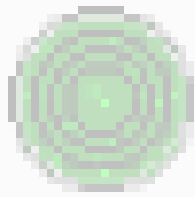




# SimonsVoss OAM Tool Version 1.3



Poll



Scan



Refresh



SimonsVoss Device V01.00

192.168.100.24 (D8-9)

Version: V01.00.00)

## OAM tool

Manual

09.07.2024

**Simons Voss**  
technologies

operating system: Microsoft Windows 1

## Contents

1. Meaning of the text formatting .....	3
2. Determining and setting the IP address .....	4
3. Browser interface .....	9
4. Help and other information .....	13

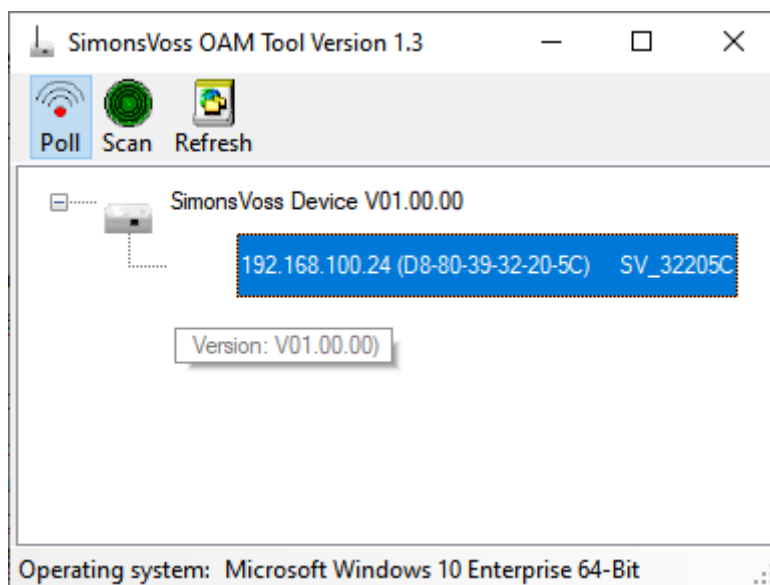
## 1. Meaning of the text formatting

This documentation uses text formatting and design elements to facilitate understanding. The table explains the meaning of possible text formatting:

<b>Example</b>	button
<input checked="" type="checkbox"/> Example <input type="checkbox"/> Example	checkbox
<input checked="" type="radio"/> Example	Option
[Example]	Tab
"Example"	Name of a displayed window
Example	Upper programme bar
<b>Example</b>	Entry in the expanded upper programme bar
<b>Example</b>	Context menu entry
▼ Example	Name of a drop-down menu
"Example"	Selection option in a drop-down menu
"Example"	Area
<i>Example</i>	Field
<i>Example</i>	Name of a (Windows) service
<i>Example</i>	Commands (e.g. Windows CMD commands)
<b>Example</b>	Database entry
[Example]	MobileKey type selection

## 2. Determining and setting the IP address

With the Operation, Administration and Maintenance Tool (OAM tool) you can both read and set the IP address. The OAM tool is available free of charge in the download area of the SimonsVoss website (<https://www.simons-voss.com>). You do not need to install the OAM tool.



### IMPORTANT

#### Unauthorised changing of the IP address

The OAM tool is freely accessible. The OAM tool can be misused by unauthorized persons to change the IP address of your RouterNodes, GatewayNodes or SmartBridges.

- ❑ Block changing the IP address in the OAM Tool via the browser interface (see *Browser interface* [▶ 9]).



### NOTE

#### Unauthorised access with standard access data

The standard access data can be viewed freely. Unauthorised persons cannot change the access authorisations, but they can change the network configuration. You will then no longer be able to reach the device via the network and will have to reset it.

Some browsers do not transmit spaces at the beginning of the password.

1. Change the default password.
2. Do not start or end the password with spaces.

## Determining the IP



### NOTE

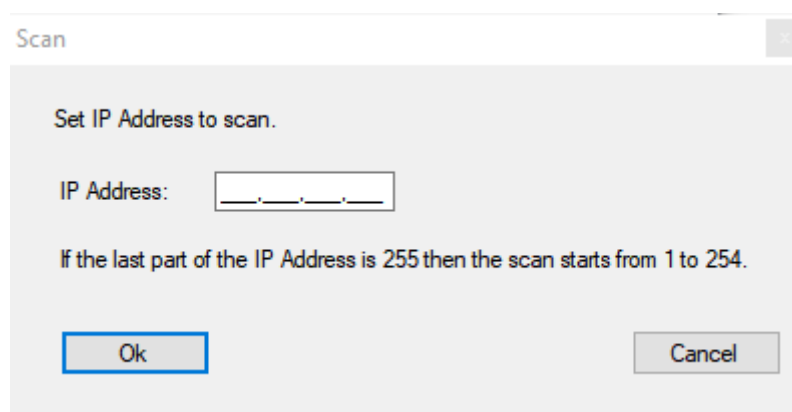
#### Error when connecting to several networks at the same time

The OAM tool searches the network for SimonsVoss network devices. Computers can be connected to several networks (e.g. cable and WiFi). In such a case, it is not clear to the OAM tool which network is to be searched and not all SimonsVoss network devices may be found.

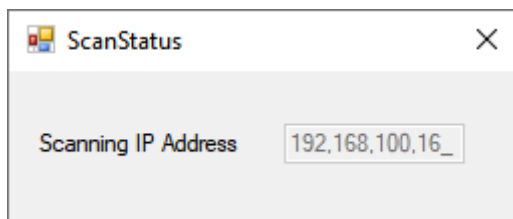
1. Disconnect network connections that are not needed.
2. Only connect the computer to the network that contains the network devices.

The procedure is described for RouterNodes. Use the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

- ✓ OAM tool available and unzipped.
  - ✓ RouterNode connected to the network.
  - ✓ Subnet known.
1. Double-click on the executable file to launch the OAM tool.
    - ↳ The OAM tool will open.
  2. Click the **Scan** button.
    - ↳ The "Scan" window will open.



3. Enter a known IP address of a device in the (WaveNet) network (other or new devices will also be found. If you do not know an IP address, then use the following IP address: 192.168.100.255 - may differ depending on the subnet).
4. Click on the **OK** button.
  - ↳ "Scan" window closes.
  - ↳ OAM tool scans the address range.



↳ OAM tool displays detected devices in the list.

Choose between DHCP server or static IP. You can also make the settings described below in the browser interface (see *Browser interface* [▶ 9]).

The procedure is described for RouterNodes. Use the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

### Set IP for DHCP mode (default)

If you use a DHCP server, a DHCP server will configure the IP address.

- ✓ OAM tool available and unzipped.
  - ✓ RouterNode connected to the network.
1. Double-click on the executable file to launch the OAM tool.
    - ↳ The OAM tool will open.
  2. Click the **Refresh** button.
    - ↳ RouterNode's IP address updated.
  3. Right-click the entry for the RouterNode's IP address you want to update to open the context menu.



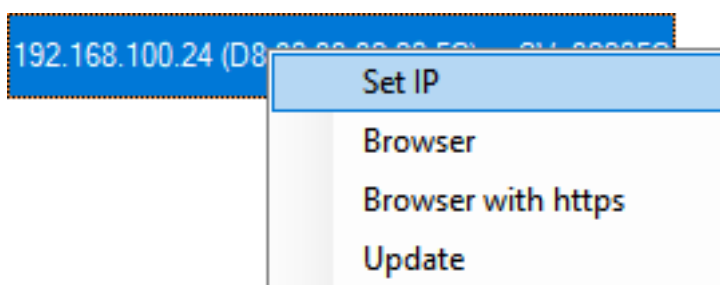
### NOTE

#### Compare MAC

If you select the wrong RouterNode, you could assign the same IP address multiple times.

- ❑ Compare the MAC address of the entry with the label on your RouterNode.

4. Click the **Set IP** entry.



↳ The "Network configuration" window will open.

5. Make sure that the checkbox  Enable DHCP is activated.

6. If no address reservation is provided for this RouterNode on the DHCP server, note down the *hostname* (e.g. *SV\_32205C*). You will need it later when you carry out configuration in WaveNet Manager (see WaveNet manual - Add RouterNode to WaveNet).
7. Click on the **OK** button.
  - ↳ "Network configuration" window closes.
  - ↳ RouterNode restarts.
8. Close the reboot notification window.
9. Close the OAM tool.
  - ↳ DHCP mode is configured.

### Configuring the IP for operation with static IP address

If you do not use a DHCP server, the IP address is configured with the default factory setting. You must change the IP address in this case; if you don't, several RouterNodes will have the same IP (i.e. the default factory IP) and will not be able to communicate.

- ✓ OAM tool available and unzipped.
  - ✓ RouterNode connected to the network.
1. Double-click on the executable file to launch the OAM tool.
    - ↳ The OAM tool will open.
  2. Click the **Refresh** button.
    - ↳ The RouterNode's IP address is now updated.
  3. Right-click the entry for the RouterNode's IP address you want to update to open the context menu.



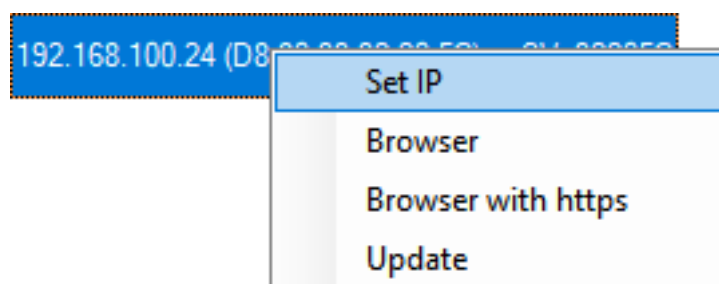
#### NOTE

#### Compare MAC

If you select the wrong RouterNode, you could assign the same IP address multiple times.

- Compare the MAC address of the entry with the label on your RouterNode.

4. Click the **Set IP** entry.



↳ The "Network configuration" window will open.

Network configuration

Set your network configuration.

Host name: SV\_32205C

MAC Address: D8-80-39-32-20-5C

Enable DHCP

IP Address: 192.168.100.024

Subnet Mask: 255.255.255.000

Default Gateway: 192.168.100.001

Ok Cancel

5. Disable the  Enable DHCP check box.
6. Enter a new IP address if required.
7. Click on the **OK** button.
  - ↳ "Network configuration" window closes.
  - ↳ RouterNode restarts.
8. Close the reboot notification window.
9. Close the OAM tool.
  - ↳ IP address is now configured.



### 3. Browser interface

You can use the Ethernet interface in the browser to configure the following for RouterNodes, GatewayNodes and SmartBridges:

- Allow changes using the OAM tool
- Password for the web interface
- IP address/DHCP mode
- Opening and closing the SMTP port

#### Launching

You receive the device with the following factory configuration:

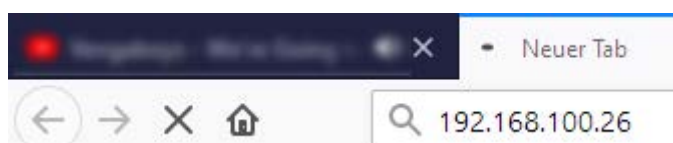
IP address	192.168.100.100 (if no DHCP server is found)
Subnet mask	255.255.0.0
User name	SimonsVoss
Password	SimonsVoss

The procedure is described for RouterNodes. Use the same procedure for SmartIntego GatewayNodes and MobileKey SmartBridges.

Change the default password after you launch for the first time.

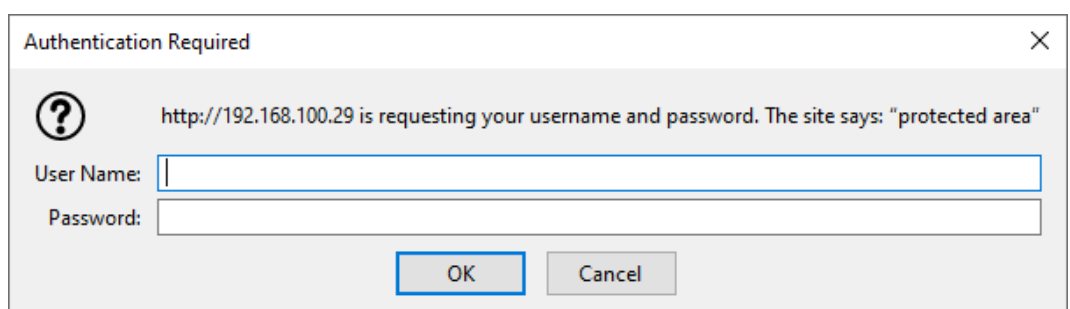
- ✓ Browser open.
- ✓ User credentials known for the browser interface (name and password).

1. Enter the IP address in your browser's address field.



2. Press the Enter key to confirm.

- ↳ The "Authentication required" window will open.



3. Enter the login credentials.

4. Click on the **OK** button.

↳ The browser interface system overview is visible.

OVERVIEW  
WAVENET  
CONNECTION

## System Information: Overview

**Version:**

**Firmware version:** 40.11.00

**Basic network settings:**

<b>MAC Address:</b>	94:50:89:00:36:44
<b>Host Name:</b>	SV_003644
<b>DHCP:</b>	On
<b>IP-Address:</b>	192.168.100.26
<b>Subnetmask:</b>	255.255.255.0
<b>Gateway:</b>	192.168.100.1
<b>DNS-Server1:</b>	192.168.100.1
<b>DNS-Server2:</b>	0.0.0.0
<b>SV Port:</b>	2101
<b>SV SecPort:</b>	2153



### NOTE

**Web interface can no longer be used with the default password with firmware 40.12 and above**

The browser interface remains blocked in firmware version 40.12 or above until the default password has been changed.

❏ Change the default password.

↳ Browser interface is unblocked and settings can be changed.



### NOTE

**Unauthorised access with standard access data**

The standard access data can be viewed freely. Unauthorised persons cannot change the access authorisations, but they can change the network configuration. You will then no longer be able to reach the device via the network and will have to reset it.

Some browsers do not transmit spaces at the beginning of the password.

1. Change the default password.
2. Do not start or end the password with spaces.

## Blocking/enable change to the IP address using the OAM tool

If you do not enable the ▼ OAM-Tool allow, you will not be able to use the OAM tool to perform updates.

- ✓ Browser interface opened.
- 1. Open the [PORT] tab using | CONFIGURATION |.
  - ↳ You will see an overview of the TCP port settings for RouterNode 2.

NETWORK  
PORT  
ETHERNET INTERFACE  
WAVENET

---

## Configuration: port settings

---

### TCP port settings:

SV Port:	<input type="text" value="2101"/>
SV SecPort:	<input type="text" value="2153"/>
SV connection timeout [s]:	<input type="text" value="30"/>
HTTP:	<input type="text" value="On"/>
Telnet:	<input type="text" value="Off"/>
OAM-Tool allow:	<input type="text" value="Yes"/>

- 2. Select the option "Yes" (enable the OAM tool to change the IP) or the option "No" (block change to the IP by the OAM tool) from the ▼ OAM-Tool allow drop-down menu.
- 3. Click on the button  .
  - ↳ Changing the IP address using the OAM tool is locked/allowed.

## Change password

Some browsers do not register any spaces included at the start of a password, so do not begin your password with spaces.

- ✓ Browser interface opened.
- 1. Open the [PASSWORD] tab using | ADMINISTRATION |.

PAS SWORD  
CERTIFICATE  
FACTORY  
REBOOT

---

## Administration: Change password

---

### New password:

New password:	<input type="text"/>
Confirm password:	<input type="text"/>

2. Enter your new password.
  3. Repeat your new password.
  4. Click on the **Save password** button.
- ↳ Password is now changed.

### Opening and closing the SMTP port

The SMTP port is open ex works and after each reset. As a general rule, ports that are not required should be closed. If you close the SMTP port, the OAM tool will no longer find RouterNode 2.

- ✓ Browser interface opened.
1. Open the [PORT] tab using | CONFIGURATION |.
- ↳ You will see an overview of the TCP port settings for RouterNode 2.

NETWORK  
PORT  
ETHERNET INTERFACE  
WAVENET

---

## Configuration: port settings

---

### TCP port settings:

SV Port:	<input type="text" value="2101"/>
SV SecPort:	<input type="text" value="2153"/>
SV connection timeout [s]:	<input type="text" value="30"/>
HTTP:	<input type="text" value="On"/> ▾
Telnet:	<input type="text" value="Off"/> ▾
OAM-Tool allow:	<input type="text" value="Yes"/> ▾

2. Select the "Yes" option (open SMTP port) or the "No" option (close SMTP port) from the ▼ SMTP Port drop-down menu.
  3. Click on the button **Save**.
- ↳ The SMTP port is open or closed.

## 4. Help and other information

### Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

<https://www.simons-voss.com/en/documents.html>

### Software and drivers

Software and drivers can be found on the website:

<https://www.simons-voss.com/en/service/software-downloads.html>

### Declarations of conformity

You will find declarations of conformity and other certificates on the website:

<https://www.simons-voss.com/en/certificates.html>

### Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

### Email

You may prefer to send us an email.

[support-simonsvoss@allegion.com](mailto:support-simonsvoss@allegion.com)

### FAQs

You will find information and help in the FAQ section:

<https://faq.simons-voss.com/otrs/public.pl>

### Address

SimonsVoss Technologies GmbH  
Feringastr. 4  
D-85774 Unterfoehring  
Germany



## This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide ([www.allegion.com](http://www.allegion.com)).

### Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

© 2024, SimonsVoss Technologies GmbH, Unterföhring

All rights are reserved. Text, images and diagrams are protected under copyright law.

The content of this document must not be copied, distributed or modified. More information about this product can be found on the SimonsVoss website. Subject to technical changes.

SimonsVoss and MobileKey are registered brands belonging to SimonsVoss Technologies GmbH.

**SimonsVoss**  
technologies

Made in Germany

A BRAND OF

  
**ALLEGION**