

Contents

Contents.....	2
1 Overview.....	4
1.1 What is AML Setup?	4
1.2 How to use AML Setup?	4
1.3 Who would use AML Setup?	4
2 AML Setup Console.....	5
2.1 Creating a Configuration.....	5
2.2 Network Settings	5
2.2.1 Adding a Network.....	6
2.2.2 Editing a Network.....	6
2.2.3 Deleting a Network	7
2.3 Connected Device Settings	7
2.3.1 Adding a Connected Device	7
2.3.2 Editing a Connected Device	7
2.3.3 Deleting a Connected Device	8
2.4 AML App Settings	8
2.4.1 AML Lockdown.....	8
2.4.2 AML Setup	10
2.4.3 AML Barcode Scanner	11
2.4.4 AppLync	15
2.4.5 AML Clone	19
2.5 MDM Setup Settings.....	20
2.5.1 Generic MDM	20
2.5.2 AirWatch MDM.....	21
2.5.3 Avalanche MDM	22
2.6 File Settings	23
2.6.1 Delete Files.....	23
2.6.2 Download Files	24
2.7 Audio Settings.....	25
2.7.1 Alarm Volume	25
2.7.2 Media Volume.....	25
2.7.3 System Volume	25
2.7.4 Touch Sound Effects	25
2.8 Display Settings	26
2.8.1 Screen Brightness	26
2.8.2 Auto-Screen Brightness	26
2.8.3 Sleep Timer	26

2.8.4	Font Size	26
2.9	Security Settings	27
2.9.1	Screen Lock Pin.....	27
2.9.2	Location Mode	27
2.10	Default App Settings.....	28
2.10.1	Default Home App	28
2.10.2	Default Browser App.....	28
2.11	Connectivity Settings.....	29
2.11.1	Airplane Mode	29
2.11.2	NFC	29
2.11.3	Bluetooth.....	29
2.11.4	Wi-Fi	29
2.11.5	USB Port Mode	29
2.11.6	Ethernet Settings (Firebird)	30
2.12	Date Settings	30
2.12.1	Auto-Time Zone	30
2.13	OS Update Settings.....	31
2.13.1	Update If Needed.....	31
2.13.2	Force Update.....	31
2.13.3	Manual Update	31
2.14	Generating Config Barcodes.....	32
2.15	Generating Config Payload	32
2.16	Managing Configurations	33
2.16.1	Saving Configurations.....	33
2.16.2	Deleting Configurations.....	33
2.16.3	Duplicating Configurations.....	33
2.16.4	Renaming Configurations.....	33
2.16.5	Make Configuration Default	33
2.17	AML Setup Server	34
2.17.1	Server Settings	34
2.17.2	Toggling Server	34
3	AML Setup	35
3.1	Configuration Barcode Method.....	35
3.2	Payload Method	35
3.3	Task History	36
4	Security.....	37
4.1	AML Setup Key	37
End User License Agreement		38

1 Overview

1.1 What is AML Setup?

AML Setup consists of an Android application, AML Setup™, and a desktop application, AML Setup Console™. AML Setup is a device configuration software that allows the user to configure their AML device by scanning configuration barcodes through the AML Barcode Service. AML Setup Console is a desktop application that works in tandem with AML Setup to set up the configuration and barcodes for the AML device that the user wants to configure.

1.2 How to use AML Setup?

To use AML Setup to configure the AML device, use [AML Setup Console](#) to [create a configuration](#) with the desired device settings. Then generate a [configuration barcode](#) or a [configuration payload](#) that can be used by the device to set it up. When you scan the configuration barcode with the device, [AML Setup](#) will open and start displaying the tasks that it is completing. If you are downloading files as part of the configuration, you can use [AML Setup Console Server](#) to host the files on your local PC so the device is able to download them. Optionally, you can host them with a URL.

1.3 Who would use AML Setup?

AML Setup can be used by IT managers to quickly set up their new or existing AML devices.

2 AML Setup Console

2.1 Creating a Configuration

1. Click the Create New button in the left menu.
2. In the create configuration popup, type the name of the configuration you would like to create. Select the checkbox if you would like the configuration to be the default.

Create New Configuration

Enter a new configuration name:

(Characters not allowed in configuration name: \ | : / ? < > " *)

Make this the default configuration?

Create New Configuration

2.2 Network Settings

Network | Connected Devices | Device Apps | Files | Device Settings | OS Update | Generate Config

Network

Select All

guest

Network Name (SSID)

Use as configuration network?
 Connect at the end of configuration?
 Forget other saved networks besides this one?
 Hidden SSID

Security

None

Advanced Options [↗](#)

Add

2.2.1 Adding a Network

1. Enter the Network SSID
2. Select the checkbox for "Use as configuration network?" if you would like this network to be configured before any other task are done in the setup process. Select "Forget network after configuration is complete?" to delete this network after the setup process on the device. Select the checkbox for "Connect at the end of configuration?" if you would like this network to be a persistent network that is connected at the end of the setup process.
3. Select "Forget other saved networks besides this one?" to delete any device networks saved on the device.
4. Select "Hidden SSID" if the network is configured with a hidden SSID.
5. Select the Security type. The options are None, WPA/WPA2 PSK, WEP, and 802.1x EAP.
6. Enter the EAP method if Security type is EAP. The options are PEAP, TLS, TTLS, and PWD.
7. Enter the network password if the network is WPA/WPA2 PSK, WEP, or EAP (PEAP, TTLS, or PWD).
8. Click on the Advanced Options button to open the other network options.
9. Select the Phase 2 Authentication if the network is EAP (PEAP or TTLS).
10. Select the CA Certificate if the network is EAP (PEAP, TLS, or TTLS). The options for the CA Certificate are hosting the file on AML Setup Server or at a URL. To host the file, select the icon to select the certificate from the file browser. To host at a URL, type the URL in the input box. Select the Do Not Validate checkbox if not providing a CA Certificate.
11. Select the User Certificate if the network is EAP (TLS). The options for the User Certificate are hosting the file on AML Setup Server or at a URL. To host the file, select the icon to select the certificate from the file browser. To host at a URL, type the URL in the input box. Select the Do Not Provide checkbox if not providing a User Certificate.
12. Enter the Certificate password if the network is EAP (PEAP, TLS, or TTLS).
13. Enter the Domain if the network is EAP (PEAP, TLS, or TTLS).
14. Enter the Identity if the network is EAP (PEAP, TLS, TTLS, or PWD).
15. Enter the Anonymous Identity if the network is EAP (PEAP or TTLS).
16. Select the IP Settings type. The options are DHCP or Static.
17. Enter the IP Address if Static IP.
18. Enter the Gateway if Static IP.
19. Enter the Network Prefix Length if Static IP.
20. Enter the DNS1 if Static IP.
21. Enter the DNS2 if Static IP.
22. Select the Proxy type. The options are None, Manual, or Proxy Auto-Config.
23. Enter the Proxy hostname if Manual proxy.
24. Enter the Proxy port if Manual proxy.
25. Enter the Bypass proxy if Manual proxy.
26. Enter the PAC URL if Proxy Auto-Config.
27. Click the green OK button to save the network options and close the Advanced Options menu.
28. Click the blue Add button to save the network and add it to the configuration. It should now show up in the Network list on the screen.
29. Make sure the networks checkbox is checked in the network list to make it included in the configuration. To exclude it from the configuration, uncheck the checkbox in the network list.

2.2.2 Editing a Network

1. Hover over the network in the network list and click the Edit button. The input fields should now be populated with that network's information.
2. Edit the networks fields as needed.

3. Click the blue Update button when finished to save the network.

2.2.3 Deleting a Network

1. Hover over the network in the network list and click the Edit button. The input fields should now be populated with that network's information.
2. Click the Delete button to delete the network from the configuration. The network should now disappear from the network list.

2.3 Connected Device Settings

Network Connected Devices Device Apps Files Device Settings OS Update Generate Config

Connected Devices

Select All

bluetoothdevice

Device Name (Bluetooth)

Mac Address

Pin Code Required?

Add

2.3.1 Adding a Connected Device

1. Enter the Device Name.
2. Enter the Mac Address of the device.
3. Select "Pin Code Required?" if the device requires a pin code for pairing.
4. Enter the Pin Code if needed.
5. Click the blue Add button to save the connected device and add it to the configuration. It should now show up in the Connected Devices list on the screen.
6. Make sure the connected devices checkbox is checked in the connected devices list to make it included in the configuration. To exclude it from the configuration, uncheck the checkbox in the connected devices list.

2.3.2 Editing a Connected Device

1. Hover over the connected device in the connected devices list and click the Edit button. The input fields should now be populated with that connected device information.
2. Edit the connected device fields as needed.
3. Click the blue Update button when finished to save the connected device.

2.3.3 Deleting a Connected Device

1. Hover over the connected device in the connected devices list and click the Edit button. The input fields should now be populated with that connected device information.
2. Click the Delete button to delete the connected device from the configuration. The connected device should now disappear from the connected devices list.

2.4 AML App Settings

2.4.1 AML Lockdown

The screenshot shows the 'AML Lockdown Settings' page in a web browser. The navigation bar includes 'Network', 'Connected Devices', 'Device Apps', 'Files', 'Device Settings', 'OS Update', and 'Generate Config'. The sub-navigation bar includes 'AML Lockdown', 'AML Setup', 'AML Barcode Scanner', 'AppLync', 'AML Clone', and 'MDM Setup'. The main content area is titled 'AML Lockdown Settings' and contains the following elements:

- A note: "The AML Setup key will be set to the first four characters of the Lockdown password when the device is in Lockdown mode. This key will need to be included in configurations once it is set."
- A checkbox labeled 'AML Lockdown Password' which is checked. To its right is a password input field containing '*****' and a small icon.
- A checkbox labeled 'AML Lockdown Wallpaper' which is checked. To its right are two radio buttons: 'Default Wallpaper' (unselected) and 'System Wallpaper' (selected).
- A section titled 'Add AML Lockdown Website' with a 'Select All' checkbox (unchecked). It features a list box containing 'google' (checked) and an 'Add' button. To the right of the list box are input fields for 'URL' and 'Label Name'.
- A section titled 'Add AML Lockdown App' with a 'Select All' checkbox (unchecked). It features a list box containing 'Chrome' (checked) and an input field for 'App Friendly Name'.

Setting Lockdown Password

This sets the AML Lockdown password on the device. Users have to enter this password to exit lockdown mode on the device.

1. Click the checkbox to include the AML Lockdown password in the configuration.
2. Click the popup button to open the Lockdown password input.
3. Enter the password in the input field.
4. Click the green OK button to save the AML Lockdown password and add it to the configuration.

Setting Lockdown Wallpaper

This sets the AML Lockdown wallpaper on the device. The options are the default lockdown wallpaper or use system wallpaper.

1. Click the checkbox to include the AML Lockdown wallpaper in the configuration.
2. Select either Default Wallpaper or System Wallpaper.

Setting Lockdown Websites

This configures the AML Lockdown website links that users have access to in lockdown mode.

Adding a Lockdown Website

1. Enter the website URL.
2. Enter the website label name.
3. Click the blue Add button to save the website and add it to the configuration. It should now show up in the lockdown website list on the screen.
4. Make sure the websites checkbox is checked in the lockdown website list to make it included in the configuration. To exclude it from the configuration, uncheck the checkbox in the lockdown website list.

Editing a Lockdown Website

1. Hover over the website in the lockdown website list and click the Edit button. The input fields should now be populated with that website's information.
2. Edit the websites fields as needed.
3. Click the blue Update button when finished to save the website.

Deleting a Lockdown Website

1. Hover over the website in the lockdown website list and click the Edit button. The input fields should now be populated with that website's information.
2. Click the Delete button to delete the website from the configuration. The website should now disappear from the lockdown website list.

Setting Lockdown Apps

This configures the AML Lockdown apps that users have access to in lockdown mode.

Adding a Lockdown App

1. Enter the friendly name. This is whatever the app is named on the device in the installed apps list. For example, the google chrome app is name Chrome.
2. Select the "Set to Auto-Launch on device startup?" to have the app auto launch on device startup in lockdown mode.
3. Click the blue Add button to save the app and add it to the configuration. It should now show up in the lockdown app list on the screen.
4. Make sure the apps checkbox is checked in the lockdown app list to make it included in the configuration. To exclude it from the configuration, uncheck the checkbox in the lockdown app list.

Editing a Lockdown App

1. Hover over the app in the lockdown app list and click the Edit button. The input fields should now be populated with that app's information.
2. Edit the apps fields as needed.
3. Click the blue Update button when finished to save the app.

Deleting a Lockdown App

1. Hover over the app in the lockdown app list and click the Edit button. The input fields should now be populated with that app's information.
2. Click the Delete button to delete the app from the configuration. The app should now disappear from the lockdown app list.

2.4.2 AML Setup

The screenshot shows a web application interface with a navigation bar at the top containing tabs: Network, Connected Devices, Device Apps, Files, Device Settings, OS Update, and Generate Config. Below this is a sub-navigation bar with tabs: AML Lockdown, AML Setup, AML Barcode Scanner, AppLync, AML Clone, and MDM Setup. The main content area is titled "AML Setup Pass Key" with an information icon. It contains two configuration items, each with a checked checkbox, a label, a popup button, and a masked input field (****):

- AML Setup Current Key** [popup] ****
- Set AML Setup Key** [popup] ****

Setting Current Key

This sets the current AML Setup key in the configuration, so it is authorized to complete tasks when used by the device setup.

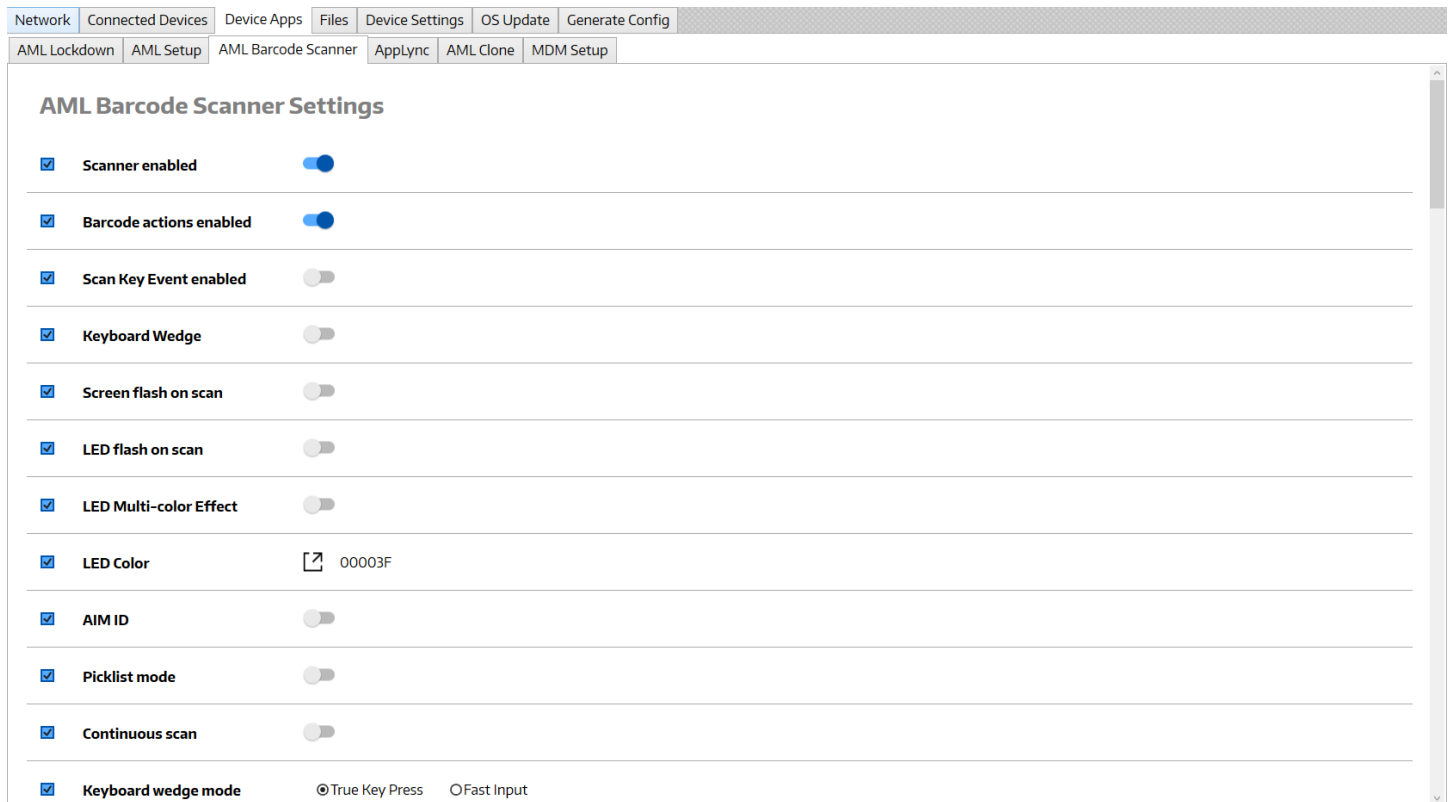
1. Click the checkbox to include the current key in the configuration.
2. Click the popup button to open the key input.
3. Enter the current key.
4. Click the green OK button to save the current key in the configuration.

Setting New Key

This sets a new AML Setup key. This will overwrite the current key if it is authorized.

1. Click the checkbox to include the new key in the configuration.
2. Click the popup button to open the key input.
3. Enter the new key.
4. Click the green OK button to save the new key in the configuration.

2.4.3 AML Barcode Scanner



Scanner

This enables or disables the barcode scanner.

1. Click the checkbox of "Scanner enabled" to include in the configuration.
2. Toggle the switch on or off to enable/disable the scanner.

Barcode Actions

This enables or disables barcode actions on the device. This essentially enables/disables using AML Setup to configure the device.

1. Click the checkbox of "Barcode actions enabled" to include in the configuration.
2. Toggle the switch on or off to enable/disable barcode actions.

Scan Key Event

This enables or disables scan key event mode. Scan key event mode inputs a scan key event every time a barcode is scanned.

1. Click the checkbox of "Scan Key Event enabled" to include in the configuration.
2. Toggle the switch on or off to enable/disable scan key event mode.

Keyboard Wedge

This enables or disables the keyboard wedge.

1. Click the checkbox of "Keyboard Wedge" to include in the configuration.
2. Toggle the switch on or off to enable/disable the keyboard wedge.

Screen Flash on Scan

This enables or disables screen flash on scan mode. Screen flash on scan mode flashes the device screen green on valid scans and red on bad scans.

1. Click the checkbox of "Screen flash on scan" to include in the configuration.
2. Toggle the switch on or off to enable/disable screen flash on scan mode.

LED Flash on Scan (Firebird)

This enable or disables LED flash on scan mode. LED flash on scan mode flashes the LED green on valid scans and red on bad scans. This feature is only for the AML Firebird model.

1. Click the checkbox of "LED flash on scan" to include in the configuration.
2. Toggle the switch on or off to enable/disable LED flash on scan mode.

LED Multi-Color Effect (Firebird)

This enables or disables LED multi-color effect. LED multi-color effect causes the LED light to strobe and constantly change colors. This feature is only for the AML Firebird model.

1. Click the checkbox of "LED Multi-color effect" to include in the configuration.
2. Toggle the switch on or off to enable/disable LED multi-color effect.

LED Color (Firebird)

This sets the LED Color of the device. This feature is only for the AML Firebird model.

1. Click the checkbox of "LED Color" to include in the configuration.
2. Click the popup button to open the color picker.
3. Select the color from the color picker and press the OK button to save the color.

AIM ID

This enables or disables the AIM ID. The AIM ID is the barcode type identifier. If enabled the AIM ID will be returned with the barcode data when each barcode is scanned.

1. Click the checkbox of "AIM ID" to include in the configuration.
2. Toggle the switch on or off to enable/disable AIM ID.

Picklist Mode

This enables or disables picklist mode. If picklist mode is enabled barcodes can only be scanned when the scanner laser is centered on the barcode.

1. Click the checkbox of "Picklist mode" to include in the configuration.
2. Toggle the switch on or off to enable/disable picklist mode.

Debounce Timeout

This sets the debounce timeout for the trigger. The timeout is applied every time the trigger is released.

1. Click the checkbox of “Debounce Timeout” to include in the configuration.
2. Click the popup button to open the input.
3. Enter the timeout from 100 – 2000 in milliseconds and click OK to save the timeout.

Continuous Scan

This enables or disables continuous scan mode. If continuous scan mode is enabled multiple barcodes can be scanned with one trigger pull.

1. Click the checkbox of "Continuous scan" to include in the configuration.
2. Toggle the switch on or off to enable/disable continuous scan mode.

Different Symbol Timeout (Zebra Engines)

This sets the different symbol timeout. This only works when continuous scan mode is enabled.

1. Click the checkbox of "Different Symbol Timeout" to include in the configuration.
2. Click the popup button to open the input.
3. Enter the timeout from 1 – 9999 in milliseconds and click OK to save the timeout.

Decode Timeout (Zebra Engines)

This enables or disables decode timeout. If decode timeout is enabled, a same symbol timeout can be set and used.

1. Click the checkbox of “Decode Timeout” to include in the configuration.
2. Toggle the switch on or off to enable/disable decode timeout.

Same Symbol Timeout (Zebra Engines)

This sets the same symbol timeout. This only works when decode timeout is enabled.

1. Click the checkbox of “Same Symbol Timeout” to include in the configuration.
2. Click the popup button to open the input.
3. Enter the timeout from 0 – 9999 in milliseconds and click OK to save the timeout.

Illumination (Zebra Engines)

This sets the illumination brightness of the scan engine.

1. Click the checkbox of “Illumination” to include in the configuration.
2. Click the popup button to open selection.
3. Select the illumination from the list and click OK to save the timeout. 10 is the brightest.

Allow Manual Configuration

This enables/disables manual scanner configuration. If this is enabled, you can scan manufacturer barcodes to configure the scanner.

1. Click the checkbox of "Allow Manual Configuration" to include in the configuration.
2. Toggle the switch on or off to enable/disable manual configuration.

Keyboard Wedge Mode

This sets the keyboard wedge mode. The options are true key press and fast input modes. True key press sends barcode data to the keyboard wedge one character at a time like actual key presses.

1. Click the checkbox of "Keyboard wedge mode" to include in the configuration.
2. Select the keyboard wedge mode.

Barcode Prefix

This sets the barcode prefix. The barcode prefix will be appended to the beginning of each barcode scan.

1. Click the checkbox of "Barcode Prefix" to include in the configuration.
2. Click the popup button to open the input.
3. Enter the barcode prefix and click OK to save the prefix.

Barcode Suffix

This sets the barcode suffix. The barcode suffix will be appended to the end of each barcode scan.

1. Click the checkbox of "Barcode Suffix" to include in the configuration.
2. Click the popup button to open the input.
3. Enter the barcode suffix and click OK to save the suffix.

Barcode Scan Sound

This sets the barcode scan sound. The scan sound audio is played every time a barcode is scanned.

1. Click the checkbox of "Barcode Scan Sound" to include in the configuration.
2. Click the popup button to open the input.
3. Enter the barcode scan sound name and click OK to save the barcode scan sound. This is the friendly name of the sound on the device in the audio setting ringtones.

Symbologies

This enables or disables barcode symbologies.

1. Click the checkbox of the symbology to enable/disable from the Symbologies list.
2. Toggle the switch of the symbology on or off to enable/disable.

2.4.4 AppLync

The screenshot shows the AppLync configuration interface. At the top, there is a navigation bar with tabs: Network, Connected Devices, Device Apps, Files, Device Settings, OS Update, Generate Config, AML Lockdown, AML Setup, AML Barcode Scanner, AppLync, AML Clone, and MDM Setup. The 'AppLync' tab is selected. Below the navigation bar, the 'General' section is visible. It contains a 'Home Page' checkbox which is checked, with a URL input field containing 'https://google.com'. Below that is a 'Clear Browser Cache on Launch' checkbox which is checked, with a toggle switch to its right. The 'Startup Tab(s)' section has a 'Select All' checkbox which is unchecked. It contains a list of URLs, with 'https://www.yahoo.com' selected. To the right of this list is a 'URL' input field. Below the list are two checkboxes: 'Clear all startup URL's before adding?' and 'Delete selected URL from startup tabs?'. There is an 'Add' button. The 'Whitelisted URL's' section has a 'Select All' checkbox which is unchecked. It contains a list of URLs, with 'https://www.microsoft.com' selected. To the right of this list is a 'URL' input field. Below the list is a checkbox: 'Clear all whitelisted URL's before adding?'.

Home Page

This sets the home page URL. The home page will be opened when clicking the home button in AppLync.

1. Click the checkbox of "Home Page" to include in the configuration.
2. Click the popup button to open input.
3. Enter the home page URL and click OK to save the home page URL.

Clear Browser Cache on Launch

This enable or disables clear browser cache on launch mode. Clear browser cache on launch mode will clear the browser cache every time AppLync is launched.

1. Click the checkbox of "Clear Browser Cache on Launch" to include in the configuration.
2. Toggle the switch on or off to enable/disable clear browser cache on launch mode.

Startup URLs

This configures the startup URLs for AppLync. The startup URLs will start every time AppLync is started.

Adding a Startup URL

1. Enter the website URL.
2. Select "Clear all startup URL's before adding?" to clear other startup URLs besides this one.
3. Select "Delete selected URL from startup tabs?" to delete this URL from the startup URLs.

4. Click the blue Add button to save the website and add it to the configuration. It should now show up in the startup URL list on the screen.
5. Make sure the websites checkbox is checked in the startup URL list to make it included in the configuration. To exclude it from the configuration, uncheck the checkbox in the startup URL list.

Editing a Startup URL

1. Hover over the website in the startup URL list and click the Edit button. The input fields should now be populated with that website's information.
2. Edit the websites fields as needed.
3. Click the blue Update button when finished to save the website.

Deleting a Startup URL

1. Hover over the website in the startup URL list and click the Edit button. The input fields should now be populated with that website's information.
2. Click the Delete button to delete the website from the configuration. The website should now disappear from the startup URL list.

Whitelisted URLs

This configures the whitelisted URLs for AppLync. The whitelisted URLs are the URLs that are allowed to be opened by the user in AppLync.

Adding a Whitelisted URL

1. Enter the website URL.
2. Select "Clear all startup URL's before adding?" to clear other whitelisted URLs besides this one.
3. Select "Delete selected URL from startup tabs?" to delete this URL from the whitelisted URLs.
4. Click the blue Add button to save the website and add it to the configuration. It should now show up in the whitelisted URL list on the screen.
5. Make sure the websites checkbox is checked in the whitelisted URL list to make it included in the configuration. To exclude it from the configuration, uncheck the checkbox in the whitelisted URL list.

Editing a Whitelisted URL

1. Hover over the website in the whitelisted URL list and click the Edit button. The input fields should now be populated with that website's information.
2. Edit the websites fields as needed.
3. Click the blue Update button when finished to save the website.

Deleting a Whitelisted URL

1. Hover over the website in the whitelisted URL list and click the Edit button. The input fields should now be populated with that website's information.
2. Click the Delete button to delete the website from the configuration. The website should now disappear from the whitelisted URL list.

Initial Zoom

This sets the initial zoom of web pages in AppLync. There are options from 25% zoom to 500% zoom.

1. Click the checkbox of "Initial Zoom" to include in the configuration.
2. Click the popup to open input.
3. Click the zoom percentage from the list or click custom to enter a custom zoom amount.
4. Click OK to save the initial zoom value.

User Zoom

This enables or disables user zoom mode.

1. Click the checkbox of "Enable User Zoom" to include in the configuration.
2. Toggle the switch on or off to enable/disable user zoom mode.

Auto-Centering

This enables or disable auto-centering mode.

1. Click the checkbox of "Enable Auto-Centering" to include in the configuration.
2. Toggle the switch on or off to enable/disable auto-centering mode.

Desktop Mode

This enables or disables desktop mode.

1. Click the checkbox of "Enable Desktop Mode" to include in the configuration.
2. Toggle the switch on or off to enable/disable desktop mode.

HTML Viewport Support

This enables or disables HTML Viewport Support.

1. Click the checkbox of "HTML Viewport Support" to include in the configuration.
2. Toggle the switch on or off to enable/disable HTML viewport support.

Lock Notification Bar

This enables or disables lock notification bar mode.

1. Click the checkbox of "Lock Notification Bar" to include in the configuration.
2. Toggle the switch on or off to enable/disable lock notification bar mode.

Browser Context Menu

This enables or disable the browser context menu.

1. Click the checkbox of "Enable Browser Context Menu" to include in the configuration.
2. Toggle the switch on or off to enable/disable the browser context menu.

Clear Browser Data

This clears the AppLync browser data. The options are for clearing history, cookies, cached images and files, and form data.

1. Click the checkbox of "Clear Browser Data" to include in the configuration.
2. Click the popup button to open input.
3. Select which browser data items to clear from the list and click OK to save.

Admin Password

This sets the admin password to be able to change settings in AppLync.

1. Click the checkbox of "Admin Password" to include in the configuration.
2. Click the popup button to open input.
3. Enter the admin password and click OK to save.

Save Passwords

This enables or disables save passwords mode.

1. Click the checkbox of "Save Passwords" to include in the configuration.
2. Toggle the switch on or off to enable/disable save passwords mode.

Save Form Data

This enables or disables save form data mode.

1. Click the checkbox of "Enable Save Form Data" to include in the configuration.
2. Toggle the switch on or off to enable/disable save form data mode.

Client Certificate

This sets the client certificate for AppLync. The certificate can be downloaded with AML Setup Server or from a URL.

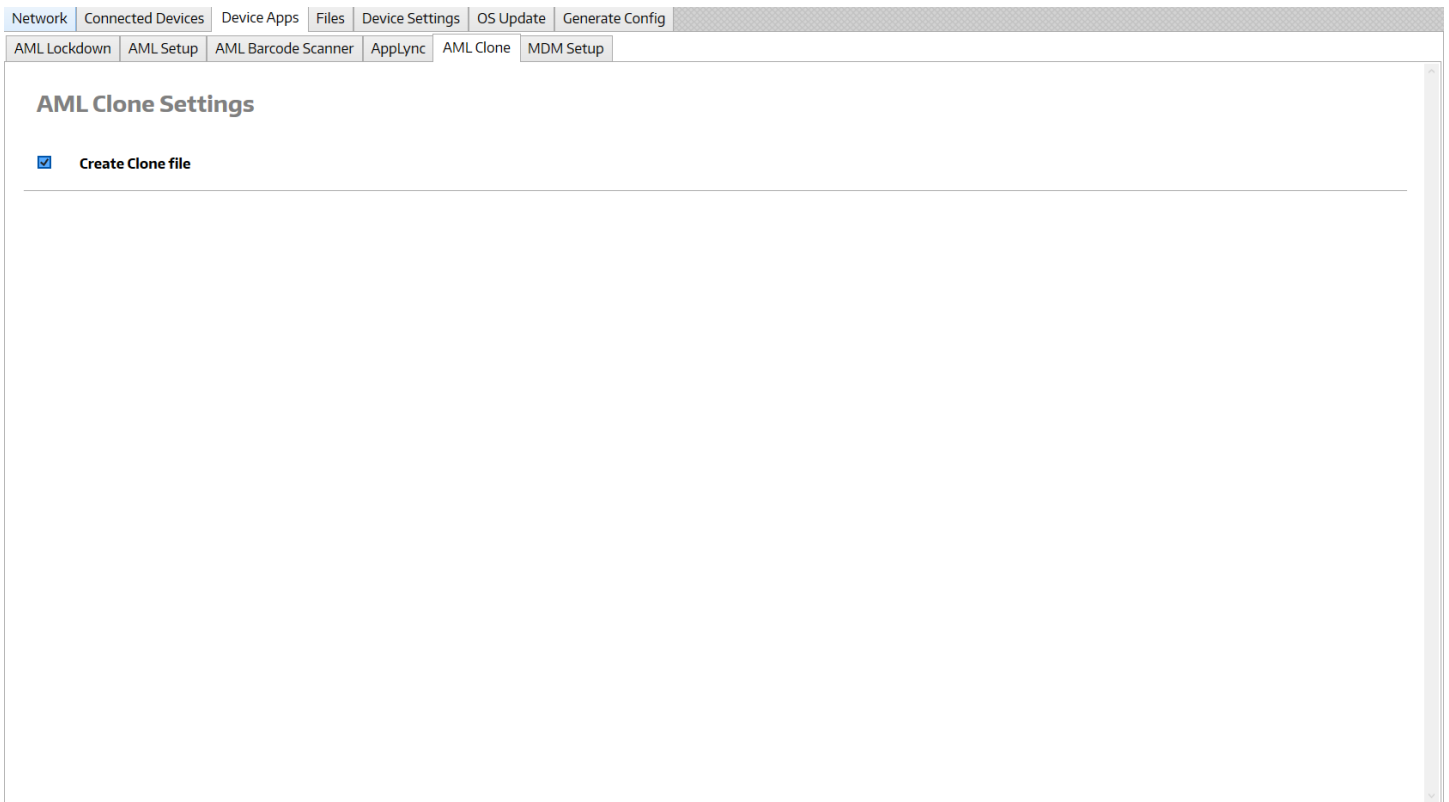
1. Click the popup button to open input.
2. Select the type of download. Options are URL or Local.
3. If the type is URL, enter the URL in the input field.
4. If the type is Local, click the icon to open the file browser and select the certificate.
5. Enter the certificate password in the input field.
6. Click OK to save.

Bypass SSL Errors

This enables or disables bypass SSL errors mode.

1. Click the checkbox of "Bypass SSL Errors" to include in the configuration.
2. Toggle the switch on or off to enable/disable bypass SSL errors mode.

2.4.5 AML Clone



Create Clone File

This creates a clone file of the device and stores it in the downloads folder of the device.

1. Click the checkbox of "Create Clone file" to include in the configuration.

2.5 MDM Setup Settings

2.5.1 Generic MDM

Network | Connected Devices | Device Apps | Files | Device Settings | OS Update | Generate Config

AML Lockdown | AML Setup | AML Barcode Scanner | AppLync | AML Clone | MDM Setup

MDM Type:
Generic

APK Type
 App Name | AMLSetup

Set Device Admin
 Set Device Owner

This sets up a generic MDM from an APK. The options are setting up a already installed application, installing a MDM APK from a URL, or installing a MDM APK from AML Setup Server. The application can be set as device admin and/or device owner.

1. Click the checkbox to include in the configuration.
2. Select "Generic" as the MDM Type.
3. Select the APK Type. The options are URL, Local, or App Name.
4. If APK Type is URL, enter the URL to download the APK in the input field.
5. If APK Type is Local, click the icon to open the file browser and select the APK.
6. If APK Type is App Name, enter the app friendly name in the input field. The app friendly name is the display name of the app on the device under installed applications.
7. Click "Set Device Admin" to set the application as device admin.
8. Click "Set Device Owner" to set the application as device owner.

2.5.2 AirWatch MDM

The screenshot shows the 'MDM Setup' configuration page in the AML Setup application. The 'MDM Type' is set to 'AirWatch'. Under 'APK Type', 'URL' is selected, and the URL 'https://packages.vmware.com/wsone/airwatchagent.apk' is entered. The 'Credentials Type' checkbox is checked, and 'Local' is selected. The file path 'credentials.bin' is entered in the adjacent input field.

This sets up a AirWatch MDM from an APK. The options are downloading the AirWatch APK from a URL or from AML Setup Server. The credentials.bin file for the AirWatch enrollment can be downloaded from a URL or from AML Setup Server.

1. Click the checkbox to include in the configuration.
2. Select "AirWatch" as the MDM Type.
3. Select the APK Type. The options are URL or Local.
4. If APK Type is URL, enter the URL to download the APK in the input field.
5. If APK Type is Local, click the icon to open the file browser and select the APK.
6. Select Credentials Type. The options are URL or Local.
7. If Credentials Type is URL, enter the URL to download the credentials.bin file in the input field.
8. If Credentials Type is Local, click the icon to open the file browser and select the credentials.bin file.

2.5.3 Avalanche MDM

The screenshot shows a web interface for MDM Setup. At the top, there are navigation tabs: Network, Connected Devices, Device Apps, Files, Device Settings, OS Update, and Generate Config. Below these are sub-tabs: AML Lockdown, AML Setup, AML Barcode Scanner, AppLync, AML Clone, and MDM Setup. The main content area is titled 'MDM Type:' and has a dropdown menu set to 'Avalanche'. Below this, there is a section for 'APK Type' with a checked checkbox and a dropdown menu set to 'URL'. To the right of the dropdown is a text input field containing the URL 'https://download.wavelink.com/Files/WLE_Universal_Android_7-1'. Below the URL field are three text input fields: 'Enrollment Id' with the value 'AML', 'Password' with three dots and an eye icon, and 'Server' with the value 'avapoc.ivanticloud.com'. At the bottom of this section is a checked checkbox labeled 'Set as device owner?'. The bottom half of the page is a large empty white space.

This sets up Avalanche MDM from an APK. The options are downloading the Avalanche APK from a URL or from AML Setup Server.

1. Click the checkbox to include in the configuration.
2. Select "Avalanche" as the MDM Type.
3. Select the APK Type. The options are URL or Local.
4. If the APK Type is URL, enter the URL to download the APK in the input field.
5. If APK Type is Local, click the icon to open the file browser and select the APK.
6. Enter the enrollment id of the enrollment rule from Avalanche console.
7. Enter the enrollment password of the enrollment rule from Avalanche console.
8. Enter the enrollment server of the enrollment rule from Avalanche console. This is usually the console URL without the port.
9. Click "Set as device owner?" to make the Avalanche application device owner as well.

2.6 File Settings

2.6.1 Delete Files

The screenshot shows the 'Delete Files' configuration page. At the top, there is a navigation bar with tabs: Network, Connected Devices, Device Apps, Files, Device Settings, OS Update, and Generate Config. The 'Delete Files' section contains the following elements:

- A 'Select All' checkbox.
- A list of files with checkboxes:
 - Downloads/*
 - Images/image.png
- An input field for 'Filepath (ex. Images/ ex. Pictures/ ex. Downloads/)'.
- A checkbox for 'Delete all files in the filepath?'.
- An input field for 'Filename (ex. mydoc.pdf, ex. mypic.jpg)'.
- A blue 'Add' button.

This configures delete files. It is used to delete files on the device. The options are deleting single files, deleting all files in a folder, and deleting files based on a wildcard.

Adding a Delete File

1. Enter the file path location of the file on the device.
2. Select "Delete all files in the file path?" to delete all the files in that file path.
3. Enter the filename if a specific file or wildcard to delete based on a structure. For example, to delete all .jpg files, enter *.jpg for the filename.
4. Click the blue Add button to save the delete file and add it to the configuration. It should now show up in the delete file list on the screen.
5. Make sure the delete files checkbox is checked in the delete file list to make it included in the configuration. To exclude it from the configuration, uncheck the checkbox in the delete file list.

Editing a Delete File

1. Hover over the delete file in the delete file list and click the Edit button. The input fields should now be populated with that delete files information.
2. Edit the delete files fields as needed.
3. Click the blue Update button when finished to save the delete file.

Deleting a Delete File

1. Hover over the delete file in the delete file list and click the Edit button. The input fields should now be populated with that delete files information.
2. Click the Delete button to delete the delete file from the configuration. The delete file should now disappear from the delete file list.


2.6.2 Download Files

Download Files

Get started by selecting the "Type" of download. Select "Local" to download from the AML Setup Server, or select "URL" to download from a web address (http/https). Then, select a file from your device or enter a download URL.

Type

Set image as system wallpaper?
File path on the device: (ex. Images/ ex. Pictures/ ex. Downloads/)

Include device download filepath? 

+ Add

Select All

- my.apk
- my.jpg
- aml-setup.pdf

This configures download files. It is used to download files to the device. The options are downloading files from a URL or the AML Setup Server. Image files can be downloaded and set as the system wallpaper. A specific file path can be chosen for the files. APK files will be downloaded and installed on the device. Clone files will be downloaded, and the device will be cloned.

Adding a Download File

1. Select the download type. The options are URL or Local.
2. If download type is URL, enter the URL to download the file from in the input field.
3. If download type is Local, click the icon to open the file browser and select the file.
4. Click "Set image as system wallpaper?" if the file is an image and needs to be set as the system wallpaper after downloading.
5. Click "Include device download file path?" to enter a specific file path to download the file to.
6. Click the blue Add button to save the download file and add it to the configuration. It should now show up in the download file list on the screen.
7. Make sure the download files checkbox is checked in the download file list to make it included in the configuration. To exclude it from the configuration, uncheck the checkbox in the download file list.

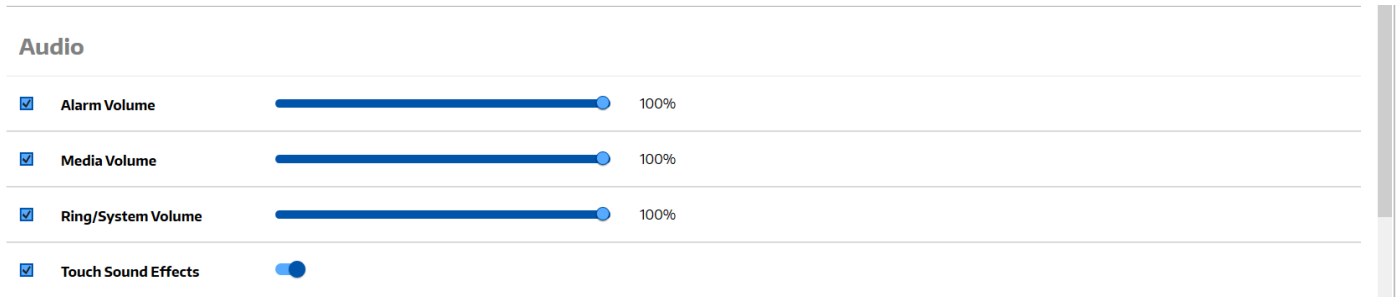
Editing a Download File

1. Hover over the download file in the download file list and click the Edit button. The input fields should now be populated with that download files information.
2. Edit the download files fields as needed.
3. Click the blue Update button when finished to save the download file.

Deleting a Download File

1. Hover over the download file in the download file list and click the Edit button. The input fields should now be populated with that download files information.
2. Click the Delete button to delete the download file from the configuration. The download file should now disappear from the download file list.

2.7 Audio Settings



2.7.1 Alarm Volume

This sets the device alarm volume.

1. Click the checkbox for "Alarm Volume" to include in the configuration.
2. Toggle the slider to the correct volume percentage.

2.7.2 Media Volume

This sets the device media volume.

1. Click the checkbox for "Media Volume" to include in the configuration.
2. Toggle the slider to the correct volume percentage.

2.7.3 System Volume

This sets the device system volume.

1. Click the checkbox for "System Volume" to include in the configuration.
2. Toggle the slider to the correct volume percentage.

2.7.4 Touch Sound Effects

This enables or disables touch sound effects.

1. Click the checkbox for "Touch Sound Effects" to include in the configuration.
2. Toggle the switch on or off to enable/disable touch sound effects.

2.8 Display Settings

The screenshot shows a 'Display' settings menu with four items, each with a checked checkbox:

- Screen Brightness:** A horizontal slider is positioned at the far right, labeled '100%'.
- Auto-Screen Brightness:** A toggle switch is in the 'off' position.
- Sleep Timer:** A popup button (square with an 'x') is shown next to the text 'Never'.
- Font Size:** A horizontal slider is positioned at the far left, labeled 'Default'.

2.8.1 Screen Brightness

This sets the device screen brightness.

1. Click the checkbox for "Screen Brightness" to include in the configuration.
2. Toggle the slider to the correct brightness percentage.

2.8.2 Auto-Screen Brightness

This enables or disables auto-screen brightness.

1. Click the checkbox for "Auto-Screen Brightness" to include in the configuration.
2. Toggle the switch on or off to enable/disable auto-screen brightness.

2.8.3 Sleep Timer

This sets the device screen sleep timer.

1. Click the checkbox for "Sleep Timer" to include in the configuration.
2. Click the popup button to open input.
3. Select the device sleep timer value from the list and click OK to save.

2.8.4 Font Size

This sets the devices text font size.

1. Click the checkbox for "Font Size" to include in the configuration.
2. Toggle the slider to the correct font size value.

2.9 Security Settings

Security & Location

Screen Lock Password/Pin ****

Location Mode

2.9.1 Screen Lock Pin

This sets the device screen lock password/pin.

1. Click the checkbox for "Screen Lock Password/Pin" to include in the configuration.
2. Click the popup button to open input.
3. Enter the screen lock pin and click OK to save.



2.9.2 Location Mode

This enables or disables location mode.

1. Click the checkbox for "Location Mode" to include in the configuration.
2. Toggle the switch on or off to enable/disable location mode.

2.10 Default App Settings

Default Apps

<input checked="" type="checkbox"/>	Default Home App		AML Lockdown
<input checked="" type="checkbox"/>	Default Browser App		Chrome

2.10.1 Default Home App

This sets the device default home app. The default home app is launched on device startup and any time the home key is pressed.

1. Click the checkbox for "Default Home App" to include in the configuration.
2. Click the popup button to open input.
3. Enter the app friendly name to set as the default home app. This is the app display name of the app from the installed apps list on the device. For instance, the AML Lockdown app friendly name is AML Lockdown.

2.10.2 Default Browser App

This sets the device default browser app. The default browser app is launched for any URL.

1. Click the checkbox for "Default Browser App" to include in the configuration.
2. Click the popup button to open input.
3. Enter the app friendly name to set as the default home app. This is the app display name of the app from the installed apps list on the device. For instance, the google chrome app friendly name is Chrome.

2.11 Connectivity Settings

Connectivity

<input checked="" type="checkbox"/>	Airplane Mode	<input type="checkbox"/>
<input checked="" type="checkbox"/>	NFC	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Bluetooth	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Wi-Fi	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	USB Port Mode	<input checked="" type="radio"/> USB Port Computer <input type="radio"/> USB Port Device (Ethernet)
<input checked="" type="checkbox"/>	Ethernet Settings	<input type="checkbox"/> DHCP

2.11.1 Airplane Mode

This enables or disables airplane mode.

1. Click the checkbox for "Airplane Mode" to include in the configuration.
2. Toggle the switch on or off to enable/disable airplane mode.

2.11.2 NFC

This enables or disables the device NFC reader.

1. Click the checkbox for "NFC" to include in the configuration.
2. Toggle the switch on or off to enable/disable NFC.

2.11.3 Bluetooth

This enables or disables Bluetooth.

1. Click the checkbox for "Bluetooth" to include in the configuration.
2. Toggle the switch on or off to enable/disable Bluetooth.

2.11.4 Wi-Fi

This enable or disables Wi-Fi.

1. Click the checkbox for "Wi-Fi" to include in the configuration.
2. Toggle the switch on or off to enable/disable Wi-Fi.

2.11.5 USB Port Mode

This sets the device USB Port Mode. The options are USB Port Computer or USB Port Device (Ethernet).

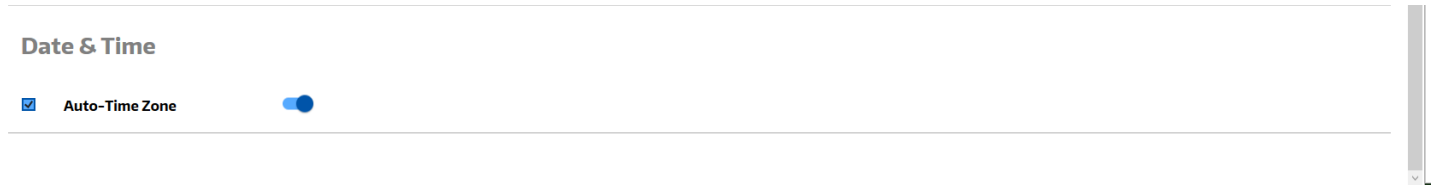
1. Click the checkbox for "USB Port Mode" to include in the configuration.
2. Select the USB port mode.

2.11.6 Ethernet Settings (Firebird)

This configures the device ethernet settings. The options are DHCP or Static. For the Firebird model only.

1. Click the checkbox for "Ethernet Settings" to include in the configuration.
2. Click the popup button to open input.
3. Select the ethernet IP mode. The options are DHCP or Static.
4. If Static, enter in the Ip address, gateway, network mask, DNS1, and DNS2.
5. Click the OK button to save.

2.12 Date Settings



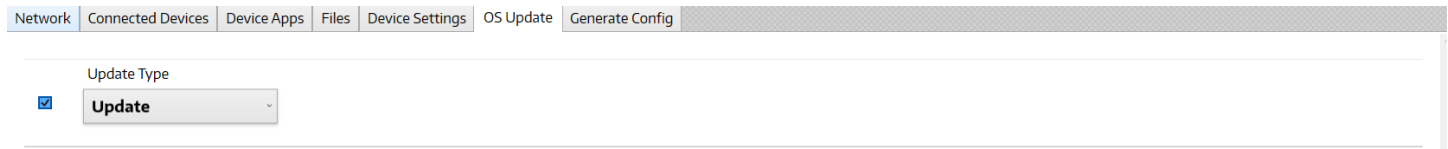
2.12.1 Auto-Time Zone

This enables or disables auto-time zone.

1. Click the checkbox for "Auto-Time Zone" to include in the configuration.
2. Toggle the switch on or off to enable/disable auto-time zone.

2.13 OS Update Settings

2.13.1 Update If Needed

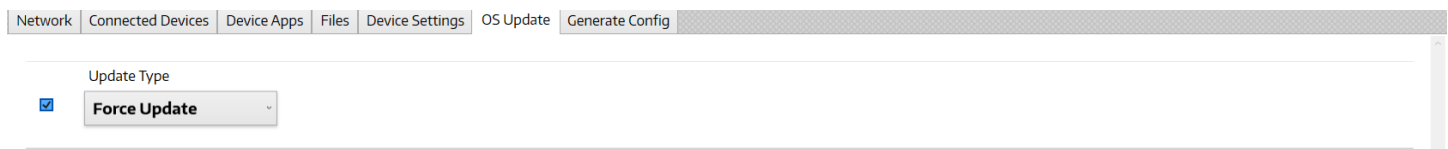


The screenshot shows a navigation bar with tabs: Network, Connected Devices, Device Apps, Files, Device Settings, OS Update, and Generate Config. Below the navigation bar, there is a section titled 'Update Type' with a checked checkbox and a dropdown menu set to 'Update'.

This has the device update its OS if not on the latest version.

1. Click the checkbox to include in the configuration.
2. Select "Update" for the Update Type.

2.13.2 Force Update

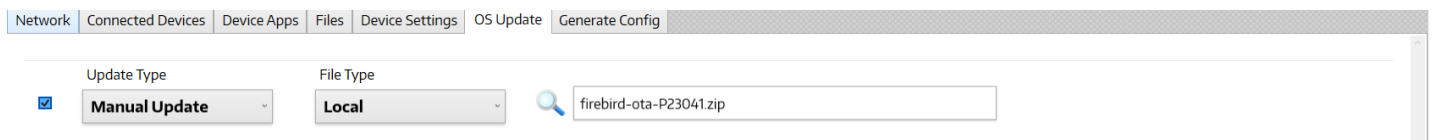


The screenshot shows a navigation bar with tabs: Network, Connected Devices, Device Apps, Files, Device Settings, OS Update, and Generate Config. Below the navigation bar, there is a section titled 'Update Type' with a checked checkbox and a dropdown menu set to 'Force Update'.

This has the device update its OS to the latest version no matter what.

1. Click the checkbox to include in the configuration.
2. Select "Force Update" for the Update Type.

2.13.3 Manual Update



The screenshot shows a navigation bar with tabs: Network, Connected Devices, Device Apps, Files, Device Settings, OS Update, and Generate Config. Below the navigation bar, there are three fields: 'Update Type' with a checked checkbox and a dropdown set to 'Manual Update', 'File Type' with a dropdown set to 'Local', and a text input field containing 'firebird-ota-P23041.zip' with a search icon to its left.

This has the device update its OS from an OTA zip file that is either downloaded from a URL or AML Setup Server.

1. Click the checkbox to include in the configuration.
2. Select "Manual Update" for the Update Type.
3. Select Local or URL for the File Type.
4. If Local, click the icon to open the file browser and select the OTA zip file.
5. If URL, enter the URL to download the OTA zip file from.

2.14 Generating Config Barcodes

Current Configuration: Device Configuration

Network Connected Devices Device Apps Files Device Settings OS Update Generate Config

Config Barcode(s)

Barcode Type

2-D 1-D

Configuration Type

Server Manual

Generate PDF

Config Payload

Payload Schedule:

Date

Select a date [15]

Time

00:00 09:00 23:59

Generate Payload

2-D Config Manual

Barcode Contents: %6@%6/
[CPW:76R26OVFWNMIM0-B9CCOVv+""FD1""P Downloads/N DA 1""FD1""P images/N image.png,DA
0""NPK0""https://www.aml.com/my.ack""DF 0""https://www.aml.com/my.jpg,P:Pictures/
Wallpapers/""DF1""92 168 100 126 aml-setup.pdf,AL14""T.U.R.I.U https://aml.com/
cert.pls,N cert.pls,P:9p9k9899/P:PRWB838k-VUg+""AL10""H LK C L F T LCK2""L.google.U https://
www.google.com""LCK3""N.Chrome.L.true""LCK3""N.google.L.false""SWP""my.jpg""Wifi 1""1.Open.S.guest""
BT""M 123456789101N.bluetooth.device:P-Bos3qDvzpk8700kQXjy90w--""SU0""U https://
www.yahoo.com.D.O.C.O""AL3""U https://
www.microsoft.com.D.O.C.O""B0""1""W0""1""B50""SE:1.SKE:0.KW:0.SF:0.LF:0.AIO:PL:0.CS:0.KWM:truekey
:BP:;BS:1.PS:Pbde

1. Click the green Save Configuration button to save all items in the configuration. This will regenerate the configuration barcode.
2. Select the Barcode Type. The options are 2-D Manual, 2-D Server, 1-D Manual, and 1-D Server.
3. Click the blue Generate PDF button. The PDF application should open with a PDF file that has the configuration barcodes in it. You can print this PDF file and scan the configuration barcode any time you need to set up a device.

NOTE: If you are using AML Setup Server to host files, make sure you set up and enable the server. See the instructions [here](#).

2.15 Generating Config Payload

Current Configuration: Device Configuration

Network Connected Devices Device Apps Files Device Settings OS Update Generate Config

Config Barcode(s)

Barcode Type

2-D 1-D

Configuration Type

Server Manual

Generate PDF

Config Payload

Payload Schedule:

Date

2/16/2023 [15]

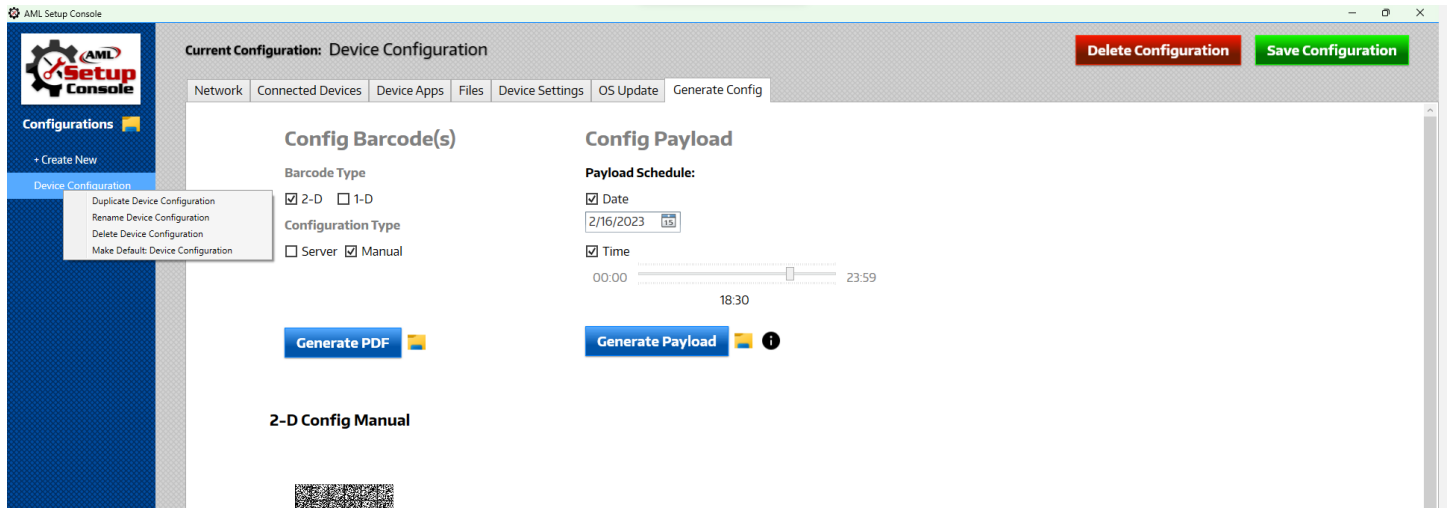
Time

00:00 18:30 23:59

Generate Payload

1. Click the green Save Configuration button to save all items in the configuration.
2. Select the Date and/or Time checkboxes to set a specific time to run the payload on the device (**Optional**).
3. Click the blue Generate Payload button. A file browser should open at the location of the generated payload zip file. Put this zip file on the device at the file path `/sdcard/Android/data/com.amltd.amlsetup/config/`. The payload will be processed at the date and time specified or within five minutes if no date/time was selected.

2.16 Managing Configurations



2.16.1 Saving Configurations

While in a configuration, click the green Save Configuration button to save it.

2.16.2 Deleting Configurations

While in a configuration, click the red Delete Configuration button to delete it. You can also right click on the configuration in the configurations panel menu and click Delete Device Configuration.

2.16.3 Duplicating Configurations

Configurations can be duplicated by right clicking the configuration in the configurations panel menu and selecting Duplicate Device Configuration.

2.16.4 Renaming Configurations

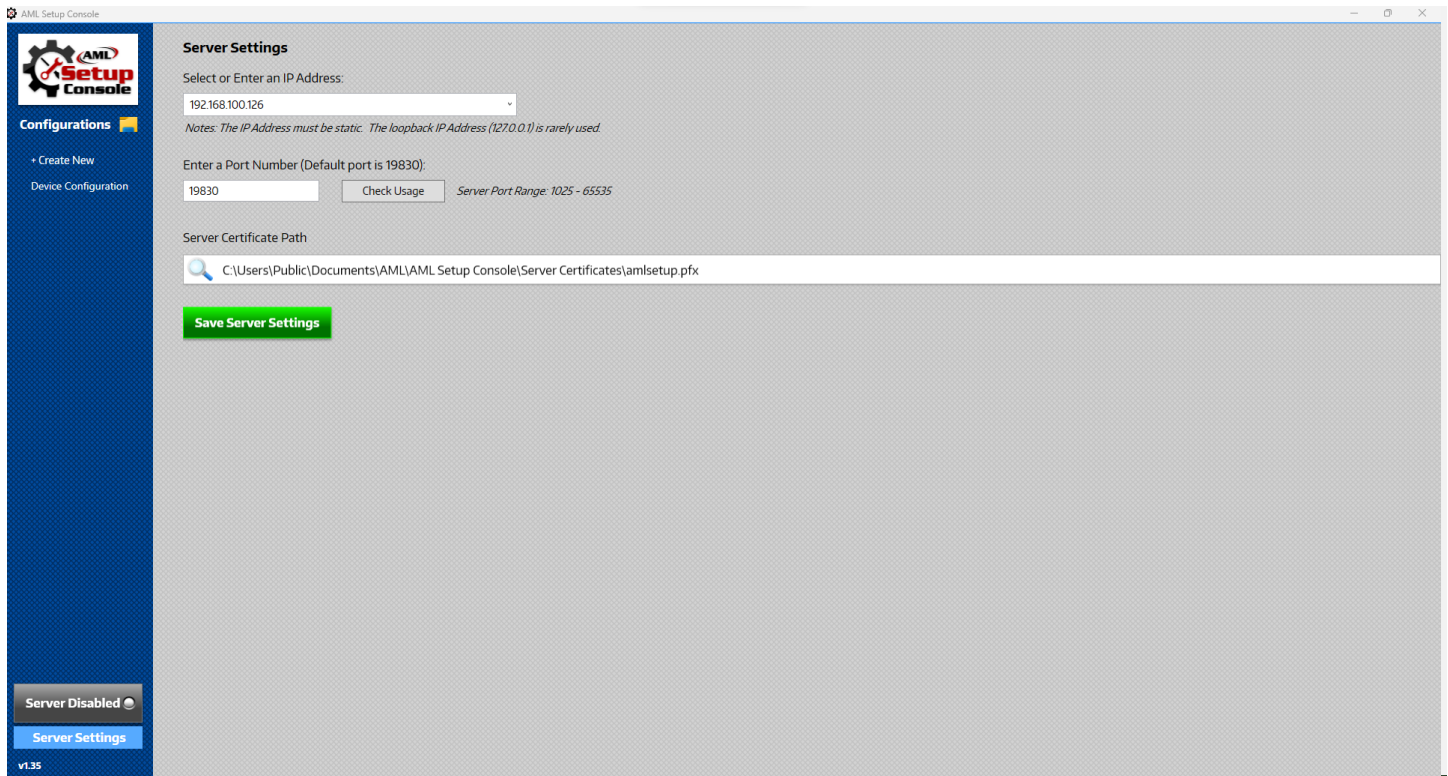
Configurations can be renamed by right clicking the configuration in the configurations panel menu and selecting Rename Device Configuration.

2.16.5 Make Configuration Default

Configurations can be made the default configuration by right clicking the configuration in the configurations panel menu and selecting Make Default Device Configuration.

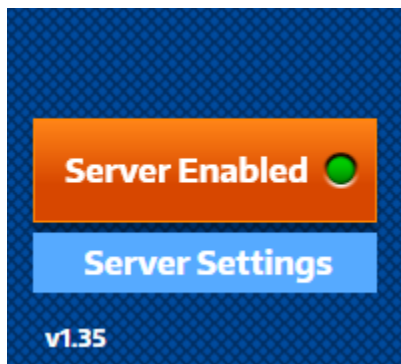
2.17 AML Setup Server

2.17.1 Server Settings



1. Select the network IP address from the IP address list.
2. Enter a port number or leave the default 19830 port.
3. Select a server certificate or leave the default server certificate that is included with AML Setup Console.
4. Click the Save Server Settings button.

2.17.2 Toggling Server



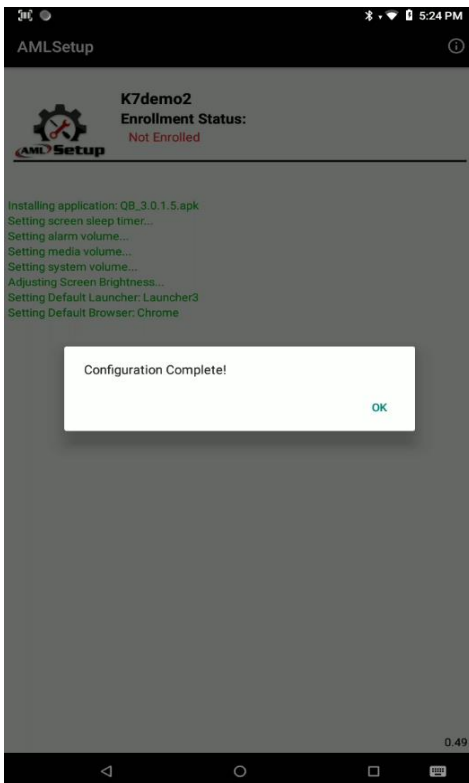
To turn the server on click the Server button until it turns orange with a green dot. To turn the server off click the Server button until it turns grey with a white dot.

3 AML Setup

3.1 Configuration Barcode Method

1. Use [AML Setup Console](#) to create a configuration barcode.
2. Scan the configuration barcode.
3. Wait for the AML Setup application to open and start processing the tasks.

When AML Setup is done processing the tasks there will be a popup stating "Configuration Complete". Any tasks that failed will be highlighted red and successful tasks will be highlighted green.



3.2 Payload Method

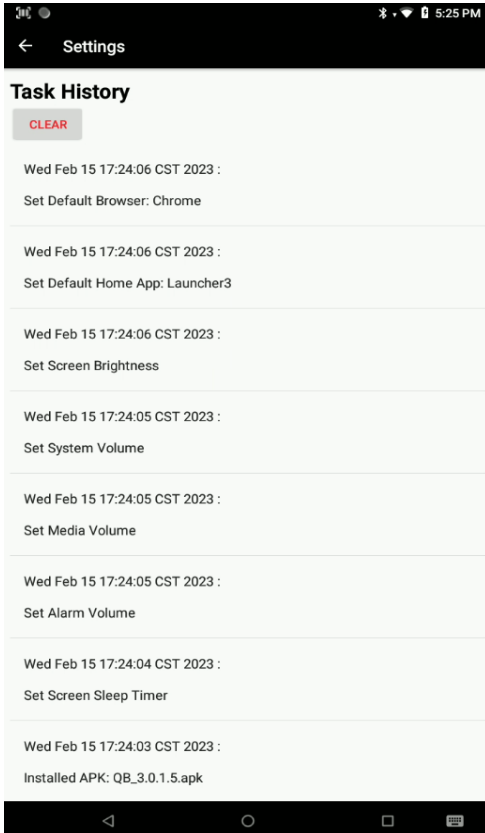
1. Use [AML Setup Console](#) to generate a configuration payload.
2. Push the payload zip file to the path `/sdcard/Android/data/com.amltd.amlsetup/config/` on the device

Within five minutes AML Setup will process the payload zip file and handle the configuration in it. There is no display for this process as it is handled completely in the background.

3.3 Task History

1. Open AML Setup application on the device
2. Click the settings gear icon in the menu.

All task history is listed under the task history section in AML Setup so the user can see what tasks AML Setup has done in the past. The task history can be cleared by clicking the Clear button.



4 Security

4.1 AML Setup Key

The AML Setup Key can be set to add security to your AML device and protect it from unwanted AML Setup configuration barcode scans. When the AML Setup Key is set, the key is required in an AML Setup configuration barcode for authorization. If a configuration barcode is scanned without the key in it, the device will not complete the tasks and will display a Invalid Key message. To set the AML Setup Key, use AML Setup Console to [generate a barcode with the new key](#). If AML Lockdown or Store Scan are locked down on the device and a AML Setup Key is not already set, the device will set its AML Setup Key to the first four characters of the AML Lockdown or Store Scan password. This key will be required in any subsequent configurations. To set the key in the AML Setup Console configuration, see [Setting Current AML Setup Key](#).

End User License Agreement

The copy of the AML Setup Console, AML Setup Console Server, AML Setup 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 2020. All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from AML.



AML
7361 Airport Fwy
Richland Hills, TX 76118

800.648.4452

www.amltd.com