

Dongle Manager



Installation manual for system providers

5/20/2019

Product line neo, version 6.x

The described functions can be used with the following ASC products:

EVOIPneo

EVOLUTIONneo / XXL / eco

INSPIRATIONneo

Please note that you can always find the most up-to-date technical documentation and product updates in the partner area on our website at <http://www.asctechnologies.com>.

Copyright © 2019 ASC Technologies AG. All rights reserved.

Windows is a registered trademark of Microsoft Corporation. VMware® is a registered trademark of VMware, Inc. All other marks and names mentioned herein may be trademarks of their respective companies.

Contents

1	General information	4
2	Introduction	5
3	Installation requirements	6
4	Installation	7
5	Uninstalling.....	13
6	Availability and downtime of the Dongle Manager	15
	List of figures	16
	List of tables	17
	Glossary	18

General information

In the context of this document ASC represents ASC Technologies AG, its subsidiaries, branch offices, and distributors. An up-to-date overview of the aforementioned entities can be found at <https://www.asctechnologies.com>

ASC assumes no guarantee for the actuality, correctness, integrity or quality of the information provided in the manuals.

ASC regularly checks the content of the released manuals for consistency with the described hardware and software. Nevertheless, deviations cannot be excluded. Necessary revisions are included in subsequent editions.

Some aspects of the ASC technology are described in general terms to protect the ownership and the confidential information or trade secrets of ASC.

The software programs and the manuals of ASC are protected by copyright law. All rights on the manuals are reserved including the rights of reproduction and multiplication of any kind, be it photo mechanical, typographical or on digital data media. This also applies to translations. Copying the manuals, completely or in parts, is only allowed with written authorization of ASC.

Representative, if not defined otherwise, is the technical status at the time of the delivery of the software, the devices and the manuals of ASC. Technical changes without specified announcements are reserved. Previous manuals lose their validity.

The general conditions of sales and delivery of ASC in their latest version apply.

2 Introduction

This manual describes the installation of the application Dongle Manager.

The application Dongle Manager fulfils the following functions:

- Reading the dongle

If you operate the recording system in a virtual environment and no Internet connection to ASC is available, a dongle is required. The dongle contains the order number and the system ID. This system information serves to authenticate and /or to release the license file.

For information about the configuration of a virtualization refer to the installation manual *Configuration virtualization*.

- Management of the password database for neo key management

The passwords for the neo key management are saved in a separate database. This database can be installed [geo-redundantly](#). The application Dongle Manager manages the storage of passwords in the database and the synchronization of the geo-redundant database server.

For information about the neo key management refer to the administration manual *Encryption of recordings*.

3 Installation requirements

- **Licenses**

You do not need an additional license to use the application Dongle Manager.

- **Installation file**

The installation file of the application Dongle Manager must be decompressed on a local hard disk of the server.

You can download the installation file on the website <http://www.asctechnologies.com>. You find all released versions of the application in the partner area in *FTP - Software Download > neo Suite > DongleMan*.

- **Usage of a dongle**

If you use the application Dongle Manager together with a dongle, the application must be installed on the same server that the dongle has been connected to.

4 Installation

1. Select the menu item *Mount* from the context menu of the installation file (ISO format).
⇒ The content of the setup package is displayed.

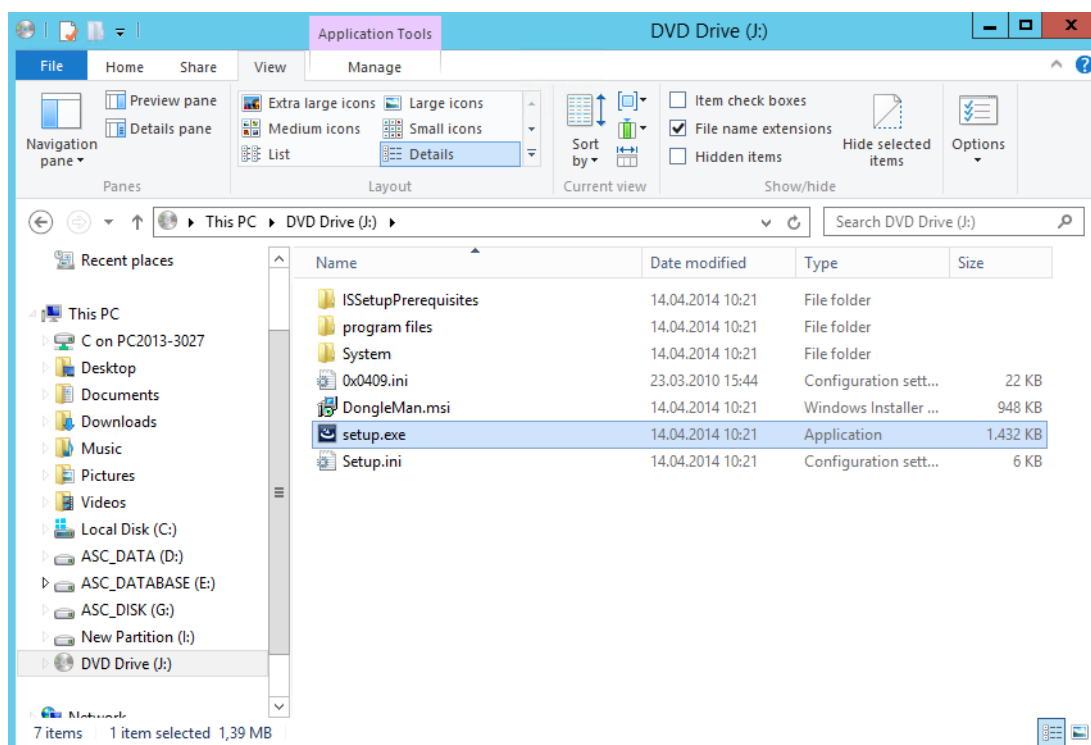


Fig. 1: File Setup.exe

2. From the context menu of the file *setup.exe*, select the menu item *Run as Administrator*.
⇒ The welcome screen appears.

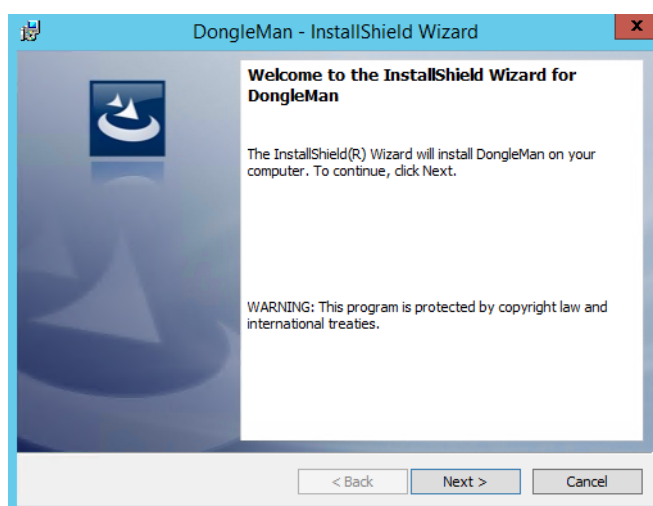


Fig. 2: Welcome screen - Dongle Manager

3. Click on the button *Next*.
⇒ The following window appears displaying the components to be installed:

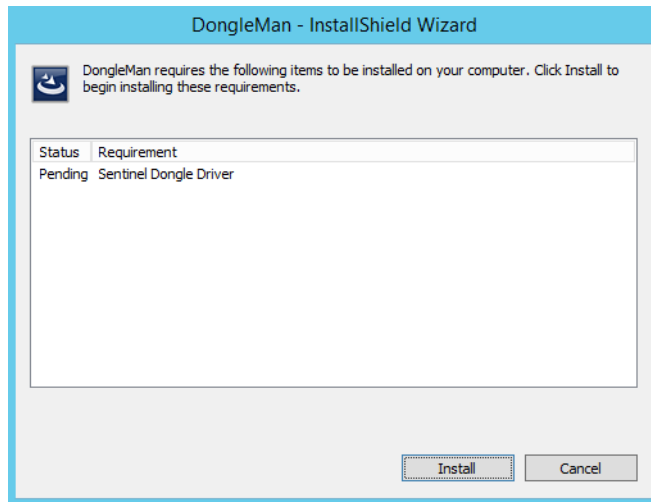


Fig. 3: Install Sentinel System Driver

4. Click on the button *Install* to start the installation routine for the Sentinel System Driver.
 - ⇒ The welcome screen appears.



Fig. 4: Welcome screen - Sentinel System Driver

5. Click on the button *Next*.
 - ⇒ The window *License Agreement* appears.

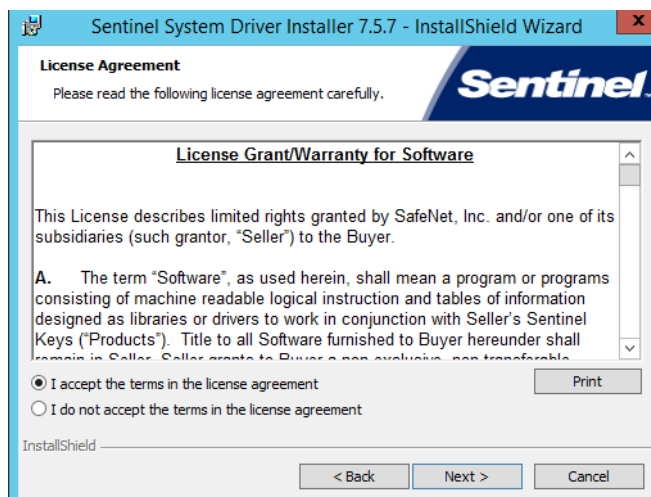


Fig. 5: Confirm license agreement - Sentinel System Driver

6. Select the option *I accept the terms in the license agreement* to confirm the license agreement for the Sentinel System Driver.
7. Click on the button *Next*.
 - ⇒ The window *Setup Type* appears.

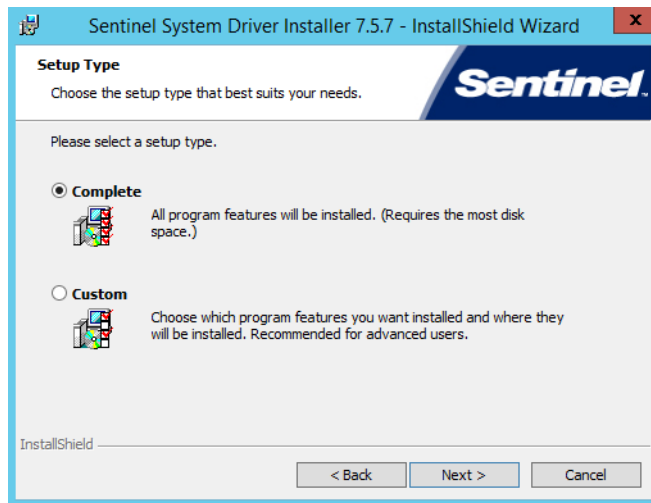


Fig. 6: Select setup type - Sentinel System Driver

8. Select the option *Complete* as installation type.
9. Click on the button *Next*.
 - ⇒ The window to start the installation of the Sentinel System Driver appears.

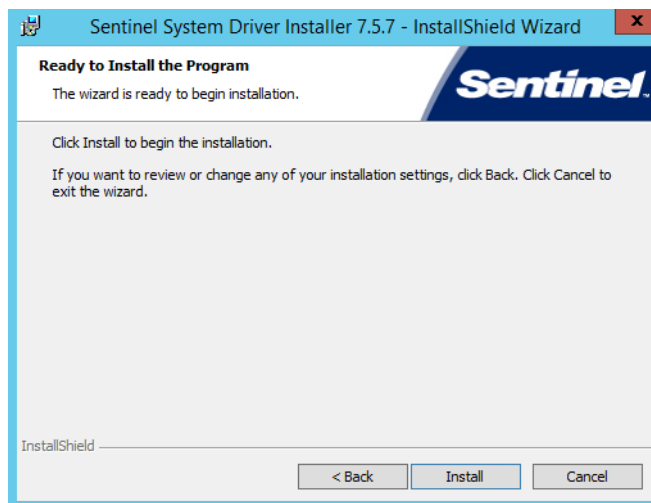


Fig. 7: Start installation process - Sentinel System Driver

10. Click on the button *Install*.
 - ⇒ After the installation process a window informing users about the successful installation of the Sentinel System Driver appears.

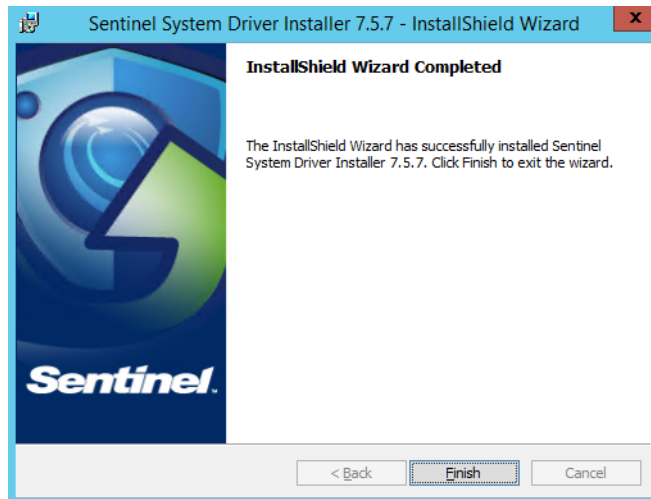


Fig. 8: Finish installation - Sentinel System Driver

11. Click on the button *Finish*.

⇒ The welcome screen of the InstallShield Wizard for the Dongle Manager appears.

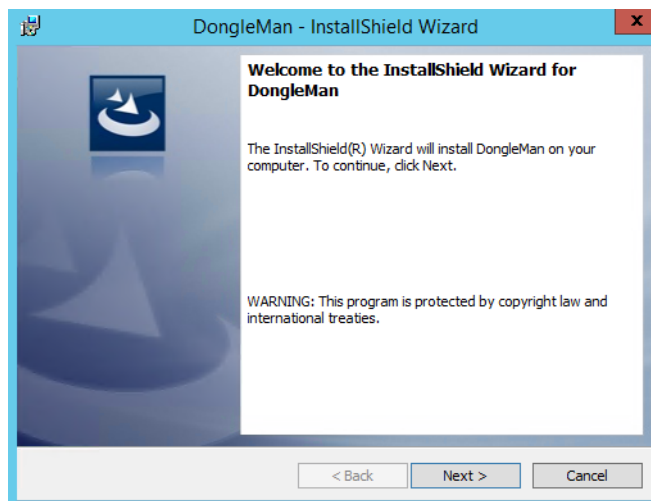


Fig. 9: Welcome screen - Dongle Manager

12. Click on the button *Next*.

⇒ The window to select the installation path appears.

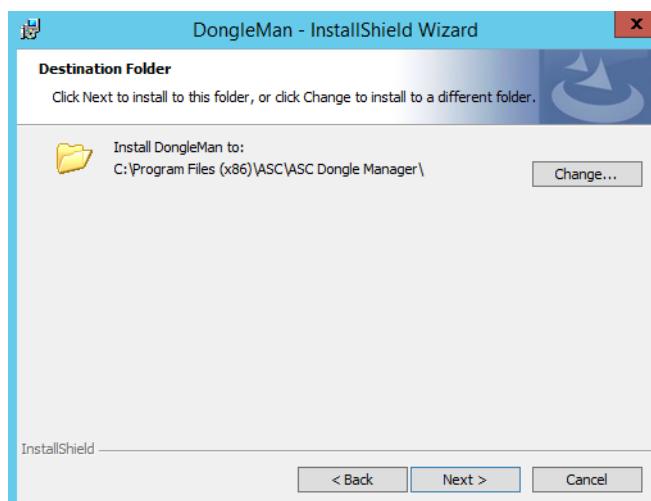


Fig. 10: Select installation path - Dongle Manager

13. Click on the button *Change* to change the target directory of the installation.

14. Click on the button *Next* to confirm the path.
 ⇒ The window for entering the listener port appears.

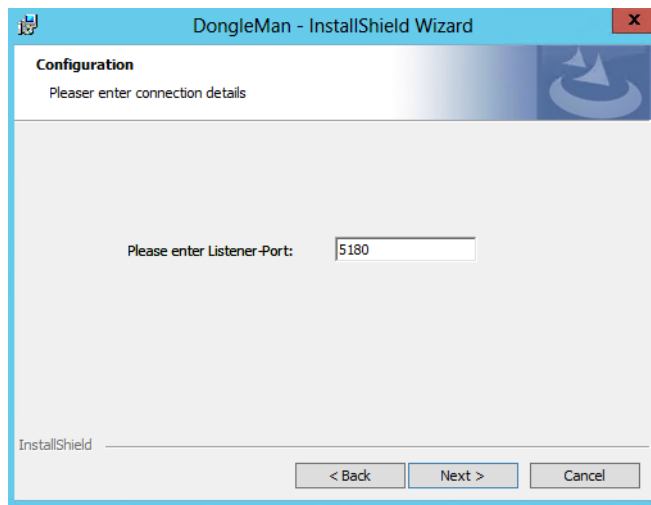


Fig. 11: Configure port - Dongle Manager

15. Enter the listener port.
 On this port, the Dongle Manager receives the incoming requests of all configured IP addresses and uses this port to send its answers.
16. Click on the button *Next* to confirm the entry.
 ⇒ The window to enter the **geo-redundant** servers for the password database of the key management appears.

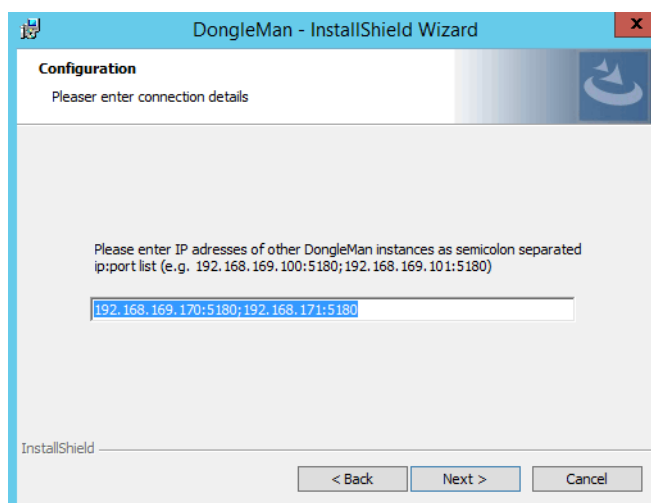


Fig. 12: Enter IP addresses and ports of the geo-redundant server - Dongle Manager



To ensure recording in the event the application Dongle Manager fails, you can install the application and thus the password database redundantly on additional servers. The application Dongle Manager ensures that the geo-redundant password databases are synchronized regularly. If a server that the application Dongle Manager runs on fails, you can activate the application Dongle Manager manually on another server.

For further information about the synchronization and geo-redundancy of the password database refer to the administration manual *Encryption of recordings*.

17. Enter the IP addresses and the ports of the geo-redundant servers for the password database of the key management appears.
NOTICE! Use a semicolon as separator.
18. Click on the button *Next* to confirm the entry.

⇒ The window to select the availability appears.

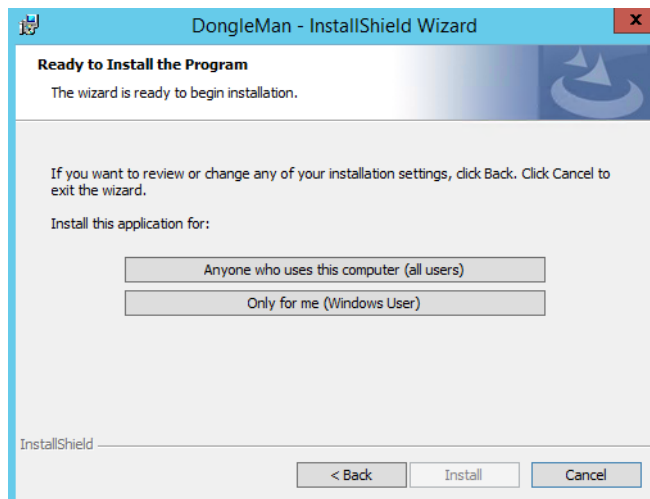


Fig. 13: Select availability for users - Dongle Manager

19. Click on the button *Anyone who uses this computer (all users)* to make the application available to all users.

⇒ The button *Install* becomes active.

20. Click on the button *Install* to start the installation process.

⇒ After the installation process a window informing users about the successful installation of the Dongle Manager appears.

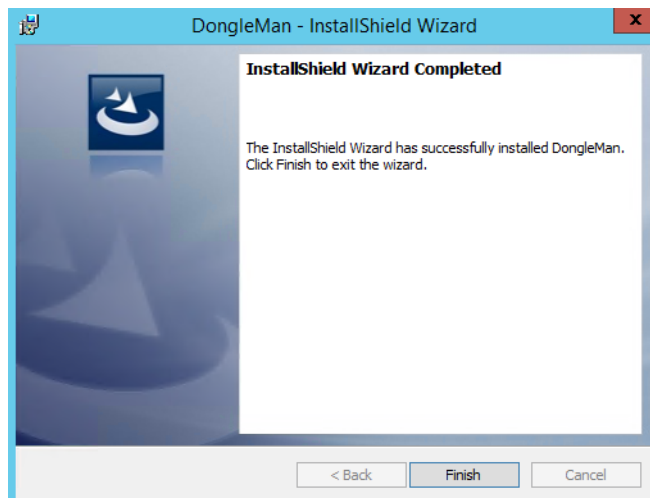


Fig. 14: Finish installation - Dongle Manager

21. Click on the button *Finish* to finish the installation.

⇒ The application has been installed.

⇒ You find the services DongleMan and DongleManConnector under *Server Manager > Tools > Services*.

22. Restart the server to start the application.



If you would like to change the port for the communication with the Enterprise Core subsequently, you have to adjust this parameter in the configuration file *ASC.DongleMan.ini*. You find this file in the installation path, e. g. *C:\Program Files (x86)\ASC\ASC Product Suite\data*.

5

Uninstalling

1. Select the menu item *Mount* from the context menu of the installation file (ISO format).
⇒ The content of the setup package is displayed.
2. From the context menu of the file *setup.exe*, select the menu item *Run as Administrator*.
⇒ The welcome screen of the InstallShield Wizard appears.

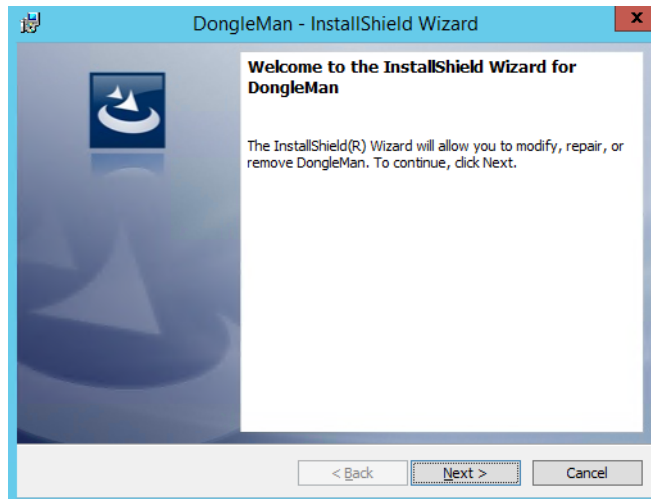


Fig. 15: Welcome screen - InstallShield Wizard

3. Click on the button *Next*.
⇒ The window *Program Maintenance* appears.

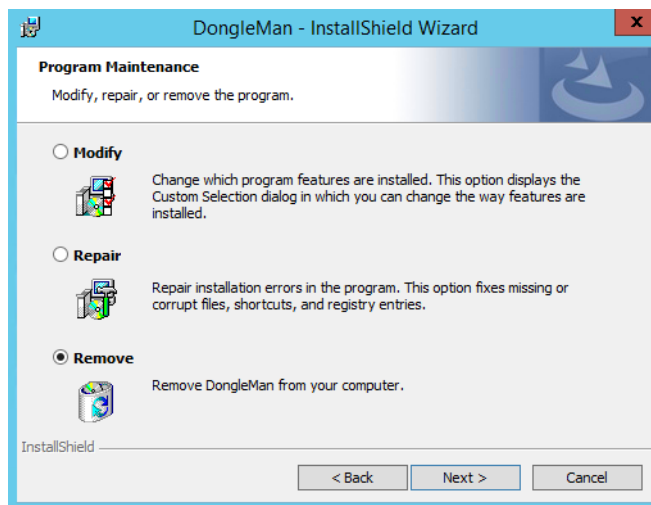


Fig. 16: Options for program maintenance

4. Select the option *Remove* to remove the application.
5. Click on the button *Next*.
⇒ The window with the security prompt appears.

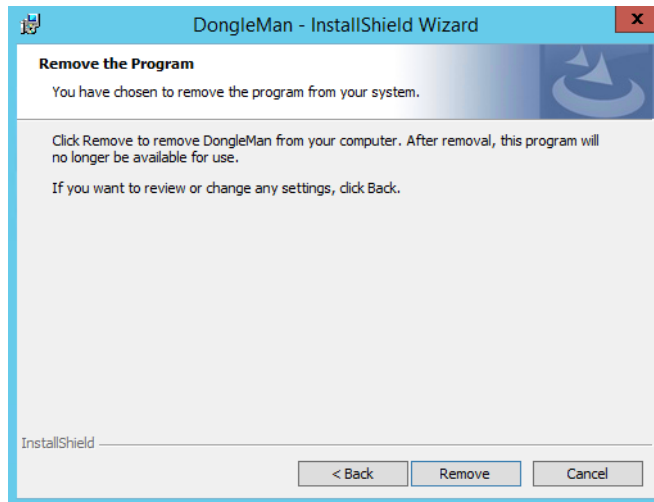
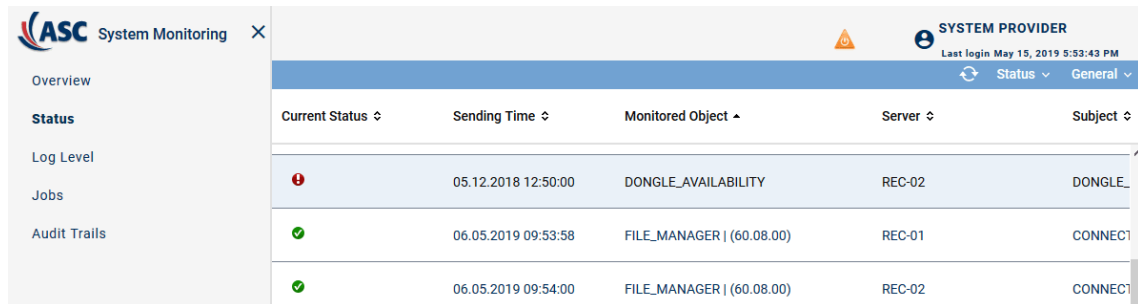


Fig. 17: Confirm security prompt

6. Click on the button *Remove*.
 - ⇒ Uninstallation of the software is being finished.
 - ⇒ The application is removed permanently.

Availability and downtime of the Dongle Manager

If *neo* key management has been activated, the availability of the service DongleMan is displayed in the Status module of the application System Monitoring in the monitored object *Authentication Server*.



Current Status	Sending Time	Monitored Object	Server	Subject
❌	05.12.2018 12:50:00	DONGLE_AVAILABILITY	REC-02	DONGLE_
✅	06.05.2019 09:53:58	FILE_MANAGER (60.08.00)	REC-01	CONNECT
✅	06.05.2019 09:54:00	FILE_MANAGER (60.08.00)	REC-02	CONNECT

Fig. 18: DongleMan status display

If an error is displayed here, this means that the service DongleMan is not available.

If the service is not available, tenants can neither activate the *neo* key management nor change their password.

When the key management has been activated, recordings are only captured if the system can access the tenants' password, since no unencrypted recording data is stored in the system. To make sure that recordings can be captured during temporary downtime of the service, the tenants' passwords are buffered in the cache of the [application server](#). As long as the passwords are stored in the cache, the recording continues even if the service should be temporarily unavailable.

Possible causes for a bug status of the object *Authentication Server*:

Cause	Measure
Communication between the services Dongle-ManConnector and DongleMan is disturbed.	<ul style="list-style-type: none"> Check connection data, see Tab Keystore/Virtualization. Check status of the services.

Tab. 1: Authentication server status troubleshooting



For further error analysis check the log file *ASC.DongleMan.log* in the installation path, e. g. C: \Program Files (x86)\ASC\ASC Product Suite\logs\DongleMan\.

List of figures

Fig. 1	File Setup.exe	7
Fig. 2	Welcome screen - Dongle Manager.....	7
Fig. 3	Install Sentinel System Driver	8
Fig. 4	Welcome screen - Sentinel System Driver.....	8
Fig. 5	Confirm license agreement - Sentinel System Driver	8
Fig. 6	Select setup type - Sentinel System Driver	9
Fig. 7	Start installation process - Sentinel System Driver	9
Fig. 8	Finish installation - Sentinel System Driver.....	10
Fig. 9	Welcome screen - Dongle Manager.....	10
Fig. 10	Select installation path - Dongle Manager	10
Fig. 11	Configure port - Dongle Manager.....	11
Fig. 12	Enter IP addresses and ports of the geo-redundant server - Dongle Manager	11
Fig. 13	Select availability for users - Dongle Manager.....	12
Fig. 14	Finish installation - Dongle Manager.....	12
Fig. 15	Welcome screen - InstallShield Wizard.....	13
Fig. 16	Options for program maintenance.....	13
Fig. 17	Confirm security prompt.....	14
Fig. 18	DongleMan status display.....	15



List of tables

Tab. 1 Authentication server status troubleshooting 15

Glossary

App server

Application server or web server. In the system architectures: the server on which the Enterprise Core and the GlassFish software have been installed.

geo-redundant

Geo-redundant servers are interconnected servers at different locations which can be used as failover in case one site fails.