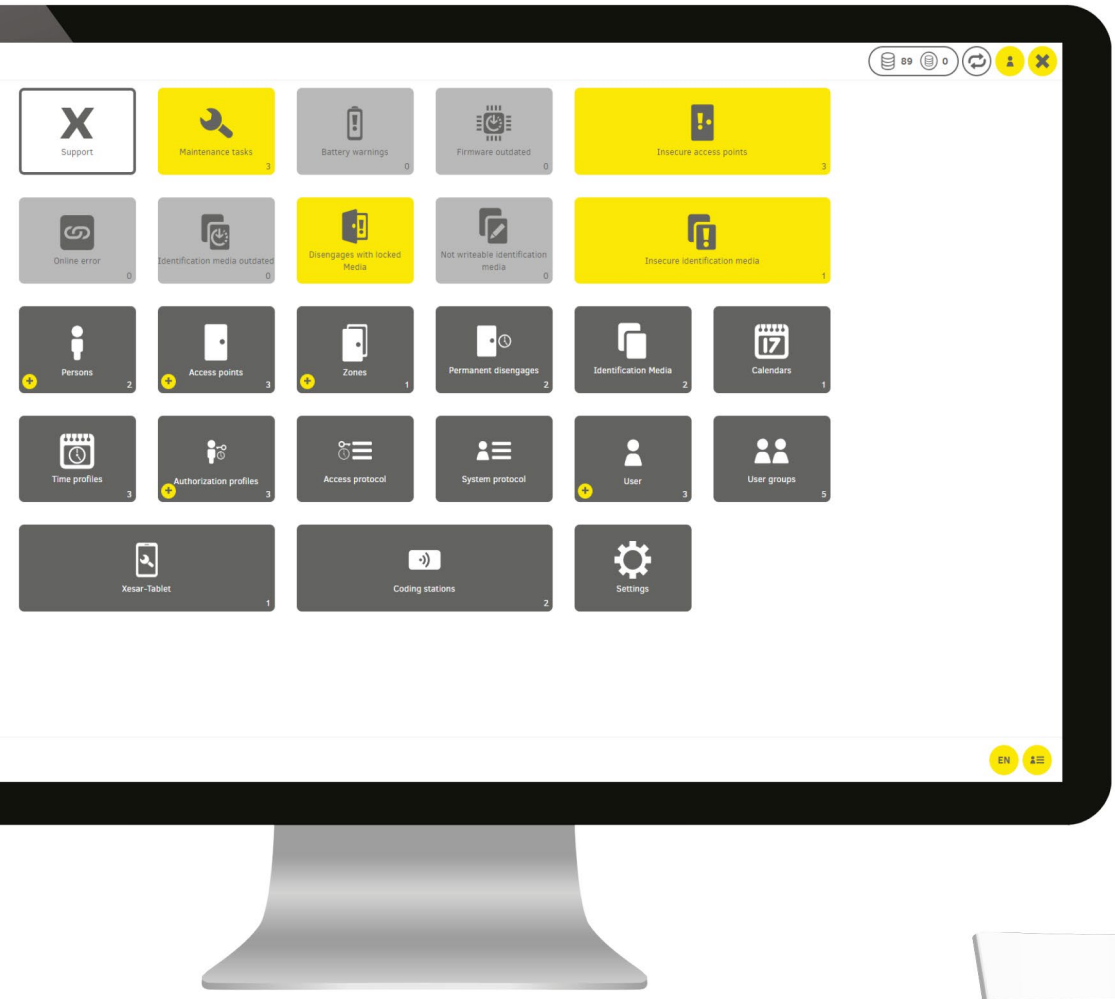


Xesar

Installation Instructions
Windows Server 2019 Datacenter Hypervisor

Imprint

Product code: I.X.3-2-HYPV.AN.INST.SEN.LN

Version: Xesar 3.2 | 3.2.x
Edition: 06/2024 UK
The original operating manual was written in German.

Publisher
EVVA Sicherheitstechnologie GmbH

Responsible for content
EVVA Sicherheitstechnologie GmbH

This edition shall not longer be valid upon publication of a new system manual.

You can find the latest edition in the EVVA download area:

https://www.evva.com/uk-en/service/downloads/

This manual is based on the state of the art at the time of creation. The content of the manual has been checked for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. We shall not assume any liability for technical or printing errors and their potential consequences. However, the data in this system manual is revised regularly and corrections are incorporated.

Table of contents

1 Introduction

This document is an excerpt from the Xesar 3.1 system manual.

The products and/or systems described in the Xesar system manual must exclusively be operated by persons that have been adequately qualified for the corresponding task. Qualified personnel is able to identify risks when handling products/systems and prevent potential hazards on the basis of their expertise.

1.1 General legal notes

EVVA shall conclude the contract for the use of Xesar on the basis of the EVVA GTC (General Terms and Conditions) and EVVA GTC (General Terms and Conditions) for the software for the product.

You can call up the EVVA General Terms and Conditions and EVVA General Terms and Conditions:

❯ **https://www.evva.com/uk-en/legal-notice/**

Please note that the use of the Xesar locking system may trigger legal obligations, in particular data protection authorisation, reporting and registration obligations (e.g. when setting up an information network system), as well as employee co-determination rights when used in companies. The user shall bear the responsibility for the legally compliant use of the product.

The above information must be observed in accordance with the manufacturer's liability for its products as defined in the Product Liability Act and must be communicated to operators and users. Non-compliance releases EVVA from any liability.

Unauthorised use, repair work or modifications not authorised by EVVA and improper service may lead to malfunctions and must therefore be avoided. Changes not expressly approved by EVVA will result in the loss of liability, warranty and separately agreed guarantee claims.

Keep the system components away from small children and pets. Risk of suffocation due to small parts that can be swallowed.

EVVA provides **architects and consulting institutions** with all the product information they need to comply with their information and instruction obligations under the Product Liability Act.

Specialist retailers and installers must comply with the information in EVVA documentation and they must pass on such information to customers, where applicable.

Additional information can be found in the Xesar product catalogue:

› **https://www.evva.com/uk-en/xesar**

1.2 EVVA Support

With Xesar, you have a sophisticated and tested locking system at your disposal. If you require additional support, please contact your EVVA partner directly.

You can access the list of certified EVVA Partners here:

› **https://www.evva.com/uk-en/retailer-search/**

Activate the “Electronics Partner” filter option to search specifically for EVVA partners who sell electronic EVVA locking systems and have qualified specialist knowledge.

› **http://support.evva.at/xesar/en/**

General information on Xesar can be found here:

› **https://www.evva.com/uk-en/xesar**

1.3 Explanation of symbols

The following symbols are used in the system manual to support illustration:

Symbol	Meaning
	Attention, risk of material damage in the event of non-compliance with the corresponding safety measures
	Notices and additional information
	Hints and recommendations
	Avoidance of errors or error messages
Option	Options
	Links
	Steps with instructions for action

2 Installation Instructions Windows Server 2019 Datacenter Hypervisor

You will find information below on how to prepare the Xesar 3.2 installation on a Windows server that uses the Windows Server 2019 Standard operating system versions or Datacenter as hypervisor.

The creation of the necessary IT and server environment is not part of these installation instructions. These must be provided by the customer and is not the responsibility of EVVA.

» Check the system requirements for Xesar 3.2. **Before installation, you must confirm that the system requirements for Xesar 3.2 are met in accordance with the project checklist and system manual.**

Follow the current project checklist from EVVA:

› **https://www.evva.com/uk-en/xesar**

We strongly recommend that the Xesar 3.2 installation is only carried out in close cooperation with the customer's responsible IT administrator.

2.1 Requirements

A physical server is setup with Microsoft Windows Server 2019 and configured as a hypervisor. On this a VM with current Ubuntu LTS server is installed on which Docker with Xesar 3.2subsequently runs.

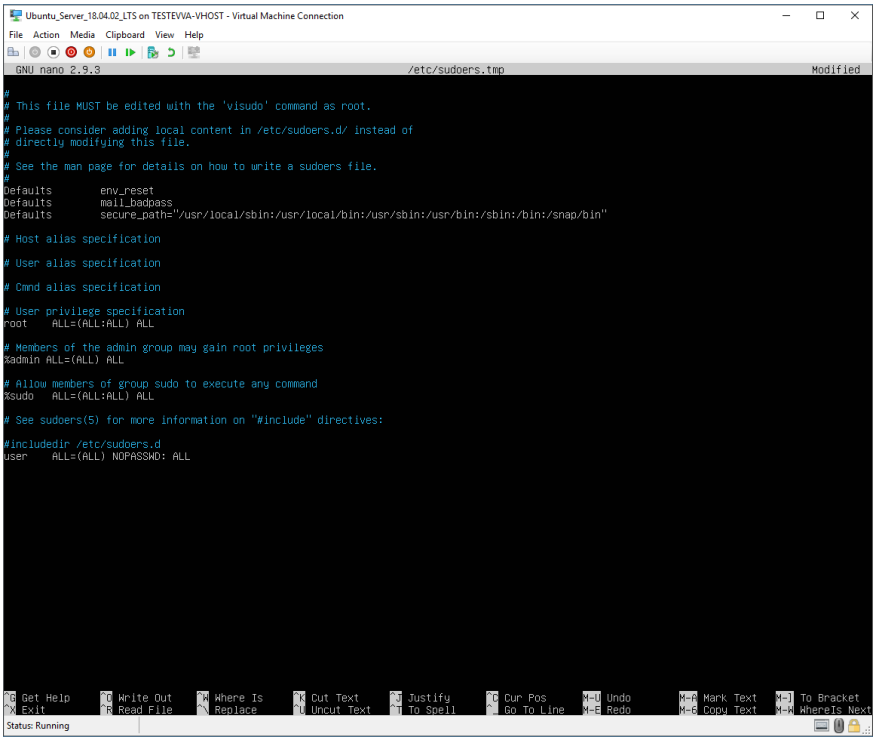
The following requirements must be met for a successful installation of Xesar 3.2 on a server running the Windows Server 2019 operating system:

- A physical server with an installed Windows Server 2019 / Datacenter operating system, from version 1607
- Configuration as hypervisor for VM (virutal machine) for Ubuntu LTS Server for Docker
- The user (customer) has Windows Server and network administration expertise
- The user (customer) has local administration rights
- There is an existing DHCP service (Dynamic Host Configuration Protocol)
- The Server time zone is set to UTC (Coordinated Universal Time)
- A Hyper-V support must be available, as well as a virtual switch with connectivity and access to the Internet
- Internet access must be available (Docker Trusted Registry with Notary Service and Licence Service, Port 443, 4443, 8072)
- The driver for the coding station must be installed, if necessary (HID Omnikey 5422 is usually detected automatically)

Due to the resource availability associated with the Windows Server, we recommend 16 GB (min. 8 GB) for the physical server. The VM requires at least 4 GB of memory.
As a general rule, the larger the system and the more people / traffic and online wall reader, the more memory should be available.

2.2 Set up Ubuntu

- Enter command **sudo visudo** for the password prompt for sudo
- At the following line to the end of the file that has now opened:
  user ALL=(ALL) NOPASSWD: ALL
- Replace the underlined word with the name of the user specified during the installation



- Save file (Ctrl+O and then ENTER)
- Close file (Ctrl+X)

- Create SSH key pair with **ssh-keygen** command. Name and password can be left blank - confirm with ENTER

```
shqadmin@ubuntumax:~$ ssh-keygen -t ecdsa -b 521
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/shqadmin/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shqadmin/.ssh/id_ecdsa
Your public key has been saved in /home/shqadmin/.ssh/id_ecdsa.pub
The key fingerprint is:
SHA256:Y/IE6YgmH6qzn/Qh1ync9LTBlyBoyhT/ODri0DvTvPs shqadmin@ubuntumax
The key's randomart image is:
+---[ECDSA 521]---+
|  .              |
|   o . .         |
|  . + + .        |
| o + = + . .     |
|. * + = S o      |
| * + = O =       |
|+ Bo= + +        |
|=ooBoo           |
```

- Add the SSH Public Key to the authorised keys:
  - **cd /home/user/.ssh/**
  - **cat id_ecdsa.pub > authorized_keys**
    cat id_ed25519.pub > authorized_keys
- Replace the underlined word with the name of the user specified during the installation

```
shqadmin@ubuntumax:~$ cd /home/shqadmin/.ssh
shqadmin@ubuntumax:~/.ssh$ cat id_ecdsa.pub > authorized_keys
```

2.3 Install Ubuntu updates

Download and install the latest updates and then restart with the following commands:

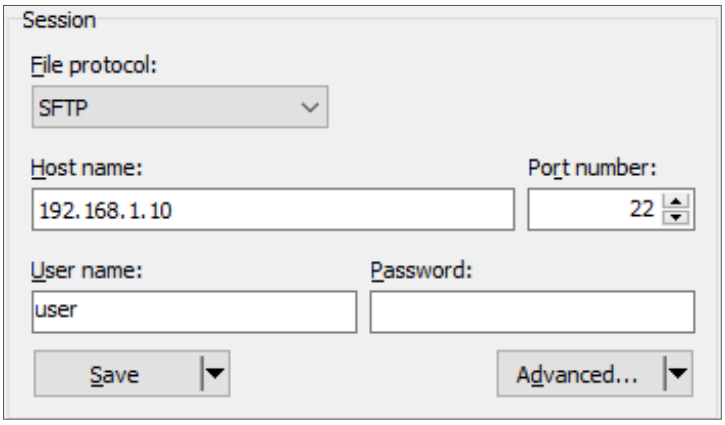
- **sudo apt-get update**
- **sudo apt-get upgrade**
- **sudo apt-get dist-upgrade**
- **sudo apt-get autoremove**
- **sudo reboot now**

2.4 Set up Windows 10 Pro Administrator PC

» Download and install WINSCP (Windows Secure Copy) to transfer the SSH key

› https://winscp.net/eng/download.php

» Start WINSCP
To do this, you will need the computer name, port, usernames and the password of the Ubuntu server that was previously set up.



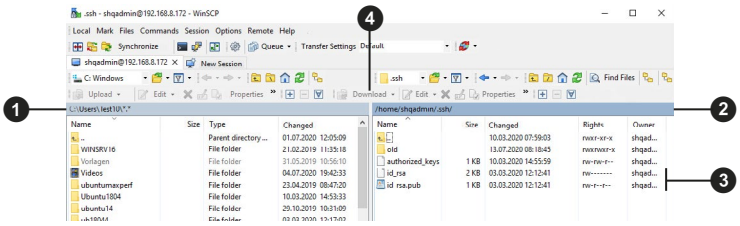
» Display the files and folders cached in WINSCP (Ctrl+Alt+H)

» Go to a folder on the local Windows PC (on the left ❶).

» Go to the Ubuntu server in the ".ssh" folder on the right ❷

» Select the files "id_rsa" und "d_rsa.pub" ❸

» Click on **Download** ❹ to download the selected files onto the Windows PC.



» Then download and install the latest version of Docker CE

› https://docs.docker.com/docker-for-windows/release-notes/

» Restart Windows PC

» Check installation.

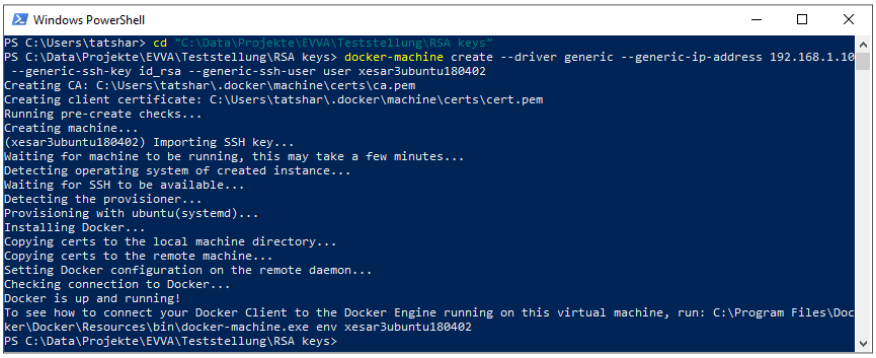
```
PS C:\Users\tatshar> docker version
Client: Docker Engine - Community
 Version:           18.09.2
 API version:       1.39
 Go version:        go1.10.8
 Git commit:        6247962
 Built:             Sun Feb 10 04:12:31 2019
 OS/Arch:           windows/amd64
 Experimental:      false

Server: Docker Engine - Community
 Engine:
  Version:          18.09.2
  API version:      1.39 (minimum version 1.12)
  Go version:       go1.10.6
  Git commit:       6247962
  Built:            Sun Feb 10 04:13:06 2019
  OS/Arch:          linux/amd64
  Experimental:     false
PS C:\Users\tatshar> docker-machine version
docker-machine.exe version 0.16.1, build cce350d7
PS C:\Users\tatshar> docker-compose version
docker-compose version 1.23.2, build 1110ad01
docker-py version: 3.6.0
CPython version: 3.6.6
OpenSSL version: OpenSSL 1.0.2o  27 Mar 2018
```

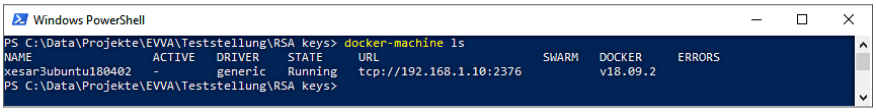
Use the following commands in the Powershell or Windows Console to create the Docker Machine:

» **cd "C:\Data\Projekte\EVVA\Teststellung\RSA keys" docker-machine create --driver generic --generic-ip-address 192.168.1.10 --generic-ssh-key id_rsa --generic-ssh-user user xesar3ubuntu180402**

- Replace **C:\Data\Projekte\EVVA\Teststellung\RSA keys** with the path into which you previously copied the files with WINSCP
- **192.168.1.10** is the IP address of the Ubuntu server, which was statically assigned during the installation
- **user** is the username of the Ubuntu server that was created during the installation
- **xesar3ubuntu180402** is the name that should be given to the Docker Machine



» Using the command**docker-machine ls** check that the Docker Machine is running



» Connect the **coding station** via USB to your administrator PC

» Insert your **AdminCard** into the card slot in the coding station.

2.5 Xesar 3.2 installation

» Download the latest Xesar 3.2 software

› **https://www.evva.com/uk-en/products/electroniclockingsystem-saccesscontrolsystems/xesar/download-xesar-software/**

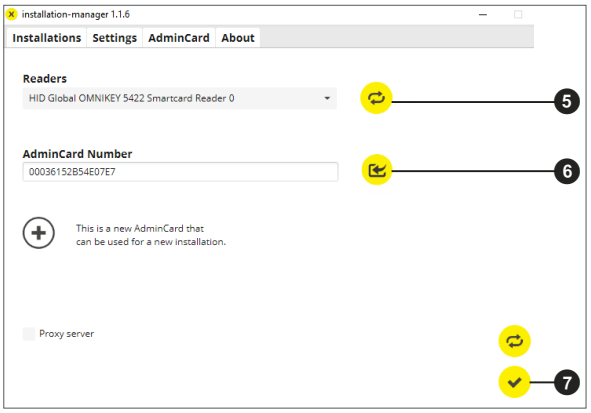
» Open the Installation Manager

» Select the tab **AdminCard**

» Load the card reader ❺

» Load the AdminCard ❻

» Confirm the entry ❼

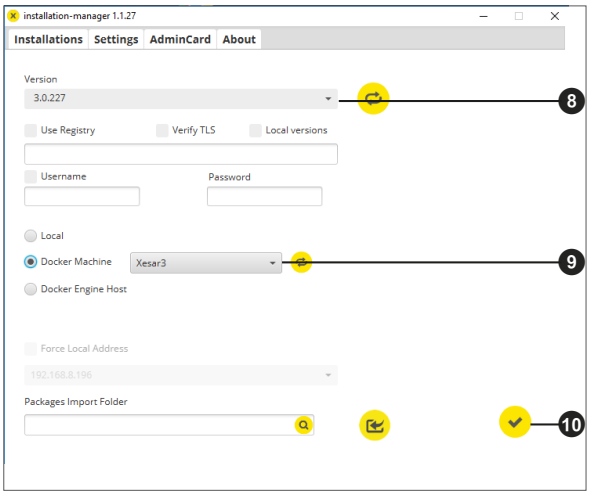


» Select the tab **Configuration**

» Select the Xesar software version❽

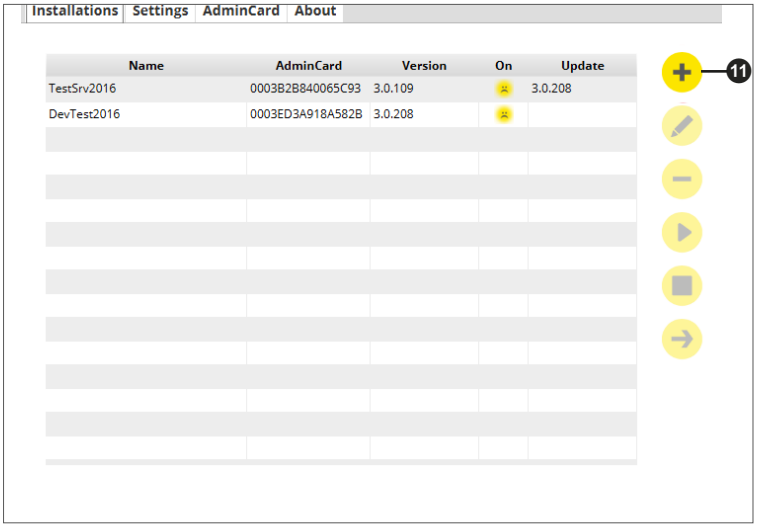
» Select the previously created Docking Machine ❾

» Confirm the entry ❿



» Select the tab **Installations**

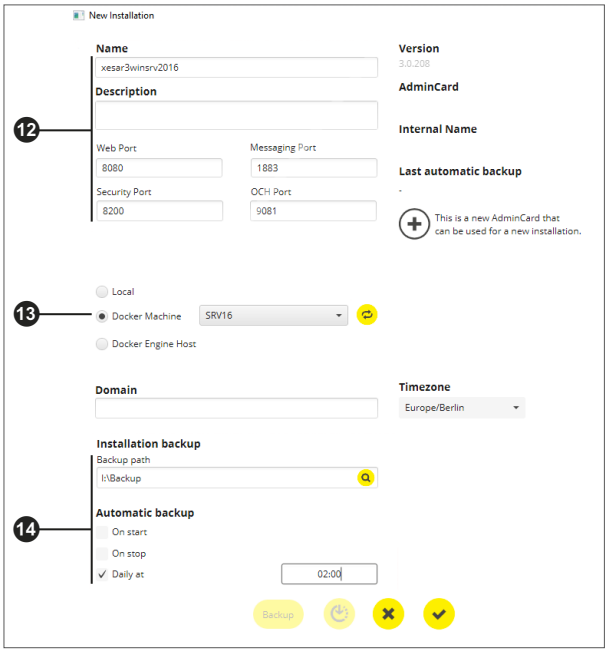
» Using the "+" button, ⓫ add a new system



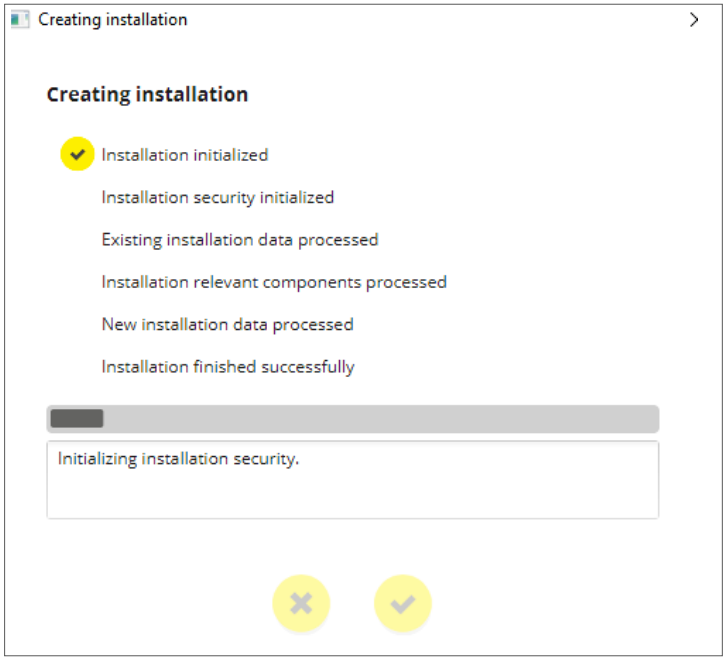
» Fill in the data ⓬

» Select the Docker Machine ⓭

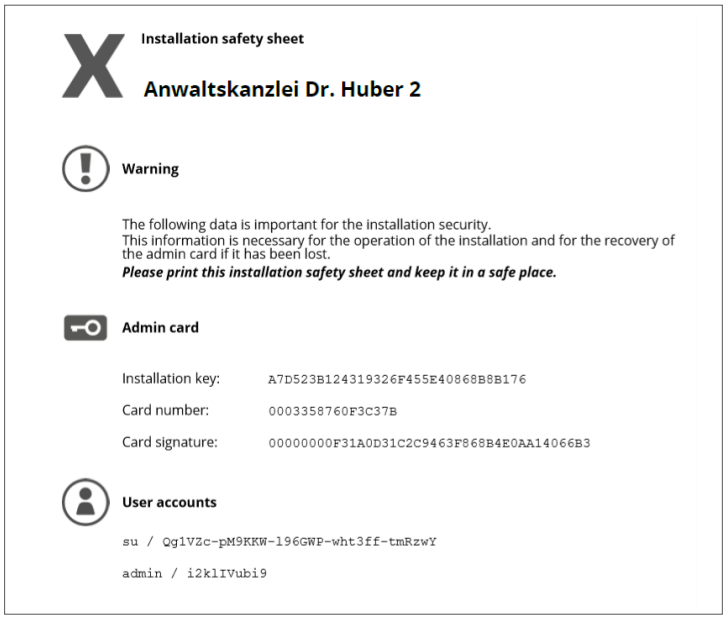
» Set up the automatic backup ⓮



The system is created (important installation information is shown).



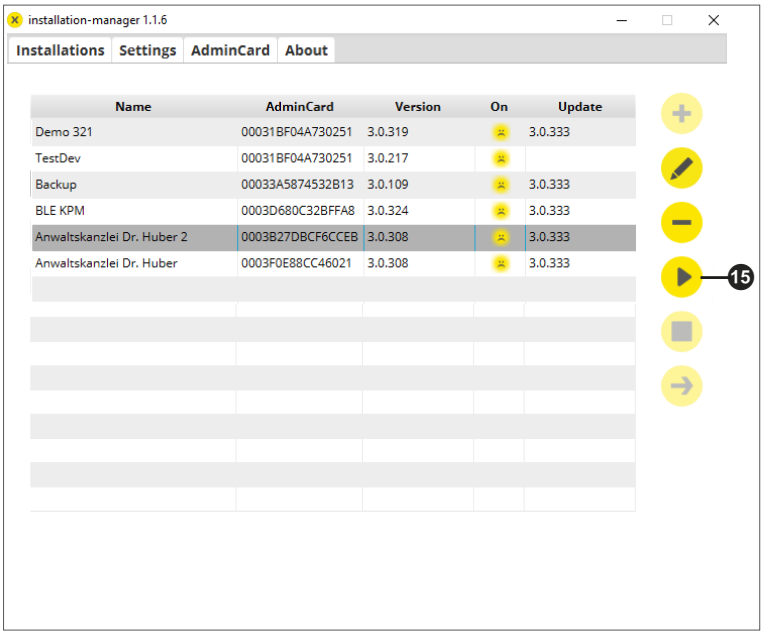
The most important system data are output in the document “Installation Information”.



Important:
Without this data, the system can not be restored in the event of a fault.
Print “Installation Information” document and keep in a safe place.

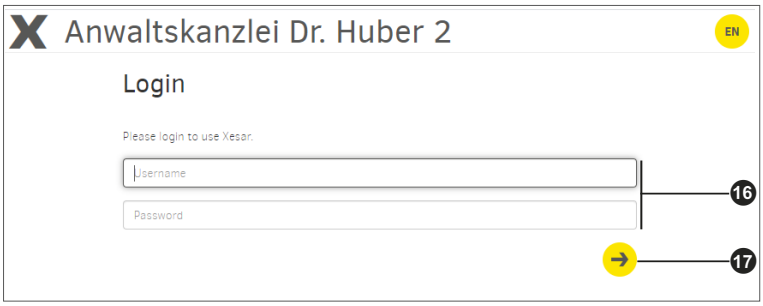
» Select the desired system

» Start by clicking on the arrow ⓯



» Log in with the login details you received in the "Installation Information" document (admin / password) ⓰

» Click on the arrow ⓱



You will now be taken to the Xesar 3.2 dashboard and can operate the system.

www.evva.com