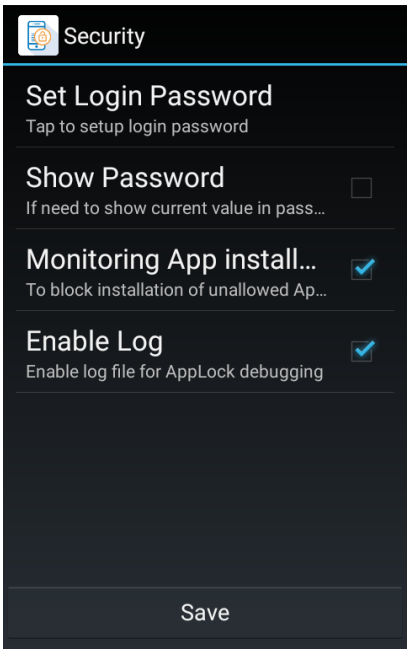


Enable "Show Password"



MONITORING APP INSTALLATION

Once “**Monitoring App Installation**” is enabled, users cannot install any apk of the apps which are not on the “**Allowed App**” list.



The default setting of “**Monitoring App Installation**” is disabled. Users can install the apk of the disallowed app, but the app cannot be launched.

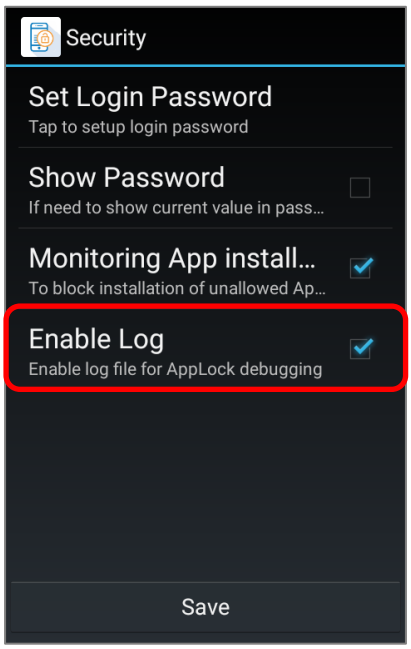
If you have your own developed application installed in the device, and it opens an activity from other app designated by your own developed app, e.g. application update or installation by package installer, package installer will be blocked by AppLock when “**Monitoring App Installation**” is enabled because AppLock cannot verify that the app to be updated or installed is on the **Allowed Apps** list. Thus it is suggested to disable “**Monitoring App Installation**” for the aforesaid circumstances.

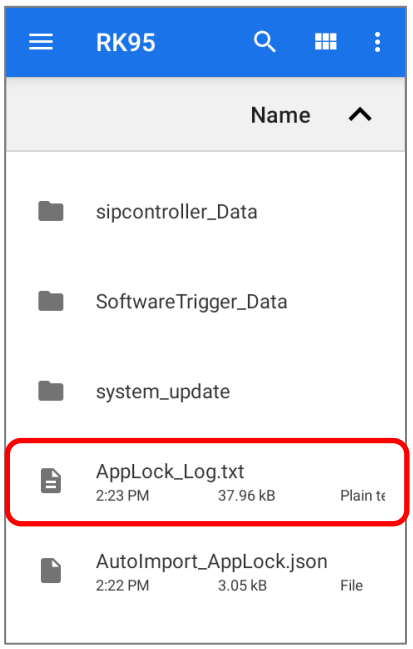
Note: The device with Android 10 or later doesn’t support “**Monitoring App Installation**”.

ENABLE LOG

Enable Log is to record the event log performed in AppLock. The default setting is enable.

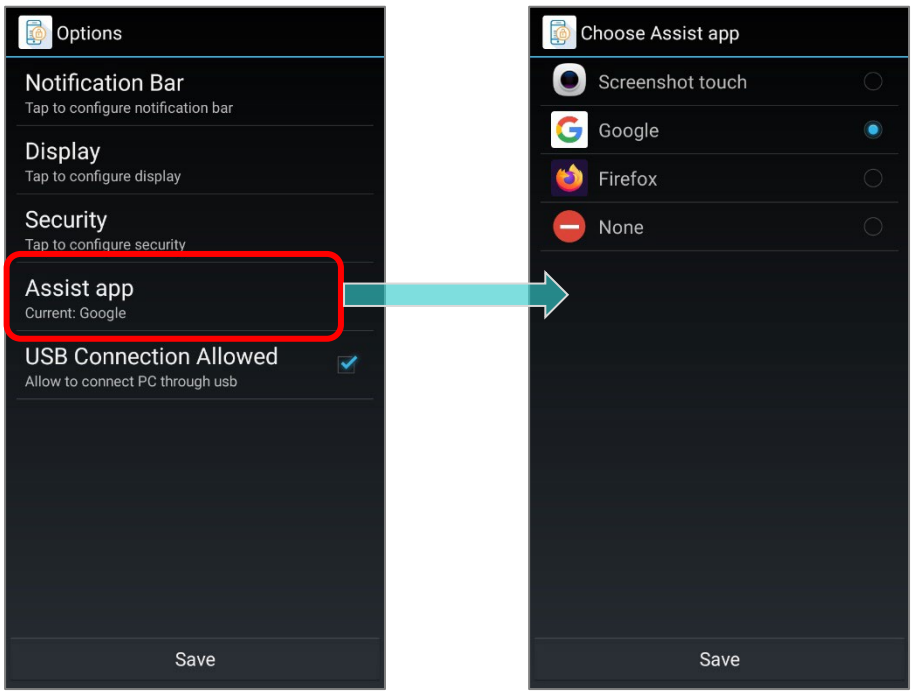
The log will be saved as “**AppLock_Log.txt**” in the internal storage.



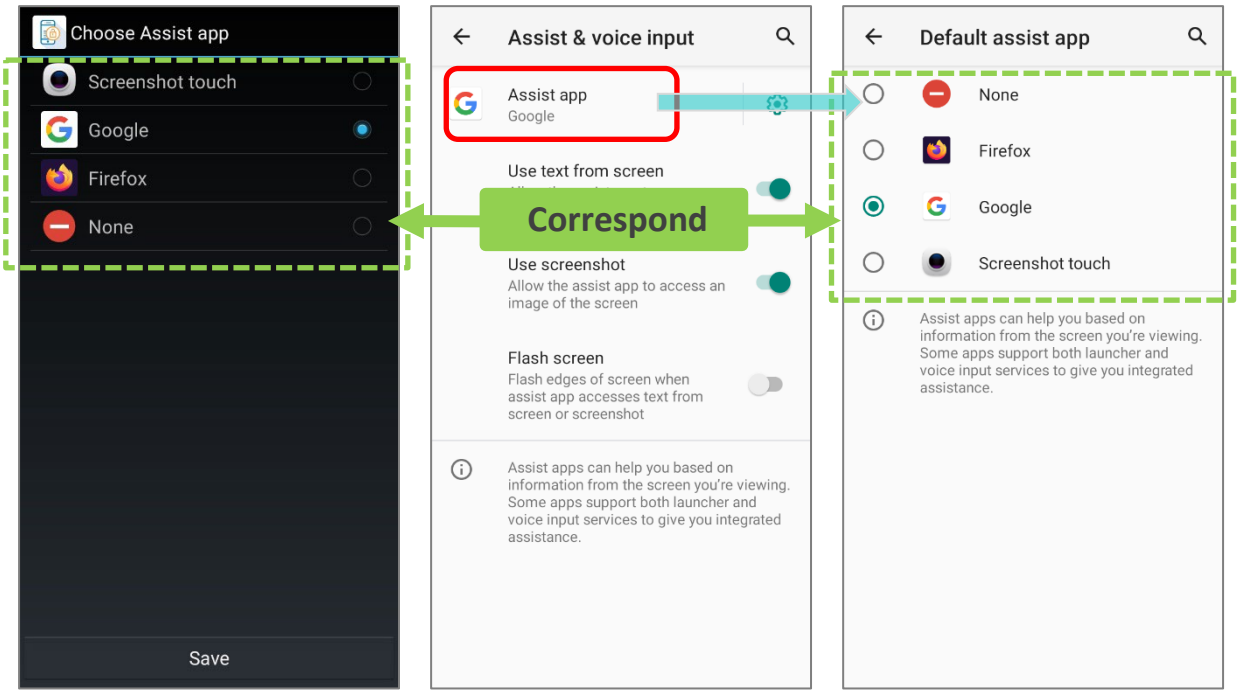


4.5 ASSIST APP

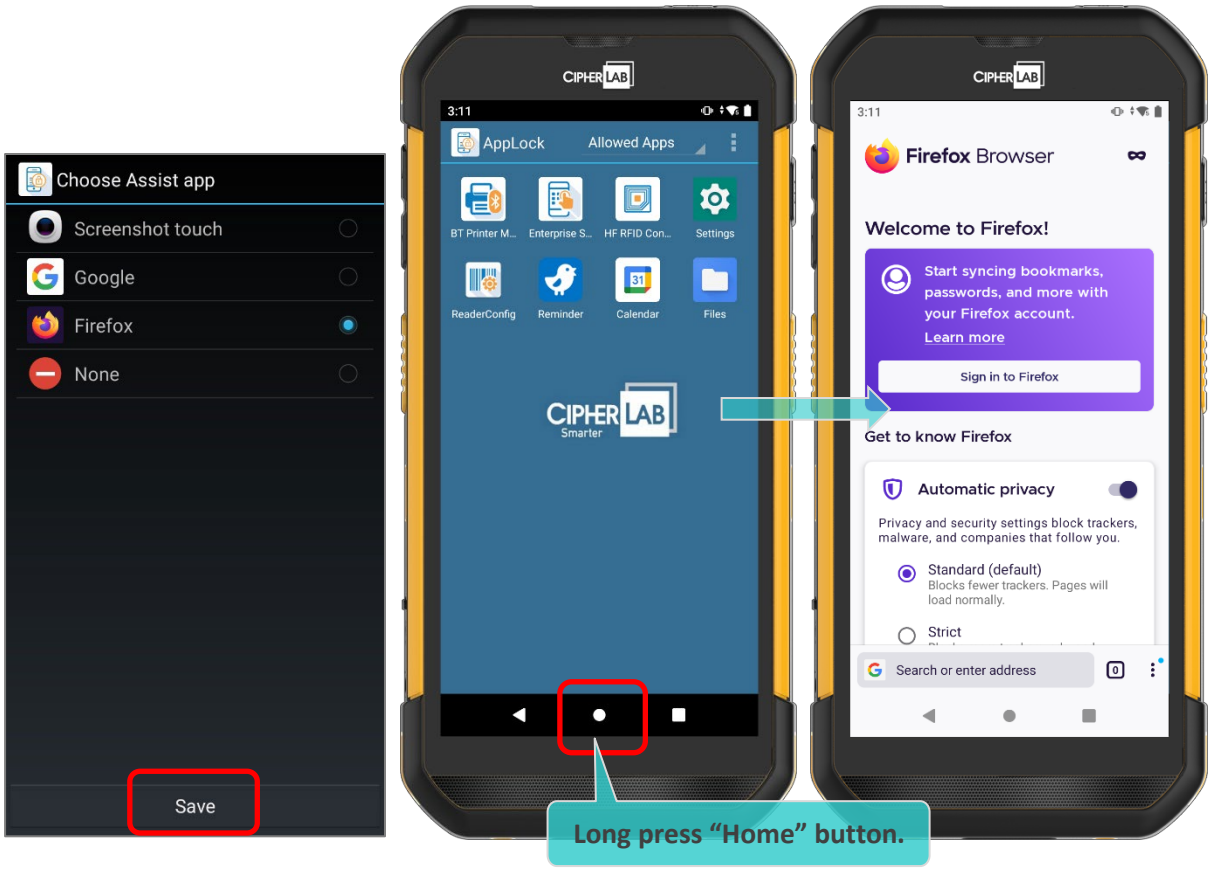
Tap **Assist app** to choose the assist app you need:



Enter AppLock for the 1st time, the **Assist app** is automatically set as "**None**". All the applications listed in **Assist app** page of AppLock are correspond to Android system settings (**Assist & voice input**).



In AppLock, you could choose the assist app or remain it as none. The selected assist app could be opened by no matter Admin or users with long press **Home** button.



The **Assist app** will be restored to the setting before entering AppLock once exiting AppLock from **Admin** Mode, while it will be restored to the previous settings when re-entering AppLock.

Note:

1. The system function"**Assist app"** is not supported for RS30 mobile computer.

2. **Assist & voice input** can be accessed from:

- For Android 6 (**RS50**):

  App Drawer (All apps) | Settings | Apps | Configure apps | Default Apps |Assist & voice input | Assist app

- For Ansroid 7 (**RS31** & **RK25 for Android Nougat**):

  App Drawer (All apps) | Settings | Apps | Configure apps | Assist & voice input | Assist app

- For Android 8 (**RS51** & **HERA51**):

  App Drawer (All apps) | Settings | Apps & notifications | Advanced | Default apps |Assist & voice input | Assist app

- For Android 9 (**RK25 for Android Pie** & **RK95**):

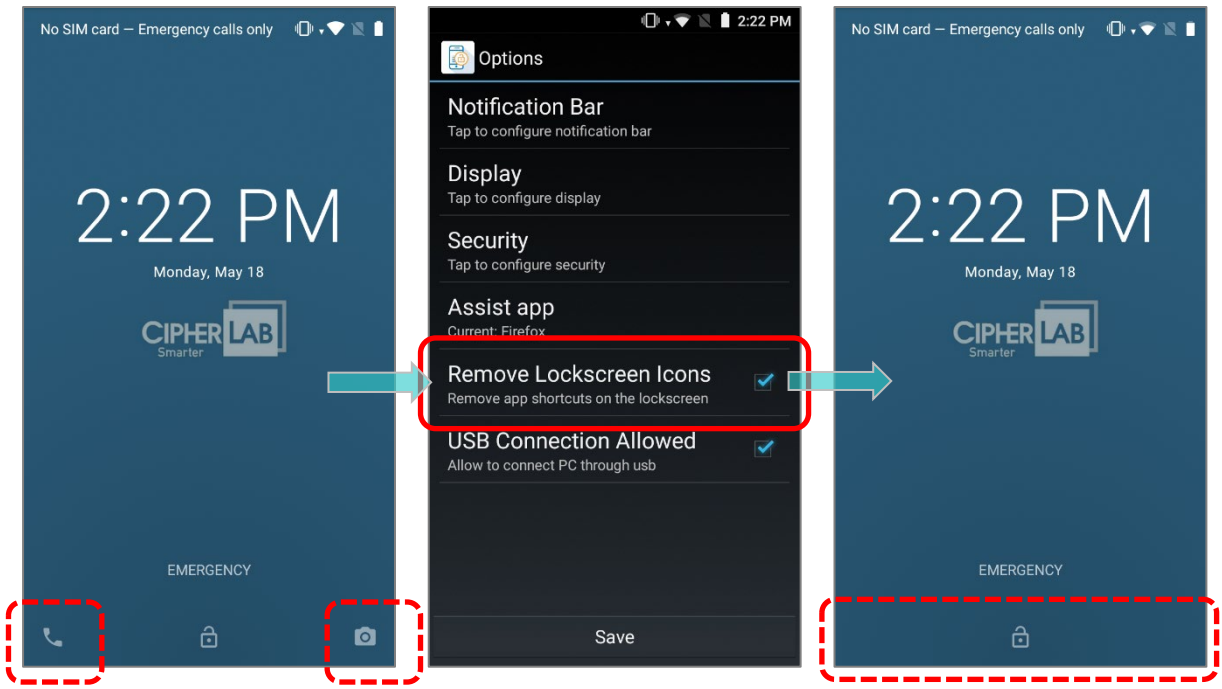
  App Drawer (All apps) | Settings | Apps & notifications | Default apps | Assist & voice input | Assist app

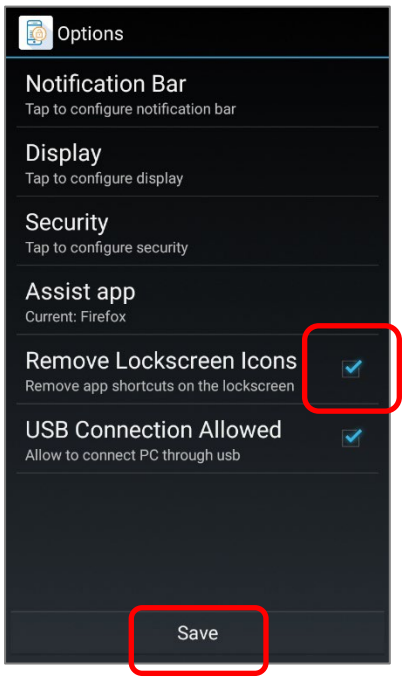
- For Android 10 (**RS35**):

  App Drawer (All apps) | Settings | Apps & notifications | Default apps | Assist app | Assist app

4.6 REMOVE LOCKSCREEN ICONS

By ticking the checkbox of "**Remove Lockscreen Icon**", the app shortcut on the Lockscreen will be hidden:





To enable this function:

1) Tap the menu button , and tap on "**Options…**".

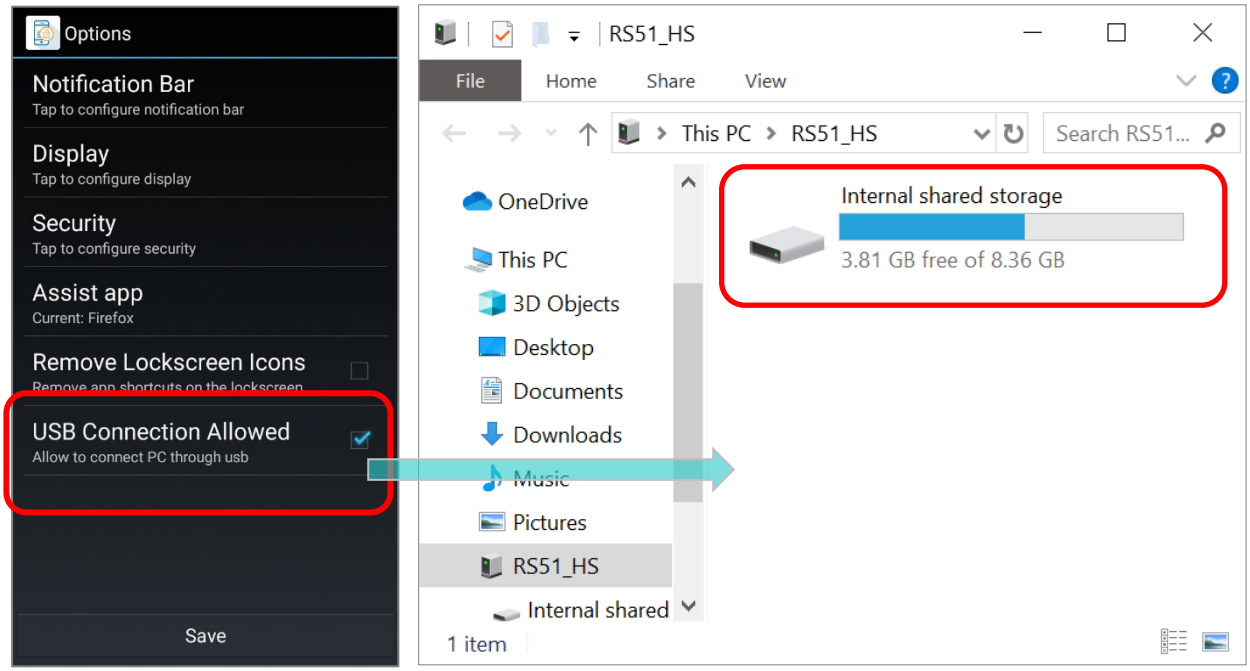
2) Tick "**Remove Lockscreen Icons**".

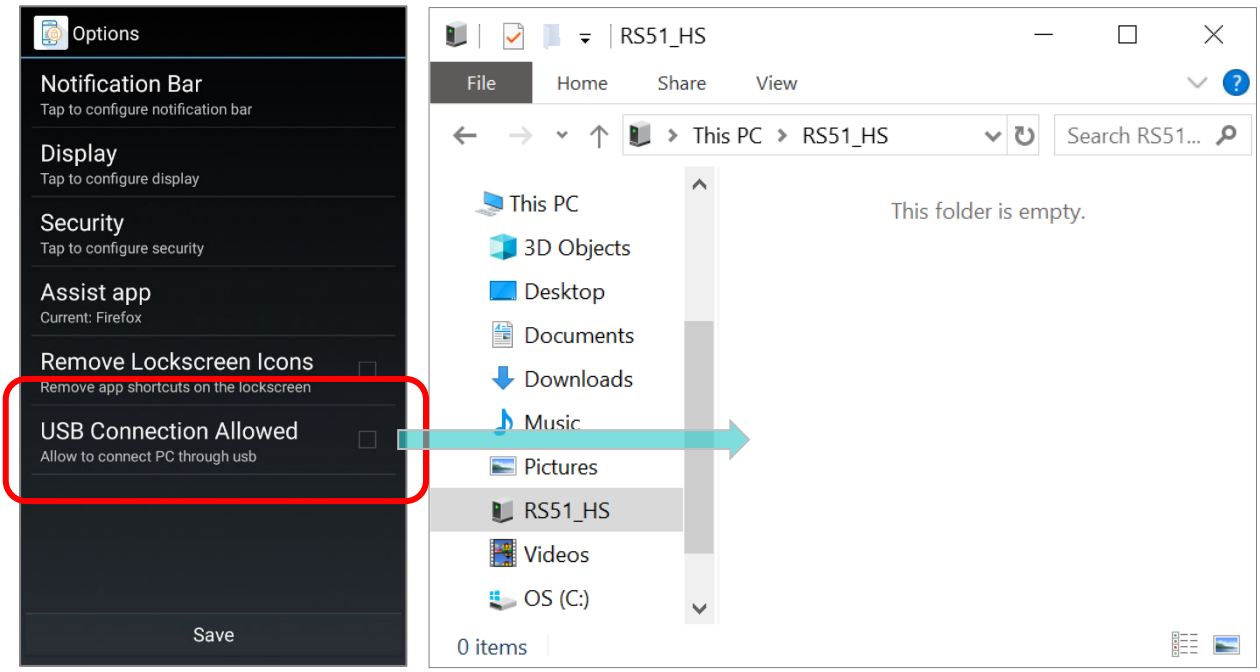
3) Tap "**Save**" to save the setting.

Note: The function "**Remove Lockscreen Icons**" would not be listed in "**Options**" page if it is not supported by the Operating System of your device.

4.7 USB CONNECTION ALLOWED

In user mode, if "**USB Connection Allowed**" is enabled, the storage of the mobile computer is visible from PC client when it is connected with PC by USB cable, whereas it is invisible if "**USB Connection Allowed**" is unticked:





Chapter 5

OTHER FUNCTIONS (ADMINISTRATOR ONLY)

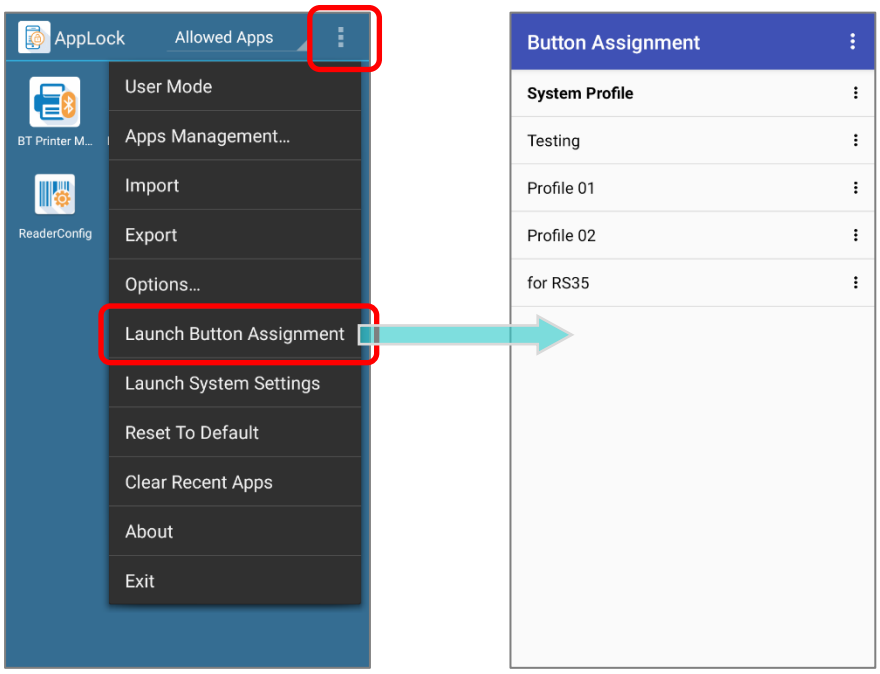
This chapter is about other functions for administrator.

IN THIS CHAPTER

5.1 Launch Button Assignment 101
5.2 Launch System Settings 101
5.3 Reset to Default 102
5.4 Clear Recent Apps 102
5.5 About 102
5.6 Exit 103

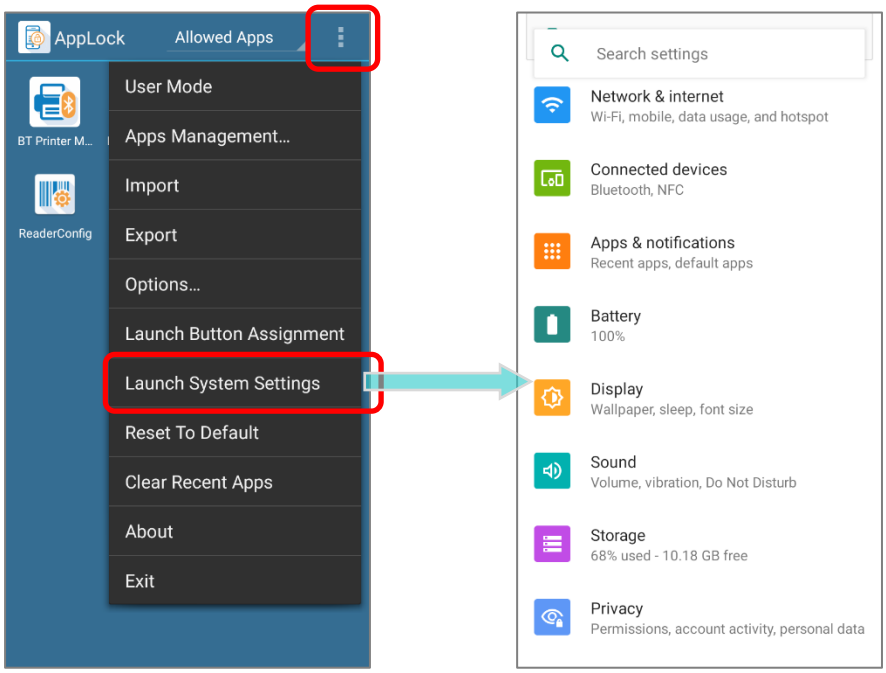
5.1 LAUNCH BUTTON ASSIGNMENT

"**Launch Button Assignment**" is only for RK25, RK95, & RS35. Please tap the menu button ⋮ and then "**Launch Button Assignment**" to launch the built-in application "**Button Assignment**" for redefining the functions of physical keys.



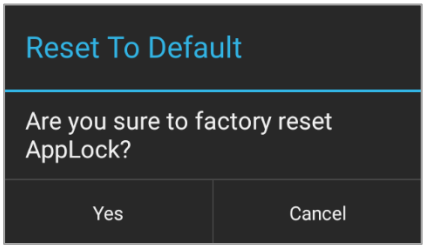
5.2 LAUNCH SYSTEM SETTINGS

To access system settings, tap the menu button ⋮ and then "**Launch System Settings**" to open the system settings menu.



5.3 RESET TO DEFAULT

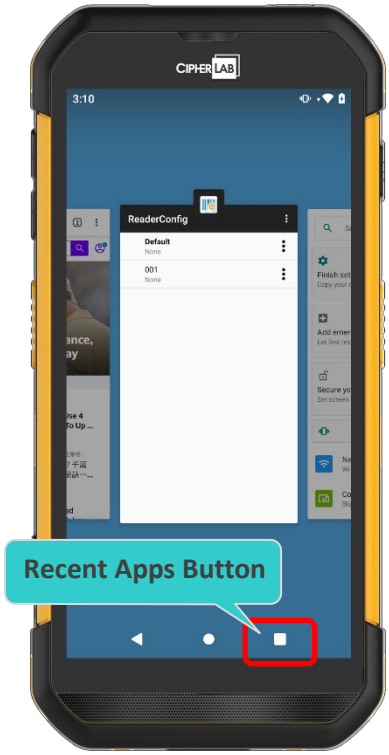
Tap the menu button ⋮ . Tap on “**Reset to Default**” and a dialogue shows. Tap on “**Yes**” to reset AppLock to factory default.



5.4 CLEAR RECENT APPS

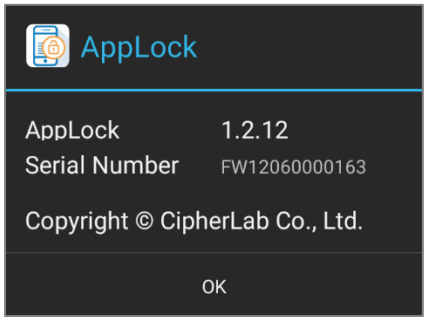
Pressing “**Recent Apps**” button to open a list of recently used applications. You can also tap the menu button ⋮ and then “**Clear Recent Apps**” to erase this record. This can prevent accidentally switching to applications other than the applications available on the Allowed Apps view.

If there are certain applications that you would like to keep in the list, add them to the Recent Apps Whitelist.

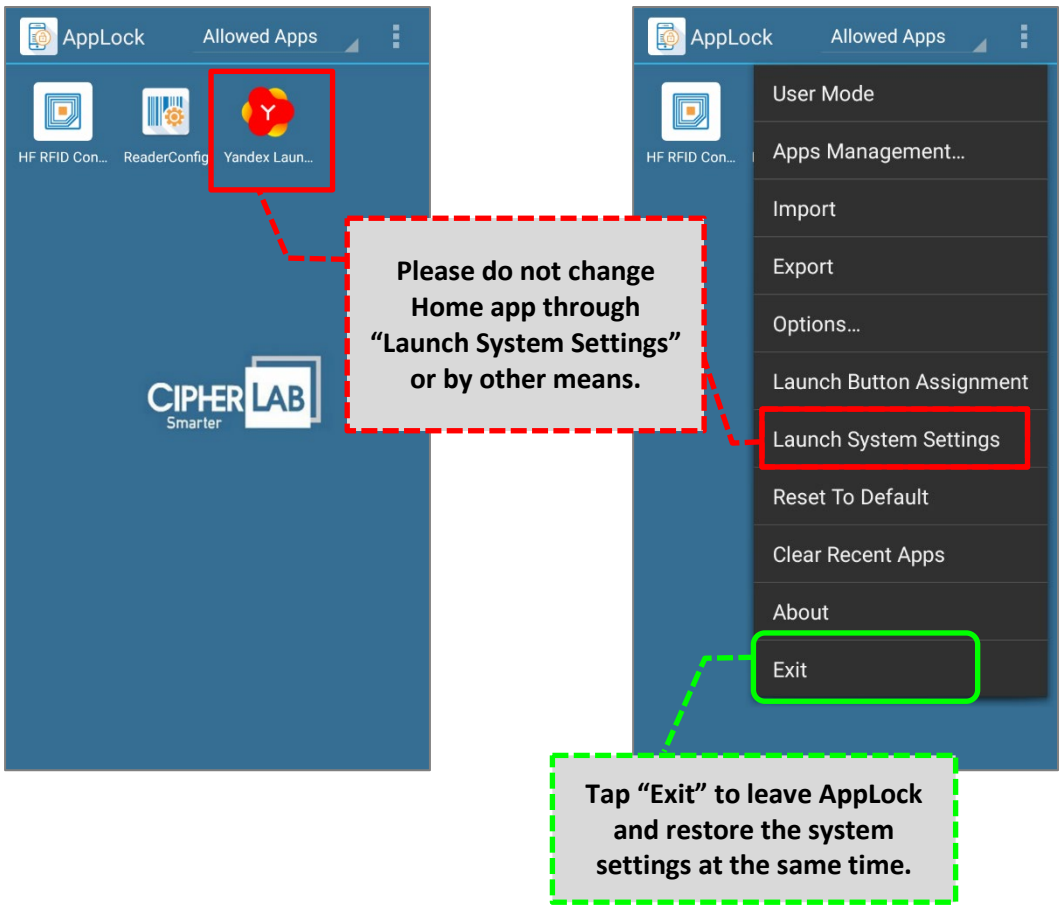


5.5 ABOUT

Tap the menu button ⋮ . Tap on “**About**” to check software version information.



5.6 EXIT

Tap the menu button ⋮ and then "**Exit**" to leave the application.

Changing Home app from AppLock to other launchers through Launch System Settings or by other means may result in some system settings remain as what they are set by AppLock. Thus, if you would like to leave AppLock and change Home app to other launchers, it is strongly suggested that leaving AppLock by tapping "**Exit**" to restore the system settings changed by AppLock to default at the same time.