

ASTRA HSC Server (Hardware And Software Complex)



Platform for the collection of telemetry data and remote control of engineering systems.

What is Astra CSH?

A cloud platform to organize a unified monitoring system for remote objects over the Internet.

Astra CSH nomination

Additional comfort, security and efficient use of energy for the owners.

Server hardware varies depending on the number of objects supported, as well as other factors.

Features

The complex is built on the basis of the "High Performance Multifunctional Server Platform of the Central Monitoring System", whose base is the "Gentoo Linux" operating system, as the most productive of the entire "Unix" family.

Its main feature is that it is supplied in source codes, which allows, in the first place, to use it in all existing hardware platforms without restrictions, from supercomputers to mobile devices, and secondly, to have total control in terms of security (in the system it is not possible to implement open source bookmarks, which is especially important in light of the latest virus attacks on Windows computers, where attackers use markers set by the manufacturer).

The operating system update is carried out in the form of a continuous version (Rolling-Release) without a clear division into versions, which allows you to keep all versions running in the same current state.

After a long test, the InnoDB database engine was chosen as a subsystem to store information.

To isolate data from unauthorized access, the server platform provides access to them through strictly regulated interfaces of the corresponding services (and never directly through the DBMS or with each other). For this, in the complex as part of the server platform there are corresponding services:

"Application service": is designed to exchange information with observers (operators of workstations, mobile applications and user websites)

"Event service", which provides the exchange of information with the controllers of the information transfer systems (ITS) of terminal object devices

The "ITS controllers", which are isolated from the DBMS through the "Event Service" and implement the exchange of data in the communication channels of the corresponding STI and can be implemented in both hardware and software, and in different platforms.

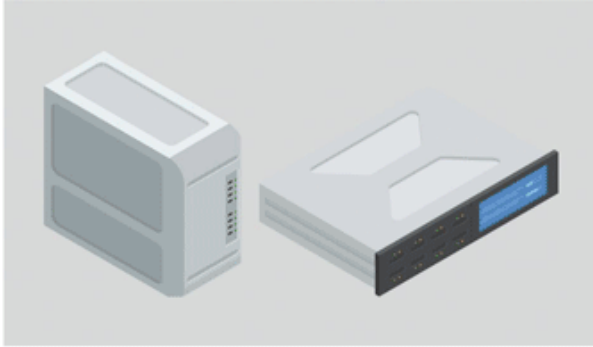
Astra CMS is a multi-user system with strict delimitation of access rights by groups of objects and by user roles.

A server platform can provide independent operation of several separate organizations or structural divisions. Within each organization, an unlimited number of separate groups can be created: "domains", which can be separate monitoring centers and end user groups (for example, family members who have access to a shared department).

A unique data transmission system has been developed on a constantly open TCP channel for CSH. This means that the Astra team constantly maintains an asynchronous communication channel open with the server and is ready for exchange at any time, regardless of who initiates the exchange. At the same time, this functionality is provided without additional VPNs, tunnels, opening IP ports on terminal devices, as well as without the use of "white" IP addresses.

Astra CSH is designed in such a way that it can be integrated into any existing STI as soon as possible, as well as transmit information to third-party information processing systems. For these purposes, standardized interfaces and information exchange protocols have been developed: "Interface point with SPI" and "Interface point with AWP".

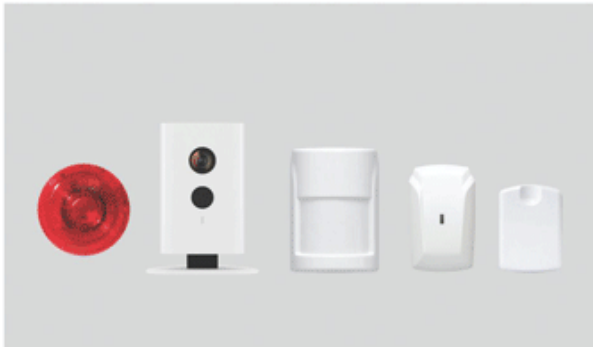
Astra HSC Content



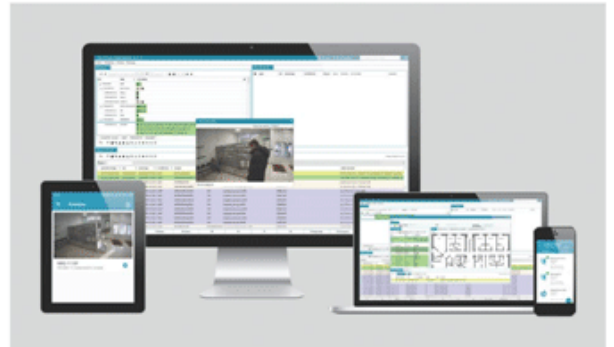
4. Cloud server



3. Security Hub intelligent controller



2. Wireless devices



1. Client servers

CLOUD SERVER

Parameter	Value
operating system	UNIX (Gentoo Linux)
CPU	Intel Core i3
RAM	16 Gb
solid state drive SSD	250 GB
hard disk drive HDD	1 TB
used communication channels	LAN
communication channel control	constant
exchange protocol encryption	Keys

	128bit
integration with third-party services	iVideon, Firebase Cloud Messaging, Irbis, Surgard

Technical data

Technical requirements for server parameters:

operating system	UNIX (Gentoo Linux) that supports the POSIX.1c branching mechanism, thread extensions (IEEE Std 1003.1c-1995)
processor capacity	32 or 64 bits (compatible with x86 or ARM), for a specific implementation it is recommended to use the Intel x64 platform (family of Core iX and Xeon processors of the fourth generation of Haswell microarchitecture)
processor performance	2 gigaflops
random access memory volume	1 GB
HDD / RAID volume	250x2 GB / RAID software per operating system
ethernet speed	100 Mb /s

Technical requirements for PC parameters to install AWS (Automated Workstation):

operating system	Windows 7 or late version
other software	.NET Framework 4.5 y superior
processor	Intel Core i3 de 1.4 GHz o superior o equivalente AMD
random access memory	al menos 2 GB
hard disk space at least	50 MB
monitor (recommended configuration):	

- diagonal	20 inches
- aspect ratio	16: 9
- permit format	1920x1080

Astra HSC capacity:

subscriber (object) controllers, not less than	1,000,000
subscriber applications, not less than	300,000
simultaneous sessions of web interfaces, not less than	10000

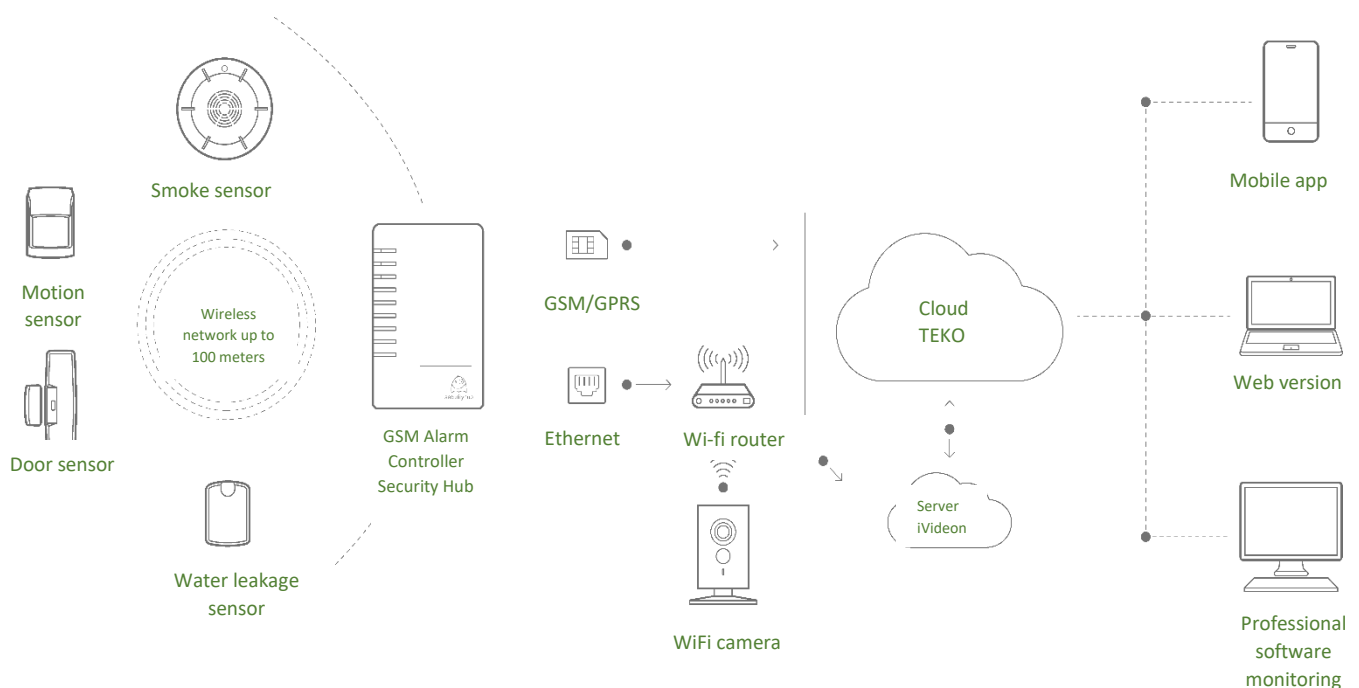
Solutions:

➤ TIMELY NOTIFICATION ABOUT:

- invasion and fire
- gas and water leaks
- electrical power interruption
- temperature changes and problems in the heating system

➤ COMFORTABLE LIFE :

- control of lighting, blinds and / or curtains
- climate control in apartments
- collecting data from resource metering devices
- remote video surveillance



Hosting on the SECURITY-HUB public server:

Service	Integrator
Subscription cost	no
Number of connections	up to 1000
Mobile app	free
Web Application	free
Local configuration, administration, surrender and management software	free
Technical support	24/7
Updates	yes
Partner base and software interface ads	yes

Services	More than 1000 connections	When buying 300 and more Security Hub devices
Precio de software	1000 \$	free
Instalación y activación de software	free	free
Aplicación móvil propia	free	free
Aplicación WEB	free	free
Software local de configuración, administración, rendición y gestión	free	free
Server technical support	8/5	8/5

Integration with third party software (SurGuard)	yes	yes
Controller's own brand	agreed	free
Total own brand, integration to business processes	agreed	agreed
Integration with third-party programmatic platforms	free without changing the platform structure	free without changing the platform structure
Access to updates (annual)	-	-


Download Astra HSC Client

The program can be downloaded here: <https://dl.security-hub.ru/Test/public/install-1.4.0.1.exe>

Monitoring system

To begin, you must enter the username and password of the organization administrator received from the public server administrator.

Authorization
✕



Login:

Password:

Remember me

Version: 1.4.0.1

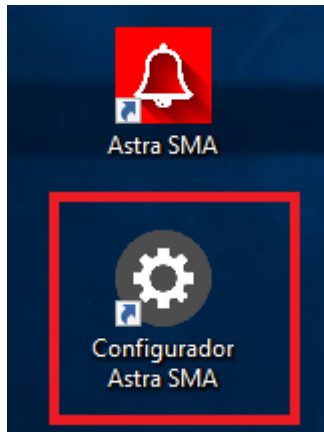
ATTENTION!

With the same account you cannot log in from different devices at the same time!

Configurator

The Astra Configurator monitoring station is a utility that allows you to configure Astra HSC. For example, configure / change server IP addresses.

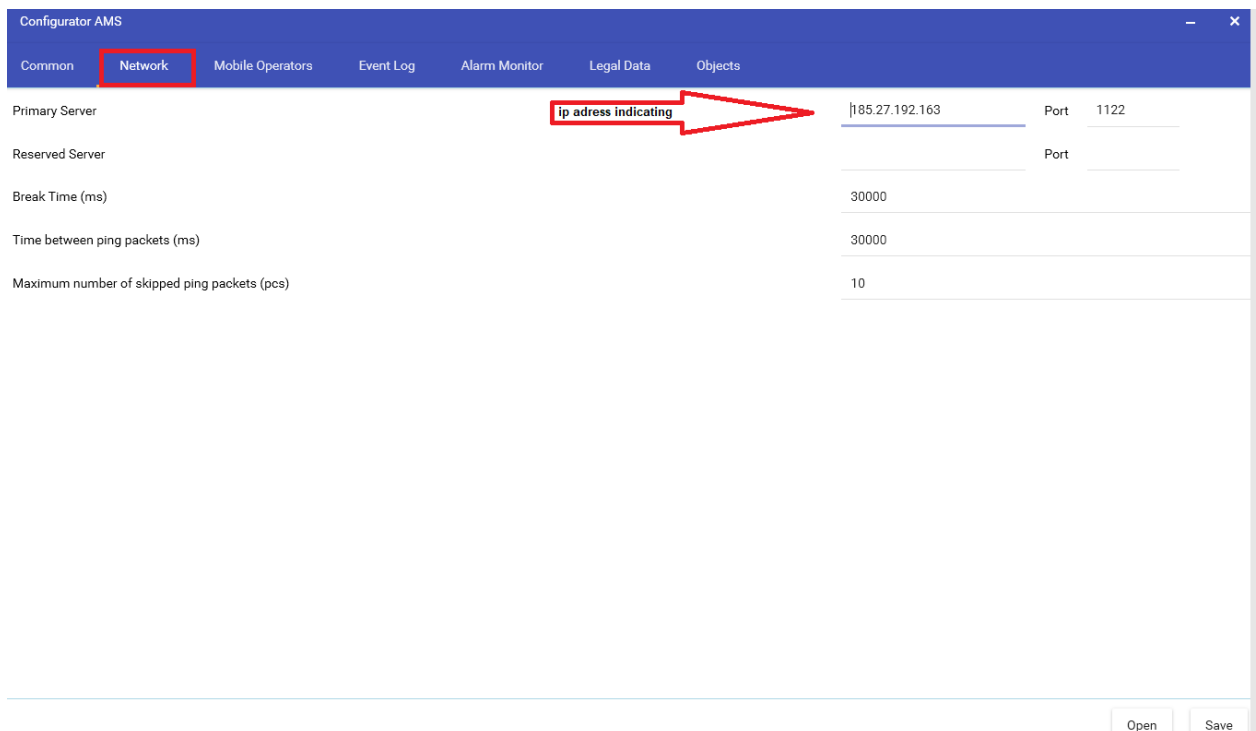
When installing the Astra HSC workstation, the configurator shortcut is installed on the desktop of your computer.



All settings are default, you can change them if necessary.

After changing the settings in the Configurator, click on the "Save" button and re-enter the workstation.

In the Network tab, you can change the server address. The remaining configuration, with a good Internet connection ($\leq 10\text{Mb}$), we recommend not modifying it.



On the **Event Log** tab, activate in the fields that should be displayed.

Events on objects without contracts: if the opposite is ✓, the effects on these objects will not occur if they do not have a valid contract.

The image shows a screenshot of the 'Configurador AMS' application window. The top navigation bar includes tabs for 'Common', 'Network', 'Mobile Operators', 'Event Log' (highlighted with a red box), 'Alarm Monitor', 'Legal Data', and 'Objects'. The main content area lists several configuration options:

- Event Key: Show
- Occurrence: Show
- Event Source: Show
- Events on objects without contracts: Hide
- The time period for which to request events: 1
- Informativeness: Maximum (dropdown menu) with a 'Customize' button.

At the bottom right of the window, there are 'Open' and 'Save' buttons, with the 'Save' button highlighted by a red box.

In the **Legal Data** tab, it is possible to include fields such as TIN, OGRN and PPC. These fields are shown when creating organizations, contracts, contractors.

The image shows a screenshot of the 'Configurador SMA' application window. The top navigation bar includes tabs for 'Común', 'Network', 'Operadores móviles', 'Registro de eventos', 'Monitor de alarma', 'Datos legales' (highlighted with a red box), and 'Objetos'. The main content area lists three configuration options:

- Campo TIN: Habilitado
- Campo OGRN: Habilitado
- Campo PPC: Habilitado

At the bottom right of the window, there are 'Abrir' and 'Save' buttons, with the 'Save' button highlighted by a red box.

Organization Creation

The server administrator creates the organization on the server administrator's workstation.

Server administrator

Server administrator: is the user responsible for creating security organizations (Security guard, private security) that work on a public server. Appoint administrators of security organizations.

Public Server Administrator Workstation

The public server administrator's workstation is designed to create organizations that plan to organize the protection of objects on a public server. After activating the server administrator function, the user has the opportunity to carry out the creation of organizations, as well as to designate their administrators.

* By purchasing your own server, you have the possibility of creating organizations as a general administrator (super administrator)

Create users of the organization

The users of the organization are created by the administrator of the organization.

The ORGANIZATION ADMINISTRATOR can create non-domain users and domain users.

Server Roles:

Server administrator

Server Administrator: the user responsible for creating security organizations that work on the Astra HSC server. Appoint administrators of security organizations.

Rights:

- Create and delete organizations.
- Management (creation / elimination / edition) of users of organizations and their visualization.
- Import devices to the server.

Organizational Roles:

Administrator (organization)

Organization administrator: a user responsible for creating domains and determining their address space. Assign domain administrators and create users between domains:

"Lawyer", "Engineer" and "Operator". A different combination of roles is possible for a user. All roles can be added to the Organization Administrator.

Rights:

- Domain Management
- Manage domain users.
- Local management organization.
- Object creation assistant: creation and delegation of objects to the PTO domain.

BCS operator (organization)

BCS operator: a user who has the ability to view devices, events, delegations of objects, in domains that belong to this organization

Rights:

See devices, objects, users, delegations, events, etc.

Lawyer (organization)

Lawyer of the organization: pre-contractual and contractual work with contractors. Creation of a contract for the protection of the installation. Provide a procedure to finish objects. The database created by this role is used by all domains of the organization.

Rights:

- Object management (add /delete /edit).
- Counterparty management.
- Contract management.
- Revocation of delegation of objects.

Engineer (organizations)

Organization engineer: a user who has the following rights: add, edit and delete devices from objects related to this organization; to link a device to a domain, send commands to a device, etc.

Rights:

- Device management (link to domain, object, decoupling) and visualization.

- Send commands to the device.
- Rename / delete zones.
- See delegations.

Domain Roles:

Administrator (domain)

Domain administrator - user - domain curator. Create users with the rights of "service monitoring station", "operator", "engineer";

Rights:

- Manage domain users.
- See and remember delegations.

Operator (domain)

A domain operator is a user who organizes work with clients to ensure that objects are taken under protection, primary processing of alarm messages and service, for subsequent transfer to the duty officer and the detention group.

Rights:

- See objects, their schemes, protection programs, devices, events, etc.
- Alarm management:
- Taking alarm for processing.
- Transfer of an alarm to the destination.
- Closing the alarm.
- See users (economic organizations) of a delegated object.

Domain Roles:

Administrator (domain)

Domain administrator - user - domain curator. Create users with the rights of "service monitoring station", "operator", "engineer";

Rights:

- Manage domain users.
- See and remember delegations.

Operator (domain)

A domain operator is a user who organizes work with clients to ensure that objects are taken under protection, primary processing of alarm messages and service, for subsequent transfer to the duty officer and the detention group.

Rights:

- See objects, their schemes, protection programs, devices, events, etc.
- Alarm management:
- Taking alarm for processing.
- Transfer of an alarm to the destination.
- Closing the alarm.
- See users (economic organizations) of a delegated object.

Lawyer (domain)

Domain lawyer: the functionality of the role is similar to that of the "lawyer of the organization", limited by the domain.

Rights:

- Object management and visualization.
- See counterparts.
- See contracts.
- Manage the delegation of objects using a code engine.

Engineer (domain)

Domain Engineer: the user who sets the composition of the equipment used in the protected object. Perform analysis on false positives and routine maintenance.

Rights:

- Management of objects, their schemes and visualization.
- Device management (link to domain, object, decoupling) and visualization.
- Rename / delete partitions / zones.
- See delegations.
- Management and visualization of the safety schedule.
- See users (economic organizations) of a delegated object.

PTsO in service (domain)

The monitoring station in service: a user who has this role can manage alarms, that is, take alarms for processing, send them to the alarm clock, close alarms, etc.

Rights:

- Alarm management
- Taking alarm for processing.
- Accept an operator alarm.
- GZ alarm transmission.
- Closing the alarm.
- See objects, devices, events, security schedules, etc.

Home Authority (domain)

Economic organization: a user who has this role can send commands to devices, for example, take / remove an object, etc.

Rights:

- Sending commands to the device.
- Detention group (domain)

Stop group: the user who verifies the protected object after the alarm message.

Rights:

- See objects, their schemes, protection programs, devices, events, etc.
- Alarm management
- Acceptance of an alert for processing.
- Alarm transmission and shutdown.

PT Dispatcher(domain)

PT Manager: A user who receives and processes alarms, transmits information about alarms and can also close an alarm on behalf of PT that are in the same domain. This role works simultaneously with the Duty CCO role.

Rights:

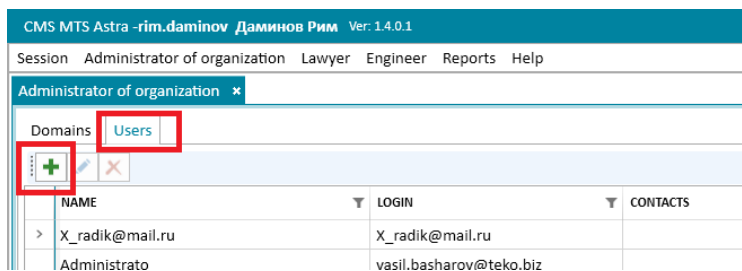
- See objects, their schemes, protection programs, devices, events, etc.
- Alarm management
- Acceptance of an alert for processing.

- Alarm transmission and shutdown.

Create a domain user and mobile application user

Domain creation

The creation of a domain is realized by the organization administrator. Click **+** to add the user or domain.



Create new user

Name:

Login:

Password:

Contacts:

Phone:

Active:

Domain user

Domain:

Mobile app user

Administrator Lawyer

Operator CMS duty person

Engineer Admin.body

DG DG dispatcher

Out-of-domain user

CSB operator:

Lawyer:

Accountant:

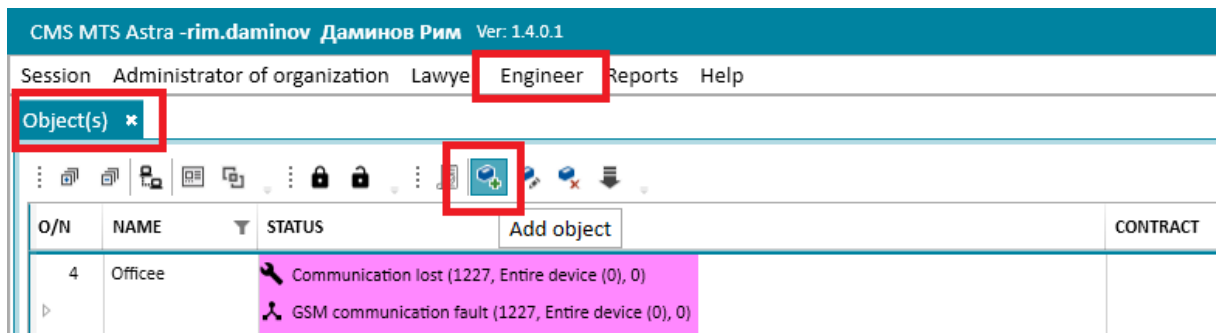
Engineer:

Save

Add an object

The user adds an installation with the roles of Lawyer of the organization or Lawyer of the domain.

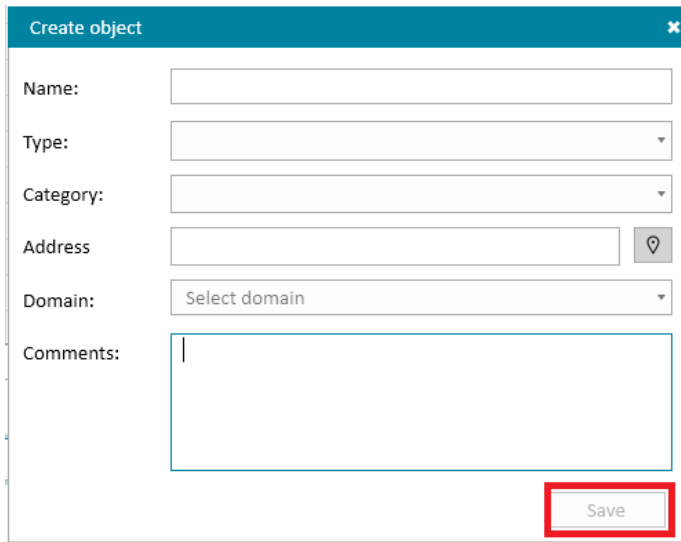
In the "Objects" tab, select the add installation icon.



Enter the installation name under the contract, determine its type, category and enter your address.

To enter the address, the Russian KLADR classifier is used, you must enter 4 to 5 letters of the city name and SELECT the proposed name from the list. Without SPACES, enter the name of the street. We enter the house and apartment number in usual order. Below is a box for comments, if necessary, you can write additional information about the installation.

Click on the "Save" button.



The screenshot shows a 'Create object' form with the following fields: Name (text input), Type (dropdown), Category (dropdown), Address (text input with a location pin icon), Domain (dropdown with 'Select domain' text), and Comments (text area). A red box highlights the 'Save' button at the bottom right.

New installation created successfully. It will appear on the "Objects" tab.

Add a device (Security Hub)

The addition of a device is done in the Astra HSC by a user with the role of Domain Engineer.

In the "Devices" tab, select the Add device to domain icon.



The screenshot shows the Astra HSC interface. The top bar displays 'CMS MTS Astra -rim.daminov ДАМИНОВ РИМ Ver: 1.4.0.1'. The user is logged in as 'Administrator of organization Lawyer Engineer'. The 'Devices' tab is selected, and the 'Add device to domain' icon is highlighted with a red box. Below the icons is a table with columns: O/N, NAME, BJECT(S), DOMAIN, DELAY, TYPE, and STATUS.

O/N	NAME	BJECT(S)	DOMAIN	DELAY	TYPE	STATUS
-----	------	----------	--------	-------	------	--------

The basis of the identifier when adding the "Security Hub" terminal device is the barcode located on the device board.

There are two types of barcodes on a device:

1. The barcode of a device released before January 2019 looks like this:



Complete: device address - device serial number, PIN code - last 4 digits in the device barcode. And select the cluster ("Security Hub or Astra Pro 4.0"). Click on the "Add" button.

Assign device to domain	
Device address (account):	<input type="text" value="00002333"/>
PIN:	<input type="text" value="2789"/>
Cluster:	<input type="text" value="Security Hub или Астра Pro 4.0"/>
<input type="button" value="Add"/>	

2. The barcode of a device launched since January 2019 looks like this:

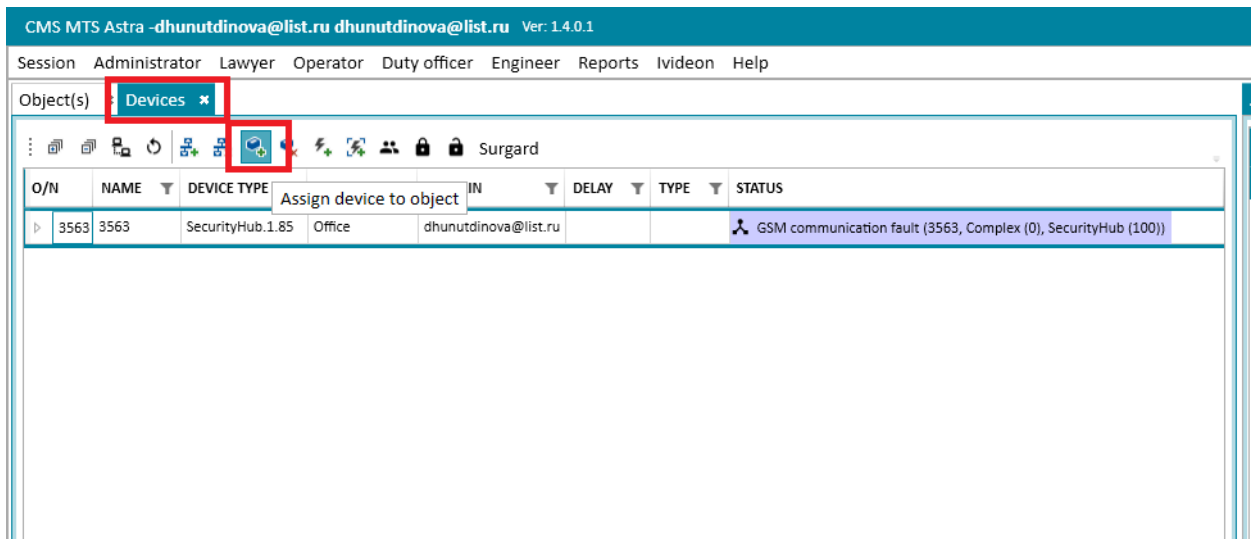


Complete: device address - device serial number, PIN code - last 4 digits in the device barcode. And select the cluster ("Security Hub or Astra Pro 4.0"). Click on the "Add" button.

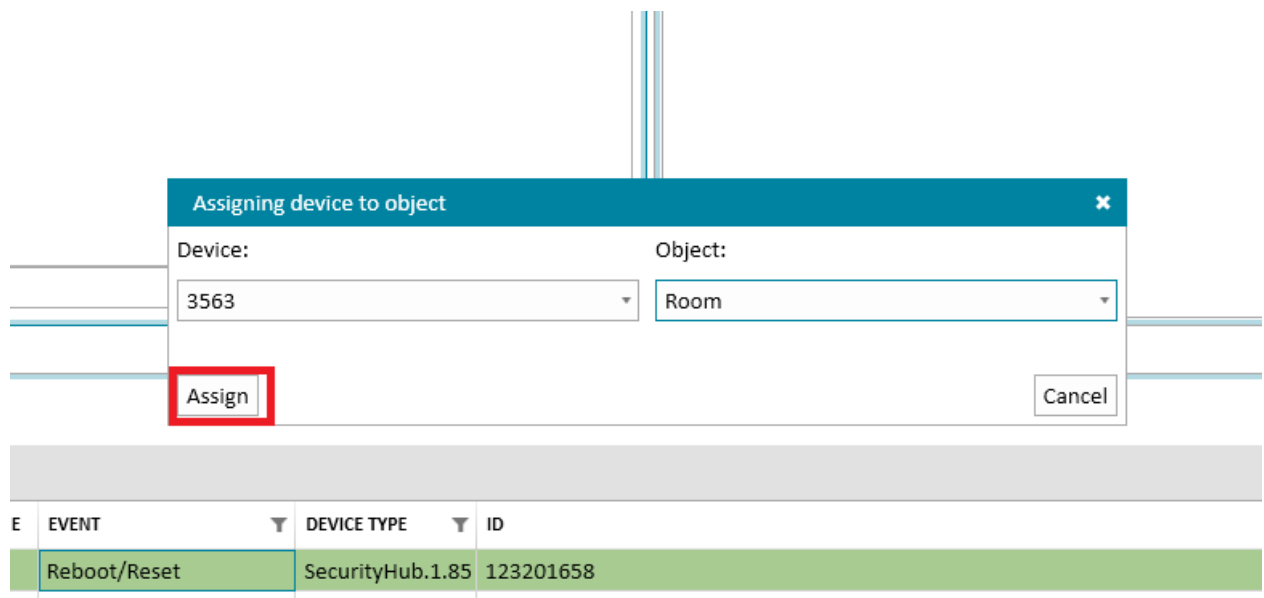
Assign device to domain	
Device address (account):	12345678
PIN:	1234
Cluster:	Security Hub или Астра Про 4.0
<input type="button" value="Add"/>	

Assigning the device to the object

On the "Devices" tab, right-click to assign the device to the object.



Appears a window in which in our device we select the desired installation from the list. Click on "Assign the device".



Deassign domain device

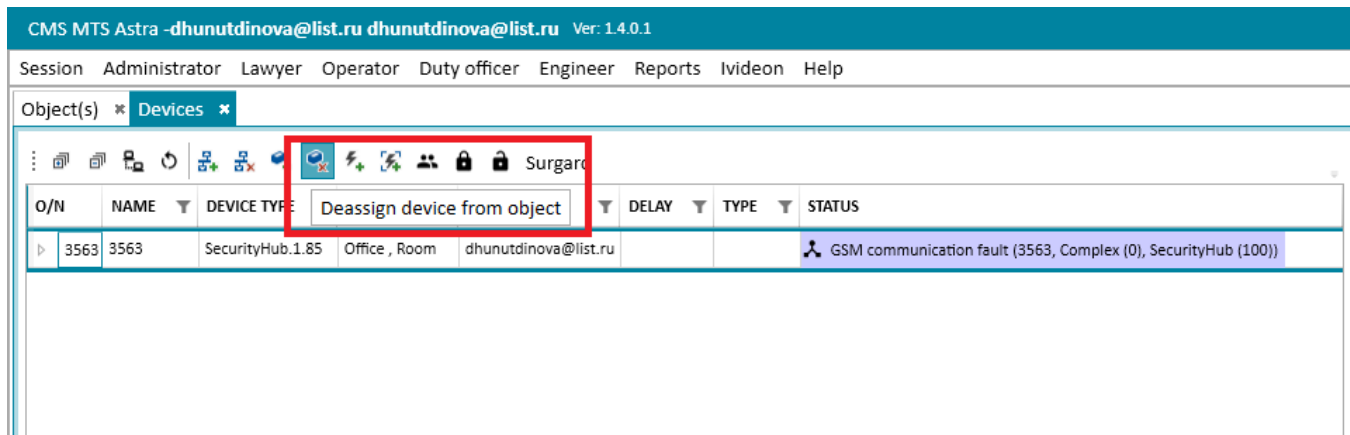
ATTENTION!

When you deassign the device from the domain, it will also be deassigned from the current installation!

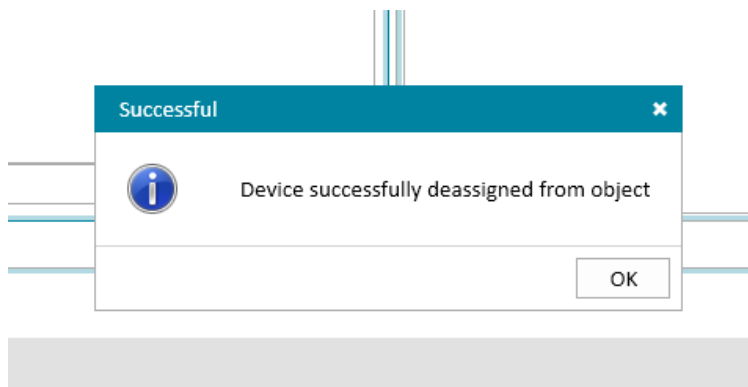
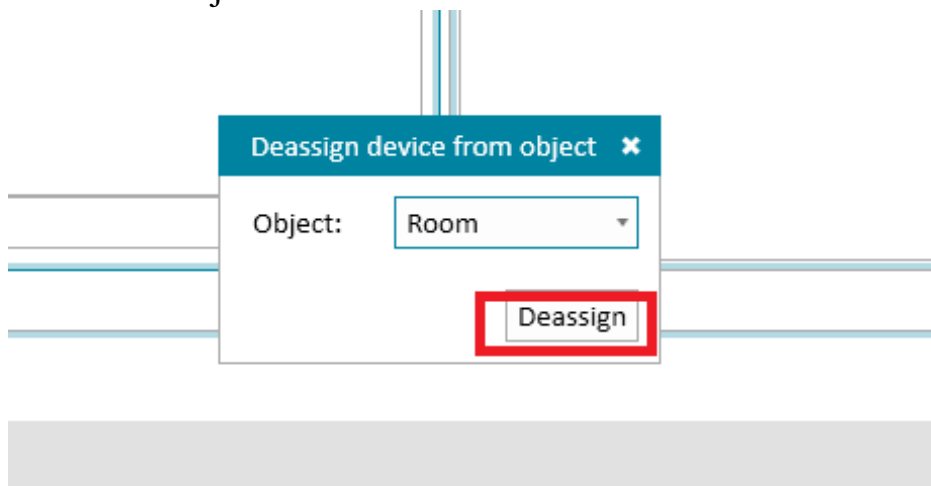
To deassign the domain device:

1. Go to the "Devices" tab.

2. Select the required device by right clicking and select **Deassign device from object** from object.

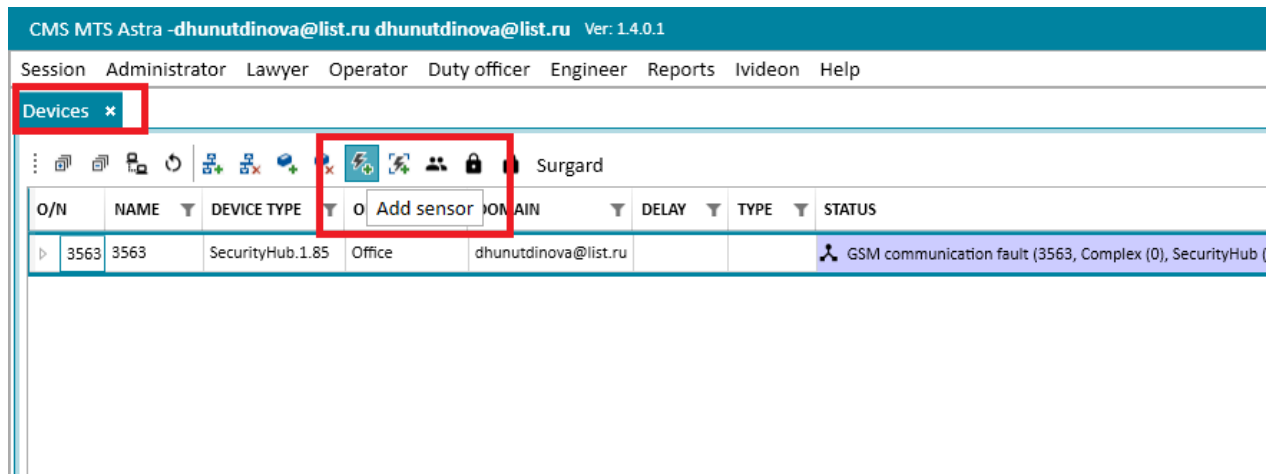


3. Choose an object



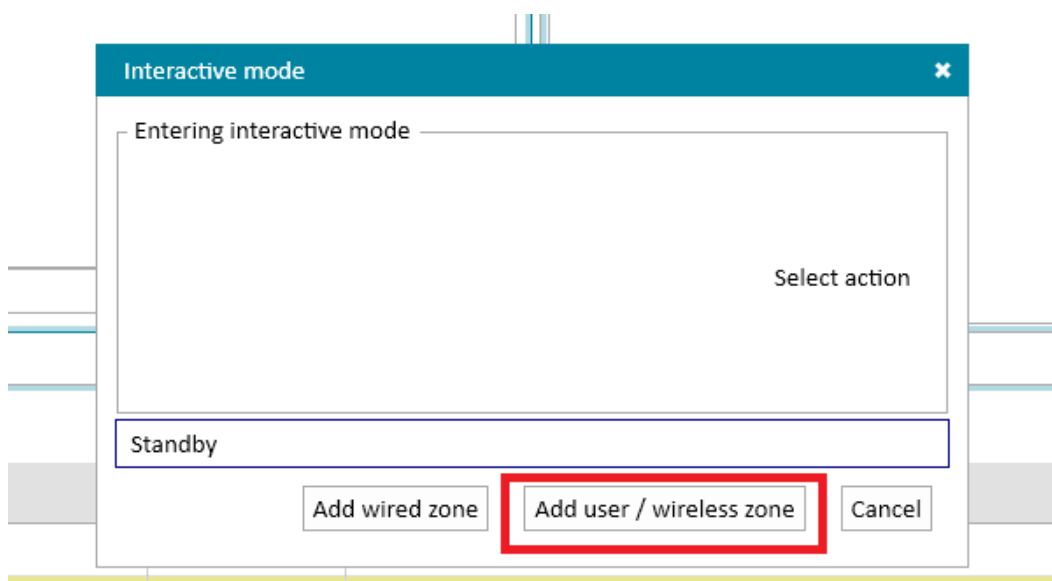
Wireless sensors set up

In the "Devices" tab, right-click to link the sensor.

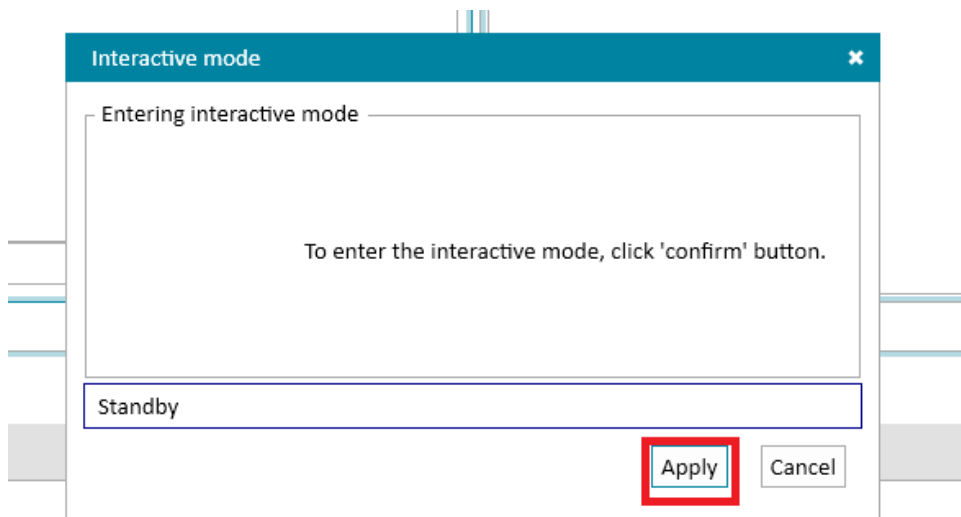


Choose which sensor we connect with wired or wireless.

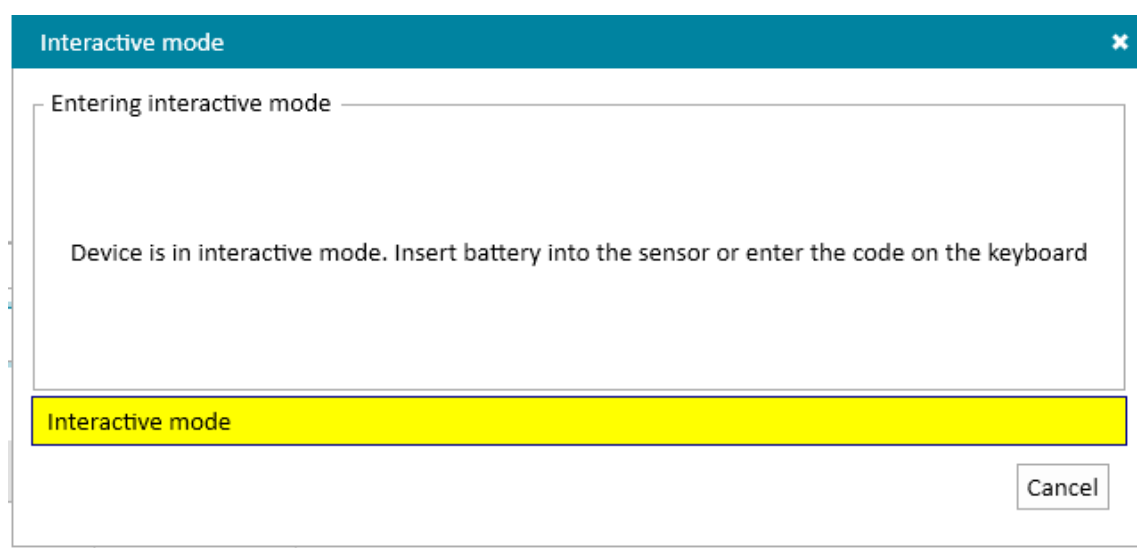
Click on the "Add user / wireless zone" button.



The program offers to exit the device in interactive mode. Click on the "Confirm" button.

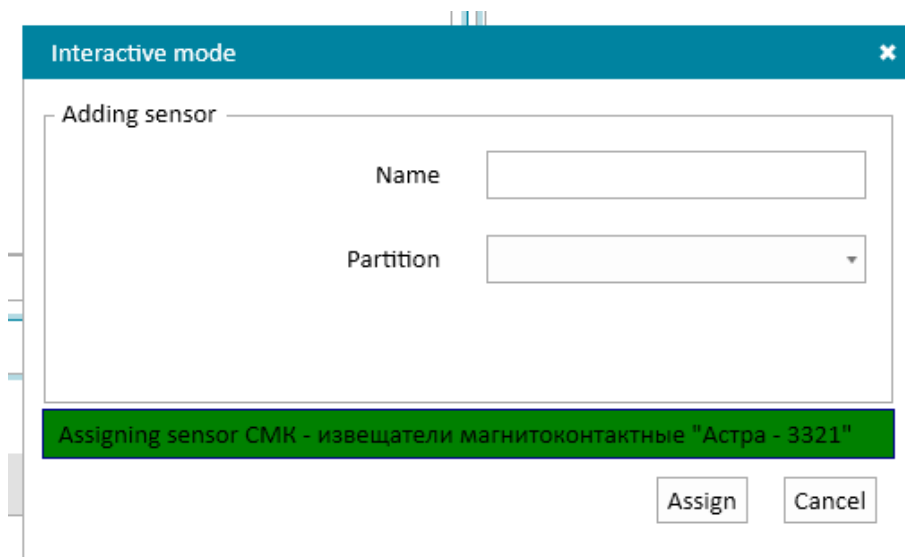


The device is interactively trying to detect the sensor.



Insert the battery to the sensor.

When the sensor is detected, name it and select a section for it. For the intrusion section, it is possible to select a delay * for arming / disarming.



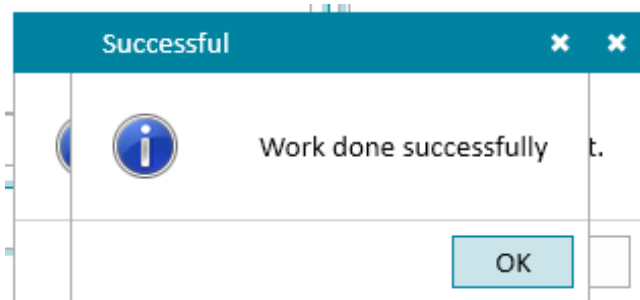
Press the "Assign" button. A message appears that the sensor was added successfully.

The screenshot shows a dialog box titled "Interactive mode" with a close button (X) in the top right corner. Inside the dialog, there is a section titled "Adding sensor" with the following fields:

- Name:** A text input field containing "Door".
- Partition:** A dropdown menu showing "General office".
- Delay:** A checkbox that is currently unchecked.

Below the "Adding sensor" section, there is a green status bar with the text "Assigning sensor CMK - извещатели магнитоконтактные "Астра - 3321"". At the bottom right of the dialog, there are two buttons: "Assign" and "Cancel".

* The entry delay is the time after which the sensor turns on after arming. In the Security Center: at the entrance of 45 seconds and at the exit of 60 seconds. (It allows, for example, to activate the arming on the panel and leave the room before the alarm sounds).



The connected sensor is shown in the "Devices" tab.

Users * Object(s) * **Devices** *

⋮ ⏪ ⏩ 🔍 🗑️ 🔒 🔓

O/N	NAME	DEVICE TYPE	OBJECT(S)	DOMAIN	DELAY	TYPE	STATUS
▲ 3563	3563	SecurityHub.1.85	Office	dhunutdinova@list.ru			
▶ 3563/0	Device 3563						
	General office						Tampering (3563, General office)
▲ 3563/1							Signal level 100% (3563, General office)
							Signal level 100% (3563, General office)
							Temperature value 25°C (3563, General office)
3563/1/2	Motion				0	Intrusion alarm zone: Volume	
3563/1/1	Door				0	Intrusion alarm zone: Entrance (door)	


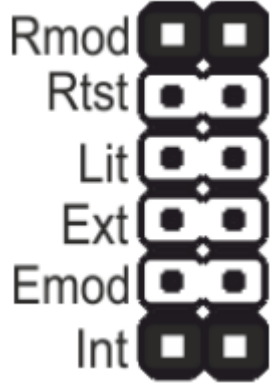
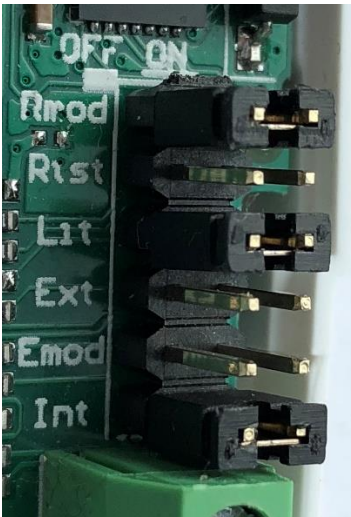

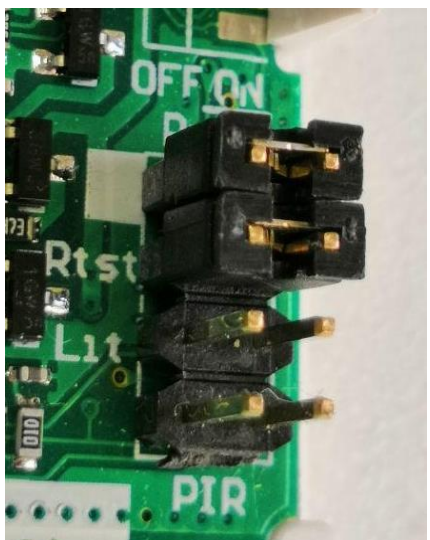
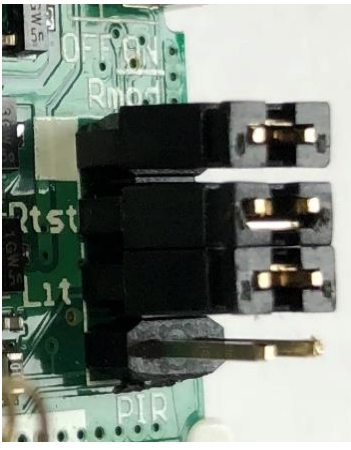
ATTENTION!

Make sure the jumpers and sensor characters are in the correct position.

The position of the jumpers in the sensors to connect to the Security Hub

Security Hub can operate on 2 frequencies 433.42 MHz and 434.42 MHz The operating frequency of the DOE depends on the launch date of the Security Hub. In addition, the operating frequency of the DOE can be changed through the Localconfig utility.

When adding a sensor to the system, you must ensure that the location of the sensor jumpers corresponds to the operating frequency of the Security Hub.

Sensor number	Lit 1 (433,42 MHz)	Lit 3 (434,42 MHz)
<p>Astra-3321</p> 		
<p>Astra-5121</p> 		

Functional characteristics

Registration in non-volatile memory of up to 30 serial numbers of sensors of the Astra-RI-M system;

It provides information exchange with mobile and web applications through the server:

1. Through a wired channel, through an RJ45 connector (Ethernet 10 BASE-T) and the provider's network,
2. Through a wireless channel, through two SIM cards (GPRS / EDGE) of a GSM mobile operator;

Technical parameters of the radio channel.

Security Hub (2.0) released since March 2019:

Operating frequency, MHz	433.42 MHz (letter "1")
Radio of the radio channel, m, not less than	100 (in direct visibility)
Radiation power, mW, no more than	10

Security Hub (2.0) released until March 2019:

Operating frequency, MHz.....	434.42 MHz (letter "3")
Radio of the radio channel, m, not less than	100 (in direct visibility)
Radiation power, mW, no more than.....	10

For the joint work of the Astra RI-M radio channel system detectors and the Security Hub (2.0) UOO (issued since March 2019) as part of Astra CMS, it is necessary to set the operating mode to "2" and the frequency letter "1" for the detectors. The change of the operating mode and the frequency letter is carried out in accordance with the operating manual of the Astra RI-M radio channel system detectors.

Power supply

The power supply of the terminal device is carried out:

From USB 2.0 Type V input with a nominal voltage of 5 V and a current of 1 A (network adapter), USB 2.0 AM-BM cable marked 28 AWG / 2C + 24 AWG / 2C, length up to 1.5 m.

From external power supplies with 12V voltage (through "+ 12V" and "+ 12VR" terminals).

In the absence of an external power supply from the built-in redundant power supply, a standard size 2 / 3A lithium-ion battery with a nominal voltage of 3.7 V, a capacity of 600 or 700 mA / h (supplied).

The battery is used only as a backup power supply (up to 8 hours), to turn on the device you need to connect the external power.

Nominal current consumption of the device during the power supply:

- from the USB port - 200 mA (maximum 500 mA);
- battery: no more than 50 mA;

- through terminals "+ 12V" and "+ 12VR" - 150 mA (maximum 300 mA).

Eliminating sensor

1. You must ensure that the object is disarmed.
2. The sensor must be deassigned from the partition. To do this, go to the "Devices" tab and select the sensor that needs to be deassigned.

There are two ways to remove the sensor:

- Choose the sensor you wish to remove and right-click, select "Deassign the sensor".

CMS MTS Astra - dhunutdinova@list.ru dhunutdinova@list.ru Ver: 1.4.0.1

Session Administrator Lawyer Operator Duty officer Engineer Reports Ivideon Help

Users * Object(s) * **Devices** *

O/N	NAME	DEVICE TYPE	OBJECT(S)	DOMAIN	DELAY	TYPE	STATUS
3563	3563	SecurityHub.1.85	Office	dhunutdinova@list.ru			
3563/0	Device 3563						
3563/1	General office						
3563/1/2	Motion				0	Intruaion alarm zone: Volume	
3563/1/1	Door				0	Intruaion alarm zone: Entrance (door)	Tampering (3563, General office (1), D Signal level 100% (3563, General office

Change sensor settings
Deassign sensor

"3563" "General office" "Door"

Choose the sensor and at the top, select the "Deassign sensor" icon.

CMS MTS Astra - dhunutdinova@list.ru dhunutdinova@list.ru Ver: 1.4.0.1

Session Administrator Lawyer Operator Duty officer Engineer Reports Ivideon Help

Users * Object(s) * **Devices** *

O/N	NAME	DEVICE TYPE	OBJECT(S)	DOMAIN	DELAY	TYPE	STATUS
3563	3563	SecurityHub.1.85	Office	dhunutdinova@list.ru			
3563/0	Device 3563						
3563/1	General office						
3563/1/2	Motion				0	Intruaion alarm zone: Volume	
3563/1/1	Door				0	Intruaion alarm zone: Entrance (door)	Tampering (3563, General office (1), D Signal level 100% (3563, General office

Deassign sensor

Program Frequently Asked Questions

I cannot change the name of the section in the application.

To ensure that changes are made, the system must be disarmed and kept in touch.

When the battery is installed, the sensor indicator does not respond.

Check that the battery supplied or matches the passport of the device.

Verify that the battery is installed with the correct polarity.

Try using a different instance of the battery.

Why, when I turn off the main power with the backup power installed (battery), does the controller lose connection to the cloud?

When disconnecting the power adapter, the Ethernet channel does not work. All communication with the cloud is done through the GPRS channel. The battery is designed to support the power of the controller only when working with SIM cards. It is recommended to install a SIM card.

The battery may be discharged or may not have had time to charge.

Why, when disconnecting the Internet and GSM, there is no signal of loss of communication with the object?

To exclude messages about the loss of communication channels associated with a variable communication quality, a message about the loss of communication with the object is issued after 10 minutes of the absence of object responses. The loss of communication on one of the channels is broadcast instantly.

Connect to a router with a Yota modem.

In the router configuration, enable DHCP and open port 2222. The controller constantly verifies the communication channels with the server; If the connection is not stable in the area where the object is located, we recommend changing the operator.

The controller (object) is not added

The basis of the identifier when adding the Security Hub terminal device is the serial number located on the device board.

Make sure the device address and PIN are entered correctly, as well as in the cluster selection. The device address consists of the first 4 digits, after

zeros, the device number. PIN code: the last 4 digits of the device. Group select "Security Hub or Astra Pro 4.0".

System specifications

What is the range of sensors?

The range of the sensors in the line of sight is not less than 100 meters.

What is the maximum number of sensors that can be connected to a controller?

The maximum number of sensors that can be connected to the system cannot exceed 30 to 16 key chains.

What sensors are compatible with the controller?

The sensor of opening of the Astra-3321 door

The motion sensor that does not respond to animals (up to 20 kg.) Astra-5121

The "curtain" motion sensor to block the door / window openings Astra-5131 A

The motion sensor for installation on the roof Astra-7 ver. RC

Combined motion and glass break sensor for ceiling installation Astra-8 ver. RC

Astra-421 RC smoke sensor

Astra-6131 glass breakage sensor

Water leakage sensor Astra-361 ver. RC

Astra-3731 temperature sensor

Mermaid Astra-2331

Astra-8231 relay block

Astra-3221 panic button

Remote control keyfob with panic button function Astra-RC

How many partitions can I create?

Up to 8 sections in the range of 1 to 8.

What operators does the controller work with?

The controller works with all providers of Internet and GSM cable communications operators, and GPRS (2G) Internet speeds are sufficient to establish communication with the server.