

Smart Home Controller





Thanks for choosing the Ezlo Secure

You've taken the first step toward making your home smarter and safer.

It's easy to set up your hub. Here is what you have to do.

SET UP

For starters, your Ezlo Secure hub operates on the Vera app.

Install the Vera app on your mobile device. Just look for the **V** in the iOS App Store or on Google Play.

If you already have the Vera app, just log in.

If you just downloaded the app, tap on New to Vera and select Ezlo Secure from the list of controllers.

If you already have an account, tap Add New Controller and select the Ezlo Secure from the My Controllers list.





Next, connect the A/C power adapter to your Ezlo Secure. Once it is powered on, the LED should slowly change from green to blue.

Wait for a steady blue light before proceeding.





The Ezlo Secure supports both wired and wireless setup. Select your preferred option and follow the prompts.



Congratulations! Your Ezlo Secure is now connected and its LED will remain steady blue.



If you don't already have one, it's time to create your account. The app will walk you through it.

Make your home safer. Make your life easier.

The Ezlo Secure lets you control Z-Wave™, Zigbee, and Wi-Fi devices from a single app. When you add devices such as lights, thermostats, sensors, cameras, and door locks to your Vera system, you'll be able to enjoy greater comfort and peace of mind with just a touch.

Control your home from anywhere.

The Vera app offers some key features that help you simplify things at home and help you keep an eye on things when you're away.

Modes

Modes give you the power to control all your devices with a single tap. There are pre-set modes for Home, Away, Night, and Vacation.

Scenes

The true power of home automation is when your home can do things for you. With Scenes you can schedule your lights to turn off when you leave for work in the morning, or to fade up as day turns to night.

A Notifications

Your Vera system can send push notifications and emails to let you—or other users—know about what's going on at home.

Need help setting up?

You can reach our Customer Care team seven days a week at 866.966.2272 between 6am and 10pm US CST/EST* or at support@getvera.com

You can also purchase our Vera Easy Start service and get one hour of personalized setup assistance through a phone call with one of our most experienced agents. Visit getvera.com to learn more.

To find the complete User Guide, as well as information about the products FCC/IC registration, visit getvera.com/ support and click on "Downloads, Firmware & Manuals."

Inclusion and Exclusion

Your Ezlo Secure Controller can work with all Z-Wave devices, such as sensors, alarms, door locks, thermostats, etc. Over a thousand Z-Wave devices are available from many brands. (Z-Wave is a wireless communications system; check the package or specs to see if a device uses Z-Wave.)

The Ezlo Secure can be operated in any Z-Wave network with other Z-Wave certified devices from other manufacturers. All mains operated nodes within the network will act as repeaters regardless of vendor to increase reliability of the network

Before Ezlo Secure can control a device, it must be included into the Vera system.

Vera Custom Device Wizards are available for select devices that pass stringent Vera Labs testing for compatibility and quality. The Custom Device Wizards make Inclusion/Exclusion easiest, with specific details for each device. A list of these devices is available and updated at https://ezlo.com/device-compatibility/

For all other Z-Wave devices, a Generic Device Wizard is used for Inclusion/ Exclusion. A Generic Device Wizard is available for each device category (thermostats, sensors, alarms, etc.)

Adding Z-Wave Devices to your Ezlo Secure

Before Ezlo Secure can control a device, it must be added into the system.

Start using your Ezlo Secure by adding devices like lights, thermostats, sensors, and more. Just tap the menu icon at the top left of the dashboard, select Devices, and then tap the + sign to launch the Device Pairing Wizard.

 From your Dashboard, go to Devices > tap on the + in the top right corner and select or search the name or type of device that you wish to pair with your Ezlo Secure.

Rora			Devices Q 1 + Done Device Wizard	
Smarter Home Contro		EzloPl	By Room By Type Failed Step 1: Select Your Device	
EzloPlus			Alarms	>
Client number 90000441			🕎 Dimmers and Lights	>
Dashboard Devices	•	Scenes	Door Locks	>
Scenes	•	Chur	Garage Doors	>
Rooms	۲	Choo		
Ezio VOI™	۲		You have no devices paired with	>
Verts	•		this controller 🔠 Hand Held	>
Users	•	Devices	(III) Keypada	>
Settings	•			
My Controllers	۲		<i>M</i> _☉ Other Devices	>
Logout	×	Choo	Conter Zigbee device	>
			Sensors	>

2. To add a generic Z-Wave device, select the Generic Z-Wave device from the device categories.



3. To add the device with your Ezlo Secure, if the device requires assembly read the manual, follow the assembly instructions there, power the device, and click Next.



4. Once the blue message at the top of the page says Add new device now, follow the process as described in the user manual.



5. If successful, you will get a blue message at the top of the page saying Device was configured and a Device Detected message.



6. To finish, choose a name for the new device, add the device to favorites (optional), edit the name, assign it to a room, and click I'm done adding devices.

3: Name Your Device Device Detected! vice was added. but can name the device and indicate what cancel Room cancel Room Add more devices I'm done adding devices	Device Wizard		Device Wizard	
Device Detected! A was added. A an name the device and indicate what will put it in. To Pin to your Dashboard. Add more devices I'm done adding devices	Name Your Device	Cancel	Rooms	+
vas added. In name the device and indicate what ill put it in. Pin to your Dashboard. Mow Sensor 6 m Add more devices I'm done adding devices	Device Detected!	No Room Name		Action
and the device and indicate what at it in. to your Dashboard. Sensor 6 Add more devices a done adding devices	added.	 Bedroom		0
n to your Dashboard.	name the device and indicate what put it in.		Dane	
nsor 6	your Dashboard.			
dow Sensor 6 m > Add more devices I'm done adding devices				
Add more devices 'm done adding devices	v Sensor 6			
Add more devices I'm done adding devices	n >			
I'm done adding devices	Add more devices			
	I'm done adding devices			

Note: If the device was previously included with a different Z-Wave system, you'll need to exclude it before adding it with your Ezlo Secure. (You may also need to do this if you have problems Inclusion/Exclusion the first time.) Press the Retry button to start the exclusion process. Once the device is excluded, add it by following the inclusion steps.

Adding a Z-Wave Device to Ezlo Secure (SmartStart adding)

With SmartStart, you can add Z-Wave devices automatically by scanning their QR codes.

 From your Dashboard, go to Devices > tap on the + in the top right corner.

2. Select the Z-Wave SmartStart entry. Tap on the Arrow next to the text.





3. On the box of your device, you should find a QR code, usually labeled with a SmartStart title. When you select "Z-Wave SmartStart" in the iOS app, the camera of your phone will be turned on to scan the QR-code. Once a QR code has been scanned the adding process starts.



4. The device is added to the system and you will see a Set Up Device screen. To continue, choose a name for the new device, edit the name, assign it to a room, and click Continue.

5. Select the connection. S2 Access - selected by default

6. Select the inclusion type - SmartStart. Tap on the Continue button.



<	Connection	n
E Slit	tinto NX-SP201 12345 *** 09876	()
Connection advanced functional	ection security on between hub and dev security level and enabl lity.	ice will have les additional
S2 Accer Full secur	ss ity	
Advance Full list of	d options security options	
You can se the Smart Classic Z-1	ion type Hect between automati Start or add device ma Wave inclusion.	c inclusion using mually with
Smart st	art	0
Classic Z	-Wave	0
	Continue	
	Scan more devic	ces

- 7. Select another connection security type. Enable the toggle to see the list with all connection types available. Once you've selected the type of encryption, tap on Continue.
 - S2 Access Full security
 - Access Control Encrypted connection
 - S2 Authenticated Encrypted connection
 - S2 Unauthenticated Encrypted connection
 - S0 Encrypted connection

If the S2 Access is checked, by default all options under Advanced are checked.

If the S2 Access is unchecked, all options under Advanced are unchecked.

You are able to select whichever options you choose from the Advanced list.



×	Connectio	n securit	iy.	
	New device DSK: 12345 *** 0987	5	G)
Selec	t connectio	on secu	rity	
Connecti advanced functiona	on between hub an d security level and lity.	d device will activates add	have ditional	
S2 Acco Full secu	ess rity		l	~
Advanc	ed options			D
P GIE HOL G	security options			
Access Encryptic	Control on connection		I	~
S2-Aut	henticated		I	~
60 Um	whenticated			
Encryptic	on connection			~
S0 Encryptic	an connection			~
er og fjern				
	Co	ntinue		
	Scan m	ore devices	1	

8. In the next step, you will see the confirmation screen that your device is ready.

Just turn on your device and it will be added automatically. You can check the SmartStart device state in Settings.



Tap on the notification and the VeraMobile app is opened to the list of SmartStart devices.





10. On the SmartStart devices, you can see all added devices with statuses.



To manage all SmartStart devices you scanned you need to tap on the side menu, tap on Settings.



On the settings screen, tap on SmartStart Devices.



If you don't have any device that has SmartStart support, you will see an empty SmartStart Devices screen. Also, from this screen, you can add a SmartStart device by tapping the Add a SmartStart device button.

If you added at least one Z-Wave device via SmartStart, you will see a SmartStart Devices screen with a list of devices.



Smart Start Devices

 \equiv

Q



Tap on the Info button and see the device details in an additional screen.

On this screen you can change the device name, the encryption connection, and the inclusion type. To change the encryption connection, tap on the > button.

Once you press the > button, the connection security screen will be opened. You will see the list of all available connections types under Advanced options

- S2 Access Current connection
- S2 Authenticated Encrypted connection
- S2 Unauthenticated Encrypted connection
- S0 Encrypted connection
- CSA Client side authenticated

You can select as many options as you like. If S2 Access is checked by default, all options under Advanced are checked. IS2 Access is unchecked, then all options under Advanced are unchecked.

To apply the changes, you need to remove and add this device again.

Device name Sitinto NX-SP201 Selected Encryption connection S2-Unauthentificated Current Encryption connection S2 Access Inclusion type Smart start DSK code 12345 09876 09876 12345 12345 09876 Status Pending Image: Controller or another z-wave powered on and placed near this controller or another z-wave powered device.			
Slitinto NX-SP201 Selected Encryption connection S2-Unauthentificated Current Encryption connection S2 Access Inclusion type Smart start DSK code 12345 09876 09876 12345 12345 09876 12345 09876 Status Pending Please check if your device is powered on and placed near this controller or another Z-Wave powered device.	Device name		
Selected Encryption connection S2-Unauthentificated Current Encryption connection S2 Access Inclusion type Smart start DSK code 12345 09876 09876 12345 12345 09876 09876 12345 12345 09876 09876 12345 Status Pending Please check if your device is powered on and placed near this controller or another Z-Wave powered device.	Slitinto NX-	SP201	
Current Encryption connection S2 Access Inclusion type Smart start DSK code 12345 09876 09876 12345 12345 09876 12345 09876 Status Pending Please check if your device is powered on and placed near this controller or another z-Wave powered device.	Selected Encryptic S2-Unauthen	on connection tificated	
Inclusion type Smart start DSK code 12345 09876 09876 12345 12345 09876 12345 0987 12345 0987 1234 0 123 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Current Encryption	nconnection	2
DSK code 12345 09876 09876 12345 12345 09876 12345 09876 Status Pending Please check if your device is powered on and placed near this controller or another Z-Wave powered device.	Inclusion type Smart start		>
Status Pending Please check if your device is powered on and placed near this controller or another Z-Wave powered device.	DSK code 12345 09876 12345 09876	09876 12345 3 12345 09876	
Please check if your device is powered on and placed near this controller or another Z-Wave powered device.	Status Pending		
Please check if your device is powered on and placed near this controller or another Z-Wave powered device.	G		
	Please check and placed ne Z-Wave powe	if your device is powered on ear this controller or another ered device.	

Tap on the save button. The changes are saved and if there is a new type of connection selected, you will see in the device details and the current connection. Below it you will see a message Please re-include this device to apply the following connection and the connection types selected previously. These changes will be applied only after you re-include the device.

<	Connection security	
S2 Access Full Security		
Advanc	ced options	
Access Co Encrypted o	ontrol onnection	
S2-Auther	ntificated	~
S2-Unauth Encrypted o	nenticated onnection	<u>~</u>
SO Encrypted c	onnection	<u>~</u>
(;) To apply th and includ	ne changes you need to exclu le this device again.	ude
	Save	

< Conne	ection securit	y		
S2 Access Full Security				
Advanced op	tions			
Access Control Encrypted connection				
S2-Authentificated Encrypted connection				
S2-Unauthenticated Encrypted connection	i			
S0 Encrypted connection				
G To apply the changes you need to exclude and include this device again.				
	Save			

<	Connection security	
S2 Access Full Security		
Advanc	ed options	
Access Col Encrypted co	ntrol	
S2-Authen Encrypted co	tificated nnection	
S2-Unauth Encrypted co	enticated	
SO Encrypted co	nnection	
To apply th and include	e changes you need to exclude a this device again.	
	Save	

< Device details
Device name
Siltinto NX-SP201
Colorited Energetian connection
S2-Unauthentificated
S2 Access (current)
Please re-include this device to apply the following connection: S2-Authenticated
S2-Unauthenticated
DSK orde
12345 09876 09876 12345
12345 09876 12345 09876
Status
Included

On the device details screen you can see the device status:

- Included
- Pending Please check if your device is powered on and placed near this controller or another Z-Wave powered device.
- Failed Please remove the device from your system and try again. After you scan the QR code, make sure when you power ON the device, it is placed near this controller or another Z-Wave powered device.
- Other system device To add the device to this controller you have to first delete the SmartStart entry and remove the device from the current controller. After that, you have to add the device to this controller.
- Add manually When Z-Wave classic connection type is used you need to add the device manually.

< Device details		<	Device de	tails
Device name			Device name	
Slitinto NX-SP201			Slitinto NX-SP201	
Selected Encryption connection S2-Unauthentificated		s	ielected Encryption connection 52-Unauthentificated	
Current Encryption connection S2 Access	>	s	Current Encryption connection	>
Inclusion type Smart start	>	S	nclusion type Smart start	>
DSK code 12345 09876 09876 12345 12345 09876 12345 09876		0 1 1	ISK code 2345 09876 09876 12345 2345 09876 12345 09876	5
Status Pending		S F	Status Failed	
Ģ		((j)	
Please check if your device is powered o and placed near this controller or anothe Z-Wave powered device.	in ir	F a n is Z	Please exclude the device f and try again. After you sca make sure when you power s placed near this controlle Z-Wave powered device.	rom your system in the QR code, r ON the device, it r or another

Device details		< Device detai	ls
Device name		Device name	
Slitinto NX-SP201		Lamp 5	
Selected Encryption connection S2-Unauthentificated	_	Selected Encryption connection S2-Unauthentificated	
Current Encryption connection S2 Access	>	Current Encryption connection S2 Access	
Inclusion type Smart start	>	Inclusion type Z-Wave classic	
^{DSK code} 12345 09876 09876 12345 12345 09876 12345 09876	_	DSK code 12345 09876 09876 12345 12345 09876 12345 09876	
Status Other system device	- 1	Status Add manually	
Ģ	- 1	Ģ	
To include the device to this controlle have to first delete the smart start en exlude the device from the current co	er you htry and ontroller.	When Z-Wave classic connect used you need to add device n	ion type is nanually.
After that you have to include the de this controller.	vice to	Add manually	

To change the inclusion type tap on > button and select the inclusion type

- SmartStart: The device will be added via SmartStart flow
- Z-Wave classic: tap the Add manually button and add the device via Z-Wave generic flow



If you were unable to add a SmartStart device by scanning the QR code, you can add it manually. Tap on the button Enter DSK code manually.



Scan device QR code

QR code can be found on the box of your device usually labeled with Smart Start title.

Enter DSK code manually

Enter the 40 digits of the DSK code shown on the box of your device. Make sure this code belongs to a SmartStart device for automatic inclusion. Once you have entered all 40 digits, tap Continue.





<	Enter DSK cod	le				
Enter the 40 the box of yo belongs to a inclusion.	digits of the DSK or our device. Make su smart start device f	ode shown on re this code for automatic				
XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX XXXXX						
8	69	² <u> 6 </u>				
Continue						
1	1 2 3					
4 6HI	5 JKL	6 MNO				
7 PQRS	8 TUV	9 wxyz				
+ * #	0	$\langle \times \rangle$				

The device is added to the system and you will see a Set Up Device screen.

To continue the flow, follow the previously described steps.



How to add S2 only (non-SmartStart) devices via the SmartStart flow

1. From your Dashboard, go to the Devices screen and tap on the + icon in the top right corner.

2. Select the Z-Wave SmartStart entry. Tap on the Arrow next to the text.





3. On the box of your device, you should find a QR code, usually labeled with a SmartStart title. Use the camera of your phone to scan the QR code. Once the device's QR code has been scanned, the inclusion process begins.



4. The device is added to the system and you will be taken to the Set Up Device screen. To continue, choose a name for the new device, edit the name, assign it to a room, and click "Continue".

5. Select the connection. S2 Access is selected by default.

6. Tap on the Add manually now button or scan more devices.



< Connection	
Slitinto NX-SP201 DSK: 12345 *** 09876	Ģ
Connection security Connection between hub and device advanced security level and enables functionality.	will have additional
S2 Access Full security	
Advanced options Full list of security options	
Inclusion type S2 device can only be added manual Classic Z-Wave inclusion. You can ad later using the Smart Start Devices I	ly using the d it now or ist in settings.
Classic Z-Wave	
Add manually now	
Scan more devices	

7. The device will be added to the SmartStart device list.

8. Go to the SmartStart Devices list and select the device with the status Add manually and tap on the info icon.

9. Rename the device if needed and tap on the Add manually button.

10. Add the device via the Z-Wave generic flow.



C	Device details	
Device name		
Lamp 5		
Selected Encryptio	n connection	
S2-Unauthen	tificated	
Current Encryption	connection	
S2 Access)
Inclusion type		
Z-Wave class	ic	
DSK code 12345 09876 12345 09876	09876 12345 12345 09876	
Status Add manually		
G		
When Z-Wave used you nee	e classic connection type is d to add device manually.	
	Add manually	

How to remove a Z-Wave device from an Ezlo Secure

- 1. From the list of devices, tap on the selected device and go to that device's settings.
- Devices Q Ŵ +Failed By Room By Type Bedroom 29.7°C Senso > > UV Sensor Kitchen Light Level Sensor 0.0% > C Motion Sensor > DISARMED No room 🔿 Amazon Alexa > Fibaro Wall Plug õ < C 0.0watt Device failed to communicate
- 2. On the device settings page press delete device.



- 3. Select unpair if your device is still connected to your network, and delete if the device is no longer connected.
 - a. Unpair will redirect you through the excluding wizard of the device. You need to have physical access to the device as well.
 - b. Delete will simply delete the device from your Vera dashboard. This is used when the device is no longer present in your network.

Vite name Auton Sensor Boom Delete Up on have the device and it is still working and you want to remove it devices in missing or its broken Event Up on have the device and it is still working and you want to remove it devices in missing or its broken Event Up on have the device and it is still working and you want to remove it devices in missing or its broken Event Up on have the device and it is still working and you want to remove it devices in missing or its broken Event Up on have the device is missing or its broken Delete <	Motion Sensor	Remove devices now	× Remove devices now
Interpretation Room Room Delete If you have the device and it is still working and you want to remove it a system clicks. If is, if the device is missing or maturationing you can click Delete to remove it to uppart. If is, is, end the device is gone or broken so purget. Insure the device. Insure the device. Insure the device is gone or broken so purget. Insure the device is gone or broken so purget. Insure the device is gone or broken so purget. Insure the device is gone or broken so purget. Insure the device is gone or broken so purget. Insure the device. Insure the device. Insu	vice name	Unpair your device	Step 2: Pair Your Device
If you have the device and it is still working and you want to remove it from the system click Ungair. Else, if the device is missing or mafunctioning you can click Delete to remove it is process. I don't have the device anymore or it's broken I don't have the device anymore or it's broken Lick I don't have the device anymore or broken anymore or b	ation Sensor ligned to Room Room Delete	The controller is ready to remove the device and reset it. Please follow the devices exclusion instructions as described in the manual that came along with it.	If you still have the device and it is functional you should remove it by unpairing it properly, which rese the device so it can be included on another network and does not interfere with other devices on this network. If you are sure that the device is missing or
without going through the unpairing process. I have the device. Go back and try to reset it. Cancel Cancel Unpair Cancel	If you have the device and it is still working and you want to remove it from the system click Unpair. Else, if the device is missing or malfunctioning you can click Delete to remove it	I don't have the device anymore or it's broken Exit	it. This may take a few minute as we must first scan the network to be sure the device is not still responding. If it is, the purge will abort and you will have to remove the device by resetting it.
Unpair	without going through the unpairing process.		I have the device. Go back and try to reset it. Cancel
	Unpair		
			J

Note: Please make sure you choose the appropriate removal procedure based on your scenario. Using Delete on a device that is still powered and present in your network will cause the device to push itself back into your dashboard. This method does not reset the device's memory. Unpairing does.

The unpairing procedure is usually the same as the pairing procedure, but it requires that you have physical access to that device. For the devices that have a pairing button, it usually involves pressing that button a number of times. Check the device manufacturer manual as well. Sometimes the procedure needs to be repeated a number of times if the device is not paired with your first attempt.

4. If the unpairing was successful and the device was detected, you will get the following confirmation screen:



How to Connect Ezlo Secure to Another Z-Wave controller (Learn Mode)

Add an Ezlo Secure to another Z-Wave network

1. Go to the Settings from the side menu.

2. From the Settings, tap on Learning Mode.



	_	
	Settings	
CONTROLLER		
Net & Wi-fi		>
Energy monitoring		>
Unit Settings		>
Tech Support		>
Learning mode		>
Smart start devices		>
Z-Wave Settings		>
Notifications		>
LUA Scripts		>
APPLICATION		
PIN Codes		>

3. To add this hub as a secondary controller, tap on Enable Learning mode.

Note: Keep the controller powered during the inclusion process.



4. Once you press Enable Learning mode, you will see the Learning mode process is started. It may take a few minutes.



5. On the screen with a Learning mode process, you will see DSK code (contains 5 digits).

The Z-Wave S2 DSK PIN 5 digits are located on the bottom of the Ezlo Secure. You can also find the full DSK on the package box.



6. Copy this code and enter in the 3rd party app to add your controller as a secondary controller with a secure connection.



7. In the next step, you will see the progress while the controller is being added as a secondary controller in case the process didn't finish.



8. Once the inclusion is successfully finished you can start the Controller Copying process.

"Controller Copying is the process of updating network information from a primary controller to secondary controllers, such as node list and routing information. These steps are usually not required unless you have a multiple controller network. To initiate this process, start the Add Mode on the primary controller and the Learn Mode on the secondary controller. All Z-Wave network relevant information will be updated for the secondary controller."

9. Tap on the Start discovery button.



10. The discovery process has been started and you can see how many devices are discovered in the Z-Wave network

Note: Discovering devices may take a few minutes



11. Discovered devices will appear on the list of discovered devices. You can rename the discovered devices and assign them to a room. If you don't want to rename or assign to a room, just tap the Finish button.



12. To rename a discovered device or assign it to a room, select and tap on the device. Edit the device name in the field Device Name. To assign to a room, select the room from the list or create a new one, following the previously discussed process.

	_	
<	Device set up	
Device name		
Light bulb		
Room		
No room		>
_		
	Save	

Add another Z-Wave controller to an Ezlo controller's network

To add another controller to the existing Z-Wave network:

- 1. Go to side menu \rightarrow Devices
- 2. Tap on the +



3. Select from the list Controller and tap on it



 This option allows you to add another controller to your Z-Wave network. Tap Ready to include. When you tap Ready to Include the countdown of 60 seconds will appear.

Follow the instructions to activate the learning mode inside the controller's application. This function is usually located in the app settings or in the hub settings.

Note: Please make sure the controller you want to add doesn't have any Z-Wave devices added to it

< Add Controller	< Add Controller
This option allows you to add a secondary	This option allows you to add a secondary
controller to your Z-Wave network.	controller to your Z-Wave network.
Please make sure the controller you want to add	Please make sure the controller you want to add
doesn't have any Z-Wave devices included to it.	doesn't have any Z-Wave devices included to it.
Want to add an Ezio Controller ?	Want to add an Ezio Controller ?
Add Ezio controller	Add Ezio controller
Tap on "Ready to include" and then follow the	Tap on "Ready to include" and then follow the
instructions to activate the lerning mode	instructions to activate the lerning mode
inside the secondary controller's application.	inside the secondary controller's application.
Ready to include	00:59

5. If the controller has encryption and authorization supported

Select the connection security. S2 Access selected by default. To add the controller with the security connection you need to generate the DSK code in the controller's app or scan the QR code from the controller's box. Then tap on "Scan QR code" button



- 6. You can change the type of encryption. Enable toggle you will see the list of all connection types available.
 - Access Control Encryption connection
 - S2-Authenticated Encryption connection
 - S2-Unauthenticated Encryption connection
 - S0 Encryption connection
 - CSA Client Side Authenticated

Once you selected the type of encryption tap on the "Scan QR code"

If the S2 Access is checked, by default all options under Advanced are checked.

If the S2 Access is unchecked, all options under Advanced are unchecked.

You are able to select whatever options you want from the Advanced list.

S2 Access Full Security	
Advanced options Full list of security options	
Access Control Encryption connection	
S2-Authenticated Encryption connection	
S2-Unauthenticated Encryption connection	
S0 Encryption connection	
CSA Client side authenticated	

To add the controller with security connection you need to generate the DSK code in the controller's app or scan the QR code from the controller's box.

Scan QR code

On the box of the controller, you should find a QR code. You need to scan the QR code with your phone's camera. Once a QR code has been scanned, the inclusion process starts.



Scan QR code

QR code can be found on the box of your controller.

Enter DSK code manually



Enter DSK code manually

7. If you were unable to scan the QR code, you can add it manually.

Tap on the button Enter DSK code manually on the Scan Code screen.

Enter the first five digits of DSK code shown on the box of the controller.

- Enter DSK code Enter the first 5 digits of DSK code shown on the box of your device. 8 6 9 2 Continue 1 2 ^BC 3 DEF 4 сні 5 JKL 6 ^{м N O} 7 PORS 8 9 ^{w x y z} + * # 0 \otimes
- 8. If the controller has not encryption and authorization supported you will see the including controller process.



9. The controller is added to the system and you will see the Set Up Device screen. To continue, edit the name of the controller (by default will be displayed as "Controller"), assign it to a room, and click "I'm done."



 If the controller was added without encryption you will see the warning message on the top of the Set Up Device screen.



Remove Z-Wave controller from Ezlo hub network

- 1. Go to devices from the menu.
- 2. Select the controller you want to remove and tap on it.



Devices Q

Ву Туре

By Room

No room

前 +

Failed

3. On the Controller settings screen tap on the Delete button



4. On the confirmation pop-up tap Delete.

5. Go to a 3rd party app and activate learning mode.

6. The controller will be removed from the list of devices.



Controller

Delete controller To delete this secondary controller you need to press the delete button and after that you have 60 seconds to go in secondary controller's settings and select disable learning mode.

Cancel

 \times

<

Device name

Assigned to Room





Remove Ezlo controller from another Z-Wave controller's network

There are two ways to leave another controller's network:

Option 1

- 1. Go to devices from the menu.
- 2. Select the controller.
- 3. On the Controller settings screen tap on the Delete button
- 4. On the confirmation pop-up tap Delete.

ζ Controller	
Device name	
Controller	
Assigned to Room No Room	>
Z-Wave Settings	>
Scenes	>
Delete	

ς	Controller
Device name	
Controller	
Assigned to Ro	oom
No Room	
	× Delete controller
If you delete to disable lea exclude the E	the primary controller you'll need arning mode button in settings to Ezlo hub from the Z-wave network.
	Delete
	Cancel

5. Go to the 3rd party app from which you want to remove an Ezlo controller and follow the instructions in that app.

6. In the Vera app, tap on the Disable learning mode button.

7. In the confirmation pop-up, tap Disable.





Learning Mode

Learning mode

<

Tap on "Disable learning mode" button to exclude this controller from the primary controller.

This action will remove from this controller all Z-Wave devices - you'll have to use the primary controller to manage them. Option 2

1. Go to the Settings screen from the side menu.



2. From the Settings screen, tap on Learning Mode.

	Settings	
CONTROLLER	2	
Net & Wi-fi		>
Energy mon	itoring	>
Unit Setting	5	>
Tech Suppo	rt	>
Learning mo	ode	>
Smart start	devices	>
Z-Wave Sett	ings	>
Notification	s	>
LUA Scripts		>
Battery		>
APPLICATION		
PIN Codes		>

3. To remove Ezlo hub from another controller, tap on Enable Learning mode

Note: Keep the controller powered and near others during the removing process.

4. Go to a 3rd party app from which you want to remove an Ezlo controller and follow the instructions in that app.



Controller Reset

Push and hold the RESET button at least 5 sec (on Ezlo Secure LED starts blinking RED), After that your Ezlo controller will be reset to factory defaults.



Note: If this controller is the primary controller for your network, resetting it will result in the nodes in your network being orphaned and it will be necessary after the reset to exclude and re-include all of the nodes in the network. If this controller is being used as a secondary controller in the network, use this procedure to reset this controller only in the event that the network primary controller is missing or otherwise inoperable

Reset to Factory Settings remove all the information about added devices and reset Z-Wave chip (new Home ID, new S0/S2 keys, remove all Z-Wave nodes), scenes created, House modes settings, etc. The process is irreversible.

How to rediscover the device node

 Go to the Devices screen and tap on the > button to see the device options and tap on the Z-Wave settings option

2. In General settings, select Rediscover device and tap on it.



Z-Wave settings General Reset to default settings All parameters added manually will be deleted. Rediscover device Z-Wave parameters Z-Wave parameters allow you to manually fine-tune device settings and you can add a new parameter. 30 Alarm configuration - 1st slot Synchronized 44 Power reports Synchronized (2) (4) (2) (3) (3) (3) (3) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4)			
General Reset to default settings All parameters added manually will be deleted. Rediscover device > List of parameters Z-Wave parameters allow you to manually fine-tune device settings and you can add a new parameter. 30 Alarm configuration - 1st slot Synchronized 44 Power reports Synchronized Expected and the set of the set o	<	Z-Wave settings	
Reset to default settings All parameters added manually will be deleted. Rediscover device > List of parameters Z-Wave parameters allow you to manually fine-tune device settings and you can add a new parameter. 30 Alarm configuration - 1st slot synchronized 35 Duration of alarm signalization synchronized 44 Power reports synchronized	Genera	I	
Rediscover device > List of parameters Z Z-Wave parameters allow you to manually fine-tune device settings and you can add a new parameter. 30 Alarm configuration - 1st slot 30 Alarm configuration - 1st slot Image: Comparison of alarm signalization synchronized 35 Duration of alarm signalization synchronized Image: Comparison of alarm signalization synchronized 44 Power reports synchronized Image: Comparison of alarm signalization synchronized 44 Power reports synchronized Image: Comparison of alarm signalization synchronized	Reset to All paramete	default settings rs added manually will be deleted.	
List of parameters Z-Wave parameters allow you to manually fine-tune device settings and you can add a new parameter. 30 Alarm configuration - 1st slot Synchronized 35 Duration of alarm signalization Synchronized 44 Power reports Synchronized	Redisco	ver device	>
List of parameters Z-Wave parameters allow you to manually fine-tune device settings and you can add a new parameter. 30 Alarm configuration - 1st slot Synchronized 35 Duration of alarm signalization Synchronized 44 Power reports Synchronized			
Z-Wave parameters allow you to manually fine-tune device settings and you can add a new parameter. 30 Alarm configuration - 1st slot Synchronized 2 35 Duration of alarm signalization 2 44 Power reports 2 Synchronized 2 44 Power reports 2 45 Power reports 2 46 Power reports 2 47 Power reports 2 47 Power reports 2 47 Power reports 2 47 Power reports 2 48 Power	List of p	parameters	
device settings and you can add a new parameter. 30 Alarm configuration - 1st slot Synchronized 2 35 Duration of alarm signalization 2 44 Power reports 2 Synchronized 2 44 Power reports 2 (2)	Z-Wave p	arameters allow you to manually	fine-tune
30 Alarm configuration - 1st slot 35 Duration of alarm signalization 44 Power reports synchronized	device se	ttings and you can add a new pa	rameter.
30 Alarm configuration - 1st slot 2 Synchronized 35 Duration of alarm signalization Synchronized 2 44 Power reports 2 Synchronized 2			
35 Duration of alarm signalization Synchronized 44 Power reports Synchronized +	30 Alarn Synchronize	n configuration - 1st slot	L
44 Power reports 2	35 Dura Synchronize	tion of alarm signalization	L
÷	44 Powe Synchronize	er reports	L
Ŧ			
+			
•			
•			
-			(+)
			-

3. On the rediscovery device screen tap on the Rediscover button. The rediscovery process will start.



You're now ready to enjoy smarter home control.

