AppLync Browser User Manual

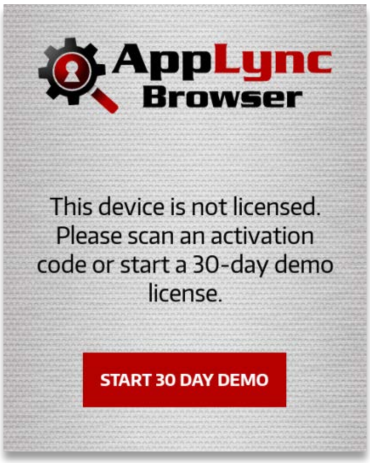
AML

AML Striker
Enterprise Mobile Computer

Contents

1 Get Started

1.1 Licensing



AppLync Browser

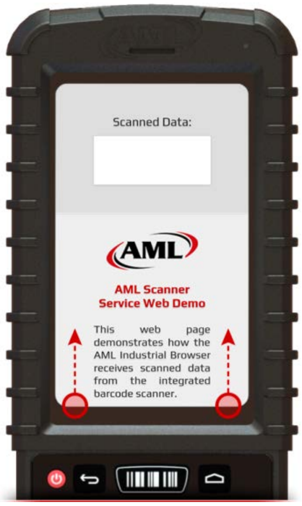
This device is not licensed. Please scan an activation code or start a 30-day demo license.

START 30 DAY DEMO

To get started using the AppLync Browser, users will need to license the device. Users can choose one of two options:

1. Start a 30 Day Demo License by pressing the red button shown in the image to the right.
2. Purchase a license and use an Activation Code, provided by AML, to license AppLync Browser on the device.

1.2 Test Scanner Demo



Scanned Data:

AML

AML Scanner Service Web Demo

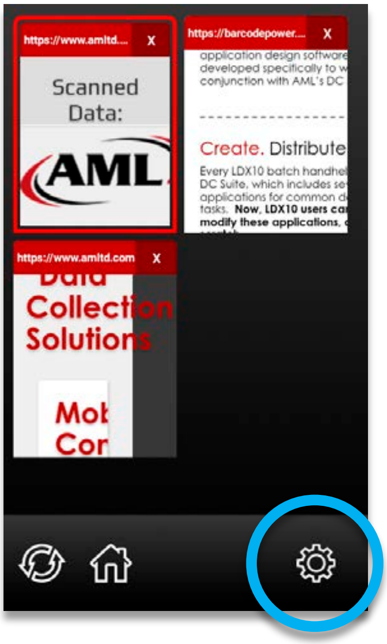
This web page demonstrates how the AML Industrial Browser receives scanned data from the integrated barcode scanner.

Once the device is licensed, users can begin setup. The default homepage is a scanner demo page. To test this page, simply scan a barcode. The white box will be populated by the barcode data.

1.3 Open the Menu

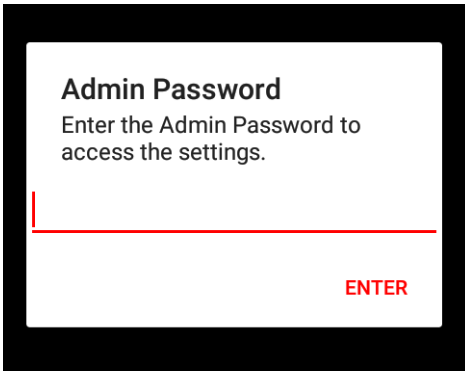
To get started configuring the AppLync Browser, swipe up from the bottom-edge to open the menu.

1.4 Open Settings


https://www.amltd....
X
Scanned Data:
AML
https://barcodepower....
X
application design software developed specifically to w conjunction with AML's DC
Create. Distribute
Every LDX10 batch handhel DC Suite, which includes se applications for common d tasks. Now, LDX10 users ca modify these applications,
https://www.amltd.com
X
Data Collection Solutions
Mob Cor

Select the gear icon in the bottom, right-hand corner of the menu (blue circle).

An Administrative Password prompt will appear. The default password is ‘aml’. Enter the default password and select ‘Enter’.

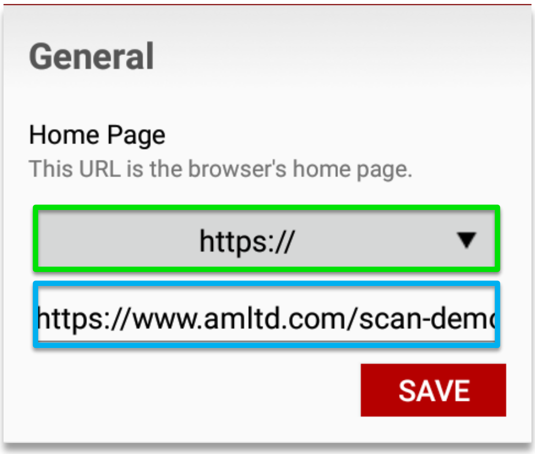


Admin Password

Enter the Admin Password to access the settings.

ENTER

1.5 Set Homepage



General

Home Page

This URL is the browser's home page.

https:// ▼

https://www.amltd.com/scan-dem

Enter the homepage URL for the browser in the text box under the ‘Home Page’ section (blue highlight). The homepage will be the first tab that is opened and loaded when AppLync Browser is launched.

Either tap the drop-down menu to select the protocol (green highlight) or manually enter https:// or http:// at the start of the URL. If no protocol is entered, https:// will automatically be added.

After completing setup, close and restart the app to see the changes.

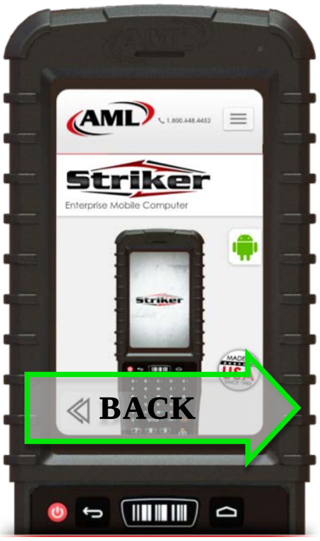
2 Browser Gestures

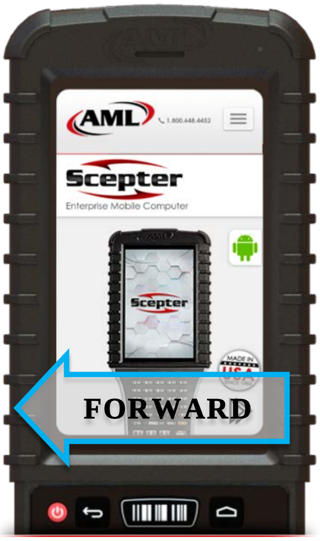
This section describes the various swipe gestures and their respective functions.

2.1 Browser Navigation

To go back and forward in each respective tab’s browsing history, swipe along the bottom-edge of the browser left or right.

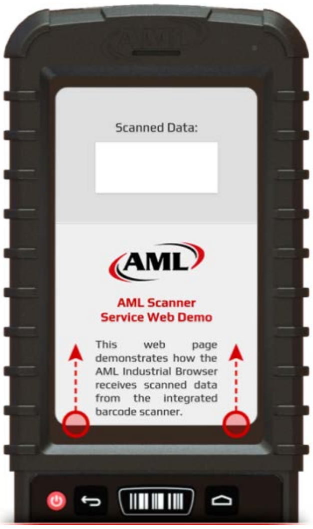
The green arrow indicates gesture area and direction to go back and the blue arrow indicates area and direction to go forward.





2.2 Open Menu

To access AppLync Browser menu, swipe up from the bottom-edge of the browser.



Scanned Data:

AML Scanner Service Web Demo

This web page demonstrates how the AML Industrial Browser receives scanned data from the integrated barcode scanner.

3 Settings

This section describes how to configure each setting in the settings menu.

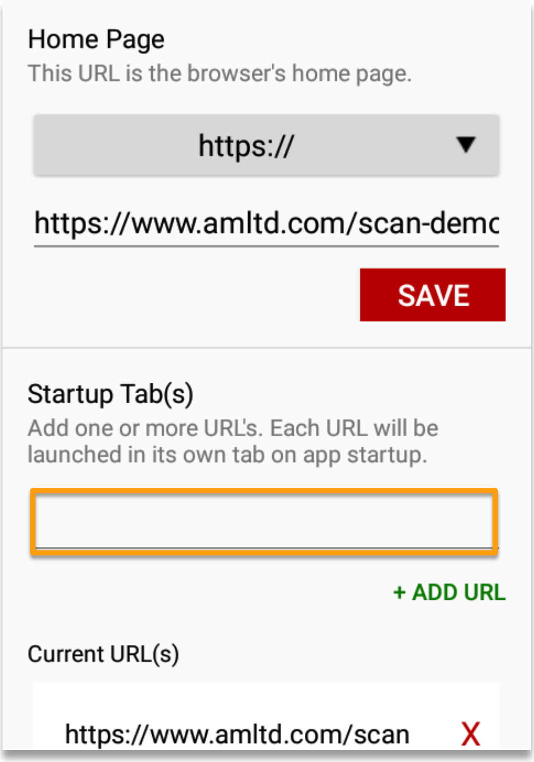
3.1 Homepage

The homepage will be the first tab that is opened and loaded when AppLync Browser is launched. See section **1.5 Set Homepage** for details about how to set this value.

3.2 Startup Tabs

If multiple pages should be loaded on startup, add one or more URL's to the 'Startup Tab(s)' list.

To add tabs, enter the URL to be loaded on startup in the text box under the 'Startup Tab(s)' section (orange highlight). Then, tap the "+ ADD URL" button. Each tab will be added to the list shown below the 'Current URL(s)' title.



Home Page

This URL is the browser's home page.

https://www.amltd.com/scan-demc

Startup Tab(s)

Add one or more URL's. Each URL will be launched in its own tab on app startup.

Current URL(s)

https://www.amltd.com/scan

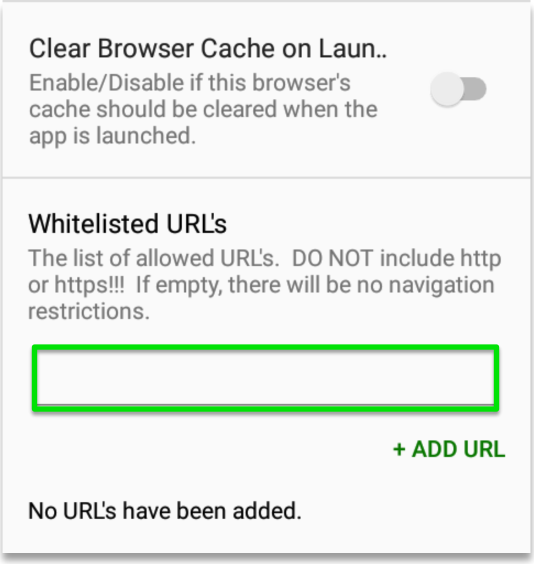
3.3 Clear Browser Cache on Launch

Turn this setting on to clear the browser's image and file cache when the app is launched. Any images or other resources that were previously loaded will be reloaded when the correlating web page is loaded.

3.4 Whitelisted URL's

To prevent users from navigating to web pages outside of any business web application, add a domain or complete URL to this list. ***Note: If no URL's are added to the 'Whitelist', there will be no navigation restrictions.***

To add a URL to the 'Whitelist', enter a domain, partial or complete URL in the text box under the 'Whitelisted URL's' section (green highlight). Then, tap the '+ ADD URL' button to add the entered value to the 'Whitelist'.



Clear Browser Cache on Laun..

Enable/Disable if this browser's cache should be cleared when the app is launched.

Whitelisted URL's

The list of allowed URL's. DO NOT include http or https!!! If empty, there will be no navigation restrictions.

No URL's have been added.

3.4.1 Implied Wildcards

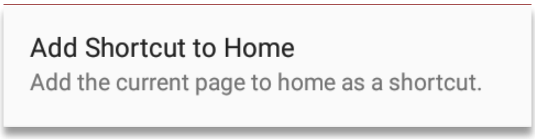
With domains and partial URL's, there is an implied wildcard. ***IMPORTANT: Do not include http or https in the whitelist entries!***

This means that if a user adds 'amltd.com' to the whitelist, then all web pages under that domain will be allowed and all web pages outside of that domain will be blocked.

Also, if a user adds a partial URL such as 'amltd.com/products/', then all web pages under the '/products/' section of the 'amltd.com' domain will be allowed and everything outside of the '/products/' section of the 'amltd.com' domain along with all other domains will be blocked.

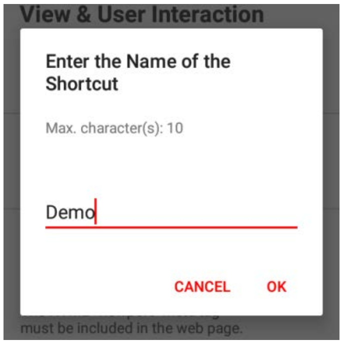
3.5 Add Shortcut to Home

Select this option to add a shortcut for the currently loaded URL to the desktop.



Add Shortcut to Home

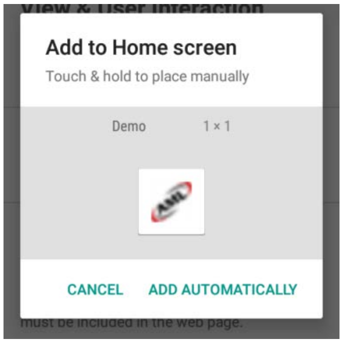
Add the current page to home as a shortcut.



Enter the Name of the Shortcut

Max. character(s): 10

Demo



Add to Home screen

Touch & hold to place manually

Demo 1 × 1

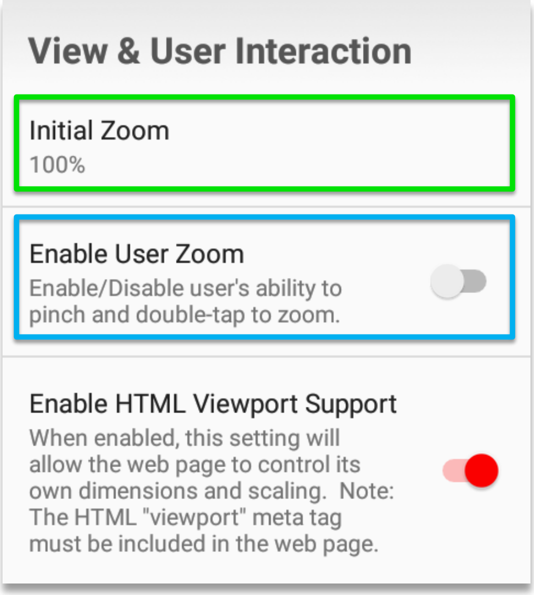
When a user selects this option, a dialog will appear to enter a name for the shortcut.

On the AML Striker with Android Oreo OS, users will be shown a confirmation.

Select 'ADD AUTOMATICALLY' to add the shortcut.

3.6 Initial Zoom

If the loaded web page(s) were designed to fit specific display dimensions, users can set the 'Initial Zoom' to load the page at a specific zoom level. To set the zoom level, tap the 'Initial Zoom' row (green highlight).

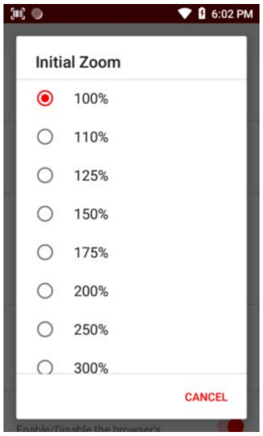


View & User Interaction

Initial Zoom
100%

Enable User Zoom
Enable/Disable user's ability to pinch and double-tap to zoom.

Enable HTML Viewport Support
When enabled, this setting will allow the web page to control its own dimensions and scaling. Note: The HTML "viewport" meta tag must be included in the web page.



Initial Zoom

● 100%
○ 110%
○ 125%
○ 150%
○ 175%
○ 200%
○ 250%
○ 300%

A popup list will appear. Select a preset value or scroll to the bottom of this list to select 'Custom'. If users select, 'Custom' a text box will appear to enter a numeric value.

To "lock- in" the 'Initial Zoom' level, be sure to turn off the 'Enable User Zoom' setting (blue highlight).

3.7 Enable User Zoom

To allow users to pinch to zoom in/out in each tab, enable this setting.

3.8 Enable HTML Viewport Support

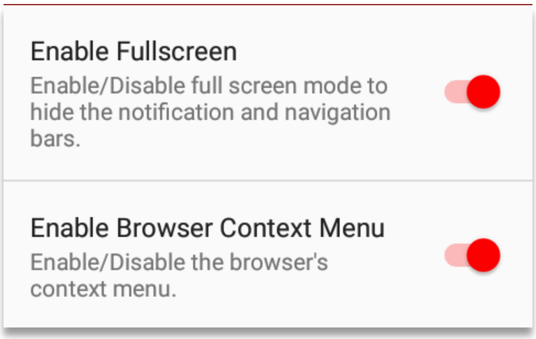
When enabled, this setting will allow any loaded web page to control its own dimensions and scaling with the user of a HTML "viewport" meta tag. This meta tag must be included in the HTML <head> tag of the web page. Note: Enabling support for the viewport meta tag will override the Initial Zoom setting.

3.9 Enable Fullscreen

When enabled, this setting will auto-hide the notification bar at the top of the Android display. The notification bar can still be accessed by swiping down from the top edge of the display.

3.10 Enable Browser Context Menu

When enabled, this setting will allow access to a context menu with options to Select, Copy, Cut and Paste within each tab by tapping and holding until the popup menu appears.



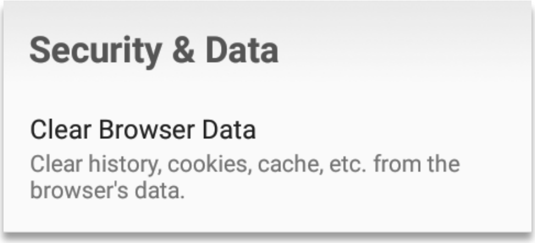
Enable Fullscreen
Enable/Disable full screen mode to hide the notification and navigation bars.

Enable Browser Context Menu
Enable/Disable the browser's context menu.

3.11 Clear Browser Data

This option will allow users to clear data from the browser on demand.

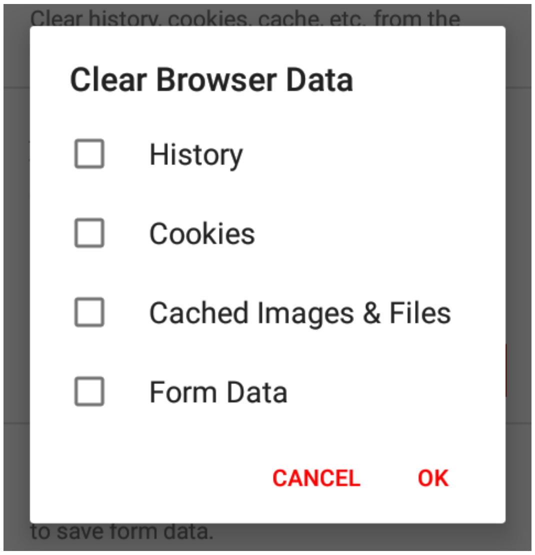
When users select this row a popup with a selection list will appear. Users must choose which data to clear and tap ‘OK’.



Security & Data

Clear Browser Data

Clear history, cookies, cache, etc. from the browser's data.



Clear history, cookies, cache, etc. from the

Clear Browser Data

□ History

□ Cookies

□ Cached Images & Files

□ Form Data

to save form data.

3.12 Admin Password

This setting is the password to access the settings menu. To preview the password, tap the eye icon to the right of the password text box (green highlight).

3.13 Enable Save Form Data

This setting enables the browser to save data entered into web forms.

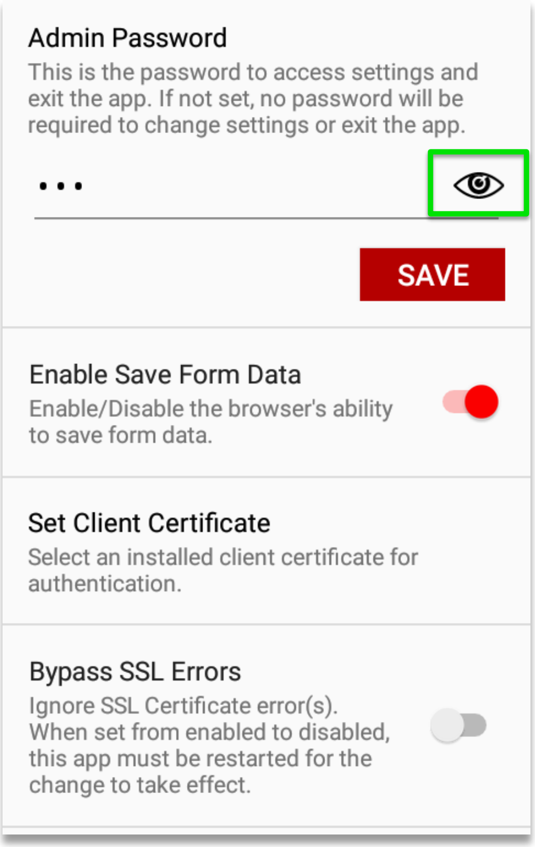
3.14 Set Client Certificate

Select a certificate for authentication. Any certificates to be used in this setting must first be installed on the Android device.

Client Certificate Authentication is a mutual certificate based authentication where the client provides a Client Certificate to a requesting server to prove its identity.

3.15 Bypass SSL Errors

This setting will allow the browser to ignore SSL/certificate errors and load the page.



Admin Password

This is the password to access settings and exit the app. If not set, no password will be required to change settings or exit the app.

•••

Enable Save Form Data

Enable/Disable the browser's ability to save form data.

Set Client Certificate

Select an installed client certificate for authentication.

Bypass SSL Errors

Ignore SSL Certificate error(s). When set from enabled to disabled, this app must be restarted for the change to take effect.

3.16 Database Path

This setting sets the path to where database storage API databases should be saved. In order for the database storage API to function correctly, this method must be called with a path to which the application can write.

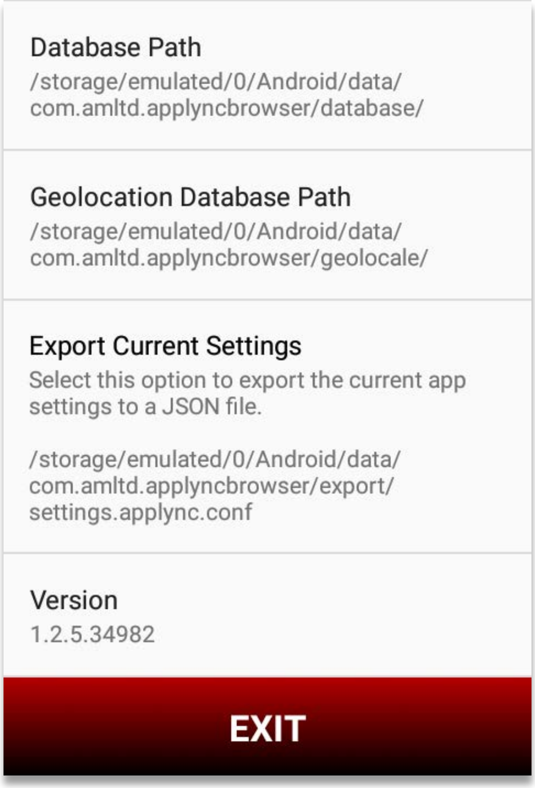
3.17 Geolocation Database Path

This setting sets the path where the Geolocation databases should be saved. In order for Geolocation permissions and cached positions to be persisted, this method must be called with a path to which the application can write.

3.18 Export Current Settings

Select this option to export the current settings to the app data directory.

The export file is located here: "/storage/emulated/0/Android/data/com.amltd.applyncbrowser/export/settings.applync.conf"



Database Path
/storage/emulated/0/Android/data/com.amltd.applyncbrowser/database/

Geolocation Database Path
/storage/emulated/0/Android/data/com.amltd.applyncbrowser/geolocale/

Export Current Settings
Select this option to export the current app settings to a JSON file.

/storage/emulated/0/Android/data/com.amltd.applyncbrowser/export/settings.applync.conf

Version
1.2.5.34982

3.18.1 Download Exported Settings

After connecting the AML device to a PC via USB, open a File Explorer on the PC. Then, navigate to "Internal Shared Storage" → "Android" → "data" → "com.amltd.applyncbrowser". The exported settings file will be titled, "settings.applync.conf". Users can also use a USB drive and insert it into the cradle.

3.19 Version

This is the full version number of the AppLync Browser app.

3.20 Exit

Select this option to exit the settings menu or press 'Back'.

4 Import Settings

To import settings that were previously exported copy the settings file to the app data directory. Then, launch AppLync Browser.

AppLync will import the settings and move the imported file to a ‘config_archive’ directory under the app data directory.

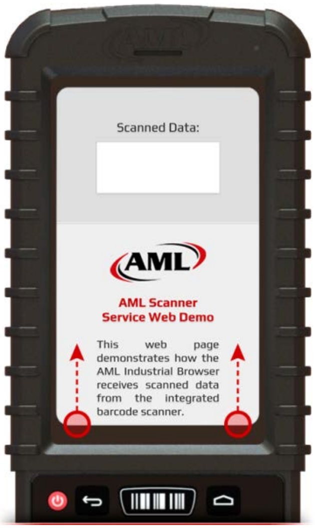
4.1 Placing a Settings File for Import

After connecting the AML device to a PC via USB, open a File Explorer on the PC. Then, navigate to “Internal Shared Storage” → “Android” → “data” → “com.amltd.applyncbrowser”. Place the settings file to be imported here.

Once the settings file is in place launch AppLync Browser to import.

5 Menu

This section describes each option found and how to access the menu.



Scanned Data:

AML Scanner Service Web Demo

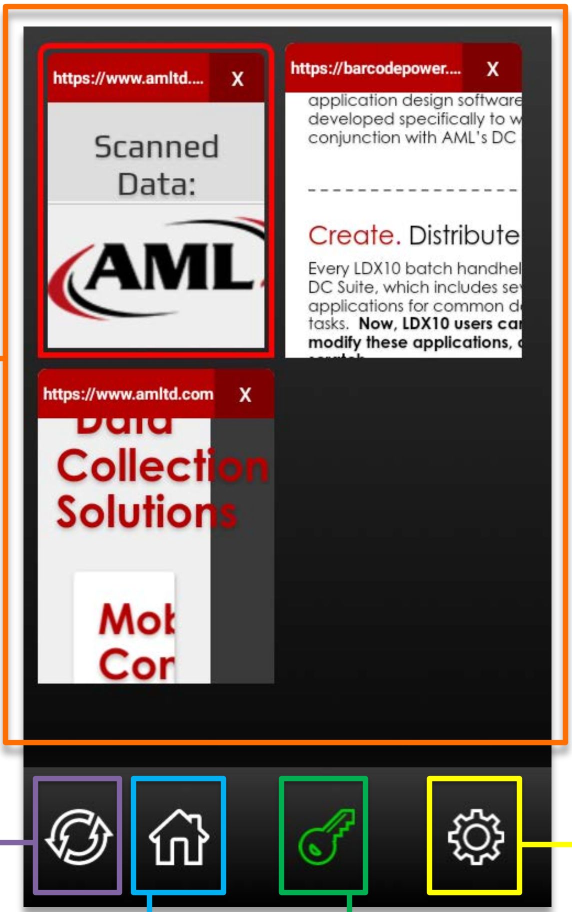
This web page demonstrates how the AML Industrial Browser receives scanned data from the integrated barcode scanner.

5.1 Accessing the Menu

When viewing a browser tab, swipe up from the bottom edge of the display to bring the menu into view.

5.2 Menu Options

Below is a breakdown of each feature found in the browser's menu.



https://www.amltd....
X
Scanned Data:
AML
https://barcodepower....
X
application design software developed specifically to w conjunction with AML's DC
Create. Distribute
Every LDX10 batch handhel DC Suite, which includes se applications for common d tasks. Now, LDX10 users ca modify these applications,
https://www.amltd.com
X
Collection Solutions
Mol Cor

Browser Tab(s) Area
This is a scrollable space that will contain all opened tabs.

The currently selected tab will have a red outline.

Refresh
Refresh the currently selected tab.

Settings
Open the app's settings menu.

Home
This option will load the app's homepage URL in the currently selected tab.

License
When the device has a demo license, this option will appear to allow users to replace the demo license with a full license.

6 Licensing

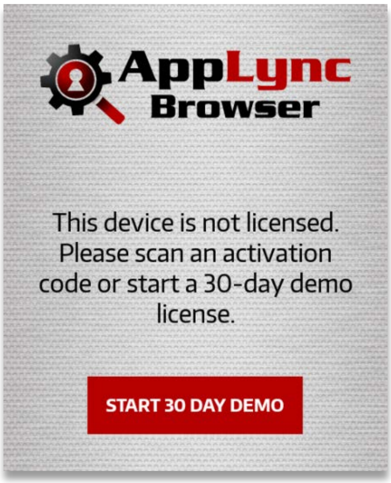
This section describes license types and how to license this app.

6.1 Initial Launch Options

On first launch of the app, AppLync Browser will give the user two licensing options.

1. Tap the button to start a 30 Day Demo license.

2. Scan an Activation Code, which is acquired from AML after purchasing a license.



This device is not licensed. Please scan an activation code or start a 30-day demo license.

6.2 Upgrading from 30 Day Demo License

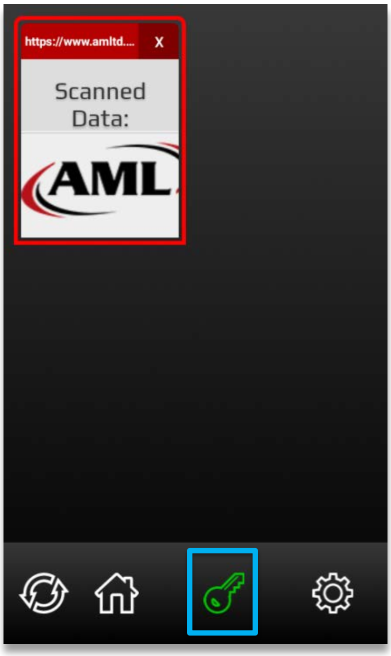
To upgrade the app license from a 30 Day Demo license to a full, perpetual license, users will need to purchase the license from AML. After purchasing the license, users will receive an Activation Code for every license purchased. Each Activation Code will be used once to license each device.

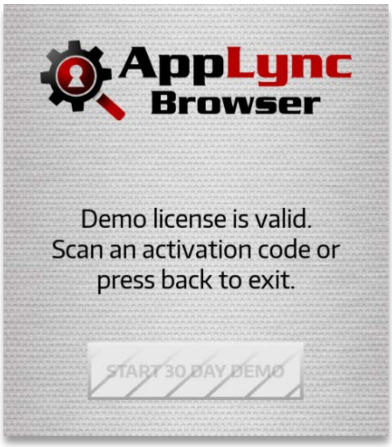
Upgrade from a 30 Day Demo License:

1. Open the app's menu.
   See section **4.1 Accessing the Menu**.

2. In the menu, select the key icon located at the bottom of the menu (blue highlight).

3. The screen below will appear prompting the user to scan an Activation Code to license.





Demo license is valid. Scan an activation code or press back to exit.

7 Get Scanner Data

There are two ways to receive the data from the integrated barcode scanner.

7.1 Keyboard Wedge Mode

When “Keyboard Wedge” is enabled in the AML Barcode Scanner app, the scanner data will be sent to any input field that has focus at the time of scanning a barcode. This method sends the scanned data to the Android system as keyboard input.

7.2 Handle Scanner Data in Javascript

To get the scanner data directly in javascript, simply add the javascript method below to the <head> tag of the web page. Once the data is passed into the method below, users can do what they wish with the data.

Note: In order to implement this javascript method, users must have access and the ability to edit the source code of a given web application.

7.2.1 Javascript Method to Receive Scanner Data

```
function handleScannerData(barcode) {
      if (barcode) {
            barcode = decodeURI(barcode);
            // Execute code here
      }
}
```

8 Revision History

RevA (11-18-2020):

- Initial document.

RevB (11-22-2020):

- Added “Browser Gestures” section.

9 End User License Agreement

The copy of the AppLync Browser and accompanying files ("the Software Product"), are licensed and not sold. The Software Product is protected by copyright laws and treaties, as well as laws and treaties related to other forms of intellectual property. American Microsystems Ltd. or its subsidiaries, affiliates, and suppliers (collectively "AML") own intellectual property rights in the Software Product. The Licensee's ("you" or "your") license to use, copy, or change the Software Product is subject to these rights and to all the terms and conditions of this End User License Agreement ("Agreement").

Acceptance
YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT BY SELECTING THE "I AGREE" OPTION AND INSTALLING, USING, OR COPYING THE SOFTWARE PRODUCT. YOU MUST AGREE TO ALL OF THE TERMS OF THIS AGREEMENT BEFORE YOU WILL BE ALLOWED TO INSTALL THE SOFTWARE PRODUCT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, YOU MUST NOT INSTALL, USE, OR COPY THE SOFTWARE PRODUCT.

License Grant
This Agreement entitles you to install and use the Software Product for AML devices only. Without first obtaining the express written consent of AML, this Agreement does not permit the installation or use of the Software Product for any other device not made by AML.

Restrictions on Transfer
Without first obtaining the express written consent of AML, you may not assign your rights and obligations under this Agreement, or redistribute, encumber, sell, rent, lease, sublicense, or otherwise transfer your rights to the Software Product.

Restrictions on Use
You may not decompile, "reverse-engineer", disassemble, or otherwise attempt to derive the source code for the Software Product.

Restrictions on Alteration
You may not modify the Software Product or create any derivative work of the Software Product or its accompanying documentation. Derivative works include but are not limited to translations. You may not alter any files or libraries in any portion of the Software Product.

Disclaimer of Warranties and Limitation of Liability
UNLESS OTHERWISE EXPLICITLY AGREED TO IN WRITING BY AML, AML MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, IN FACT OR IN LAW, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OTHER THAN AS SET FORTH IN THIS AGREEMENT.

AML makes no warranty that the Software Product will meet your requirements or operate under your specific conditions of use. AML makes no warranty that operation of the Software Product will be secure, error free, or free from interruption. YOU MUST DETERMINE WHETHER THE SOFTWARE PRODUCT SUFFICIENTLY MEETS YOUR REQUIREMENTS FOR SECURITY AND UNINTERRUPTABILITY. YOU BEAR SOLE RESPONSIBILITY AND ALL LIABILITY FOR ANY LOSS INCURRED DUE TO FAILURE OF THE SOFTWARE PRODUCT TO MEET YOUR REQUIREMENTS. AML WILL NOT, UNDER ANY CIRCUMSTANCES, BE RESPONSIBLE OR LIABLE FOR THE LOSS OF DATA ON ANY COMPUTER OR INFORMATION STORAGE DEVICE.

UNDER NO CIRCUMSTANCES SHALL AML, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE TO YOU OR ANY OTHER PARTY FOR INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE, OR EXEMPLARY DAMAGES OF ANY KIND (INCLUDING LOST REVENUES OR PROFITS OR LOSS OF BUSINESS) RESULTING FROM THIS AGREEMENT, OR FROM THE FURNISHING, PERFORMANCE, INSTALLATION, OR USE OF THE SOFTWARE PRODUCT, WHETHER DUE TO A

BREACH OF CONTRACT, BREACH OF WARRANTY, OR THE NEGLIGENCE OF AML OR ANY OTHER PARTY, EVEN IF AML IS ADVISED BEFOREHAND OF THE POSSIBILITY OF SUCH DAMAGES. TO THE EXTENT THAT THE APPLICABLE JURISDICTION LIMITS AML'S ABILITY TO DISCLAIM ANY IMPLIED WARRANTIES, THIS DISCLAIMER SHALL BE EFFECTIVE TO THE MAXIMUM EXTENT PERMITTED.

Limitation of Remedies and Damages
Your remedy for a breach of this Agreement or of any warranty included in this Agreement is the removal of the Software Product. You agree to indemnify and hold AML harmless from all claims, judgments, liabilities, expenses, or costs arising from your breach of this Agreement and/or acts or omissions.

Severability
If any provision of this Agreement shall be held to be invalid or unenforceable, the remainder of this Agreement shall remain in full force and effect. To the extent any express or implied restrictions are not permitted by applicable laws, these express or implied restrictions shall remain in force and effect to the maximum extent permitted by such applicable laws.

AML
2190 Regal Parkway
Euless, Texas 76040

800.648.4452
www.amltd.com