CEStronics Suite 2

Manual for the OMEGA Client

English

Version VA

BRO2234

Contents

1 About this manual

This manual contains basic knowledge about how to manage a system with OMEGA Client. For detailed information please refer to the CEStronics Suite online help which is supplied with CEStronics Suite.

ℹ The CEStronics Suite online help has to be stored in a local memory so that you can use it. It is not possible to open the online help with CITRIX.

Design characteristics

📄 Refers to other documents

ℹ Marks additional information and tips

⚠ Marks warnings in step-by-step instructions and specially important information

Further assistance

The following manuals might be of assistance to you, too:

Topic	Manual
Firmware updates	Programming Adaptors and firmware updates
CEStronics Suite tools	CEStronics Suite online help
Variant upgrade	CEStronics Suite online help

Notes on trademark protection

MIFARE, MIFARE classic and MIFARE DESFire are registered trademarks of NXP B.V. and are used under licence.

2 Basics of the OMEGA FLEX system administration

To be able to use this manual, you should be familiar with the following concepts:

2.1 System family

The **family of systems** is the top most differentiating level for the OMEGA FLEX systems. It specifies which transponder technology (LEGIC or MIFARE) is used in the system:

- OMEGA FLEX MIFARE
- OMEGA FLEX LEGIC

With OMEGA Client, you can manage every system family; however, you can only manage **one** system family **per system** . The OMEGA Client user interface looks slightly different depending on the system family managed.

2.2 Operating mode (only for MIFARE systems)

The **operating mode** specifies, where the locking media authorisations are stored. There are two operating modes for the OMEGA FLEX MIFARE systems:

- **LINE**: Authorisations are stored in the locking device
- **V-NET**: Authorisations are stored in the locking media

2.3 Administration mode (only for MIFARE systems)

Within the two operating modes LINE and V-NET, different **administration types** are possible:

LINE			V-NET
Offline		Online	Virtual
Settings are transmitted to the **locking device** with **master media** übertragen	Data is transmitted from the software via an **RF-Stick** to the **locking devices** übertragen	Data is transmitted centrally from the software via **wireless online network** to the **locking devices** übertragen	Data is transmitted from the software via **Desktop-Writer** to the **locking medium** übertragen
Everything can be combined in one OMEGA FLEX system			

LINE

Offline with master media	No software is deployed. Settings are transmitted via master media to the locking devices (see "Basics of the OMEGA FLEX system administration" Auf der vorherigen Seite)..
Offline with an RF-Stick	Settings are specified in the OMEGA Client software and transmitted via an RF-Stick to the locking device (see "Basics of the OMEGA FLEX system administration" Auf der vorherigen Seite)..
Online with wireless online network	Settings are specified in the OMEGA Client software and transmitted via wireless online network to the locking device (see "Basics of the OMEGA FLEX system administration" Auf der vorherigen Seite).

V NET

Virtual	Settings are specified in the OMEGA Client software and are not transmitted to the locking device but to the locking media (see "Basics of the OMEGA FLEX system administration" Auf der vorherigen Seite).

2.4 ID technique (only for MIFARE systems)

The **ID technology** of locking devices and locking media differ in term of the used security technology used. For OMEGAFLEX MIFARE systems, the following ID techniques are distinguished:

Locking media

Classic locking media	MIFARE Classic and ISO Locking media
DESFire Locking media	With 3DES encrypted DESFire Locking media

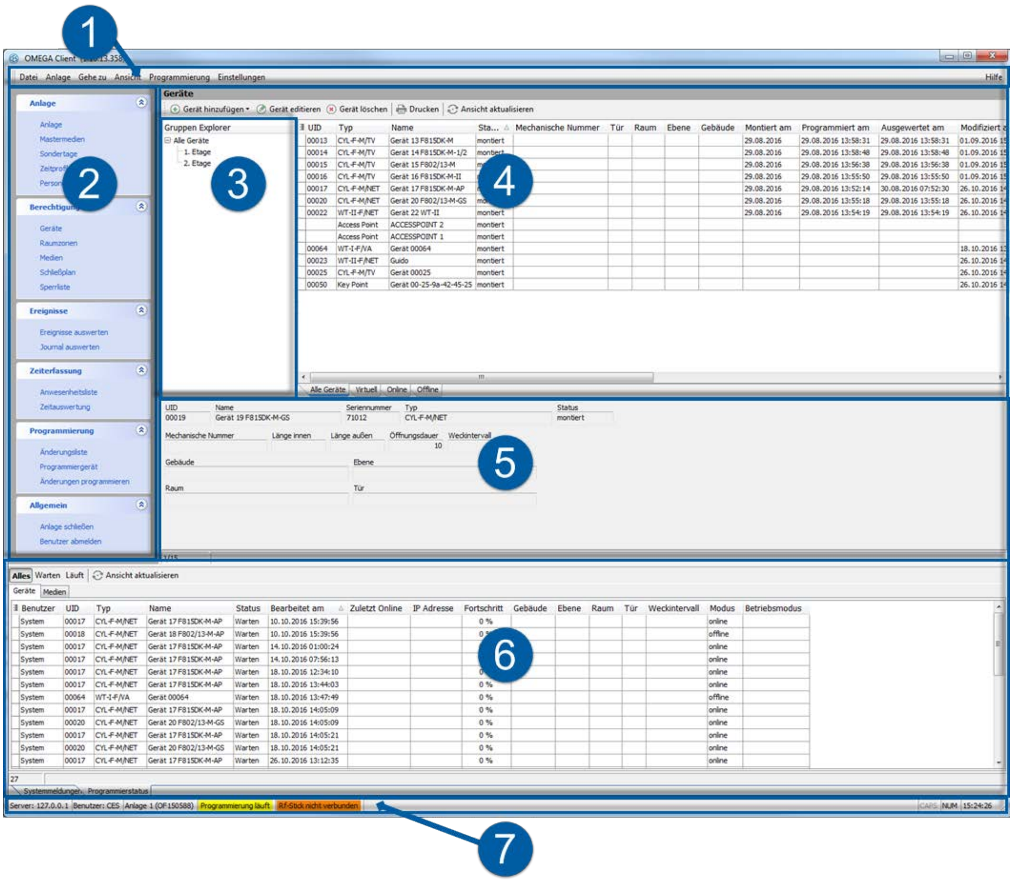
Locking devices

CS Locking devices (CS = "Classic Support")	Reading Classic and DESFire Locking media
D Locking devices (D = "DESFire")	Reading only DESFire Locking media

Operating mode compatibility of ID techniques in MIFARE systems

				MIFARE Locking media			
				LINE		V NET	
				Classic	DESFire	Classic	DESFire
MIFARE- Locking devices	LINE	/N /T /NET	CS	✓	✓	✓	✓
			D		✓		✓
	V NET	/TV /VA	CS			✓	✓
			D				✓

3 User interface of OMEGA Client



UID	Typ	Name	Sta...	Mechanische Nummer	Tür	Raum	Ebene	Gebäude	Montiert am	Programmiert am	Ausgewertet am	Modifiziert a
00013	CYL-F-M/TV	Gerät 13 F815DK-M	montiert						29.08.2016	29.08.2016 13:58:31	29.08.2016 13:58:31	01.09.2016 15
00014	CYL-F-M/TV	Gerät 14 F815DK-M-1/2	montiert						29.08.2016	29.08.2016 13:58:48	29.08.2016 13:58:48	01.09.2016 15
00015	CYL-F-M/TV	Gerät 15 F802/13-M	m[illegible]						29.08.2016	29.08.2016 13:56:38	29.08.2016 13:56:38	01.09.2016 15
00016	CYL-F-M/TV	Gerät 16 F815DK-M-II	[illegible]						29.08.2016	29.08.2016 13:55:50	29.08.2016 13:55:50	01.09.2016 15
00017	CYL-F-M/NET	Gerät 17 F815DK-M-AP	[illegible]						29.08.2016	29.08.2016 13:52:14	30.08.2016 07:52:30	26.10.2016 14
00020	CYL-F-M/NET	Gerät 20 F802/13-M-GS	mo[illegible]						29.08.2016	29.08.2016 13:55:18	29.08.2016 13:55:18	26.10.2016 14
00022	WT-II-F/NET	Gerät 22 WT-II	montiert						29.08.2016	29.08.2016 13:54:19	29.08.2016 13:54:19	26.10.2016 14
	Access Point	ACCESSPOINT 2	montiert									
	Access Point	ACCESSPOINT 1	montiert									
00064	WT-I-F/VA	Gerät 00064	montiert									18.10.2016 13
00023	WT-II-F/NET	Guido	montiert									26.10.2016 14
00025	CYL-F-M/TV	Gerät 00025	montiert									26.10.2016 14
00050	Key Point	Gerät 00-25-9a-42-45-25	montiert									26.10.2016 14

UID	Name	Seriennummer	Typ	Status
00019	Gerät 19 F815DK-M-GS	71012	CYL-F-M/NET	montiert

Mechanische Nummer	Länge innen	Länge außen	Öffnungsdauer	Weckintervall
			10	

Gebäude

Ebene

Raum

Tür

Benutzer	UID	Typ	Name	Status	Bearbeitet am	Zuletzt Online	IP Adresse	Fortschritt	Gebäude	Ebene	Raum	Tür	Weckintervall	Modus	Betriebsmodus
System	00017	CYL-F-M/NET	Gerät 17 F815DK-M-AP	Warten	10.10.2016 15:39:56			0 %						online	
System	00018	CYL-F-M/NET	Gerät 18 F802/13-M-AP	Warten	10.10.2016 15:39:56			0 [illegible]						offline	
System	00017	CYL-F-M/NET	Gerät 17 F815DK-M-AP	Warten	14.10.2016 01:00:24			[illegible]						online	
System	00017	CYL-F-M/NET	Gerät 17 F815DK-M-AP	Warten	14.10.2016 07:56:13			[illegible]						online	
System	00017	CYL-F-M/NET	Gerät 17 F815DK-M-AP	Warten	18.10.2016 12:34:10			0 [illegible]						online	
System	00017	CYL-F-M/NET	Gerät 17 F815DK-M-AP	Warten	18.10.2016 13:44:03			0 %						online	
System	00064	WT-I-F/VA	Gerät 00064	Warten	18.10.2016 13:47:49			0 %						offline	
System	00017	CYL-F-M/NET	Gerät 17 F815DK-M-AP	Warten	18.10.2016 14:05:09			0 %						online	
System	00020	CYL-F-M/NET	Gerät 20 F802/13-M-GS	Warten	18.10.2016 14:05:09			0 %						online	
System	00017	CYL-F-M/NET	Gerät 17 F815DK-M-AP	Warten	18.10.2016 14:05:21			0 %						online	
System	00020	CYL-F-M/NET	Gerät 20 F802/13-M-GS	Warten	18.10.2016 14:05:21			0 %						online	
System	00017	CYL-F-M/NET	Gerät 17 F815DK-M-AP	Warten	26.10.2016 13:12:35			0 %						online	

Server: 127.0.0.1 | Benutzer: CES | Anlage 1 (OF150588) | Programmierung läuft | Rf-Stick nicht verbunden

1 Main menu

The main menu contains all menu items of the navigation menu plus additional menu items to change the view settings, to view options, services, etc.

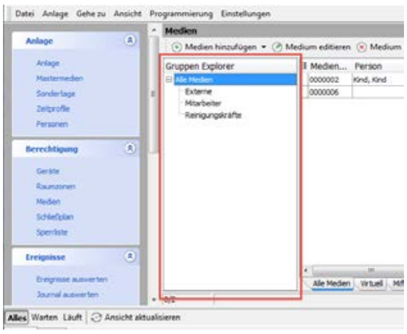
2 Navigation menu

Here you can access the views. The menu items are organised in navigation groups you can open and close with the ⌃ button.

3 Group explorer

The **group explorer** shows the GROUPS which have been created for the respective view. The group explorer is only shown in the views PEOPLE, DEVICES , and LOCKING MEDIA .

If you cannot find the component you are looking for in the view, please check whether you have selected a group in the group explorer to which this component does not belong. In the upper part of the group explorer, click on ALL PEOPLE/DEVICES/LOCKING MEDIA to view all components without being limited to one group.



Medien...	Person
0000002	Kind, Kind
0000006	

4 View

The various views show information, e.g. the number of locking media which exist within the system. Views have their own menu which contains the menu items which are necessary for this work area (e.g. add locking medium).

5 Details view

In some work areas, the **details view** can be shown additionally. It can either show the **preview** or the **reference list** of a component:

- The preview contains information about the selected component, e.g. name, type, serial number etc. of a locking device.
- The reference list shows links, e.g. which locking media are authorised for a locking device.

In some work areas, the details view contains special information (e.g. work area BLOCKING LIST, there the details view shows upcoming programming jobs).

6 Information view

The display of the information view depends on the tabs (in the lower part of the information view) you have selected:

- System messages
- Programming status
- Events

You can show or hide the tabs display via MAIN MENU > VIEW.

System messages tab

The system messages tab shows the list of the current system messages. You can limit the view to the various categories using the Information, Warnings and Errors buttons (in the upper part of the information view).

Programming status tab

The **Programming job log** is shown in the information view in the tab Programming status . With the buttons Wait and In progress you can filter the programming job log according to pending and current programming jobs.

The devices tab

Each line shows a programming job. The programming jobs for each device are processed in chronological order in the order of their creation.

ℹ The column Prog. mode shows you whether programming jobs are automatically transmitted via the wireless online network (Onlineprogramming mode), or whether they have to be transmitted manually via RF-Stick (Offlineprogramming mode).

Locking media tab

Each line shows a locking medium and can contain several programming jobs for this specific locking medium.

ℹ The Locking media tab is only shown if you use an update terminal with your system.

ℹ The list only contains programming jobs which have been transferred by update terminals. You can find programming jobs which have been transferred via Desktop-Writer in the change log.

Events tab

The events tab shows the list of the current events.

7 Status view

The status view show the following information:

- IP address of the OMEGA Server which is connected to the OMEGA Client
- User name of the user logged-in user
- Name of the system which is currently opened
- Programming status (e.g. programming required, programming in progress, etc.)
- RF-Stick status (connected or not connected)

4 Logging in to OMEGA Client

4.1 Logging in to OMEGA Client for the first time

Special features when logging in to OMEGA Client for the first time

- You have to enter the OMEGA Server IP address
- As you do not have a user account yet, you have to log in with the standard administrator account

ℹ For safety reasons, you have to change the password of the standard administrator account after you log on for the first time.

4.1.1 Enter the OMEGA Server IP address

1. Open OMEGA Client.

2. If the login window is shown, click on ABORT**.**

3. In the navigation menu, click on START > SERVER CONFIGURATION**.**

4. Enter the IP address of the OMEGA Server.

5. Click on OK**.**

The connection will be tested. After the connection has been tested successfully, you will see the login window.

Now, you are successfully connected to the selected server.

4.1.2 About the standard administrator account

The standard administrator account in each CEStronics Suite is:

Username: CES

Password: ces

This administrator has unrestricted rights and can create users and user accounts with limited functions.

ℹ For safety reasons, you have to change the password of the standard administrator account after you log on for the first time.

4.2 Login window

Show or hide server list

With the

<< button, you can show or hide the list of the saved server IPs in the login window. If you are using various servers, you can quickly and easily select the desired server for login.

Show connection to the directory service

🟩 Green	Connection to the directory service established
🟥 Red	Connection to the directory service interrupted
Hidden view	Directory service function not used

Information about the authorisation with directory service

Security settings of the login window

To change the security settings of the login window, you have to be logged into OMEGA Client.

You can define what kind of information is shown in the login window.

1. In the main menu, click on SETTINGS > OPTIONS**.**

The window "Options" opens.

2. In the SECURITY **menu item, click on** LOGIN**.**

3. Activate or deactivate the checkbox next to the corresponding setpoint:

- Set whether the username is to be filled in automatically, and whether the drop-down menu is to be shown with the user list
- Set whether the user profile of this user is to be shown after his or her user name has been entered
- Set whether the last login of the user is to be shown after his or her user name has been entered

The corresponding information is now shown, or it is no longer shown.

5 Systems

5.1 About systems

A locking system (in short: **system**) is comprised of all components which are required to control access, e.g. locking devices, locking media, and administration devices. Each system has a unique **system identification code**. Only devices with the same system identification code can communicate with each other.

5.2 Adding a system automatically

5.2.1 Adding a system automatically during installation

If you install CEStronics Suite by means of the CD or USB stick which have been included in the delivery, your system (licence file and locking system file) will be imported automatically during installation.

5.2.2 Adding a system automatically after installation

ℹ When OMEGA Client has already been installed (e.g. on netbooks delivered by CES) but OMEGA Client does not contain a system yet, you can automatically import the system with the USB stick which has been included in the delivery. If a system has already been installed, you have to import the system manually.

1. **Start the OMEGA Client and log in with your user name and password.**
2. **Insert the USB stick delivered to you, which contains the licence file and the locking system file, into a free USB port.**
   As soon as your PC has detected the USB stick, the system will be imported automatically.

5.3 Adding a system manually

Adding a system manually is comprised of two steps:

1. How to import the licence file

2. How to import the locking system file

About licence files

The **licence** you have purchased for CEStronics Suite determines inter alia:

- the number of the devices which can be operated in the system
- the number of OMEGA Clients which can be operated in the system
- whether the system can be operated online
- which system family the system belongs to

The **licence file** contains the licences of the CEStronics Suite purchased by you. There are two types of licence files:

the A licence

- contains the system family and basic features of the system
- cannot be imported subsequently

the B licence

- contains licence extensions, e.g. if you want to convert your offline system into an online system
- can be imported subsequently

Both licence files have the file extension .lic. They can be differentiated by their file name which either starts with A or B.

Please note the following exception for OMEGA LEGIC systems: the licence file for OMEGA LEGIC systems are **always** B licences. For this reason, licences are used to add new systems and to extend extending existing ones for OMEGA LEGIC.

About locking system files

With the Locking system file, you can conveniently import all the components of a system into the OMEGA Client without having to input data manually. One Locking system file contains

- Locking devices
- Locking media
- Access points

- Key points
- Master media

of the system.

The Locking system file is is delivered with every system and has the .dat format. If new devices are added to the system, you will receive a new Locking system file which includes the new devices.

It is also possible to import locking plans and device setting via Locking system files. For such extended Locking system files, please contact the CEStronics service department.

5.4 How to import the licence file

For imports or in order to edit the system, the system has to be closed.

How to close the system, and open the system administration

3. Open CEStronics Suite

4. and log in. If you have not created a user yet, log in with the standard administrator account (user name “CES”, password “ces”).

For safety reasons, you have to change the password of the standard administrator account after you log on for the first time.

a) If you do not own a system yet:

5. In the navigation menu, click on START > SYSTEM ADMINISTRATION**.**

The system administration opens.

b) If you already own a system (it will be opened automatically after log-in):

5. In the main menu, click on START > CLOSE SYSTEM**, and then click in the navigation menu on** START > SYSTEM ADMINISTRATION**.**

The system administration opens.

c) If you own several systems (the window “System” opens after log-in):

5. Click on OPEN SYSTEM **and** SYSTEM ADMINISTRATION **in the window.**

The system administration opens.

d) If you own several systems, and one system is already open:

5. **In the main menu, click on** START > CLOSE SYSTEM **, and then click in the navigation menu on** START > SYSTEM ADMINISTRATION**.**

   The system administration opens.

How to import the licence file

ℹ If you want to edit your system, you have to import an **A licence**. To extend an existing system, you have to import a **B licence** into OMEGA Client. Exception: OMEGA LEGIC systems only have B licences, and therefore they are added and extended with B licences.

How to import a licence file for a new system

1. **In** SYSTEM ADMINISTRATION **, click on** ADD SYSTEM**.**

   The system editor opens.

2. **In the tab** SYSTEM FILES **, enter the name for a new system.**
3. **Open the tab** LICENCE**.**
4. **Click on** ADD**.**
5. **Select the licence file, and click on** OPEN**.**
6. **Click on** SAVE**.**

   You are referred back to “System administration”.

   Now the system has been created, but does not yet contain any devices, locking media, etc. You can add the system components with the locking system file.

How to import a licence file for a new system

1. **In** SYSTEM ADMINISTRATION **, select the desired system, and click on** EDIT SYSTEM**.**

   The SYSTEM EDITOR *opens.*

2. **Open the tab** LICENCE**.**
3. **Click on** ADD**.**

   The window IMPORT OMEGA LICENCE *opens.*

4. **Select the desired licence file, and click on** OPEN**.**
5. **Click on** OPEN**.**

   The new licence file will now be imported.

6. **Click on** SAVE**.**

   The new licence has now been saved.

5.5 How to import the locking system file

For imports or in order to edit the system, the system has to be closed.

How to close the system, and open the system administration

1. Open CEStronics Suite

2. and log in. If you have not created a user yet, log in with the standard administrator account (user name “CES”, password “ces”).

For safety reasons, you have to change the password of the standard administrator account after you log on for the first time.

a) If you do not own a system yet:

3. In the navigation menu, click on START > SYSTEM ADMINISTRATION**.**

The system administration opens.

b) If you already own a system (it will be opened automatically after log-in):

3. In the main menu, click on START > CLOSE SYSTEM**, and then click in the navigation menu on** START > SYSTEM ADMINISTRATION**.**

The system administration opens.

c) If you own several systems (the window “System” opens after log-in):

3. Click on OPEN SYSTEM **and** SYSTEM ADMINISTRATION **in the window.**

The system administration opens.

d) If you own several systems, and one system is already open:

3. In the main menu, click on START > CLOSE SYSTEM **, and then click in the navigation menu on** START > SYSTEM ADMINISTRATION**.**

The system administration opens.

How to import the locking system file

1. In “System installation”, click with the right mouse button on the desired system.

2. In the context menu, click on IMPORT DATA**.**

If the item “Import data” is greyed out, you have not imported licence for this system yet.

3. Select the locking system file from the system, and click on OPEN**.**

Now, the locking system file will be imported.

ℹ If the locking system file contains devices which already exist in OMEGA Client, you will receive a message, and you can decide whether these devices are to be overwritten with the locking system file data or not.

All new locking devices of the system have to undergo initial re-programming. The necessary programming jobs are generated automatically and are already in the programming job log.

6 Components

The following components can be added to OMEGA Client:

- Locking media
- Devices (locking device, Access-Points, Key-Points)
- People
- Master media

What is the purpose of adding locking media and devices?

To be able to manage these components, you must add them to the OMEGA Client. Subsequently, you can interlink the locking media and locking devices in the locking plan, then you can authorise locking media for locking devices. For example, you can define radio cells for Access-Points.

What is the purpose of adding people?

You can save **people** and their personal data such as name, staff ID, department, etc., to OMEGA Client. Linking people to locking media allows you to retrace what kind of locking medium has been received, and by whom. Additionally, you can define for each person individually whether time recording is to be enabled for this person or not.

What is the purpose of adding master media?

When you add master media to the OMEGA Client (see "Components" oben), then, along with the **new programming**, these are also transmitted to the locking device and are thus authorised for the locking device.

This applies to **all** master media **except the Program-Master**. Although this can be read into OMEGA Client, it is not transmitted to the locking device (see "Components" oben).

Through the transmission of the master media from OMEGA Client to the locking device, all master media which are **not** known to the software will also be deleted from the locking device. It is therefore advisable to read the master media into OMEGA Client.

⚠ When using the Program-Masters please note the following:

If you are using the OMEGA Client, you should dispense with the Program-Master, because the OMEGA Client itself acts as “Program-Master” while awarding locking authorisations. Since the locking media can only be authorised and deleted by the same Program-Master, therefore, although the Program-Masters can be read into OMEGA Client but cannot be transmitted to the locking device.

It means that:

1. The authorisations assigned by Program-Master will **not be displayed in OMEGA Client**. As a consequence, the locking plan displayed in OMEGA client

is out of sync with the actual locking authorisations.

2. Individual or dedicated deletion of authorisations assigned by the Program-Master is not possible via software; instead, to delete you have to use the **Program-Master** or reprogram the locking device.
3. A **reprogramming** of locking devices automatically results in deletion of all authorisations created by a Program-Master.

6.1 What components can be added and how?

Components	Locking system file	Desktop-Reader/ Desktop-Writer	Manually	Excel import	After adding to the OMEGA Client to be found under...
Locking media	possible	possible	possible (only for LINE)	possible	AUTHORISATIONS > LOCKING MEDIA
Master media	possible	possible	possible	possible	SYSTEM > MASTER MEDIA
Locking devices	possible	-	possible	possible	AUTHORISATION > DEVICES
Access-Point	possible	-	possible	possible	AUTHORISATION > DEVICES
People	possible	-	-	possible	SYSTEM > PEOPLE
RF-Stick	*will be automatically added during connection to the PC*				PROGRAMMING > PROGRAMMING DEVICE
Desktop-Reader	*is not shown in OMEGA Client*				
Desktop-Writer	*is not shown in OMEGA Client*				
Programming cable	*is not shown in OMEGA Client*				
Programming Adaptor	*is not shown in OMEGA Client*				
Repeater	*is not shown in OMEGA Client*				

6.2 Adding all components with the locking system file

See "How to import the locking system file" auf Seite19

6.3 How to add components by reading them in

6.3.1 How to read in a LINE locking medium

ℹ LINE locking media can be read in with Desktop-Readers and Desktop-Writers.

1. **Connect the Desktop-Reader or Desktop-Writer to your PC.**
2. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
3. **In the view, click on** LOCKING MEDIUM**and then on** ADD > LINE LOCKING MEDIUM**.**
4. **Place the locking medium onto Desktop-Reader or Desktop-Writer.**
5. **Click on the button** READ IN**.**

ℹ When the button is greyed out, no Desktop-Reader or Desktop-Writer is connected.

The locking medium is now read in. Thus, the TYPE*,* UID *and* MEMORY *fields will be filled in automatically.*

6. **(optional) You can add more data such as the locking medium type or the owner of this locking medium.**
7. **Click on** APPLY**.**

The locking medium has now been added. To add further locking media, you can now repeat these steps, or close the locking medium editor.

ℹ To read in the locking medium as a DESFire locking medium, you have to use a Desktop-**Writer** with a **firmware version 1.2.5 or higher**.

The locking medium has now been read in.

6.3.2 How to read in a V-NET locking medium

ℹ V-NET locking media can only be read in with Desktop-Writers.

1. **Close the Desktop-Writer in your PC.**
2. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
3. **In the** LOCKING MEDIUM**view, click** ADD - V-NET LOCKING MEDIUM.
4. **Place a locking medium onto Desktop-Writer.**

Option 1 - reading in via programming:

1. **In the** AUTHORISATIONS **tab, add the desired authorisations for this locking medium.**

How to assign authorisations for locking media in the locking medium editor

ℹ The locking medium editor only allows you to add authorisations for V-NET locking devices and areas. Authorisations for LINE locking devices can be added only via the locking plan.

2. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
3. **Double-click on the V-NET locking medium whose authorisations you want to edit.**
4. **Open the tab** AUTHORISATIONS**.**
5. **To add an authorisation, move the areas or locking devices with drag and drop into the** AUTHORISATIONS **view. Then, click in the** AUTHORISATIONS **view in the column** TIME PROFILE **to select the desired time profile for this area or this device.**
   Now, the authorisation has been added with the selected time profile.

It is possible to issue individual locking device authorisations for a locking medium **and** authorisations for the area to which the locking device belongs. If both authorisations use different time profiles, the following happens:

First, the locking device verifies whether it is authorised to act at this time because of its individual authorisation. If this is not the case, the locking device then checks whether it is authorised to act because of the area authorisation. If this is the case, access is granted.

> **Example:** according to the individual authorisation, the locking medium is allowed to open the locking device between 12 and 6 pm; according to the area authorisation, it can open between 11 am and 5 pm. If at 11 o'clock someone tries to open the door, the locking device first checks its individual authorisation but does not find any authorisation. Then, it checks the area authorisation and grants access.

ℹ This means the locking device always checks **both** authorisations. As soon as there is an individual or area authorisation, access can be granted.

6. **To delete an authorisation, move the areas or locking devices with drag and drop from the view** Authorisations **to the** Areas **or** Devices **view.**

   Now, the authorisation has been deleted.

   ⚠ You have to program the locking medium to make the changes come into effect (see "Programming V-NET locking media" auf Seite101).

7. **Click on** Programming **for the changes to come into effect immediately.**
8. **Click on** Save **for the changes to come into effect later.**

1. **If the alocking medium number utomatically assigned does not correspond to the number you want to assign to the locking medium, or which is printed on the locking medium, you can simply overwrite it in the** locking medium number **field before programming.**
2. **Click on** Programming**.**

   You receive a message when programming the locking medium has been successful. The Type, Memory size *and* UID *fields will be filled in automatically. Locking medium has now been read into OMEGA Client with all its authorisations.*

   Having read in the data successfully, the locking medium editor immediately moves to the next consecutive locking medium number so you can continue reading in further locking media.

3. **If you do not want to continue reading in further locking media, click on** Close**.**

   The locking medium will now be displayed in the locking media list.

Option 2 - reading in via formatting:

Formatting is a way of adding V-NET locking media to OMEGA Client without having to issue authorisations at this point.

About formatting locking media

When a locking medium is formatted, it is reset. Please note:

⚠ When formatting **MIFARE DESFire** locking media, **all** data is deleted from the locking medium. If you use your locking medium for other purposes too (e.g. for a canteen payment system), these additional functions are deleted as well!

ℹ When formatting **MIFARE Classic** locking media, only the data which was created by CEStronics Suite is deleted. Third party data (e.g. a canteen payment system) will not be deleted.

1. **If the automatically-assigned locking medium number does not correspond to the number you want to assign to the locking medium, or which is printed on the locking medium, you can simply overwrite it in the** LOCKING MEDIUM NUMBER **field before formatting.**
2. **Click on** OPTIONS > FORMATTING**.**

   You receive a message when programming the locking medium has been successful. The TYPE, MEMORY SIZE *and* UID *fields will be filled in automatically. Now, the locking medium is read into OMEGA Client without authorisations.*

   Having read in the data successfully, the locking medium editor immediately moves to the next consecutive locking medium number so you can continue reading in further locking media.
3. **If you do not want to continue reading in further locking media, click on** CLOSE**.**

   The locking medium will now be displayed in the locking media list.

6.3.3 How to read in master medium

ℹ Master media can be read in with Desktop-Readers and Desktop-Writers.

1. **Connect the Desktop-Reader or Desktop-Writer to your PC.**
2. **In the navigation menu, click on** SYSTEM > MASTER MEDIA**.**
3. **In the view, click on** MASTER MEDIUM **and then on** ADD**.**
4. **Place a master medium onto the Desktop-Reader or Desktop Writer.**
5. **Click on the button** READ IN**.**

   ℹ When the button is greyed out, no Desktop-Reader or Desktop-Writer is connected.

   The master medium is now read in. The TYPE, NAME *and* UID *fields will be filled in automatically.*
6. **(Optional) You can now change the name of the master medium, add the owner of the master medium as a person, or enter a remark.**
7. **Click on** APPLY**.**

   The master medium has now been added. To add further master media, you can now repeat these steps, or close the master medium editor.

6.4 How to add components with an Excel import

How to fill in an Excel template

CEStronics Suite contains an excellent template which helps you to import people, devices, and locking media quickly and easily. You can find this template at the install location (e.g. PROGRAMS) under OMEGA > CLIENT. Apart from the column headings, the first line contains help texts which help you fill in the template.

1. Enter the data you want to import into the Excel template, and save the file with the new name.

Now, you can use the new file to import the data.

ℹ For imports or in order to edit the system, the system has to be closed.

How to close the system, and open the system administration

1. Open CEStronics Suite

2. and log in. If you have not created a user yet, log in with the standard administrator account (user name “CES”, password “ces”).

ℹ For safety reasons, you have to change the password of the standard administrator account after you log on for the first time.

a) If you do not own a system yet:

3. In the navigation menu, click on START > SYSTEM ADMINISTRATION**.**

The system administration opens.

b) If you already own a system (it will be opened automatically after log-in):

3. In the main menu, click on START > CLOSE SYSTEM**, and then click in the navigation menu on** START > SYSTEM ADMINISTRATION**.**

The system administration opens.

c) If you own several systems (the window “System” opens after log-in):

3. Click on OPEN SYSTEM **and** SYSTEM ADMINISTRATION **in the window.**

The system administration opens.

d) If you own several systems, and one system is already open:

3. In the main menu, click on START > CLOSE SYSTEM **, and then click in the navigation menu on** START > SYSTEM ADMINISTRATION**.**

The system administration opens.

How to import data

1. To open the context menu, click with the right mouse button on the desired system.

2. In the context menu, click on IMPORT DATA**.**

The window OPEN FILE *opens.*

3. Select the desired import file, and click on OPEN**.**

ℹ If the import file is not shown, the file type view may be restricted. In such case, switch the drop-down menu from OMEGA EXPORT to ALL DATA or EXCEL FILE.

4. Click on IMPORT**.**

5. Please confirm.

After the import has been successful, you will receive a message. Now, files have been imported.

6.5 How to add devices manually

ℹ The easiest way to add components to the system is to import them via the locking system file. You can also add components manually.

6. In the navigation menu, click on AUTHORISATION > DEVICES**.**

7. In the view, click on ADD DEVICE > DESIRED DEVICE**.**

The device editor opens.

Depending on the selected device type, the following fields are required:

LINE locking device, V-NET locking device, or wall terminal

You have to fill in the UID and TYPE fields. You can fill in the remaining fields if you wish. Then, click on SAVE.

Key-Point

You have to fill in the UID, NAME and MAC ADDRESS fields. You can fill in the remaining fields if you wish. Then, click on SAVE.

Access-Point

You have to fill in the UID and MAC ADDRESS fields. You can fill in the remaining fields if you wish. Then, click on SAVE.

Online locking device

You will see an overview of the available online devices. Select the desired device, and click on ADD.

ℹ The online mode has to be activated for the locking device to be shown in the overview.

ℹ If you do **not want to define a radio cell**, you can set FLEX devices directly into the online mode and add them via this option. If you **want to define a radio cell**, leave the locking device in the offline mode (factory default setting), and add it with “LINE locking devices" because you have to define the radio cell in the offline mode. **About how to activate the online mode with or without radio cell**

The locking device has now been added.

6.6 How to add master media manually

ℹ The easiest way to add components to the system is to import them via the locking system file. You can also add components manually.

1. **In the navigation menu, click on** SYSTEM > MASTER MEDIA**.**
2. **In the view, click on** MASTER MEDIUM **and then on** ADD**.**
3. **Enter the master medium type and UID.**

ℹ You can have the master medium UID shown to you when you hold it closely to a locking device and read the events this has generated.

4. **(Optional) You can change the name of the master medium, add the owner of the master medium as a person, or enter a remark.**
5. **Click on** APPLY**.**

   The master medium has now been added. To add further master media, you can now repeat these steps, or close the master medium editor.

6.7 How to add LINE locking media manually

ℹ Only LINE locking media can be added manually to OMEGA Client.

1. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
2. **In the view, click on** ADD LOCKING MEDIUM**.**
3. **Click on** ADD LINE LOCKING MEDIUM**.**
4. **At the locking medium type and UID.**

ℹ You can have the locking medium UID shown to you when you hold it closely to a locking device and read the events this has generated.

5. **(optional) You can add more data such as the locking medium type or the owner of this locking medium.**
6. **Click on** APPLY**.**

   The locking medium has now been added. To add further locking media, you can now repeat these steps, or close the locking medium editor.

6.8 How to add people manually

1. In the navigation menu, click on PEOPLE**.**

2. Click on the HOW TO ADD PEOPLE **view.**

The PEOPLE EDITOR *opens.*

About the people editor

General tab

Salutation	ℹ The text you enter here is saved to be available as a quick selection in the future.
Picture	Here, you can add a photo of the person. In order to add a photo, click into the field with the right mouse button.
First name, family name, street, etc.	ℹ This data is for information purposes only and has no technical effect.
Time recording	Here, you can set if you want to activate time recording for this person.

Details tab

Here, you can add further details such as PERSONNEL NUMBER or DEPARTMENT . These details are for information purposes only and have no technical effect.

ℹ Data you have entered in the fields UNIT, ACTIVITY, DEPARTMENT, COST CENTRE , and ROOM , is added as entry suggestions. For example, if you have entered “Sales” in the DEPARTMENT field, you will see “sales” as an entry suggestion in a drop-down menu of this field.

3. Enter the corresponding data in the GENERAL **tab.**

a) In order to add a photo, click into the PICTURE field with the right mouse button, select UPLOAD , and select the desired picture (JPG format). You can enter pictures directly from the clipboard with INSERT .

b) In the time recording field, you can define whether time recording is to be activated for this person.

yes	Time recording will be activated for this person, which means he or she is shown on the attendance list and in time evaluation.
no	Although time recording has been activated for locking devices, time recording is not activated for this person, and he or she will not be shown on the attendance list or in time evaluation.

4. **Enter the corresponding data in the** DETAILS **tab.**
5. **If you have already created a group for people, you can add the individual persons of this group in the** GROUPS **tab.**
6. **Click on** APPLY**.**

   Now the data for this person has been changed.

7 Authorisations

7.1 The locking plan

The **locking plan** is used to set authorisations, i.e. what kind of locking devices are authorised to open which locking medium.

The number and the colour fill of a cell always correspond to the number and colour fill of the authorisations time profile.

No colour fill	□	There are no authorisations for the locking device or the area.
Number and colour fill	1	There is an authorisation for the locking device. This has already been programmed.
Red bar	1	An authorisation has been issued for the locking device. It is part of the change log and has not yet been programmed.
Blue bar	1	An authorisation has been issued for the locking device. There is already a programming job to program the change.
Colour fill with a small tile	1	Shows that the authorisation is a area authorisation (only V-NET).
Triangular in the upper right part		Shows that the V-NET office function has additionally been activated for this authorisation:
	1	V-NET office function active with an individual authorisation
	1	V-NET office function active with an area authorisation
Cross in the cell	☒	Shows that this cell has already been edited by another user and that it is blocked for editing.
Small cross in the cell	x	Shows that there is an authorisation for a locking device of the N or NV variant. Due to the fact that these locking devices do not work with time profiles, the authorisation is independent of any time profiles.

7.2 How to manage authorisations for LINE locking media

ℹ LINE locking media cannot be authorised for V-NET locking devices.

1. In the navigation menu, click on System > Locking plan**.**

2. Click with the right mouse button into the field of the locking medium and locking device you want to edit.

3.

a) To add an authorisation, in the context menu, click on Create link > desired time profile. If the locking device is of the N or NV variants, just click on Create link because it is not possible to allocate time profiles.

b) To delete an authorisation, in the context menu, click on Delete link.

The changes are now shown with the corresponding colours and symbols. A red bar in the field shows that the changes have been entered into the change log.

ℹ If you want to undo changes, click the right mouse button into the field, and in the context menu, click on Undo. This does not generate any changes in the change log, and programming is not necessary.

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

7.3 How to manage authorisations for V-NET locking media

7.3.1 About individual authorisations and areas

Individual authorisations

An **individual authorisation** is the authorisation for one individual locking device in V-NET.

Areas

Areas combine several V-NET locking devices, so that you can issue V-NET locking media authorisations for all devices of this area quickly and easily. Areas are available for V-NET only. One locking device can belong to **one** area only.

7.3.2 How to manage authorisations with the locking plan

1. In the navigation menu, click on SYSTEM > LOCKING PLAN**.**

2. Click with the right mouse button into the field of the locking medium and locking device or area you want to edit.

3.

c) To add an authorisation, in the context menu, click on CREATE LINK > DESIRED TIME PROFILE. If the locking device is of the NV variant, just click on CREATE LINK because it is not possible to allocate time profiles.

d) To delete an authorisation, in the context menu, click on DELETE LINK.

The changes are now shown with the corresponding colours and symbols. A red bar in the field shows that the changes have been entered into the change log.

ℹ If you want to undo changes, click the right mouse button into the field, and in the context menu, click on UNDO. This does not generate any changes in the change log, and programming is not necessary.

If you have changed an authorisation for a V-NET locking device:

⚠ You have to program the locking medium to make the changes come into effect (see "Programming V-NET locking media" auf Seite101).

If you have changed an authorisation for a LINE locking device:

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

ℹ If you have changed authorisations for LINE locking devices only, it is not necessary to program the locking medium.

Information on how to assign individual authorisations and area authorisastions:
It is possible to issue individual locking device authorisations for a locking medium **and** authorisations for the area to which the locking device belongs. If both authorisations use different time profiles, the following happens:

First, the locking device verifies whether it is authorised to act at this time because of its individual authorisation. If this is not the case, the locking device then checks whether it is authorised to act because of the area authorisation. If this is the case, access is granted.

Example: according to the individual authorisation, the locking medium is allowed to open the locking device between 12 and 6 pm; according to the area authorisation, it can open between 11 am and 5 pm. If at 11 o'clock someone tries to open the door, the locking device first checks its individual authorisation but does not find any authorisation. Then, it checks the area authorisation and grants access.

ℹ This means the locking device always checks **both** authorisations. As soon as there is an individual or area authorisation, access can be granted.

7.3.3 How to manage authorisations with the V-NET locking medium editor

ℹ The locking medium editor only allows you to add authorisations for V-NET locking devices and areas. Authorisations for LINE locking devices can be added only via the locking plan.

1. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
2. **Double-click on the V-NET locking medium whose authorisations you want to edit.**
3. **Open the tab** AUTHORISATIONS**.**
4. **To add an authorisation, move the areas or locking devices with drag and drop into the** AUTHORISATIONS **view. Then, click in the** AUTHORISATIONS **view in the column** TIME PROFILE **to select the desired time profile for this area or this device.**
   Now, the authorisation has been added with the selected time profile.

   It is possible to issue individual locking device authorisations for a locking medium **and** authorisations for the area to which the locking device belongs. If both authorisations use different time profiles, the following happens:

   First, the locking device verifies whether it is authorised to act at this time because of its individual authorisation. If this is not the case, the locking device then checks whether it is authorised to act because of the area authorisation. If this is the case, access is granted.

Example: according to the individual authorisation, the locking medium is allowed to open the locking device between 12 and 6 pm; according to the area authorisation, it can open between 11 am and 5 pm. If at 11 o'clock someone tries to open the door, the locking device first checks its individual authorisation but does not find any authorisation. Then, it checks the area authorisation and grants access.

ℹ This means the locking device always checks **both** authorisations. As soon as there is an individual or area authorisation, access can be granted.

5. **To delete an authorisation, move the areas or locking devices with drag and drop from the view** AUTHORISATIONS **to the** AREAS **or** DEVICES **view.**
   Now, the authorisation has been deleted.

⚠ You have to program the locking medium to make the changes come into effect (see "Programming V-NET locking media" auf Seite101).

6. **Click on** PROGRAMMING **for the changes to come into effect immediately.**
7. **Click on** SAVE **for the changes to come into effect later.**

8 Functions of your CES OMEGA FLEX system

8.1 Controlling access times with time profiles

8.1.1 About time profiles

There are three types of time profiles:

1. **Release times** (up to three time slots for every weekday and a special day within which the locking device is released, i.e. the door is always open)
2. **block times** (up to three time slots for every weekday and a special day within which the locking device is blocked, i.e. the door cannot be opened)
3. Up to 29 **individual time profiles** (for each time profile up to three time slots per weekday and an additional special day; the locking media is authorised to open the locking device only at times set there)

Individual time profiles (in short: **time profiles**) control the times at which the authorisations issued are valid. Therefore, these time profiles are required to issue authorisations. A time profile has to be assigned to each authorisation.

8.1.1.1 Special days

The various time profiles allow you to define for each weekday at what time

- blocking times are activated (block time profile)
- release times are activated (release time profile)
- authorisations of locking media are valid (individual time profiles)

Special days allow you to define additional days with blocking times, release times, or authorisation times which differ from those of the remaining weekdays.

Example: Certain locking devices are to be set into block mode on public holidays. For that purpose, you save the dates of the public holidays as special days. You can define in the block time profile of the respective locking devices that from 00:00 until 11:59 the block time profile is to be active on special days. This means that for the respective locking devices the block time profile is active on public holidays.

ℹ A maximum number of one hundred special days can be saved.

ℹ As soon as a special day has expired, it is automatically deleted.

ℹ If today is a special day, this will be shown with an information symbol in the navigation menu next to SPECIAL DAYS .

8.1.2 How to create a time profile for authorisations

You have two options:

a) You can use an existing time profile as a template for the new time profile

b) You can create a new time profile without a template

a) How to use an existing time profile as a template for a new time profile

1. In the navigation menu, click on SYSTEM > TIME PROFILES**.**

2. Double-click on the time profile you want to edit.

The TIME PROFILE EDITOR *opens.*

3. Fill in the weekday-time window matrix for this time profile:

- Each line represents a work day (MON, TUE, WED, etc.). There is an additional row for special days (SD). This line applies to every date which has been defined as a **special day**.
- The columns represent the time windows (three time windows, indicating start and end of the respective time window) during which the authorisations of the locking media are to be valid.

Example: The authorisations are to be valid on each workday from 8 am to 5 pm. Therefore, in WINDOW 1 you enter for every workday “8 am” into START and “5 pm” into END .
However, on Mondays and Wednesdays the authorisations are to be valid additionally between 6 pm and 9 pm. Therefore, in WINDOW 2 you enter for Mondays and Wednesdays “6 pm” into START and “9 pm” into END .

ℹ If 00:00 is entered as end time in a time window, this time window is not counted, i.e. during this time the authorisations are not valid.

ℹ If authorisations are to be valid until 12 pm of one day, enter “23:59” as the end time.

ℹ If you want authorisations to be valid for longer than one day, enter the following:

Example: the authorisation is to be valid from 6 pm on Monday until 12 am on Tuesday:
MON 18:00 - 23:59
TUE 00:00 - 12:00

4. Click on SAVE > SAVE UNDER**.**

5. In the NO. **field, select the number of the time profile.**

⚠ Once the number of the time profile has been saved, it can no longer be changed.

6. In the Name **field, enter the name of the time profile.**

7. In the colour **field, select a colour for the time profile.**

ℹ Due to the colours, you can easily distinguish the time profiles in the locking plan.

8. Click on OK**.**

The new time profile has now been saved.

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

ℹ After a time profile has been changed, **all** locking devices must be programmed (with the exception of /N and /NV devices). If your system contains a high number of locking devices, programming may require some time.

b) How to create a new time profile without a template

1. In the navigation menu, click on System > Time profiles**.**

2. In the view, click on New time profile**.**

The Time profile editor *opens.*

3. In the No. **field, select the number of the time profile.**

⚠ Once the number of the time profile has been saved, it can no longer be changed.

4. In the Name **field, enter the name of the time profile.**

5. In the colour **field, select a colour for the time profile.**

ℹ Due to the colours, you can easily distinguish the time profiles in the locking plan.

6. Fill in the weekday-time window matrix:

- Each line represents a work day (MON, TUE, WED, etc.). There is an additional row for special days (SD). This line applies to every date which has been defined as a **special day**.
- The columns represent the time windows (three time windows, indicating start and end of the respective time window) during which the authorisations of the locking media are to be valid.

Example: The authorisations are to be valid on each workday from 8 am to 5 pm. Therefore, in WINDOW 1 you enter for every workday “8 am” into START and “5 pm” into END .
However, on Mondays and Wednesdays the authorisations are to be valid additionally between 6 pm and 9 pm. Therefore, in WINDOW 2 you enter for Mondays and Wednesdays “6 pm” into START and “9 pm” into END .

If 00:00 is entered as end time in a time window, this time window is not counted, i.e. during this time the authorisations are not valid.

If authorisations are to be valid until 12 pm of one day, enter “23:59” as the end time.

If you want authorisations to be valid for longer than one day, enter the following:

Example: the authorisation is to be valid from 6 pm on Monday until 12 am on Tuesday:
MON 18:00 - 23:59
TUE 00:00 - 12:00

7. (optional) Enter a remark about this time profile in the REMARK field.

8. Click on SAVE.

The new time profile has now been saved.

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

After a time profile has been changed, **all** locking devices must be programmed (with the exception of /N and /NV devices). If your system contains a high number of locking devices, programming may require some time.

8.1.3 How to set a release time profile for a locking device

1. In the navigation menu, click on AUTHORISATION > DEVICES**.**

2. Double-click on the desired locking device.

The DEVICE EDITOR *opens.*

3. Open the RELEASE TIME PROFILE **tab.**

4. Fill in the weekday-time window matrix:

- Each line represents a work day (MON, TUE, WED, etc.). There is an additional row for special days (SD). This line applies to every date which has been defined as a **special day**.

- The columns represent the time windows (start and end time) during which the release time of the locking device is to be valid.

ℹ If 00:00 is entered as the end time in a time window, this time window is not counted, i.e. during this time the release time is not active.

ℹ If the release time is to be active until midnight of one day, enter “23:59” as the end time.

ℹ If you want the release time to be active for longer than one day, enter the following:

Example: the release time is to be valid from 6 pm on Monday until 12 pm on Tuesday:

MON 18:00 - 23:59

TUE 00:00 - 12:00

5. Click on SAVE**.**

The release time profile for this locking device has now been saved.

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

8.1.4 How to set a block time profile for a locking device

1. In the navigation menu, click on AUTHORISATION > DEVICES**.**

2. Double-click on the desired locking device, or highlight it in the list, and click on the EDIT DEVICE **view.**

The DEVICE EDITOR *opens.*

3. Open the BLOCK TIME PROFILE **tab.**

4. Fill in the weekday-time window matrix:

- Each line represents a work day (MON, TUE, WED, etc.). There is an additional row for special days (SD). This line applies to every date which has been defined as a **special day**.
- The columns represent the time windows (start and end time) during which the blocking time of the locking device is to be valid.

ℹ If 00:00 is entered as the end time in a time window, this time window is not counted, i.e. during this time the blocking time is not valid.

ℹ If the blocking time is to be active until midnight of one day, enter "23:59" as the end time.

ℹ If you want the blocking time to be valid for longer than one day, enter the following:

Example: the blocking time is to be valid from 6 pm on Monday until 12 pm on Tuesday:

MON 18:00 - 23:59

TUE 00:00 - 12:00

5. Click on SAVE**.**

The block time profile for this locking device has now been saved.

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

8.2 How to control access times with the office function

8.2.1 About the office function

The office function in locking media can put locking devices **into** office mode. In the office mode, locking devices are released for a certain period of time, i.e.during this time, the door can be opened even without the locking media. After expiry of the time period, the locking device reverts back to normal mode automatically. In V-NET, the office mode is not limited by time, i.e. a locking device remains coupled until the office mode is deactivated by the locking media again.

To be able to use the office function, both locking device and locking medium must be set up for the office function in OMEGA Client. Therefore, the OMEGA Client specifies

- which locking devices shall have the office function (only for LINE locking devices)
- which locking media are authorised to trigger the offline mode
- in which time period these locking media can use the office function, for example, Monday to Friday from 8am to 5 pm.

8.2.2 How to set up the office function for LINE locking devices

1. **In the navigation menu, click on** Authorisation > Devices**.**
2. **Double-click on the desired locking device, or highlight it in the list, and click on the** Edit device **view.**

   The device editor *opens.*

3. **Open the** office function **tab.**

The Office function tab is only displayed if the **office function has been released for the locking device**.

4. **Click on** Add**.**
5. **In the** Medium number **column, select the number of the locking medium for which you want to set up the office function.**

Only the locking media which are **authorised for this locking device** are shown.

If you select All , the office function will be set up for all locking media which are authorised for this locking device.

If a locking medium exists in several times (it appears in several lines) for the office function, then it is able to activate the office function at all of the times indicated:

Example: you have defined two times for the office function:

#	Defined time		Locking medium number
#1	Monday - Wednesday	12 pm to 6 pm	all
#2	Monday and Tuesday	4 pm to 8 pm	0000004

Locking medium 0000004 can activate the office function at both times, at time #1 as well as at time #2. This means:

on Mondays	between 12 pm and 8 pm *(#1: from 12 pm to 6 pm, extended to 8 pm by #2)*
on Tuesdays	between 12 pm and 8 pm *(#1: from 12 pm to 6 pm, extended to 8 pm by #2)*
on Wednesdays	between 12 pm and 6 pm *(by #1)*

6. Enter the start and end time of the office function, and activate the checkboxes of the days on which the office function is to be available.

ℹ To set the office function for two days, you have to enter the start and end time (e.g. from 6 pm to 12 pm), and activate the checkboxes for both days.

ℹ Only four LINE locking devices time settings are possible. Time settings are not available for V-NET locking devices.

The **start time** of the office function determines the time when a locking medium can activate the office function. The **end time** determines the time the office function is terminated automatically, i.e. the locking device is disengaged automatically, and access is no longer possible without a locking medium. The start and end time can be set individually for each locking medium. The locking devices are able to detect which locking medium was used to set the office function, and they work according to the times set with the respective locking medium.

Example: Mr Smith's locking medium can activate the office function from 8 am to 5 pm. Mr Jones' locking medium can activate the office function from 8 am to 6 pm. Mr Smith activated the office function in the morning, therefore the locking device is automatically disengaged at 5 pm. If Mr Jones now reactivates the office function, the locking device will be disengaged again at 6 pm.

The office function can be set for several days too, e.g. from Monday 6 pm until Tuesday 12 pm.

ℹ Since there are no start and end-times for the Office function in the V-NET, there is no end-time at which the locking device automatically reconnects. Therefore, the office mode in V-NET must be deactivated with an authorised locking media.

7. Click on Save**.**

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

The office function is now available for the locking medium for the times set.

8.2.3 How to set up the office function for V-NET locking devices

The office function of V-NET locking devices is only available with V-NET locking media.

Option 1: set up using the locking plan

1. **In the navigation menu, click on** SYSTEM > LOCKING PLAN**.**
2. **Click with the right mouse button into the field of the locking medium and locking device or area you want to edit.**
3. **In the context menu, click on** OFFICE FUNCTION > ON **to activate the office function.**

   Now the activated office function is shown by a triangular in the upper right corner of the field. The red bar in the field shows that the changes have been entered into the change log.

   If you want to undo changes, click the right mouse button into the field, and in the context menu, click on UNDO. This does not generate any changes in the change log, and programming is not necessary.

   It is not possible in V-NET to enter **Time settings** for the office function

   ⚠ You have to program the locking medium to make the changes come into effect (see "Programming V-NET locking media" auf Seite101).

4. **In the context menu, click on** OFFICE FUNCTION > OFF **to deactivate the office function.**

   The triangle which indicated the activated office function, will be deleted from the field. The red bar in the field shows that the changes have been entered into the change log.

   If you want to undo changes, click the right mouse button into the field, and in the context menu, click on UNDO. This does not generate any changes in the change log, and programming is not necessary.

   ⚠ You have to program the locking medium to make the changes come into effect (see "Programming V-NET locking media" auf Seite101).

Option 2: set up with the locking medium editor

1. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
2. **Double-click on the V-NET locking medium for which you want to set up the office function.**
3. **Open the tab** AUTHORISATIONS**.**
4. **In the** AUTHORISATIONS **view, activate or deactivate the** OFFICE FUNCTION **checkbox for the desired locking device.**

   The office function for this locking device has now been activated or deactivated.

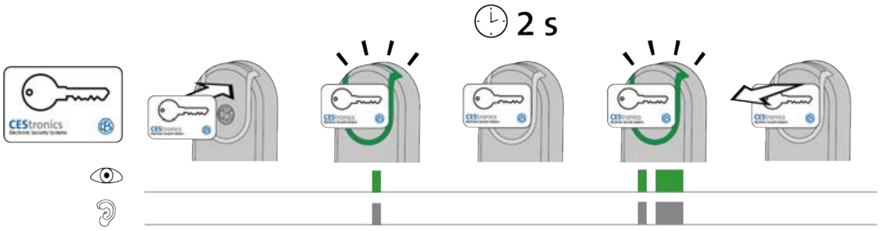
⚠ You have to program the locking medium to make the changes come into effect (see "Programming V-NET locking media" auf Seite101).

8.2.4 How to activate the office mode for a locking device

Required devices and locking media:

- Locking medium which is authorised for the office function
- Locking device which is authorised for the office function

How to proceed:



1. **Hold the locking medium which is authorised for the office function in the reading field of the locking device for approx. 2 seconds.**

   As soon as the locking medium is in the reading field, the following signal appears:

   1x short green and 1x short beep

   After approx. 2 second, another signal appears:

   1x short green and 1x short beep, 1x long green and 1x long beep

   The office mode is now active. The door can now be opened without locking media until the end of the office hours has been reached. LINE locking devices automatically disengage at the end time set in OMEGA Client.

⚠ In V-NET, there is no end time at which the locking device automatically disengages. Therefore, the office mode in V-NET locking devices must be deactivated with an authorised locking medium.

Troubleshooting:

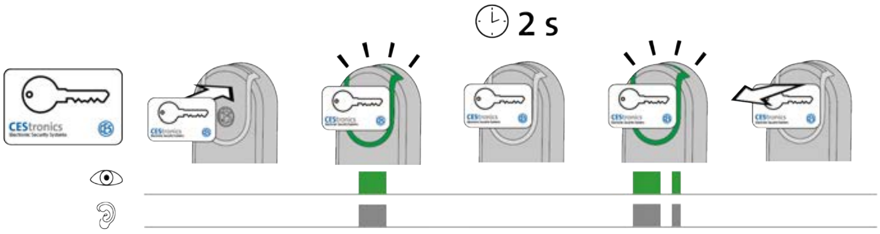
Problem/Signalling	Reason	Solution
No signal after approx. 2 seconds. The office mode is not active. The coupling of the locking device engages, but disengages again after expiry of the opening period.	The locking device is not authorised for the office function.	Have the locking device authorised for the office function by the system administrator.
	The office function is not available at this time.	Ask the system administrator for this system when the office function in this locking device can be activated.
	The locking medium is not authorised for the office function.	Have the locking medium authorised for the office function by the system administrator.

8.2.5 How to deactivate the office mode for a locking device

Required devices and locking media:

- Locking media, which is authorised for the office function
- Locking device, which is authorised for the office function

Procedure:



1. **Hold the locking media authorised for the office function for ca 2 seconds in the reading field of the locking device.**

   As soon as the locking media is in the reading field, the following signal appears:

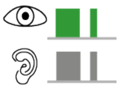
   1x long green and 1x long beep

   After ca 2 second, another signal appears:

   1x long green and 1x long beep, 1x short green and 1x short beep

   The office mode is now deactivated. The door can be opened now only with authorised locking media.

Troubleshooting:

Signalling	Reason	Solution
Is not displayed after 2  seconds.	The office mode cannot be deactivated because the locking media is not authorised for the office function.	Have your locking media authorised for the office function by the system administrator.

8.3 Validity

8.3.1 About validity

With the **validity,** you can specify a time period within which the locking medium can be used.

Example: you want to issue a locking medium to a new employee before the commencement of his or her work, however, the locking medium should only be usable from his or her first working day.

In addition, the end date of the validity ensures that from a chosen time onwards, no access can be made.

Locking media must be valid so that they can

- open locking devices
- be validated

The validity is specified in OMEGA Client. Validity can be assigned to both the V-NET and the LINE locking media. However, specifying the validity of locking media is not mandatory.

In V-NET, the validity data can be transmitted through a Desktop-Writer, Key-Point, or an Update-Terminal to a locking medium. After the validity has expired, a locking medium must be reprogrammed so that it can be used again.

In LINE, validity can only be used for online systems. Once the validity has expired, programming jobs are automatically created and transmitted for the online locking devices which are in the “online” programming mode.

8.3.2 How to set up validity for LINE

In a LINE system, locking devices do not check locking media for validity. Instead, programming jobs which add or delete locking media authorisations in accordance with their validity, are automatically generated. Therefore, validity can be used only in a wireless online network.

1. Set the locking medium validity.

How to set the validity for LINE locking media

1. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
2. **Highlight one or more locking media in the list (use SHIFT and CTRL to highlight more than one locking media), and click with the right mouse button to open the context menu.**
3. **In the context menu, click on** CHANGE VALIDITY**.**
4. **If the locking medium is to be used from a future date onwards, then enter this date in the** VALID AS OF **field.**
5. **If the locking medium is to be used until a certain date, then enter this date in the** VALID UNTIL **field.**
6. **Click on** OK**.**

   The validity for the locking medium or locking media has now been changed.

In the same way, you can set the validity of a locking medium in the LOCKING PLAN view.

2. As soon as a locking medium becomes valid, or its validity expires, programming jobs for online locking devices are generated and transferred.

Programming jobs are generated and transferred only for online locking devices which are in the ONLINE programming mode.

How to define the programming mode and operating mode of a locking device

The programming mode can only be activated for devices of the NET and VA variants.

1. **In the navigation menu, click on** AUTHORISATION > DEVICES**.**
2. **Double-click on the locking device you want to edit.**

   The device editor opens.

3. In the PROGR. MODE **field, select the programming mode for the locking device.**

4. If you have selected the ONLINE **programming mode: open the** PARAMETERS **tab, and select the operating mode and the wake-up interval.**

5. Click on SAVE**.**

The programming mode has now been saved. If you have only changed the programming mode, it is not necessary to program the locking device.

If you have changed the operating mode or the wake-up interval:

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

8.3.3 How to set up validity for V-NET

1. **Set the locking medium validity.**

How to set the validity of a V-NET locking medium

1. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA.
2. **Highlight one or more locking media in the list (use SHIFT and CTRL to highlight more than one locking media), and click with the right mouse button to open the context menu.**
3. **In the context menu, click on** CHANGE VALIDITY.
4. **If the locking medium is to be used from a future date onwards, then enter this date in the** VALID AS OF **field.**
5. **If the locking medium is to be used until a certain date, then enter this date in the** VALID UNTIL **field.**
6. **Click on** OK.

⚠ You have to program the locking medium to make the changes come into effect (see "Programming V-NET locking media" auf Seite101).

The validity for the locking medium or locking media will be changed after programming.

ℹ In the same way, you can set the validity of a locking medium in the LOCKING PLAN view.

2. **After a locking medium has been programmed, it can only be used with V-NET locking devices within the validity set.**

ℹ If validity has lapsed, but you want to reuse the locking medium, you have to define the validity in the locking medium editor and have to re-program it. You can do this using Desktop-Writer or a Key-Point.

⚠ If the locking medium has authorisations for LINE locking devices too, these need to be programmed at the start and end of the validity. In a wireless online network, the programming jobs are generated and transferred automatically.

8.4 Validation (only V-NET)

8.4.1 About validation

The **validation** is a backup function in the V-NET. It specifies an **expiry date** for the locking media. From this date onwards, the locking media cannot be used anymore.

Through the validation devices (Wall terminals, Key-Points and Update-Terminals) the expiry date can be extended. How frequently the expiry date must be extended is determined by you in that you specify the **validation interval** in the OMEGA Client.

Company employees must validate their locking media every day at a Wall terminal at the company entrance, so that their locking media are usable.

Wall terminals and Update-Terminals are connected to the OMEGA Server via wireless online network; Key-Points via LAN. This enables all validation devices to read all events stored in the locking media and transmit it to the OMEGA Server. Key Points additionally transmit all other pending programming jobs to the locking medium (e.g. alterations in the locking permissions) during validation.

A regularly necessary validation ensures that a locking media that has fallen into the hands of unauthorized persons, can be **blocked** quickly and easily by the validation devices. Blocked locking media are not accepted by the locking devices as a rule.

Only locking media which are in service, can be validated.

A locking media is **valid**for one year, however, it must be **validated** every day anew.

8.4.2 How to define validation settings for locking devices

1. In the navigation menu, click on AUTHORISATION > DEVICES**.**

2. Double-click on the desired locking device.

The DEVICE EDITOR *opens.*

3. Open the DEVICE DATA **tab.**

4. Enter the validation settings for the locking device:

Point in time	Here, you can set the period during which the validation can be carried out:	
	Reference period	The validation can be carried out only during the set period. You can set this period using the fields FROM - UNTIL (time of the day) and the weekday checkboxes.
	Once per day	Validation can be carried out at any time; however, each locking medium will be validated only once a day. If the locking medium is held into the reading field of the validation device more than once a day, there will be no additional validation.
	At any time	Validation can be carried out at any time. Any time a locking medium is held into the reading field of the validation device, it is validated.
Updating mode	Here, you set how often a locking medium has to be validated, i.e. which new expiry date has to be set on the locking medium:	
	Period	The expiry date is extended with the VALUE and the UNIT set, e.g. with “1 day” or “8 hours".
	End of day	The expiry date is set to the end of the current day (23:59).
	End of reference period	(Only available if you have selected “reference period” in the POINT IN TIME field) The expiry date is set to the **end time of the current date** of the reference period. The locking medium cannot be validated on any other days. **Example:** the reference period is set from 8 am to 6 pm for the weekdays Monday and Tuesday. If a locking medium is validated on a Monday, the expiry date is set to 6 pm of this Monday.

5. Click on “Save”.

The validation settings for the locking device have now been saved.

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

8.4.3 How to set an expiry date for a locking medium

1. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
2. **Double-click on the desired locking medium.**
3. **Open the tab** DATA**.**
4. **In the field** EXPIRY DATE **, enter the date on which the locking medium should no longer be usable.**

⚠ You have to program the locking medium to make the changes come into effect (see "Programming V-NET locking media" auf Seite101).

5. **Click on** PROGRAMMING **for the changes to come into effect immediately.**
6. **Click on** SAVE **for the changes to come into effect later.**

8.5 Email messages

8.5.1 About email messages

Email messages can be sent automatically if certain events or system messages have occurred.

Example: you want to receive an email message immediately as soon as the second-stage battery warning level of a locking device has been reached.

With email messages you can define

- for what kind of events and system messages emails are to be sent
- how often emails are to be sent (e.g. as soon as the event has occurred, or just once a week)
- to whom the emails are to be sent

8.5.2 How to create email messages

1. If desired: set up your own SMTP server to send emails.

If you do not change any standard settings (checkbox AUTOMATIC is activated), the emails are sent via the CES SMTP server.

How to set up an SMTP server

7. In the main menu, click on SETTINGS > OPTIONS**.**

The window OPTIONS *opens.*

8. Click on EMAIL MESSAGES > SMTP SERVER**.**

9. Enter the settings of the SMTP server you want to use to send the email messages.

If you do not change any standard settings (checkbox AUTOMATIC is activated), the emails are sent via the CES SMTP server.

10. Click on the TEST EMAIL **button to check whether the settings are correct.**

11. Click on OK.

The settings for the SMTP server have now been saved.

2. If this is not yet the case: create a template for your email messages.

How to create a template for email messages

1. In the main menu, click on SETTINGS > OPTIONS**.**

The window OPTIONS *opens.*

2. **Click on** EMAIL MESSAGES > TEMPLATES**.**
3. **Click on the tab with the language you want to use to create the template.**

ℹ Subsequently, for every email message you can set what language is to be used for the emails.

4. **In the** SUBJECT **field, you can define the contents of the subject line of the email message.**

ℹ You can use variables to define what kind of information is shown for an event or a system message. To do so, you can use the available variants to compile the %EVENT% variable, which you can then use in the email text (EMAILfield).

5. **Use the** %EVENT% VARIABLE CONTENTS **field to define the contents of the %EVENT% variable in the field: click the right mouse button in the field, and select the desired variables. In addition, you can also add normal text and line breaks.**

For the significance of variables for email messages, please refer to "The significance of variables for email messages" auf Seite65.

6. **Define the contents of the email messages in the** EMAIL **field. To do so, you can use normal text, line breaks, and the %EVENT% variable.**

ℹ Variables from the %EVENT% VARIABLES CONTENTS cannot be used as individual variables in the EMAIL field.

Example:

In the field CONTENTS OF THE %EVENT% VARIABLE you enter:

On %EVENT_TIME%, the following happened: %EVENT_NAME%.

The following device is affected: %DEVICE_NAME%.

In the EMAIL field, you enter:

An event has occurred:

%EVENT%

For example, the email message will show:

An event has occurred:

On 14.07.2018 10:44:58, the following event occurred: RF-Stick detected.

The following device is affected: device 19 F815DK-M-GS.

7. **Click on the** TEST EMAIL **button to send an email message with test values. This allows you to check the correct representation of the variables.**
8. **Click on** OK**.**

   The template for the email messages has now been saved.

3. **Define the settings for the email messages.**

How to define the settings for email messages

1. **In the main menu, click on** SETTINGS > OPTIONS**.**

   The window OPTIONS *opens.*

2. **Click on** EMAIL MESSAGES > EVENTS **or** EMAIL MESSAGES > SYSTEM MESSAGES**.**
3. **Click the right mouse button into the right part of the** OPTIONS **window, and in the context menu, click on** ADD DATA**.**

   The window MESSAGES *opens.*

4. **In the field** NAME **, enter the name of the new message.**
5. **Then, select the language of the template to be used for this message.**

ℹ You can edit the contents of the templates in various languages in EMAIL MESSAGES > TEMPLATES .

6. In the EVENTS **or** SYSTEM MESSAGES **view, select what kind of events or system messages are to trigger an email message.**

7. In the TYPE **and** SCHEDULE **views, select when you want to receive an email message:**

Immediately	As soon as the event or system message has occurred and been transferred to OMEGA Client, an email is sent.
Daily	Enter the date on which you want to receive an email message for the first time. The time set applies to this and all subsequent messages. The repeat interval allows you to define whether you want to receive the message on a daily basis (1) or e.g. every three days (3). If the event or system message has occurred, you will receive an email message at the time you have selected.
Weekly	Enter the date on which you want to receive an email message for the first time. The time set applies to this and all subsequent messages. The checkboxes of the weekdays allow you to define the weekdays when you want to receive a message. You can also select several weekdays. If the event or system message has occurred, you will receive an email message at the time you have selected.
Monthly	Enter the date on which you want to receive an email message for the first time. The time set applies to this and all subsequent messages. With the fields “Months” and “Days” you can set the month and the day on which you want to receive the messages. You can also select several months and days. If the event or system message has occurred, you will receive an email message at the time you have selected.

8. In the field EMAIL ADDRESSES**, enter the email address to which the email messages are to be sent.**

9. Click on OK**.**

10. Activate the checkbox in the ACTIVATED **column to activate the messages.**

Now, email messages are sent in accordance with the messages settings.

8.5.3 The significance of variables for email messages

	If there are events, it contains	If there are system messages, it contains
%NO%	Consecutive number of the event	Consecutive number of the system message
%EVENT_NAME%	Name of the event type (e.g. "RF-Stick-Master detected")	Name of the system message (e.g. “Key-Point offline")
%EVENT_ID%	The internal ID of the event type (e.g. "219" (=RF-Stick-Master detected))	The internal ID of the system message
%EVENT_TIME%	Point in time when the event was saved in the locking device	Point in time when the event was saved in the database of the server
%DATABASE_TIME%	Point in time when the event was saved in the database of the server	Point in time when the system message was saved in the database of the server
%DEVICE_NAME%	Name of the locking device where the event occurred	Name of the locking device where the event occurred
%DEVICE_UID%	Locking device UID	Locking device UID
%MEDIA_NUMBER%	Locking medium number	Locking medium number
%MEDIA_UID%	Locking medium UID	Locking medium UID
%PERSON%;	Surname and first name of the person who triggered the event (only possible if locking medium has been allocated to a person)	Surname and first name of the person who triggered the event (only possible if locking medium has been allocated to a person)
%EVENT_TYPE%	-	System message type (warning or information)
%EVENT_CATEGORY%	-	System message category (e.g. OMEGAFlex Key-Point)
%IP_ADDRESS%	-	IP address of the device which has generated the system message
%EVENT%	Is generated from the abovementioned variables and used for the text of the email message	

8.6 Reports

8.6.1 About reports

OMEGA Client offers two different report types:

- Events
- Journal

ℹ Events log incidents taking place at **locking devices** . The Journal logs incidents taking place in **OMEGA Client**.

Events

Technical processes in the OMEGA FLEX system are stored as **events** in the locking device (for V-NET in locking media) and are read-out in OMEGA Client. This, for example includes, which locking media has been authorized when for which locking device; which locking media got access when to which locking device, battery warning etc.

If desired, the recording of events can be completely deactivated.

Journal

The **Journal** logs the user activities in OMEGA Client, such as changes to settings.

8.6.2 How to import events from locking media

With IMPORT EVENTS, you can read events saved on a V-NET locking medium and import them into OMEGA Client. After the import, the events will be deleted from the locking medium memory.

1. **Connect Desktop-Reader or Desktop-Writer.**
2. **Place the locking medium whose events you want to import on top of the Desktop-Reader or Desktop-Writer.**
3. **In the navigation menu, click on** REPORTS > EVENTS**.**
4. **In the** EVENTS **view, click on** IMPORT EVENTS**.**
   Now, the events will be imported into OMEGA Client and will subsequently be deleted from the locking medium.

8.7 Time recording

Time recording is a function of OMEGA Client which allows you to log and evaluate access times. You can use the data for two kinds of evaluation:

- the attendance list
- time evaluation

Attendance list

The **attendance list** shows who is currently present or absent. For that purpose, the people have to be assigned to the locking media first. The attendance list contains your data from locking devices which were activated for time recording.

Time evaluation

Time evaluation shows when someone arrived and left during the day, and it can be used to record the working time. Time evaluation contains both, your data from locking devices that have been activated to record times, and data from those people who have been assigned to the respective locking media.

8.7.1 Setting up time recording

4. If this is not yet the case: please contact your CES partner to receive a time-recording licence.
5. If this is not yet the case: add people to OMEGA Client.
6. If this is not yet the case: Link the locking media to the people in the locking medium editor.
7. Activate time recording of locking devices (“entry event & leave event").
8. (Optional) Define the period after which a “leave event” has to be recorded automatically in the time evaluation or attendance list.

8.7.1.1 Adding persons to OMEGA Client

1. In the navigation menu, click on People.
2. Click on the How to add people view.

   The People editor *opens.*

About the people editor

General tab

Salutation	ℹ The text you enter here is saved to be available as a quick selection in the future.
Picture	Here, you can add a photo of the person. In order to add a photo, click into the field with the right mouse button.
First name, family name, street, etc.	ℹ This data is for information purposes only and has no technical effect.
Time recording	Here, you can set if you want to activate time recording for this person.

Details tab

Here, you can add further details such as personnel number or department . These details are for information purposes only and have no technical effect.

ℹ Data you have entered in the fields unit, activity, department, cost centre , and room , is added as entry suggestions. For example, if you have entered “Sales” in the Department field, you will see “sales” as an entry suggestion in a drop-down menu of this field.

3. Enter the corresponding data in the GENERAL **tab.**

a) In order to add a photo, click into the PICTURE field with the right mouse button, select UPLOAD , and select the desired picture (JPG format). You can enter pictures directly from the clipboard with INSERT .

b) In the time recording field, you can define whether time recording is to be activated for this person.

yes	Time recording will be activated for this person, which means he or she is shown on the attendance list and in time evaluation.
no	Although time recording has been activated for locking devices, time recording is not activated for this person, and he or she will not be shown on the attendance list or in time evaluation.

4. Enter the corresponding data in the DETAILS **tab.**

5. If you have already created a group for people, you can add the individual persons of this group in the GROUPS **tab.**

6. Click on APPLY**.**

Now the data for this person has been changed.

8.7.1.2 How to link a locking medium to a person

You can link people to locking media in order to

- be able to trace in OMEGA Client which person a locking medium has been issued to
- use time evaluation for this person
- be able to use the attendance list of this person

7. In the navigation menu, click on AUTHORISATION > LOCKING MEDIA**.**

8. Double-click on the locking medium you want to replace.

The LOCKING MEDIUM EDITOR OPENS.

9. From PERSON **drop-down menu, select the person whom you want to link the locking medium to.**

Here, you can also create a new person (using the ADD button), or you can edit a person who has already been created (using the EDIT button).

With the DELETE button , you can delete the allocation of this specific person to the locking medium.

10. Click on SAVE**.**

Now, the person has been linked to the locking medium.

8.7.1.3 How to activate time recording for locking devices

ℹ Time recording can be activated for the locking devices of the T, VT, NET, and VA variants.

ℹ If the relay mode of a locking device is Off , this locking device does not collect data for time recording.

1. In the navigation menu, click on Authorisation > Devices**.**

2. Double-click on the locking device you want to edit.

The device editor opens.

3. In the Time recording **field, select the desired type of time recording:**

Off	No time recording
Entry event	An authorised locking medium which authenticates itself at a locking device will trigger an “entry event”.
Leave event	An authorised locking medium which authenticates itself at a locking device will trigger a “leave event”.
Entry event & leave event	The authentication of authorised locking media at this locking device is alternatingly considered to be an “entry event” or “leave event”, starting with an “entry event”.

4. Click on Save**.**

The changes for the locking device have now been saved. It is not necessary to program the locking device.

8.7.1.4 How to set up an automatic absence or deregistration

You can define whether people listed in the attendance list or in the time evaluation will be automatically registered as absent or locked off after a certain period of time. You can set the number of hours separately for the attendance list and the time evaluation.

1. **In the main menu, click on** SETTINGS > OPTIONS**.**

   The window OPTIONS *opens.*

2. **Click on** ATTENDANCE LIST**, if people are automatically registered as absent after an entry event has occurred and a certain number of hours has elapsed.**

   Click on TIME EVALUATION**, if people are automatically logged off after a certain number of hours has lapsed.**

3. **In the “hours” field, enter the desired number of hours. If you enter “0”, automatic absence is deactivated.**

Example: in TIME EVALUATION , you enter "8" in the hours feared, and in ATTENDANCE LIST, you enter “20”. As a result, people will automatically be logged off in the time evaluation after eight hours, and in the attendance list after 20 hours if an entry event was registered for them.

9 Settings for locking devices

9.1 Setting in the “Parameters” tab

1. In the navigation menu, click on AUTHORISATION > DEVICES.

2. Double-click on the locking device you want to edit.

The device editor opens.

You can change the following settings in the PARAMETERS *tab:*

Opening duration

The opening period is the length of time during which the locking device remains coupled, after an authorised locking media was held in the reading field of the locking device.

The longer the opening period, the more time people have to operate the locking device after the authenticating with a locking media. The maximum opening period is 180 seconds.

Relay mode

(Only available for wall terminals and validation devices)

The **Relay mode** shows how the relay of the wall terminal is switched:

Off
(Only for the VA variant and Key-Points)

The relay is not controlled, and authorisations are not checked. With this setting, the wall terminal does not work as a locking device, it only validates data. i.e. it updates the expiry date and reads events. Should the locking medium be on the blocking list, it will be blocked.

As there are no authorisation events, wall terminals where the relay is in "off" mode do not send any time recording data.

Impulse

Having read an authorised locking medium, the relay will be triggered for the period set in the OPENING DURATION field.

The office function can only be used in this relay mode.

Toggle

Having read an authorised locking medium, the relay will switch between two states. For example, the first reading process triggers the status "gate open", and the second reading process triggers the status "gate closed".

Dead-man

The relay will switch as long as an authorised locking medium is held in front of it.

Relay delay

(Only available for wall terminals and validation devices)

In this field, you can set whether the relay is to switch after a certain delay only. The maximum relay delay is 20 seconds.

Example: if you have set a relay delay of 5 seconds, you have to hold the locking medium 5 seconds into the reading field before the relay will switch.
If you want to activate the office mode, you have to hold the locking medium into the reading field for seven seconds (5 seconds relay delay + 2 seconds to activate the office mode).

Operating mode

(Only available for locking devices of the NET variant)

The **operating mode** determines how often the locking device communicates with the Access-Point.

ℹ The programming mode has to be set to "Online” so that a locking device can communicate with an Access-Point.

The following occurs during communication:

- Programming jobs from OMEGA Client are transmitted to the locking device.
- New events in the locking device are transmitted to OMEGA Client.
- The clock is set

ℹ In both operating modes, the locking device **always** logs **additionally** into the Access-Point when it is operated (e.g. a locking medium is held in front of it).

ℹ Both operating modes have in common that, when a locking device logs into the Access-Point, new events are transmitted to OMEGA Client, even when there are no programming jobs.

Wake-up interval	In the Wake-up interval operating mode, the locking device regularly checks with the Access-Point where there are any programming jobs.
Wakeup-On-Radio	In the Wakeup-On-Radio operating mode, the locking device is constantly waiting for the Access-Point signal. As soon as there are new programming jobs, the Access-Point wakes up the locking device, and their communication starts. Due to this mode, new programming jobs are always transmitted immediately. In addition, a wake-up interval is set for the Wakeup-On-Radio operating mode. If there are no programming jobs, or the locking device has not been operated properly, the wake-up interval makes sure that the locking device regularly connects to the Access-Point.

ℹ This setting influences battery consumption.

Wake-up interval

(only available for the locking devices of the NET variant, wall terminals and update terminals)

The wake-up interval determines the intervals at which the locking device contacts the Access-Point to ask whether there are new programming jobs. The standard value is set to 15 minutes.

ℹ This setting influences battery consumption.

Radio cell

(only available for the locking devices of the NET variant, wall terminals and update terminals)

Here, you can define the radio cell of the device.

You can use radio cells to determine which locking devices are supposed to communicate with Access-Points, and which Access-Points these are. This is useful if the radio range of two Access-Points overlap.

> **Example:** one Access-Point is situated on the ground floor, and one on the first floor. Due to fluctuations in the radio network, it can sometimes happen that locking devices on the first floor connect to the Access-Point on the ground floor, which decreases the quality of the radio link. For this reason, you assign radio cell 1 to the Access-Point and the locking devices on the ground floor, and radio cell 2 to the Access-Point and locking devices on the first floor. Therefore, the locking devices on the first floor no longer connect to the Access-Point on the ground floor.

Radio cell 0 is a standout radio cell for all Access-Points and locking devices, which means that radio cell 0 corresponds to the setting "no radio cell".

Language

(Only for Key-Points)

Here, you can set the language of the Key-Point display.

Max. programming duration

(Only for Key-Points)

Here, you can define the maximum programming duration for locking media at this Key-Point. If programming takes more time than set, the Key-Point refers the user to the administrator so that the locking medium can be programmed with the Desktop-Writer.

Radio Key

Here, you define whether the locking device accepts Radio Keys.

Beeper

The **beeper** of a locking device emits acoustic signals which support the visual signals. The beeper can be switched on and off via OMEGA Client. When the beeper is switched off, the locking device no longer emits any acoustic signals.

ℹ This setting influences battery consumption.

Double beep

Here, you define whether a double beep is omitted after disengaging.

ℹ This setting influences battery consumption.

9.2 Programming mode (only for online locking devices)

9.2.1 About the programming mode

The programming mode determines in which way programming jobs are transferred to the locking device:

Online Programming jobs are automatically transferred to the locking devices via the wireless online network (via the Access-Point). How frequently the programming jobs are transferred depends on the settings of the OPERATING MODE .

Offline Programming jobs are manually transferred to the locking devices via RF-Stick.

9.2.2 How to set the programming mode

The programming mode can only be activated for devices of the NET and VA variants.

1. **In the navigation menu, click on** AUTHORISATION > DEVICES**.**
2. **Double-click on the locking device you want to edit.**

   The device editor opens.
3. **In the** PROGR. MODE **field, select the programming mode for the locking device.**
4. **If you have selected the** ONLINE **programming mode: open the** PARAMETERS **tab, and select the operating mode and the wake-up interval.**
5. **Click on** SAVE**.**

   The programming mode has now been saved. If you have only changed the programming mode, it is not necessary to program the locking device.

If you have changed the operating mode or the wake-up interval:

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

9.2.3 About the operating mode

The **operating mode** determines how often the locking device communicates with the Access-Point.

The programming mode has to be set to "Online” so that a locking device can communicate with an Access-Point.

The following occurs during communication:

- Programming jobs from OMEGA Client are transmitted to the locking device.
- New events in the locking device are transmitted to OMEGA Client.
- The clock is set

ℹ In both operating modes, the locking device **always** logs **additionally** into the Access-Point when it is operated (e.g. a locking medium is held in front of it).

ℹ Both operating modes have in common that, when a locking device logs into the Access-Point, new events are transmitted to OMEGA Client, even when there are no programming jobs.

Wake-up interval	In the Wake-up interval operating mode, the locking device regularly checks with the Access-Point where there are any programming jobs.
Wakeup-On-Radio	In the Wakeup-On-Radio operating mode, the locking device is constantly waiting for the Access-Point signal. As soon as there are new programming jobs, the Access-Point wakes up the locking device, and their communication starts. Due to this mode, new programming jobs are always transmitted immediately. In addition, a wake-up interval is set for the Wakeup-On-Radio operating mode. If there are no programming jobs, or the locking device has not been operated properly, the wake-up interval makes sure that the locking device regularly connects to the Access-Point.

9.2.3.1 About the wake-up interval

The wake-up interval determines the intervals at which the locking device contacts the Access-Point to ask whether there are new programming jobs. The standard value is set to 15 minutes.

9.3 How to set standard values for the battery consumption

See "20.4 How to set standard values for the battery consumption" auf Seite147.

9.4 How to set the mounting date for locking devices automatically

You can have the ASSEMBLY DATE field filled in automatically. When locking devices are programmed, it will then be checked whether the ASSEMBLY DATE field is empty. If this is the case, the programming date will be entered as the assembly date. This happens for both new locking devices as well as locking devices which have already been added and whose field is still empty.

1. In the main menu, click on SETTINGS > OPTIONS**.**

The window “Options” opens.

2. In the menu item VIEW **, click on** GENERAL**.**

3. Activate or deactivate the checkbox next to SET ASSEMBLY DATE FOR DEVICES AUTOMATICALLY.

If you have deactivated the checkbox, the assembly date will not be filled in automatically.

If you have activated the checkbox, the assembly date will be filled in automatically when the locking device is next programmed, if the assembly date field is empty. The programming date will be entered as the assembly date.

9.5 How to set the assembly status of a locking device during its import

You can define whether the assembly status of a locking device should be automatically set to “not assembled” during import. Otherwise, this value will be taken over from the locking system file.

1. In the main menu, click on SETTINGS > OPTIONS**.**

The window OPTIONS *opens.*

2. Click on the IMPORT/EXPORT **menu item.**

3. Activate or deactivate the checkbox.

If you have deactivated the checkbox, the value of the locking system file will be used as the assembly status.

If you have activated the checkbox, the assembly status of a locking device will be set to “not assembled” during import.

9.6 CTC mode settings (only for LEGIC locking devices)

9.6.1 About the CTC mode

The CTC mode allows you to set the reading behaviour of LEGIC locking devices. You can set the CTC mode only within OMEGA FLEX LEGIC systems.

Technical background

LEGIC devices can read different locking media types with different transponder technologies, e.g. LEGIC prime or LEGIC advant. The CTC mode allows you to set which transponder technology is read first or is not read at all.

Settings options

	Settings	Meaning
Reading behaviour	**auto prime (Standard)**	**LEGIC prime is read first**
	auto advant	LEGIC advant is read first
	prime	Only LEGIC prime is read
	advant	Only LEGIC is read
ISO mode	**on (Standard)**	**ISO locking media are read**
	off	ISO locking media are not read

If you use **HID iClass locking media**, you have two sets "auto prime" or "auto advant" to define the reading behaviour. Otherwise, the locking media cannot be read. The locking mode is irrelevant for iClass locking media.

Note on using CTC locking media

Normally, locking media contain just one transponder, e.g. LEGIC prime. CTC locking media contain two transponders (LEGIC prime and LEGIC advant), and thus they have two UIDs (one for LEGIC prime, and one for LEGIC advant). If you read in CTC locking media with the Desktop-Reader, both UIDs are transmitted to OMEGA Client and are shown there.

If you authorise CTC locking media with the Program-Master, only **one** of the two UIDs will be authorised. This can lead to the effect that with certain CTC mode settings, the CTC locking medium may be refused. For this reason you should always read CTC locking media into OMEGA Client, and authorise the locking media with the locking plan.

Example: Using the Program-Master, you authorise a CTC locking medium for a locking device with "auto prime” CTC mode. This will authorise only the prime UID. If you now set the CTC mode of your devices to "advant", the locking medium will not be accepted, because the advant UID has not been authorised. If you set the CTC mode to "auto advant", the locking medium will also not be accepted, because the locking device first reads the advant UID which has not been authorised.

Example of use

auto prime/auto advant

For technical reasons, LEGIC prime will be read first. However, you can change this by changing the settings to "auto advant". The "auto advant” settings make sense if your system mainly contains LEGIC advant locking media and just a few LEGIC prime locking media. Thus, LEGIC advant locking media are read faster.

prime/advant

You can totally exclude one of these two technologies. If, for example, you want to increase the security of your system, you can define that only LEGIC advant will be read.

9.6.2 About CTC locking media

Normally, locking media contain just one transponder, e.g. LEGIC prime. CTC locking media contain two transponders (LEGIC prime and LEGIC advant), and thus they have two UIDs (one for LEGIC prime, and one for LEGIC advant). If you read in CTC locking media with the Desktop-Reader, both UIDs are transmitted to OMEGA Client and are shown there.

9.6.3 How to set the CTC mode

The CTC mode is available for OMEGA FLEX LEGIC systems only.

1. **In the main menu, click on** Settings > Options**.**

   The window Options *opens.*

2. **In the menu item** Other **, click on** CTC configuration.

3. **Option A:**

   Select an existing CTC mode: activate the Use as standard **checkbox. Double-click on “CTC mode” to show details. Continue with step 8.**

   Option B:

   Create a new CTC mode: click onto a free space anywhere in the window using the right mouse button. In the context menu, click on Add**.**

   The CTC mode editor opens.

4. **In the field** Name **, enter the name of the new CTC mode.**

5. **Select the** reading behaviour **and the** ISO mode**:**

	Settings	Meaning
Reading behaviour	**auto prime (Standard)**	**LEGIC prime is read first**
	auto advant	LEGIC advant is read first
	prime	Only LEGIC prime is read
	advant	Only LEGIC is read
ISO mode	**on (Standard)**	**ISO locking media are read**

	Settings	Meaning
	off	ISO locking media are not read

6. Click on SAVE**.**

The CTC mode has now been saved.

7. Activate the USE AS STANDARD **checkbox next to the desired CTC mode.**

8. Click on OK**.**

The CTC mode has now been set up for all locking devices.

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

10 How to embed locking devices in online systems

10.1 About the online mode

In the online mode, locking devices communicate with Access-Points via OMEGA Server. In the process, they receive new programming jobs from and send events to the OMEGA Server.

About radio cells

You can use radio cells to determine which locking devices are supposed to communicate with Access-Points, and which Access-Points these are. This is useful if the radio range of two Access-Points overlap.

Example: one Access-Point is situated on the ground floor, and one on the first floor. Due to fluctuations in the radio network, it can sometimes happen that locking devices on the first floor connect to the Access-Point on the ground floor, which decreases the quality of the radio link. For this reason, you assign radio cell 1 to the Access-Point and the locking devices on the ground floor, and radio cell 2 to the Access-Point and locking devices on the first floor. Therefore, the locking devices on the first floor no longer connect to the Access-Point on the ground floor.

Radio cell 0 is a standout radio cell for all Access-Points and locking devices, which means that radio cell 0 corresponds to the setting "no radio cell".

10.2 How to embed locking devices in an online system

1. Optional: specify the radio cell for the locking device.

How to define a radio cell for locking devices

ℹ When supplied to the customer, online locking devices are always in the offline mode.

⚠ If you want to change the radio cell of a locking device, the locking device has to be in the offline mode.

1. In the navigation menu, click on AUTHORISATION > DEVICES**.**

2. Double-click on a locking device of the NET variant.

The device editor opens.

3. In the RADIO CELL **field, enter the desired radio cell (number between 0 and 255).**

4. Click on SAVE**.**

The radio cell for this locking device has now been saved.

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

2. **Make sure that the locking device is in the vicinity of an Access-Point, and activate its online mode.**

Access-Points and Repeater ranges

Device	Maximum range
Access point	25 m
Access-Point with outdoor antenna	40 m
Repeater	extends Access-Point range by 25 m.

How to activate the online mode of a locking device

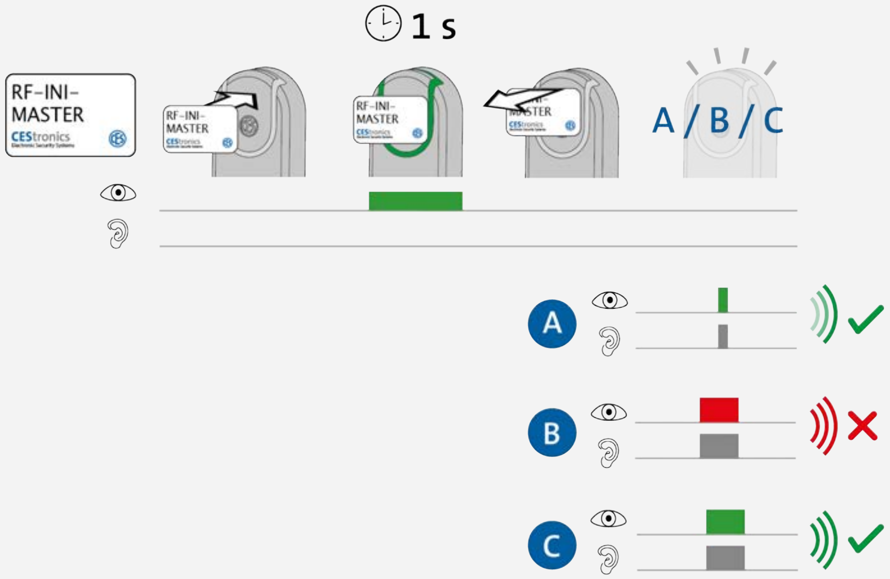
ℹ The online mode can only be activated for locking devices of the NET and VA variants (siehe "Varianten der OMEGA FLEX Schließgeräte" auf Seite 1).

Required master media:

- RF-Ini-Master

ℹ It is *not* necessary to authorise the RF-Ini-Master in advance to activate the online mode.

How to proceed:



1. Hold the RF-Ini-Master for 1 second in the reading field of the locking device.

The following signal appears:

A: 1x short green and 1x short beep	Successfully connected to the Access-Point
B: 1x long red and 1x long beep	No connection to the Access-Point possible
C: 1x long green and 1x long beep	Connection to the Access-Point already existed

Irrespective of whether it was possible to establish contact to an Access-Point or not, the online mode is now activated. As soon as an Access-Point can be found, the locking device automatically contacts it.

Troubleshooting:

Signalling	Reason	Solution
While the RF-Ini-Master is held in the reading field:		
👁 🟥 👂 ⬛	The locking device does not belong to the NET or VA variant.	The online mode is not available for this locking device.

If you have defined a radio cell for this locking device, the Access-Point needs to **be in the same radio cell as the locking device.** Otherwise, the locking device and the Access-Point cannot communicate with each other.

How to define a radio cell for Access-Points

⚠ If the Access-Point is already connected to locking devices via the radio cell, but you

⚠ want to change the radio cell of the Access-Point, the locking devices will be disconnected. Access-Points and locking devices can connect to each other only if they are part of the same radio cell.

1. In the navigation menu, click on AUTHORISATION > DEVICES**.**

2. Double-click on the desired Access-Point.

The Device editor opens.

3. In the RADIO CELL **field, enter the desired radio cell.**

4. Click on "Save".

The radio cell for this Access-Point has now been specified.

ℹ Having activated the online mode, the locking device connects to the Access-Point in the near vicinity.

Information about coupling and decoupling locking devices and Access-Points

Having successfully being coupled to the Access-Point, the locking device only communicates with the coupled Access-Point. In the following cases, coupling is automatically cancelled:

- If the locking device was unable to establish contact with the Access-Point in three consecutive wake-up intervals.
- After new batteries have been inserted, or after re-start.

In both cases, the locking device searches for Access-Points in the vicinity and couples with the first Access-Point it can find.

If you want the locking device to communicate with a different Access-Point, you can initiate re-coupling yourself by moving the new Access-Point into the vicinity of the locking device and

- by holding the RF-Ini-Master for approximately one second into the reading field of the locking device, or
- by deactivating and re-activating the online mode of the locking device.

3. Check the quality of the radio link.

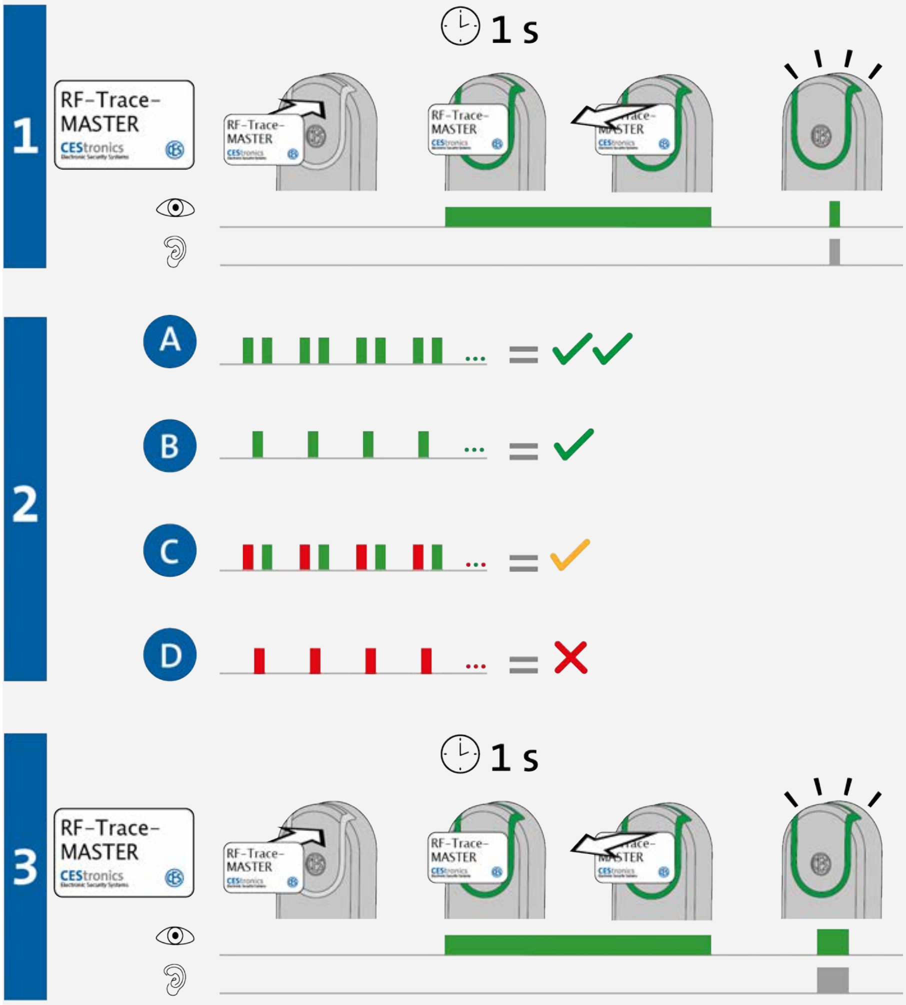
How to check the quality of a radio link

Required master media:

- RF-Trace-Master

The RF-Trace-Master is ready for immediate use and does not have to authorised first.

Procedure:

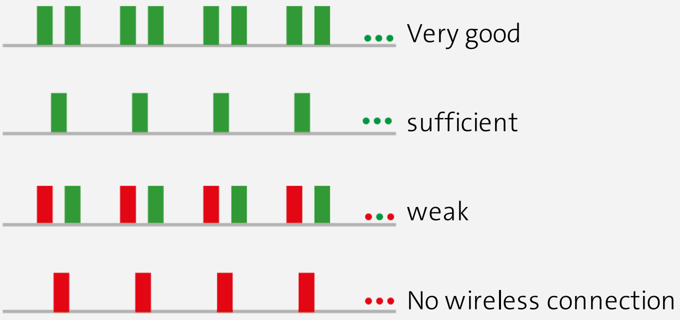


1. Hold the RF-Trace-Master ca. 1 second before the reading field of the locking device.

    The following signal appears:

    1x short green and 1x short beep

2. The locking device shows now the quality of the wireless connection:



The Access-Point associated with the locking device shows during wireless connection test die quality of the wireless connection with the same signalling as the locking device.

3. Hold the RF-Trace-Master ca. 1 second in the reading field to end the wireless connection quality display.

The following signal appears:

1x long green and 1x long beep

The testing of the wireless connection quality is finished herewith.

After 3 minutes, the wireless connection quality display will end automatically.

Troubleshooting:

Signalling	Reason	Solution
👁 🟥 👂 ⬛	The locking device does not belong to the variant NET or VA .	The RF-Trace-Master can only be used with a NET and VA devices.

4. Set the programming mode of the locking device to Online**, so that future programming jobs can be transferred via the wireless online network, and define the desired operating mode.**

How to define the programming mode and operating mode of a locking device

The programming mode can only be activated for devices of the NET and VA variants.

1. In the navigation menu, click on Authorisation > Devices**.**

2. Double-click on the locking device you want to edit.

The device editor opens.

3. In the PROGR. MODE **field, select the programming mode for the locking device.**

4. If you have selected the ONLINE **programming mode: open the** PARAMETERS **tab, and select the operating mode and the wake-up interval.**

5. Click on SAVE**.**

The programming mode has now been saved. If you have only changed the programming mode, it is not necessary to program the locking device.

If you have changed the operating mode or the wake-up interval:

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" Auf der nächsten Seite).

11 Programming locking devices

Locking devices can be programmed in various manners:

- **Programming changes** in locking devices, e.g. when authorisations have been changed (programming jobs are transmitted via RF-Stick or wireless online network)
- **Re-programming** locking devices, e.g. to fully synchronise locking devices with the current status of OMEGA Client (programming jobs are transferred via RF-Stick or wireless online network)
- Programming **firmware updates** (programming jobs are transferred via programming cable, Programming Adaptor or RF-Stick)
- Programming **variant upgrades** (programming jobs are transferred via RF-Stick)

Change log

The **change log** contains all changes which have not yet been programmed. Every change in OMEGA Client which requires the locking device or locking medium to be programmed automatically generates an entry in the change log (e.g. changes to authorisations or time profiles). Programming jobs have to be created from the change log so the changes can be transmitted to the locking devices. Locking media can be programmed directly and without programming job with the change log or the locking medium editor. If you use an update terminal, it is possible to create programming jobs for locking media.

11.1 Programming changes

Programming changes is comprised of two steps:

1. To generate programming jobs from the changes

2. How to transmit programming jobs to the locking devices

11.1.1 Transmitting programming jobs

Option 1: how to create programming jobs for all changed locking devices

ℹ As soon as new changes appear in the change log, the menu item PROGRAM CHANGES will appear in the navigation menu.

1. **In the navigation menu, click on** PROGRAMMING> PROGRAM CHANGES, **or click on** PROGRAMMING > PROGRAM ALL CHANGES IN THE MAIN MENU.
2. **If you want to program offline locking devices, you will be asked whether you want to view the action list.**

> **About the action list**
>
> The **action list** shows which locking devices have to be programmed. You can print the action list and use it as a checklist. This way you know which locking devices you will have to walk to in order to transmit programming jobs.
>
> ℹ The action list serves as an aid when it comes to programming. You can program the locking devices even without the action list being displayed.

Now, the programming jobs are shown in the information view. Now, they only need to be transferred to the locking devices.

Option 2: how to generate programming jobs for specific locking devices

1. **In the navigation menu, click on** PROGRAMMING > CHANGE LOG**.**
2. **Open the desired tab in the change log (**ONLINE DEVICES **or** OFFLINE DEVICES**), and click on** PROGRAMMING**.**

ℹ If you deactivate the checkboxes next to an entry, no programming job will be generated from this entry.

3. **If you want to program offline locking devices, you will be asked whether you want to view the action list.**
   Now, the changes for the selected locking devices are shown as programming jobs in the information view. Now, they only need to be transferred to the locking devices.

Option 3: how to generate programming jobs for one individual locking device

1. **In the navigation menu, click on** AUTHORISATION > DEVICES**.**
2. **Use the right mouse button to click on the locking device for which you want to generate programming jobs.**
3. **In the context menu, click on** PROGRAM CHANGES**.**
   Now, the changes for this specific locking device are shown as programming jobs in the information view. Now, they only need to be transferred to the locking device.

11.1.2 How to transmit programming jobs to the locking devices

11.1.2.1 How to transmit programming jobs to the locking devices with the RF-Stick

Required master media and administration devices:

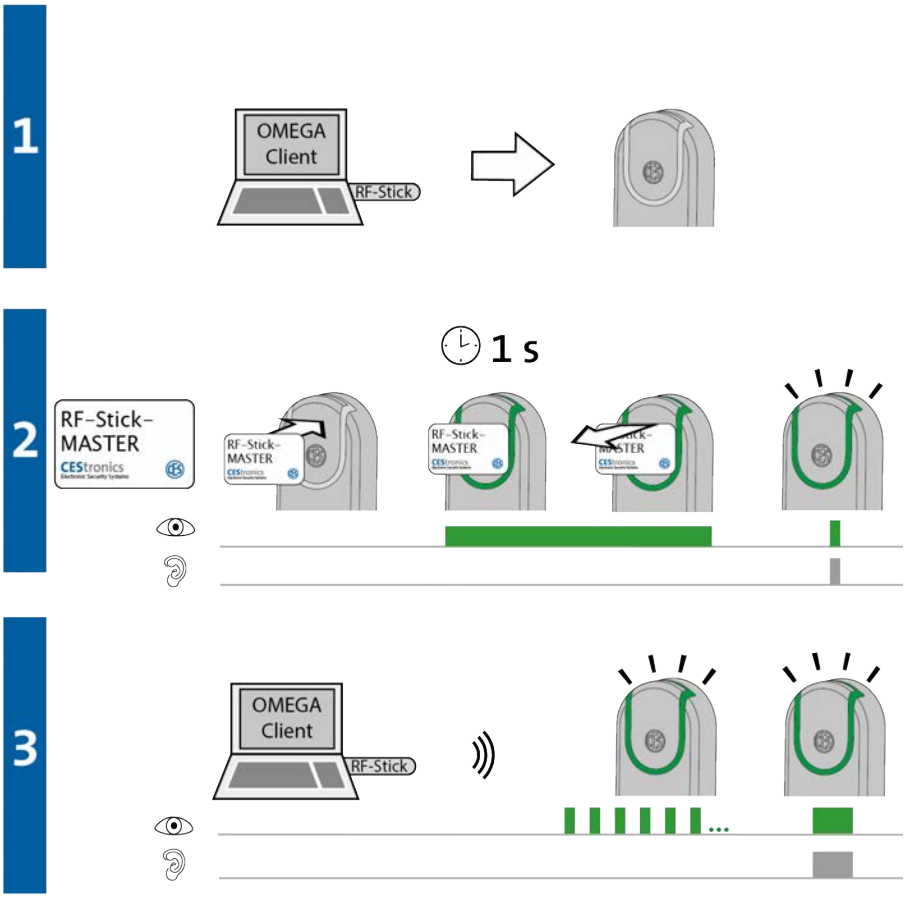
- RF-Stick-Master
- RF-Stick
- PC with OMEGA Client installed

ℹ The RF-Stick-Master must first be authorised for all locking devices with which it is to be used, (siehe "Weitere Master-Medien für Schließgeräte berechtigen" auf Seite 1). Each RF-Stick-Master that has been authorised once is compatible with every RF-Stick of an OMEGA FLEX system.

Procedure for creating programming jobs:

1. **Start the OMEGA Client and log in with your user name and password.**
2. **Set the desired changes in the OMEGA Client.**
3. **Start your changes accordingly as a change programming or new programming, e.g. through** PROGRAMMING > PROGRAM ALL CHANGES.
   The status display of the OMEGA Client shows now "programming required". The individual programming jobs are shown under "Programming status".

Procedure for transmitting programming jobs via an RF-Stick:



1. **Proceed with your PC and the RF-Stick connected to it to the locking device into which the program is to be transmitted.**

   If you want to transmit the programming jobs into multiple locking devices, you can freely choose the sequence in which you look for the locking devices.

2. **Hold the RF-Stick-Master briefly before the reading field of the locking device.**

   The following signal appears:

   1x short green and 1x short beep

3. **The locking device now searches for an RF-Stick nearby.**

   The distance between the locking device and the RF-Stick may not exceed ten meters.at the maximum.

   As soon as the RF-Stick has been detected, the transmission begins. During transmission, the locking device flashes green.

   During transmission the following occurs:

- All programming jobs for this locking device are transmitted to this locking device. During programming, the programming status display shows the progress in percentage.

- All events stored in the locking device, which were not available to the OMEGA Client yet, will be copied into the OMEGA Client.

- The clock is set.

ℹ If no programming jobs are available, only the events are copied and the clock is set. In this case, the locking device does not flash during the transmission.

After transmission of all data, the RF-Stick and the locking device are disconnected automatically. After transmission completion, the programming job is deleted from the "Programming status" list.

The programming job transmission is completed when the locking device signals 1x long green and 1x long beep.

Troubleshooting:

Signalling	Reason	Solution
During step 2:		
👁 🟥 👂 ◼	The locking device cannot detect any RF-Stick nearby.	Move with a properly connected RF-Stick closer to the locking device and try to transmit the programming jobs once again.

11.1.2.2 How to transmit programming jobs to the locking devices with a wireless online network

In a wireless online network, programming jobs are automatically transmitted to the locking devices.

ℹ To ensure that programming jobs are transferred automatically, the **programming mode** of the locking device must be set to ONLINE . The **operating mode** of the locking device decides when these programming jobs will be transferred.

How to set the programming mode und operating mode for locking devices

ℹ The programming mode can only be activated for devices of the NET and VA variants.

1. **In the navigation menu, click on** AUTHORISATION > DEVICES**.**
2. **Double-click on the locking device you want to edit.**

   The device editor opens.
3. **In the** PROGR. MODE **field, select the programming mode for the locking device.**
4. **If you have selected the** ONLINE **programming mode: open the** PARAMETERS **tab, and select the operating mode and the wake-up interval.**
5. **Click on** SAVE**.**

   The programming mode has now been saved. If you have only changed the programming mode, it is not necessary to program the locking device.

If you have changed the operating mode or the wake-up interval:

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

ℹ If many locking devices are allocated to one Access-Point, it may happen that the Access-Point is already communicating with a locking device when another locking device attempts to communicate with this Access-Point. In this case, the locking device will wait for the time set in the wake-up interval to elapse, and will then attempt again to communicate with the Access-Point. This may lead to delays during the transfer of programming jobs.

ℹ If the radio link between the locking device and Access-Point is very weak, there may be delays during the transfer of programming jobs.

ℹ If you want to transfer a programming job waiting to be transferred via the wireless online network manually with a programming device (e.g. with an RF-Stick), you can abort this programming job. Then, set the programming mode of the locking device to OFFLINE. Now, you can manually transfer programming jobs using a **programming device**.

How to abort programming jobs

1. **In the information view in the** PROGRAMMING STATUS **tab, click with the right mouse button on the programming job you want to abort.**
2. **In the context menu, click on** ABORT**.**

   The programming job is now back in the change log.

ℹ If programming jobs are shown on the list in the information view, and an RF-Stick is connected to the PC, the programming jobs are automatically connected with the RF-Stick. If you remove the RF-Stick and then abort programming jobs, you have to reconnect the RF-Stick to the PC so the programming jobs can be reappear in the change log.

ℹ Programming jobs which have been generated by a different user cannot be aborted.

ℹ Only the CES user can abort system jobs generated by other users.

How to set the programming mode und operating mode for a locking device

ℹ The programming mode can only be activated for devices of the NET and VA variants.

1. **In the navigation menu, click on** AUTHORISATION > DEVICES**.**
2. **Double-click on the locking device you want to edit.**

   The device editor opens.
3. **In the** PROGR. MODE **field, select the programming mode for the locking device.**
4. **If you have selected the** ONLINE **programming mode: open the** PARAMETERS **tab, and select the operating mode and the wake-up interval.**
5. **Click on** SAVE**.**

   The programming mode has now been saved. If you have only changed the programming mode, it is not necessary to program the locking device.

If you have changed the operating mode or the wake-up interval:

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

11.2 Re-programming

Re-programming is comprised of two steps:

1. How to generate programming jobs for re-programming

2. How to transmit programming jobs to the locking devices

11.2.1 How to generate programming jobs for re-programming

Option 1: start re-programming all locking devices

In the main menu, click on “Programming” > “Re-program all locking devices”.

Confirm the message with “Yes”.

The programming job log now contains all programming jobs necessary to re-program all the system’s locking devices. Now, they only need to be transferred to the locking devices.

Option 2: start re-programming for an individual locking device

1. In the navigation menu, click on AUTHORISATION > DEVICES**.**

2. Click with the right mouse button on the locking device which you want to re-program.

3. In the context menu, click on RE-PROGRAMMING**.**

The programming job log now contains the programming job necessary for re-programming. Now, it only needs to be transferred to the locking devices.

11.2.2 How to transmit programming jobs to the locking devices

See "How to transmit programming jobs to the locking devices" auf Seite92.

11.3 Firmware updates

For information about firmware updates, please refer to the "Programming Adaptor und Firmware Updates" manual or the CEStronics Suite online help.

11.4 Variant upgrade

ⓘ Variant upgrades and changing the event memory are possible for all OMEGA FLEX locking devices.

ⓘ Variant upgrades and changing the event memory require a new licence, which is subject to a fee.

1. Create a job to upgrade the variant or change the event memory.

How to create jobs to upgrade variants or change the event memory

1. In the main menu, click on Settings > Services.

The window "Services" opens.

There, you see all the locking devices of your system. The blue box highlights the current variant of a locking device. The column SAVE ACCESS EVENTS *shows whether the locking device saves access events (the checkbox is activated), or whether saving of excess events is deactivated (the checkbox is deactivated). System events are always stored.*

To change the variant:

2. In the row for the desired locking device, click on the variant which the locking device should have in future.

To activate/deactivate the event memory:

3. Activate or deactivate the checkbox next to the SAVE ACCESS EVENTS **column in the line of the desired locking device.**

4. If you do not want to send the job file immediately (e.g. because you are not yet connected to the Internet), click on SAVE JOB**.**
If you want to send the job immediately, click on SEND JOB**.**

5. Confirm the message with YES**.**

6. Enter the job data, and click on CONTINUE**.**

7. Accept the terms and conditions, and click on OK.

If you clicked on SAVE JOB **beforehand:**

8. Select the storage location for the job file, and click on SAVE**.**

The job file has now been saved at the desired location, and you can send it by email to CES Service (bestellung@ces.eu). CES Service will send you a new licence file.

If you clicked on SEND JOB **beforehand:**

> *Your standard email program will open automatically with an email to which the job file is attached.*
>
> 9. **Send the email.**
>
>   *The email has been sent to CES Service. You will receive a new licence file.*

2. **Send the job file by email to CES Service (bestellung@ces.eu).**
3. **CES Service will send you a licence file which contains the desired changes. Import this licence file to OMEGA Client.**
4. **This automatically creates programming jobs for the corresponding locking devices. Program the locking devices so the changes can come into effect.**

12 Programming V-NET locking media

In V-NET, authorisations are not saved in the locking devices but in the locking media. For this reason, it is necessary to program locking media in V-NET.

There are two types of programming:

Re-programming (programming with Desktop-Writers)
When a locking medium is re-programmed, its entire memory is re-programmed. Re-programming can be carried out only with Desktop-Writers. Programming a locking medium with Desktop-Writer always automatically re-programs the locking medium.

Programming changes (programming with update terminals)
When changes are programmed, only the changes (e.g. changes to authorisations) are transmitted to the locking medium. Programming changes is much quicker than re-programming, and they are transmitted via update terminals (Key-Points or Update-Terminals).

Prerequisites for programming changes:

- V-NET (Classic or DESFire)
- Update-Terminals
- CEStronics Suite version 1.13.13.363 or higher

If you want to program changes for the first time and are already using V-NET locking media, you have to re-program these V-NET locking media once with the Desktop-Writer. Depending on the Desktop Writer used, this may take some time. Then, the programmed changes are available at the Update-Terminals.

ℹ When programming is interrupted, e.g. because the locking medium is removed from the reading field prematurely, update terminals resume programming where it was interrupted when the locking medium is held in front of it the next time.

12.1 Programming with the Desktop-Writer

Option 1: program an individual locking medium with the locking medium editor

1. Connect the Desktop-Writer to your PC.

2. Place a locking medium onto Desktop-Writer.

3. In the navigation menu, click on AUTHORISATION > LOCKING MEDIA**.**

4. Double-click on the desired locking medium in the list.

You will receive a message telling you that this locking medium has not been programmed yet.

5. Click on Programming**. If you use a Key-Point in your system, click on** Programming > Desktop-Writer**.**

The locking medium is now being programmed.

Option 2: programming one or more locking media using the change log

1. Connect the Desktop-Writer to your PC.

2. Place a locking medium onto Desktop-Writer.

3. In the navigation menu, click on Programming > Change log**.**

4. Open the Locking media **tab.**

5. Click on Programming**. If you use a Key-Point in your system, click on** Programming > Desktop-Writer**.**

ℹ If you deactivate the checkboxes next to an entry, no programming job will be generated from this entry yet.

The locking media will now be programmed.

12.2 Programming with the Update-Terminal

ⓘ Only if you use update terminals (Key-Points or Update-Terminals) with your system is the following programming possible.

Option 1: for an indivdual locking medium

1. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
2. **Double-click on the desired locking medium in order to open the locking medium editor.**
3. **Click on** PROGRAMMING > KEY-POINT OR UPDATE TERMINAL.

   If programming contains a great deal of data, you will receive a message. You can then select whether you still want to continue programming at the desired Update-Terminal, or whether you want to program the locking medium with the Desktop-Writer instead.

ⓘ If the programming time exceeds the maximum programming time set for a Key-Point (max. 180 seconds), the user will receive a message in the Key-Point display that the locking medium has to be programmed with the Desktop-Writer when s/he holds a locking medium to the Key-Point.

Now, the changes are shown as programming jobs in the information view in the LOCKING MEDIA *tab.*
The programming jobs are transferred to the locking medium as soon as it is placed in the reading field of the Update-Terminal.

ⓘ When programming is interrupted, e.g. because the locking medium is removed from the reading field prematurely, update terminals resume programming where it was interrupted when the locking medium is held in front of it the next time.

Option 2: for multiple locking media at the same time

1. **In the navigation menu, click on** PROGRAMMING > CHANGE LOG**.**
2. **Open the** LOCKING MEDIA **tab.**

   You see all the changes which still have to be converted into programming jobs. If you deactivate the checkbox next to an entry, no programming job will be generated from this entry.

3. **Click on** PROGRAMMING > KEY-POINT **or** UPDATE TERMINAL**.**

   If programming contains a great deal of data, you will receive a message. You can then select whether you still want to continue programming at the desired Update-Terminal, or whether you want to program the locking medium with the Desktop-Writer instead.

ℹ If the programming time exceeds the maximum programming time set for a Key-Point (max. 180 seconds), the user will receive a message in the Key-Point display that the locking medium has to be programmed with the Desktop-Writer when s/he holds a locking medium to the Key-Point.

Now, the changes are shown as programming jobs in the information view in the LOCKING MEDIA *tab.*
The programming jobs are transferred to the locking medium as soon as it is placed in the reading field of the Update-Terminal.

ℹ When programming is interrupted, e.g. because the locking medium is removed from the reading field prematurely, update terminals resume programming where it was interrupted when the locking medium is held in front of it the next time.

ℹ The menu item PROGRAMMING > PROGRAM CHANGES in the navigation menu, and the menu item PROGRAMMING > PROGRAM ALL CHANGES in the main menu generate programming jobs for locking devices only, not for locking media.

13 Loss of locking media

13.1 LINE locking media

When a LINE locking medium is lost, you have to delete this locking medium from OMEGA Client to restore the safety of your system.

Deleting a locking medium

⚠ When a LINE locking medium is deleted, all authorisations which exist for this locking medium will be deleted.

1. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
2. **Click the right mouse button on the desired locking medium, and in the context menu, click on** DELETE LOCKING MEDIUM**.**
3. **Confirm the message with** YES**.**
   The locking medium has now been deleted and it is no longer shown in the locking medium view or in the locking plan. The programming job log now contains programming jobs for all locking devices for which the locking medium is authorised, in order to delete the authorisations.

⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

⚠ Important note on using the Program-Master:

If you are using the OMEGA Client, you should dispense with the Program-Master, because the OMEGA Client itself acts as “Program-Master” while awarding locking authorisations. Since the locking media can only be authorised and deleted by the same Program-Master, therefore, although the Program-Masters can be read into OMEGA Client but cannot be transmitted to the locking device.

It means that:

1. The authorisations assigned by Program-Master will **not be displayed in OMEGA Client**. As a consequence, the locking plan displayed in OMEGA client is out of sync with the actual locking authorisations.
2. Individual or dedicated deletion of authorisations assigned by the Program-Master is not possible via software; instead, to delete you have to use the **Program-Master** or reprogram the locking device.
3. A **reprogramming** of locking devices automatically results in deletion of all authorisations created by a Program-Master.

13.2 V-NET locking media

When a V-NET locking medium is lost, you have to delete this locking medium from OMEGA Client to restore the safety of your system. You can do it using the **blocking list**.

"Blocking locking media (only V-NET)" Auf der gegenüberliegenden Seite.

14 Blocking locking media (only V-NET)

14.1 About blocking locking media

In V-NET, the locking media which are not supposed to be in use are not deleted but rather **blocked**. The information that a locking media is blocked is stored in the locking media. Locking devices have **block lists**, which contain the blocked locking media. Each authorisation attempt triggers the following:

- The locking device checks whether the locking media is blocked. Only unblocked locking media are accepted.
- If a locking media is unblocked but is on the block list, the locking device transmits information to the locking media that this locking media is blocked.

14.2 About the blocking list

ℹ The blocking list is relevant only in V-NET.

There are two blocking list types:

Global blocking list

The global blocking list is the general blocking list of the system. Each locking medium which is blocked is entered into this blocking list. From there, the locking medium is transferred to the device-specific blocking list. The way you block a locking medium decides which device-specific blocking list the locking medium is transferred to, and how this is done.

You can call up the global blocking list by clicking on AUTHORISATIONS > BLOCKING LIST in the navigation menu.

ℹ Locking media which figure in the global blocking list are no longer shown in AUTHORISATIONS > LOCKING MEDIA, they are only shown on the blocking list.

Device-specific blocking lists

The device-specific blocking list is a blocking list which is saved in a locking device. You can only add locking media to a blocking list which have already been entered into the global blocking list.

You can call up the device specific blocking lists if you open the tab BLOCKING LIST in the device editor of a V-NET locking device.

14.2.1 What are the effects of a locking medium being placed on the global blocking list?

- The locking medium is no longer displayed under AUTHORISATIONS > LOCKING MEDIA , but rather only in the global blocking list.
- The locking medium is listed on the device-specific blocking lists of all V-NET locking devices for which it was authorised.
- Should the blocked locking medium have been authorised for LINE locking devices, the programming jobs for the LINE locking devices are automatically created to delete the authorisations from the locking devices.

  ⚠ A blocked locking medium still can be used for LINE locking devices if you do not delete the authorisations from this particular locking device. Therefore, make sure that you delete the authorisations from the LINE locking devices in a timely manner. You have to **program the locking devices** to make the changes come into effect.

- Only applicable for blocking with status changes: the change log contains the changes for all V-NET locking devices for which the locking medium has been authorised, so that the device-specific blocking lists of the locking devices can be updated. If the locking medium has been placed on the blocking list by creating a replacement medium, the replacement medium transmits the blocking list to the locking devices. This does not require programming jobs.

  ⚠ As long as the blocking list has not yet been transmitted to the device-specific blocking lists of the locking devices, the locking devices still can be opened with the locking medium even though this has already been put on the global blocking list. Only after the locking medium has been blocked by one of the locking devices does it then become unusable. Therefore, make sure that you transmit the blocking list to the locking devices in a timely manner.

14.3 How to block a locking medium by changing its status

Instead of using the status change to block a medium, you can also create a replacement medium for the respective locking medium (see "How to block a locking medium with a replacement medium" Auf der nächsten Seite).

1. **In the navigation menu, click on** AUTHORISATION > LOCKING MEDIA**.**
2. **Double-click on the locking medium you want to block.**

   The locking medium editor opens.
3. **Open the tab** DATA**.**
4. **In the** STATUS **field, you can select either** LOST **or** BLOCKED **.**
5. **Confirm the message with** OK**.**
6. **Click on** SAVE**.**

   Now, the locking medium has been placed on the global blocking list.

A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

Instead of programming the locking devices with the RF-Stick, you can also create a blocking list medium (see "How to create and transmit a blocking list medium" auf Seite112).

14.4 How to block a locking medium with a replacement medium

14.4.1 About replacement media

A **replacement media** is a locking media in V-NET which contains the data of its predecessor media. If a replacement media is used on locking devices, it transmits information to the locking devices that its predecessor media must be blocked. If the replacement media is used on these locking devices, then the replacement media will be blocked and cannot be used on any locking device.

A replacement medium transmits the blocking information only to the locking devices for which the predecessor medium was authorised. If the replacement medium is to be authorised for more locking devices than the predecessor medium, it transfers the blocking information to those additional locking devices too.

14.4.2 How to create and use replacement medium

1. In the navigation menu, click on AUTHORISATION > LOCKING MEDIA**.**

2.

a) If you want to edit an existing locking medium: double-click on the desired locking medium.

b) If you want to add a new locking medium: click on the ADD LOCKING MEDIA > ADD V-NET LOCKING MEDIUM view.

The LOCKING MEDIUM EDITOR *opens.*

3. In the DATA **tab in the** PREDECESSOR MEDIUM **field, select the locking medium you want to block and which is to become the replacement medium for the current locking medium.**

Now, the locking medium has been converted into a replacement medium for the predecessor medium.

⚠ You have to program the locking medium to make the changes come into effect (see "Programming V-NET locking media" auf Seite101).

The predecessor medium will automatically be set in the global blocking list.

4. Now, you have two options:

- You can now transfer the blocking list with the replacement medium to the locking devices. To do so, simply hold the replacement medium into the reading field of the locking devices for which the predecessor medium was authorised.
- You can create a blocking list medium and thus transfer the blocking list to the locking devices.

- You can create programming jobs in the BLOCKING LIST view (AUTHORISATIONS > BLOCKING LIST) by clicking on PROGRAM BLOCKING LISTS > ADD TO BLOCKING LIST. This creates entries in the change log which you can convert into programming jobs and transfer to the devices with the RF-Stick.

14.5 How to create and transmit a blocking list medium

5. **Place the locking medium you want to change into a blocking list medium on top of the Desktop-Writer.**
6. **In the navigation menu, click on** AUTHORISATION > BLOCKING LIST**.**
7. **Select the locking media you want to transfer to the locking devices with this blocking list medium. If you keep the** CRTL **button pressed, you can select several locking media.**
8. **In the view, click on the** CREATE BLOCKING LIST MEDIUM**.**

   The blocking list editor opens.

9. **Click on** PROGRAMMING**.**

   The locking medium is now being programmed. Thereafter, it is a blocking list medium which is able to transfer the selected locking media to the blocking lists of the locking devices. To do so, simply hold it into the reading field of the locking devices.

15 MIFARE DESFire settings

15.1 How to enable or prevent formatting of DESFire locking media

⚠ The following setting cannot be **undone**, and therefore, only authorised persons may change it!

You can define whether formatting MIFARE DESFire locking media is generally possible or not. You can prevent formatting and thus make sure that accidentally rendering the locking media inoperable can no longer happen.

ℹ As standard, it is possible to format MIFARE DESFire locking media.

If you change the standard settings, the deviating settings are saved on the locking media when:

- You **add** a new locking medium to OMEGA Client
- You **program** a locking medium (e.g. because authorisations have been changed, or similar)
- You **format**a locking medium

⚠ Please note: standard settings can be changed only **once** . As soon as different settings are saved on a locking medium, **it cannot be undone or overwritten! Therefore, the locking medium has to be replaced if you have changed or saved the settings by mistake.**

1. **In the main menu, click on** SETTINGS > OPTIONS**.**

   The window OPTIONS *opens.*

2. **In the menu item** OTHER **, click on** DESFIRE.

3. **If you activate the checkbox** ALLOW FORMATTING THE LOCKING MEDIUM **, MIFARE DESFire locking media can be formatted. If you deactivate the checkbox, this is no longer possible.**

4. **To save the settings, click on** OK**.**

   The settings have now been saved.

15.2 How to activate or deactivate Random-ID

⚠ The following setting cannot be **undone**, and therefore, only authorised persons may change it!

With MIFARE DESFire,**random IDs**can be sent instead of UID (UID 1) when the UID of the locking medium is requested. A different random UID is generated upon every request. This ensures that the UID cannot be read without authorisation. After authentication, UID 2 can be read.

ℹ The random ID function is deactivated as standard.

If you change the standard settings, the deviating settings are saved on the locking media when:

- You **add** a new locking medium to OMEGA Client
- You **program** a locking medium (e.g. because authorisations have been changed, or similar)
- You **format**a locking medium

⚠ Please note: standard settings can be changed only **once** . As soon as different settings are saved on a locking medium, **it cannot be undone or overwritten! Therefore, the locking medium has to be replaced if you have changed or saved the settings by mistake.**

⚠ Locking media which use the random ID function, can only be used with **V-NET locking devices** or **LINE-D locking devices** . **For further information, please refer to**

1. In the main menu, click on SETTINGS > OPTIONS**.**

The window OPTIONS *opens.*

2. In the menu item OTHER **, click on** DESFIRE**.**

3. If you activate the checkbox ACTIVATE RANDOM ID **, a random UID is sent instead of UID1.**

4. To save the settings, click on OK**.**

The settings have now been saved.

15.3 How to define a Master-Key

You can change the Master-Key settings if you are already using locking media of other manufacturers together with your system, and if these use Master-Keys or an encryption which differs from the pre-set ones. In this case, enter the encryption and the Master-Key for your system.

1. **In the main menu, click on** SETTINGS > OPTIONS**.**

   The window OPTIONS *opens.*

2. **In the menu item** OTHER **, click on** DESFIRE**.**

3. **In the** MASTER-KEY **view, select the encryption, and enter the key.**

4. **Click on OK.**

   The new settings have now been saved. You have to program all the system's locking devices to make the changes come into effect.

15.4 How to define the size of the authorisations file

ℹ The size of the authorisations file is only relevant for V-NET locking media.

ℹ The standard size of the authorisations file is 4,000 bytes.

With the size of the authorisations file you can define how much memory space is to be used for areas and individual authorisations (authorisations for individual locking devices) on a V-NET locking medium. This is useful if you are already using locking media of other manufacturers together with your system and if you need the memory space for additional tasks (e.g. an invoicing system for the staff restaurant).

1. **In the main menu, click on** SETTINGS > OPTIONS**.**

   The window OPTIONS *opens.*

2. **In the menu item** OTHER **, click on** V-NET**.**

3. **Click on** CALCULATE**.**

   The window OPTIONS *opens. Here, you can enter the number of areas and individual authorisations you are using, and you can have the necessary memory space on the locking medium calculated.*

4. **Enter the number of the areas and locking devices which exist in your system, and click on** OK**.**

   You will now be shown the size of the required memory space in SIZE OF THE AUTHORISATIONS FILE*.*

5. **Connect Desktop-Writer, and place one of your already existing locking media on top of it.**

6. **Click on** CHECK**.**

   You will receive a message whether the locking medium has the required memory space. You will also be informed how much additional memory space is available.

7. **Optional: if additional memory space is available, you can manually increase the size of the authorisations file.**

8. **Click on** OK**.**

   The new settings have now been saved. The new settings will be transferred to the locking media when

   - a new locking medium is being read in

   - a locking medium is being formatted

   - a locking medium is being converted

16 User administration

16.1 About the user administration

The **User administration** allows you to add or delete users to OMEGA Client. Creating users allows you to grant additional users access to OMEGA Client.

With **user profiles,** you can define the rights of individual users in OMEGA Client.

16.2 Working with the user administration

How to add or edit users

1. In the main menu, click on SETTINGS > USER ADMINISTRATION**.**

2. Click on NEW USER. **or on** EDIT USER**.**

The user editor opens.

3. Select the authorisations type:

Internal	Login data is internally saved in OMEGA Client.
Directory service	Login data is taken over from the directory service.

4. If you have selected the authorisations type “internal”:

Specify the LOGIN NAME **and** PASSWORD **of the new user.**

ⓘ Please pay attention to lower case and upper case letters.

ⓘ The login name has to contain the following characters only: a-z, A-Z, 0-9, # *
Other characters are not accepted in this input field.

4. If you have selected the authorisation type "directory service":

Enter the login name of the user which the user has in the directory service.

The fields of the password are hidden, because the password is taken over from the directory service. Therefore, you cannot change the password in OMEGA Client.

ⓘ The login name has to match exactly the login name of the directory service. Please pay attention to lower case and upper case letters.

5. Allocate one of the user profiles to the user.

ⓘ With **user profiles,** you can define the rights of individual users in OMEGA Client.

6. **In the field** NAME **, you enter the name of the user.**

7. **Click on** SAVE**.**

   If you have created a new user: the new user has now been saved, and using his/her login name and password, s/he can log into OMEGA Client immediately.

   If you have edited an existing user: should s/he still be logged in to OMEGA Client, the changes will come into effect when this user logs into OMEGA Client the next time.

How to delete users

1. **In the main menu, click on** SETTINGS > USER ADMINISTRATION**.**

2. **In the list, select the user you want to delete.**

3. **Click on** DELETE USER**.**

4. **Confirm the message.**

   Now, the user is deleted.

16.3 User profiles

16.3.1 About user profiles

With **user profiles,** you can define the rights of individual users in OMEGA Client.

You can enter user profiles at three different levels:

- Settings for access to **systems** (if you are operating more than one system)
- If you use the multi-client module: settings to access components and events **within one system**
- **Rights** associated with the user profile (e.g. “Add personal data", “Delete device data")

The system has to be closed to be able to define the settings for system access. The system has to be open if you want to define the settings to access components and events within a system. You can set the rights of a user profile irrespective of whether the system is closed or open.

16.3.2 The importance of the client module for user profiles

With the multi-client module, you can create even more detailed user profiles. You can determine which individual components of the system (devices, locking media, people, events, and time profiles) can be accessed by a user. In doing so, you can select whether e.g. a locking device is to be constantly hidden for certain users, or whether it is to be shown in read-only mode.

Example: the system belongs to a shopping mall. You manage the entire system, however, you want the individual shops to be able to access their locking devices. In the multi-client module, you can create user profiles for every shop, and you can define that every shop can exclusively see and edit its own locking devices. In addition, you can show e.g. the locking device at the main entrance to all the shops, and you can define that it is possible to add authorisations for it.

16.3.3 Working with user profiles

How to add or edit user profiles

1. **Close the system if you want to define the systems which the user profile should be allowed to access. In the main menu, click on** SYSTEM > CLOSE SYSTEM.
   If you want to define the components and events of a system which the user profile should be allowed to access (requires the multi-client module): open the system in question. In the main menu, click on SYSTEM > OPEN SYSTEM.
   You can define the rights of a user profile when the system is closed and when it is open.
2. **In the main menu, click on** SETTINGS > USER ADMINISTRATION**.**
3. **Click on** ADMINISTRATING USER PROFILES**.**
4. **Click on** NEW USER PROFILE **or** EDIT USER PROFILE**.**

   Now, you see the tab USER PROFILE.

The user profile tab

In the USER PROFILE tab, you define the name and the rights of the user profile. The modules (e.g. user administration, system administration, etc.) are shown to you in a tree structure. You can set the rights (e.g. view data, add data, etc.) for each module individually.

1. **Open the desired module (e.g.** UER ADMINISTRATION **or** DEVICES**) by clicking on the plus symbol.**
2. **Activate or deactivate the checkboxes for the desired rights (e.g.** VIEW DATA **or** EDIT DATA**).**

The system tab

ℹ You see the system tab only if you have closed the system in step 1.

You can use the SYSTEMS tab to define which systems the user profile can access. If no systems are listed in the SYSTEMS tab, the user profile can access all systems. As soon as you add systems to this list, the user profile can only access the systems on the list.

To restrict access:

1. Click on ADD**.**

2. Now, select the systems you want to add to the list.

3. Click on ADD**. If you do not want to add more of them, click on** CLOSE**.**

4. If you want to define that a user can see the selected system in his/her user profile, but cannot edit it, please activate the checkbox in the WRITE PROTECT **column.**

To revoke an access restriction:

5. Select the entry from the list, and click on REMOVE**.**
A user with this user profile can only access the systems added to the list. If the list is empty, access is not restricted.

The devices, locking media, time profiles, people and events tab

ℹ You see these tabs only if you have opened the corresponding system in step 1.

ℹ You can see these tabs only if you have the multi-client module.

These tabs allow you to define access to individual devices, locking media, time profiles, people, and event types in the corresponding tabs. If this list in the tab is empty, access is not restricted. As soon as you add an entry, such as a locking device in the DEVICES tab, the user with the corresponding user profile will be only shown this locking device, or any further devices you may add to this list.

1. Click on the corresponding tab.

To restrict access:

2. Click on ADD.
3. Select the device, locking medium, time profile, person, or events type you want to add to the list.
4. Click on ADD. If you do not want to add more of them, click on CLOSE.
5. If you want to define that a user can see the selected components in his/her user profile, but cannot edit it, please activate the checkbox in the WRITE PROTECT column.

ℹ Write-protect of event types means that users cannot add comments to this type of events.

To revoke an access restriction:

6. Select the entry from the list, and click on REMOVE.

A user with this user profile can view in OMEGA Client only the devices, locking media, time profiles, people and events types added to this list. If the list is empty, access is not restricted.

5. Click on SAVE to save the settings for the user profile.

If you have created a new user profile: the new user profile has now been saved. Now, you can allocate it to users in the USER ADMINISTRATION *.*

If you have edited a user profile: the changes have now been saved. The new settings come into effect after users have logged off and then into the Client with this user profile.

How to delete user profiles

ℹ User profiles can only be deleted if they are no longer allocated to a user.

1. In the main menu, click on SETTINGS > USER ADMINISTRATION.
2. Click on ADMINISTRATING USER PROFILES.
3. Select the desired user profile from the list.
4. Click on DELETE USER PROFILE.
5. Confirm the message with YES.

Now, the user profile is deleted.

17 Server settings

17.1 The Server configuration menu item in OMEGA Client

If you manage several systems on different servers, you can add the Server configuration menu item to add the servers you want to access with OMEGA Client.

With the << button, you can show or hide the list of the saved server IPs in the login window. If you are using various servers, you can quickly and easily select the desired server for login.

How to add the OMEGA Server for OMEGA Client

1. **In the main menu, click on** Settings > Server configuration**.**

   The window Configure OMEGA Server *opens.*

2. **Enter the IP address and the port of the OMEGA Server.**

   If the OMEGA Server is installed on the same PC than OMEGA Client, the IP address is 127.0.0.1.

3. **Click on** OK**.**

   If you have already been connected to OMEGA Server, the connection is established immediately, and you will see the login window of OMEGA Client.

   If OMEGA Client has not yet been connected to the server, you will be asked whether you want to test the connection.

4. **Click on** Yes **to test the connection.**

   The connection will be tested. The result will be shown in the window.

5. **Click on** OK **after the connection has been tested successfully.**

   OMEGA Client will now connect to the OMEGA Server, and you will see the login window of OMEGA Client.

17.2 The Server configuration tool (part of CEStronics Suite).

The OMEGA Server configuration has to be run on the same computer where the OMEGA Server is installed. It is not possible to connect to it externally.

General

OMEGA Service

Here, you can:

- view the status of the OMEGA Server
- start or stop the OMEGA Server
- link the OMEGA Server to a particular network card

start or stop the OMEGA Server

6. Close OMEGA Client.

7. Open the program OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**

8. Click on GENERAL > OMEGA SERVICE**.**

9.

a) If you want to stop the OMEGA Server, click on the STOP button.

In the STATUS *field, you will now see the message "is being stopped", and you see what kind of activities are currently being stopped. Wait until you see is the message "has been stopped" in the* STATUS *field. The OMEGA Server has now been stopped.*

b) If you want to start the OMEGA Server, click on the START button.

In the STATUS *field you will now see the message "is being started", and you see what kind of activities are currently being started. Wait until you see is the message "has been started" in the* STATUS *field. The OMEGA Server has now been started.*

link the OMEGA Server to a particular network card

The IP address is 0.0.0.0 as standard, which means that all existing network cards are being used. If you use more than one network card, you can link OMEGA Server to one of these network cards by setting the IP address of a certain network card.

1. Stop the OMEGA Server.

2. Open the program OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**

3. Click on GENERAL > OMEGA SERVICE**.**

Now, the OMEGA Server can be addressed only via the network card set.

Tasks

Here, you see the tasks, e.g. for the server communication with online devices. For instance, if you do not use a system, you can stop this task in order to decrease the CPU load. To do so, select the task on the list and click on STOP. With START you can re-start the task.

Database

Database

Here, you can view the current status of the OMEGA Server database. In order to test the connection to the database server, click on TEST CONNECTION.

How to use an external Firebird server for the OMEGA Server

You can operate the OMEGA Server with an external Firebird server. Performance will be improved if only the Firebird server is running on an (external) machine.

ℹ Even after an update of CEStronics Suite, all settings to be used for the external Firebird server are preserved.

⚠ Only experienced users or administrators should set up an external Firebird server.

1. Install Firebird server version 3.0.X on an external machine.

ℹ Please note:
- No virus scanner should be installed on the external machine.
- The external machine should not be a domain member.
- The firewall of the external machine should allow incoming and outgoing connections to be established via the Firebird ports. All other ports should be closed.

ℹ For the installation file, please refer to **http://www.firebirdsql.org/en/firebird-3-0**

2. Adapt the Firebird configuration file.

3. Adapt Firebird server.

4. Stop the OMEGA Server.

How to stop the OMEGA Server

1. **Close OMEGA Client.**
2. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
3. **Click on** GENERAL > OMEGA SERVICE**.**
4.

c) If you want to stop the OMEGA Server, click on the STOP button.

In the STATUS *field, you will now see the message "is being stopped", and you see what kind of activities are currently being stopped. Wait until you see is the message "has been stopped" in the* STATUS *field. The OMEGA Server has now been stopped.*

d) If you want to start the OMEGA Server, click on the START button.

In the STATUS *field you will now see the message "is being started", and you see what kind of activities are currently being started. Wait until you see is the message "has been started" in the* STATUS *field. The OMEGA Server has now been started.*

5. **In the** SERVER CONFIGURATION**, set the kind of server to "external".**

How to define the kind of server for the OMEGA Server

1. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
2. **In the navigation menu, click on** DATABASE > DATABASE**.**
3. **In the drop-down menu** KIND OF SERVER **, click on "Internal" or "External".**
4. **In the drop-down menu** SERVER VERSION **, select the server version.**
5. **Enter the IP address and the port.**
6. **If you have selected the "external" kind of server: enter the database alias, username, and password.**
7. **Click on** TEST CONNECTION**.**

   After the connection has been tested successfully, the new server is connected.

6. **Start the OMEGA Server.**

How to start the OMEGA Server

1. Close OMEGA Client.

2. Open the program OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**

3. Click on GENERAL > OMEGA SERVICE**.**

4.

e) If you want to stop the OMEGA Server, click on the STOP button.

In the STATUS *field, you will now see the message "is being stopped", and you see what kind of activities are currently being stopped. Wait until you see is the message "has been stopped" in the* STATUS *field. The OMEGA Server has now been stopped.*

f) If you want to start the OMEGA Server, click on the START button.

In the STATUS *field you will now see the message "is being started", and you see what kind of activities are currently being started. Wait until you see is the message "has been started" in the* STATUS *field. The OMEGA Server has now been started.*

Now, the OMEGA Server will be operated with the external Firebird server.

Import

If you change from CEStronics Suite 1 to CEStronics Suite 2, you can import the CEStronics Suite 1 database here.

How to import the CEStronics Suite 1 database into CEStronics Suite 2

⚠ The database import serves exclusively to migrate **CEStronics Suite 1** backups to **CEStronics Suite 2**!

You have to read in backups which have already been generated with CEStronics Suite 2 with the restore function in CEStronics Suite 2 (see "Recovering server backups" auf Seite131).

1. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
2. **In the navigation menu, click on** DATABASE > IMPORT**.**
3. **Select the database file you want to import (you can import the fdg and osb file formats).**

   Expert mode
   Importing large databases may take some time. If you activate the checkbox EXPERT MODE , you can shorten the time necessary for the import by excluding journal and events from the import. To do so, deactivate the corresponding checkboxes. If you activate the checkbox SHOW DIAGNOSTICS DATA , you will see detailed messages in the window.

4. **Click on** IMPORT**.**

   The database will now be imported.

Administration

Client management

Here, you can define which PCs are allowed to connect to the OMEGA Server.

How to limit access to the OMEGA Server

Which server do the access settings apply to?
If you exclude a PC from server access in OMEGA SERVER CONFIGURATION, access **to the server on which the** OMEGA SERVER CONFIGURATION **is running** will be prevented for this PC. A PC which has been excluded can no longer connect OMEGA Client to this particular OMEGA Server. However, the excluded PC can still connect to other OMEGA Servers.

1. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
2. **In the navigation menu, click on** ADMINISTRATION > CLIENT MANAGEMENT**.**
3. **You have two options:**

Permit all clients	Permits **all** PCs, irrespective of whether they are in the list or not
Permit client	**Only** permits those PCs which are on the list
Reject client	Only permits those PCs which are **not** on the list

4. **Click on** NEW**.**

   The window SET FEATURES *opens.*

5. **In** CLIENT **, enter the name or the owner of the PC. These details here are for your information purposes only and have no technical effect.**
6. **Here, you enter the** MAC ADDRESS **of the PC.**
7. **Click on** SAVE**.**
8. **Enter further PCs, or click on** ABORT**.**

   The PCs you have entered have now been added.

   Depending on the settings, the PCs in the list will now be permitted or excluded.

Backup management

The backup management allows you to generate automatic backups of the database.

1. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
2. **In the navigation menu, click on** ADMINISTRATION > BACKUP MANAGEMENT**.**
3. **Click on** NEW**.**

   The window CREATE TASK *opens.*
4. **In the** GENERAL **tab, enter a description for this automatic backup.**
5. **Select the desired storage location for the backup.**
6. **Open the** SCHEDULE **tab.**
7. **Now indicate when the first backup is to be generated.**
8. **Indicate how often automatic backups are to be generated after this start time.**
9. **Click on** SAVE**.**
10. **If you wish, you can set more automatic backups. When you have finished, click on** CANCEL**.**

    Now, you can view the generated automatic backups in the list. The backups are generated automatically at the indicated time.

Sessions

Client sessions

Here, you see all active tasks and connections of CEStronics Suite.

User sessions

Here, you can see which users are currently logged onto OMEGA Client, and you can log them off manually.

How to log off user from OMEGA Client

ℹ To log off users via the server configuration, OMEGA Client has to be closed.

1. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
2. **In the navigation menu, click on** SESSIONS > USER SESSIONS**.**
3. **Click the right mouse button on the user you want to log off, and in the context menu, click on** LOG OFF USER**.**
   Now, the user is logged off from OMEGA Client.

17.3 How to link the OMEGA Server to a particular network card

The IP address is 0.0.0.0 as standard, which means that all existing network cards are being used. If you use more than one network card, you can link OMEGA Server to one of these network cards by setting the IP address of a certain network card.

1. **Stop the OMEGA Server.**
2. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
3. **Click on** GENERAL > OMEGA SERVICE**.**
   Now, the OMEGA Server can be addressed only via the network card set.

17.4 How to limit access to the OMEGA Server

ℹ **Which server do the access settings apply to?**

If you exclude a PC from server access in OMEGA SERVER CONFIGURATION, access **to the server on which the** OMEGA SERVER CONFIGURATION **is running** will be prevented for this PC. A PC which has been excluded can no longer connect OMEGA Client to this particular OMEGA Server. However, the excluded PC can still connect to other OMEGA Servers.

1. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
2. **In the navigation menu, click on** ADMINISTRATION > CLIENT MANAGEMENT**.**
3. **You have two options:**

Permit all clients	Permits **all** PCs, irrespective of whether they are in the list or not
Permit client	**Only** permits those PCs which are on the list
Reject client	Only permits those PCs which are **not** on the list

4. **Click on** NEW**.**
   The window SET FEATURES *opens.*

5. **In** CLIENT **, enter the name or the owner of the PC. These details here are for your information purposes only and have no technical effect.**

6. **Here, you enter the** MAC ADDRESS **of the PC.**

7. **Click on** SAVE**.**

8. **Enter further PCs, or click on** ABORT**.**

   The PCs you have entered have now been added.

   Depending on the settings, the PCs in the list will now be permitted or excluded.

17.5 Server backups

17.5.1 About server backups

A **server backup** contains the entire database of the CEStronics Suite, i.e. systems, components, locking plan settings, etc. It is not necessary to save additional data. Server backups should be run on a regular basis. A backup can be imported if

- the current database is defective, and the OMEGA Server cannot be booted,
- the software is to be installed on a new PC, or
- the database has other defects.

17.5.2 Creating manual server backups

How to create a server backup

ℹ When a server backup is created, OMEGA Server must be running, which means it must not be stopped.

1. **Close OMEGA Client.**

2. **Open the program** OMEGA SERVER BACKUP **(part of CEStronics Suite).**

   A CMD window opens which executes the backup. Having completed the backup, the window will close automatically.

ℹ You will find the generated backup files (osb file format) in the database folder. Its location depends on the install location of CEStronics Suite, e.g. C:\Program Files\CEStronics 2\server\database.

17.5.3 Creating automatic server backups

How to create automatic server backups

The backup management in SERVER CONFIGURATION allows you to generate automatic, periodic backups of the database.

3. Open the program OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**

4. In the navigation menu, click on ADMINISTRATION > BACKUP MANAGEMENT**.**

5. Click on NEW**.**

The window CREATE TASK *opens.*

6. In the "General" tab, enter a description for this automatic backup.

7. Select the desired storage location for the backup.

8. Open the SCHEDULE **tab.**

9. Now indicate when the first backup is to be generated.

10. Indicate how often automatic backups are to be generated after this start time.

11. Click on SAVE**.**

12. If you wish, you can set more automatic backups. When you have finished, click on CANCEL**.**

Now, you can view the generated automatic backups in the list. The backups are generated automatically at the indicated time.

17.5.4 Recovering server backups

How to recover a server backup

⚠ Only experienced users or administrators should read in a server backup.

⚠ Do not import **CEStronics Suite 1** backups to **CEStronics Suite 2**in the way shown here! Backups from CEStronics Suite 1 have to be imported via SERVER CONFIGURATION, because they have to be processed so they can be used in CEStronics Suite 2 (see "How to migrate the CEStronics Suite 1 database into CEStronics Suite 2" auf Seite136).

ℹ To be able to carry out the following steps, OMEGA Server must be running, which means it is not to be stopped.

1. **Close OMEGA Client.**
2. **Open the folder which contains your server backup file (osb file format):**
   If you have created the backup with the OMEGA Server backup program, the file has automatically been saved in the database folder of CEStronics Suite. Its location depends on the install location of CEStronics Suite, e.g. C:\Program Files\CEStronics 2\server\database.
   If the backup has been created with the automatic backup management (in the OMEGA Server management tool), the file has been saved in the location you have defined.

   ℹ Backups contain a timestamp in their filename (OmegaServerDatabase_ ZEITSTEMPEL_.osb). You can identify the desired backup file with the timestamp.

3. **Rename the desired server backup file to "OmegaServerDatabase.osb".**

   ℹ By renaming it (that is to say, removing the timestamp), you define that this backup file is the file to be used by the OMEGA SERVER RESTORE program to restore the server. The other backup files remain unaffected by this process.

4. **Open the program** OMEGA SERVER RESTORE **(part of CEStronics Suite).**
   A CMD window opens which executes the recovery. Having completed the recovery, the window will close automatically.
   The recovery will create a file named RESTORE.OMEGA_SERVER_DATABASE.FB30 which you will find in the C:\Program Files\CEStronics 2\server\database folder.
5. **Open the database folder of CEStronics Suite. Its location depends on the install location of CEStronics Suite, e.g. C:\Program Files\CEStronics 2\server\database.**
   There, you will find two files with the fdb file format:
   OMEGA_SERVER_DATABASE.FB30 (=current server database)
   RESTORE.OMEGA_SERVER_DATABASE.FB30 (=recovery file for the server database)
6. **Now, stop OMEGA Server.**

How to stop the OMEGA Server

7. **Close OMEGA Client.**

8. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**

9. **Click on** GENERAL > OMEGA SERVICE**.**

10.

g) If you want to stop the OMEGA Server, click on the STOP button.
In the STATUS field, you will now see the message “is being stopped”, and you see what kind of activities are currently being stopped. Wait until you see is the message “has been stopped” in the STATUS field. The OMEGA Server has now been stopped.

h) If you want to start the OMEGA Server, click on the START button.
In the STATUS field you will now see the message “is being started”, and you see what kind of activities are currently being started. Wait until you see is the message “has been started” in the STATUS field. The OMEGA Server has now been started.

1. **Rename the current server database OMEGA_SERVER_DATABASE.FB30 e.g. to OMEGA_SERVER_DATABASE.FB30.DEFECTIVE.**

2. **Remove “RESTORE” from the filename of the recovery file, so that it is now named OMEGA_SERVER_DATABASE.FB30.**

3. **Start the OMEGA Server.**

How to start the OMEGA Server

4. **Close OMEGA Client.**

5. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**

6. **Click on** GENERAL > OMEGA SERVICE**.**

7.

i) If you want to stop the OMEGA Server, click on the STOP button.
In the STATUS field, you will now see the message “is being stopped”, and you see what kind of activities are currently being stopped. Wait until you see is the message “has been stopped” in the STATUS field. The OMEGA Server has now been stopped.

j) If you want to start the OMEGA Server, click on the START button.

In the STATUS field you will now see the message "is being started", and you see what kind of activities are currently being started. Wait until you see is the message "has been started" in the STATUS field. The OMEGA Server has now been started.

As soon as you see "started" in the STATUS field in the OMEGA SERVER CONFIGURATION program, the server backup has been read in, and recovery has successfully been completed.

17.6 How to use an external Firebird server for the OMEGA Server

You can operate the OMEGA Server with an external Firebird server. Performance will be improved if only the Firebird server is running on an (external) machine.

ⓘ Even after an update of CEStronics Suite, all settings to be used for the external Firebird server are preserved.

⚠ Only experienced users or administrators should set up an external Firebird server.

7. Install Firebird server version 3.0.X on an external machine.

ⓘ Please note:

- No virus scanner should be installed on the external machine.

- The external machine should not be a domain member.

- The firewall of the external machine should allow incoming and outgoing connections to be established via the Firebird ports. All other ports should be closed.

ⓘ For the installation file, please refer to **http://www.firebirdsql.org/en/firebird-3-0**

8. Adapt the Firebird configuration file.

9. Adapt Firebird server.

10. Stop the OMEGA Server.

How to stop the OMEGA Server

1. **Close OMEGA Client.**
2. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
3. **Click on** GENERAL > OMEGA SERVICE**.**
4.

k) If you want to stop the OMEGA Server, click on the STOP button.

In the STATUS field, you will now see the message "is being stopped", and you see what kind of activities are currently being stopped. Wait until you see is the message "has been stopped" in the STATUS field. The OMEGA Server has now been stopped.

l) If you want to start the OMEGA Server, click on the START button.

In the STATUS field you will now see the message "is being started", and you see what kind of activities are currently being started. Wait until you see is the message "has been started" in the STATUS field. The OMEGA Server has now been started.

11. **In the** SERVER CONFIGURATION**, set the kind of server to "external".**

How to define the kind of server for the OMEGA Server

1. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
2. **In the navigation menu, click on** DATABASE > DATABASE**.**
3. **In the drop-down menu** KIND OF SERVER **, click on "Internal" or "External".**
4. **In the drop-down menu** SERVER VERSION **, select the server version.**
5. **Enter the IP address and the port.**
6. **If you have selected the "external" kind of server: enter the database alias, username, and password.**
7. **Click on** TEST CONNECTION**.**

   After the connection has been tested successfully, the new server is connected.

12. **Start the OMEGA Server.**

How to start the OMEGA Server

1. Close OMEGA Client.

2. Open the program OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**

3. Click on GENERAL > OMEGA SERVICE**.**

4.

m) If you want to stop the OMEGA Server, click on the STOP button.

In the STATUS field, you will now see the message “is being stopped”, and you see what kind of activities are currently being stopped. Wait until you see is the message “has been stopped” in the STATUS field. The OMEGA Server has now been stopped.

n) If you want to start the OMEGA Server, click on the START button.

In the STATUS field you will now see the message “is being started”, and you see what kind of activities are currently being started. Wait until you see is the message “has been started” in the STATUS field. The OMEGA Server has now been started.

Now, the OMEGA Server will be operated with the external Firebird server.

17.7 How to migrate the CEStronics Suite 1 database into CEStronics Suite 2

⚠ The database import serves exclusively to migrate **CEStronics Suite 1** backups to **CEStronics Suite 2**!

You have to read in backups which have already been generated with CEStronics Suite 2 with the restore function in CEStronics Suite 2 (see "Recovering server backups" auf Seite131).

1. Open the program OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**

2. In the navigation menu, click on DATABASE > IMPORT**.**

3. Select the database file you want to import (you can import the fdg and osb file formats).

Expert mode

Importing large databases may take some time. If you activate the checkbox EXPERT MODE , you can shorten the time necessary for the import by excluding journal and events from the import. To do so, deactivate the corresponding checkboxes. If you activate the checkbox SHOW DIAGNOSTICS DATA , you will see detailed messages in the window.

4. Click on IMPORT**.**

The database will now be imported.

18 Troubleshooting

18.1 Server problems

Connecting to the OMEGA Server not possible

If you cannot connect to the OMEGA Server, please proceed as follows:

1. **If the OMEGA Server is not installed locally on your PC, but rather is on an external server: check whether the external server is running.**
2. **Check whether the OMEGA Server is running.**

1. **Open the** OMEGA SERVER CONFIGURATION **program (via** START MENU > ALL PROGRAMS > OMEGA > OMEGA SERVER CONFIGURATION**).**
2. **Check whether you can see “has been started” in the** STATUS **field. This means that the OMEGA Server is running.**

If the STATUS field does not show “has been started”:

3. **Close OMEGA Client.**
4. **In the** OMEGA SERVER CONFIGURATION **program, click on the** START **button.**

   The OMEGA Server will now be started.

ℹ If you cannot start the OMEGA Server, please contact CES Service.

3. **Check whether you are using the correct server IP when logging in.**

1. **Open OMEGA Client.**
2. **If the login window is shown, click on** ABORT**.**
3. **In the navigation menu, click on** START > SERVER CONFIGURATION**.**
4. **Enter the IP address of the OMEGA Server.**
5. **Click on** OK**.**

   The connection will be tested. After the connection has been tested successfully, you will see the login window.

   Now, you are successfully connected to the selected server.

ℹ If you cannot connect to the Server, please contact CES service.

18.2 Problems when logging into OMEGA Client

18.2.1 Message: max. number of users exceeded

The maximum number of users who can be logged into OMEGA Client at the same time is determined by the licence. Ask a user to log off. You can log off users via the SERVER CONFIGURATION program.

How to log off users via the SERVER CONFIGURATION **program**

ⓘ To log off users via the server configuration, OMEGA Client has to be closed.

1. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
2. **In the navigation menu, click on** SESSIONS > USER SESSIONS**.**
3. **Click the right mouse button on the user you want to log off, and in the context menu, click on** LOG OFF USER**.**

   Now, the user is logged off from OMEGA Client.

18.2.2 Message: user is already logged in

If you have not been logged off correctly after the last session (e.g. the program crashed) it might be that you are still logged on when you try to log on the next time. Wait some minutes. After some time, you are logged off automatically. You can also immediately log off manually via the SERVER CONFIGURATION program.

How to log off users via the SERVER CONFIGURATION **program**

ⓘ To log off users via the server configuration, OMEGA Client has to be closed.

1. **Open the program** OMEGA SERVER CONFIGURATION **(part of CEStronics Suite).**
2. **In the navigation menu, click on** SESSIONS > USER SESSIONS**.**
3. **Click the right mouse button on the user you want to log off, and in the context menu, click on** LOG OFF USER**.**

   Now, the user is logged off from OMEGA Client.

19 FAQs

How can I read events from a locking medium?

Events are automatically read and sent to OMEGA Server by Key-Points and wall terminals. When locking media are programmed with a Desktop-Writer, events are not automatically read; however, you can start the import manually.

How to import events with a Desktop-Writer

With IMPORT EVENTS, you can read events saved on a V-NET locking medium and import them into OMEGA Client. After the import, the events will be deleted from the locking medium memory.

1. **Connect Desktop-Reader or Desktop-Writer.**
2. **Place the locking medium whose events you want to import on top of the Desktop-Reader or Desktop-Writer.**
3. **In the navigation menu, click on** REPORTS > EVENTS**.**
4. **In the** EVENTS **view, click on** IMPORT EVENTS**.**

   Now, the events will be imported into OMEGA Client and will subsequently be deleted from the locking medium.

After the events have been read, they are saved in REPORTS > EVENTS.

ℹ Events are only saved on V-NET locking media, not on MIFARE locking media.

I have accidentally deleted events. Can I restore them?

OMEGA Client saves the timestamp of the last transmitted event for every locking device. This timestamp is preserved even if you delete events from OMEGA Client. When events are transferred next time, only the events which occurred after the timestamp are transferred.

If you want to restore events which happened before the timestamp, you have to delete the locking device and add it again. This deletes the timestamp, and every event stored in the locking device is transferred to OMEGA Client.

When locking devices are programmed, events are no longer transmitted to OMEGA Client. What could the reason be?

1. Check whether you have de-activated the checkbox READ OUT EVENTS in the PROGRAMMING DEVICE window. Tick the checkbox, so events at the locking devices are transmitted also during programming.

2. If you only receive system events but no access events: check whether you have activated the checkbox ACCESS EVENTS in SETTINGS > SERVICES. If this checkbox is de-activated, the locking device is configured in such a way that no access events are saved in it. If you want to change it, send a change order to CES using the SERVICES window.

How can I see how many locking devices and media there are?

In the navigation menu, click on SYSTEM > SYSTEM. You can now see in the view how many locking media, locking devices, and administration devices exist in the system in total.

Where do I find technical information about my existing locking devices, such as safety class, article number, weather resistance, etc.?

You find technical information you need e.g. for orders or follow-up orders in the locking device editor in the INFORMATION tab.

20 Battery management

20.1 Battery warning system

You can receive **battery warnings automatically by email** notification.

Battery status in OMEGA Client

In the device list in the column BATTERY STATUS you see a symbol which indicates the battery status and the time when this status was updated.

The battery status is automatically updated in OMEGA Client in the following conditions:

LINE - Offline	• During each programming with the RF-Stick
LINE - Online	• During each programming with the RF-Stick • During each communication of the locking device with the Access-Point
V-NET	• During each programming with the RF-Stick • When battery status events from locking media are transmitted to **OMEGA Client**

Battery warnings of the locking device

When the battery power becomes weak, the locking device displays additional signals if

- authorised or unauthorised locking media were held in the reading field of the locking device or
- the locking device couples, e.g. after the release or emergency mode was activated.

These additional signals are the **battery warnings**.

The battery capacity always depends upon the discharge so far and the current temperature.

20.1.1 Warning levels of the battery warning system in OMEGA Client and the locking device

⚠ Lock-out risk: The door can no longer be opened when the batteries are empty. The remaining battery life depends on **many different factors**. Therefore, replace the battery immediately **at warning level 1**!

Warning levels for all locking devices to firmware 3.4.x

Battery status in OMEGA Client		Signalling at the locking device	Required action
🟩 Green	OK	None	
🟨 Yellow	Warning level 1	👁 🟥	Replace the battery immediately
🟧 Orange	Warning level 2	👁 🟥🟥	Replace the battery immediately
🟧 Orange-red	Warning level 3	👁 🟥🟥🟥	Replace the battery immediately
🟥 Red	Critical	Locking device is off	Replace the battery immediately

Warning levels for electronic cylinders from firmware 3.5.14

From firmware 3.5.14, battery warnings were set back from 3 levels to 1 level. There is only *one* warning level which means: change the batteries! This change applies to electronic cylinders in the first isntance, but will also apply to electronic handle sets in the future.

Battery status in OMEGA Client		Signalling at the locking device	Required action
🟩 Green	OK	None	
🟧 Orange-red	Battery low	👁 🟥	Replace the battery immediately
🟥 Red	Battery empty	Locking device is off	Replace the battery immediately

20.2 Battery replacement

In the device list in the column entitled BATTERY REPLACEMENT you see the point in time when this status was updated. You have to set this time manually. If you have set a date for the battery replacement, the battery status of the device will automatically switch to "OK".

ℹ It is recommended that the date of the battery replacement be documented. This way you can trace the frequencies at which the batteries of the various locking devices of your system need to be changed, because battery consumption depends on many **different factors**.

Documenting the battery replacements helps to prevent obsolete battery warning in OMEGA Client. If a V-NET locking medium has saved a battery warning as an event *before* the battery was replaced, and this event was read in OMEGA Client *after* the batteries were replaced, setting the battery replacement will lead to an “OK” of the battery status, and the warning will be ignored.

Setting the point in time for battery replacement

1. **In the view, click with the right mouse button in** DEVICES **or in the** LOCKING PLAN **on the device desired.**

   The context menu opens.

2. **In the context menu, click on** SET BATTERY REPLACEMENT**.**

3. **Please confirm.**

   Now, the battery status has been set to "OK". The time of the battery replacement will be shown in the BATTERY REPLACEMENT *column.*

20.2.1 Notice on battery replacements

- Replace the batteries in accordance with a predefined maintenance schedule.

- Check the batteries every six months, and replace them if necessary. Depending on the use of the locking device and the climate, the maintenance interval could be shorter.

- Procure spare batteries in a timely manner. Only use the battery types indicated.

We recommend to read the device status and test the locking device functions every time the batteries were replaced.

Reading the device status

1. **Click on the** PROGRAMMING DEVICE **view.**

   The window PROGRAMMING DEVICE *opens.*

2. **Connect the RF-Stick to your PC.**

   Now you see the serial number and the current firmware version of the RF-Stick.

3. **If you deactivate the** READ EVENTS **checkbox, results are not read and the device status can be transferred more quickly.**

   If you deactivate the checkbox, events will not be transferred to OMEGA Client during future device programming, either. IIf you only want not to read the events in this one process, re-activate the checkbox after completion of the process.

4. **Establish communication between the locking device and the RF-Stick (same procedure as for programming with an RF-Stick). This does not require programming jobs.**

Programming via RF-Stick.

Required master media and administration devices:

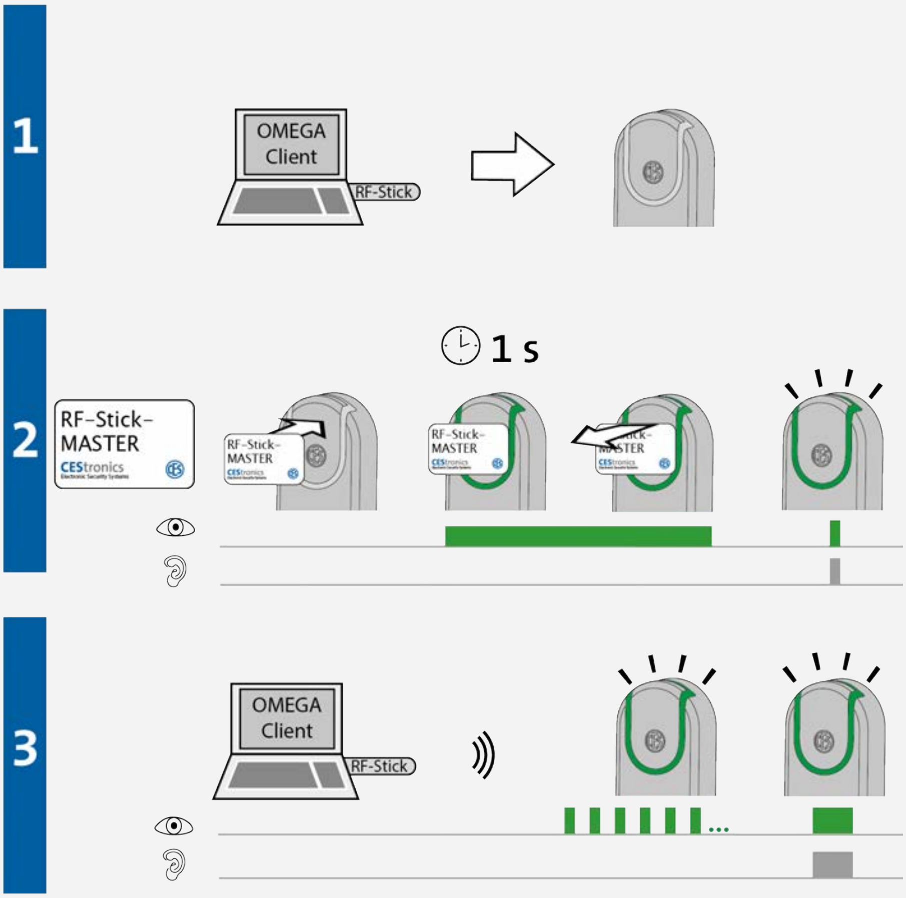
- RF-Stick-Master
- RF-Stick
- PC with OMEGA Client installed

The RF-Stick-Master must first be authorised for all locking devices with which it is to be used, (siehe "Weitere Master-Medien für Schließgeräte berechtigen" auf Seite 1). Each RF-Stick-Master that has been authorised once is compatible with every RF-Stick of an OMEGA FLEX system.

Procedure for creating programming jobs:

5. **Start the OMEGA Client and log in with your user name and password.**
6. **Set the desired changes in the OMEGA Client.**
7. **Start your changes accordingly as a change programming or new programming, e.g. through** PROGRAMMING > PROGRAM ALL CHANGES.
   The status display of the OMEGA Client shows now "programming required". The individual programming jobs are shown under “Programming status”.

Procedure for transmitting programming jobs via an RF-Stick:



1. **Proceed with your PC and the RF-Stick connected to it to the locking device into which the program is to be transmitted.**

   If you want to transmit the programming jobs into multiple locking devices, you can freely choose the sequence in which you look for the locking devices.

2. **Hold the RF-Stick-Master briefly before the reading field of the locking device.**

   The following signal appears:

   1x short green and 1x short beep

3. **The locking device now searches for an RF-Stick nearby.**

   The distance between the locking device and the RF-Stick may not exceed ten meters.at the maximum.

   As soon as the RF-Stick has been detected, the transmission begins. During transmission, the locking device flashes green.

During transmission the following occurs:

- All programming jobs for this locking device are transmitted to this locking device. During programming, the programming status display shows the progress in percentage.

- All events stored in the locking device, which were not available to the OMEGA Client yet, will be copied into the OMEGA Client.

- The clock is set.

ℹ If no programming jobs are available, only the events are copied and the clock is set. In this case, the locking device does not flash during the transmission.

After transmission of all data, the RF-Stick and the locking device are disconnected automatically. After transmission completion, the programming job is deleted from the "Programming status" list.

The programming job transmission is completed when the locking device signals 1x long green and 1x long beep.

Troubleshooting:

Signalling	Reason	Solution
During step 2:		
👁 🟥 👂 ■	The locking device cannot detect any RF-Stick nearby.	Move with a properly connected RF-Stick closer to the locking device and try to transmit the programming jobs once again.

In the PROGRAMMING DEVICE *window, you can now find detailed information on the device status, among other things:*

Firmware	The currently installed firmware version
Time	The current time of the locking device
Battery	The battery status of the locking device
Locking device status	Shows the information whether a mode, e.g. the block mode or release mode, is active

ℹ The programming in the locking device memory is maintained even when the batteries have been removed.

After removal of the battery, the date and time are maintained for about ten minutes. If the battery is taken out for longer period, the date and time must be set again.

Detailed instructions on how to change batteries can be found in the manual of the corresponding locking device.

20.3 Battery consumption

Battery consumption depends, amongst other things, on the following factors:

Quality and capacity	The higher the battery quality and capacity, the longer the batteries will last.
Ambient temperature	Battery consumption increases when the ambient temperature is low.
Beeper	Battery consumption increases when the beeper is switched on.
Double beep additional function when decoupling	The beeper is used twice as much, which increases the battery consumption.
Confirmation	Battery consumption increases with an increased device usage.
Wake-up interval	A shorter wake-up interval increases battery consumption, because the radio function is switched on more often.
Wake on Radio	This standby function (constant search for radio signals) increases battery consumption dramatically.
Faulty radio reception/wireless coverage not properly installed	Frequent interruption of the radio link leads to frequent connection attempts, which increase battery consumption.

20.4 How to set standard values for the battery consumption

With OPTIONS , you can set standard values for all locking devices of your system which affect the battery consumption.

You can change these standard values individually for each locking device.

1. In the main menu, click on SETTINGS > OPTIONS**.**

The window OPTIONS *opens.*

2. **Click on** ENERGY-SAVING MEASURES > GENERAL**.**

3. **Activate the checkbox "Apply measures to new devices"**

   Activating this checkbox has two effects:

   - If you open the context menu for a locking device in the devices list, you will find the new menu item "Apply energy-saving measures".

   - If you add a new locking device, the standard values which you have set will be proposed as initial values. However, you can change them manually.

4. **Select the desired settings:**

	Measure to extend battery life:
Wake-up interval	Select a long wake-up interval
Beeper	Off
Wakeup-On-Radio	Off
Double beep when decoupling	Off

5. **Click on** OK**.**

6. **To apply the standard values to one or mmore locking devices, mark one or more locking devices in the** DEVICES **view.**

7. **Open the context menu with the right mouse button, and select** APPLY ENERGY-SAVING MEASURES**.**

   Now, the changes are set in the change log.

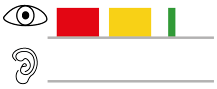
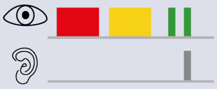
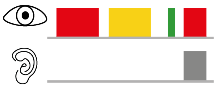
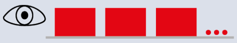
⚠ A locking device has to be programmed so that a change can come into effect (see "Programming changes" auf Seite90).

20.5 Battery types

		System	Released battery type	Service of the batteries at 20° C	Number of batteries
	Electronic cylinder	OMEGA FLEX	Panasonic CR2 Industrial Lithium 3,0 V 850 mAh	approx. 40,000	1*
	Long shield ILS	OMEGA FLEX	Energizer Ultimate Lithium 1,5V AA	approx. 100,000	2
	Smart shield SIS	OMEGA FLEX	Energizer Ultimate Lithium 1,5V AAA	approx. 80,000	2

**for dual cylinders, 2 batteries*

20.5.1 Signalling after battery insertion

Signalling	Meaning
	Start sequence for offline locking devices: No error
	Start sequence for online locking devices: Device is online and is connected to the Access-Point
	Start sequence for online locking devices: Device is online but no connection to Access-Point is possible
	Firmware error. Execute a firmware update. If the problem persists, contact your CEStronics partner.

In case a system error exists, it will be displayed immediately after the start sequence, siehe "Fehlersignalisierungen" auf Seite 1.

21 System requirements at a glance

21.1 System requirements of CEStronics Suite

To use CEStronics Suite, you need:

	✓
PC and accessories	
Up-to-date PC (desktop PC, notebook) with operating systems Windows 7™, Windows 8™, Windows Server 2008™, Windows Server 2012™ ℹ CEStronics Suite is a 32-bit application. It supports both 32-bit and 64-bit operating systems.	
Processor recommendation: • Small systems with up to 25 devices/100 media, e.g. Intel N3710 • Medium-sized systems with up to 100 devices, e.g. Intel i3 • Systems with up to 500 devices, Intel i5 • All bigger systems: Intel i7	
RAM Client: at least 2 GB RAM, 4 GB recommended Server RAM: 4 GB RAM free	
At least 100 GB free hard disk space	
CD-ROM drive or USB port to install the CEStronics Suite from the disc	
Network card with TCP/IP protocol.	
Browser (to install the CEStronics Suite from the installation menu)	
One free USB port (for using the RF-Sticks and/or Desktop-Readers or Desktop-Writers)	
Screen with at least 1024 x 768 pixel resolution	
Infrastructure	
Internet browser and Internet connection to use the OMEGA quick support (optional)	
Existing, functioning TCP/IP network (only if you want to use online devices)	

21.2 System requirements of wireless online networks

Network prerequisites for wireless online networks

A wireless online network consists of Access-Points embedded in a physical IP network. The locking devices communicate wirelessly with the Access-Points (868 MHz).

Important information on the network

You require

- a physical LAN network working with IPs (no VLAN).
- an IP address range which can be defined at your discretion (no DHCP address).
- an up-to-date server system which is permanently operating, to receive and send data. The server system must be physically embedded into the network (no Wi-Fi).

Important information on Access-Points

Device	Maximum range
Access point	25 m
Access-Point with outdoor antenna	40 m
Repeater	extends Access-Point range by 25 m.

Notes on how to install Access-Points:

- The server (Remote) has to allocate an IP address to the Access-Point.
- You have to set a subnet mask device for the Access-Point.
- You have to set a Gateway IP.

22 Index

Teaming up for security
since 1840

C. Ed. Schulte GmbH
Zylinderschlossfabrik
Friedrichstraße 243
D-42551 Velbert
☎ +49 2051 204 0
📠 +49 2051 204 229
ⓔ info@ces.eu

CESnederland B.V.
Lage Brink 9
NL- 7317 BD Apeldoorn
☎ +31 55-52 66 89 0
📠 +31 55-52 66 89 9
ⓔ infonl@ces.eu

CESfrance SARL
8 Impasse Charles Petit
F-75011 Paris
☎ +33 1 44 87 07 56
📠 +33 1 43 07 35 78
ⓔ info@fr.ces.eu

CESitalia srl
V. d. vecchie Fondamenta, 4
Straße d. A. Gründungen 4
I-39044 Egna / Neumarkt (BZ)
☎ +39 0471 812 294
📠 +39 0471 812 294
ⓔ info@it.ces.eu

CESrom srl.
Str. Metalurgistilor 3 D
RO-550137 Sibiu
☎ +40 269-206 00 2
📠 +40 269-206 00 5
ⓔ info@ro.ces.eu

United Kingdom
CES Security Solutions Ltd.
Unit 4 Kendon Business Park
Maritime Close, Medway City Estate
Rochester, Kent ME2 4JF
☎ +44 1 634713369
📠 +44 1 634786833
ⓔ info@uk.ces.eu

Middle East
A.G.P Advanced German Products LLC
PO Box 102761,
UAE Dubai
☎ +971 4 885 7050
☎ +971 4 369 7051
📠 +971 4 390 8935
ⓔ info@agp-dubai.com

Austria
Cesar A.Carcamo
Office: Wiener Bundesstrasse 33
A-4050 Traun
☎ +43 660-73 20 311
📠 +43 732-21 00 22 2681
ⓔ office@ces.at

Belgium
Locking Systems
Guy Lambrechts
Van Haeftenlaan 10
BE-2950 Kapellen
☎ +32 497 946267
ⓔ guy.lambrechts@lockingsystems.be

Spain
Benidorm Locks S.L.
Av. Marina Baixa s / n
Partida Torrent
ES-03530 La Nucia, Alicante
☎ +34 96 689 79 79
📠 +34 96 689 79 78
ⓔ info@benidormlocks.com