Server Installation Instructions

Xesar 3.0

Installation instructions

for Windows Server 2016 /Datacenter/Hypervisor

KPM.X.Installationsanleitung Server Windows 2016 Datacenter_Hypervisor EN | 04/2019 | Subject to misprints and technical changes.

Contents

1 Preface

These instructions show how to prepare the Xesar 3.0 installation on a Windows server with the operating system versions Windows Server 2016 Standard or Datacenter as hypervisor.

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

Before the installation, check and confirm that the Xesar 3.0 system requirements are met, as required by the project checklist and the system manual.

The current project checklist can be downloaded from the Xesar homepage at https://www.evva.com/at-de/produkte/elektronische-schliesssysteme-zutrittskontrolle/xesar/**.**

We strongly recommend you to only carry out the Xesar 3 installation in close cooperation with the customer's responsible IT administrator.

Instructions for installing Xesar 3.0 on Windows Server 2016 Datacenter.

2 Requirements:

A physical server is setup with Microsoft Windows Server 2016 and configured as a hypervisor. On this, a VM with a current Ubuntu LTS server is installed, on which subsequently a Docker runs with Xesar 3.

The following prerequisites are necessary for a successful installation of Xesar 3.0 on a server with the Windows Server 2016 operating system:

1. A physical server with an installed **Windows Server 2016 /Datacenter** operating system, from version 1607
2. Configuration as **Hypervisor** for **Virtual Machine (VM) for Ubuntu LTS Server for Docker**
3. The user must have Windows Server and network management know-how.
4. The user must have local administration rights.
5. There must be an existing DHCP service.
6. The server time zone must be configured as UTC.
7. Hyper-V support must be available, as well as a virtual switch with a possibility to connect to and access the Internet
8. Access to the internet (Docker Trusted Registry with Notary Service and Licence Service, Port 443, 4443, 8072) must be available.
9. It is possibly that the coding station driver must be installed. HID Omnikey 5422 is usually detected automatically.

Important: Due to the availability of resources in conjunction with Windows Server, we recommend at least 8GB, better is still 16GB of memory for the physical server. The VM requires at least 4GB of memory. Basically, the larger the installation and the greater the amount of persons / traffic / online wall readers, the more memory should be available.

3 Set up Ubuntu

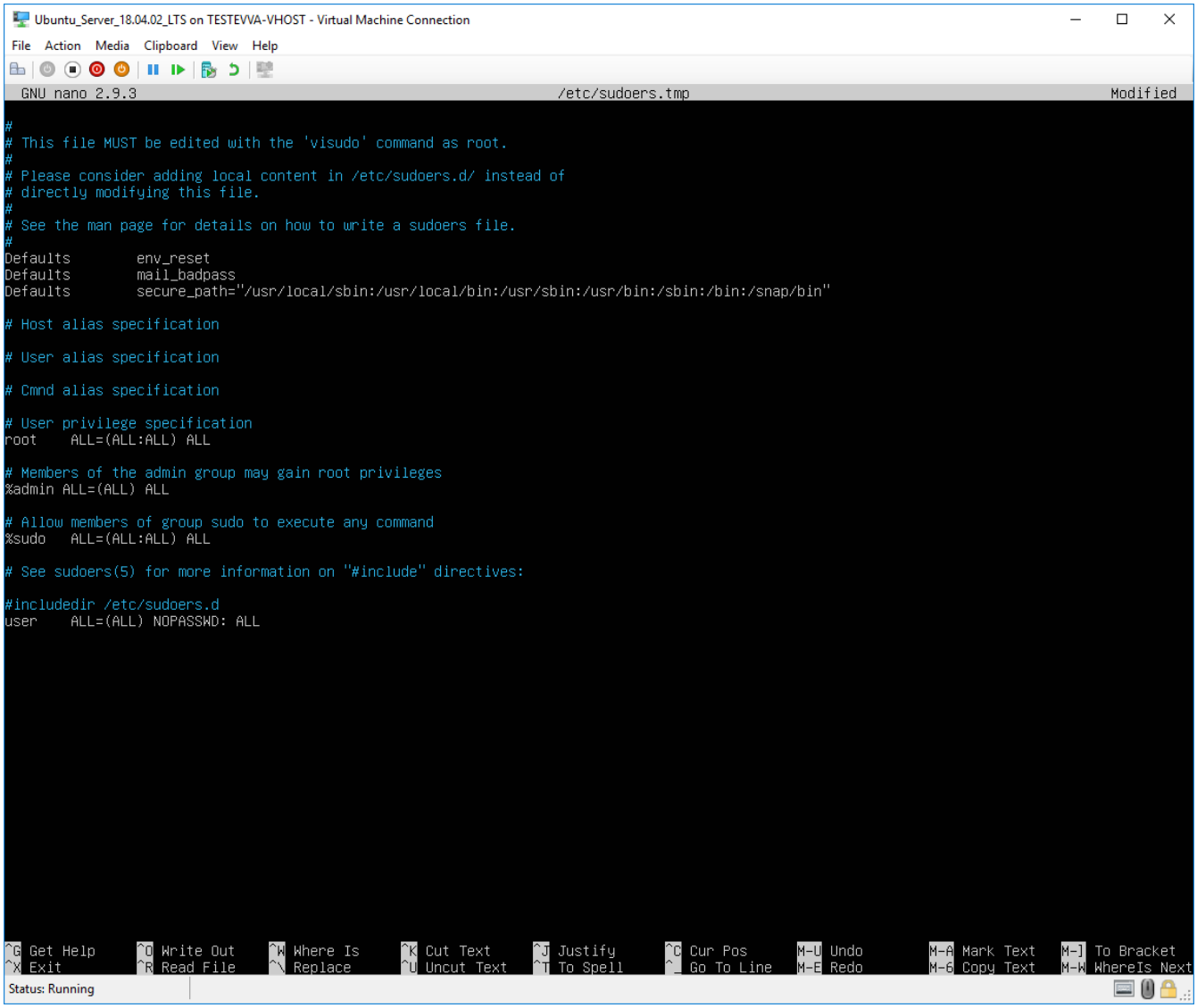
1. Password query for sudo is edited with the following command:

sudo visudo

The now open file will be added to the end of the following line:

user ALL=(ALL) NOPASSWD: ALL

The underlined area must be replaced by the name of the user, which was specified during the installation.



The file is saved with CTRL+O and Enter, and closed with CTRL+X

2. An SSH key pair is created with the following command:

ssh-keygen

Name and password can be left blank and confirmed with Enter.

```
user@localhost:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:eiT3PzOcMKpfIdpa9tUGAcg3CkQemJKeb/ZORGXick4 user@localhost.localdomain
The key's randomart image is:
+---[RSA 2048]----+
|    . ==.o..     |
|  o oo.=o o.     |
| . o. E. o ..    |
|  o  *  .    .   |
|   .  + S . .    |
|    +. B oo. o   |
|   o .+ =.o+..o  |
|     ..=.o o*.   |
|     .+o. . .+   |
+----[SHA256]-----+
user@localhost:~$ _
```

3. Add the SSH public key to the authorised keys:

cd /home/user/.ssh/

cat id_rsa.pub > authorised_keys

The underlined area must be replaced by the name of the user, which was specified during the installation.

```
user@localhost:~$ cd /home/user/.ssh/
user@localhost:~/.ssh$ ls
id_rsa  id_rsa.pub
user@localhost:~/.ssh$ cat id_rsa.pub > authorized_keys
```

4 Install Ubuntu Updates

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

sudo apt-get update

sudo apt-get upgrade

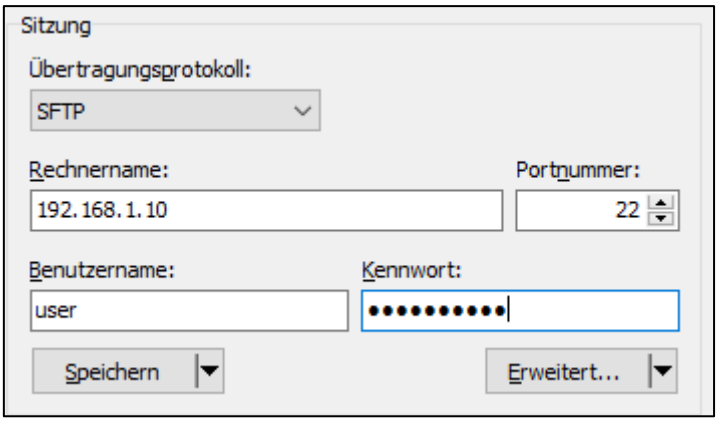
sudo apt-get dist-upgrade

sudo apt-get autoremove

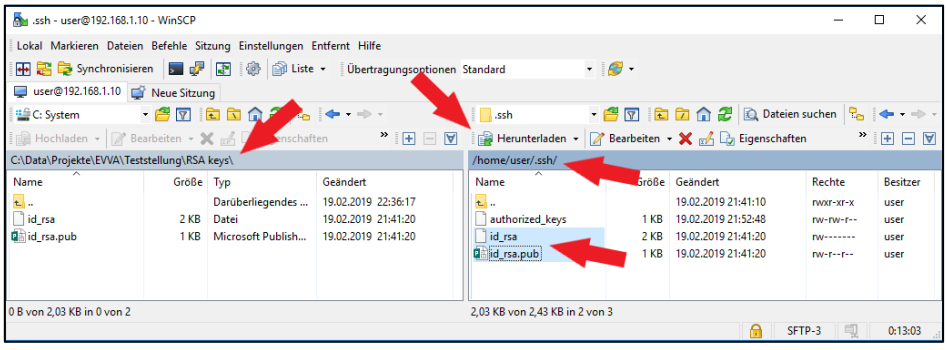
sudo reboot now

5 Set up Windows 10 Pro Admin PC

1. To transfer the SSH key, WINSCP is downloaded from https://winscp.net/eng/download.php and installed.
2. When starting WINSCP, the computer name, port, user name and password of the previously created Ubuntu server will be queried.



3. On pressing the keyboard shortcut CTRL+ALT+H you are shown hidden files and folders in WINSCP. On the left side, switch to a folder on the local Windows PC. On the right side, switch to the ".ssh" folder on the Ubuntu server, select the files id_rsa and id_rsa.pub, and load them to the Windows PC by pressing the "Download" button.



4. The current version Docker CE is then downloaded from https://docs.docker.com/docker-for-windows/release-notes/ and installed. The installation can be checked after a reboot.

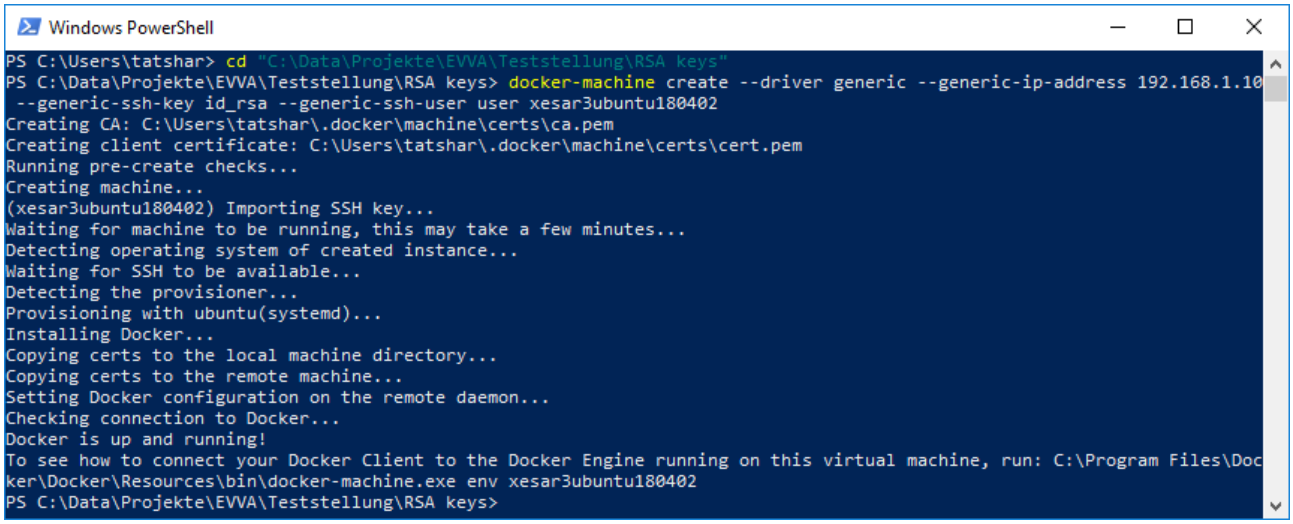
```
PS C:\Users\tatshar> docker version
Client: Docker Engine - Community
 Version:           18.09.2
 API version:       1.39
 Go version:        go1.10.8
 Git commit:        6247962
 Built:             Sun Feb 10 04:12:31 2019
 OS/Arch:           windows/amd64
 Experimental:      false

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
```

5. Enter the following commands into the Powershell or Windows console to create the Docker Machine:

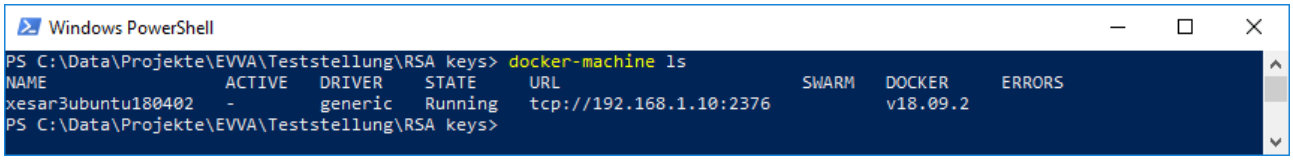
cd "C:\Data\Projekte\EVVA\Teststellung\RSA keys" docker-machine create --driver generic --generic-ip-address 192.168.1.10 --generic-ssh-key id_rsa --generic-ssh-user user xesar3ubuntu180402

The area marked in green must be replaced by the path in which the files were previously copied with WINSCP; the area marked in blue is the IP address of the Ubuntu server that was statically assigned during installation; the area marked in brown is the username of the Ubuntu server which was created during the installation; and the grey area is the name the Docker Machine should receive.



6. The following command can be used to check if the Docker Machine runs:

   docker-machine ls



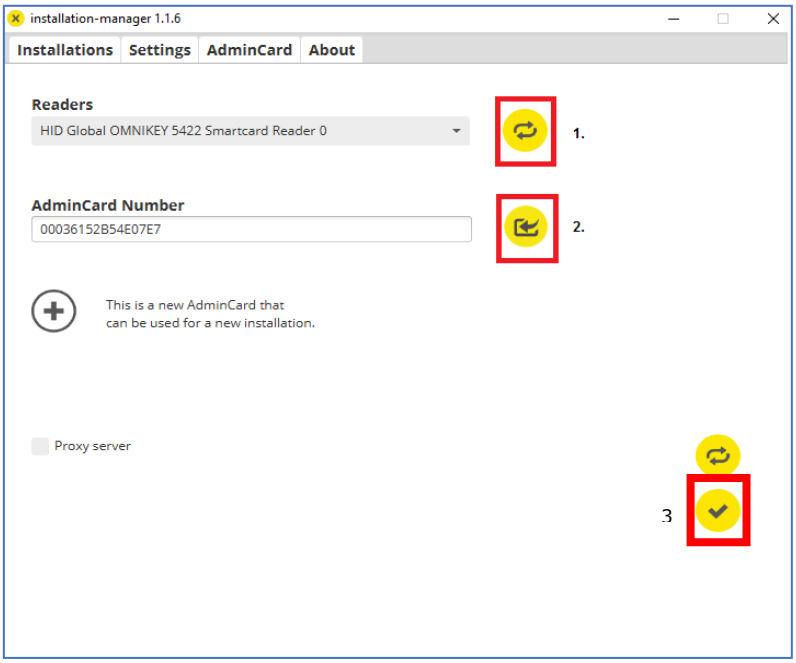
7. Connect the Xesar **coding station** via USB to your Admin PC and insert the **Admin Card** into the Xesar coding station card slot.

6 Xesar 3.0 Installation

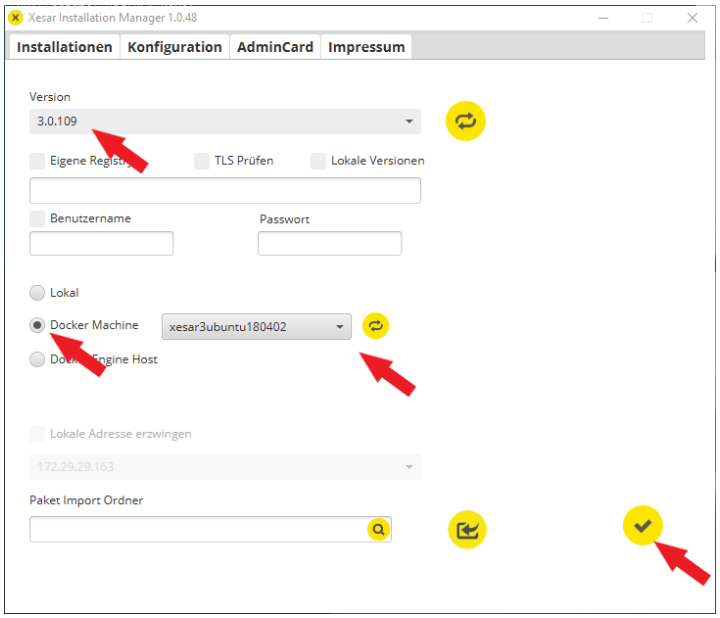
1. Download the latest Xesar 3.0 software from the EVVA homepage with the Installation Manager.

   https://www.evva.com/at-de/produkte/elektronische-schliesssysteme-zutrittskontrolle/xesar/xesar-software-download/

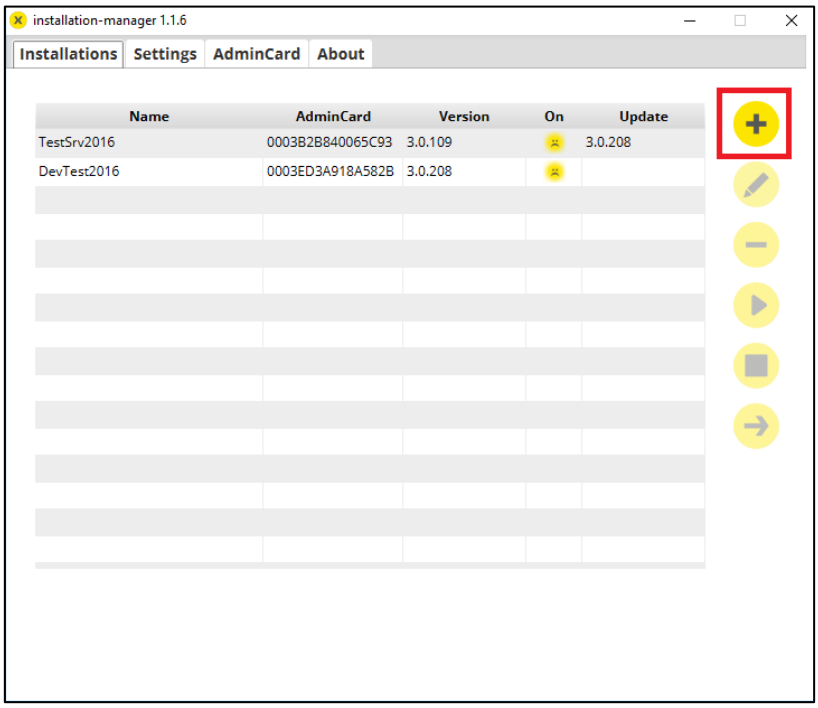
2. Open the Installation Manager. Select the AdminCard tab and load the card reader. Then load the AdminCard (2) and confirm the entry (3)



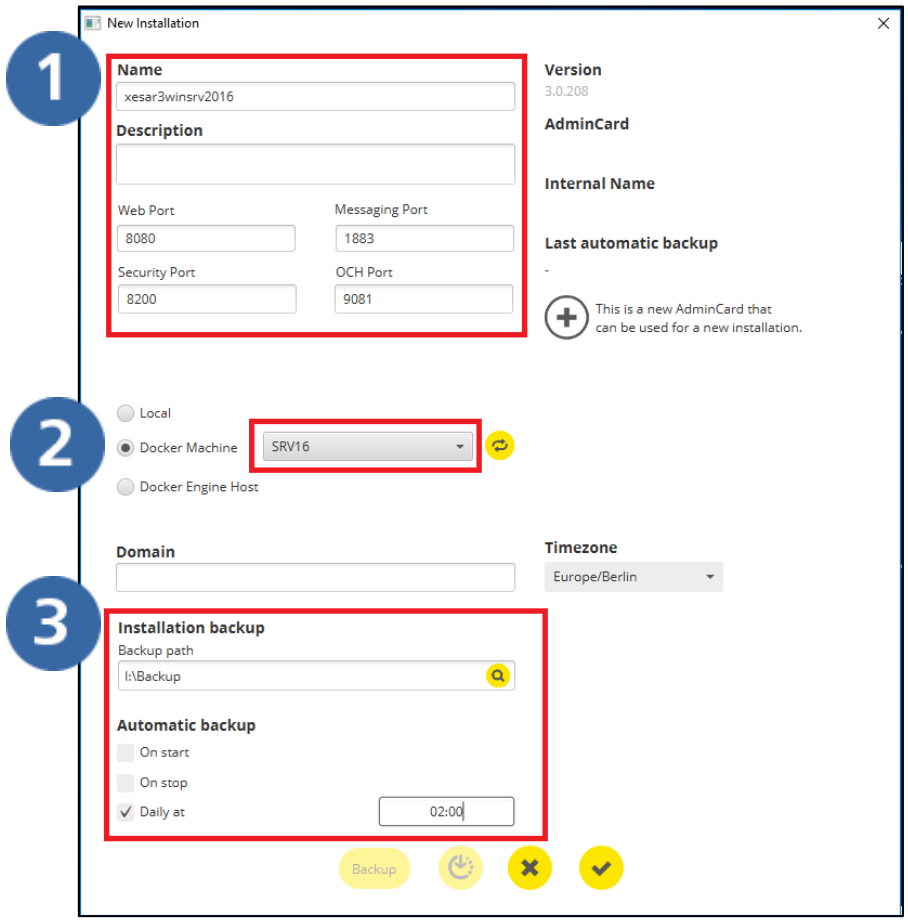
3. Select the „***Docker Machine***" section in the ***Configuration*** tab and the previously created Docker Machine. Then select and check the Xesar software version and save it.



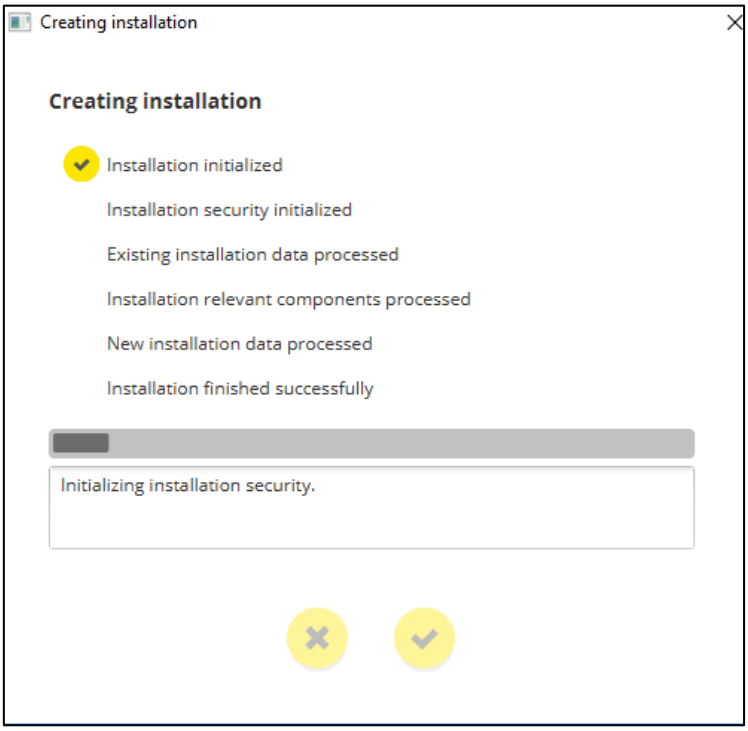
4. Select the ***Installations*** tab and add a new system with "**+**".



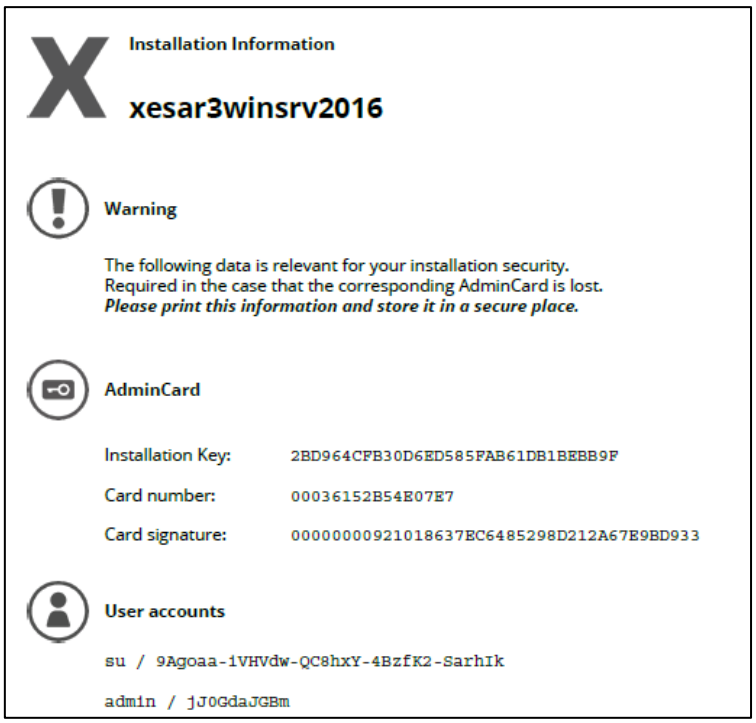
5. Enter all system data (1), select the Docker Machine (2) and define the desired automatic backup functions (Backup) (3).



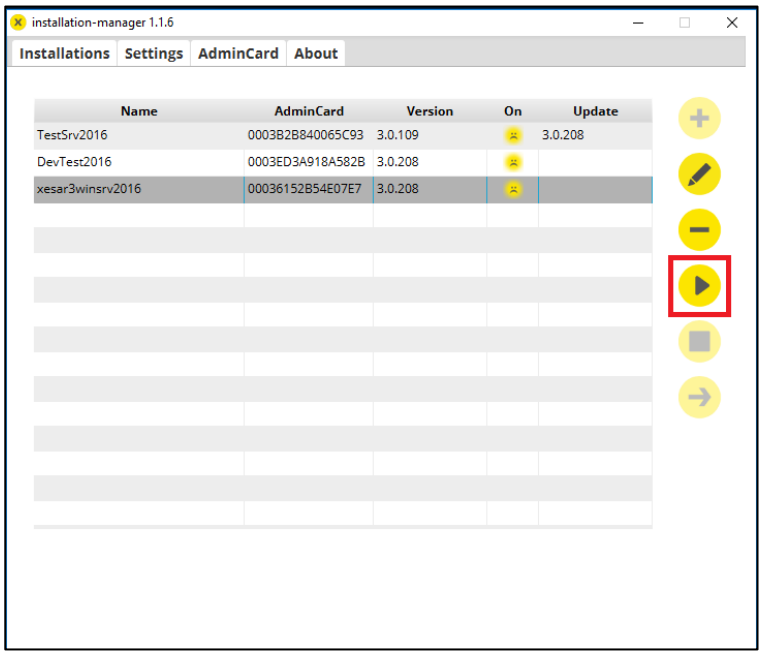
6. The system will be created and the installation information is displayed.



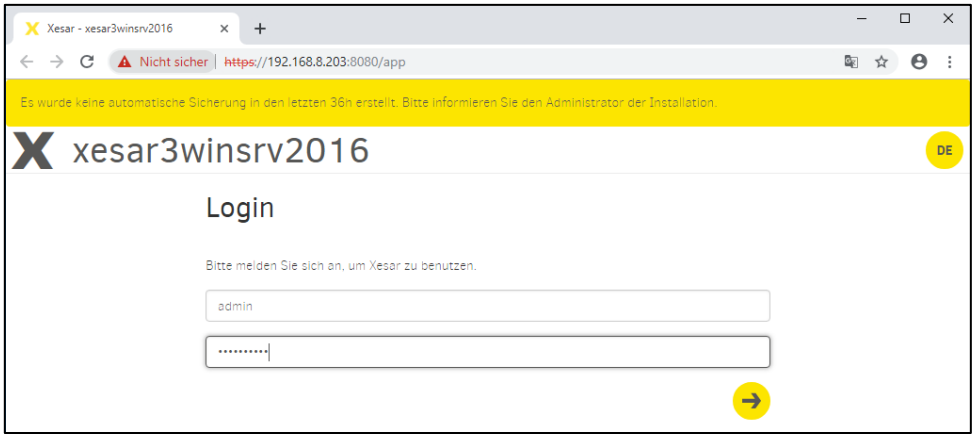
7. The most important system data are output in the document "Installation Information".



8. **<u>Important:</u> In the case that the AdminCard is lost or defective, this system information is the only way to operate the system again. Therefore, this file must be printed out and kept secure.**Select the desired installation and start it with the "Play" symbol.



9. Log in with the login data admin/password you previously received with the document *Installation Information*.



10. You are now taken to the Xesar 3.0 dashboard and can operate the installation.