

Kyocera DuraXA Equip

Device Control “How To” Guide



Table of Contents:

1. DuraXA Equip Phone	
• Overview -----	4
• Keyguard -----	8
2. Device Control Overview -----	9
3. How to enable Device Control -----	12
4. Device Control Restriction List -----	13
5. How to Create a Device Control Policy -----	14
• Example 1: How to Hide unwanted Apps -----	15
• Example 2: How to Restrict Outgoing Calls to Contacts Only -----	17
• Example 3: How to force Location setting to High Accuracy -----	19
6. How to copy a Device Control Policy to other DuraXA Equip phones --	20

Table of Contents:

7. How to check the Status of your Device Control Policy -----	21
8. How to change your Device Control Password -----	22

APPENDIX

• Device Control FAQs -----	24
• UI Device Control versus Business Select Device Control -----	25

DuraXA Equip Phone Overview

Model Number: E4831

< Front open >

Earpiece

Main screen

Left/Right soft keys

Navigation key

Center soft key

Camera*/Speaker key

SEND key

CLEAR/Back key

Speakers



Voice commands key

END/POWER key

Keypad

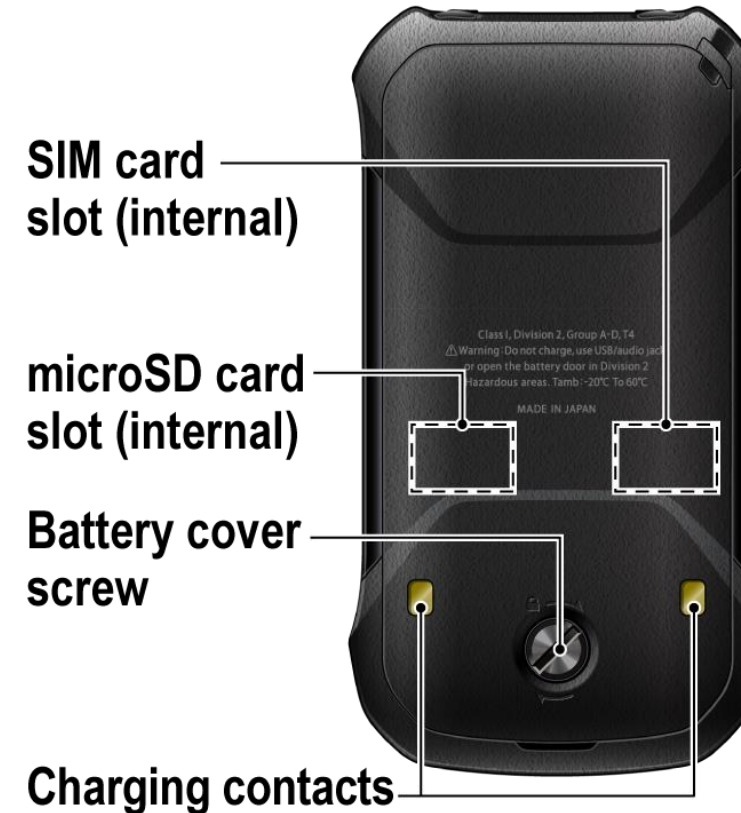
Microphone

DuraXA Equip Phone Overview (cont.)

< Front closed >

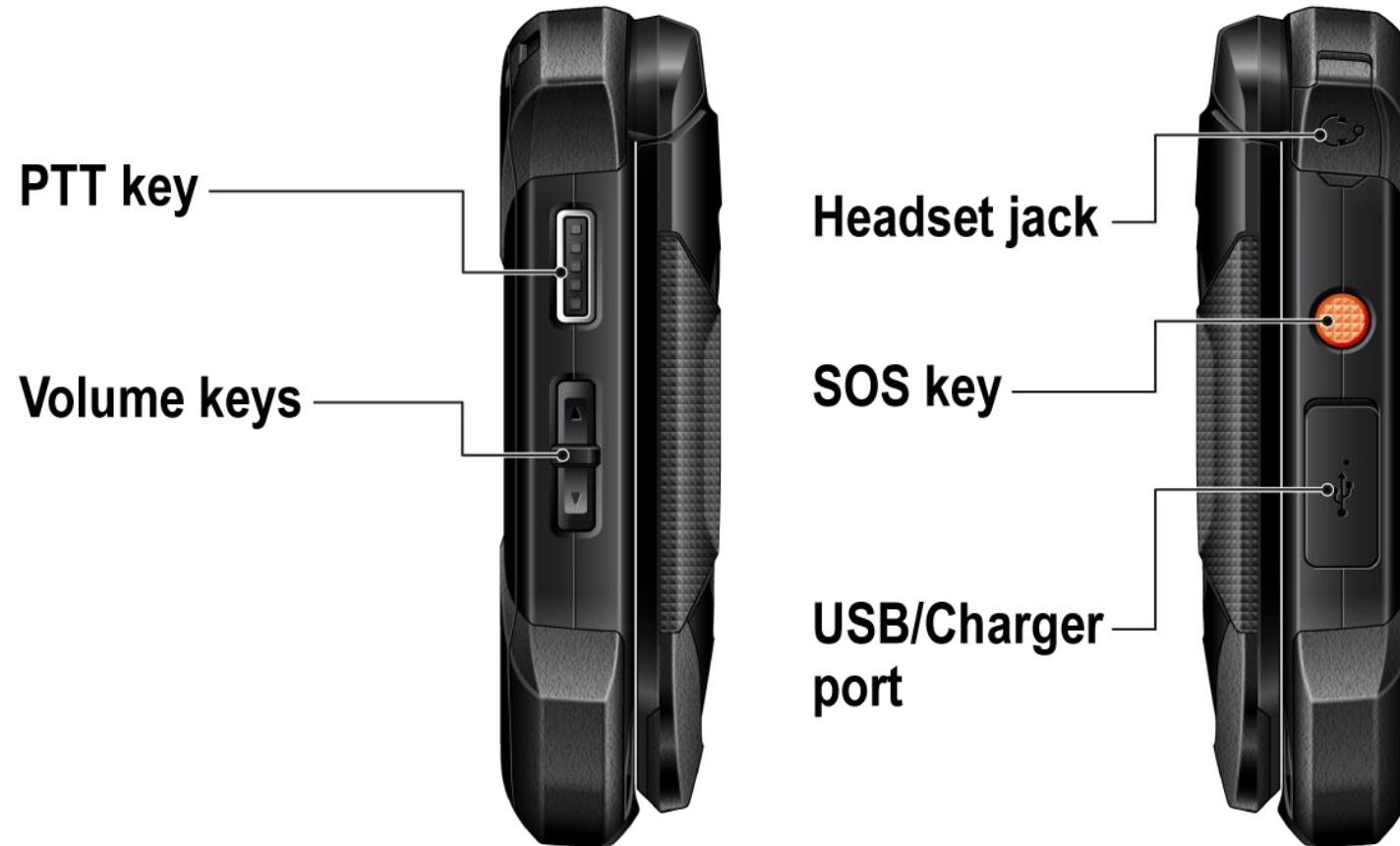


< Back >



DuraXA Equip Phone Overview (cont.)

< Sides >



Note: PTT key and SOS key are user programmable keys

DuraXA Equip Phone Overview (cont.)

< Top >

External speaker key

Lets you place or receive calls in speakerphone mode (with the phone closed), turn the speakerphone on and off during a call, or unlock the keyguard (if configured).



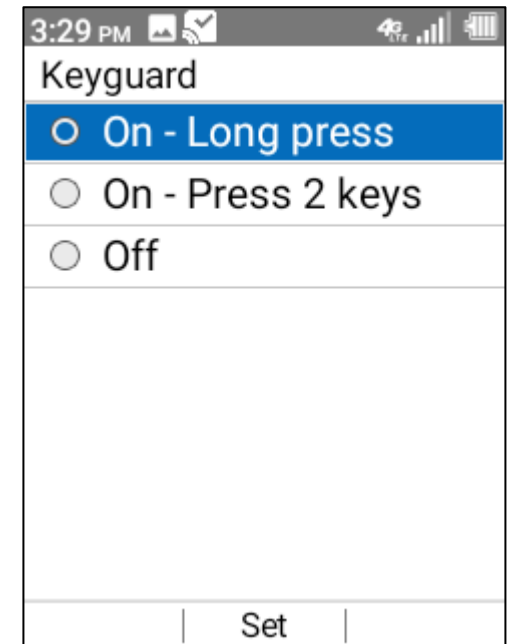
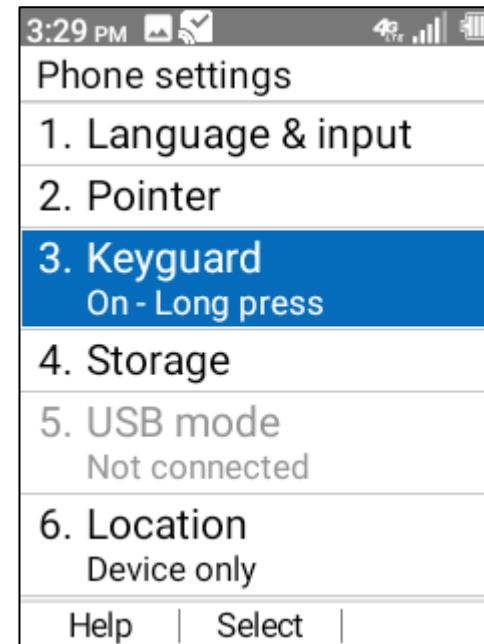
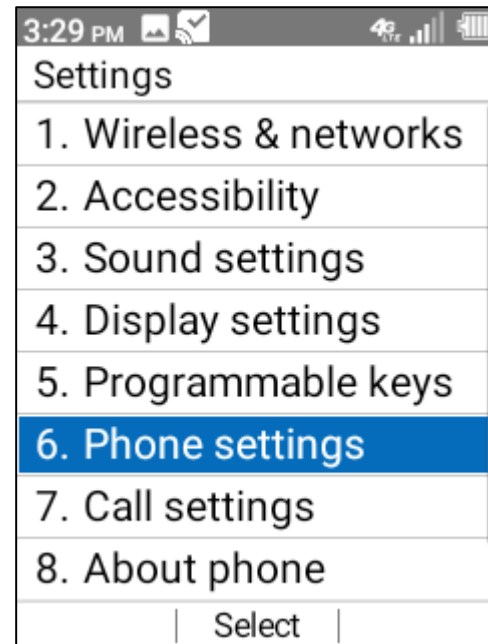
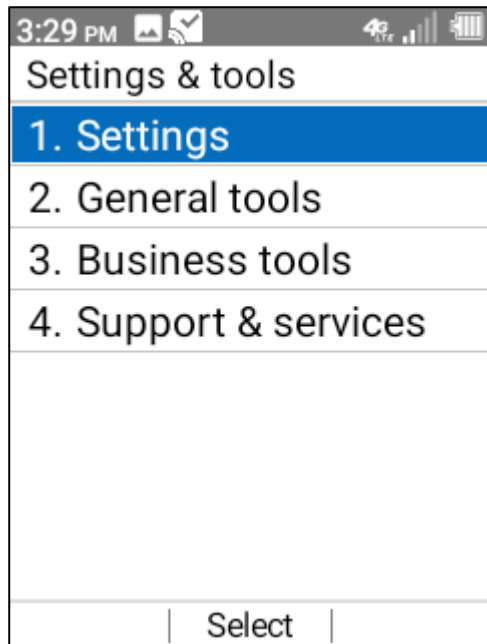
Call list key

Lets you display the recent call history (with the phone closed), ignore an incoming call, end the ongoing call, or unlock the keyguard (if configured). You can select a name or number from the call list and place the call with the phone closed by using the external speaker key.

DuraXA Equip: Keyguard

Use this feature to lock the external keys while the phone is closed to prevent accidental key presses. Select one of the following options:

- **On - Long press** to temporarily disable the keyguard by pressing and holding the External speaker key while the phone is closed.
- **On - Press 2 keys** to temporarily disable the keyguard by pressing the Call list key and the Volume down key sequentially while the phone is closed.
- **Off** to disable the keyguard.



Device Control Overview

ABOUT DEVICE CONTROL:

Device Control by Kyocera is an ideal mobile solution for businesses with small device pools where cloud-based device management is not required. The application provides control of device features without any monthly recurring charges, improving your business's bottom line. With Device Control, your employees have easy access to critical business apps.

FEATURES:

DEVICE FEATURE RESTRICTIONS – Limit or allow device capabilities to those needed for the job.

APPLICATION MANAGEMENT – Restrict list of applications supported or allowed on device.

CONTACT MANAGEMENT – Limit access privileges to designated phone numbers for incoming/outgoing calls.

Device Control Overview (cont.)

Rapidly deploy multiple devices by using a QR code to copy configurations.

Once a Device Control policy is created on one device, it can easily be transferred to multiple devices to reduce/minimize the group device configuration effort.



Device Control Overview (cont.)

Device Control is preloaded on DuraXA Equip for basic options. For advanced configurations, please contact Kyocera Business Select.

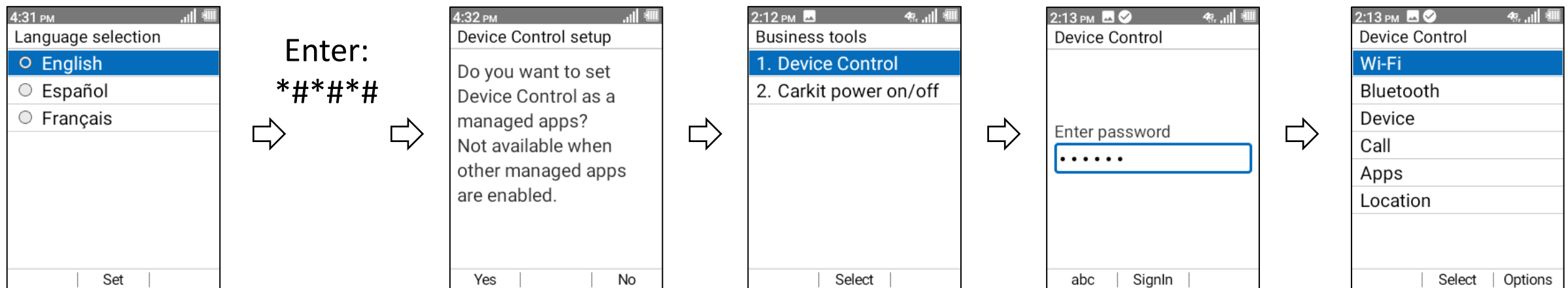
	Device Control via UI	Device Control via Kyocera Business Select
Availability	Preloaded on device	Via Kyocera Business Select
Capabilities	Basic / Limited	Advanced
Walkie-Talkie Only Mode	No	Yes
Deploy multiple devices via QR Code	Yes – Easily copy custom configuration and rapidly deploy across multiple phones using QR Code.	N/A
Configuration Retention	No – Restrictions removed if device resets to factory configuration	Yes – Restrictions and custom settings enforced even after reset of the device to factory configuration
Device Settings Retention	No – All device settings removed after device resets to factory configuration	Yes – Device settings unchanged even after reset of device to factory configuration
Update configuration through cloud	No	No
Price	FREE	One time fee – contact Kyocera Business Select. Devices must be sent to Kyocera for Business
How to access	Refer to User Guide	Contact Kyocera ☎ 866.844.7525 ✉ BusinessSelectSupport@Kyocera.com

How to enable Device Control

This app is preloaded on DuraXA Equip and has to be enabled during the initial device setup. (Note: Users who have already completed the initial device set-up will need to reset the device to perform this procedure.)

Set-up procedure:

1. Immediately after initial power up, language selection screen appears.
2. Enter secret code *##*## to initiate Device Control set up.
3. After making language selection, go to Settings & Tools/Business Tools/Device Control.
4. Enter default password (000000) and press the center soft key to sign into Device Control.
5. Device Control main menu appears. You are ready to create a Device Control Policy.



Device Control restriction list

Device Control menu item	Sub menu	Restriction / Setting	Explanation
Wi-Fi	Restriction for Wi-Fi	1. Disable Wi-Fi	
Bluetooth	Restriction for Bluetooth	1. Disable Bluetooth	
Device	Restrict device features	1. Disable SMS	Disables Messaging App
		2. Disable OTA	Disables ability to receive Software Updates
		3. Disable Camera	
		4. Disallow Unknown Sources	Will not allow Apps from unknown sources to be installed
		5. Disable SD card	Disables ability to use SD card
Call	Restrictions for Cellular Services	1. Disable Voice Roaming	
		2. Disable Data Roaming	
		3. Disable Data	
	Restrict Contact List	1. Disable Manage the Contact List	Restricts ability to add/delete contacts
	Restrictions for Incoming Calls	1. Restrict Incoming Calls	Incoming calls are disabled (unless specified below)
		2. Without Contacts	Allows only incoming calls from contact list
		3. Without whitelist numbers	Allows only incoming calls from your whitelist
		4. Whitelist numbers	Manage your incoming whitelist phone numbers
	Restrictions for Outgoing Calls	1. Restrict Outgoing Calls	Outgoing calls are disabled (unless specified below)
		2. Without Contacts	Allows only outgoing calls from contact list
		3. Without whitelist numbers	Allows only outgoing calls from your whitelist
		4. Whitelist numbers	Manage your outgoing whitelist phone numbers
Apps	Hidden Applications	1. Hidden Applications	Enables Apps in below list to be hidden
		2. Hidden Applications List	Manage the list of Applications you want to hide
Location	Enable Settings	1. Enable Location Settings	Forces Location setting to "high accuracy"
	Restrictions for Mock Location	1. Disable Mock Location	Disables ability to fake GPS location

How to create a Device Control Policy

A Policy is a group of restriction and settings which create a specific device configuration. The restriction list shown on the previous page, shows all the items you can choose to create your Policy. When you create a Policy, it can include a single restriction or multiple restrictions. After you create a Policy on one phone, you can easily export the Policy to another phone by scanning the QR code that's displayed on the phone screen.

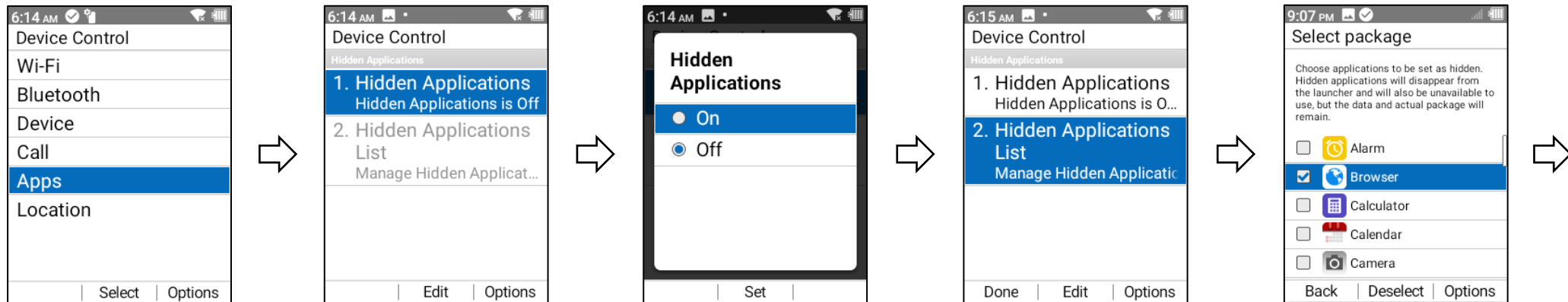
The easiest way to explain how to create a policy is to show a few examples:

- Example 1: How to Hide unwanted Apps
 - A construction company plans to give devices to all workers at remote sites but does not want them to waste time browsing the internet.
- Example 2: How to Restrict Outgoing Calls to Contacts only
 - A school wants to distribute devices to teachers for use in emergencies. The devices will be provided with a pre-defined contact list that should not be altered. Outgoing calls will be restricted to contact list.
- Example 3: How to Force Location Setting to “High Accuracy”
 - A courier has a small fleet of trucks delivering packages around the city. They want to give their drivers devices so that they can always be located and be able to contact the office. They do not want the drivers to change the GPS settings.

Example 1: How to Hide unwanted Apps

To restrict the user's ability to use one or more Apps:

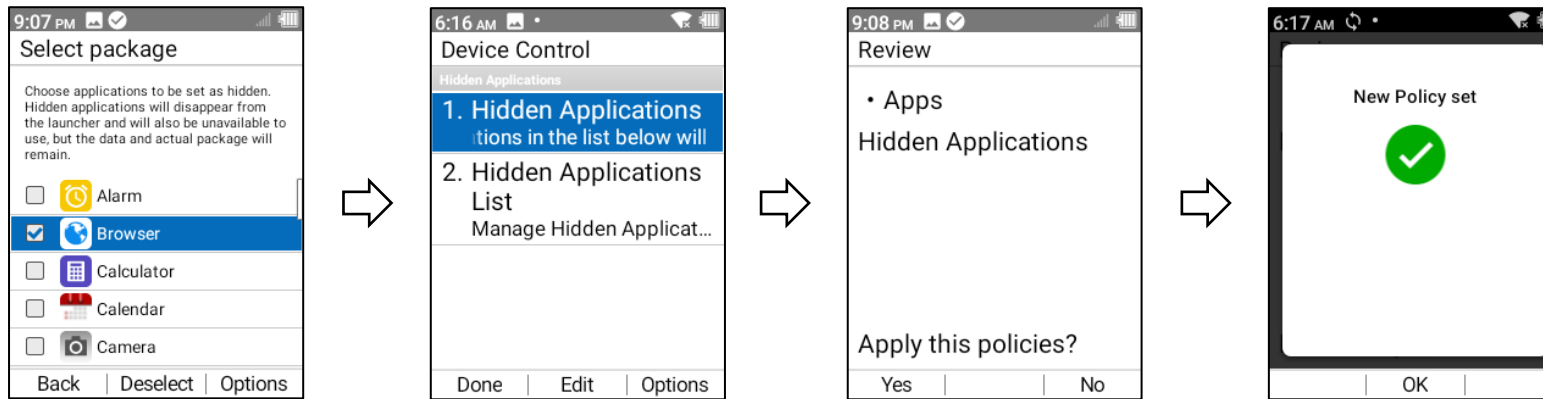
1. In Device Control menu, select Apps.
2. Select "Hidden Applications".
3. Change "Hidden Applications" from Off to On.
4. Select "Hidden Applications List".
5. Select the Apps you want to hide. (Scroll down to see all Apps).



Note: In this example, we will remove the Browser App, this will prevent users from browsing the internet.

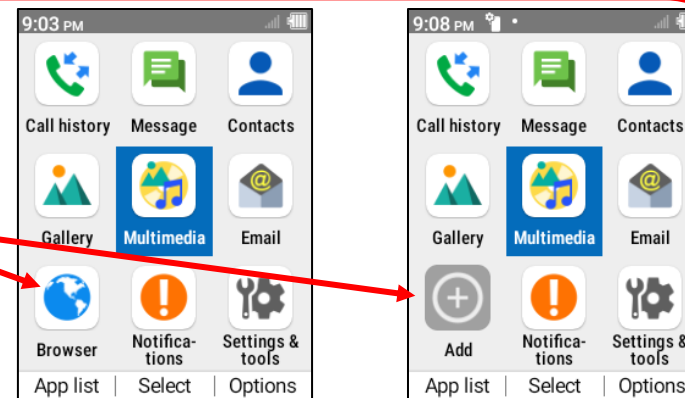
Example 1: How to Hide unwanted Apps (cont.)

6. When finished selecting the Apps, press the left soft key [Back].
7. Press the left soft key [Done].
8. Apply this policy? Press the left soft key [Yes].



RESULT:

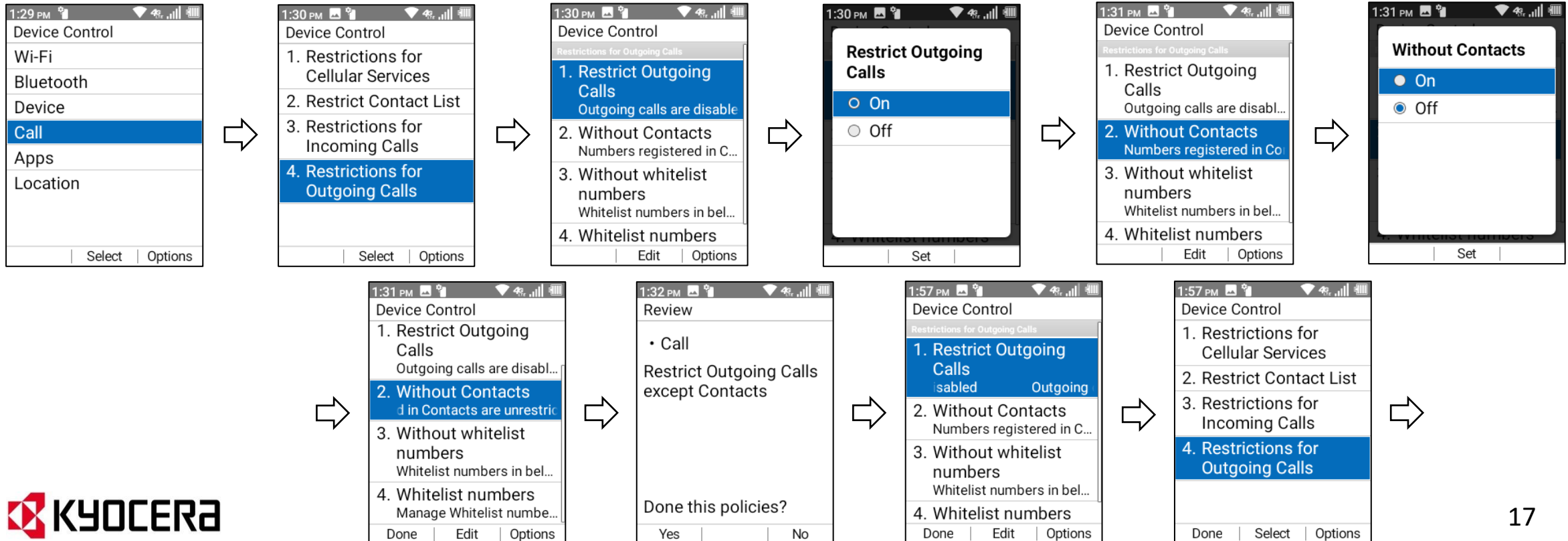
Browser has been removed from Main Menu



Example 2: How to Restrict Outgoing Calls to Contacts only

To restrict outgoing calls to only your contacts:

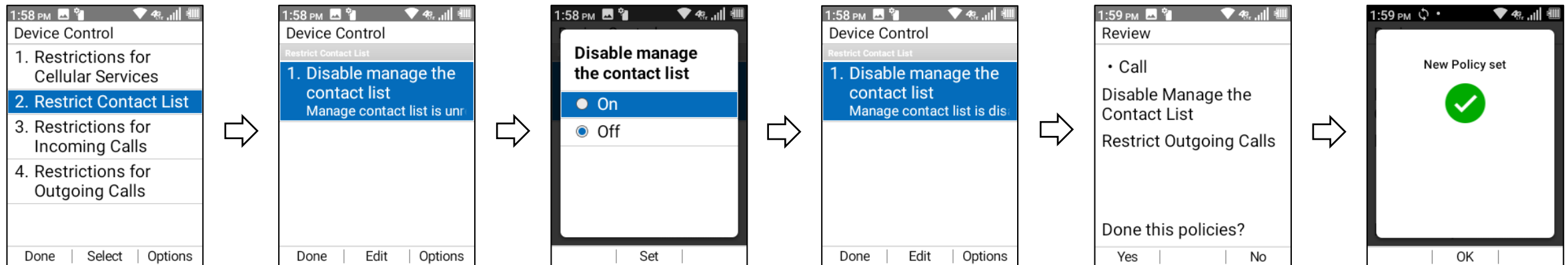
1. In Device Control menu, select Call.
2. Select “Restrictions for Outgoing Calls”; change “Restrict Outgoing Calls” from Off to On.
3. Select “Without Contacts”; and change from Off to On.
4. Press the left soft key [Done].
5. Done with this policy? Press the right soft key [No].
6. Press the CLR key on the keypad to go up one menu level.



Example 2: How to Restrict Outgoing Calls to Contacts only (cont.)

To restrict the user's ability to make changes to the phone's contacts:

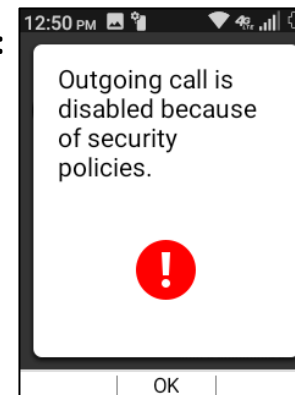
7. Scroll up to "Restrict Contact List" and press Select.
8. Select "Disable manage the contact list" and change from Off to On.
9. Press the left soft key [Done].
10. Done with this policy? Press the left soft key [Yes].



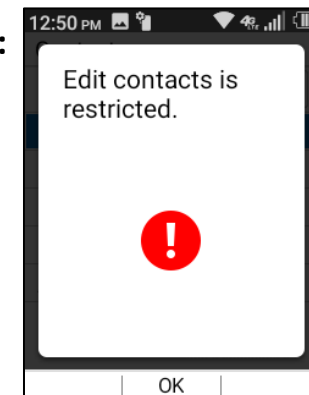
RESULT:

1. Screen A appears when user tries to call a number that's not in Contacts.
2. Screen B appears when user tries to edit Contacts.

Screen A:



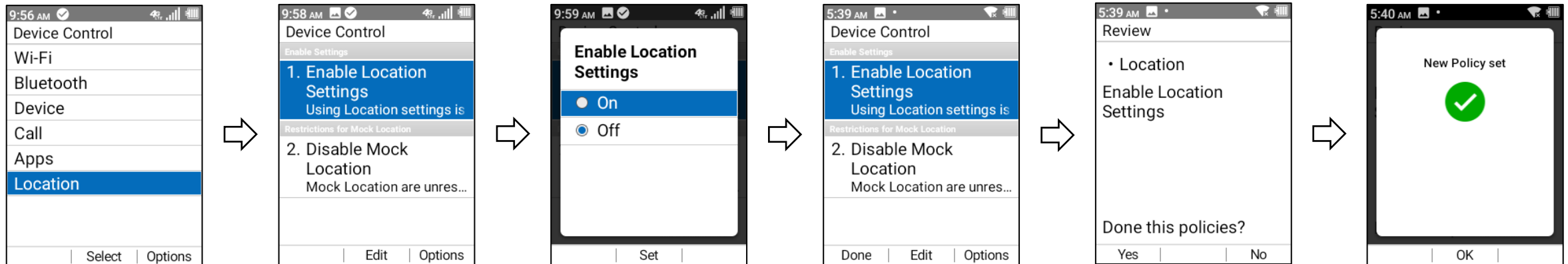
Screen B:



Example 3: How to force Location Setting to “High Accuracy”

To restrict the user's ability to disable location services:

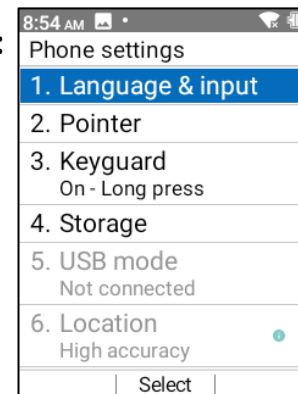
1. In Device Control menu, select Location.
2. Select “Enable Location Settings”.
3. Change “Enable Location Settings” from Off to On. (When “On” is selected, Location will be set to “High Accuracy” and user will not be able to change it.)
4. Press the left soft key [Done]. Done with this policy? Press the left soft key [Yes].



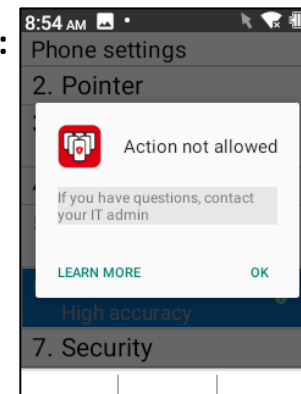
RESULT:

1. In Phone settings menu, Location is greyed out (Screen A).
2. If Location is selected, Screen B appears.

Screen A:



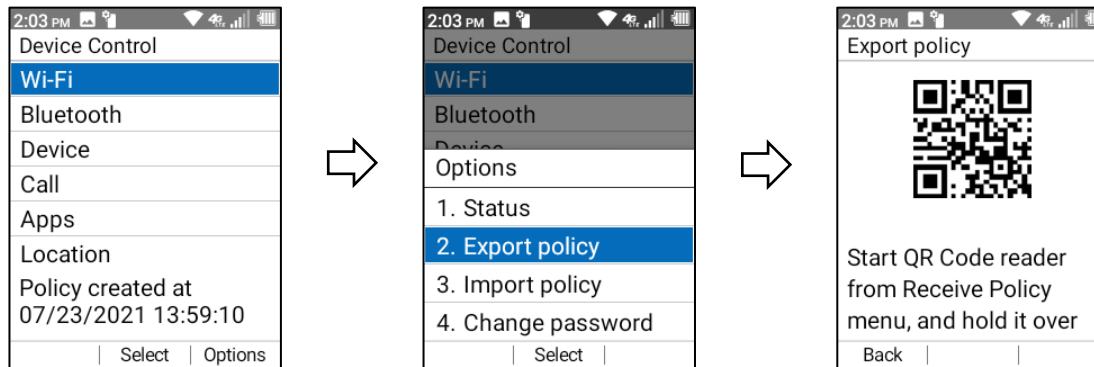
Screen B:



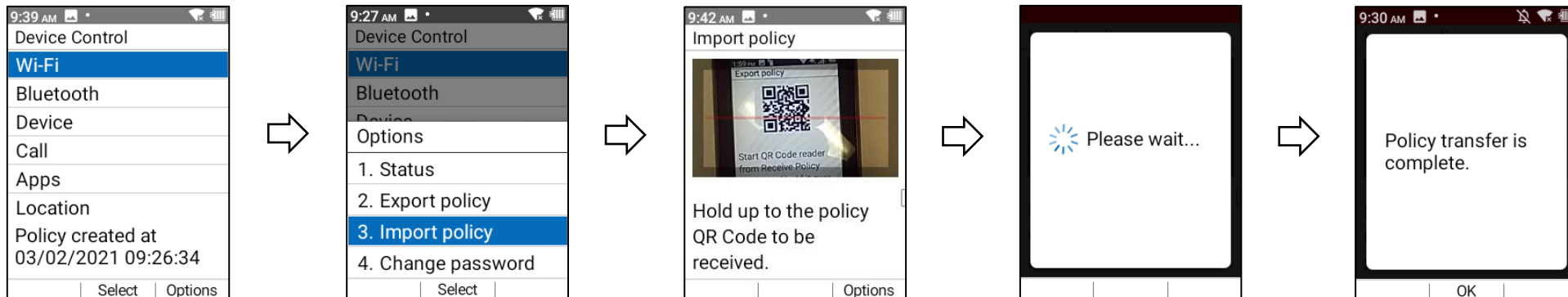
How to copy a Device Control Policy to other DuraXA Equip phones

1. Make sure both phones are connected to Wi-Fi and logged into Device Control.
2. On Phone A: in Device Control menu, press the right soft key [Options] and select “Export policy”.
3. On Phone B: in Device Control menu, press the right soft key [Options] and select “Import policy”.
4. Hold Phone B’s camera to Phone A’s screen to scan the QR code.

Phone A



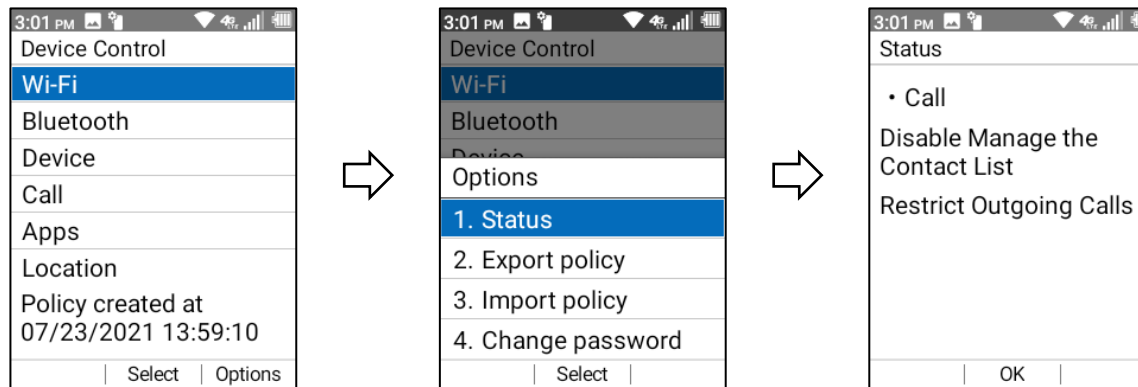
Phone B



How to check the status of your Device Control Policy

To check to see what restrictions are in your phone's Device Control Policy:

1. In Device Control menu, press the right soft key [Options] and select "Status".



In the above example, there are two Call restrictions in the Policy:

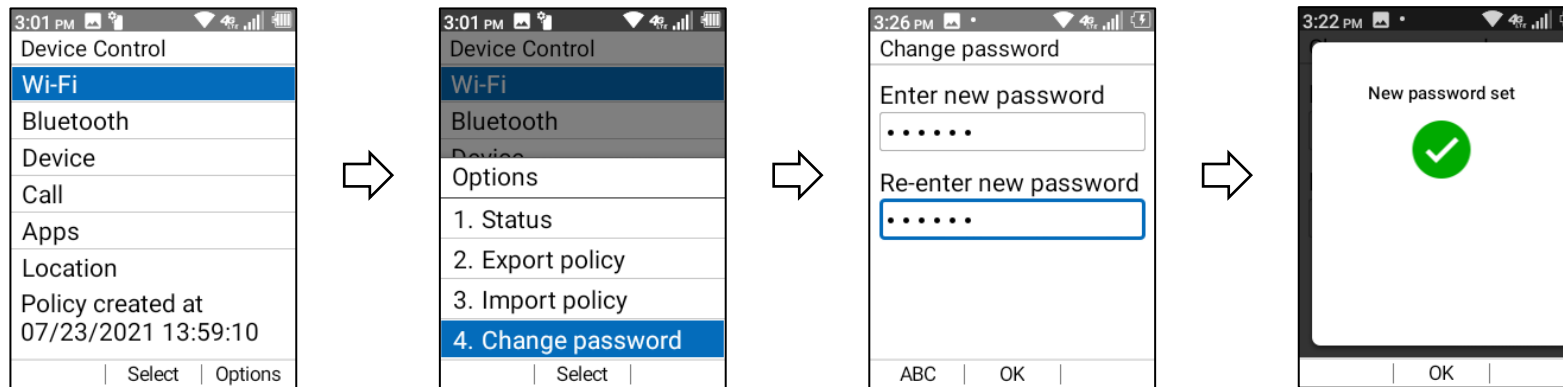
- (1) Disable Manage the Contact List and
- (2) Restrict Outgoing Calls

You can add more restrictions by going to the Device Control menu and selecting the item you want to add.

How to change your Device Control password

To change the default password from 000000 to something else:

1. In Device Control menu, press the right soft key [Options] and select “Change password”.
2. Enter new password, then re-enter to confirm.



Note: Passwords must be at least 6 characters long.

Appendix

Device Control FAQs

ID	Question	Response
1	What is Device Control?	Device Control provides a simple method to adjust the settings and configuration of supported Kyocera mobile devices by accessing the embedded Mobile Device Management (MDM) Application Programming Interface provided in the Kyocera software.
2	How do I initiate Device Control on my feature phone?	After factory reset or initial power up, on the Language Selection screen, enter *##*#. Then go to Settings & Tools/Business Tools/Device Control and enter the Device Control password.
3	What is a Device Control Policy?	A Policy is a group of settings (restrictions and features) which create a specific device configuration. A feature phone device can hold only one Policy at a time.
4	How do I transfer a Device Control Policy from one device to another?	After you create a Policy on one phone, you can easily export the Policy to another phone by scanning the QR code that's displayed on the phone screen. Both devices must be connected to Wi-Fi.
5	Is it possible to transfer policies to and from non-camera phones?	Yes, on Kyocera's non-camera phone models, you can't use the QR code reader; however, you can transfer a policy using the 5 digit code that is generated by the Device Control App on your phone.
6	After I transfer the policy to a new device, how do I activate the policy?	After the Transfer Policy operation is complete, you must press the left soft key (DONE) to activate the policy on your new device.
7	Can the Device Control Policy on a device be managed remotely?	No. Device Control is a device-based solution that does not utilize network or cloud-based controls.
8	Do I need an email account or Google account for Device Control?	No. Device Control on your feature phone, does not require an email account or Google account.
9	How many devices can I transfer my Device Control Policy to?	There is no limitation, but the transfer process must be done one phone at a time.
10	What Kyocera feature phone models are supported?	DuraXV Extreme DuraXE Epic
11	Is there any on-going technical support available for Device Control?	Yes. For help with Device Control, please contact the toll-free Kyocera Business Select Support line at 1.866.844.7525
12	Does Kyocera provide additional services or support for advanced settings or complex configurations?	Yes. Business Select support is Kyocera's white glove treatment developed especially for our valued business customers. Contact a Business Select consultant to discuss advanced Device Control settings or complex requirements and configurations. Kyocera also offers a full service solution where the Business Select team will review the requirements, create the desired configuration policies and transfer the policies to each of your devices. Contact Business Select: Email: BusinessSelectSupport@kyocera.com Phone: 866.844.7525

UI Device Control vs. Business Select Device Control (page 1 of 2)

If you would like to use Kyocera's Business Select service to configure Device Control. You have access to a much longer list of restrictions/customizations than with the Basic Device Control.

Feature	Setting	Basic Device Control via User Interface	Advanced Device Control via Business Select
Wi-Fi	Restriction for Wi-Fi	2	4
Bluetooth	Restriction for Bluetooth	1	7
Emergency Alerts	Enable Settings	0	6
Networking	Restrictions for VPN	0	1
Device	Restrict device features	5	30
Call	Restrict call settings	10	10
App	Restrictions for Applications	1	4
Reset	Restrictions for Factory Data Reset	0	1
Location	Enable Settings	2	3
Security	Restrictions for Security Settings	0	4
Other		0	2
Screen lock type	Screen lock type	0	2
VPN	VPN restrictions	0	15
Apps & notifications	Disable Apps	0	1

UI Device Control vs. Business Select Device Control (page 2 of 2)

Feature	Setting	Basic Device Control via User Interface	Advanced Device Control via Business Select
Contacts	Register address book data	0	1
Browser	Set homepage	0	2
Wi-Fi Access point	Wi-Fi profile creation	0	2
Mobile Hotspot	Mobile Hotspot restrictions	0	3
Language	English/Spanish	0	1
Email	Account settings	0	5
Volume	In-call volume	0	1
Date & time	Date & time restrictions	0	9
Call Settings	More call settings	0	7
Programmable keys	Programmable keys	0	1
Navigation keys	Navigation keys	0	1
Encryption	Encrypt SD card	0	2
Carkit power on/off	Carkit power setting	0	1
Custom main manu	Custom main manu	0	1
TOTAL # OF RESTRICTION SETTINGS:		21	127

To learn more about Advanced Device Control, contact Kyocera Business Select:

Email: BusinessSelectSupport@kyocera.com

Phone: 866.844.7525