SLV VALETO® Smart Home Gateway

Assembly and commissioning instructions

1. release English 11/2018

Table of Content

Section 1
General information

This manual helps you setting up your SLV VALETO® Smart Home System. It contains all the information needed for adding new components, debugging and optimizing your system.

Retain this manual for future reference. All documents needed for implementing your Smart Home System can be downloaded from www.slv.com

1.1 SLV VALETO® Smart Home System

The SLV VALETO® Smart Home System uses the newest technologies and standards to serve you smart components that facilitate everyday routines.
Whether you simply turn on lights or control complex scenarios including many components, the SLV VALETO® Smart Home System helps you making your home facility smarter.

The following components are required to use the VALETO® Smart Home System:

- SLV VALETO® Gateway: In your Smart Home network, the gateway is the central component. It connects the Smart Home components to your home network. If connected to your router, you can control your components via the smartphone or tablet app – even from every point in the world if using the internet.
- An individual selection of SLV VALETO® Smart Home components, e.g. bulbs, controllers etc.
- Android or iOS apps. Define groups or scenarios, get current power consumption values or create new bindings.

  Optional: Amazon Alexa Skill to control your components with your voice.

Note: For some simple applications you can use your components without needing a gateway or app. In this case, however, your components won't get any updates.

SLV VALETO® products are based on the international standards IEEE 802.15.4 and ZigBee. This guarantees a long term availability of components and a safe investment.

1.2   Security and privacy

SLV's highest priority is both the safety of yours and your facilities. From the very beginning, our development department attached importance to develop encryption and authentication algorithms ensuring that only you gain access to your Smart Home components, at any time.

1.2.1   Safety of radio links

Hacker attacks via radio links are only possible when the attacker is in range of your facility's radio network. For this reason, hackers don't prioritize these objects, but put their focus on devices that can be globally accessed, such as gateways. Nevertheless, we attached importance to make the radio interface meet high level safety requirements. As an administrator of a public facility, e.g. a hotel, holiday resort, company or a public authority, you should take the threat of such hacker attacks serious.
Radio links between the components of your SLV VALETO® Smart Home System are based on the standard ZigBee Home Automation, which is based on the ZigBee PRO core technology. ZigBee PRO includes several safety features, such as an AES-128 network key to ensure that your data can't be read by third parties near your facility. Moreover, it is not possible for attackers to send control commands to your network, or to record legit control commands for future execution ("replay attack"). Unlike proprietary solutions, the open ZigBee PRO standard has passed safety tests, allowing to be used in billing related systems.

1.2.2   Gateway safety

The gateway has several services that are needed to gain access to your facility from the outside or for certain time or event controlled processes. This includes the Smart Facility Service, which establishes the connection between the facility and the Smart Home app on your mobile device. Naturally, is has to be ensured that this service is accessible from the outside. Therefore, all connections from your apps to this service are specially protected and encrypted.

While setting up your facility via app, access authorization will be installed on your smartphone, giving you access to your facility after the setup. A lost smartphone can be locked at any time via the gateway's web interface.

Make sure that the web interface of your gateway cannot be reached from the outside. Don't set up port forwarding via the TCP port 80, use local accesses or secured connections such as VPN to gain safe access to the web interface.

1.2.3   Remote maintenance

Remote maintenance is done via a secured connection. This connection is protected by a certificate and has to be opened explicitly via the gateway's web interface. The interface indicates an active remote access.

1.2.4   Cloud services

At this time, SLV doesn't use any cloud services. Facility information and profiles aren't saved as well. Therefore, the protection of your data is not threatened.

1.2.5   Updates

Firmware updates for your gateway are certificated. Therefore, they cannot be manipulated to install threatening software. The firmware for ZigBee devices is encrypted and has an integrity test. Every time the gateway firmware is updated, the current firmware version and serial number will be stored for statistic reasons.

1.3   Function

The gateway is the central component in your network. It connects your Smart Home components, which are provided with the ZigBee technology (IEEE 802.15.4), with your home or office network and the internet. When connected to your internet router, you are able to control and monitor all components via smartphone or tablet app – and when using the internet, even from any position in this world.

The intuitive web interface allows you to set up your gateway by yourself. All you need is an internet browser. The web interface offers following functions:

- **Network configuration:** In order to connect your SLV VALETO® Smart Home System to your home or office network, you have to adjust the gateway's network settings (IP address, network mask, name server, optionally proxy settings etc.) to the network environment.
- **Firmware updates:** The gateway downloads and provides both its own firmware and the one of all other components by itself. Additionally, you regularly receive new functions. And, in case of facing problems, you can solve errors by using this function.
- **Unlocking and locking of mobile devices:** Only authorized persons shall get access to your Smart Home facility. For this purpose, you can authorize individual devices and grant them access.
- **Support access:** An integrated remote maintenance function, which can only be enabled by you, allows our customer service to get access to your device. Thereby, we can work on service cases without needing to do costly drives.

1.4   Ports

- 10/100 Base-T Ethernet,
- Supply voltage 5V/1A

- USB 2.0 high speed host port (for future expansions)

1.5   Scope of delivery

- IEEE 802.15.4/ZigBee Ethernet Gateway
- AC adapter 5V, 1A

- Network wire, CAT6, 2m, black

1.6   Technical information

System information
- ARM926 CPU, 400MHz
- 128 MB DDR2 SDRAM
- 256 MB NAND flash
- 8 MB NOR flash

Gateway server software
- Smart facility server
- ZigBee Over-the-Air upgrade server
- ZigBee/IP Gateway (GRIP)
- Linux OS

Standards
- IEEE 802.3af PD
- IEEE 802.15.4
- ZigBee 2007 PRO

Power supply
- 5V
- Power consumption < 1W

Dimensions
Length: 106mm
Width: 106mm
Height: 26mm

Color
Black, aluminum

Material
Aluminum (brushed) & plastic

Weight
est. 500g

1.7   Wall mounting

The gateway can be either simply put up or mounted on a wall. If you want to install the gateway on fixed position, make sure that you don't damage switches, power sockets, gas and water pipes, when determining the mount position and drilling next to the ones mentioned above.
Don't mount the gateway on metal boards or other environments that can impair RF transmissions. Information about troubleshooting can be found in section 10 "Notes on troubleshooting".

- Place the drilling template at the desired mount position and adjust it appropriately. Ensure that the network and power connectors and wires have enough space.
- Mark the position of both the drill holes A and B with the help of the drill template and a pencil.
- Drill at the two marked positions holes with a diameter of 5mm in the wall. After that, put a dowel in each hole. Turn the screw into the dowel so that they are about 6mm out of the wall. Put the unit with the rear recess on the screw heads and hang it on.

Section 2
Commissioning

If possible, the SLV VALETO® gateway should be installed first, before all other components. This gives you better control of the installation progress. The following sections explain the usual procedure for the initial operation.

2.1   System requirements

Power supply:
5V DC (via included power adapter up to 100 – 240V AC).

Web browser with HTML4/5, CSS2/3 and JavaScript, e.g.:
Apple Safari, Google Chrome, Microsoft ® Internet Explorer, Mozilla Firefox®, Opera, etc.

Data link:
Ethernet 10/100Mbit/s and IPv4 network environment (IPv6 will be featured by a future update)

2.2   Connecting the gateway

Connecting the gateway to your network
Use the included network wire (E) to connect the gateway to your DSL, UMTS or LTE router (see figure 2).

Connecting the gateway to power supply
Connect the included power adapter (F) to your gateway and plug it into the power socket (see figure 2). This device may only be connected to an easily accessible power socket indoors.
In case of danger the main connector has to be disconnected.

> **Caution:** To avoid damage to the device, use only the included original AC adapter as a power supply.

A	Status LED
B	Ethernet
C	Spannungsversorgung
D	Reset-Taster
E	Netzwerkkabel
F	Netzteil
G	Externer Router
H	Steckdose
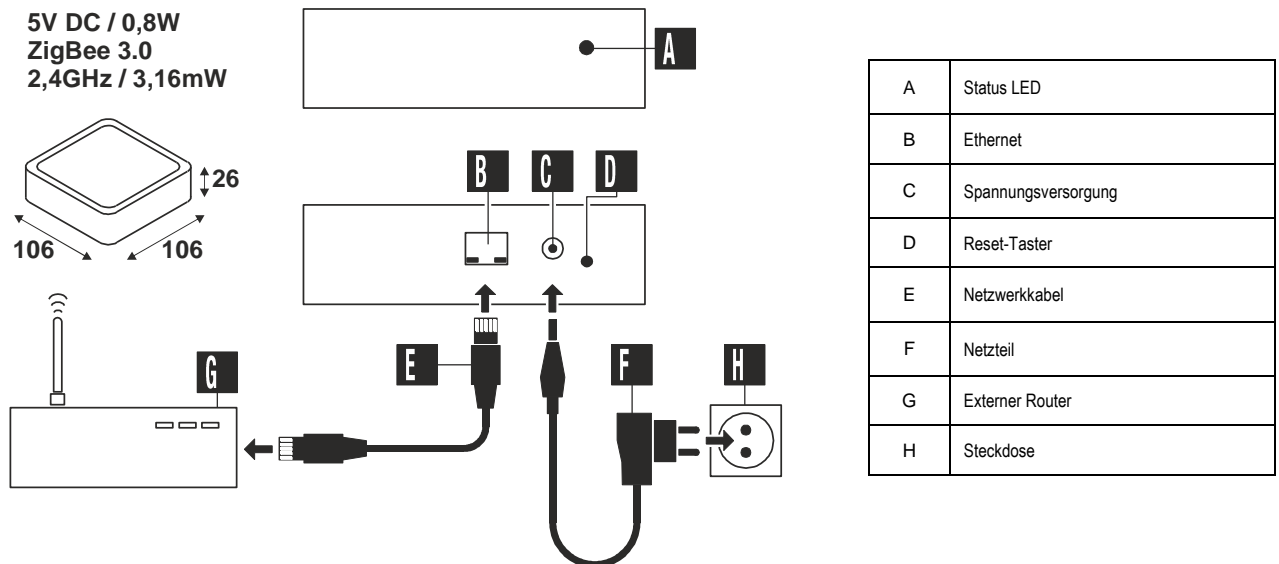
Figure 2

Your gateway is ready now for further configuration.

2.3   Logging in to the gateway

Open the SLV VALETO® Smart Home App on your mobile device. The App guides you through the activation process. You will be requested to scan the barcode on the back of the Gateway to authorize access to the SLV VALETO® Gateway and the system.

Alternative:

The gateway's web interface can be reached via web browser. After connecting your gateway to your network and providing power supply (see section 2.2 "Connecting the gateway"), you can start with the configuration. Follow these steps:

1. Open your web browser.
2. In the URL, enter the gateway's IP address (can be found in the router settings) and press the Enter key. If a prompt is displayed which indicates an address on the local network, accept this.
3. In the appearing window, enter user name and password for authorization (see figure 3). The default user name and password are both: *admin*
4. Click "Login" or press Enter.
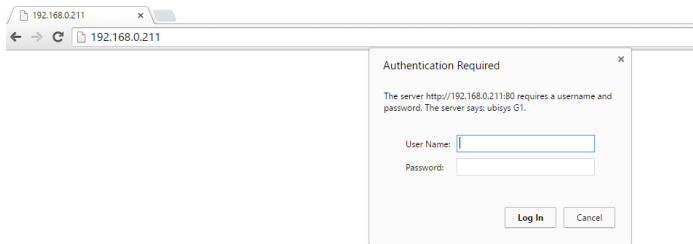
Figure 3

You are now on the web interface's home screen (see figure 4). If this site does not open, check the wiring and make sure that the gateway is in the same logical network as the device from which you opened the web interface is. The gateway's default device address is 211, in the subnet 192.168.0.X (subnet mask 255.255.255.0). If the IP address of your computer does not start with 192.168.0.*, change it temporarily in order to configure the gateway properly. More information can be found in section 3.9 "Changing network parameters for gateway access".
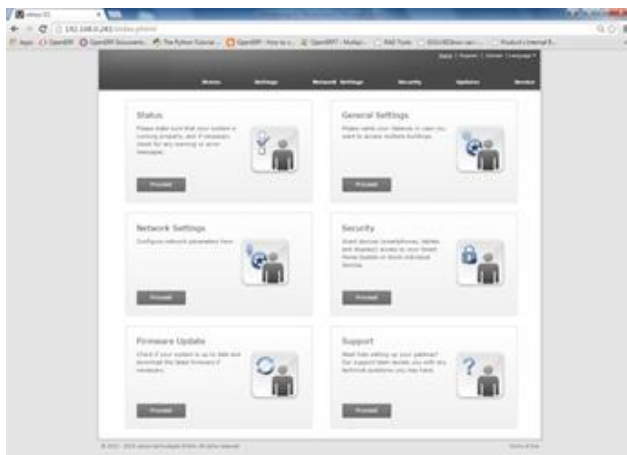
Figure 4

2.4   First steps to configure your gateway

Before you can use the gateway for your Smart Home System, the following settings have to be done:

- Adjust network settings to the network environment
- Authorize control unit
- Add components (dimmer, power switch, etc.)

2.4.1   Network settings

Configure the network parameters as described in section 3.3.1, or switch to DHCP with the help of the protected button at device's rear side, as described in section 9.

2.4.2   Authorizing control device

Before you can control and configure your Smart Home System via app, you need to authorize your smartphone or tablet as a control unit. Navigate to "Security" and follow these steps:

1. In the section "Enable access for an additional device", enter any access code in the "Access code" textbox (must be at least 4 digits). Optionally, you can remember the randomly generated 4 digit code (see figure 8). This code will be automatically generated when opening this site.
2. Click "Activate". For the next step, you have a time limit of 5 minutes. When reaching this time limit, the authorization time frame automatically closes. After each authorization attempt though an app, the time frame is automatically closed prematurely.
3. Start the app on your smartphone or tablet (available in the Apple Store or Google Play Store) and select the appropriate gateway. You will then be asked to enter the recently defined access code. After that, you have access to your Smart Home System via the configured device.

Enable access for an additional device	
Access code	4892

Please enter a random access code (minimum four digits) for the registration of a new device and click on "Activate". The code entered here must be entered identically on the device to be added to permit access for the given device.

Activate

Figure 8

2.4.3   Add components

Once you have both successfully configured your gateway and added a smartphone or tablet as a control unit, you can start to install components, such as bulbs, controllers etc.
When a component has been connected, and power is turned on again, this component will then automatically try to log in to an open Smart Home network. For this, you have to open your Smart Home network in order to add new components.
On the web interface, navigate to "Security", then head to "Open ZigBee network for new components" and click "Open" (see figure 9).

Open ZigBee network for new components

Open

Figure 9

Your Smart Home network will now be opened for 2 minutes. During this time, one or more new components can log in to the network (see figure 10).

Open ZigBee network for new components

Network open for new components...

Close
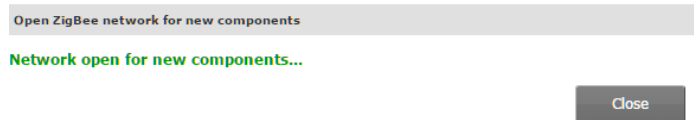
Figure 10

In your Smart Home app, go to **Configuration** -> **Basic Configuration** -> **Components**. All new components should be listed here. Optionally, you can also find these components on the "Status" site of the gateway's web interface.

Once all components have logged in to the network, you can close your Smart Home network by clicking "Close" (see figure 10).
A closed network ensures that no foreign devices get unauthorized access to your ZigBee network.

If you wish to add further components, just repeat the procedure.

> **Caution:** Smart Home components only search for an open network as long as they can successfully log in to one. After that, even in case of a power breakdown, there will be no new searching attempts. If you want to add components that have been signed to another network before, you will have to set them to default settings first. More information about how to restore default settings can found in the appropriate component's manual ("Factory Reset").

Section 3

GATEWAY Configuration

The gateway offers a web based configuration interface, which can be reached by a web browser via your PC, tablet or smartphone. This allows you to configure all required settings concerning the gateway.

For this, enter the IP address of your Smart Home gateway in the web browser's address line. After pressing the "Enter" key, a prompt will be displayed. Here, you enter the username *admin* and the password (which is *admin* as well, by default) (see figure 11).

Default parameters:

IP address: **Can be found in the router settings**
Username: **admin**
Password: **admin**
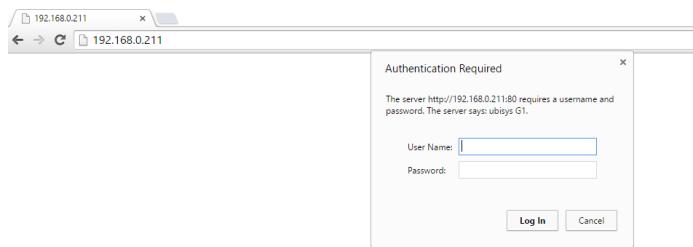
Figure 11

If you already configured your gateway, but forgot the address, you can simply look after it in the Smart Home app. More information about how to determine the IP address of your gateway can be found in section 5 "Determine the gateway's address".

> **Caution:** Your PC, tablet or smartphone has to be in the same network as the gateway is, in order to configure it. If this is not the case, more information can be found in section 3.9 "Change network parameters for gateway access".

3.1   Status menu

In the main menu, navigate to "Status". Here, you find detailed information about your Smart Home System as well as its operating status.

3.1.1 Device information

In the section "Device information" you find detailed information about your gateway, such as the model number, serial number, current firmware version etc. (see figure 12).

Device information	
Model version	2
Serial number	17
Version	1.0.58
Ethernet MAC-address	00:1F:EE:00:05:06

Figure 12

Caution: In case you contact the SLV support, these information can be very helpful for our employees. Here, you also find the Ethernet MAC address (EUI-48), which allows you, for example, to instruct a DHCP sever to always give the same address.

3.1.2 System status

In the "System status" menu, all status, warning and error messages are displayed.

Examples:

System status
System is working properly

Your ubisys Smart Home system is working properly.

Figure 13

System status
New component found

A new component (00:1F:EE:00:00:00:02:02) was found and integrated into your Smart Home System.

8/17/2015, 1:53:53 PM

Figure 14

The following feedback can occur:

Status messages (blue highlighted)

Content	Explanation
Initializing	The gateway has recently been booted and is about to be ready.
The ZigBee network is being discovered via gateway, to discover existing components and to integrate them into your Smart Home System. This procedure may take a few minutes.	At initial operation the gateway will automatically scan your Smart Home network to allocate installed components. Only after this procedure you will be able to control these components via app.
ZigBee network discovery via gateway completed. No new components were found.	During the scan of your Smart Home network, no Smart Home components have been found. In case, that installed components couldn't be found due to external parasitic inductions, you have the option to manually start a network scan via app.
ZigBee network discovery via gateway completed. One (or more) new component(s) were found.	The exact number of registered components during the network scan will be displayed. In case, that installed components couldn't be found due to external parasitic inductions, you have the option to manually start a network scan via app.
A new component (IEEE address: 00:1F:EE:00:00:00:00:01) was found and integrated into your Smart Home System.	Every Smart Home component found can now be clearly identified by its IEEE address (EUI-64).
New devices can currently be connected with your Smart Home System.	An access code for adding a new control device has been enabled via the web interface. To activate a control device in your Smart Home System, enter this code on the device that shall be added.
The device (iPhone Doe) is now having access to your Smart Home System. The device (iPhone Doe) has no access to your Smart Home System.	Access to your Smart Home System has been successfully granted to the new control device. Access to your Smart Home System is from now on restricted for the appropriate device. Reactivating access is only possible by a new access code.
The update of the network component with the IEEE address (IEEE address: 00:1F:EE:00:00:00:00:01) has been successfully completed.	A new firmware for a Smart Home component has been downloaded and will be installed afterwards. After successful installation, the component restarts and will then be available again.

Warning messages (orange highlighted)

Content	Explanation
A command directed to the component (network address 1234) failed (status code: NWK:ROUTE_ERROR). This error may occur, if the component is temporarily not available. If the error is not patched automatically after some time, contact the support (https://www.slv.com/en-de/meta-navigation/contact/contact-form.html).	This is usually a temporary radio transmission interference in your Smart Home System, wherein control commands cannot be sent to the target device. This kind of error is often caused by external parasitic induction and will be automatically fixed by the intelligent radio standard being used. If this warning message is displayed repeatedly, check, if the affected component is installed and properly connected to power. Do the same for temporarily stored ZigBee routers.
A command directed to the group (group address 0001) failed (status code: MAC:CHANNEL_ACCESS_ FAILURE). This error may occur, if the component is temporarily not available. If the error is not patched automatically after some time, contact the support (https://www.slv.com/en-de/meta-navigation/contact/contact-form.html).	This is usually a temporary interference or overload in the ZigBee network, wherein control commands cannot be sent to a group of controlling devices. This kind of error is often caused by external parasitic induction or massive radio traffic and will be automatically fixed by the intelligent radio standard being used.
A command directed to the network address (broadcast address: fffd) failed (status code: MAC:CHANNEL_ACCESS_ FAILURE). This error may occur, if the component is temporarily not available. If the error is not patched automatically after some time, contact the support (https://www.slv.com/en-de/meta-navigation/contact/contact-form.html).	This is usually a temporary radio transmission interference in your Smart Home System, wherein control commands cannot be sent to the target device. This kind of error is often caused by external parasitic induction and will be automatically fixed by the intelligent radio standard being used. If this warning message is displayed repeatedly, contact the SLV support.
Your Smart Home System denied access to the unauthorized device 192.168.0.111.	Authentication of a device has failed during the login attempt. This is usually a mobile device, which had access to your Smart Home System.
The update of the network component with the IEEE address: 00:1F:EE:00:00:00:00:01 has failed. Further attempts will follow.	The download of the new firmware for the appropriate Smart Home component has been interrupted due to transmission interferences or a power breakdown, for example. Another attempt will be done automatically.
An update could not be performed. Further attempts will follow.	A Smart Home component has prematurely cancelled the download attempt of a new firmware. A new attempt will be done automatically.

Error messages (red highlighted)

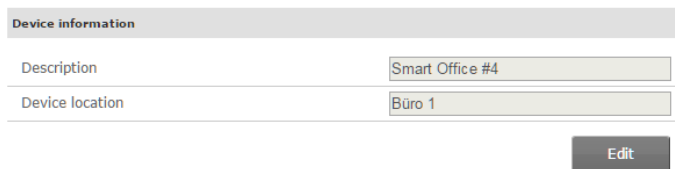| Content	Explanation
Failed to initialize the Gateway Service. If the error is not patched automatically after some time, restart the gateway. If the error still persists after the restart, contact the SLV support (https://www.slv.com/en-de/meta-navigation/contact/contact-form.html).	An error occurred while initializing the integrated ZigBee adapter of the gateway. This is an internal error, which should not occur in general. Restart the gateway. If the error occurs repeatedly, contact the SLV support.
No ZigBee adapter found. If the error is not patched automatically after some time, restart the gateway. If the error still persists after the restart, contact the SLV support (https://www.slv.com/en-de/meta-navigation/contact/contact-form.html).	An error occurred while initializing the integrated ZigBee adapter of the gateway. This is an internal error, which should not occur in general. Restart the gateway. If the error occurs repeatedly, contact the SLV support.
The ZigBee adapter could not be started. If the error is not patched automatically after some time, restart the gateway. If the error still persists after the restart, contact the SLV support (https://www.slv.com/en-de/meta-navigation/contact/contact-form.html).	An error occurred while initializing the integrated ZigBee adapter of the gateway. This is an internal error, which should not occur in general. Restart the gateway. If the error occurs repeatedly, contact the SLV support.
Failed to initialize the gateway. Further attempts will follow.	An error occurred while initializing the integrated ZigBee adapter of the gateway. This is an internal error, which should not occur in general. Restart the gateway. If the error occurs repeatedly, contact the SLV support.
The gateway is temporarily not available. Further attempts will follow.	During operation, an error occurred in the integrated ZigBee adapter of the gateway. . This is an internal error, which should not occur in general. Restart the gateway. If the error occurs repeatedly, contact the SLV support.
The component (IEEE address: 00:1F:EE:00:00:00:00:01) does not respond to configuration attempts. Further attempts will follow.	This could be a temporary radio transmission interference in the Smart Home facility, wherein a configuration command could not be sent to a target device or acknowledged. This error can be caused by external parasitic induction, an inactive ZigBee router or a deactivated target device and is usually automatically fixed, as soon as the affected device is online or the error source has been disabled. If this error occurs repeatedly, check if the affected device and temporarily stored ZigBee routers are installed and properly connected to power. If the problem still exists, contact the SLV support.

3.2   Basic settings

The basic settings are used for general configuration of your gateway:
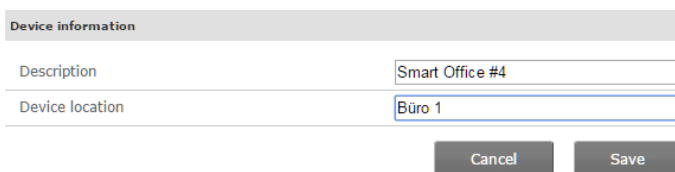
3.2.1   Device information

Device information can be freely defined. In environments with several gateways, it helps identifying every single device. Your defined description of the gateway can also be found, for example, in the SLV VALETO® Smart Home app. To make your individual information, follow these steps:

1. Click the "Edit" button (see figure 15).
2. Select the textbox you wish to edit.
3. Fill in your information.
4. After filling the information, click the "Save" button (see figure 16).
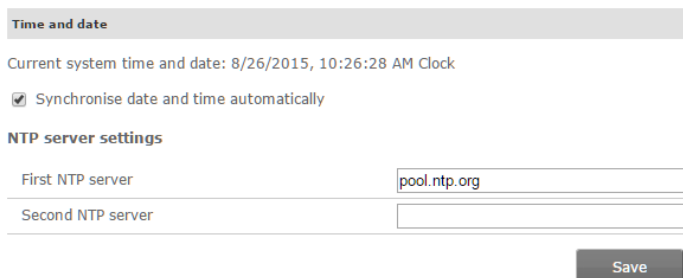
Figure 15

Figure 16

3.2.2   Time and date

In the "Time and date" section, the current date and time of your system is displayed. This information is important when configuring time dependent actions for your Smart Home System (e.g. automatically raise blinds at a certain time). If possible, date and time should be synchronized with an internet time server (NTP server). This configuration is set by default. For this, the option "Synchronize date and time automatically" should be enabled (see figure 17). A permanent internet connection, such as DSL, is required.

Figure 17

If you want to set the system date and time manually, follow these steps:

1. Deactivate the option "Synchronize date and time automatically" by clicking on the check mark (see figure 17).
2. A mask for manual configuration will automatically be displayed (see figure 18). Click the appropriate text boxes to specify date and time.
3. Click on the "Save" button after finishing the configuration.

Time and date

Current system time and date: 8/26/2015, 10:26:28 AM Clock

☑ Synchronise date and time automatically

NTP server settings

First NTP server	pool.ntp.org
Second NTP server	

Save

Figure 18

Caution: After a loss of the supply voltage, the integrated battery can hold the time updated for some time. After that the clock starts again at 0:00 a.m. on 01/01/1970.

3.2.3   Time zone

In the "Time zone" section you can define the time zone. The default value is set to Europe/Berlin. By defining the time zone, conversion of coordinated world time to local time is performed. To change the time zone, follow these steps:

1. Click the "Change time zone" button (see figure 19).
2. Use the list box to select the city that matches your local time (see figure 20).
3. Click the "Save" button to save your settings.

Time zone

Current time zone: Europe/Berlin

Change time zone

Figure 19

Time zone

Current time zone: Europe/Berlin   Europe ▼   Berlin ▼

Cancel   Save

Figure 20

3.3   Network configuration

The gateway connects the wireless ZigBee network with your home or office network and the internet. Before you can get access to your Smart Home facility via gateway with the help of the app, the gateway has to be connected to a router or access point first (see section 2.2 "Connecting gateway"). For smooth operation, the parameters for the respective network environment have to be set correctly in "Network Settings".

3.3.1   Network settings

Under the menu item "Network Settings" in the main navigation, the network settings are to be found. Here, you can choose between static and dynamic (automatic) network configuration. Choosing a dynamic IP address requires a DHCP server, which is e.g. provided by your router.

Dynamic

In the dynamic network configuration, all necessary network parameters (IP address, subnet mask, default gateway, primary and secondary name server) are automatically retrieved from the DHCP server. This procedure requires a DHCP server in your network (usually provided by your DSL router). In addition, you should instruct the DHCP server to always give the gateway the same IP address. Usually, you do this by entering both the gateway's Ethernet MAC address (EUI-48) and an address excluded from the pool of non-persistent addresses. More information can be found in the manual of your DHCP server (in home networks, usually integrated in the internet router). Make sure that you only have one active DHCP server in your network, otherwise wrong configuration can occur.

Figure 21

Static

By default, the gateway is configured with fixed (static) network parameters. A static configuration offers the advantage that no DHCP server is required. Even if you operate a DHCP server, static gateway configuration does not require a change of the DHCP server's settings. It is important to prevent address issues. Make sure that the IP address you choose is not assigned to another device in your network. For your gateway, select a free IP address from the subnet that contains your control devices (smartphone, tablet).

Adjust the network parameters to your existing network. Note the settings of a possibly existing DHCP server. The IP address of your Smart Home gateway has to be excluded from the IP address pool that is used by the DHCP server to assign non-persistent addresses to devices.
In the following example (see figure 22), a DHCP server configuration is shown, allowing only static IP addresses higher than address 200.
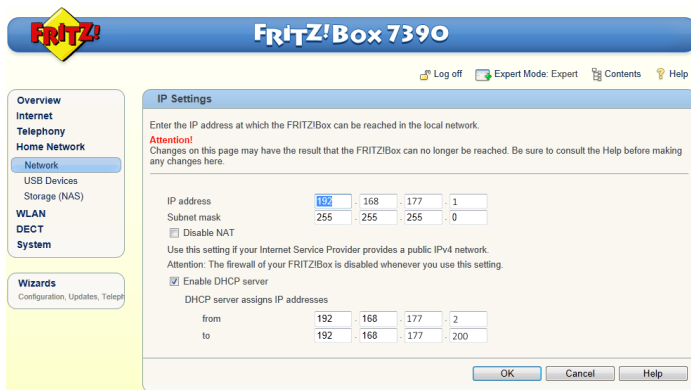
Figure 22

In this scenario, your gateway could get the static IP address 192.168.177.201, if this address is not already assigned to another device (IP camera, VoIP phone, NAS etc.).

IP address and subnet mask (also known as net mask) are mandatory required (see figure 23). Entering default gateway and DNS server is optional. It is, however, required for functions such as automatic time setting via NTP (Network Time Protocol), firmware updates and, optionally, remote maintenance by SLV. **Therefore, you should configure these settings.**

Figure 23

Detailed information about the network parameters, such as default gateway and DNS server in your network can be determined via your router or PC. More information about this can be found in section 4 "Determining the network parameters".

Once you have configured all settings, click the "Save" button. Depending on the recent changes, your gateway will now be available via the new IP address; the old address is not valid anymore.

3.2.2 Proxy settings

If web access in your network is provided by a HTTP proxy server, you can enter all necessary configuration parameters here (see figure 24). More information about the parameters can be given by your network administrator or by "Determining the network parameters" (see section 4) via your PC.
In typical network environments there is usually no proxy. That means you do not need to fill the appropriate text boxes with information.

Note: The password specified here is stored encrypted on the device.

Proxy settings	
HTTP Proxy (Host/IP address)	
Port	
User name	
password	
	Save

Figure 24

3.3.3 Role in the ZigBee network

In contrast to the settings stated above that affect the gateway's Ethernet interface, this setting relates to the wireless ZigBee network. By default, the gateway creates and manages a ZigBee network as a ZigBee coordinator and trust center. To control components in an existing ZigBee network of another manufacturer via your SLV VALETO® Smart Home app, you can also operate the gateway as a ZigBee router and join an existing network (see figure 25).

Role in the ZigBee network	
Role in the ZigBee network	Coordinator
IEEE 802.15.4 channel	11
ZigBee network ID	00:1F:EE:00:00:00:05:06

Current settings: Set up and manage a network.

Change settings:

◉ Set up and manage a network
◯ Join existing network

Save

Figure 25

Caution: If you use multiple gateways in your Smart Home network, you have to make sure that only one gateway is responsible for creating and managing. Besides, only one gateway should be active as an OTA server in the ZigBee network.
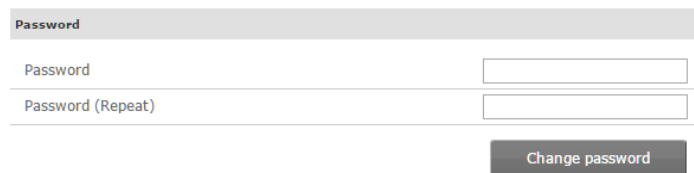
3.4   Security

Security is an essential feature of the SLV VALETO® Smart Home Systems of SLV. New components or devices can only be added to the ZigBee network with authorization. All necessary settings to provide the safety of your system can be found in the configuration menu under "Security".

3.4.1   Password

When opening the web interface, you will be prompted to enter both a username/login and a password for your gateway. Both the default username and password is **admin**.
In the "Password" section, you can specify a new password for the web interface of your gateway. The username is not changeable. To change the password, follow these steps:

1. Click the "Password" textbox (see figure 26).
2. Enter your desired password.
3. Repeat the procedure in the line below.
4. Confirm the new password by clicking the "Change password" button.
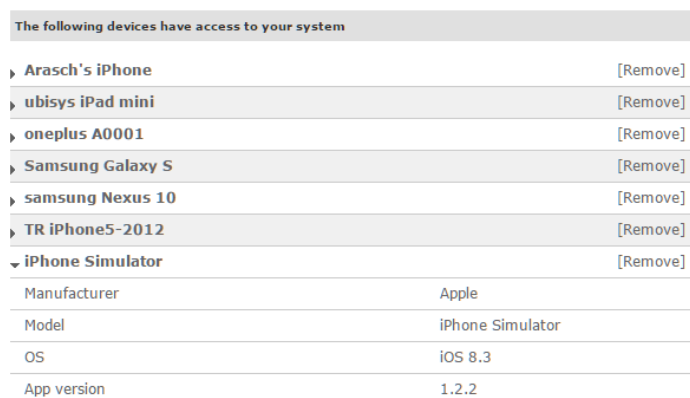
Password	
Password	
Password (Repeat)	
	Change password

Figure 26

3.4.2   The following devices have access to your system

This table includes all mobile devices that have access to your Smart Home System via app and, therefore, are authorized to control it.
To see more detailed information about a single device, click on the appropriate name. To remove a device from the list, click "Remove" (see figure 27).

The following devices have access to your system	
Arasch's iPhone	[Remove]
ubisys iPad mini	[Remove]
oneplus A0001	[Remove]
Samsung Galaxy S	[Remove]
samsung Nexus 10	[Remove]
TR iPhone5-2012	[Remove]
iPhone Simulator	[Remove]
Manufacturer	Apple
Model	iPhone Simulator
OS	iOS 8.3
App version	1.2.2

Figure 27

3.4.3 Enable access for an additional device

To authorize a smartphone or tablet as a control unit for your Smart Home System, follow these steps:

1. Click the textbox in line "Access code" and enter any access code (must be at least 4 digits). Optionally, you can notice the existing random 4 digit code that is automatically generated when opening the site.
2. Click on "Activate". The next step has to be done within 5 minutes, after that the authorization time frame automatically closes. After every authorization attempt through an app the time frame is automatically closed prematurely.
3. Start the app on your smartphone or tablet and select the appropriate gateway. You will be prompted to enter the recently defined access code. After that, you have access to your Smart Home System via the configured device.

Enable access for an additional device

Access code   7348

Please enter a random access code (minimum four digits) for the registration of a new device and click on "Activate". The code entered here must be entered identically on the device to be added to permit access for the given device.

Activate

Figure 28

3.4.4 Open ZigBee network for additional devices

If you want to add new components to your Smart Home System, you have to open your ZigBee network first. Follow these steps:

1. Click on "Open". The network will be opened for about 2 minutes to register new components (see figure 29). To close the network, click the "Close" button.

Open ZigBee network for new components

Open

Figure 29

2. Newly detected components can be found as a status message under "Status" as well as in your app under **Configuration -> Basic Configuration -> Components**.

Open ZigBee network for new components

Network open for new components...

Close

Figure 30

3.4.5   Renew ZigBee network key

Communication between the individual devices in your Smart Home System is exclusively encrypted. After setting up the Smart Home System, it may be useful to renew the network key on all devices. By this, you can ensure that devices, which once obtained the network key, but should not have access anymore (for example, the USB stick of an installer), no longer can access components via the ZigBee network. To renew the network key, click on "Refresh" (see figure 31).

Renew ZigBee network key	
	Refresh

Figure 31

3.5   Updates

To keep your Smart Home System updated, you should periodically install the newest firmware. Software updates feature improvements and new functions.
Installing updates requires a correctly configured internet connection (see section 3.3.1 "Network settings").

The number of available updates is automatically displayed in the main navigation (see figure 32). Moreover, the status LED of your gateway indicates available updates by a blue flash.

General Settings

Please name your Gateway in case you want to access multiple buildings.

Proceed
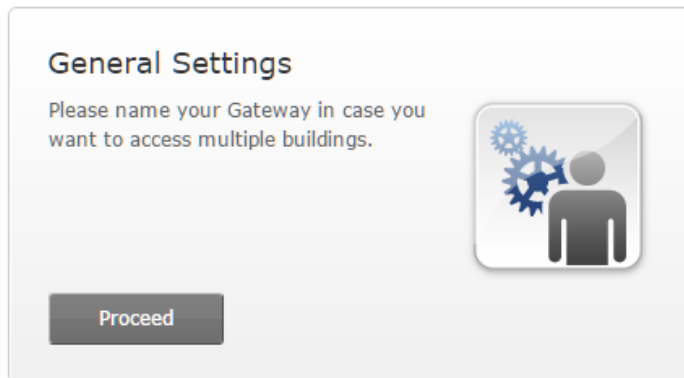
Figure 32

3.5.1   Firmware update for the gateway

If there is an update for your gateway available and you wish to download it, follow these steps:

Click the "Download now" button (see figure 33).

Firmware		
Currently installed version: 1.0.52		
A software update to version 1.0.52.2 is available.		
	Search for updates	⬇Download now
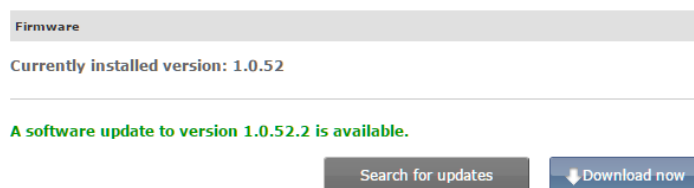
Figure 33

If an update for your gateway has been successfully downloaded, start the installation by clicking on "Install".

Firmware

Currently installed version: 1.0.52

The update to version 1.0.52.2 is ready. The installation requires a system restart and will take a couple of minutes. Please do not disconnect the gateway from power during restart!

Search for updates   Install
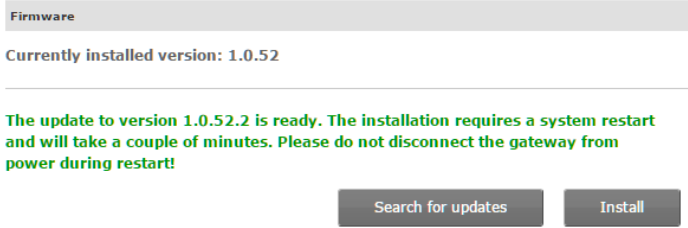
Installation time of a new update on your gateway may take up to 3 minutes. After successful installation, you will automatically be directed to the status site. An entry under "System status" informs you about the successful installation (see figure 34).

Firmware update

The firmware update to Version 1.0.52.2 was successful.

8/26/2015, 11:37:02 AM

Hide
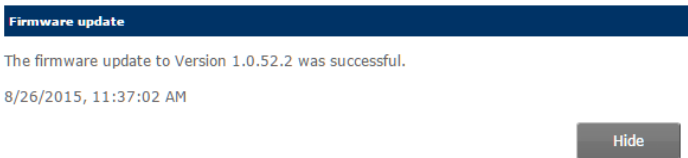
Figure 34

> **Caution:** Make sure that power supply will not be interrupted during the installation. An interruption during the installation process can lead to a defection of your device.

If the download should fail, check your internet connection, make sure that the network settings of your gateway are correct (more information about the appropriate settings to be found in section 3.3 "Network configuration") and access is not blocked by any firewall.

3.5.2 Firmware update for Smart Home components

The firmware of your Smart Home actuators and sensors are updated via radio frequency. Your gateway takes the role of the ZigBee Over-the-Air (OTA) Upgrade Server. From this server, all of your Smart Home components can get their appropriate update.
When updating your Smart Home components, the new firmware is downloaded via radio and installed afterwards.

> **Caution:** During installation of an update, the Smart Home component is not available for a few seconds. After successful installation, the component restarts. Therefore, you can define time spans. In a store, for example, you can define that the lights will not turn off while the store is opened. Therefore, they are suitable for connecting critical loads such as refrigerators, freezers, servers etc.

To activate the ZigBee OTA Upgrade Server on the gateway, enable the option "Use this gateway to supply the system with updates" (see figure 35).

Updates Smart Home System

The ubisys Smart Home Update Service keeps your components up to date

☑ Use this gateway to supply the system with updates
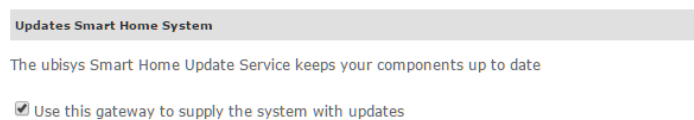
Figure 35

> **Caution:** If you are running several gateways in your network, make sure that only one gateway provides the updates at any time, so it takes the roles of the ZigBee Over-the-Air (OTA) Upgrade Server.

At the bottom of the update page, you find a list with all components of your SLV VALETO® Smart Home System that have reported on the update server. If an update is available, it will be shown in the appropriate line of your component. Figure 36 shows an example of listed components of a test installation.

Components:

▸ **S1** (00:1F:EE:00:00:00:00:9E) 🗑	up to date
▸ **D1** (00:1F:EE:00:00:00:00:A1) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:00:A9) 🗑	up to date
▸ **S2** (00:1F:EE:00:00:00:00:E8) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:01:78) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:01:7D) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:01:7E) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:01:84) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:01:85) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:01:87) 🗑	up to date
▸ **S2** (00:1F:EE:00:00:00:01:88) 🗑	up to date
▸ **S2** (00:1F:EE:00:00:00:01:8A) 🗑	up to date
▸ **D1** (00:1F:EE:00:00:00:01:A3) 🗑	up to date
▸ **D1** (00:1F:EE:00:00:00:04:21) 🗑	up to date
▸ **S2** (00:1F:EE:00:00:00:04:23) 🗑	up to date
▸ **S2** (00:1F:EE:00:00:00:04:29) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:04:2E) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:04:31) 🗑	up to date
▸ **D1** (00:1F:EE:00:00:00:04:34) 🗑	up to date
▸ **S2** (00:1F:EE:00:00:00:04:39) 🗑	up to date
▸ **S2-R** (00:1F:EE:00:00:00:04:72) 🗑	up to date
▸ **C4** (00:1F:EE:00:00:00:04:73) 🗑	up to date
▸ **D1** (00:1F:EE:00:00:00:05:66) 🗑	up to date
▸ **S2** (00:1F:EE:00:00:00:05:A7) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:05:BC) 🗑	up to date
▸ **S1** (00:1F:EE:00:00:00:05:E4) 🗑	up to date
▸ **J1** (00:1F:EE:00:00:00:07:EF) 🗑	up to date
▸ **S2** (00:1F:EE:00:00:00:08:82) 🗑	up to date

Figure 36

Delete a component

If you want to remove a component from your list (because the component has been physically removed and therefore it no longer needs to be displayed in the web interface, for example), click on the paper bucket icon (see figure 36).

Define update times

You can limit automatic updates to certain time spans. Since some components (such as the universal dimmer D1) restart after installing an update, and turn off connected components in the meanwhile, an appropriate configuration is recommended (e.g. while you sleep or when being on the road). In addition, it is ensured that your network is not charged with downloads in the main usage time.

To allow automatic downloads of updates only at specific times, enable the option "Allow update downloads only at specific times only" and configure appropriate days and time spans by setting check marks and defining times (see figure 37).

☑ Allow update downloads at specific times only

☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☑ Saturday ☑ Sunday

Start	01	:	00
End	05	:	00

[Save]

Figure 37

Update mode

When updating your Smart Home components, you have the choice between automatic or manual installation (see figure 38).

○ Distribute and install new firmware automatically on all ZigBee devices
○ For each device determine if and when new firmware is to be installed

[Save]

Figure 38

In general, it is recommended to automatically install updates. Only this ensures that your system is always up to date.
Since automatic updating does not have a specified update time, except for the configured time span, the manual installation could be advantageous for systems that have safety critical components.

Automatically update all components

When automatically updating, new firmware will be automatically downloaded and installed on your Smart Home components. For this, every 8 hours all devices check the OTA Upgrade Server for new updates. This ensures that your Smart Home System is always up to date.

Figure 39 shows the automatic download of a new firmware version.

Components:

▸ **S1** (00:1F:EE:00:00:00:00:9E) 🗑	up to date
▾ **D1** (00:1F:EE:00:00:00:00:A1) 🗑	❌
Manufacturer	ubisys
Type	Universal dimmer D1 (Rev. 1)
Serial number	00:1F:EE:00:00:00:00:A1
Installed version	Application: 1.05, Stack: 1.60
Last checked	8/26/2015, 6:28:58 AM
▸ **S1** (00:1F:EE:00:00:00:00:A9) 🗑	up to date
▸ **S2** (00:1F:EE:00:00:00:00:E8) 🗑	up to date

Figure 39

Manually update single components

To individually update your components, select "For each device determine if and when firmware is to be installed" and click on "Save" (see figure 40).
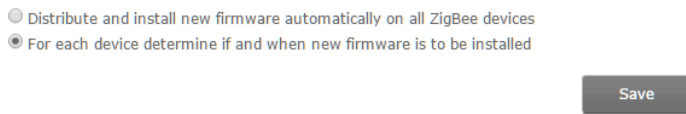
○ Distribute and install new firmware automatically on all ZigBee devices
◉ For each device determine if and when new firmware is to be installed

[Save]

Figure 40

When clicking on one of the components listed, more information about appropriate components will be displayed (see figure 41).

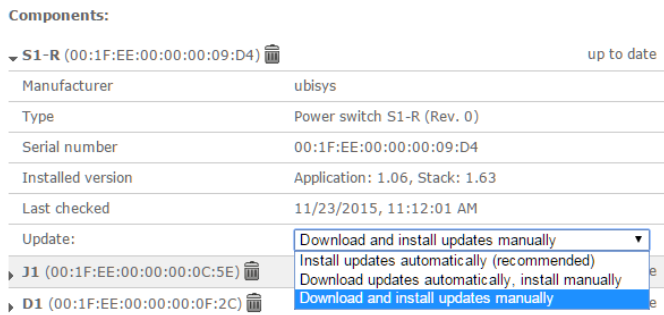**Components:**

S1-R (00:1F:EE:00:00:00:09:D4) 🗑		up to date
Manufacturer	ubisys	
Type	Power switch S1-R (Rev. 0)	
Serial number	00:1F:EE:00:00:00:09:D4	
Installed version	Application: 1.06, Stack: 1.63	
Last checked	11/23/2015, 11:12:01 AM	
Update:	Download and install updates manually ▼	

Install updates automatically (recommended)
Download updates automatically, install manually
Download and install updates manually

▸ J1 (00:1F:EE:00:00:00:0C:5E) 🗑
▸ D1 (00:1F:EE:00:00:00:0F:2C) 🗑

Figure 41

"Install updates automatically"
Recommended default setting. Automatically installs new firmware, taking into account the set periods (see above).

"Download updates automatically, install manually"
Downloading updates can a few minutes, depending on size and network traffic. To avoid having to wait longer periods of time, available updates will be downloaded automatically. Once the update has been completely downloaded, the update process can be started by clicking on "Install" (see figure 42).
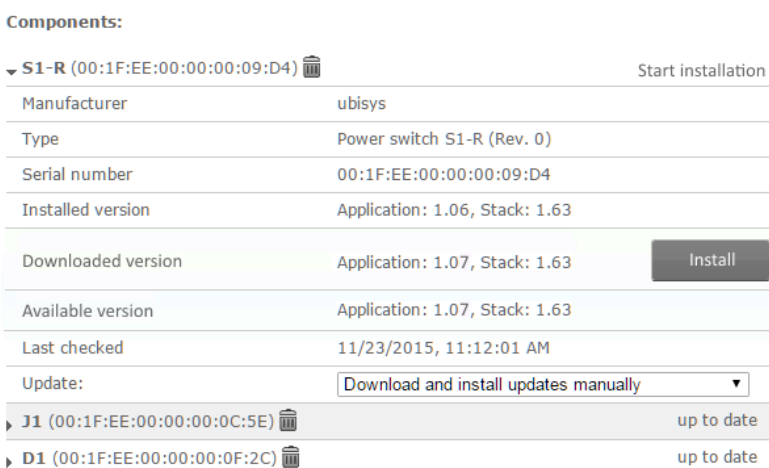
Components:

S1-R (00:1F:EE:00:00:00:09:D4) 🗑		Start installation
Manufacturer	ubisys	
Type	Power switch S1-R (Rev. 0)	
Serial number	00:1F:EE:00:00:00:09:D4	
Installed version	Application: 1.06, Stack: 1.63	
Downloaded version	Application: 1.07, Stack: 1.63	[Install]
Available version	Application: 1.07, Stack: 1.63	
Last checked	11/23/2015, 11:12:01 AM	
Update:	Download and install updates manually ▼	

▸ J1 (00:1F:EE:00:00:00:0C:5E) 🗑   up to date
▸ D1 (00:1F:EE:00:00:00:0F:2C) 🗑   up to date

Figure 42

"Download and install updates manually"
This option allows you to manually define download and upload periods. Please note that downloading updates can take some time, depending on their size.
If a new update is available, it will be displayed in line "Available version". Here, you can choose whether to simply download the update to your smart home component or to both download and install it.

When choosing "Download & install", the installation will begin right after downloading the update. The time can vary, depending on update size and network traffic.

By clicking "Download" the update will just be downloaded. After successfully downloading the update, it can be found in line "Downloaded version". Installation will be started by clicking "Install" (see figure 43).

Figure 43

3.6   Maintenance

If you have problems with your gateway or facility, the maintenance menu allows you – or the SLV support team – to fix them. To execute a maintenance function, click on "Maintenance" in the main menu.

3.6.1   Configuration backup

With this option you can save the current configuration of your Smart Home gateway. This function is recommended, when you changed the configuration, renewed the ZigBee network key or when you are about to make a factory reset on your gateway. For this, click on the "Start" button (see figure 44) and your backup will automatically be created.

Configuration back up	
	Start

Figure 44

Depending on size, this procedure can take up to 5 minutes. After successfully creating your backup, your browser asks you to save the backup on your PC or tablet (see figure 45).
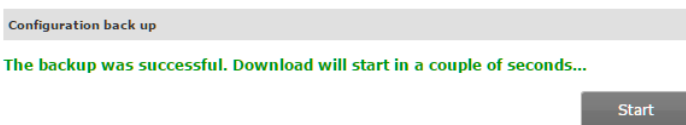
Configuration back up	
The backup was successful. Download will start in a couple of seconds...	
	Start

Figure 45

> **Caution: Store the backup in a safe place, preferably on different store devices (e.g. USB stick, intern hard drive, extern hard drive, cloud storage).**

3.6.2   Restore configuration

If you recently chose the option "Configuration backup", you can restore the saved state of your Smart Home facility here.
Once you have selected the appropriate file by clicking on the "Choose file" button (see figure 46), click on "Upload" to restore the configuration.

Restore configuration	
Choose File No file chosen	
	Upload

Figure 46

3.6.3 Restart

If the gateway does not operate properly anymore, you can restart it here. For this, click on "Restart" (see figure 47).

Restart
Restart

Figure 47

3.6.4 Error diagnosis

To improve the stability of the firmware it is possible to send intern error messages to the servers. No personal or user-specific data will be sent. If you want to contribute to an ongoing improvement of the system, put a check here (see figure 48).
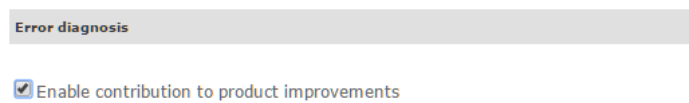
Error diagnosis
☑ Enable contribution to product improvements

Figure 48

3.6.5 Remote support

If there are technical problems with your facility that cannot be fixed by you or your installer, it is best to contact the SLV support team. With a remote maintenance, it is possible to solve certain problems. For this, you simply need to enable the remote maintenance access on your gateway. Access authorization expires automatically after some time or a restart, as long as you don't enable permanent remote maintenance (see figure 49).
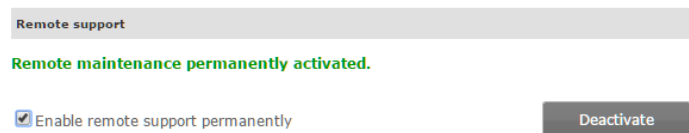
Remote support
Remote maintenance permanently activated.
☑ Enable remote support permanently   Deactivate

Figure 49

Access to your system exclusively takes place via a secured connection by employees of the SLV support teams.

3.6.6 System log files

If a problem occurs, which cannot be fixed directly via the web interface or the app, the log files help the SLV support team as well as our experienced installers to identify and solve the cause (see figure 50).
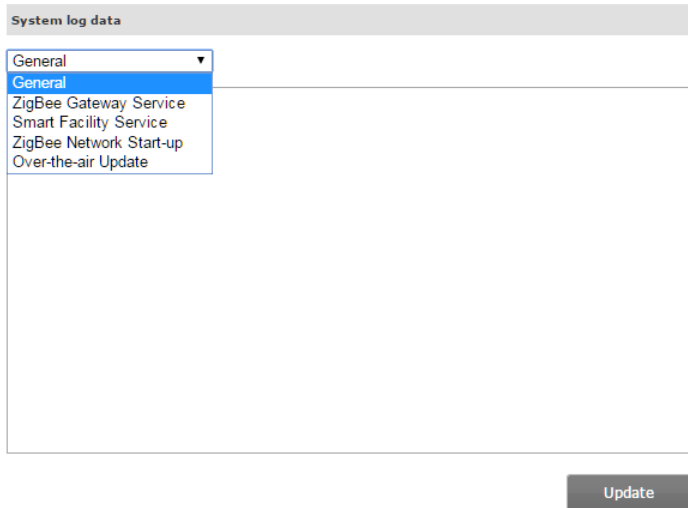

Figure 50

3.6.7 Reset to default settings

This allows the gateway to be reset to its delivery state (see figure 51). All settings will be permanently deleted and have to be reconfigured after restart or restored from a backup. You should only use this option if the gateway does not respond anymore at all or if you want to use it in another facility. If you want to solve technical issues, you should contact the SLV support team first.

Figure 51

3.7 Determining the network parameters

Configuring your gateway, considering a static configuration, requires several network parameters such as name server address, the default gateway, subnet mask etc.
You can determine them via the configuration interface of your router or via your PC.

For Windows XP/Vista/7/8/10:
To determine the network parameters with the help of your PC, follow these steps:

1. Click on **Start -> Control Panel -> Network and Internet -> Network and Sharing Center.**
2. Click on "LAN-Connection" (see figure 52). The name may be different on your PC. If the PC has multiple network adapters, make sure to select one that has an internet connection.
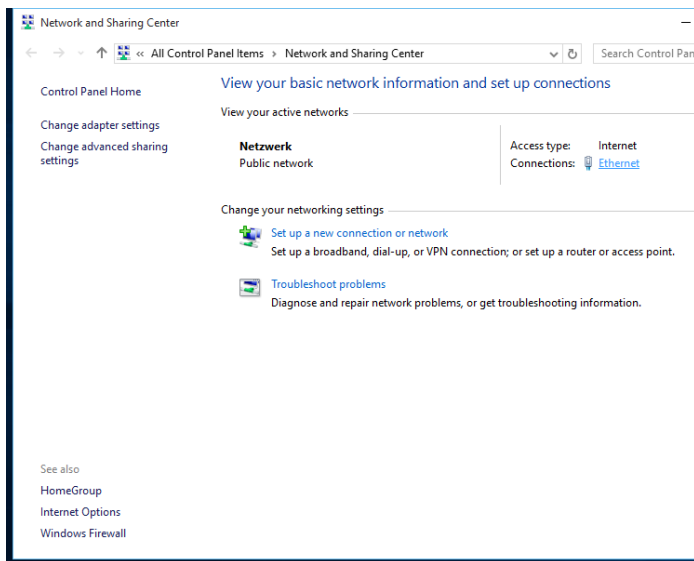

Figure 52

3. In the new window "Ethernet status", click on "Details…" (see figure 53).
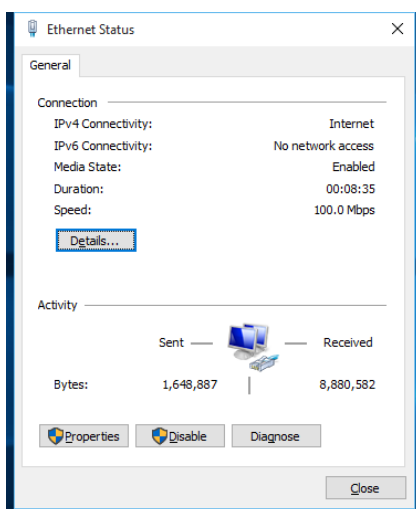

Figure 53

4. In the "Network Connection Details" window, you find the necessary information (see figure 54).
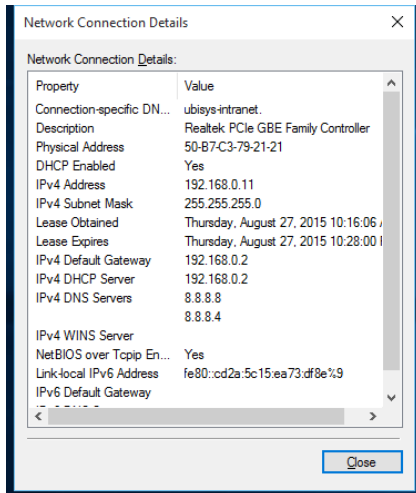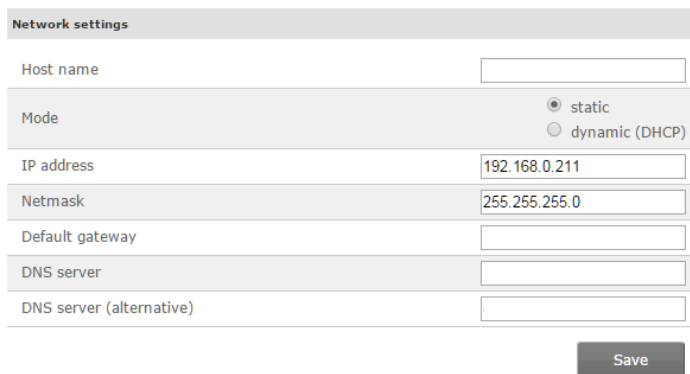

Figure 54

The IPv4 default gateway can be entered in "Default Gateway" and IPv4 DNS server in DNS server (see figure 55). Specifying an alternate DNS server is optional. The second server will be queried, if the primary one is unavailable. Note that the default is not the SLV VALETO® Gateway, but the IP router in your network.

Figure 55

3.8   Determining gateway address

If the gateway is set to DHCP or you don't know the static IP address anymore, you can simply determine it via the smartphone app.

If you are not logged in to the gateway yet, a list of available gateways automatically appears right after starting the app. You can refresh the list by tapping and dragging it down. All active gateways in the local network (Apple Bonjour) will be searched and displayed.
You can find the IP address behind the serial number of your gateway (see figure 56).

Figure 56

If you are already logged in to the gateway, you will be automatically directed to the main page after starting the app. Under Settings -> Facilities you find all gateways that you have access to (see figure 57). By tapping and dragging down the list you can refresh the view; here, all active gateways in the local network (Apple Bonjour) will be searched and displayed.
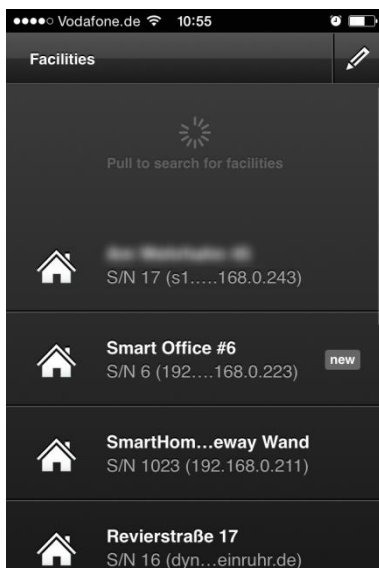

Figure 57

Note: Instead of using the app you can also use an Apple Bonjour browser (such as the ones in Apple Safari, the Avahi browser or similar applications). The SLV VALETO® Gateway

supports the Apple Bonjour technologies multicast-DNS (mDNS) and DNS Service Discovery (DNS-SD).

3.9   Change network parameters for gateway access

Configuration of your SLV VALETO® Smart Home gateway is done via a web interface in your browser. By default, the gateway IP can be found in the router settings. If you use another IP subnet in your local network (home or office network), the gateway will not be reachable.

To adjust the network settings of your gateway and configure it, these steps have to be done:

1. Connect the gateway to a PC or laptop via network cable.
2. Change the IP address of the PC.
3. Adjust network settings of the gateway to the home network.
4. Change the IP address of the PC to its old one.
5. Connect gateway to the home network via cable.

For this, follow these steps:

3.9.1   Connect gateway to PC
Connect your gateway to a PC or laptop via the included network cable (see figure).
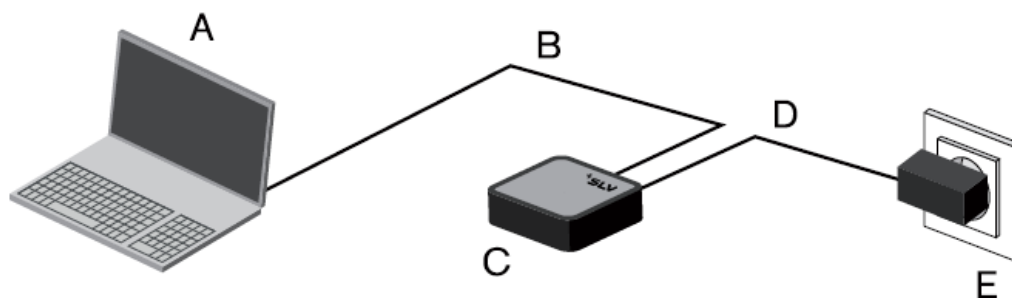
A PC/Laptop   D Power Adapter
B Network Cable   E Power Socket
C SLV VALETO® Gateway

3.9.2 Change the IP address of your PC

To change the IP address of your PC, follow these steps:

Windows XP/Vista/7/8/10

1. Click on **Start -> Control Panel -> Network and Internet -> Network and Sharing Center.**
2. Click on "LAN Connection" (see figure 58). The name may be different on your PC. If your PC has several network adapters, select the one that is connected to the gateway.
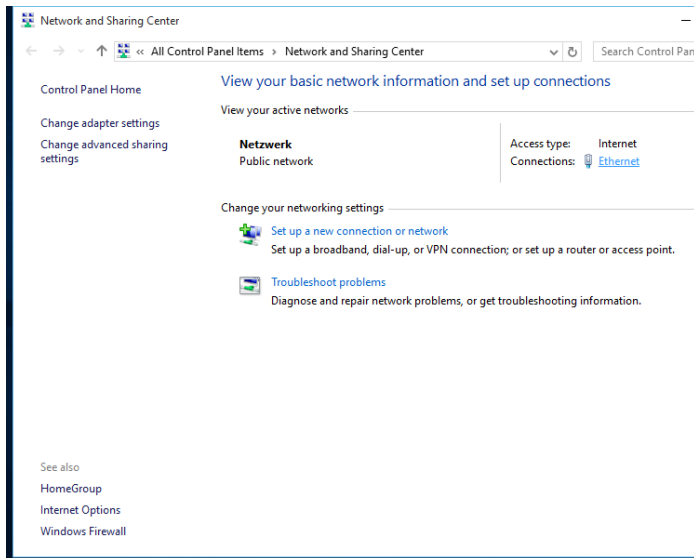
Figure 58

3. In the new window "Ethernet Status", click on the "Properties" button (see figure 59).
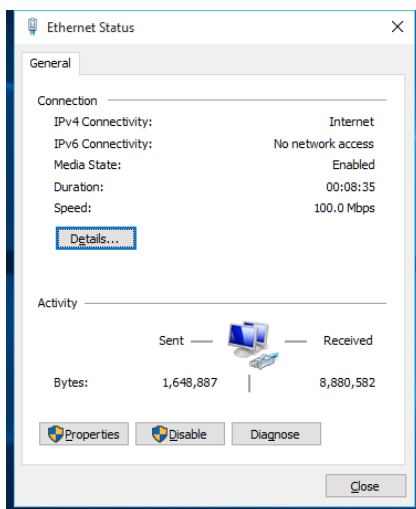
Figure 59

4. In the new window "LAN Connection Status", select "Internet Protocol Version 4 (TCP/IPv4)" and click on the "Properties" button.
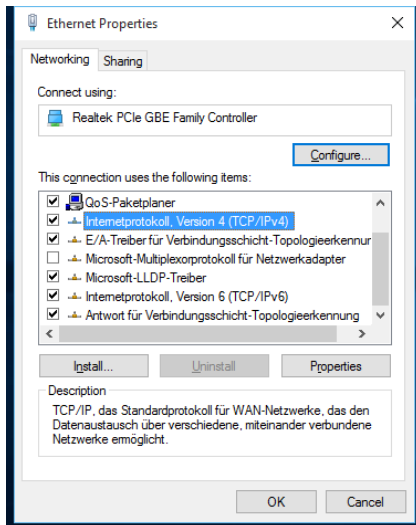
Figure 60

5. In the new window "Properties of Internet Protocol Version 4 (TCP/IPv4)", change "Automatically obtain IP address" to "Use the following IP address" (see figure 59). If this option is already set, note the values below IP address, subnet mask, default gateway and primary/secondary DNS server in order to restore them at a later time.

Figure 61

6. Under IP address, enter the address 192.168.0.200, for example. For the subnet mask, enter the value 255.255.255.0, in case this value is not entered automatically.

Figure 62

7. Accept the settings by clicking on "OK". Your PC is now in the same network as the gateway is. Note that your PC is temporarily not connected to the internet and access to other devices in your network environment (such as file server, network printer etc.) is temporarily not granted anymore.
8. Configure your gateway as described in section 3.3 "Network Configuration".
9. After successfully configuring the network settings of your gateway, it should now be available in your existing network environment. To undo the changes to the network settings of your PC, follow the steps 1 to 5.
   In the "Properties of Internet Protocol Version 4 (TCP/IPv4)" window, as in step 5, change the setting to "Automatically obtain IP address", if you previously used DHCP or change the values below IP address, subnet mask and default gateway to the previously noted values, if your PC has used a static address (see figure 59).

For MAC OS X

1. In the finder, click on the apple icon on the top left and then on "System Preferences…" (see figure 63).
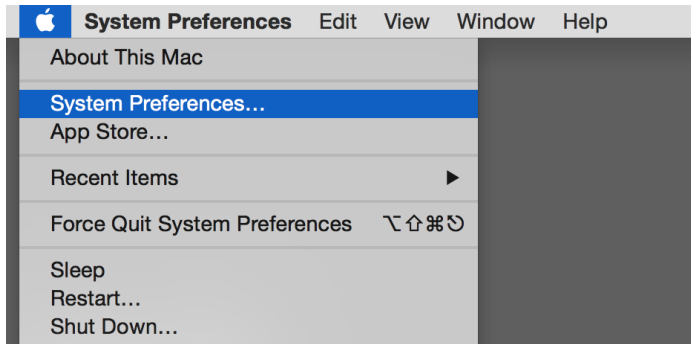
Figure 63

2. A new window opens (see figure 64).
3. In the section "Internet & Wireless Communication", click on "Network".
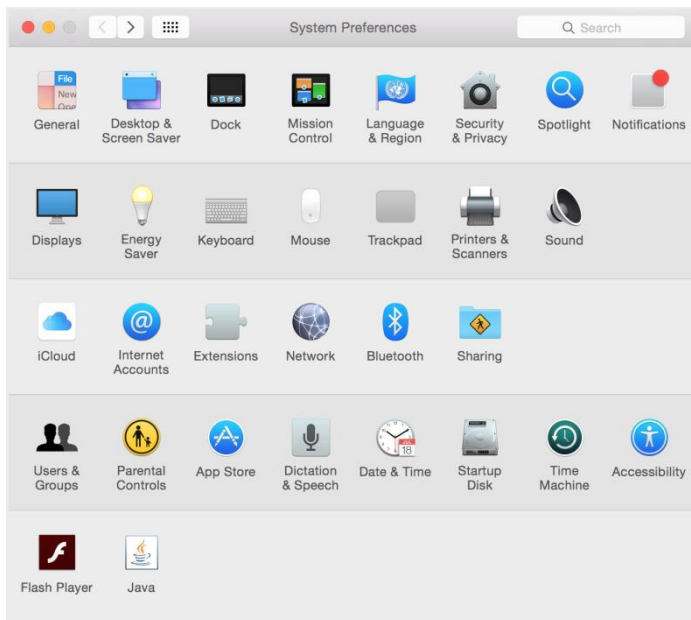
Figure 64

4. You see your network status with the appropriate settings now (see figure 65).
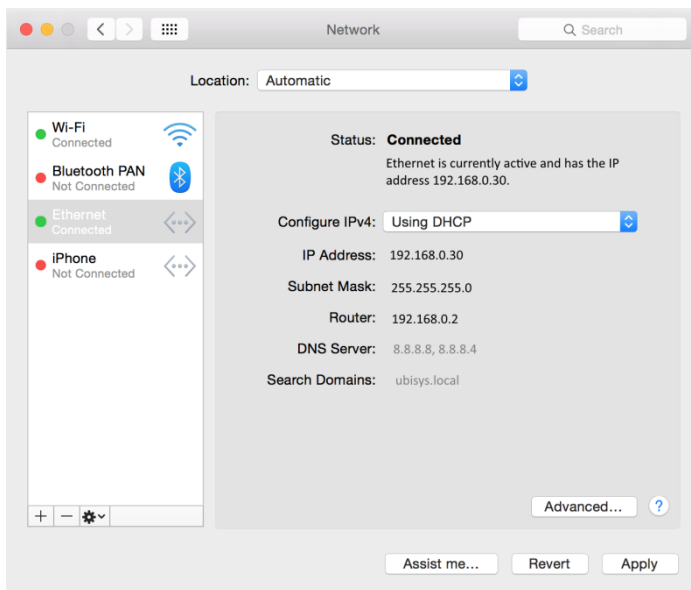
Figure 65

5. Under Configure IPv4, change "DHCP" to "Manually" (see figure 65). In case this option is already set, note the values below IP address, subnet mask, router and DNS server to restore them at a later time.
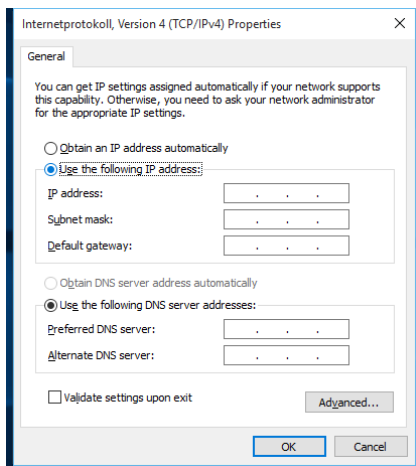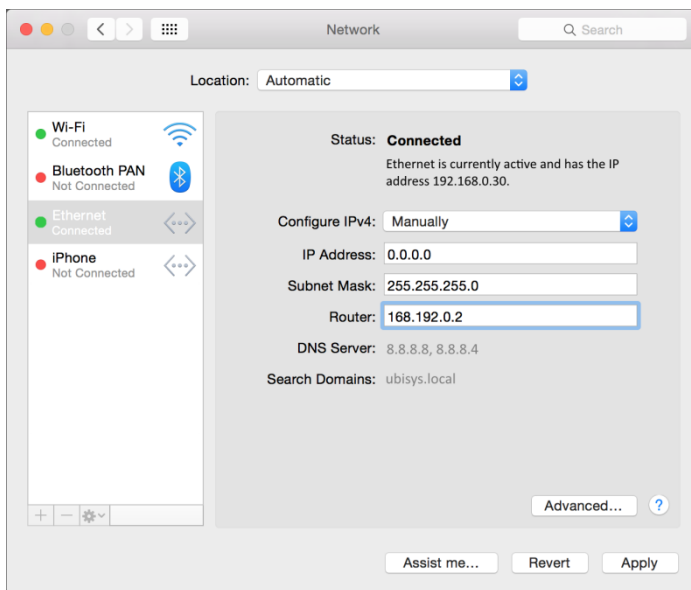

Figure 66

6. Under IP address, enter 192.168.0.200, for example. For the subnet mask, enter 255.255.255.0, in case this value is not entered automatically.
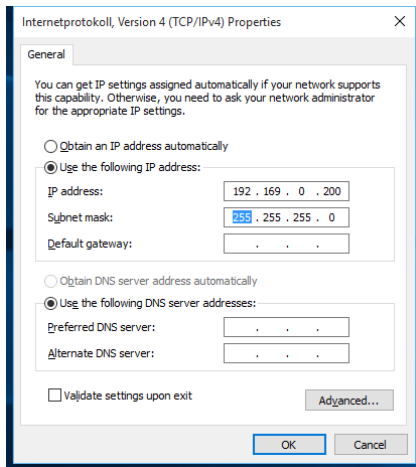7. Accept the settings by clicking on "Apply". Your Mac is now in the same network as the gateway is.
8. Configure the gateway as described in section "Network Configuration".
9. After successfully configuring the network settings of your gateway, it should now be available in your existing network environment. To undo the changes to the network settings of your MAC, follow the steps 1 to 5.
In the "Network" window, as in step 5, change the setting to "DHCP", if you previously used DHCP or change the values below IP address, subnet mask, router and DNS server

to the previously noted values, if your MAC has used a static network configuration (see figure 59).

3.10 Controlling SLV VALETO® Smart Home on the road

In order to control your SLV VALETO® Smart Home System while on the move, several settings in your router and your Smart Home app have to be configured first.

The following adjustments have to be done:

1. Port forwarding via NAT (Network Address Translation), in case the gateway does not obtain a public address. All requests from the internet will automatically be directed to the gateway by the router.
2. Public address: In order for the app to find the router, its IP address must be known. If your router does not obtain a static IP address, setting up a DDNS provider is necessary here, for example. If the router does not obtain a public address, but only one from the "private" address pool via NAT (often the case for LTE routers), you have the option of setting up a VPN tunnel, for example.
3. Configuring the app settings.

3.10.1 Configuring the internet router

In order for your router to allow communication between the mobile end devices and your Smart Home gateway, you have to set up port forwarding. For this, the TCP port 8888 of your Smart Home gateway has to be directed to the outside.

> **Caution:** Do not direct the TCP port 80 for the web interface! If you need access to the web interface when being on the road, set up a secured VPN connection, if necessary.

Depending on the configuration, port forwarding is done either via name (gateway uses DHCP) or via IP address (gateway uses a static address).

Follow these steps:

1. Open the configuration interface of your router. Usually, it is opened via the web browser. If necessary, read the documentation of your router.
2. Set up port forwarding for the TCP port 8888. This can be configured under NAT (Network Address Translation) and the port rules of the router.

   Example:

   a) Port forwarding via name: TCP port 8888 (public) -> SLV VALETO®-Gateway [1] Port 8888 (local)
   b) Port forwarding via IP address: TCP port 8888 (public) -> 192.168.xxx.xxx port 8888 (local), with 192.168.xxx.xxx being the static IP of the gateway.

[1] SLV VALETO®-Gateway is the host name of your gateway and can be changed in the configuration interface under network settings.

> **Note:** You can operate more than one gateway in a local network. For external access, then, you select another port than the default value 8888 for the public side, e.g. TCP port 8889 (public) -> SLV VALETO®-Gateway port 8888. For some routers, this function is called port forwarding and it has its own menu item in the router's configuration interface.

3.10.2 Public IP address

In order for your app to find the router in the internet, the public IP address of your router has to be known. If your router has a static IP address, you can skip this part and continue with the next section "Configuring the app".
If the router has a volatile public IP address, which is the case with most DSL connections, you require a service, such as DynDns or no-ip. On every internet login, these services automatically generate a so called DDNS entry for your router. In the router, the DDNS provider has to be configured (dlinkddns, for example, is a free version of DynDns for owners of a D-Link routers; no-ip is free as well for private usuage.). If necessary, read the documentation of your router to determine, which options are or available or check the support forums of your router manufacturer.
If your router has nonpublic IP address from the private IP pool (carrier-grade NAT), which is the case with most LTE routers, you have the option to set up a VPN tunnel to a server with a static IP address. For determining the best course of action, visit the support forums of your LTE provider or router manufacturer.

3.10.3 Enterprise networks, Firewall

If your network is protected by a firewall, as is often the case with corporate networks, make sure that an exception rule for incoming data traffic on port TPC 8888 is defined in the firewall configuration. Otherwise the firewall will block any connections between mobile end devices with the SLV VALETO® Smart Home app and your Smart Home gateway.
If you want to use the gateway in a corporate network managed by a network administrator, contact your network administrator to obtain the recommended network settings for your company.

3.10.4 Configuring the app

To control your SLV VALETO$^®$ Smart Home gateway while being on the road, its address has to be entered in the app. Basically, the connection is secured and only possible via authenticated devices. Follow these steps:

1. Start the app.
2. In the menu, under Configuration -> Facilities click on the pencil icon. If you are at the start screen (see figure 67), tap the display for 2 seconds.
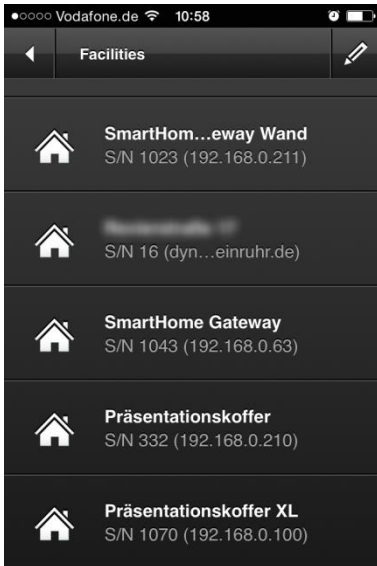
Figure 67

3. The view changes to configuration view (see figure 68).
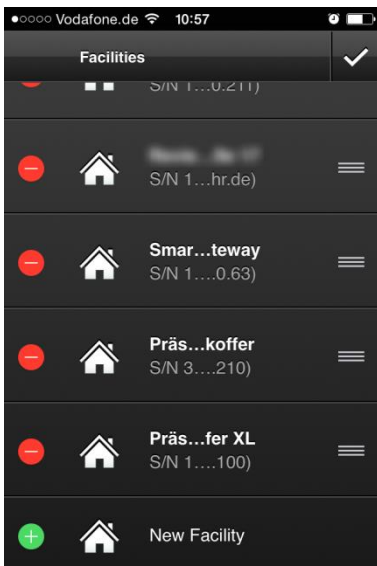
Figure 68

4. Tap "New Facility" (see figure 68) – even if you just want to additionally enter a public address for an already known facility.
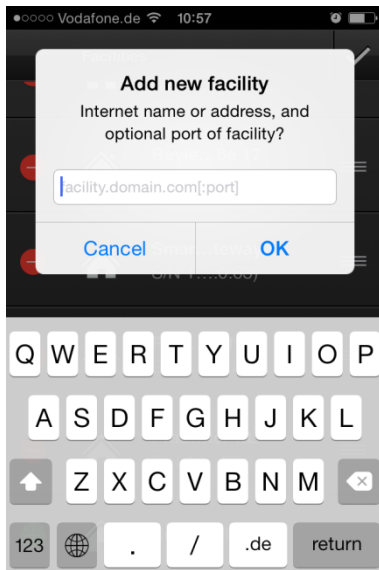
Figure 69

5. In the entry field, enter the host name (can also be a DDNS host name) or, optionally, the static, public IP address of your router or the gateway (see figure 69) and accept by tapping "OK". If you defined a port number different from 8888 for port forwarding on public side, enter a colon after the host name, followed by the port number, e.g. "smarthome.dyndns.org:8889", if you selected port 8889. "smarthome.dyndns.org" is an example name here. Instead, use the host name or the static IP address of your router.
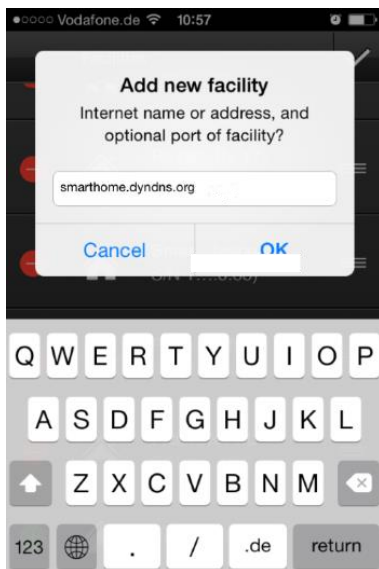
Figure 70

6. The recently entered gateway now appears in the list of available gateways. Tap and hold the list for 1 second (or tap the check mark, if you have used the pencil icon) to end the edit mode.
7. Your Smart Home System can now be reached via app while being on the move.
8. Tap the new entry to establish a connection. If the facility was already known by another (local) address, this address will be replenished and the additional entry disappears.

Caution: Not all routers are able to establish a connection from the internal network, i.e. that your smartphone is in your own Wi-Fi, via the public address, because port forwarding only works for external access. Exemplary for this behavior are the Fritzbox models of AVM and the Speedport of the Deutsche Telekom. Other models, however, such as the Vodafone easybox are able to forward requests from the local network.

If your router is not able to forward internal requests, follow these steps:

1. Temporarily disable the Wi-Fi function of your smartphone.
2. In your smartphone app, tap the gateway and wait until connection has been established. If the gateway has already been entered in the list, the second entry disappears. Instead, an entry with more than one address will exist. If not, an access code is required.
3. Enable the Wi-Fi function of your smartphone. From now on, the app automatically establishes a connection to the gateway via one of the two addresses. Turning off the Wi-Fi function of your smartphone is not necessary anymore.

Note: If you entered the public address first, you can determine the local address later by dragging down the list (swipe gesture). The list of available gateways in the local network will then be refreshed by the integrated support for Apple Bonjour. If both an external (Internet) and internal (Wi-Fi) address is found for a gateway, both entries will automatically be combined and your Smart Home System reachable via Wi-Fi on site as well as via mobile radio while being on the move.

3.11   LED status signals

The LED on the front of your gateway shows the current status of your Smart Home System.
The following status signals and error messages are defined:

Color	Status	Meaning	What to do?
Green	Constant	Everything ok	/
orange	Blinking	warning	The status site on the configuration web interface informs you about occurring warnings.
Orange & green	Blinking alternately	Updating	During the update process, power supply must not be interrupted.
Red	Blinking	Error	The status site on the configuration web interface informs you about occurring errors.
Red	Permanent	Critical error	A critical error occurred on your gateway. Please contact the support.
Blue	Flashing up	New update available	A new update for your gateway is available. You can install it via the configuration web interface of your gateway.
Blue	Flashing	Add smartphone	The function "Adding a new control device" has been activated via the configuration web interface of your gateway. Enter the access code in the app of the new control device to enable access via this device.

3.12   Protected Reset Button on the Rear Side

Your SLV VALETO® Smart Home gateway has reset button on the rear side protected
against unintended activation, which can be used to execute certain functions.
For this, push the button with the help of a thin, stub item (such as a paper clip) on the back
of the gateway (see figure 2 in section 2.2 "Connecting the gateway").
In case of occurring unexpected problems with your gateway that cannot be fixed at all (e.g.
it is not possible anymore to make settings via the web interface), the gateway provides
several reset functions.

The following functions are possible:

Function type	What happens?	What to do?	LED
Set to DHCP and reset password	Network settings are set to DHCP and the default password admin is restored.	Push the button shortly (0.5s) until green LED starts to blink. Shortly push the button again within the next 3 seconds.	2x blue flashing confirms successful adjustment.
Set to static IP address and reset password	Network settings are set to the static IP address 192.168.0.211, subnet mask 255.255.255.0 and the default password admin is restored.	Push the button shortly (0.5s) until green LED starts to blink.	1x blue flashing confirms successful adjustment.
Restore factory settings	All settings will be deleted have to be reconfigured. Device will act brand new. **All settings will be deleted!**	Unplug power from the power socket. Push the reset button, plug the AC adapter into the socket again and **hold the reset button for 3 seconds meanwhile**.	Blue, rapidly blinking

3.13 Troubleshooting guide

General information
If an error message occurs on the gateway's web interface, which cannot be traced back to a recently made change, refresh the view of your browser. If the error message still exists, restart the gateway (Click on **Maintenance -> Restart**). If the error message still exists after the reboot, contact the support, if necessary.

Basic settings

Message (below "Date and Time")	One of the NTP servers cannot be reached.
Explanation	To automatically synchronize date and time, an internet connection is required. To make sure that your gateway has also access to it, all network parameters in the network configuration, such as gateway, DNS and, optionally, proxy settings have to be set correctly.
Solution	Check the network settings and network configuration.

Updates

Message (below "Firmware")	An error has occurred. Host could not be resolved.
Explanation	There is no internet connection or the network parameters have not been configured correctly for internet access.
Solution	Please configure the network settings correctly.

Message	Proxy could not be resolved.
Explanation	In order to receive updates, an active internet connection is required. To make sure that your gateway has also access to it, all network parameters in the network configuration, such as gateway, DNS and, optionally, proxy settings have to be set correctly.
Solution	Check the network settings and network configuration.

Caution: In case of occurring error messages that are not listed here, contact the support.

Section 4

More information

4.1   Storage

Make sure that your gateway is placed in a ventilated and temperate spot. A damp basement is not a suitable place of accommodation and can lead to technical problems or even the destruction of the gateway.

4.2   Cleaning

Clean the product with a soft, clean, dry and lint-free cloth. To remove heavy soiling, the cloth can be slightly tempered with lukewarm water. Do not use cleansing supplies containing thinners, because they can damage the plastic case and the label.

4.3   Disposal Note

	Do not dispose of in household waste! Electronic devices have to be disposed of in accordance to the directive on waste electrical and electronic equipment via local depots for electronic equipment.
	The CE mark is free trade sign addressed exclusively to the authorities, and not containing warranty of any properties.

4.4   Declaration of Conformity

The company

Ubisys Technologies GmbH
Am Wehrhahn 45
40211 Düsseldorf

states, in sole responsibility, that the product

SLV VALETO® **Gateway** (article number 1002411) or **Gateway G1** (article number 1007)

which refers to this declaration, complies with the following standards directives:

R&TTE Directive **99/5/EG**	EN 300 220-1 V2.3.1 (2010-02) EN 300 220-2 V2.3.1 (2010-02) EN 62479:2010
EMC Directive **2004/108/EG**	EN 301 489-1 V1.9.2 (2011-09) EN 301 489-3 V1.4.1 (2002-08) EN 55022:2010 EN 50130-4:2011 EN 61000-3-2:2006 + A1:2009 + A2:2009 EN 61000-3-3:2008
Low Voltages Directive 2006/95/EG	EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011

Düsseldorf, 01.11.2013

Dr.-Ing. Arasch Honarbacht (CEO, Leader Research and Development)

4.5   Glossary

Carrier-grade NAT	Describes a method in which the internet provider assigns a private internet address to its customer, which is only valid for the length of one internet dial-in. This method is often used in LTE routers. Such routers cannot be provided with a permanent host name via DDNS. In this case, a VPN tunnel is an option.
DDNS	Dynamic Domain Name Service. A DNS service, whose entries are short-lived and be updated automatically. Often used for routers with a volatile, public IP address. By giving it a permanent host name, the router can be accessible. Not suitable, if the internet service provider only assigns private addresses (carrier-grade NAT). Known DDNS providers are DynDns and No-Ip.
DHCP	Dynamic Host Configuration Protocol. Allows central administration of network parameters such as IP address, subnet mask, name server etc. for all devices in a network. The Smart Home gateway is a DHCP client; a DHCP server has to be provided in the network environment.
DNS	Domain Name Service. An internet service that is able to convert easy-to-remember names such as www.google.com to IP addresses like 173.194.113.151 (IPv4) or 2a00:1450:4005:808::1018 (IPv6), which are required for communication via the internet.
DNS Server	A server providing the DNS service. The IP address of one or more such servers is uniquely entered during the network configuration of an internet-enabled device. From now on, it is possible to enter easy-to-remember host names instead of hard-to-remember, and optionally frequently changing, IP addresses on the device.
Ethernet	See IEEE 802.3
Firmware	Describes the fix installed software on a device, e.g. the gateway or single components of your Smart Home facility. Although the software is installed fix, it can be updated on SLV devices.
Host Name	Name of a device (PC, server, Smart Home gateway, NAS, printer etc.) in the internet or in the local network. Examples: www.google.com or smarthome.dyndns.org, or slv-gateway-0815.home.local.
IEEE 802.3	Also known as Ethernet. A number of international standards for wired networks connecting PCs to many other devices such as the Smart Home gateway, NAS, printer etc. Basis for the IP based network. IEEE 802.3af standardizes the power supply via the network cable, Power-over-Ethernet.
IEEE 802.11	A number of international standards for wireless networks connecting several devices such as PCs, tablets, smartphones etc. with each other. Basis for the IP based network via Wi-Fi.
IEEE 802.15.4	An international standard for wireless networking of objects. Low power consumption, high reliability and safety feature the standard. Amongst other things, it is the basis for ZigBee PRO and ZigBee IP.
IP, IPv4, IPv6	Internet Protocol. Basic protocol of networking for the internet. Currently, version 4 ("IPv4") is the most distributed; a gradual change to version 6 ("IPv6") is underway.
IP Address	Address of a web-enabled device. IPv4 addresses have the form 192.168.0.211, IPv6 addresses the form fe80::4138:954a:d196:3c37. The IP address has a part that

	indicates the network and a part, which identifies the device in the network. For this, the net mask needs to be specified in IPv4. This will determine where the subnet address ends and where the device address begins. There are public and private IP addresses. Private IP addresses can only be used within the local network; they are not being routed by the internet router and can therefore be used as many times in different networks.
Name Server	See DNS Server.
NAS	Network Attached Storage. A network-enabled storage device, usually one or several hard disk drives, which is power-efficiently embedded into the network without the need of operating an entire PC.
NAT	Network Address Translation. A method, where an internet router provides internet access to several devices in the local network through a single public IP address. For this, every device is assigned to a port. Through this port, the following data traffic can clearly be assigned to each target device. Besides automatically assigning ports when establishing a connection from the private network side to the public side, NAT routers are able to direct incoming data traffic to previously specified ports of certain devices, e.g. your Smart Home gateway, a webcam, a file server in your network etc.
Net Mask	See Subnet Mask.
NTP	Network Time Protocol. An IP based network protocol allowing automatic clock adjustment via the internet. It synchronizes the time of a device, e.g. the Smart Home gateway, with the time of a NTP server, which usually has a highly precise real time clock, such as an atomic clock or a GPS receiver.
NTP Server.	A server providing the NTP service.
OTA	Over-the-Air. Indicates transmission via radio. In this manual, it especially means the transmission of firmware update files via the ZigBee network, the so called ZigBee OTA Upgrade.
Port	A server in the internet can be addressed by the host and the port. The Smart Home gateway, for example, provides the Smart Facility Service on port 8888, which can be used by apps on mobile end devices or In-Home displays to control a Smart Home facility (Property).
Subnet Mask	Also known as net mask. In IPv4, it defines the part of an address that indicates the network. For example, the subnet mask 255.255.255.0 means that the first 3 digit groups determine the network and the last digit group indicates the device. The address 192.168.0.211, referred to a 255.255.255.0 subnet mask, means "Device No. 211" in the network 192.168.0.0. An alternative identifier is 192.168.0.211/24. It means that the first 24 bits identify the network and the remaining 8 bits the device.
TCP	Transmission Control Protocol. A protocol based on the Internet Protocol, which is responsible for reliable data transfers between devices via the internet.
VPN	Virtual Private Network. A method that allows a device to establish a secured connection to a local network via an unsecured medium, such as the internet. The connection between device and network is encrypted, so that an attacker is not able to intercept or manipulate the data traffic or infiltrate the private network.

VPN Tunnel	Connects two local networks via VPN. If the VPN server has a static, public IP address, it can be used to communicate with local networks, whose router do not have a public address, via the internet.
WLAN	Wireless Local Area Network. Synonym for IEEE 802.11, a number of international standards for wireless networks that connect PCs, tablets, smartphones and many other devices with each other via IP.
Wi-Fi	An international standard, guaranteeing smooth, non-propriety IP based networking of devices, such as PCs tablets and smartphones via IEEE 802.11 network adapters.
ZigBee	An international standard for the smart integration of everyday objects, such as lights, power sockets, shutters, heaters, air conditioners, environment sensors, washing machines, dishwashers, alarm systems etc. with features for reliable, safe, mesh, wireless networks. The devices of SLV are based on the ZigBee 3.0 standard at 2.4 GHz; ZigBee is based on IEEE 802.15.4.

4.6 Contact

SLV GmbH
Daimlerstr. 21 - 23
D - 52531 Uebach-Palenberg
T +49. (0)2451 – 4833 0
info@slv.de
www.slv.de