



# System and Dialogue Kaba exos 9300

## Installation Manual

IM\_Kabaexos9300-System-and-Dialog-R421\_202112\_en

For internal use only

**EN**

**dormakaba** 

# Table of contents

<b>1</b>	<b>Regarding this document</b>	<b>3</b>
1.1	Validity	3
1.2	Audience	3
1.3	Contents and purpose	3
1.4	Document availability	3
1.5	Supplementary documentation	3
1.6	Overview of Kaba exos documentation	4
1.7	Change log	5
1.8	Abbreviations	5
1.9	Instructions	5
1.10	Symbols used	5
<b>2</b>	<b>System description</b>	<b>6</b>
2.1	Overview	6
2.2	System structure	7
2.3	Authentication methods	7
<b>3</b>	<b>Installation</b>	<b>9</b>
3.1	Requirements	9
3.2	Installing databases	9
3.2.1	Installing the application service database	10
3.2.2	Installing the communication hub database	13
3.2.3	Logins, server roles and user mappings for databases	16
3.3	Installing services	20
3.3.1	Installing the application service	20
3.3.2	Installing the communication hub	26
3.3.3	Installing web applications	29
3.4	Installing the client	32
3.4.1	Installing desktop reader service	34
3.4.2	Installing 3M passport scanner service	35
3.4.3	Installing Mitek passport scanner service	35
3.4.4	Installing IRIS desktop readers service	35
3.4.5	Installing signature reader	36
<b>4</b>	<b>First steps</b>	<b>37</b>
4.1	Logging in	37
4.2	Tray-icon	39
4.3	Launcher	40
4.4	Authorizations	41
<b>5</b>	<b>Additional information</b>	<b>42</b>
5.1	Encrypted communication between the CH and the access manager	42
5.2	API help	47
5.2.1	Access	47
5.3	Resolution of host names	49
5.4	Replacing a self-signed certificate	49
<b>6</b>	<b>Troubleshooting</b>	<b>50</b>
6.1	Error analysis	50
6.1.1	Browser asks for login data	50
6.2	Known problems	51
6.3	Reporting a problem to support	51
6.3.1	General information regarding a support case	52

# 1 Regarding this document

This section contains information about properly using this document.

## 1.1 Validity

This document describes the product:

Product name:	Kaba exos 9300
Release:	As of 4.2.1

## 1.2 Audience

This document is solely intended for specialist personnel who have been trained by dormakaba in the release of Kaba exos 9300 used.

Specialist knowledge of the following is also required:

- the operating system used
- database products used
- web technologies (IIS and browser)
- the network technology used
- information security (e.g. certificates)
- the other dormakaba products used (e.g. b-comm ERP, evolvo components)

## 1.3 Contents and purpose

This document describes the installation procedure for Kaba exos 9300.

Installation is described based on the recommended system structure (see chapters 'System structure [▶ 2.2]' and 'Authentication methods [▶ 2.3]') with Windows authentication and an SQL Server database.

## 1.4 Document availability

Additional documentation is available on the dormakaba website. The manuals can be found in a protected area (extranet). They can be accessed using the user account of trained specialists or a temporary user account.

<https://www.dormakaba.com/extranet-emea-en/login>

## 1.5 Supplementary documentation

### **Configuration manual**

CM\_Kabaexos9300-MS-SQL-Database

CM\_Kabaexos9300-Database-Update

### **Reference manual**

RM\_Kabaexos9300-MSI

RM\_Kabaexos9300-System-and-Settings

RM\_Kabaexos9300-Web-Applications

RM\_Kabaexos9300-RabbitMQ

RM\_Kabaexos9300-Integration

**Planning guideline**

PG\_Kabaexos9300-System

**Other documents**

Online help full dialogue

Online help web application

Kabaexos9300-Security

## 1.6 Overview of Kaba exos documentation

Planning guideline (PG)	Configuration manual (CM)		Reference manual (RM)	
<b>System</b>				
System	IM System & Dialog	Cabinet Lock	Web Applications	System & Settings
Security White Paper	Translation	Online Cabinet Lock	Integration	Logbooks
	Access manager 92 xx	ARIOS*	Reporting	MSI
			REST API	RabbitMQ
<b>Databases</b>	Database Update		Database	
	MS SQL Database			
<b>Interfaces</b>	Interface 90 10	TBS Terminal	LDAP	Push API
	CC1 Interface*		b-comm ERP exos Interface	Datapoint Server
			CC1 Interface*	OPC
<b>Access control</b>				
Wireless	Badge Input Badge Output	CardLink		
	Nedap	OSS-SO		
	Alarm Zones	Wireless		
	LoxTop Depot Control	Lift Control		
<b>Integration online components</b>	B-web 9300*		Communication Access Manager*	
<b>Media</b>				
Media Extensions	Media Definitions	Mobile Access	LEGIC advant Media Definition	Dual Chip Media*
Mobile Access	KabaCard	Master Key System		
Media LEGIC*	Kaba Media Manager*	Duplicate Media Detection*		
Media MIFARE ARIOS*				

\* Documents older than release 4.0.0

## 1.7 Change log

The most important changes to the last version of this document are listed as follows:

File name	Brief description
IM_Kabaexos9300-System-and-Dialog-R421_202112	First edition for the release

## 1.8 Abbreviations

Abbreviation/name	Meaning
AS	Application server
CH	Communication hub
DB	Database composite abbreviations: AS-DB, CH-DB
IIS Web service	Internet Information Services Microsoft service platform for PCs and web servers
Kaba exos	Kaba exos 9300
SSO	Single Sign-On is used as a synonym for 'Windows authentication'.

## 1.9 Instructions

Structure and symbols of the instructions are illustrated in the following example:

- ✓ Prerequisite
- 1. Step 1
  - ⇒ Interim result
- 2. Step 2
  - ⇒ Result

## 1.10 Symbols used

The following symbols will be used in this document to identify important information and instructions:



### NOTICE

#### Instructions on the correct usage of the software.

Failure to comply with these instructions may result in malfunctions, system crashes or data loss.



Tips and useful information. These help you to make best use of the product and its functions.

# 2 System description

## 2.1 Overview

Kaba exos is based on the client-server principle and consists of the following important parts:

- **Application server (AS)**

The application server contains the application logic and provides data to the communication hubs for the connected devices. There is only 1 application server for each system. The application service and the web service (IIS) run on the application server.

- **Application service database (AS-DB)**

This database (SQL or Oracle) is used by the application service and contains the entire system data.

- **Communication hub (CH)**

The communication hub consists of individual processes that are responsible for the communication with the door/access managers (Kaba exos AMC, access manager 92 00, etc.). At least 1 communication hub is required for each system. Each communication hub saves its own data locally. This data is continuously reconciled with the application service database.

- **Interactive workstation**

The interactive workstation consists of individual sub-programs that can be started depending on the user right of a person to carry out different administrative works such as registering new devices or allocation of access rights.

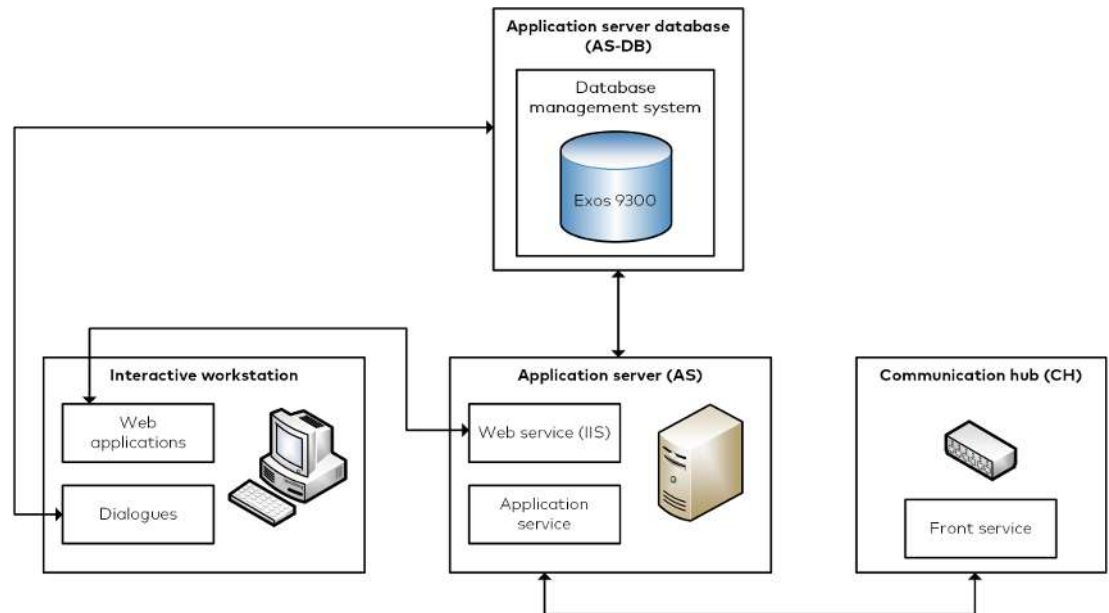
Additional functionalities (e.g. staff data management) are available in the web applications. You can also access the web applications from the interactive workstation.

The data are saved in the application service database.

Detailed information about the system structure can be found in the document 'PG\_Kabaexos9300-System'.

## 2.2 System structure

This document describes the installation procedure for Kaba exos based on the following recommended system structure:



The following table shows which installation file is required for which component. The installation procedure itself is described in the 'Installation' chapter.

Component	Installation files (Features)
Application server (AS)	<ul style="list-style-type: none"> <li>Service.msi (Application service &amp; exos API)</li> <li>WebApps.msi</li> </ul>
Communication hub (CH)	<ul style="list-style-type: none"> <li>ServiceCH.msi (Communication hub)</li> <li>DatabaseCH.msi (Communication hub database)</li> </ul>
Application service database (AS-DB)	<ul style="list-style-type: none"> <li>Database.msi (Application service database)</li> </ul>
Interactive workstation	<ul style="list-style-type: none"> <li>Client.msi</li> </ul>

## 2.3 Authentication methods

In Kaba exos, different authentication methods can be used at 2 points, namely:

- 1 Services and client login into the database
- 2 User login into Kaba exos

The authentication method recommended by dormakaba for the respective point is described below. The installation default values meet these recommendations.

Ultimately, it is the RMO's or the partner's responsibility to select the authentication method that best meets the customer's safety requirements and to install the system accordingly.

### Services and client login into the database

For services (application service & communication hub), we recommend configuring access to the application service database via Windows authentication. For Oracle, only SQL Server authentication is released.

Clients' access to the application service database is per default configured via SQL Server authentication. It is possible to configure Windows authentication with an SQL server. However, this is not recommended, as the registered Windows user essentially has access to the application service database without needing to know a password. This must be prevented with relevant counter-measures.

**User login into Kaba exos**

Logging into Kaba exos (client & web applications) is done by entering a user name and password as standard. But it is also possible to activate Windows authentication for the login process. If Windows authentication is activated, the user only has to authenticate themselves using a password when logging into their Windows user account. The login to Kaba exos via the login dialog is omitted.



# 3 Installation

This chapter describes the installation of the product.

## 3.1 Requirements

### General

- Prior to installing Kaba exos, all other Windows users must be logged out so that all registry entries can be created correctly.
- Kaba exos is a 32-bit application. 32-bit applications are installed in the 'C:\Program Files (x86)' directory by default.

### Tools

The following tools are needed for installing Kaba exos:



The required tools are supplied with Kaba exos in the 'Addons' directory (exception: Erlang and RabbitMQ).

The installation wizard refers to the tools required at the appropriate point. Compatible versions are also listed in the Release Overview Kaba exos 9300 of the respective release.

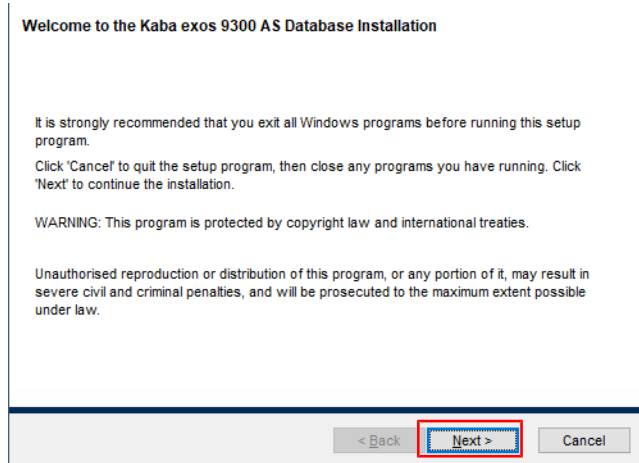
Tool	File name	Component
Microsoft .NET Core hosting bundle	dotnet-hosting-...-win.exe	Application server
Microsoft .NET Framework	NDP...-x86-x64-AI-IOS-ENU.exe	on all components
Microsoft Internet Information Services (IIS)	Needs to be activated.	Application server
Erlang OTP runtime <b>Attention:</b> If the 'Erlang OTP runtime' tool is uninstalled, it is essential to perform a restart before installing it again.	otp_win64_... .exe	Application server Communication hub
RabbitMQ (see the document 'RM_Kabaexos9300-RabbitMQ') <b>Attention:</b> The 'Erlang OTP runtime' tool must be installed before the 'RabbitMQ' tool, as otherwise it is possible for online versions to be downloaded that may not be compatible with Kaba exos.	rabbitmq-server-... .exe	Application server Communication hub
Microsoft SQL Server (see the document 'CM_Kabaexos9300-MSSQL-DBMS')	SQLServer... .exe	Application server Communication hub
Microsoft Visual C++ Redistributable	32 bit: vc_redist.x86.exe 64 bit: vc_redist.x64.exe	on all components

## 3.2 Installing databases

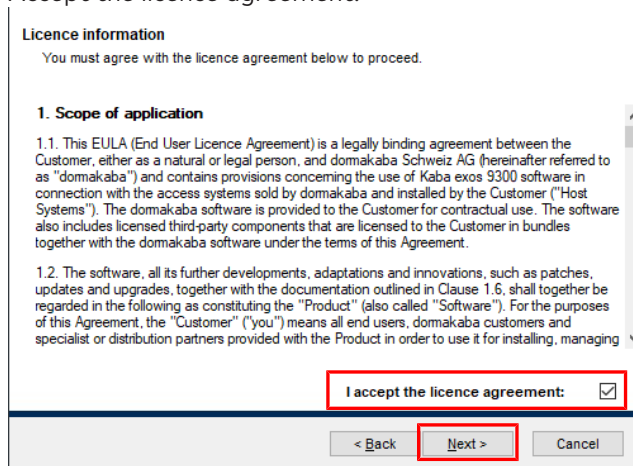
The following description applies to a new installation. The procedure for updating databases is described in the document 'CM\_Kabaexos9300-Database-Update'.

### 3.2.1 Installing the application service database

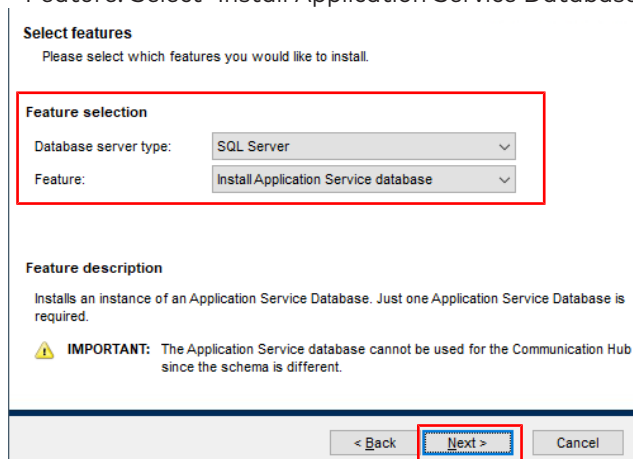
1. Launch the 'Database.msi' file.



2. Select 'Next'.
3. Accept the licence agreement.

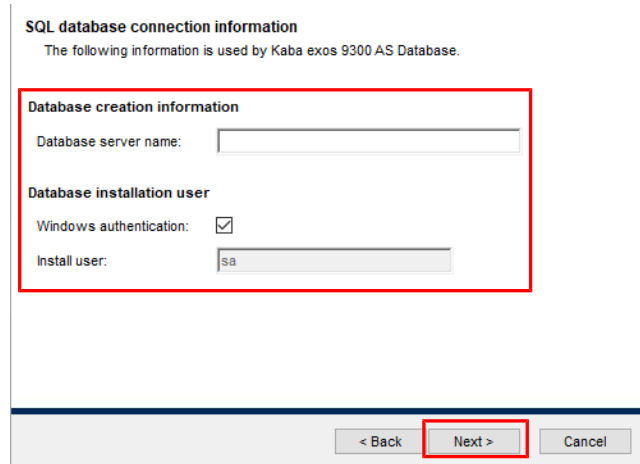


4. Select 'Next'.
5. - Database server type: Select the database server type used.  
- Feature: Select 'Install Application Service Database'.

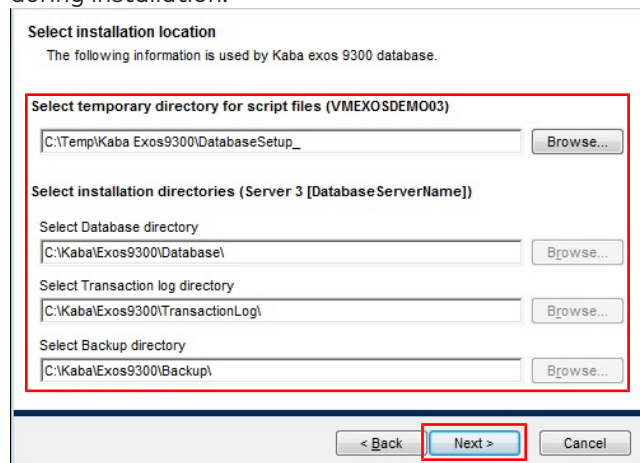


6. Select 'Next'.
7. - Database server name: Enter the name of the server on which the database is installed, including the corresponding instance if necessary (e. g.: DatabaseServer\DatabaseInstance).  
- Keep 'Windows authentication' activated so that the user does not have to enter their user name/password when installing the database. This way, the user will be logged in automatically using their Windows user account data.

**To use SQL Server authentication:** Deactivate 'Windows authentication' and enter the database user to be used for the installation under 'Install user'.



8. Select 'Next'.
9. Select the directories under which the database scripts and files should be saved.  
**Note:** To install in 'C:\Program Files', the paths in the 'Properties.ini' file must be adjusted during installation.



10. Select 'Next'.
11. - Database name: Enter the database name.  
 - Use default settings: Deactivate the checkbox to adjust the database settings:  
 - Database login (Client): Keep 'Windows authentication' disabled.  
**Attention:** If the checkbox is activated, the database connection is authorized from the full dialogue via Windows authentication. When using Windows authentication as authentication of the full dialog for the database, the registered Windows user generally has access to the Kaba exos database without requiring any password. This must be prevented with relevant counter-measures.  
**Attention:** The user logins must be registered on the SQL Server. Furthermore, the users must be authorized for the roles 'ExosDialog' and 'ExosDialogDotNet' on the SQL Server.  
 - Backup/maintenance jobs: Creates the backup and maintenance jobs. For SQL Server Express, backup jobs can only be created via the Task Scheduler.  
 - Recovery mode: Database recovery mode.  
 - Database: Initial size of the database in MB, maximum size of the database in MB, database increase in %.

- Transaction log: Initial size of the transaction log in MB, maximum size of the transaction log in MB, transaction log increase in %.

**SQL database settings**  
The following information is used by Kaba exos 9300 AS Database.

**Define a database name**  
Database name:   
Use default settings:

**Database settings**  
Database login (Client):  Windows authentication  
Backup/maintenance jobs:   
Recovery mode:

	Size (MB)	Max size (MB)	Growth (%)
Database:	<input type="text" value="500"/>	<input type="text" value="4000"/>	<input type="text" value="20"/>
Transaction log:	<input type="text" value="100"/>	<input type="text" value="4000"/>	<input type="text" value="20"/>

< Back **Next >** Cancel

12. Select 'Next'.

- AS/exos API host name: Enter the name of the server on which the application service and the exos API are installed.
- Save duration of logs and other data (in days): If desired, adjust the default values for saving the logbooks and other data.

**Kaba exos 9300 AS Database configuration**  
The following information is used by Kaba exos 9300 AS Database.

AS hostname:   
exos API hostname:

**Save duration of logs and other data (in days)**

System	<input type="text" value="90"/>	Alarm	<input type="text" value="90"/>	Access	<input type="text" value="90"/>
Audit	<input type="text" value="90"/>	Time	<input type="text" value="90"/>	Badge	<input type="text" value="3650"/>
Error	<input type="text" value="90"/>	Depot	<input type="text" value="90"/>	Parking	<input type="text" value="90"/>
Mail	<input type="text" value="90"/>	Visit	<input type="text" value="180"/>	Upcoming visit	<input type="text" value="14"/>
Visitor	<input type="text" value="900"/>	Visitor log	<input type="text" value="900"/>		

< Back **Next >** Cancel

14. Select 'Next'.

15. Click 'Install' to install the database.

**Ready to install**

Click 'Install' to begin installation. Click 'Back' to re-enter the installation information or click 'Cancel' to exit the wizard.

Automatically run batch file:

< Back **Install** Cancel

- ⇒ The files required for installation are created and copied into the temporary directory.
- ⇒ If 'Automatically run batch file' is not enabled, the installation files are not executed automatically. Detailed information can be found in the document 'RM\_Kabaexos9300-System-and-Settings'.

16. Check the setup settings. In case of SQL Server authentication, enter the password for the database administrator (e.g. for 'sa') and press ENTER.

```

C:\Windows\system32\cmd.exe
***** CHECK SETUP SETTINGS FOR DATABASE GENERATION !
SERVER=KBRUL002\SQL2014
DATABASE=Exos9300
USER=sa
DBFILENAME_LOGICAL=Exos9300
DBFILE=Exos9300_Primary.ndf
DBPATH=C:\Kaba\Exos9300\Database\
DBSIZE=500,DBMAXSIZE=4000,DBFILEGROWTH=20
LOGFILENAME_LOGICAL=Exos9300_Log
LOGFILE=Exos9300_Primary.ldf
LOGPATH=C:\Kaba\Exos9300\TransactionLog\
LOGSIZE=50,LOGMAXSIZE=4000,LOGFILEGROWTH=20
BACKUP_PATH=C:\Kaba\Exos9300\Backup\
BACKUP_NAME=Exos9300.bak
BACKUP_DEVICE=DISK
BACKUP_DEVICE_NAME=Exos9300Backup
WINDOWSAUTHENTICATION=false
SQLEXPRESS=false
INSTALLJOBS=true
SQLRECOVERYMODE=Full

Please enter the password for Database User sa:

```

17. Press any key to start the installation procedure.

```

C:\Windows\system32\cmd.exe
DATABASE=Exos9300
USER=sa
DBFILENAME_LOGICAL=Exos9300
DBFILE=Exos9300_Primary.ndf
DBPATH=C:\Kaba\Exos9300\Database\
DBSIZE=500,DBMAXSIZE=4000,DBFILEGROWTH=20
LOGFILENAME_LOGICAL=Exos9300_Log
LOGFILE=Exos9300_Primary.ldf
LOGPATH=C:\Kaba\Exos9300\TransactionLog\
LOGSIZE=50,LOGMAXSIZE=4000,LOGFILEGROWTH=20
BACKUP_PATH=C:\Kaba\Exos9300\Backup\
BACKUP_NAME=Exos9300.bak
BACKUP_DEVICE=DISK
BACKUP_DEVICE_NAME=Exos9300Backup
WINDOWSAUTHENTICATION=false
SQLEXPRESS=false
INSTALLJOBS=true
SQLRECOVERYMODE=Full

Please enter the password for Database User sa:
*****
Warning: Any existing database Exos9300 will be deleted !!!
Do you want to generate the database Exos9300 Version 4100 build 280?
Press any key to continue . . .

```

18. Once setup is complete, press any key.
- ⇒ The 'Application Service Database' is installed.
  - ⇒ Any error messages have been logged and are displayed automatically in the '%Temp%\Kaba Exos9300\DatabaseSetup\_x.x.x\SQLServer\Setup\Log' directory.
19. Click 'Finish' to end the installation.
20. Check if the backup and maintenance jobs have been set up and if the database recovery function works.



When using SQL Server, the logins and users for the database must be created manually (in the case of Windows authentication) or based on scripts (in the case of SQL server authentication, script 'RECREATE\_AS\_v4.1.0.sql'). For detailed information see document 'CM\_Kabaexos9300-MSSQL-DBMS'.



The database user for the communication hub must be created manually or based on scripts in the application service database (see also chapter 'Installing the communication hub [▶ 3.3.2](#)').

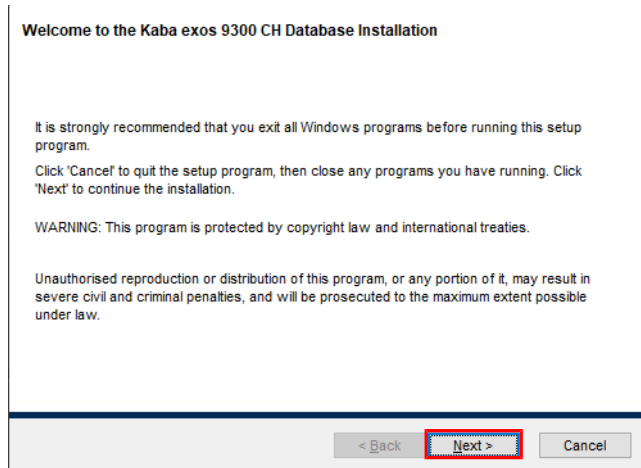
### 3.2.2 Installing the communication hub database



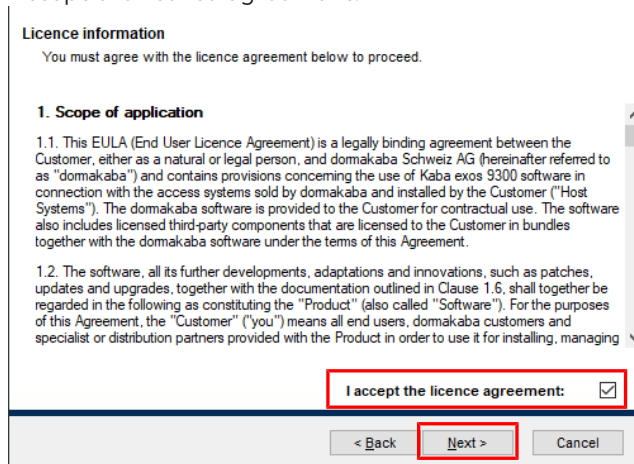
The process for installing the communication hub (CH) database is almost identical to that for installing the application service database [▶ 3.2.1](#).

The communication hub (CH) database can only be installed on an SQL server. This is not possible on an Oracle server.

1. Launch the 'DatabaseCH.msi' file.

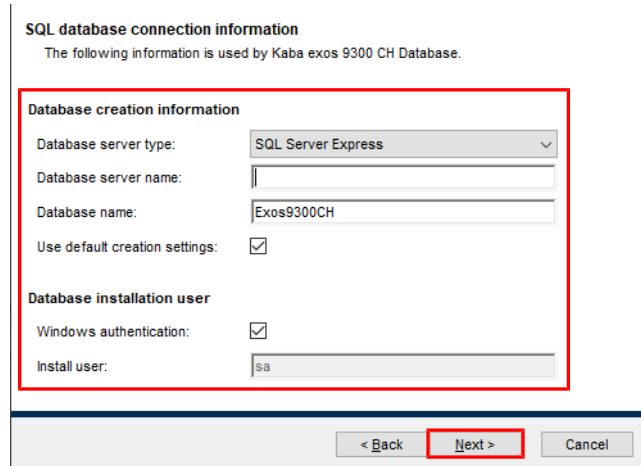


2. Select 'Next'.
  - ⇒ The licence agreement is displayed.
3. Accept the licence agreement.

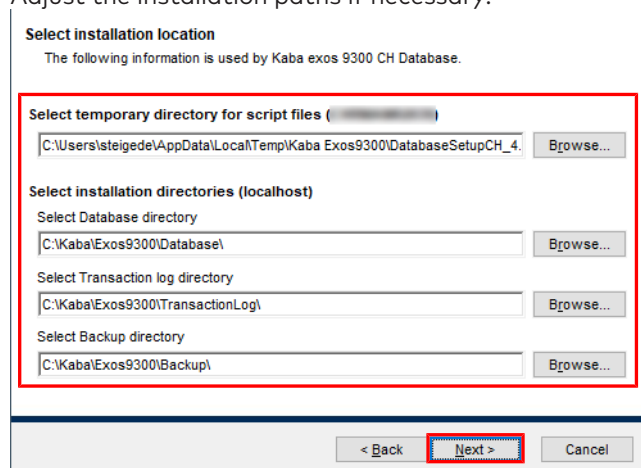


4. Select 'Next'.
  - ⇒ The database connection settings are displayed.
5. Adjust the database connection settings as needed:
  - Database server type: Select the database server type used.
  - Database server name: Enter the name of the server on which the database is installed, including the corresponding instance if necessary (for example: DatabaseServer\DatabaseInstance).
  - Database name: Enter the database name.
  - Use default creation settings: Clear the checkbox to adjust the default database settings (backup jobs, recovery mode, database size, and log files).
  - Keep 'Windows authentication' activated so that the user does not have to enter their user name/password when installing the database. This way, the user will be logged in automatically using their Windows user account data.

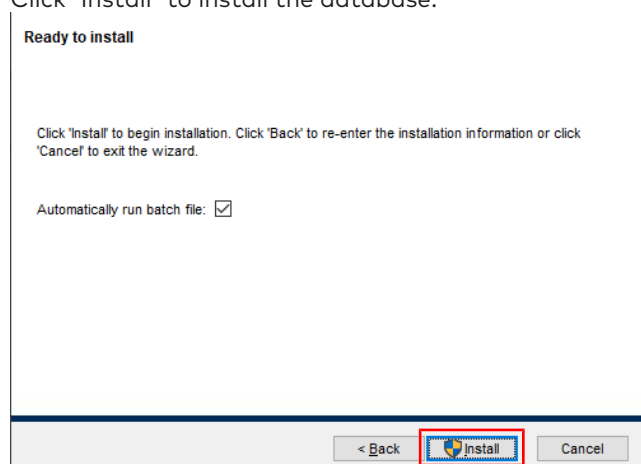
**To use SQL Server authentication:** Deactivate 'Windows authentication' and enter the database user to be used for the installation under 'Install user'.



6. Select 'Next'.
  - ⇒ The installation paths are displayed.
7. Adjust the installation paths if necessary.

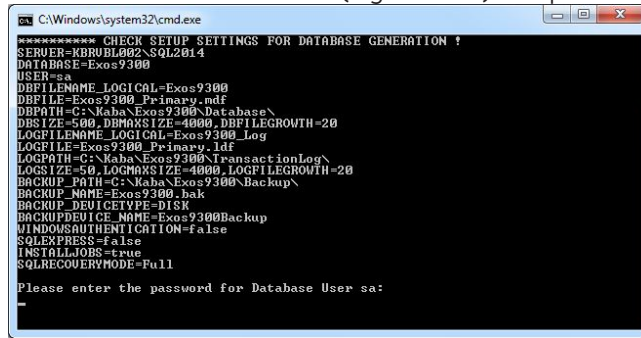


8. Select 'Next'.
9. Click 'Install' to install the database.

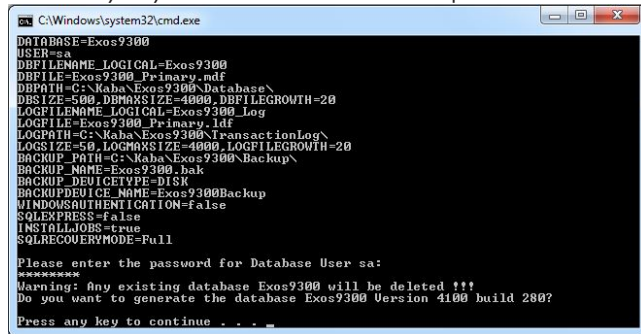


- ⇒ The files required for installation are created and copied into the temporary directory.
- ⇒ If the checkbox 'Automatically run batch file' is not activated, the installation files are not executed automatically. Detailed information can be found in the document 'RM\_Kabaexos9300-System-and-Settings'.

- Check the setup settings. In case of SQL Server authentication, enter the password for the database administrator (e.g. for 'sa') and press ENTER.



- Press any key to start the installation procedure.



- Once setup is complete, press any key.
  - ⇒ 'Communication Hub Database' has been installed.
  - ⇒ Any error messages have been logged and are displayed automatically in the '%Temp%\Kaba Exos9300\DatabaseSetup\_x.x.x\SQLServer\Setup\Log' directory.
- Click 'Finish' to end the installation.
- Check if the backup and maintenance jobs have been set up and if the database recovery function works.

### 3.2.3 Logins, server roles and user mappings for databases

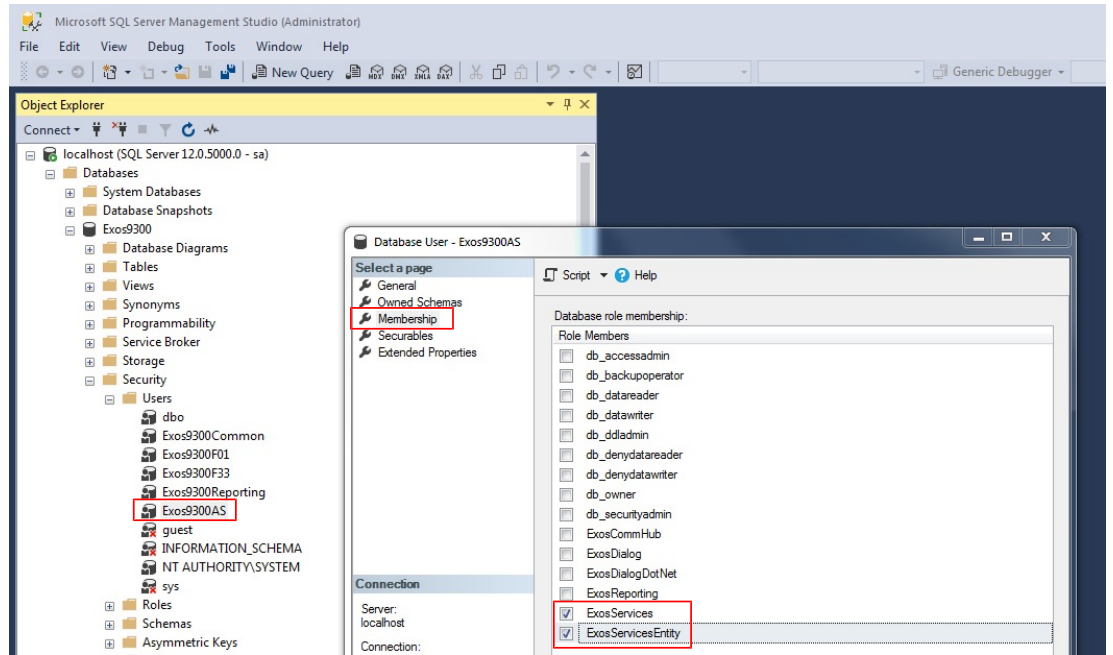
#### 3.2.3.1 Application service database

When installing the application service database, no database login is created by default. It must be created manually in MS SQL Server Management Studio or using a script.

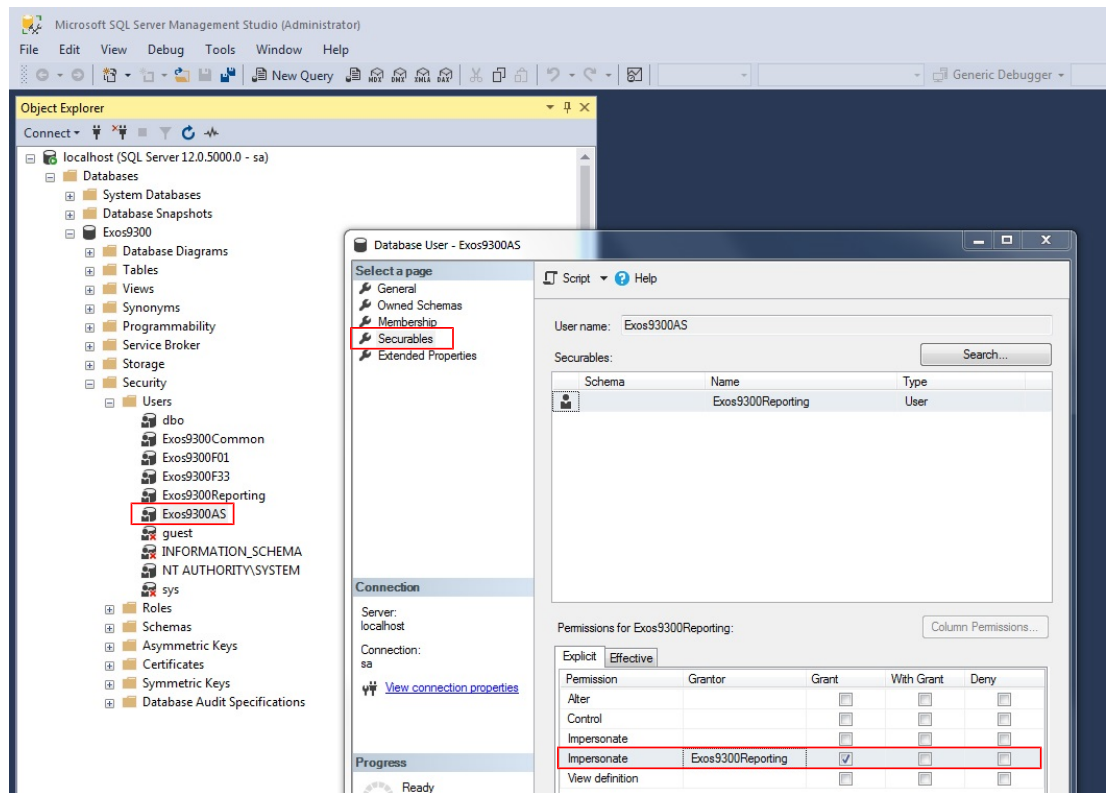
In the case of SQL Server authentication, the application service user must comply with a specified naming structure: [Database name]AS (e.g. 'Exos9300AS').

The application service user requires authorization for the roles 'ExosServices' and 'ExosServicesEntity'.

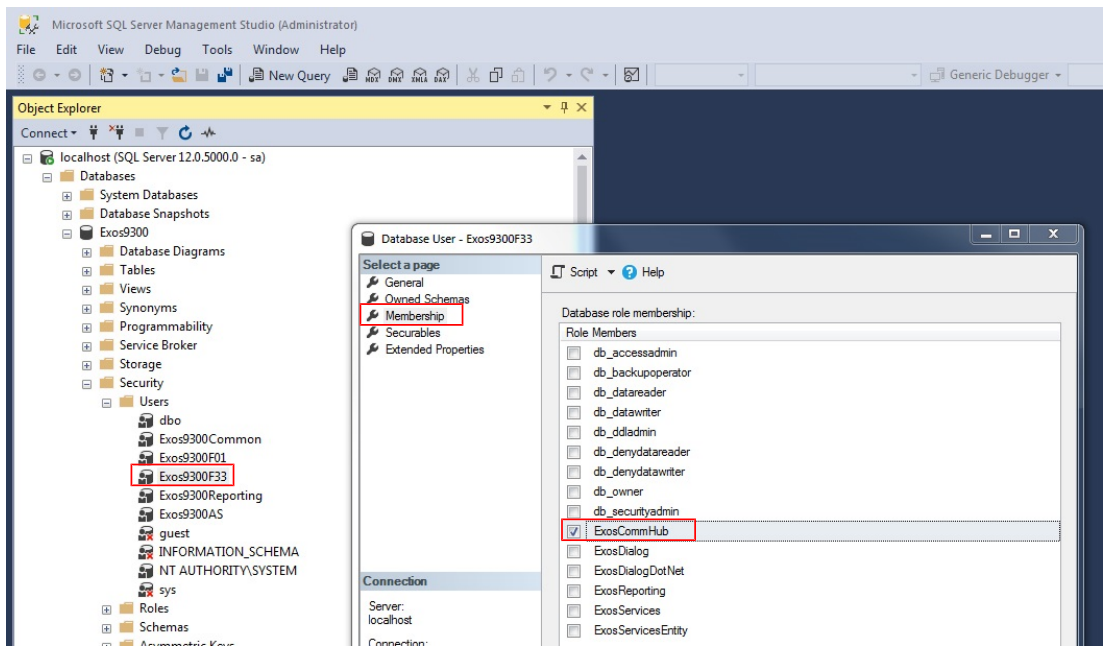




In addition, the application service user requires the 'Impersonate' authorization ('Assume identity') for the reporting user.

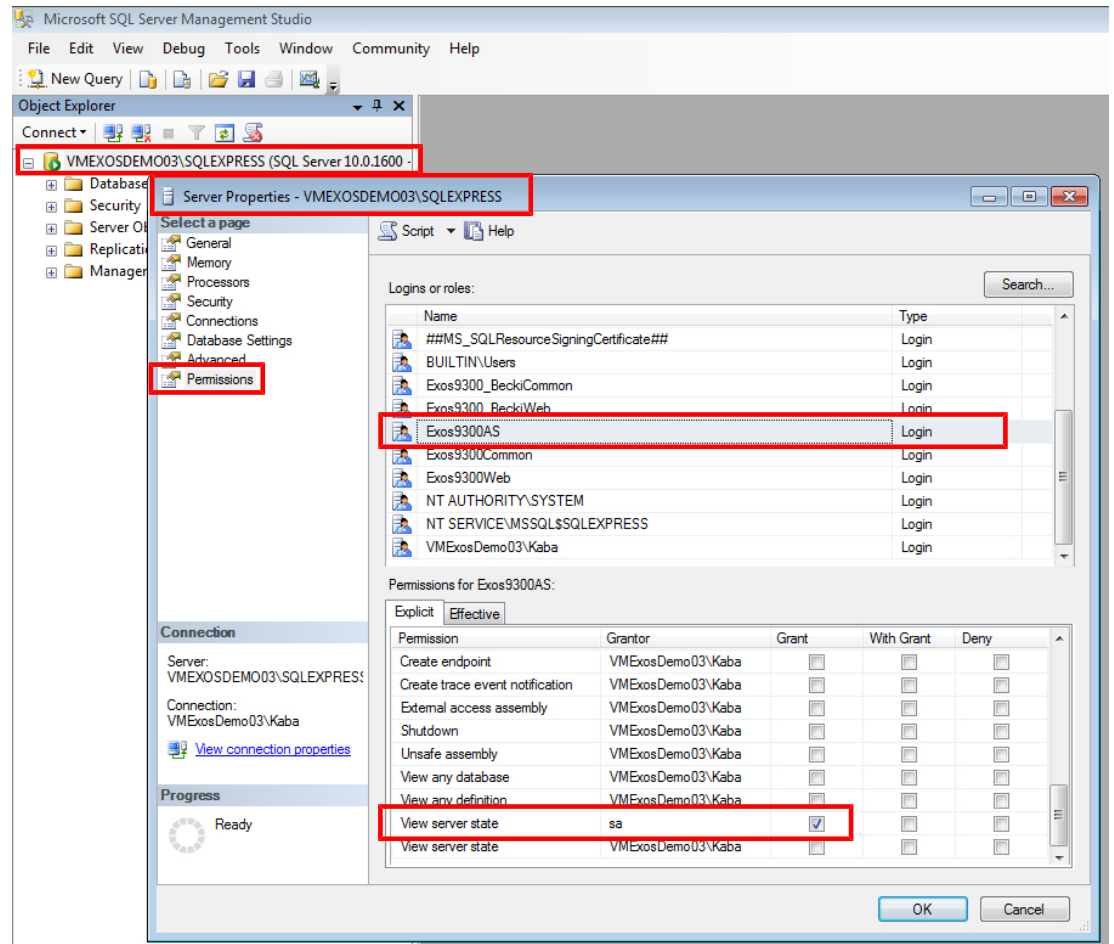


A separate database user is required for the communication hub to access the application service database (e.g. 'Exos9300F33') for SQL Server authentication. They require the role 'ExosCommHub'. The database user can access the database via SQL Server authentication or Windows authentication. The script 'RECREATE\_USER\_Fxx\_v4.1.0.sql' can be used as support.



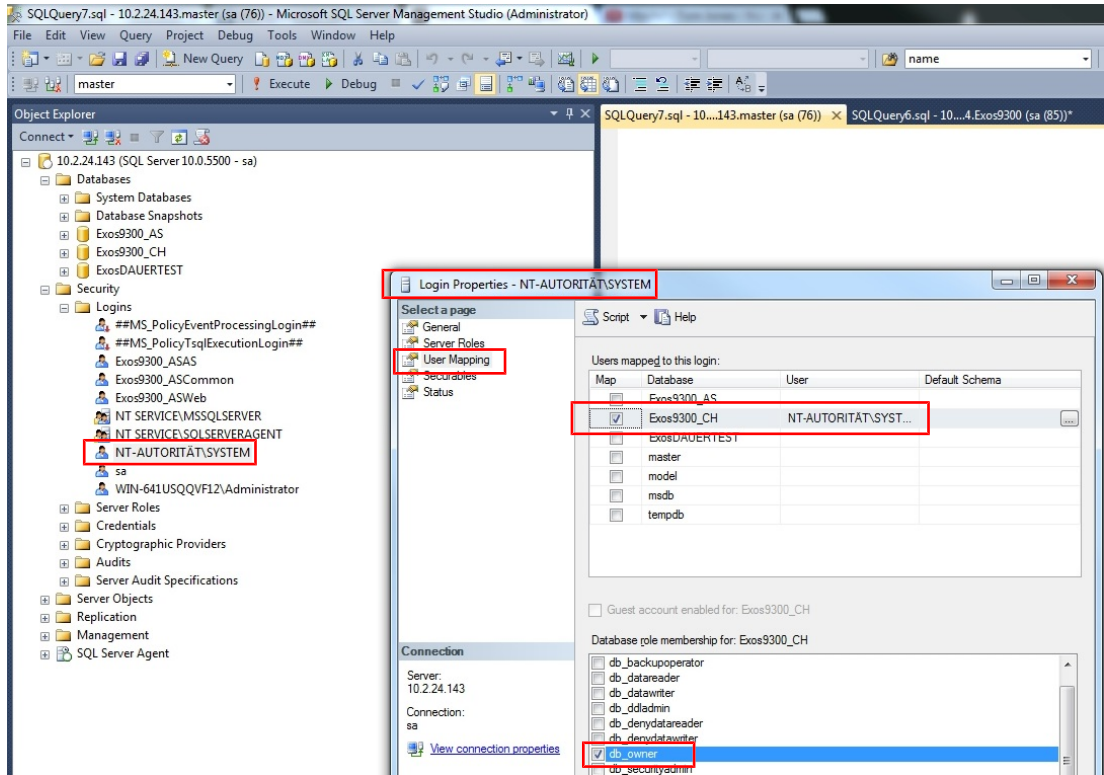
### 3.2.3.1.1 'View server state' permission

The application service user must be assigned the necessary permission ('View server state') via the database properties.



### 3.2.3.2 Communication hub database

When installing the communication hub database, no database login is created by default. Database access is enabled by default via the Windows user 'NT authority\system'. The database user needs to have the database role 'db\_owner'.



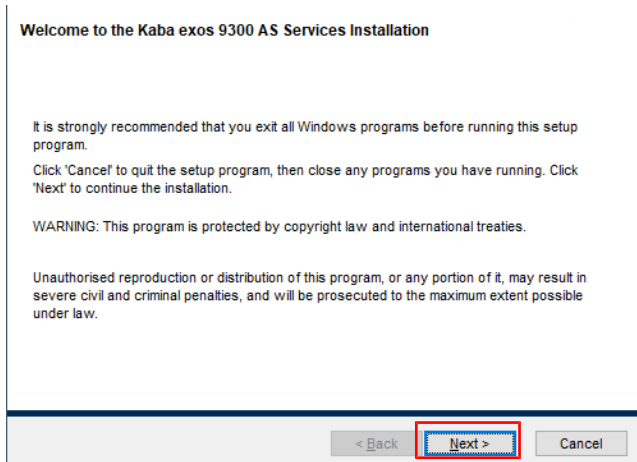
### 3.3 Installing services



All necessary tools [▶ 3.1] must be installed before the services are installed.

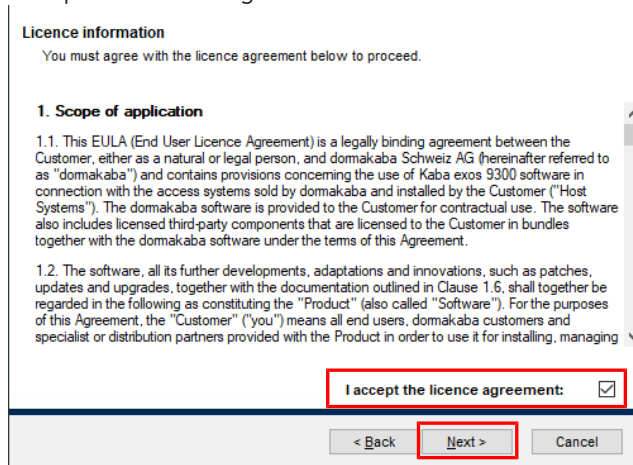
#### 3.3.1 Installing the application service

1. Launch the 'Service.msi' file.



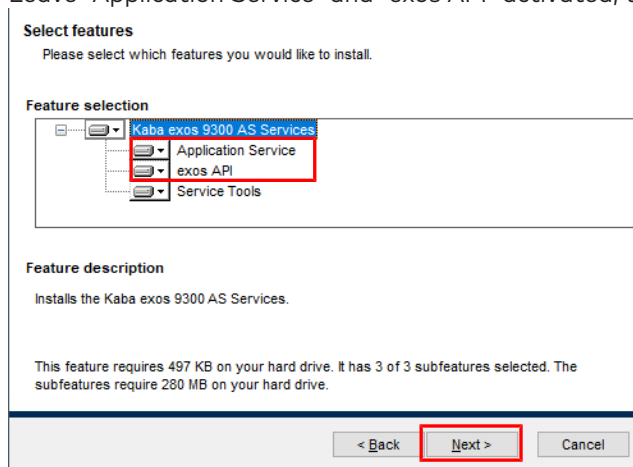
2. Select 'Next'.

3. Accept the licence agreement.



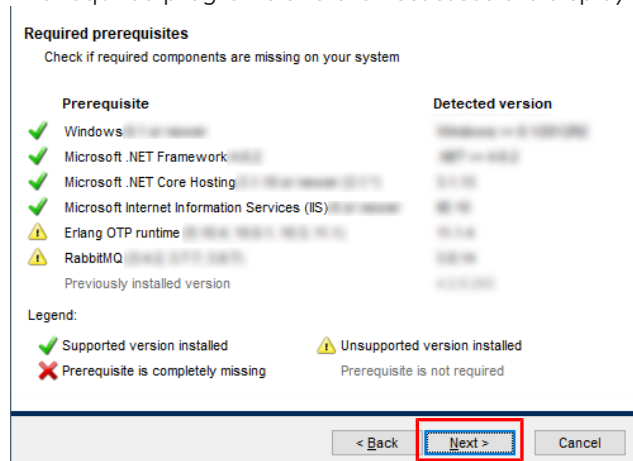
4. Select 'Next'.

5. Leave 'Application Service' and 'exos API' activated; the remaining features are optional.



6. Select 'Next'.

⇒ The required programs and their statuses are displayed.



7. Select 'Next'.

- 8. Select the corresponding licence file.

**Licence information**  
The following information is used by Kaba exos 9300 AS Services.

**Licence file**

Name :

Place :

✓

**Select licence file**

C:\Users\... Desktop\Exos9300License.txt

< Back 

- 9. Select 'Next'.

- 10. Select the installation directories.

**Select installation location**  
The following information is used by Kaba exos 9300 AS Services.

**Select services installation directory**

**Select exos API installation directory**

**Select exos API Login installation directory**

< Back 

- 11. Select 'Next'.

- 12. - AS/exos API host name: Enter the name of the server on which the application service and the exos API should be installed.
- IIS API website name/folder: If the API applications are not to be installed in the IIS under the 'default website', specify the name and/or directory of the website.
- User name/password: Enter a domain user with local administrator rights. For SQL server, additional database authorizations must also be granted to this user.

**Note:** If the fields have been left empty, the Windows user 'NT AUTHORITY\SYSTEM [▶ 3.2.3]' is used for the services.

**Common service configuration**

The following information is used by Kaba exos 9300 Services.

AS hostname:

exos API hostname:

IIS API Web Site Name:

IIS API Web Site Folder:

**Optional: Specify service user credentials**

User Name:

Password:

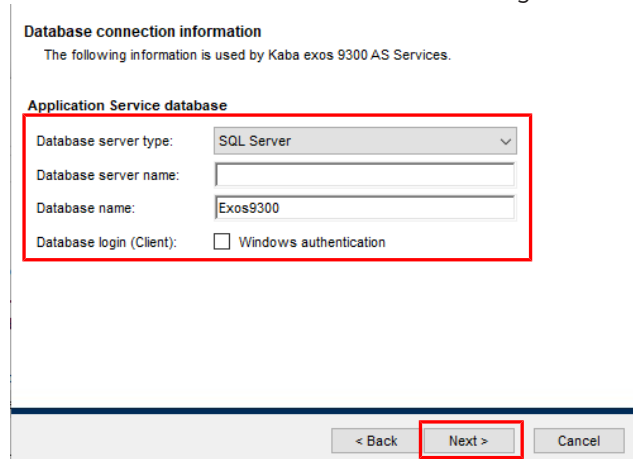
< Back 

- 13. Select 'Next'.

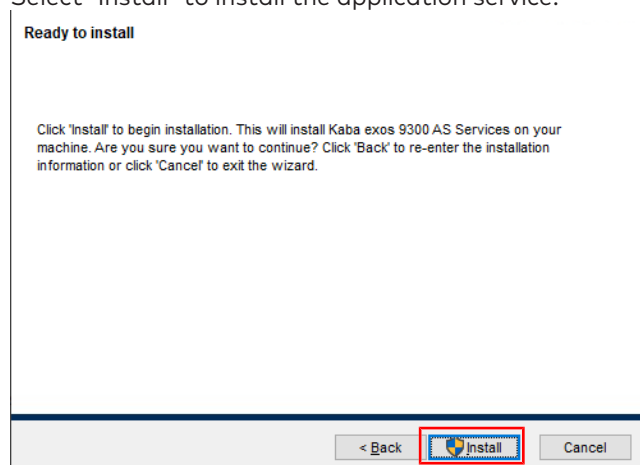
- 14. - Database server type: Select the database server type used.
- Database server name: Enter the name of the server on which the database is installed, including the corresponding instance if necessary (for example: DatabaseServer\DatabaseInstance).
- Database login (Client): Keep 'Windows authentication' disabled (same as for installation of the application service database [▶ 3.2.1]).

**Attention:** If the checkbox is activated, the database connection is authorized from the full dialogue via Windows authentication. When using Windows authentication as authentication of the full dialog for the database, the registered Windows user generally has access to the Kaba exos database without requiring any password. This must be prevented with relevant counter-measures.

**Attention:** The user logins must be registered on the SQL Server. Furthermore, the users must be authorized for the roles 'ExosDialog' and 'ExosDialogDotNet' on the SQL Server.



- 15. Select 'Next'.
- 16. Select 'Install' to install the application service.

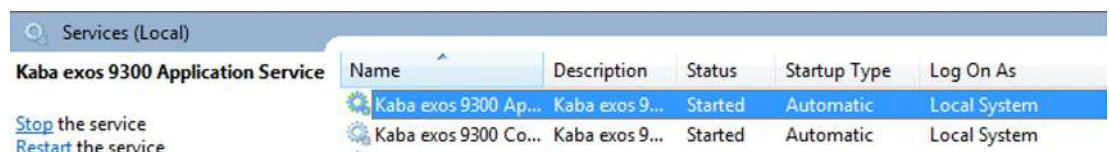


⇒ Installation starts.

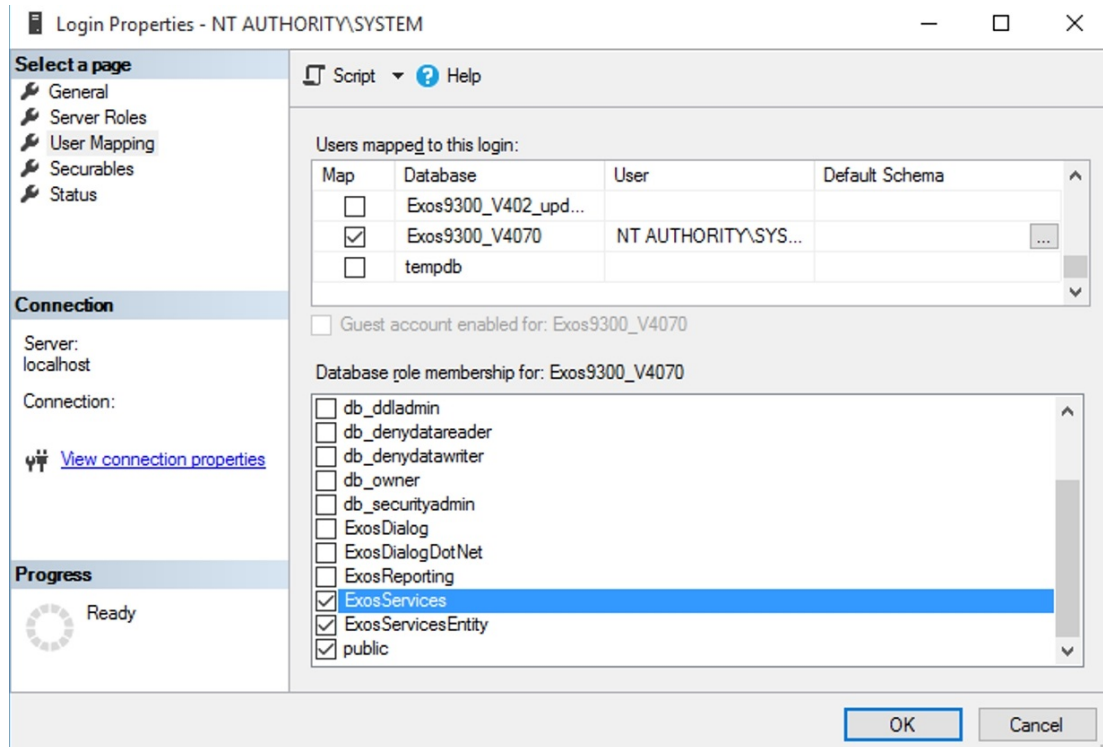
- 17. Click 'Finish' to end the installation.
- ⇒ The application service is installed.

### 3.3.1.1 Application service authorization

The application service requires the following authorization:

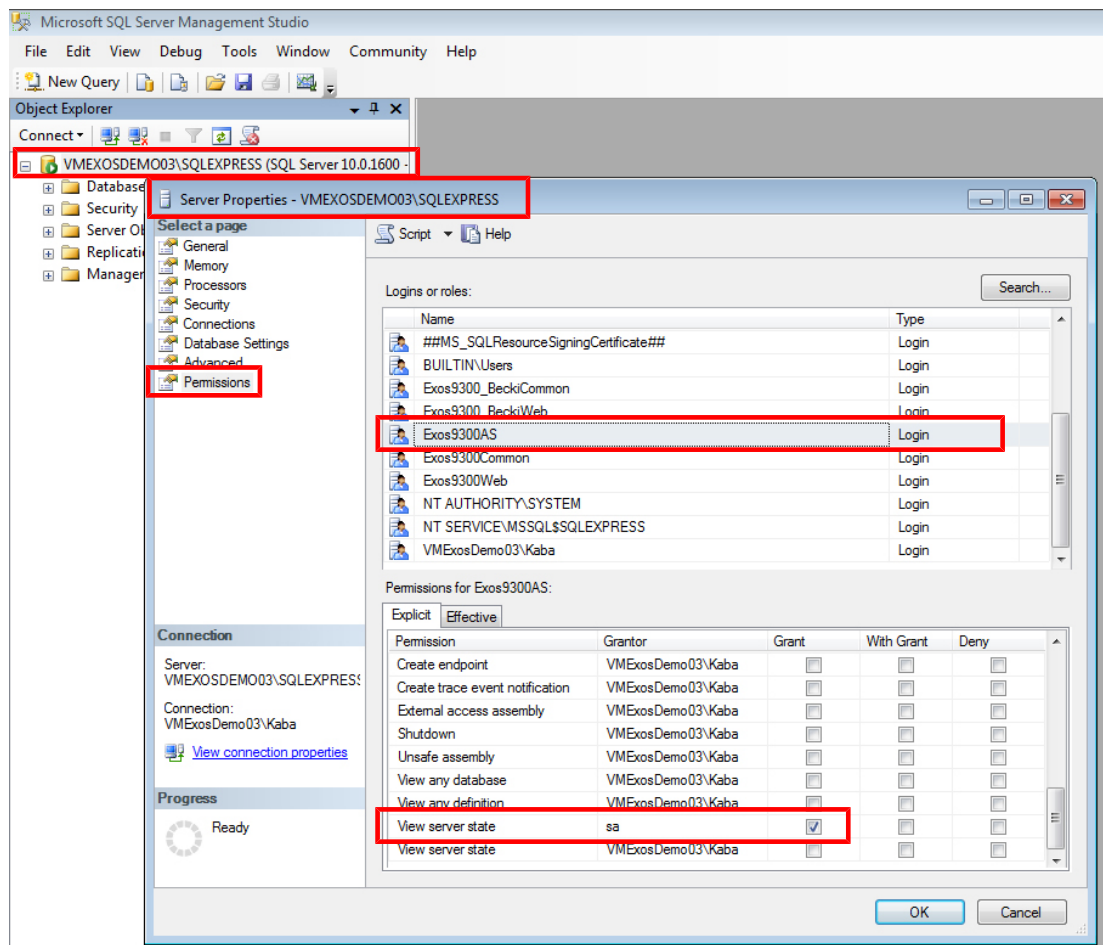


The application service requires the following database authorization:



3.3.1.2 'View server state' permission

The application service user must be assigned the necessary permission ('View server state') via the database properties.





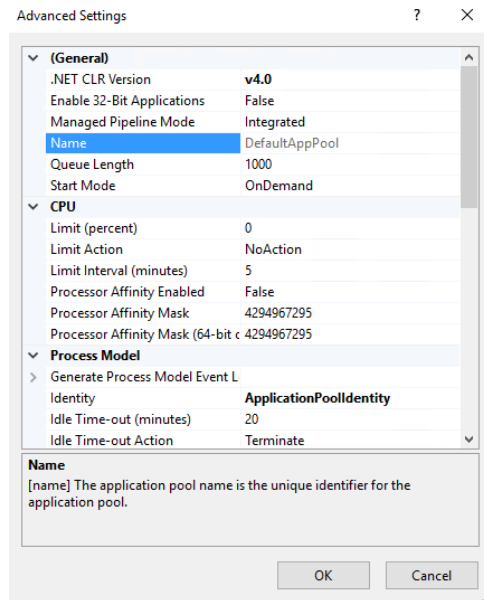
### 3.3.1.3 IIS authorization



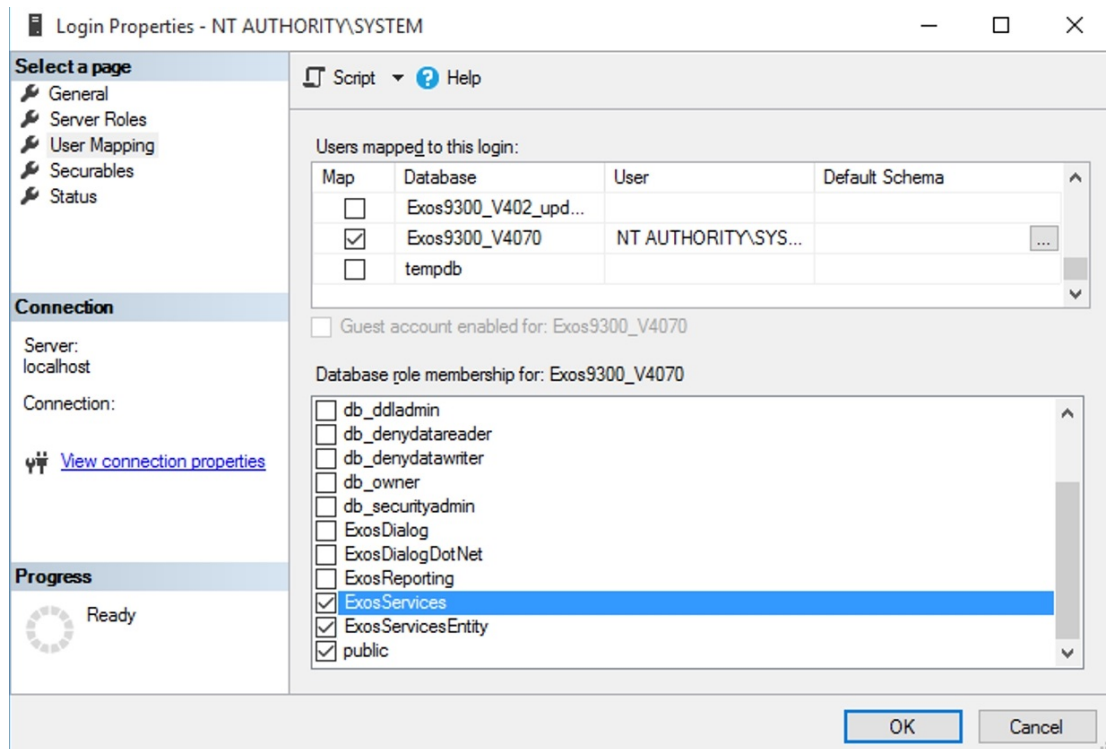
#### NOTICE

If the application server database and the web applications are installed on different servers (see chapter 'System structure [ 2.2]'), a user who has the required authorization for the AS-DB must be entered in the 'Identity' field. It is recommended to enter the user who will be used to execute the services.

#### The IIS requires the following authorization:



#### The IIS requires the following authorization on the AS-DB:



### 3.3.1.4 CORS settings for APIs



#### NOTICE

CORS must only be configured if the web applications that access the APIs run on a different server than the application service.

CORS can be configured for the following API applications using the configuration file:

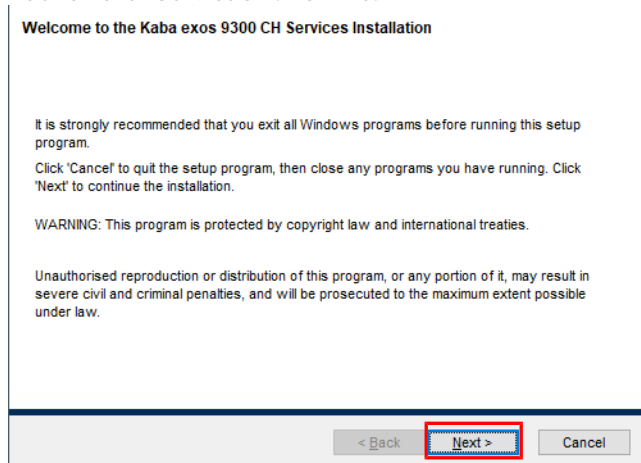
- ExosAPI (web.config)
- ExosAPILogin (web.config)
- ExosCore (appsettings.json)

Detailed information about CORS can be found under [https://en.wikipedia.org/wiki/Cross-origin\\_resource\\_sharing](https://en.wikipedia.org/wiki/Cross-origin_resource_sharing).

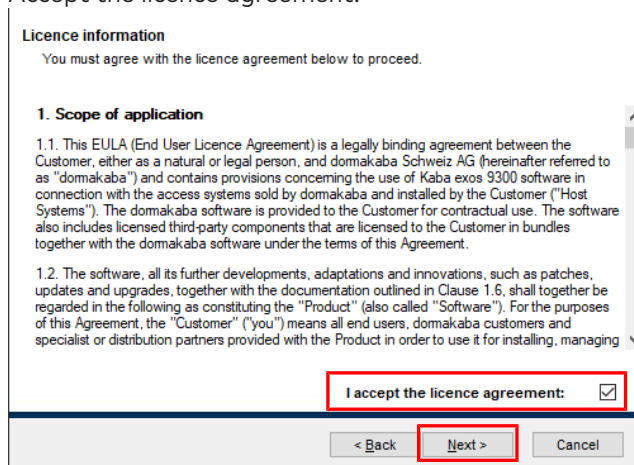
### 3.3.2 Installing the communication hub

✓ The application service is already installed on another computer.

1. Launch the 'ServiceCH.msi' file.

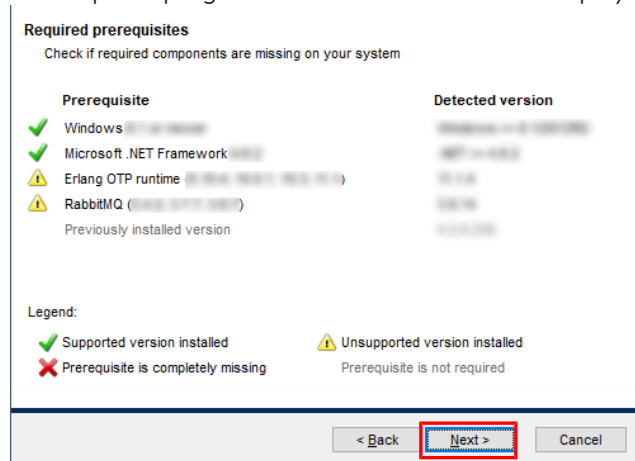


2. Select 'Next'.
3. Accept the licence agreement.

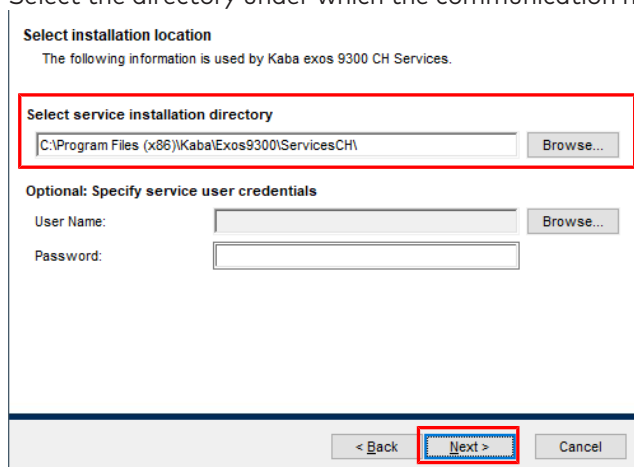


4. Select 'Next'.

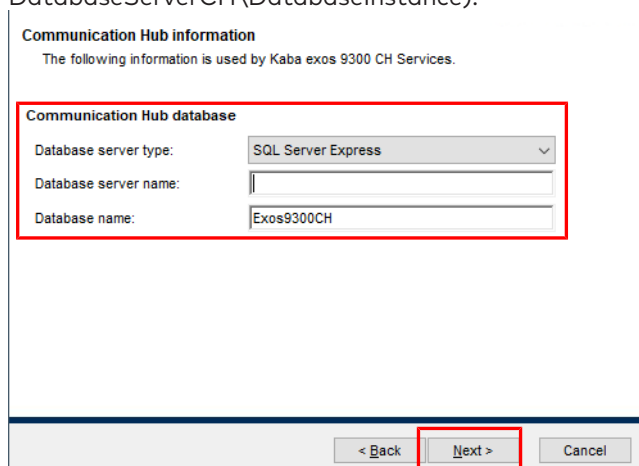
⇒ The required programs and their statuses are displayed.



5. Select 'Next'.
6. Select the directory under which the communication hub is to be installed.

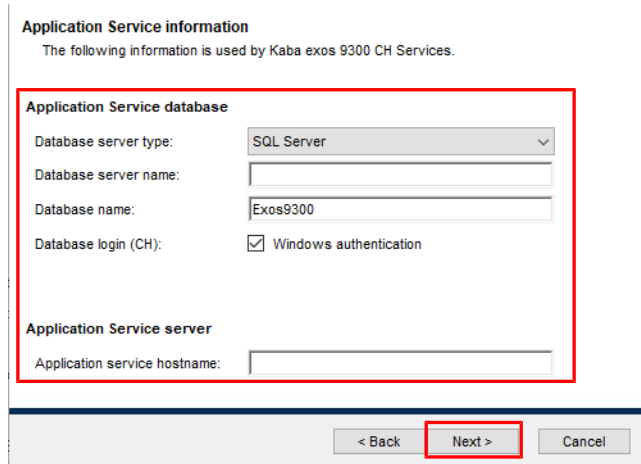


7. Select 'Next'.
8. - Database server type: Select the database server type used.  
 - Database server name: Enter the name of the server on which the communication hub database is installed, including the corresponding instance if necessary (e.g.: DatabaseServerCH\DatabaselInstance).

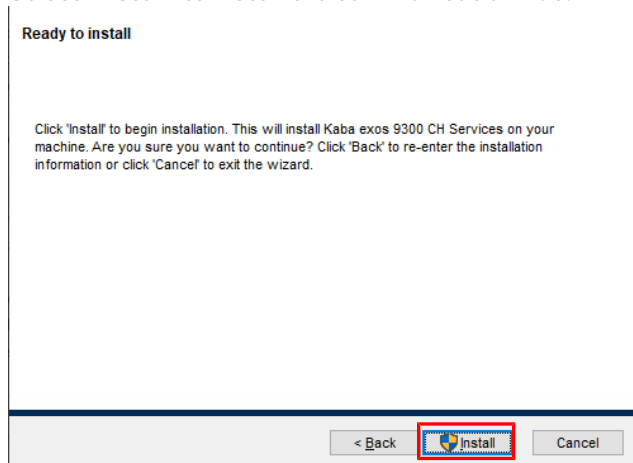


9. Select 'Next'.
10. - Database server type: Select the database server type used.  
 - Database server name: Enter the name of the server on which the application service database is installed, including the corresponding instance if necessary (for example: DatabaseServer\DatabaselInstance).

- Database name: Enter the name of the application service database.
  - Database login (CH): Keep 'Windows authentication' activated.
- To use SQL Server authentication:** Deactivate 'Windows authentication' and enter the database user.
- Attention:** For Oracle, only SQL Server authentication is approved.
- Note:** The database user (and login) must be created manually on the database. The database user requires authorization for the role 'ExosCommHub'. The scripts 'RECREATE\_USER\_Fxx\_v4.1.0.sql' (SQL Server) or 'CREATE\_USER\_Fxx\_v4.1.0.sql' (Oracle) can be used as support. Example: Create the database user 'Exos9300F01' using script and enter it as depicted in the screenshot.



11. Select 'Next'.
12. Select 'Install' to install the communication hub.



- ⇒ Installation starts.
13. Click 'Finish' to end the installation.
  14. Select 'Next'.
- ⇒ The communication hub is installed.

Also see about this

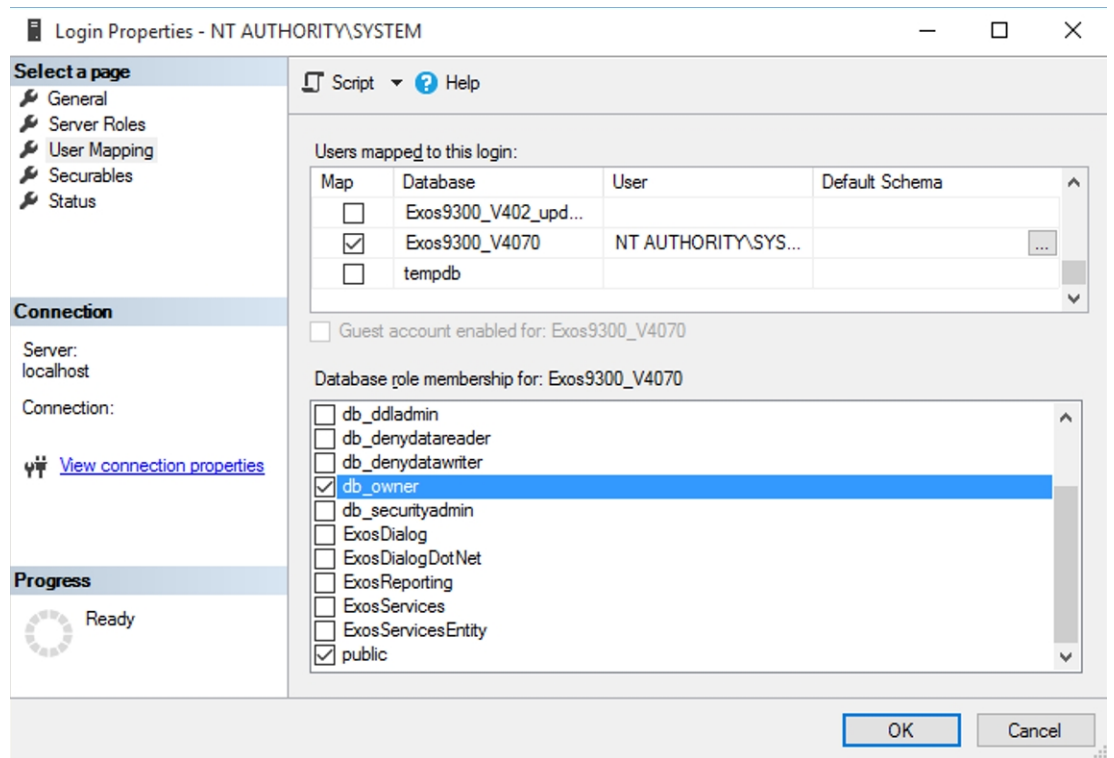
📖 Logins, server roles and user mappings for databases [▶ 16]

### 3.3.2.1 Authorization

**The communication hub requires the following authorization:**

Services (Local)					
Kaba exos 9300 Application Service					
	Name	Description	Status	Startup Type	Log On As
	Kaba exos 9300 Ap...	Kaba exos 9...	Started	Automatic	Local System
	Kaba exos 9300 Co...	Kaba exos 9...	Started	Automatic	Local System

**The communication hub requires the following database authorization:**



A Windows user can be selected in order to execute the communication hub service. If this user is not a Windows administrator, they need to be assigned 'Full access' to the following registry folder:

- 64-bit operating system: \HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\KABA
- 32-bit operating system: \HKEY\_LOCAL\_MACHINE\SOFTWARE\KABA

This command line may also need to be executed:

```
netsh http add urlacl url=http://+:8002/IIDML2CommunicationHubService/
user=DOMAIN\USER listen=yes
```

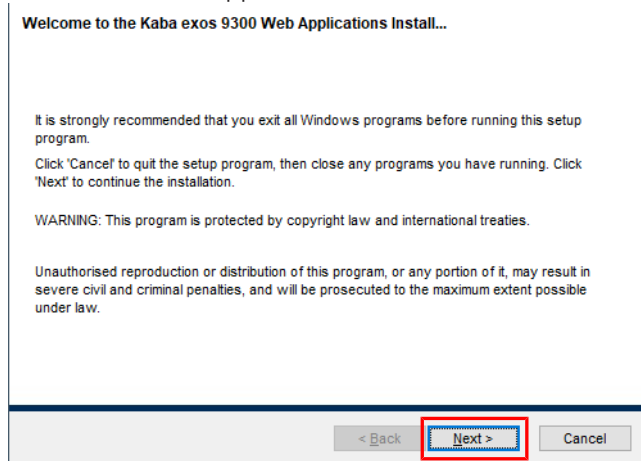
### 3.3.3 Installing web applications



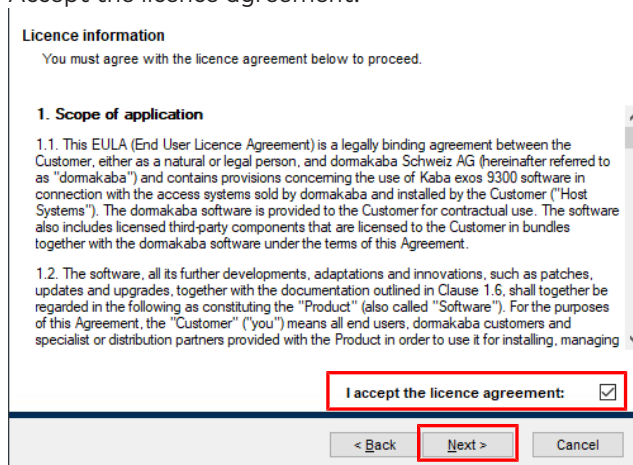
The web applications must have an SSL certificate.

If a certificate for HTTPS has already been configured in IIS, that certificate is used by the web applications by default. If the certificate supplied by Kaba exos is to be used, the existing certificate must be removed before installing the web applications (see the document 'RM\_Kabaexos9300-Web-Applications').

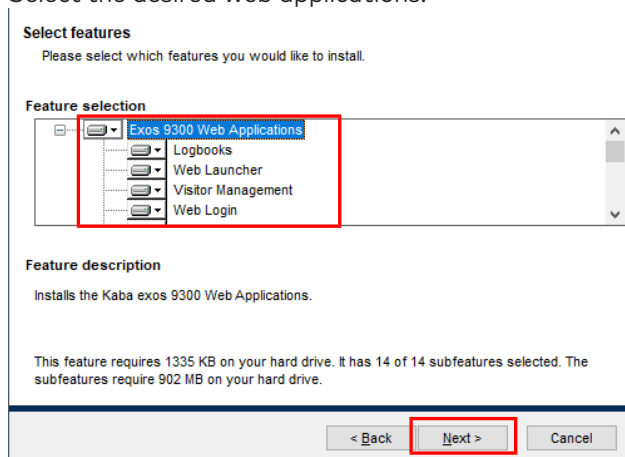
1. Launch the 'WebApps.msi' file.



2. Select 'Next'.
3. Accept the licence agreement.

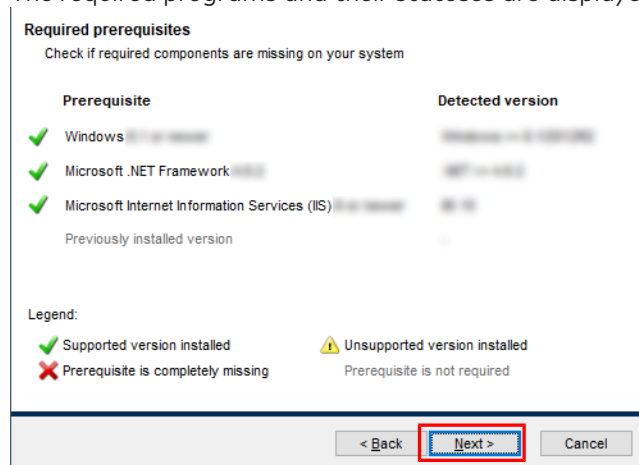


4. Select 'Next'.
5. Select the desired web applications.



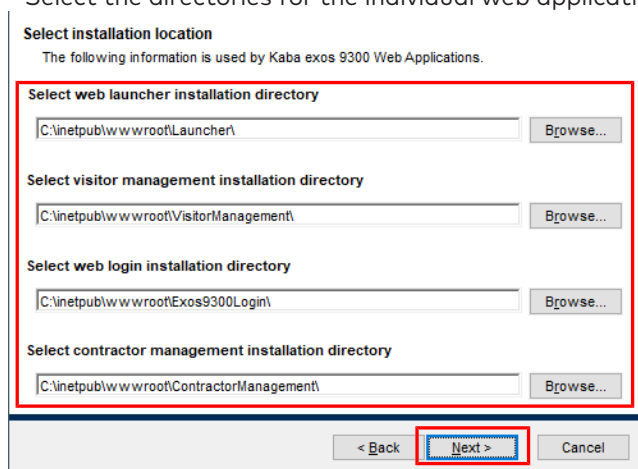
6. Select 'Next'.

⇒ The required programs and their statuses are displayed.



7. Select 'Next'.

- 8. - Select services installation directory: Select the application service directory.
- Select the directories for the individual web applications.

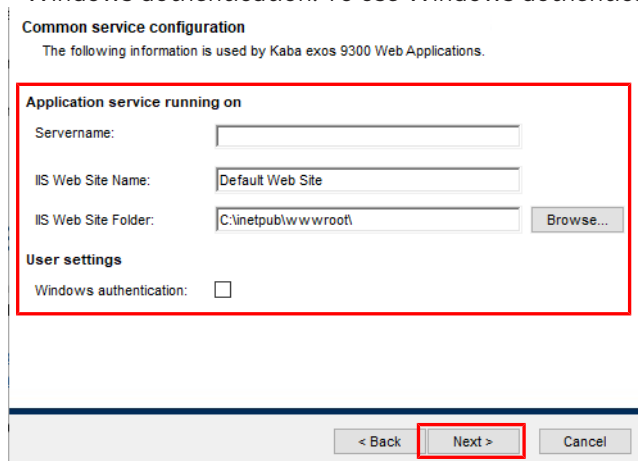


9. Choose 'Next' until you reach the page 'Common service configuration'.

- 10. - Server name: Enter the name of the server on which the application service is installed.
- IIS website name/folder: If the web applications are not to be installed in the IIS under the 'default website', specify the name and/or directory of the website.

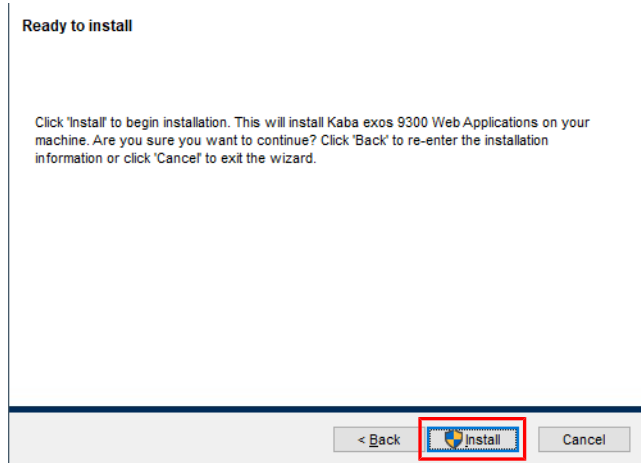
**Attention:** If the web applications are not installed in the same website as that of the API (see section 'Installing the application service'), the valid certificate for each generated website must be assigned after the installation in IIS and the HTTPS binding must be manually configured.

- Windows authentication: To use Windows authentication, select the checkbox.



11. Select 'Next'.

- 12. Select 'Install'.



⇒ Installation starts.

- 13. Click 'Finish' to end the installation.

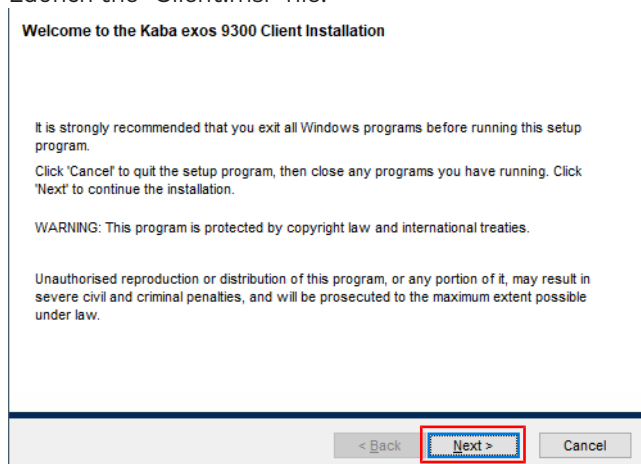
⇒ The web applications are installed.



Further information on IIS can be found in the document 'RM\_Kabaexos9300-Web-Applications'.

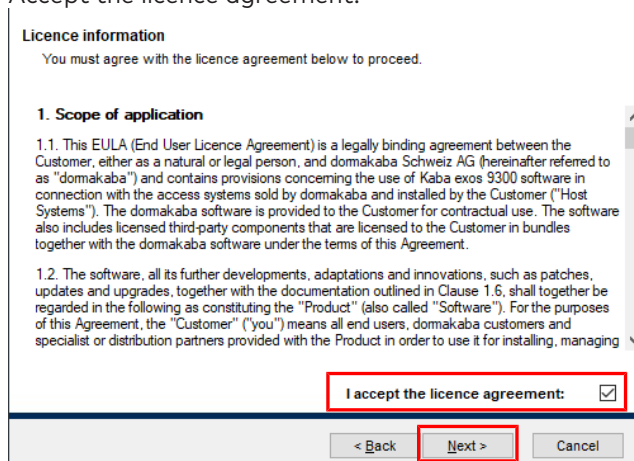
### 3.4 Installing the client

- 1. Launch the 'Client.msi' file.



- 2. Select 'Next'.

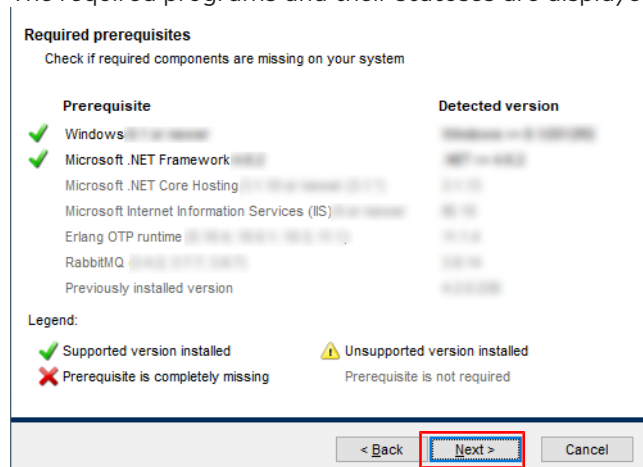
- 3. Accept the licence agreement.



- 4. Select 'Next'.

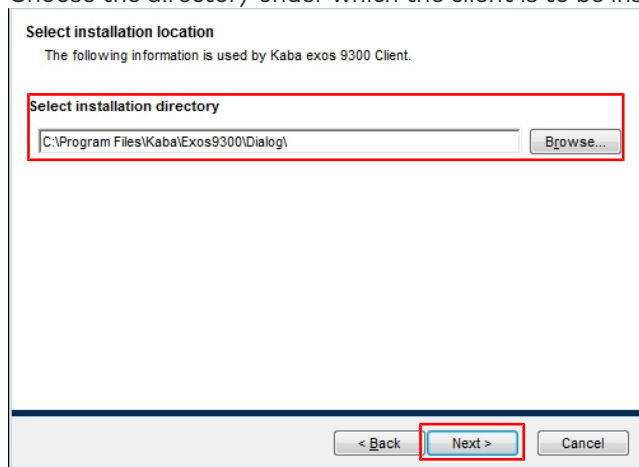


⇒ The required programs and their statuses are displayed.



5. Select 'Next'.

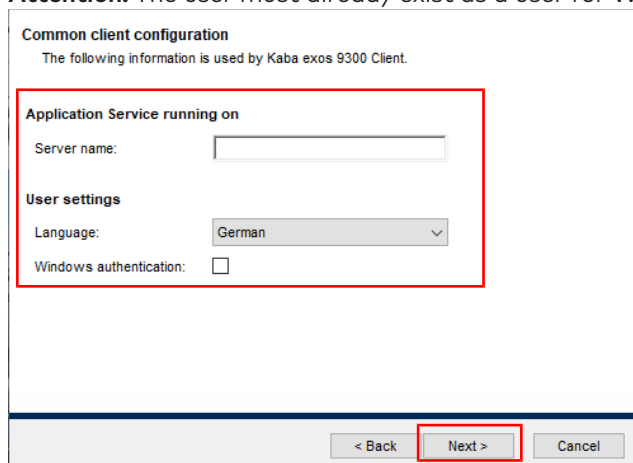
6. Choose the directory under which the client is to be installed.



7. Select 'Next'.

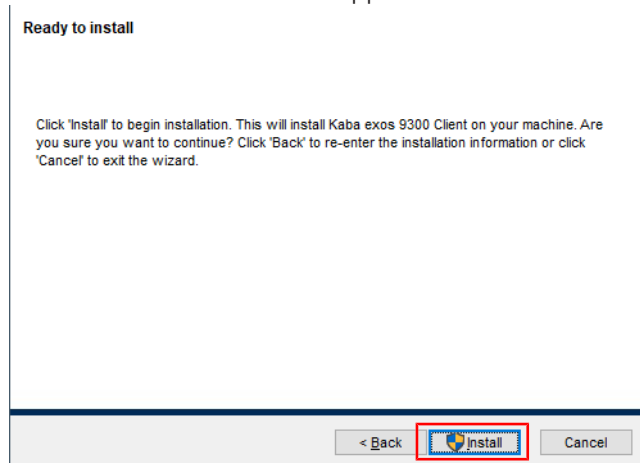
- 8. - Server name: Enter the name of the server on which the application service is installed.
- Language: Select the user language.
- Windows authentication: To use Windows authentication, select the checkbox.

**Attention:** The user must already exist as a user for Windows authentication in Kaba exos.



9. Select 'Next'.

10. Select 'Install' to install the application.



⇒ Installation starts.

11. Click 'Finish' to end the installation.

⇒ The client is installed.

Also see about this

📖 Installing desktop reader service [▶ 34]

### 3.4.1 Installing desktop reader service

If the web applications and the desktop reader are to be used, the desktop reader service must be installed locally.

For this, the 'DesktopReaderService.msi' file must be executed.

CORS must be configured during the installation. Detailed information about CORS can be found under [https://en.wikipedia.org/wiki/Cross-origin\\_resource\\_sharing](https://en.wikipedia.org/wiki/Cross-origin_resource_sharing).

The certificates 'Desktop reader service root <Computername>' and 'Desktop reader service <Computername>' are installed by default.

#### Configuring an SSL certificate

Proceed as follows to use your own SSL certificate for the desktop reader service.

✓ The certificate is installed.

1. Run 'ServiceConfiguration.exe' in the installation directory for the desktop reader service as an administrator.
2. Enter the following values:  
Host: 'localhost' or computer name  
Port: '10800'  
Activate the 'Enable SSL' checkbox
3. Select 'Select certificates'.
  - ⇒ All of the certificates installed on the computer under 'Local computer/Self-signed certificates' are displayed.
4. Select the desired certificate.
5. Select 'OK'.

⇒ The SSL certificate has been configured.



If problems arise when operating the desktop reader with Microsoft Edge, see section 'Known problems [▶ 6.2]'.

### 3.4.2 Installing 3M passport scanner service

The 3M passport scanner service enables passports to be scanned and specific functions within the web applications used.

To install the service, run the file 'MMMPageReaderService.msi' and follow the instructions in the installation assistant.

CORS must be configured during the installation. Detailed information about CORS can be found under [https://en.wikipedia.org/wiki/Cross-origin\\_resource\\_sharing](https://en.wikipedia.org/wiki/Cross-origin_resource_sharing).

After the installation:

- The port can be changed using the file 'MMMPageReaderServiceConfiguration'.
- The service '3M Page Reader Service' must be active.
- The certificates 'MMMPageReaderService<computer name>' and 'MMMPageReaderService root <computer name>' must be present.



---

In case of problems in the operation of the scanner with Microsoft Edge see chapter 'Known problems [▶ 6.2]'.

---

### 3.4.3 Installing Mitek passport scanner service

The Mitek passport scanner service enables Spanish forms of identification (passport, ID card, driving licence) to be scanned and specific functions within the web applications used.

To install the service, run the file 'MitekIDService.msi' and follow the instructions in the installation assistant.

CORS must be configured during the installation. Detailed information about CORS can be found under [https://en.wikipedia.org/wiki/Cross-origin\\_resource\\_sharing](https://en.wikipedia.org/wiki/Cross-origin_resource_sharing).

After the installation:

- The port can be changed using the file 'MitekIDServiceConfiguration'.
- The service 'Mitek ID Service' must be active.
- The certificates 'Mitek ID service <computer name>' and 'Mitek ID service root <computer name>' must be present.



---

In case of problems in the operation of the scanner with Microsoft Edge see chapter 'Known problems [▶ 6.2]'.

---

### 3.4.4 Installing IRIS desktop readers service

With the IRIS desktop reader service, information can be read from Malaysian passports so specific functions within the web applications can be used.

Before installing the IRIS desktop reader service, the 'IRIS Smart Reader SCR21U' driver must be installed as described by the manufacturer.

To install the service, run the file 'IrisCardReaderService.msi' and follow the instructions in the installation assistant.

CORS must be configured during the installation. Detailed information about CORS can be found under [https://en.wikipedia.org/wiki/Cross-origin\\_resource\\_sharing](https://en.wikipedia.org/wiki/Cross-origin_resource_sharing).

After the installation:

- The port and the certificate can be changed using the file 'IrisCardReaderServiceConfiguration.exe' in the installation folder. The process corresponds to that of the normal desktop reader: see section 'Installing desktop reader service [▶ 3.4.1]'.
- The service 'IRIS Card Reader Service' must be active.

- The certificates 'IRIS card reader service <computer name>' and 'IRIS card reader service root <computer name>' must be present.



---

In case of problems in the operation of the desktop reader with Microsoft Edge see chapter 'Known problems [▶ 6.2]'.  

---

### 3.4.5 Installing signature reader

Proceed as follows in order to install the signature reader:

1. Download the software 'WebSocket Pad Server' (from version 1.1.2) from the [Signotec website](#) and then launch the software.
  - ⇒ The installation wizard is launched.
2. Select the language, then select 'OK' and 'Next >'.
  - ⇒ The installation wizard is launched.
3. Accept the licence agreement and then select 'Next >'.
  - ⇒ The installation wizard is launched.
4. Use the preset default settings and select 'Next >' twice.
  - ⇒ The installation wizard is launched.
5. Select 'Install!'.
  - ⇒ The signature reader is installed.
6. Select 'Complete'.
  - ⇒ The installation is complete.



---

If Windows is unable to find the installed driver, the software 'WinUSB driver' must also be downloaded from the [Signotec website](#) and then launched.  

---



---

In order to use the signature reader with Mozilla Firefox, the certificate must first be imported into the certificate management. This is not necessary for other browsers.

In case of problems in the operation of the reader with Microsoft Edge see chapter 'Known problems [▶ 6.2]'.  

---



---

The 'signoPAD-API' can also be installed for other configuration options.  

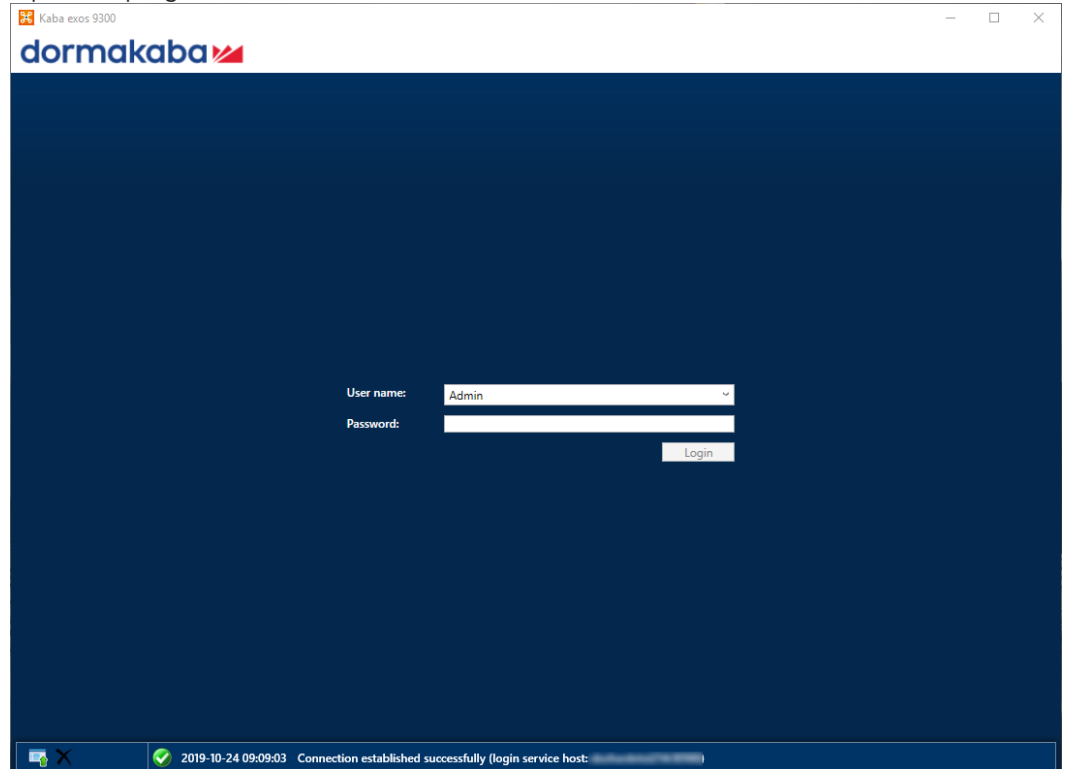
---

# 4 First steps

This section describes the first steps to be taken after the installation of Kaba exos.

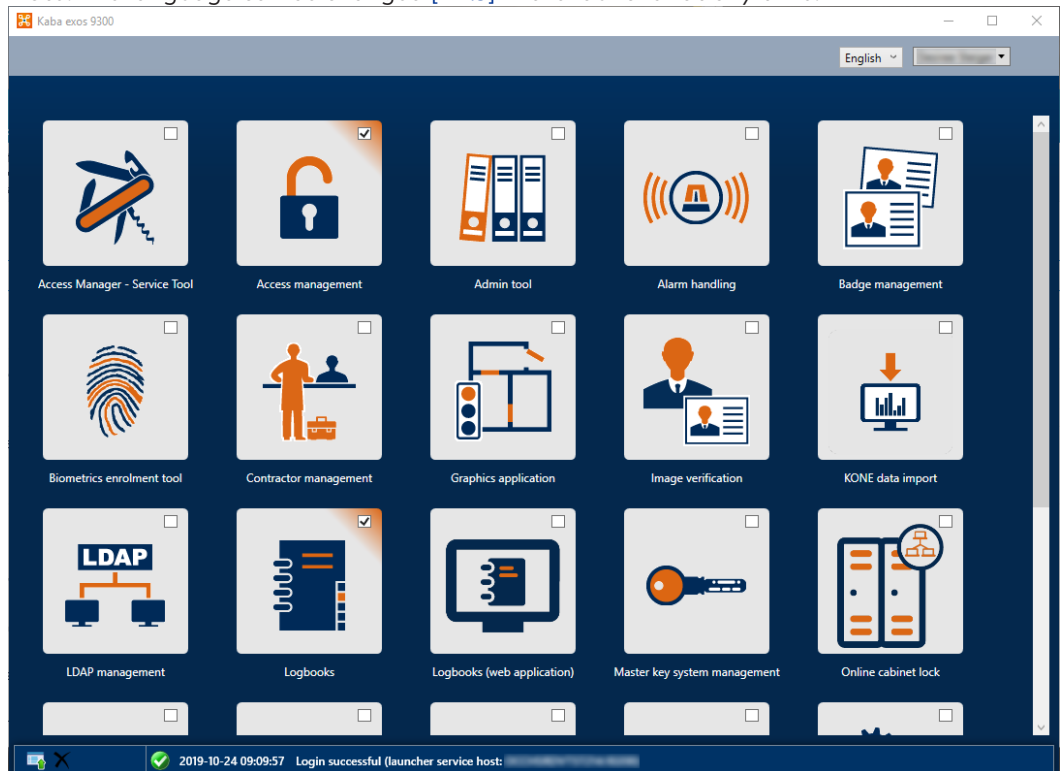
## 4.1 Logging in

1. Open the program via 'Start - Kaba exos'.



- ⇒ The launcher opens in the language saved for the link. The link is created with the language selected during setup.
  - ⇒ Status messages are displayed in the lower area of the launcher.
2. Enter the user name and password (standard: admin, 1234).  
**Note:** The user name is specified in staff data management. Each user can specify their password independently.
3. If more than one tenant is available, select a tenant.
4. On logging in for the first time, replace the old password with a new one.
5. Select 'Check in'.

- ⇒ The launcher opens in the language saved for the database.  
 Note: The language can be changed [▶ 4.3](#) in the launcher at any time.



- ⇒ The programs marked with 'Autostart' (📄) are started automatically and displayed in the taskbar.



**NOTICE**

If the 'r9KabaExosServiceLogin' service has not started or is not accessible on the application server (e.g. port blocked), 'Host selection' appears as the first mask and not 'User name/password'. In this case, contact the system administrator.



With Windows authentication, the launcher starts automatically without one having to enter the user name/password. The login screen will, however, appear after logout. In order to be able to log in with Windows authentication again, the launcher will need to be exited and restarted.



If the error message 'The maximum number of logged in operator stations has been reached' appears, then too many users are logged into the system (licence infringement). It is only possible to log into the system once other users have logged off.

## 4.2 Tray-icon



The 'Kaba exos' tray icon, via which various actions can be executed, can be found at the bottom right in the taskbar.

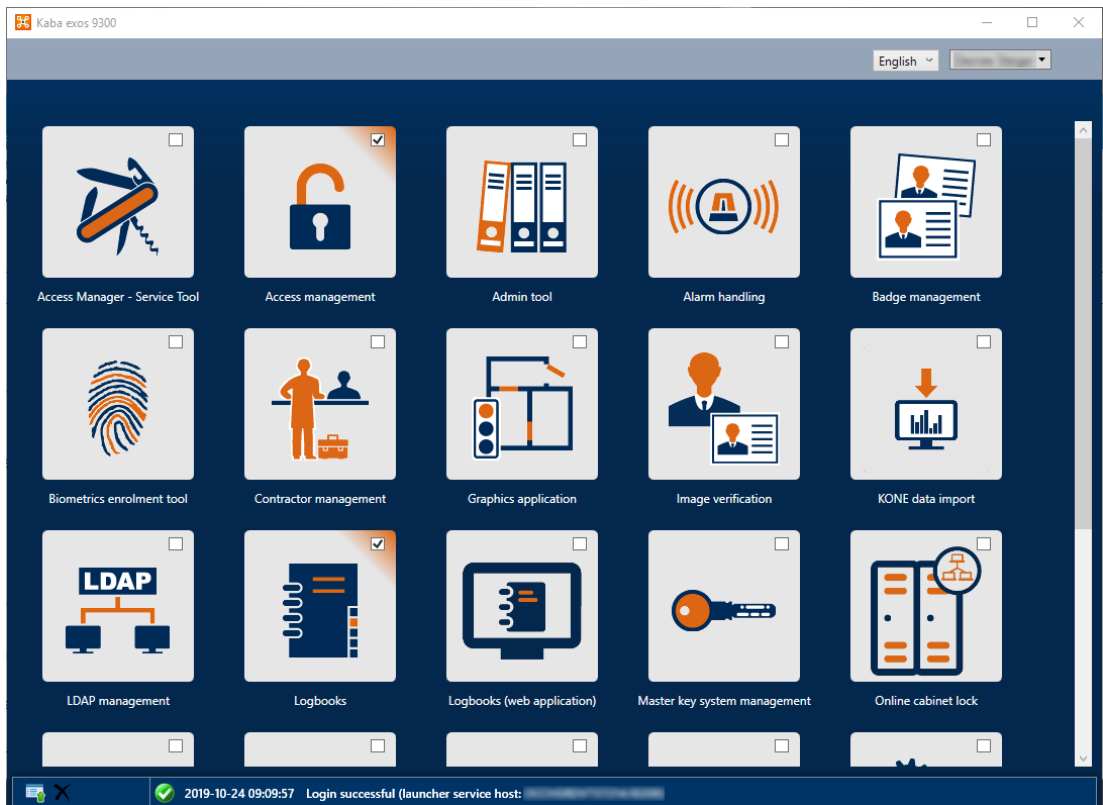
- **Mouseover:** Displays information about the version.
- **Double-click:** Opens the launcher.
- **Right-click:** Opens the tray icon menu in the current language.

The following actions are possible via the tray icon menu:

- **Display launcher:** The launcher is displayed in the foreground.
- **Applications:** The Kaba exos applications and customer-specific applications are displayed and started. Applications that have already been started are marked with a dot.
- **Languages:** The installed languages are displayed and can be changed.
- **Minimise launcher instead of closing it:** Here it is possible to define whether clicking the cross icon at the top-right of the dialogue closes the launcher and logs the user out or minimises the launcher to the tray-icon. This setting can also be made for the entire system (see the document 'RM\_Kabaexos9300-System-and-Settings'). For safety reasons, the launcher is closed by default, and the user is checked out.
- **Minimise launcher on start-up:** Here it is possible to define whether the launcher remains open in the background or whether it is minimised to the tray-icon.  
**Note:** This only works if 'Autostart' is activated for at least 1 application (see Logging in [▶ 4.1](#)).
- **Change password:** Passwords can be changed here. The launcher changes to the password dialogue and your password can be changed.
- **Logout:** The user is logged out. The tray icon disappears and the login dialogue is displayed again.
- **Close:** All Kaba exos applications including the tray icon are closed.  
**Note:** All open applications are closed automatically on these actions. Any unsaved changes will be lost.

### 4.3 Launcher

The applications are started via the launcher. The applications that will be displayed and started depends on the relevant user authorizations [▶ 4.4].



The icons in the launcher can be moved using drag-and-drop. The position of the icons will be saved for the user who is logged in and will be retained after they log off.

#### Open applications



1. Click on an icon with the left mouse button.
  - ⇒ The corresponding application opens.
  - ⇒ Applications already opened are highlighted in colour and will be brought into the foreground when they are clicked again.
  - ⇒ If the checkbox  is selected, then the application will start automatically after successful login (Autostart). This setting is user-specific.

#### Change language

The language can be changed using the selection list. After this change, all newly-started applications will be opened in the new language. The language of applications that are already open will not change.

The following languages are supported:

- German
- English
- French
- Italian



### Other actions

Other actions can also be carried out, some of which are also covered by the tray icon menu:

Additional information about Kaba exos is displayed:

Information	Remark
Company	Company to which the licence is issued
Licence	Customer name
Release	Software version
Expiration date	Licence expiration date
Dialogue release	Dialogue version
Host login	Host address of login service
Application host	Host address of application service
User	Logged-in user
Tenant	Name of the tenant

- **Change password:** Passwords can be changed here. The launcher changes to the password dialogue and your password can be changed.
- **Logout:** The user is logged out. The tray icon disappears and the login dialogue is displayed again.
- **Close:** All Kaba exos applications including the tray icon are closed.  
**Note:** All open applications are closed automatically on these actions. Any unsaved changes will be lost.

## 4.4 Authorizations

In the web applications under 'Menu – User groups management', it is possible to set the authorizations for the relevant applications. A user will have access/no access to corresponding applications depending on the authorizations. In addition, non-authorized applications will not appear for a user in the launcher.




---

Modifications to the user authorisations of a registered user are not valid immediately. The user must log out and log in again for the changed user authorisations to become valid.

---

# 5 Additional information

This chapter provides additional information about the product.

## 5.1 Encrypted communication between the CH and the access manager

A secure connection (encrypted and trusted) can be configured between the communication hub (CH) and the access manager 92 xx. To achieve this, both the CH and the access manager must have certificates.

These certificates can be generated using either an existing master root certificate or a new master root certificate. A master root certificate is a certificate with a private key that is only used for issuing additional certificates.



### NOTICE

Prior to configuration, it must be ensured that the type of access manager used supports the 'TLS' function.



If the IP address or the port of the access manager is changed, the access manager and the CH must be restarted.

### 1. Install a master root certificate

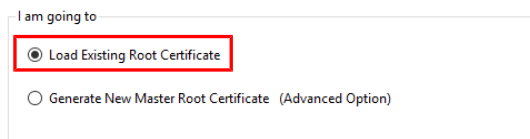
Either an existing master root certificate can be installed, or a new master root certificate can be generated and installed.

In order to install an **existing master root certificate**, proceed as follows:

1. Execute the 'FSServiceConfiguration.exe' file in the 'ServicesCH' folder of the Kaba exos installation.
2. Choose 'Load Existing Root Certificate'.

Master Root SSL

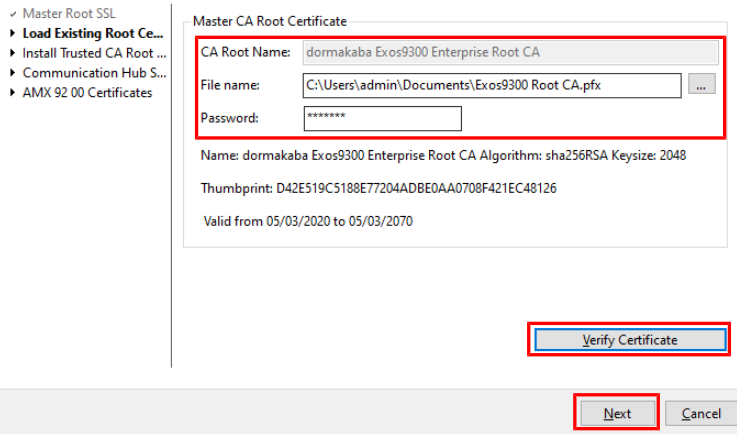
- ▶ Master Root SSL
- ▶ Load Existing Root Cert...
- ▶ Install Trusted CA Root...
- ▶ Communication Hub S...
- ▶ AMX 92 00 Certificates



3. Select 'Next'.
4. Select the storage location and file name for the master root certificate.
5. Enter the password for the master root certificate.
6. Select 'Verify Certificate'.

⇒ The master root certificate has been verified and the thumbprint is displayed.

Load Existing Root Certificate



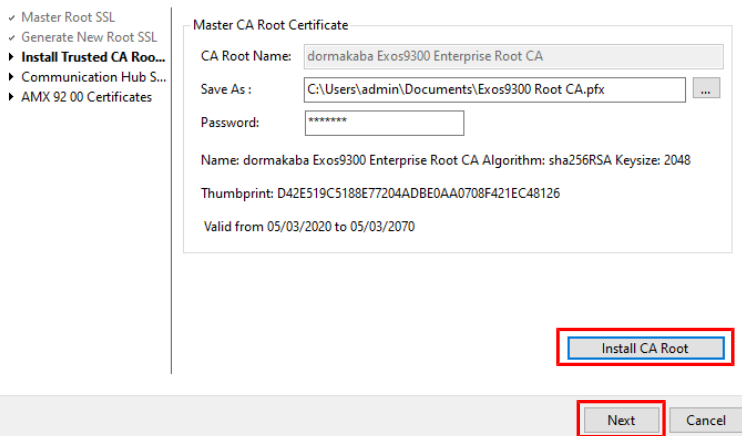
7. Select 'Next'.

8. Select 'Install CA Root'.

⇒ The master root certificate has been installed.

⇒ The certificate 'Exos Enterprise Trust root CA' can be found in the 'Microsoft Management Console' (mmc.exe).

Install Trusted CA Root Certificate



9. Select 'Next'.

10. Follow the instructions from section '2. Generating and assigning a certificate to the CH'.

In order to generate and install a **new master root certificate**, proceed as follows:



**NOTICE**

The master root certificate should be stored in a safe place and a security copy must be created.

1. Run the 'FSServiceConfiguration.exe' file in the 'Services' folder of the Kaba exos installation.

2. Select 'Generate New Master Root Certificate'.

Master Root SSL

- ▶ Master Root SSL
- ▶ Load Existing Root Cert...
- ▶ Install Trusted CA Root...
- ▶ Communication Hub S...
- ▶ AMX 92 00 Certificates

I am going to

Load Existing Root Certificate

**Generate New Master Root Certificate (Advanced Option)**

3. Select 'Next'.

4. Under 'SSL Properties' in the 'Key Length' field, select the key length, then choose the algorithm under 'Signing Algorithm'.

5. Select the storage location and file name for the master root certificate.

6. Enter a password for the master root certificate.

7. Select 'Generate Master Root Certificate'.

⇒ The master root certificate has been generated and the thumbprint is displayed.

Generate New Root SSL

- ✓ Master Root SSL
- ▶ **Generate New Root S...**
- ▶ Install Trusted CA Root ...
- ▶ Communication Hub S...
- ▶ AMX 92 00 Certificates

Master CA Root Certificate

CA Root Name: dormakaba Exos9300 Enterprise Root CA

Save As : C:\Users\admin\Documents\Exos9300 Root CA.pfx

Password: \*\*\*\*\*

Name: dormakaba Exos9300 Enterprise Root CA Algorithm: sha256RSA Keysize: 2048

Thumbprint: D42E519C5188E77204ADBE0AA0708F421EC48126

Valid from 05/03/2020 to 05/03/2070

---

SSL Properties

Key Length: 2048      Signing Algorithm: SHA256

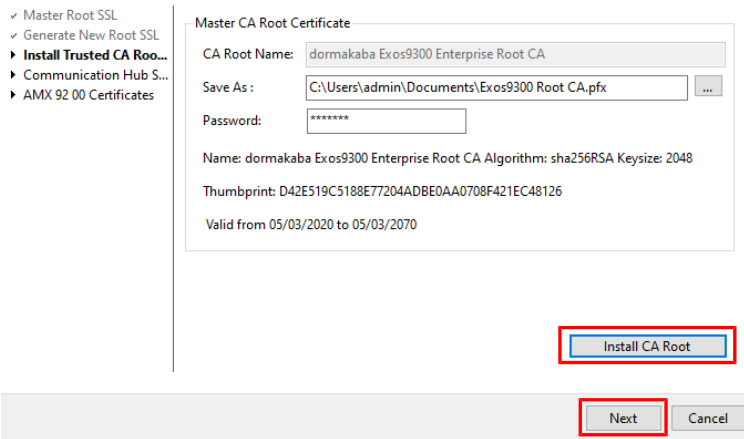
8. Select 'Next'.

9. Select 'Install CA Root'.

⇒ The master root certificate has been installed.

- ⇒ The certificate 'Exos Enterprise Trust root CA' can be found in the 'Microsoft Management Console' (mmc.exe).

**Install Trusted CA Root Certificate**

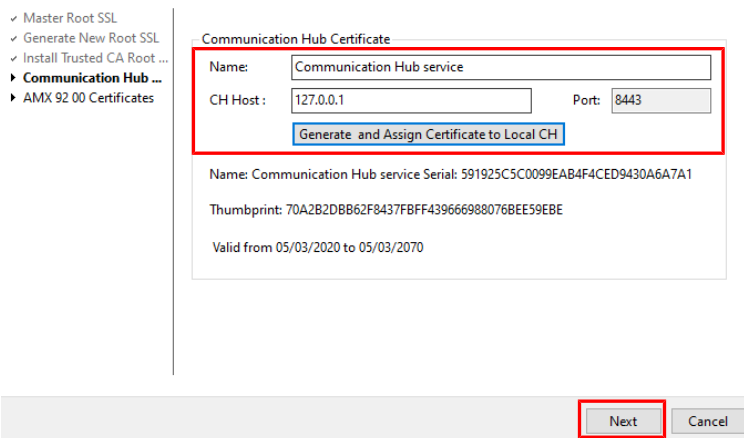


10. Select 'Next'.

**2. Generating and assigning a certificate to the CH**

1. Enter a name for the certificate.
2. Enter the IP address of the CH.
3. Select 'Generate and Assign Certificate to Local CH'.
  - ⇒ The certificate has been generated and assigned to the local CH.
  - ⇒ The certificate can be found in the 'Microsoft Management Console' (mmc.exe).

**Communication Hub SSL**



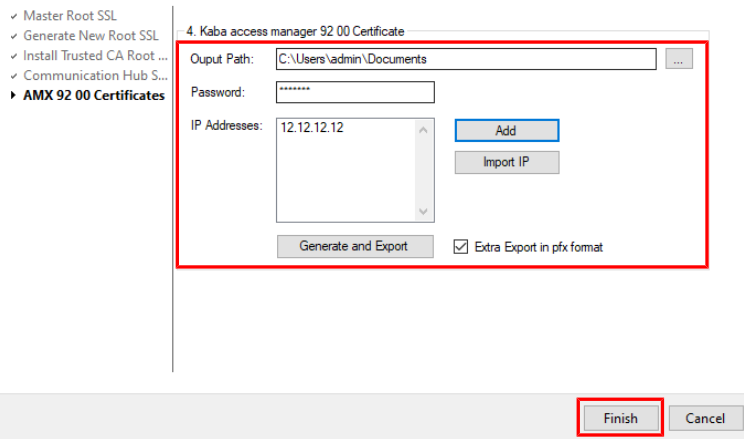
4. Select 'Next'.
5. Restart the CH.

**3. Generating an access manager certificate**

1. Select the storage location for the certificate.
2. Enter the password for the certificate.
3. Enter or import the access manager IP address via 'Add' or 'Import IP'.
4. If necessary, repeat step 3 for further access managers.
5. Select 'Generate and Export'.

- ⇒ A certificate with the file extension 'pem' has been generated and saved in the specified storage location for each IP address entered.

AMX 92 00 Certificates



- Adjust the certificate name if necessary.
- Click 'Finish'.

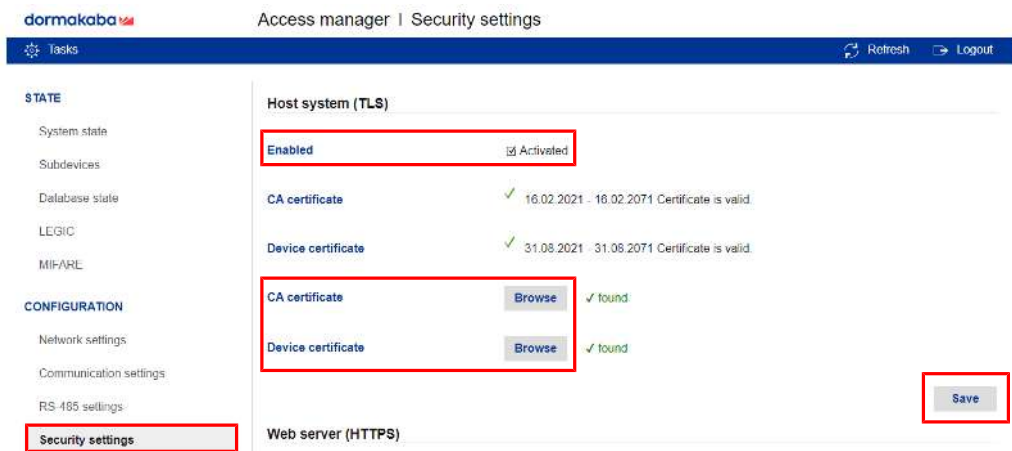
### 4. Integrating a certificate into the access manager



#### NOTICE

The following steps must be carried out in a secure environment (e.g. secure network, crosslink cable) so that the certificate and password cannot be accessed by unauthorized parties.

- ✓ The access manager web interface is open.
  - In the menu, select 'Configuration – Security settings'.
  - Set 'TLS' to 'activated'.
    - ⇒ Further options are shown.
  - For 'CA certificate', select the master root certificate (e.g. cacert.pem).
  - For 'Device certificate', select the certificate for the access manager (e.g. devicecert 12.12.12.pem) and enter the password.
  - Click 'Save'.



- Restart the access manager.
  - ⇒ The certificate has been integrated into the access manager.

### 5. Activate TLS in system management

- ✓ The system management is opened and the access manager is selected.

1. Activate 'TLS'.
2. Adjust the port number, if necessary.

The screenshot shows a configuration form for an access manager. The 'port number' field is highlighted with a red box and contains the value '8443'. The 'TLS' checkbox is checked. The 'Name' field contains 'Access manager 92 00' and the 'activated' checkbox is checked. The 'IP address' field contains '12 . 12 . 12 . 12'. The 'Type' dropdown menu is set to 'Kaba access manager 92 00 LEGIC'.

3. Restart the CH.
- ⇒ The CH has been configured.

### Display certificate

The following command in the Windows command prompt can be used to display the certificate that has been assigned to the standard port '8443':

```
netsh http show sslcert ipport=0.0.0.0:8443
```

### Integrating any certificate

The following command in the Windows command prompt can be used to assign any certificate to the standard port '8443':

```
httpcfg set ssl -i 0.0.0.0: 8443 -h <thumbprint of the certificate>
```

Example:

```
httpcfg set ssl -i 0.0.0.0: 8443 -h 0000000000003ed9cd0c315bbb6dc1c08da5e6
```

The CA root certificate integrated in this way must also be installed on the access manager.

## 5.2 API help

Swagger is used for the Kaba exos API documentation. Swagger is an open source framework for the design, creation, documentation and use of APIs.

Swagger offers the following advantages:

- Interactive documentation (direct testing of API functions via 'Try it out')
- Range of tools offered (Swagger Editor, Swagger UI, etc.)
- User-friendly interface

### 5.2.1 Access

The API help is integrated in every Kaba exos system and is generated from the JSON files that are available by default in the 'C:\inetpub\wwwroot\ExosApi\Help\Help' directory.

#### Show API help

For security reasons and to avoid misuse, the API help is hidden by default. To show the API help, the 'Web.config' or 'appsettings.json' file on the web server must be adapted in the corresponding directory:

#### Show API help for 'ExosApi'

In the .../inetpub/wwwroot/ExosApi/Web.config file,

remove the following entries:

```
<hiddenSegments>
<add segment="Help" />
<add segment="index.html" />
<add segment="errorCodes.html" />
</hiddenSegments>
```

Set the 'ShowAPIHelp' parameter to 'true':

```
<appSettings>
<add key="ShowAPIHelp" value="true" />
</appSettings>
```

#### Show API help for 'ExosAPILogin'

In the .../inetpub/wwwroot/ExosAPILogin/Web.config file,

remove the following entries:

```
<hiddenSegments>
<add segment="Help" />
<add segment="index.html" />
<add segment="errorCodes.html" />
</hiddenSegments>
```

Set the 'ShowAPIHelp' parameter to 'true':

```
<appSettings>
<add key="ShowAPIHelp" value="true" />
</appSettings>
```

In the .../inetpub/wwwroot/ExosApi/Web.config file,

remove the following entries:

```
<hiddenSegments>
<add segment="Help" />
<add segment="index.html" />
<add segment="errorCodes.html" />
</hiddenSegments>
```

#### Show API help for 'ExosFrontendAPI'

In the .../inetpub/wwwroot/ExosFrontendAPI/Web.config file,

remove the following entries:

```
<hiddenSegments>
<add segment="Help" />
<add segment="index.html" />
<add segment="errorCodes.html" />
</hiddenSegments>
```

Set the 'ShowAPIHelp' parameter to 'true':

```
<appSettings>
<add key="ShowAPIHelp" value="true" />
</appSettings>
```

#### Show API help for 'ExosCore'

##### Adapt 'appsettings.json'

In the .../inetpub/wwwroot/ExosCore/appsettings.json file,

set the 'ShowAPIHelp' parameter to 'true':

```
ShowApiHelp:true
```

The 'ExosCore' or IIS website needs to be restarted for the modification to become active in the 'appsettings.json' file.

You can call up the API help for 'ExosCore' via <https://servername/ExosCore/help/index.html>.

Use the following links to call up the API help:

[https://\[server\\_name\]/exosapilogin](https://[server_name]/exosapilogin)

[https://\[server\\_name\]/exosapi](https://[server_name]/exosapi)

If no installed Kaba exos system is available, you can access the Kaba exos demo system. Just send a request to the support team ([support.exos@dormakaba.com](mailto:support.exos@dormakaba.com)).



## 5.3 Resolution of host names

The host name should only resolve exactly 1 IP address. If the host name resolves several IP addresses, there is a risk that not all service endpoints will use the same IP address. Some services also provide their functionality for each resolved IP address, which poses an unnecessary security risk. An IP address can also be used instead of a host name. For IPv6 addresses, however, it must be noted that the address must be enclosed in square brackets ([ ]) (according to RFC 2732). The automatic addition of brackets has not yet been implemented consistently in Kaba exos.

## 5.4 Replacing a self-signed certificate

A self-signed certificate is automatically created and assigned for WCF (Windows Communication Foundation) services and the exos ERP service (interface to B-COMM ERP/EACM) when the application server is installed and updated. It is recommended to replace this certificate with a trustworthy one.

The certificate can be replaced in 2 ways:

- manually, as explained in the documentation from Microsoft
- using the provided 'Application Server Configuration' tool (u9ApplicationServerConfiguration.exe)

Follow the steps below to replace the certificate on the application server using the Application Server Configuration tool:

- ✓ Services are operated with default ports.
  - ✓ Trustworthy certificate is available.
1. Execute the 'u9ApplicationServerConfiguration.exe' file.
  2. Choose 'Select Certificate...'.
    3. Select the certificate.
    4. Click 'Save'.
- ⇒ The certificate has been replaced. The desired certificate must be manually added to the certificate store on the client computers.

# 6 Troubleshooting

This section provides important information on remedying product errors.

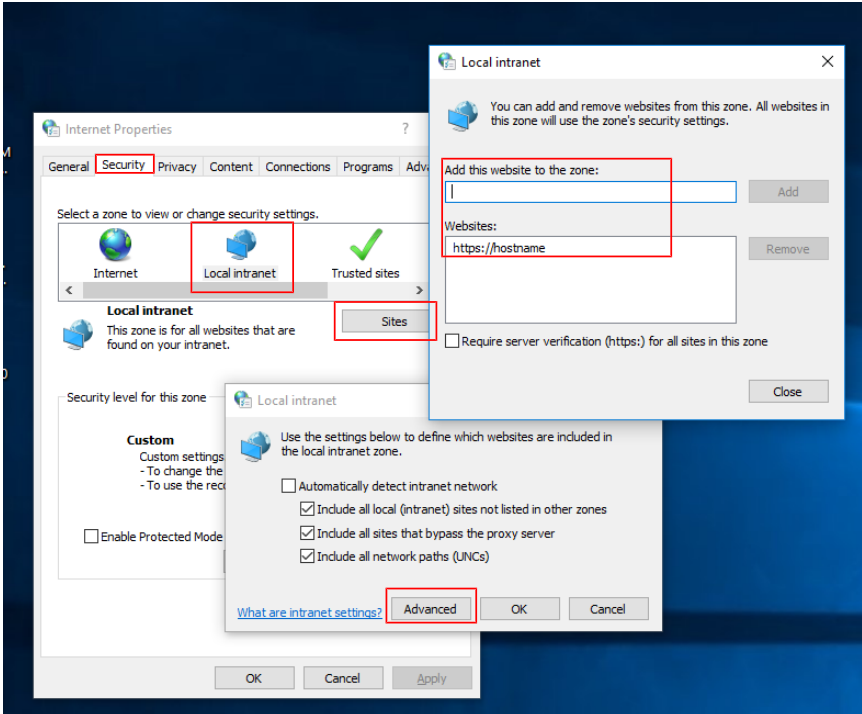
## 6.1 Error analysis

If the installation fails, the logbook can be activated to analyse the errors. To do this, open the Windows command prompt in the installation file directory and enter the following command:

```
msiexec /i "Service.msi" /L*V "log.log"
```

The task steps are recorded in the file 'log.log'.

### 6.1.1 Browser asks for login data

<p>Problem</p>	<p>When calling the web applications, the browser asks the user for login data.</p>
<p>Cause</p>	<p>The browser cannot determine whether the server, on which the web applications are installed, is located on the local intranet.</p>
<p>Solution</p>	<p>Add the server to the local intranet.</p> <p>For Microsoft Edge and Google Chrome, the internet options can be defined as follows:</p>  <p>For Mozilla Firefox, the following procedure is followed:</p> <ol style="list-style-type: none"> <li>1. In Firefox, enter 'about:config' in the address bar.</li> <li>2. In the search bar, enter 'network.automatic-ntlm-auth.trusted-uris'.</li> <li>3. In the corresponding row, add the desired page.</li> <li>4. Save the modifications.</li> <li>5. Restart the browser.</li> </ol>

## 6.2 Known problems

### API no longer available

Problem	After uninstalling the web applications, the API is no longer available.
Cause	During uninstallation of web applications (WebApps.msi), the 'Exos9300WebPool' application pool needed for the API was deleted.
Solution	Reinstall or refresh the services (feature 'exos API' from Services.msi).

### No access to APIs from browser

Problem	Unlike other applications (e.g. 'Postman'), it is not possible to access the API endpoints 'ExosAPI' and 'ExosCore' from the web application.
Cause	The CORS settings have not been correctly configured in the APIs' configuration files. The error messages can be checked with the help of the developer tools of the browser.
Solution	Correctly configure the CORS settings in the APIs' configuration file - sCORS settings for APIs <a href="#">▶ 3.3.1.4</a>

### Missing information in the access management reports

Problem	The message 'Error when retrieving data...' appears in the access management reports.
Cause	<ul style="list-style-type: none"> <li>The incorrect version of Microsoft Report Viewer is installed.</li> <li>The sequence of installation of the components was not correct.</li> </ul>
Solution	<ol style="list-style-type: none"> <li>Uninstall the current version of Microsoft Report Viewer.</li> <li>Install the correct version of Microsoft Report Viewer.</li> </ol>

### Troubleshooting for Microsoft Edge

Certain functions of local services (desktop reader, IRIS etc.) may not work correctly with Microsoft Edge.

If this is the case, proceed as follows:

- Execute the Windows command prompt as the administrator.
- Execute the following command:  

```
CheckNetIsolation LoopbackExempt -a
-n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
```
- Restart Microsoft Edge.

If the problem persists, one of the following two commands can be attempted:

```
CheckNetIsolation LoopbackExempt -a
-n=Microsoft.Windows.Spartan_cw5nlh2txyewy
```

```
CheckNetIsolation LoopbackExempt
-a -
p=S-1-15-2-3624051433-2125758914-1423191267-1740899205-1073925389-3782572162
-737981194
```

If the problem reappears after restarting the PC, then the issue lies with the PC's basic settings. In this case, the IT department must be consulted in order to deactivate the resetting of the basic settings.

## 6.3 Reporting a problem to support

### Kaba exos 9300 support

Software support is organised as follows:

- 1st level support by customer (based on individual agreement)
- 2nd level support by local dormakaba sales partner (RMO)

- 3rd level support by dormakaba Switzerland Ltd, Product Development, Access Solutions EMEA

### 6.3.1 General information regarding a support case

The 3rd level support from Kaba exos 9300 is guaranteed by dormakaba Switzerland Ltd, Product Development, Access Solutions EMEA. The problem descriptions are reported via the [web portal](#).

Please provide the following information for effective processing of support requests:

#### Basic information

- Name of the customer
- Installation location/project
- Product/version
- Communication hub
- Database version
- Hardware
- Error

#### Additional information

- Brief, concise error description in the subject line
- Detailed error description:
  - Since when has the problem been occurring? What has been changed?
  - What have you already done to solve the problem?
  - What are the results of the analyses already performed?
  - What is the priority of this case and, if high priority, what is the reason?

#### Case-specific information

- Screenshots of the error messages; if details are available, send along the text file
- Windows event logs (export them)
- Associated error messages from the cTrace database table
- Logbooks: Access, Display, Download, System, Alarm, Error and T&A, etc.
- Screenshots of the configuration, registry entries, etc.
- Hardware used and the associated firmware versions
- Operating system used, database management system including version (SQL Server or Oracle)
- Description of the system structure; a diagram of the structure may be useful for complex systems and depending on the problem




---

Provide the customer databases and the Kaba exos 9300 system license to the support only upon request.

---

#### Support contact information

##### dormakaba Support Portal:

<https://support.ead.dormakaba.com/hc>

##### Online Access Control Systems (Kaba exos, online periphery):

E-mail: [support.exos@dormakaba.com](mailto:support.exos@dormakaba.com)

Hotline: +41 44 818 93 38









[www.dormakaba.com](http://www.dormakaba.com)

dormakaba Schweiz AG  
Hofwisenstrasse 24  
8153 Rümlang  
Switzerland  
T: +41 (0)44 818 93 11  
[www.dormakaba.com](http://www.dormakaba.com)

dormakaba Schweiz AG  
Mühlebühlstrasse 23  
8620 Wetzikon  
Switzerland  
T: +41 (0)44 931 61 11  
[www.dormakaba.com](http://www.dormakaba.com)

dormakaba EAD GmbH  
Albertstraße 3  
78056 Villingen-Schwenningen  
Germany  
T: +49 7720 603-0  
[www.dormakaba.com](http://www.dormakaba.com)  
Company headquarters:  
Villingen-Schwenningen