

Installation CLIENTcommand



Installation manual for tenants

8/10/2022

Product line Neo, version 7.x

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

EVOIP^{neo}

EVOLUTION^{neo} / XXL / eco

INSPIRATION^{neo}

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 <https://www.asctechnologies.com>.

Copyright © 2022 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	System requirements	6
4	Installation requirements	7
4.1	Licenses.....	7
5	Overview install and configure product	8
5.1	Configure login by means of OAuth.....	8
6	Installation.....	10
6.1	Install client software	10
6.2	Install client software via MSI	13
7	Start application.....	16
7.1	Start connection attempt manually	17
7.2	Repeat login attempt in OAuth login	17
7.3	Connection options	17
8	Update.....	19
9	Maintenance and troubleshooting	20
10	Uninstalling	21
10.1	Uninstall client software	21
10.2	Uninstall client software via MSI	22
	List of figures	23
	List of tables.....	24
	Glossary	25

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 client software for the application CLIENTcom-mand.

CLIENTcommand is an application to control the recording and add additional data. The central point of control is the CLIENTcommand icon in the taskbar. This icon allows users to call up a menu with different functions, options and information

CLIENTcommand offers 3 functions for recording control:

- Start or stop recording
- Keep or delete recording
- Mute or unmute recording

Furthermore, CLIENTcommand offers the following functions:

- Add additional data to call
- Start or stop coaching advisor session
- Display notifications
- Display conversation details

The application does not require a browser environment.



If the languages Chinese or Japanese are supposed to be available for this client application, it is a precondition that the operating system supports the respective language. If this is not the case, the Chinese and Japanese characters may be depicted incorrectly. Language support has to be activated manually in the operating system then.



CLIENTcommand is a client application. It has to be installed on each client computer which is supposed to use it.

3 System requirements

3 System requirements



For basic information about the necessary hardware and software components refer to the installation manual *Installation requirements*.

4 Installation requirements



For basic information about the used default ports refer to the installation manual *Installation requirements* in chapter *Communication matrix*.



If you have configured customer-specific ports, you have to open them in the firewall separately.

4.1 Licenses

License name	Number
CLIENT <code>command</code>	1 license per concurrent user
or	or
System license CLIENT <code>com-mand</code>	1 license per system

Tab. 1: Licenses

5 Overview install and configure product

The following steps have to be carried out:

1. Install the CLIENTcommand software on the client computers (see [chapter "Install client software", p. 10](#)).
2. Configure users for the usage of CLIENTcommand:
 - Define agents.
 - Assign extensions to the agents.
 - Assign the authorization *Coaching Advisor* to all agents who are supposed to be able to record coaching advisor sessions with the application CLIENTcommand.
3. Configure the options for use of the application CLIENTcommand.



For information about the configuration of users refer to the administration manual for tenants *User management for tenants*.



Information about the application CLIENTcommand can be found in the administration manual for tenants *Configuration CLIENTcommand*.

Additional preconditions for the usage of the application

The **system provider** has to activate the external recording control and release the additional data to be used in the application.

Your system provider finds information about these topics in the following manuals:



- Activating external recording control: administration manual for system providers *Configuration servers and recording architectures*
- Releasing additional data: administration manual *System Configuration - Additional Data module*

Contact the administrator of your system provider to ensure that the required settings have been configured.

5.1 Configure login by means of OAuth

CLIENTcommand supports the login procedure OAuth2 OpenID Connect. If OAuth has been configured for CLIENTcommand, CLIENTcommand opens the OAuth authorization website configured in the application System Configuration in the default browser upon starting where users can then log in. Upon successful authentication, the user is logged in to the application CLIENTcommand.

The OAuth settings can be defined as parameters during the installation by means of *CLIENT-command.msi*, see [chapter "Install client software via MSI", p. 13](#). In addition, usage of OAuth must be activated by the system provider in the Tenants module of the application System Configuration.



For information about the configuration refer to the administration manual *System Configuration - User management for system providers*.

Activate OAuth login in the Tenants module

1. Log in to the application System Configuration as system administrator.
2. In the navigation bar, open the Tenants module and select the user *System* in the main view.
 - ⇒ The detail view opens.
3. In the tab *General Settings*, open the group field *Login Settings*.

System

×

<

Details*

Passwords

General Settings*

LDAP Connection Data*

V >

Inactivity

▶

SMTP Account

▶

SNMP Agent

▶

Login Settings

▼

Activate SSO login

☐

Activate JWT login

☐

Activate OAuth login

☒

OAuth API end point

<https://authentication.example.org.tol>

OAuth Client ID

[ef0129223a2e3bf76e7c3d8422b15b](#)

Alternative login error page

☐ None
☐ Default
☒ User-defined

www.example-login-error.com

Activate LDAP login

☐

Miscellaneous Settings

▶

Terms of Use

▶


Save

Reset

Fig. 1: Activate OAuth login - example

4. Activate the check box *Activate OAuth login* and enter your individual OAuth settings.
5. Click on the button *Save* to save the entries.
Click on the button *Cancel* to discard the entries.

Configure OAuth user in the Employees module

1. Log in to the application System Configuration as administrator of the tenant.
2. In the navigation bar, open the Employees module and create an OAuth user by clicking on the icon . Assign the same login name that is also used on the corresponding OAuth website. **WARNING!** The password should **NOT** be the same as on the OAuth website.
3. Click on the button *Save* to save the entries.
Click on the button *Cancel* to discard the entries.

6

Installation

6.1

Install client software



Note that the installation of client software requires administrator rights to be carried out.

1. Insert the installation medium for the CLIENTcommand software.
2. Open the directory of the CLIENTcommand software.
3. From the context menu of the file *setup.exe*, select the menu item *Run as Administrator*.
4. In the welcome screen, click on the button *Next* to continue.
5. If required, change the destination folder by clicking on the button *Change*.

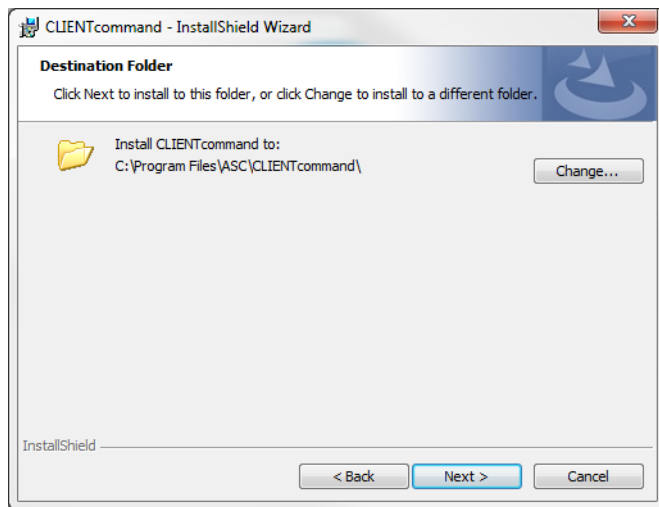


Fig. 2: Change destination folder

6. Select a destination folder.

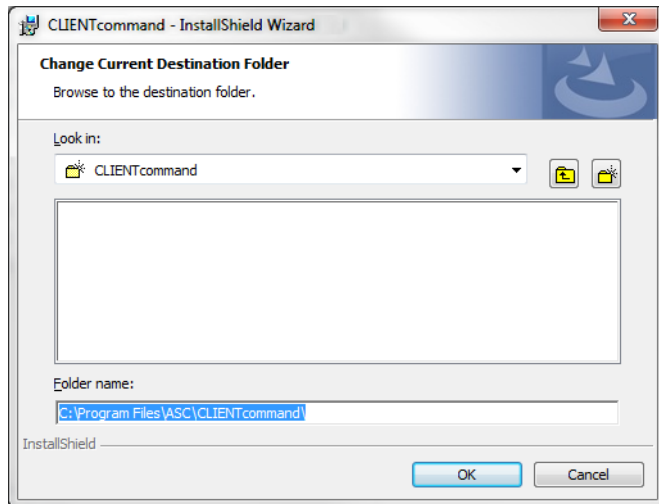


Fig. 3: Select destination folder

7. Click on the button *OK* to save the settings.
8. Click on the button *Next* to continue.
9. Enter the **IP** address of the **API server** of your system for which the feature *Recording control/Monitoring* has been activated in the Servers module in the tab *Usage*.

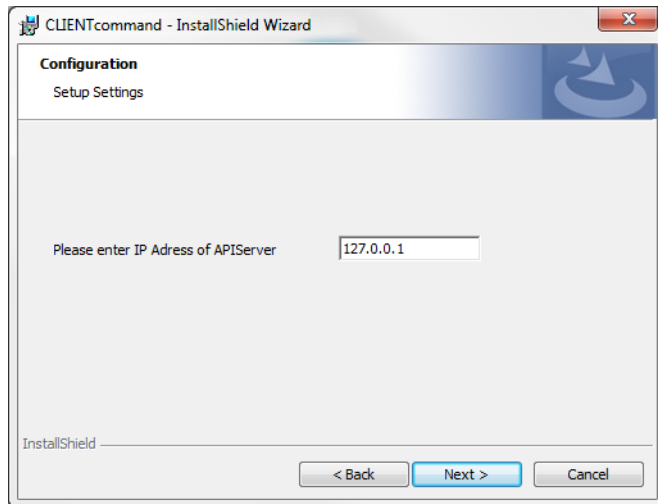


Fig. 4: Configure application server

10. Confirm the entry by clicking on the button *Next*.



For information about the configuration of servers and recording architectures refer to the administration manual for system providers *Configuration servers and recording architectures*.

11. If your system has been set up redundantly, enter the IP address of the standby application server.
If there is no standby server, leave the entry field empty.

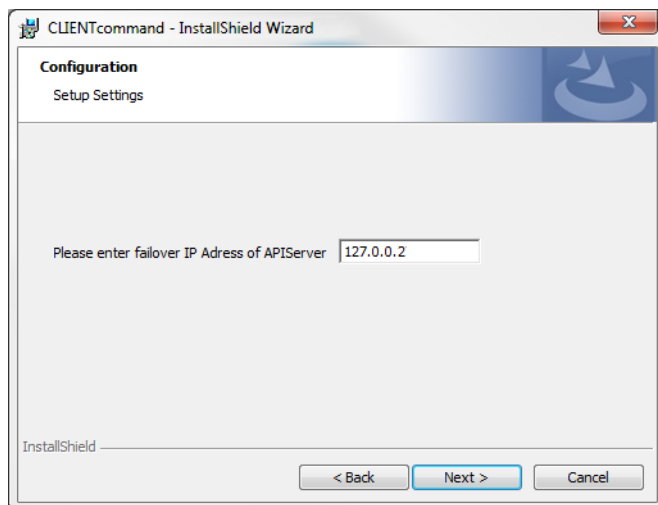


Fig. 5: Configure standby server

12. Confirm the entry by clicking on the button *Next*.
13. Select whether the operating system is supposed to start the application CLIENTcommand automatically

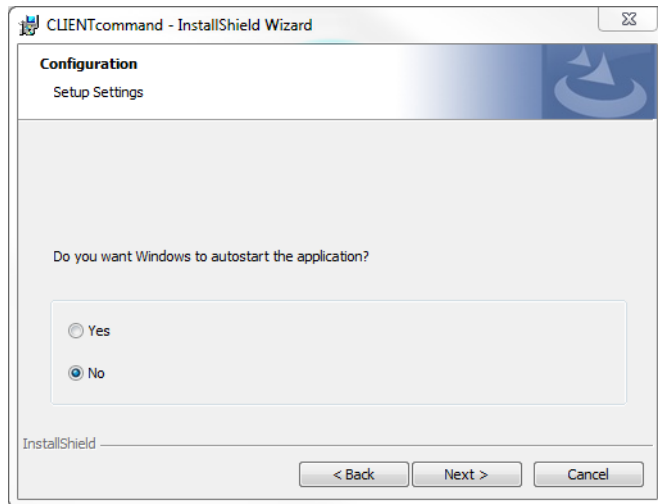


Fig. 6: Start the client application automatically

14. Confirm the selection by clicking on the button *Next*.
15. Select whether the application is supposed to be available for all users of the computer or only for the administrator.
Start the installation by clicking on the respective button:
 - *Anyone who uses this computer* - Application is available for all users
 - *Only for me* - Application is available for the currently logged-in user only

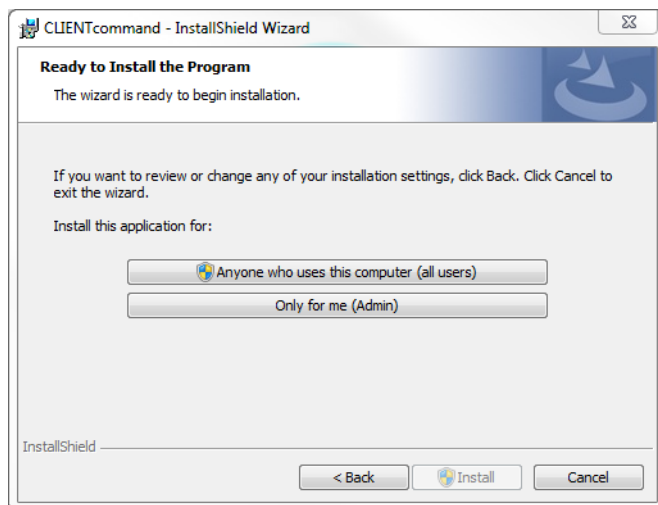


Fig. 7: Start installation

⇒ The installation progress is displayed.

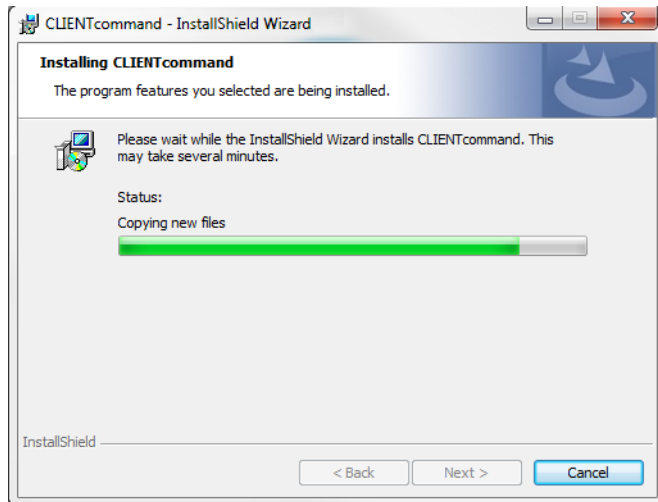


Fig. 8: Information about the installation progress

16. Finish the installation of the *CLIENTcommand* software by clicking on the button *Finish*.

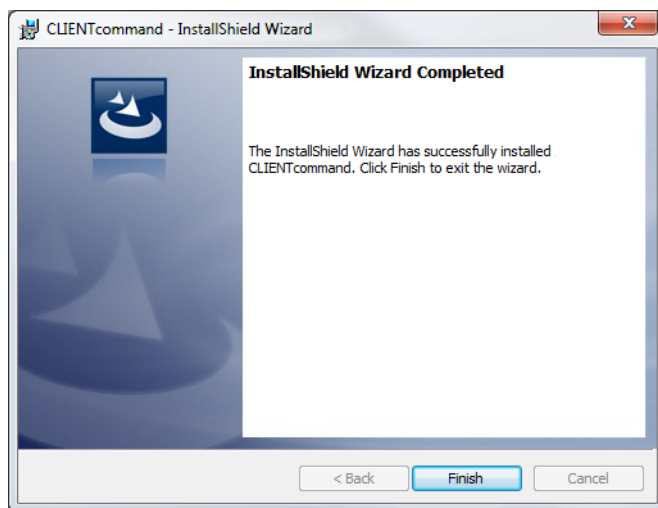


Fig. 9: Finish installation

6.2 Install client software via MSI



Basic information about the installation via [MSI](https://msdn.microsoft.com/en-us/library/cc759262(v=ws.10).aspx) can be found at:
[https://msdn.microsoft.com/en-us/library/cc759262\(v=ws.10\).aspx](https://msdn.microsoft.com/en-us/library/cc759262(v=ws.10).aspx).



Before running [MSI](#), Microsoft Visual C++ 2017 must be installed. The file *vc_redist.x86.exe* is included in the ASC image.

To install the software via MSI, the file *msiexec.exe* must be executed with the corresponding parameters.

You can carry out the installation with the following command:

```
msiexec.exe /i "CLIENTcommand.msi" /quiet
```

<code>/i</code>	Installation of the software package " <i>CLIENTcommand.msi</i> "
<code>/quiet</code>	Starts the installation in the background.

To define the default installation in greater detail, you can add the following parameters:

<code>CONNECTIP=</code>	IP of the recording server, e. g. <i>192.168.169.143</i>
<code>CONNECTIPBACKUP=</code>	IP of the backup recording server, e. g. <i>192.168.169.144</i>

SHOULD_AUTOSTART=	"1"	Autostart activated
	""	Autostart deactivated
ALLUSERS=	""	User-dependent
	"1"	Computer-dependent
	"2"	Computer-dependent installation; installs user-dependently, though, if the executing user has no access authorization for this computer.
CACHEDIR=	File path of the cache directory to be used	
LOCALSDIR=	File path of the locals directory to be used	
SHOW_LAST_PARAMETER_INPUT=	"true" or "false"	Overwrites the setting "Show last parameter input"
OAUTH_ENABLED=	"true" or "false"	Defines whether OAuth is supposed to be used as login.
OAUTH_ACCESS_TOKEN_URL=	e. g. https://authentication.example.org/token	URL which is used to request the OAuth token
OAUTH_AUTHORIZATION_URL=	e. g. https://authentication.example.org/authorize	URL which is used to authorize the user
OAUTH_CLIENT_IDENTIFIER=	ID predefined by the OAuth authorization server which serves as user identification in <code>CLIENTcommand</code> .	
OAUTH_CLIENT_IDENTIFIER_SHARED_KEY=	Application secret sent together with the client ID	
OAUTH_SCOPE=	Defines the scope of the application.	

Example for a user-dependent installation of `CLIENTcommand` in the background with the IP address 192.168.168.143 for the recording server and the IP address 192.168.168.144 for the failover recording server with activated autostart:

```
msiexec.exe /i "CLIENTcommand.msi" /quiet CONNECTIP=192.168.169.143 CONNECTIP-
BACKUP=192.168.169.144 SHOULD_AUTOSTART="1" ALLUSERS=""
```

Example for a user-dependent installation of `CLIENTcommand` in the background with the IP address 192.168.168.143 for the recording server and the IP address 192.168.168.144 for the OAuth method:

```
msiexec.exe /i "CLIENTcommand.msi" CONNECTIP=127.0.0.1 OAUTH_ENABLED=true
OAUTH_ACCESS_TOKEN_URL="https://authentication.dev.api.io/2017-09-01/token"
OAUTH_AUTHORIZATION_URL="https://auth.dev.io/authorize" OAUTH_CLIENT_IDENTIFIER=ef0129223a2e3bf76e7c3d8422b15b53 OAUTH_CLIENT_IDENTIFIER_SHARED_KEY=abc
OAUTH_SCOPE=gauth
```



If one of those parameters is set explicitly, it overwrites the settings of previous installations.



For further information about the parameters for ALLUSERS refer to [https://msdn.microsoft.com/en-us/library/aa367559\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/aa367559(v=vs.85).aspx).

If required, the storage location of the working directories `locals` and `cache` can be adjusted individually as long as the directories are **not** saved in the same folder. In this case, Windows variables are used which are framed by # instead of %, e. g. `#appdata#` instead of `%appdata%`.

Example for a user-dependent installation of `CLIENTcommand` with non-default storage locations for the working directories `locals` and `cache`:

```
msiexec /i CLIENTcommand.msi /quiet CONNECTIP=192.168.169.143 CONNECTIP-
BACKUP=192.168.169.144 CACHEDIR="#localappdata%\ASC\CC\cache" LOCALS-
DIR="#userprofile%\ASC\CC\locals".
```



The working directories *locals* and *cache* must **not** be saved in the same folder.



Only users who have been added as agents in the application System Configuration and who have been assigned an extension will be able to log into the application successfully (see administration manual *System Configuration - User management for tenants*).

During the installation you determine whether the application is supposed to be started manually or automatically, see [chapter "Install client software", p. 10](#).

For the manual start, a program group is created in the start menu of Windows and a program icon is placed on the desktop.

1. To start the application manually, click on the CLIENTcommand program icon.



Fig. 10: Program icon



If a login via [SSO](#) has been configured for the application, active authentication is omitted. Connection establishment is started directly.

Precondition for this function:

The function Single Sign On ([SSO](#)) has been activated by the administrator during the configuration of the system.



If an OAuth login has been configured for the application, a customer-specific authorization website opens in the default browser where users can log in.

Precondition for this function:

The OAuth2 parameter has been configured during the installation of CLIENTcommand and the procedure has been activated in the application System Configuration by the system provider.

2. If you do not log in via SSO, enter your user name and password.

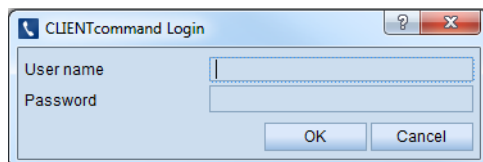





Fig. 11: Login window

3. Click on the button **OK**.
 - ⇒ The application is started.
 - ⇒ The connection to the [app server](#) is established.
 - ⇒ You will receive a message whether you have logged in successfully.
 - Upon logging in successfully, the icon  (*Client is connected*) appears in the Windows system tray.
 - If no connection to the [app server](#) could be established, the icon  (*Client is not connected*) appears in the Windows system tray.
4. If no connection to the [app server](#) could be established, you can check and adjust the connection options. To do so, right-click on the icon  (*Client is not connected*) and open the menu item *Options*.
5. Check the settings in the tab *Connection Options*.
6. Adjust the settings if required.
7. Click on the button **OK** to save the changes.

- ⇒ CLIENT`command` will reattempt automatically to establish a connection to the [app server](#).

If all automatic attempts of establishing a connection to the server have failed, you can start additional connection attempts manually, see [chapter "Start connection attempt manually"](#), p. 17.

7.1 Start connection attempt manually

You have 2 options to start a connection attempt to the [app server](#) manually:

1. In the message about the failed connection attempts, click on *Retry*.

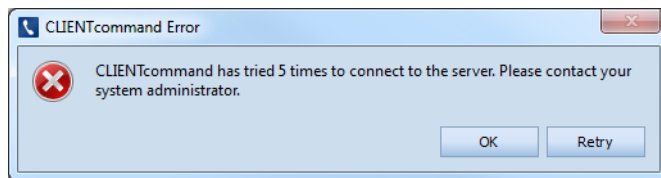


Fig. 12: Message Connection error

2. Open the context menu of the icon  and select the menu item *Retry Connection*.

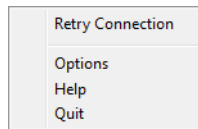


Fig. 13: Context menu in case of a connection error

7.2 Repeat login attempt in OAuth login

If OAuth has been configured for CLIENT`command`, a failed login attempt can be repeated in the context menu of CLIENT`command`, e. g. if the OAuth authorization website configured in the application System Configuration has been closed inadvertently before the user could be logged in to CLIENT`command`.

1. Open the context menu of the icon  and select the menu item *Retry Login*.

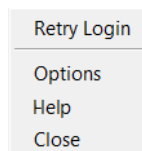
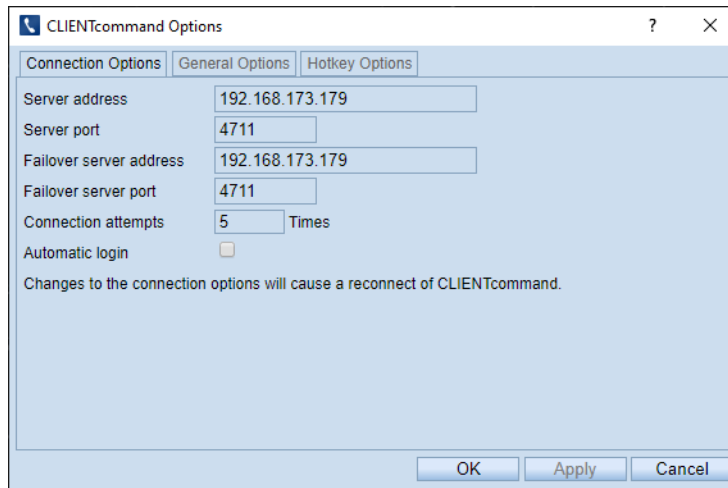


Fig. 14: Context menu in case of failed login

- ⇒ The customer-specific OAuth authorization website opens and the user can log in once again.

7.3 Connection options

Here, you can display the current connection options and adjust them if required.



The image shows a Windows-style dialog box titled "CLIENTcommand Options". It has three tabs: "Connection Options" (selected), "General Options", and "Hotkey Options". Under "Connection Options", there are several input fields: "Server address" (192.168.173.179), "Server port" (4711), "Failover server address" (192.168.173.179), "Failover server port" (4711), and "Connection attempts" (5 Times). There is also an "Automatic login" checkbox which is unchecked. A note at the bottom states: "Changes to the connection options will cause a reconnect of CLIENTcommand." At the bottom right are "OK", "Apply", and "Cancel" buttons.

Fig. 15: Connection options

<i>Server address</i>	IP address of the primary application server (app server).
<i>Server port</i>	IP port which is supposed to communicate with the primary app server .
<i>Failover server address</i>	IP address of the server which has been set up as standby application server. The application <u>CLIENTcommand</u> connects to the standby server if the primary server fails. If there is no standby server, leave the entry field empty.
<i>Failover server port</i>	IP port of the standby server. This port allows communicating with the standby server if the primary server fails. If there is no standby server, leave the entry field empty.
<i>Connection attempts</i>	Maximum number of connection attempts before an error message will be issued and no further automatic connection attempts will be made. Enter the value 0 if you would like to prompt automatic connection attempts without restrictions until the connection could be established.
<i>Automatic login</i>	Select whether the user is supposed to be logged in to the application <u>CLIENTcommand</u> again automatically if the connection to the app server was lost during the previous session. <input checked="" type="checkbox"/> = Function has been activated. The user is logged in again automatically in case the connection was lost. <input type="checkbox"/> = Function has not been activated. The user is not logged in again automatically in case the connection was lost.



If a terminal server is deployed, changes of the IP address made here **exclusively** apply to the logged-in user. If the IP address is supposed to be changed for all users of the terminal server, the administrator can adjust the IP address in the file *setup.xml* in path *C:\Program Files (x86)\ASC\ASC CLIENTcommand*.

8 Update

8 Update

For client applications, no updates are available.

Clients are updated by installing a new version. During the installation, the old version is uninstalled automatically and replaced with the new version.

9 Maintenance and troubleshooting

9 Maintenance and troubleshooting



If problems with the installed software or unexpected error messages occur, please contact your local ASC support or the ASC support by calling +49 700 27278776.

Do **not** use the functions *Repair* and *Modify* in the setup menu!



Before the application can be uninstalled, you have to exit it.

10.1

Uninstall client software

1. Insert the installation medium for the CLIENTcommand software.
2. Open the directory of the CLIENTcommand software.
3. From the context menu of the file *setup.exe*, select the menu item *Run as Administrator*.
4. On the welcome screen, click on the button *Next* to continue.
5. In the window *Program Maintenance*, select the option *Remove*.

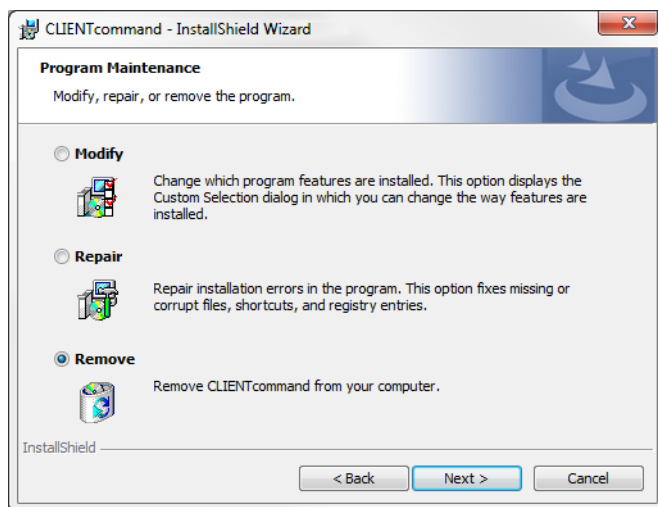


Fig. 16: Uninstall software

6. Confirm the selection by clicking on the button *Next*.
7. To actually uninstall the application, confirm the security prompt by clicking on the button *Remove*.

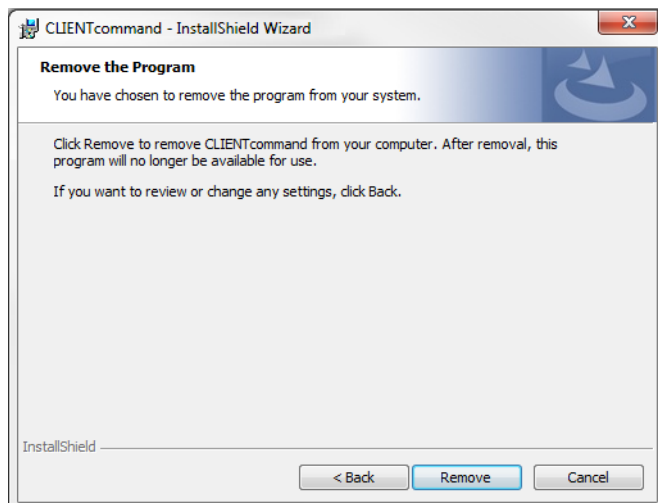


Fig. 17: Confirm uninstallation

8. Finish the uninstallation by clicking on the button *Finish*.

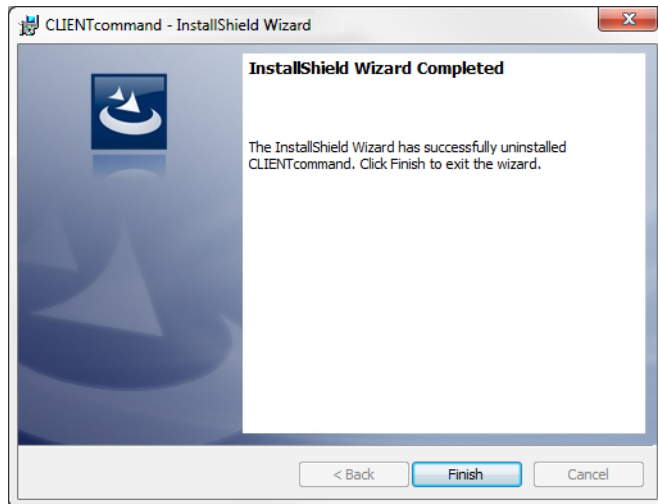


Fig. 18: Finish uninstallation

- ⇒ Uninstallation of the software is being finished.
- ⇒ The program icons are being removed from the desktop and from the start menu of Windows.



If the computer has to be rebooted, a separate window with a corresponding message will appear.

10.2

Uninstall client software via MSI

To uninstall the software via MSI, the file *msiexec.exe* has to be executed with the respective parameters.

1. For the uninstallation, enter the following command in the command line prompt:

msiexec.exe /x "CLIENTcommand.msi" /quiet

<i>/x</i>	Uninstalls the software packet " <i>CLIENTcommand.msi</i> "
<i>/quiet</i>	Uninstalls in the background

List of figures

Fig. 1	Activate OAuth login - example	9
Fig. 2	Change destination folder.....	10
Fig. 3	Select destination folder	10
Fig. 4	Configure application server	11
Fig. 5	Configure standby server.....	11
Fig. 6	Start the client application automatically.....	12
Fig. 7	Start installation	12
Fig. 8	Information about the installation progress.....	13
Fig. 9	Finish installation	13
Fig. 10	Program icon	16
Fig. 11	Login window	16
Fig. 12	Message Connection error	17
Fig. 13	Context menu in case of a connection error	17
Fig. 14	Context menu in case of failed login	17
Fig. 15	Connection options	18
Fig. 16	Uninstall software	21
Fig. 17	Confirm uninstallation	21
Fig. 18	Finish uninstallation	22



List of tables

Tab. 1 Licenses..... 7

Glossary

API server

Server on which the API service runs. (API=Application Programming Interface)

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.

ID

Identifier, ID

IP

Internet Protocol, basic protocol for Internet communication

MSI

Microsoft Installer or Windows Installer provides a runtime environment for installation routines on a Microsoft Windows operating system.

OAuth

OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. (Source: Wikipedia 19th August 2020)

SSO

Single Sign On; Simplified login mode. After a one-off authentication at one workplace users will be able to use all services and applications that they have been authorized for from this workplace. They do not have to authenticate for the individual applications again.

URL

Uniform resource locator. Identifies and locates a resource (e. g. a website) about the used access method (e. g. the used network protocol as HTTP or FTP) and the location of the resource in the computer network. (Source: Wikipedia 20th November 2013)