



S360 BOX

QUICK START GUIDE

INTEGRATIONS & API

Package contents

- 1x S360 BOX
- 1x DC power supply
- 1x Screws & plug set
- 1x Quick start guide



S360 Box

QUICK START GUIDE

Important before usage

When **booting** the device **for the first time**, it is **essential** to connect the device to the internet and to **don't reboot or unplug the device for a timeframe of 15 minutes**, so that all latest updates can be downloaded.

If this procedure is not followed, software problems can occur.

After updates are downloaded, the box can be plugged/unplugged or rebooted as desired.

Mounting the device

It is possible to wall mount, rackmount or place the S360 Box on a flat stable surface.

To mount the S360 Box on a wall, please use the included M4 screws and drill a hole 50mm deep.

Use the included wall anchors to screw the S360 Box to the wall, taking care not to over-tighten the screws which could damage the S360 Box housing.

Connecting the device

Plug in the internet access cable, the camera network access cable and DC power supply.

Network connection

Verify if a dynamic IP address for the internet port is obtained automatically by a local DHCP server. When there is no DHCP server available, manually set an IP address.

More information on how to do this can be found on the Partner Portal.



Using the device

When turning on the device, the power LED on the front of the device should be **red**.

The status LED will turn **orange** when the device starts booting.

When the status LED starts blinking **red** and the IP addresses occur on the screen, the device is booted and ready for action.

Log in to your S360 Partner portal to register the device.

The serial number needed to register the device is located on the side of the S360 Box and on the outside label of the shipping box.

Once the device is configured in the Partner Portal and the camera's (with the correct settings) are connected, the status LED turns **green**.





How do I login to my S360 BOX?

Verify that your computer is connected to the same network (INTERNET & CAMERA) as the S360 BOX and that the S360 BOX is running, then follow the steps below:

STEP 1: Open your web browser and enter the serial number of the S360 BOX into the address bar (not in google). Use **http://** in the url: **http://SERIALNUMBER**

STEP 2: You should be taken to the S360 login page. Use the same credentials as you do when you login to our Partner Portal

If your login is successful, you will be redirected to the S360 BOX web interface, where you can:

- verify cameras (connections & recent detections)
- change complete network configuration (INTERNET & CAMERA)
- test outputs
- reboot the device

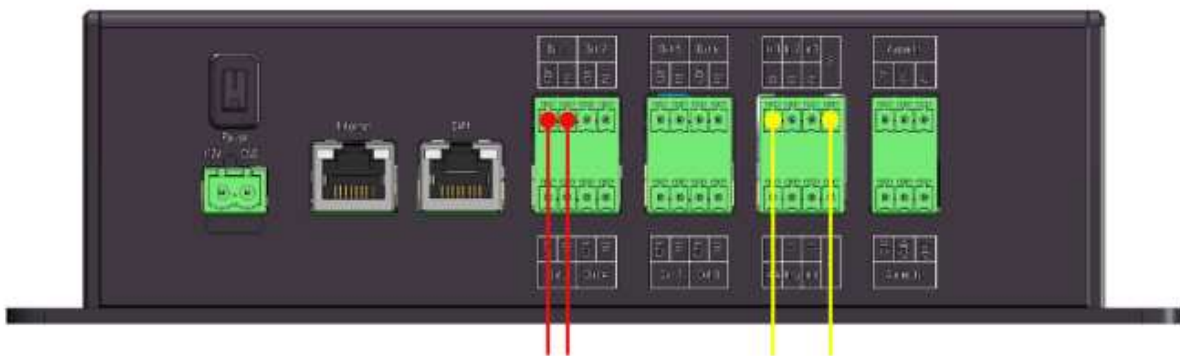
Check your firewall and port configuration rules

Our S360 BOX allows communication from an on-premises server to our cloud using supported protocols. The following table can be used as a guideline when configuring firewall rules for the underlying servers where our S360 BOX is hosted:

PROTOCOL	PORT	
MQTT	8883 (tcp)	Outgoing
AMQP	5671 (tcp)	Outgoing
HTTP	80 (tcp)	Incoming/Outgoing
HTTPS	443 (tcp)	Incoming/Outgoing
CUSTOM	3262 (tcp)	Incoming/Outgoing
CUSTOM	36022 (tcp)	Incoming/Outgoing
SSH	22 (tcp)	Incoming/Outgoing (NOT needed by default. Only when debugging issues within local network)
NTP	123 (tcp)	Outgoing

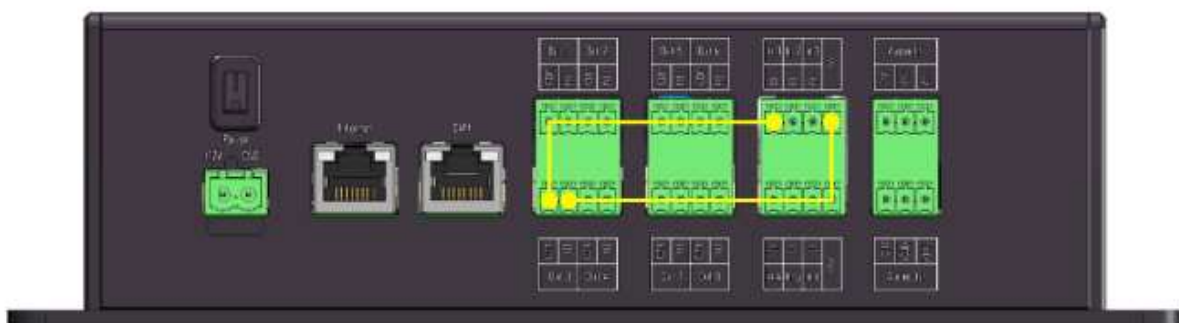
Activate S360 BOX through an alarm panel

Attach the alarm panel's alarm input to S360 BOX output 1 COM and NO (Alarm Output 1).
 Attach the alarm panel's output to the S360 BOX input 1 (Zone 1 Input).
 You can configure different zones.



Activate S360 BOX through a weekly schedule part 1

Attach one of the box outputs to the input.
 If you have multiple zones, you need to link one output to one input per zone.
 In the example below, output 3 is linked to input 1.
 Then configure the same connection in our Partner Portal.
 You can then setup your weekly schedule.



Activate S360 BOX through a weekly schedule part 2

Also go to the Partner Portal and go to tab 'S360 boxes'.

Then click on the '...' under 'Actions' and select 'Zones, inputs & outputs'.

Then click on 'Next' and add 'SO1' under Output 3 to configure the connection in the Partner Portal.

I/O Configuration

On this screen, you see a list of all available output & input actions. The alarm outputs linked to a partition are fixed and not changeable.

You can configure the remaining outputs by selecting an output action for every remaining output.

Inputs 1-3 are reserved for arming/disarming partitions, inputs 4-6 are reserved for error input (eg sabotage detection from camera)



Error output

You can connect one of our outputs to your alarm panel as a self-check. Whenever the S360 BOX is in "error" state, this output will be triggered.

By default 'output 2' will be used, but another output can also be configured by the installer.

More info on the output/input configuration can be found in our Partner Portal FAQ.



Warnings and notices

- Use of controls or adjustments or performance of procedures other than those specified here, may result in hazardous radiation exposure.
- Do not attempt to service or repair this product --> return it to Secury360 for service.
- Do not permit anyone other than Secury360 to service, repair or adjust this product.
- Do not attempt to open or modify this device except as described in this document.
- Do not operate this device if it is damaged or if the covers/seals are missing or damaged.
- Warranty void if the device is opened or if the covers and/or seals are missing.

For product support, contact support@secury-360.com

Operating temperature	-20°C - 50°C	
Storage temperature	-40°C - 70°C	
Maximum humidity	10% - 90% non condensing	
Discrete I/O operating limits	Input	conductor size 0,2 - 2,5 mm ² (24 - 12 AWG)
	Output	conductor size 0,2 - 2,5 mm ² (24 - 12 AWG) 2A@30VDC / 0.5A@125VAC
Power	Nominal 12 V DC +/- 20%, maximum power 12W, maximum current 1A	



S360 Box Integrations & API

Integrating Secury360 with other software

Secury360 now offers the possibility to integrate its revolutionary artificial intelligence with third party software. At this moment we've made it possible to communicate with the following software and video management systems.

Integration with SIA



Through SIA-DC-09 Secury360 can send an event to the receiver.

HOST	IP address receiver
PORT	Port receiver
ACCOUNT NUMBER	PROM number receiver
ENCRYPTION KEY (optional)	In case encryption of the message is required
EVENTS	Enable additional event types to your central station integration by checking the boxes as shown in the figure below

Events

S360 intrusion detection events to the central station are always activated.
You can enable additional event types to your central station integration by thicking the boxes:

S360 events:
☒ Intrusion detection
☐ Heartbeat
☐ Camera error
☐ Zone armed
☐ Zone disarmed
☐ Internet error
☐ Box connected
☐ Box disconnected

Input based events:
☐ Camera tamper input 4-5



Integration with immix

Through immix, an email is sent to the control room in case of detection. This email contains details of the alarm (place, time, camera) and a link to the video fragment of detection.

SMTP	IP address of the control room
SMTP PORT	Port of the control room
SITE IDENTIFIER	Unique immix ID

If feedback of the control room is wanted:

CS IDENTIFIER	Username of the feedback address (username@domain)
ALARM FEEDBACK DOMAIN	Domain of the feedback address

Alarm trigger based on:

AI	Our AI triggers the alarm and control room simultaneously
CENTRAL STATION RESPONSE	Alarm is only triggered if control room confirms the detection



Integration with Genetec

SERVER	IP address of the Genetec server
USERNAME	Username of the API
PASSWORD	Password of the API
USERGROUP	GUID of the usergroup to which the alarms need to be sent (it is necessary to make a specific usergroup for Secury360)

Integration with NetworkOptix

HDD installation

Open the bottom lid of the S360 box by loosening 2 screws on the bottom of the S360 box. Place your HDD between the brackets on the inside of the lid. Then attach the HDD to the lid using the 4 M3x8 screws.

When opening the lid, a SATA cable is visible, connect the cable to your HDD.

Close the lid of the S360 box by fastening the 2 screws on the bottom of the box.

Configuration in Secury360's Partner Portal

Important: A local connection is required to do the first setup.

Log in to the Secury360 Partner Portal through your web browser: <https://partner.secury-360.app/>

Go to the tab 'S360 boxes' (Clients>Name>S360 boxes)

Add your S360 box by entering the Serial Number.

Go to 'Actions' and click on 'Settings'

Enable Network Optix VMS by checking the box, then click 'Save'.

The button 'Mount HD' appears, click on it, then click 'Save'.

The Network Optix software is now running on your S360 box.

Go to <https://nxvms.com/download/> and download the Network Optix Client software compatible with your system.

When opening the Network Optix client software, a new server will be detected named after the serial number of your S360 box. You will be asked to register a login name and a password.

Important: To start recording video, a Network Optix license key is necessary.

Visit <https://www.networkoptix.com/nx-witness/request-nx-witness-pricing> to obtain a license.



Bookmark detections of Secury360 in NetworkOptix

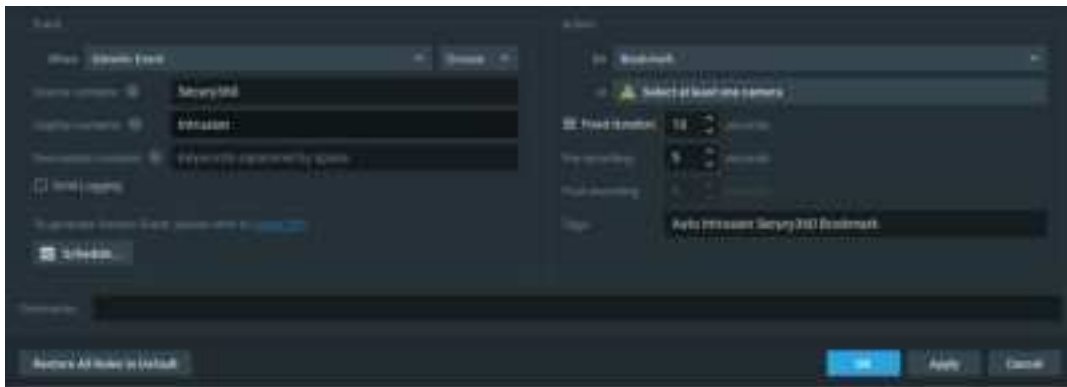
Configuring the Partner Portal

USERNAME	Username used in NetworkOptix
PASSWORD	Password used in NetworkOptix

Configuring NetworkOptix

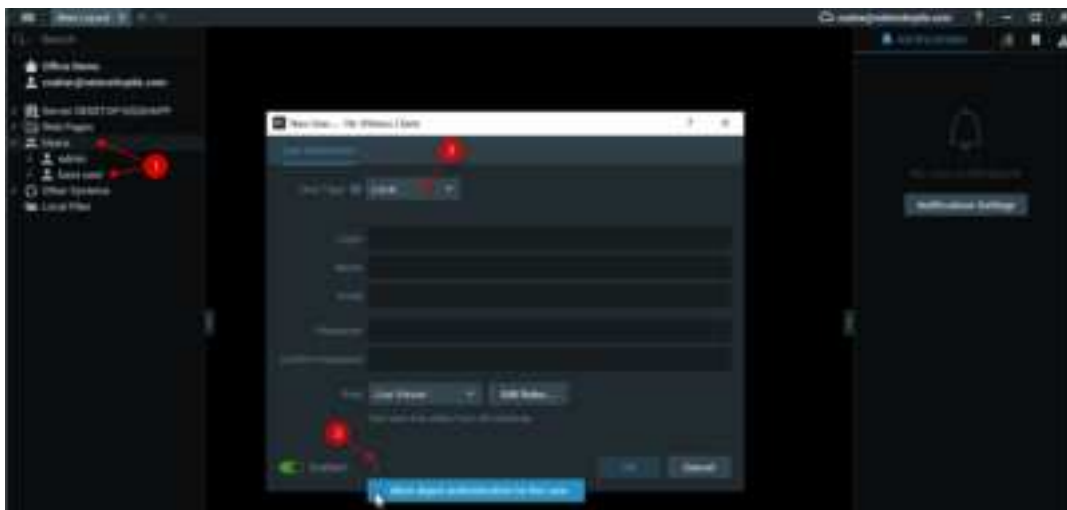
In NetworkOptix it is necessary to add a Rule in order for the detection to appear as a bookmark.

1. Right click on 'Notifications' and select 'Event Rules...'
2. Click on '+ Add'
3. Make a rule as shown below:

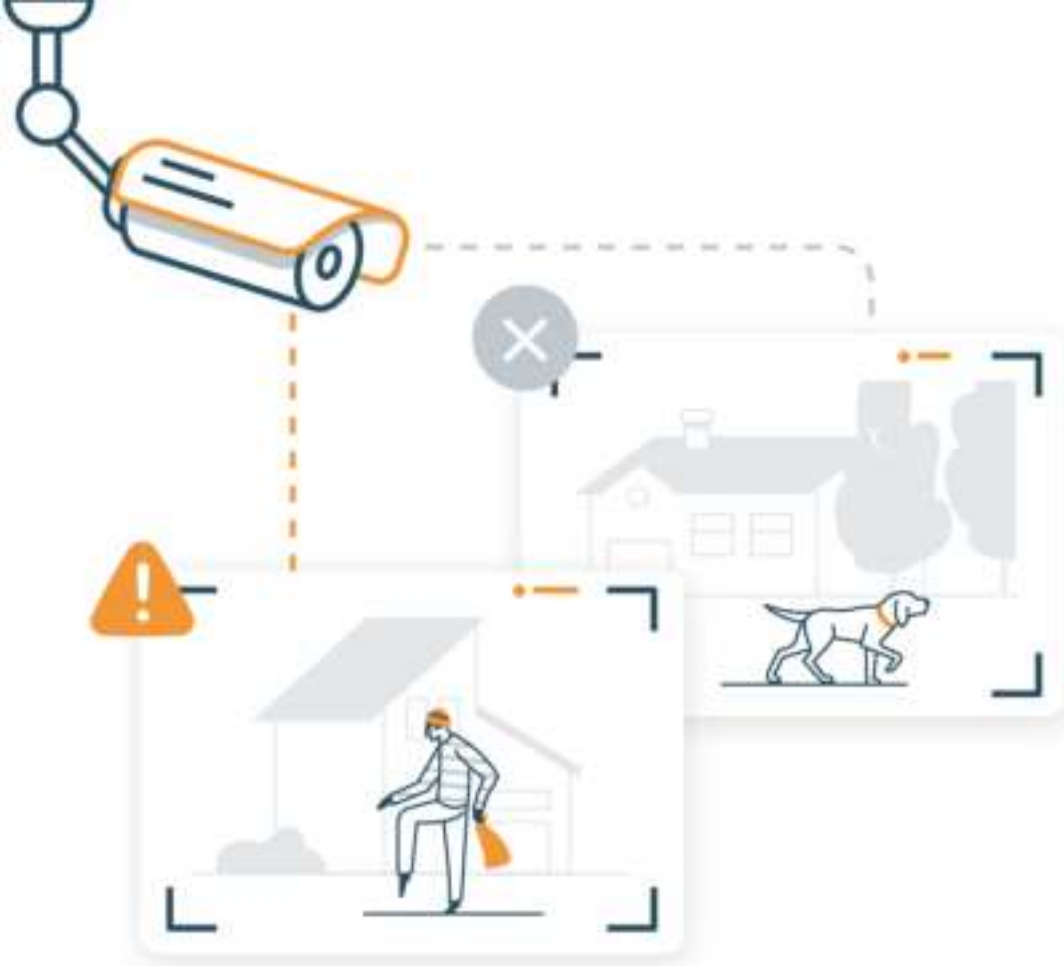


Enable digest authentication for the user:

1. Do one of the following:
 - Right-click on an existing Local User and select **User Settings**.
 - Right-click **Users** and select **New User**.
2. If creating a new user, select **Local** and enter the desired information.
3. Click on the 3 vertical dots and select **Allow digest authentication for this user**.
4. Click **OK**.



NOTE: When using authentication, it is mandatory to use lowercase credentials. We aim to support uppercase credentials in the future.



Contact information

info@secury-360.com

+32 (0) 11 36 26 46

Or go to: www.secury-360.com