INSTALLATIONSANLEITUNG

forcont Desktop Connector mit Zusatzkomponenten

Stand: 06.11.2025

forcont business technology gmbh / Markranstädter Str. 1 / 04229 Leipzig / Telefon +49 341 48503-0
E-Mail office@forcont.de / Internet www.forcont.de / Blog www.forcont.de/blog

Impressum Autor: forcont business technology gmbh

Inhaltsverzeichnis

1 Einleitung

Folgende Funktionen in den Produkten der forcont factory Suite erfordern eine Interaktion mit installierten Desktop-Anwendungen auf dem PC des Benutzers:

forpeople
- Drag-and-drop von E-Mails aus MS Outlook in den Postkorb
- Öffnen von Dokumenten zur Bearbeitung in der nativen Desktop-Anwendung (z. B.: MS Word, MS Excel)
- Anzeigen von Originaldokumenten aus der Personalakte

forcontract
- Öffnen von bestimmten Dokumentformaten zur Anzeige (bis zur Version 7.1a)
- Bearbeiten von Vorlagen zur Dokumenterstellung

forprocess (abhängig von deren Verwendung in den eingesetzten individuellen Anwendungen)
- Drag-and-Drop von Dokumenten bzw. E-Mails in eine forprocess-Anwendung
- Öffnen von Dokumenten zur Bearbeitung in der nativen Desktop-Anwendung
- Öffnen von bestimmten Dokumentformaten zur Anzeige
- Generieren und Versenden von E-Mails
- Kopieren von Dokumenten in die Windows-Zwischenablage
- Ggf. anwendungsspezifische, individuelle Funktionen

Um diese Funktionen nutzen zu können, muss die Komponente **forcont Desktop Connector** auf dem PC des Benutzers (Client-PC) installiert sein.

Bei dem forcont Desktop Desktop Connector – im Weiteren **fdc** genannt – handelt es sich um eine Anwendung, die aus dem Browser heraus gestartet wird. Sie vollzieht die notwendigen Schritte für die Ausführung der jeweiligen Funktion und wird anschließend wieder beendet.

Bei den Zusatzkomponenten handelt es sich um Softwarekomponenten der forcont factory Suite, über die Dokumente direkt aus ihrer Arbeitsumgebung in factory-Anwendungen abgelegt werden können. Folgende Funktionen werden dabei ermöglicht:

- Ablegen von Dokumenten direkt aus unterstützten MS Office-Anwendungen (32- und 64-Bit-Version) in factory-Anwendungen
  - **MS Outlook**
  - **MS Word**
  - **MS Excel**
  - **MS PowerPoint**

- Ablegen von Dokumenten direkt aus **Adobe Acrobat** in factory-Anwendungen

» Ablegen von Dokumenten aus lokalem Dateisystem über **Drag-and-Drop** (Droplet) in factory-Anwendungen

Um diese Funktionen nutzen zu können, müssen die Zusatzkomponenten auf dem PC des Benutzers (Client-PC) installiert sein. Die Zusatzkomponenten setzen sich aus den folgenden Bestandteilen zusammen:

» **Office Integration**
» **Acrobat Integration**
» **COM-Schnittstelle (Droplet)**

Die folgenden Kapitel beschreiben, welche Softwarevoraussetzungen gegeben sein müssen und welche Schritte für die Konfiguration und Installation des fdc notwendig sind.

2 Softwarevoraussetzungen

2.1 Client-PCs

Zur Installation und Anwendung des fdc müssen folgende Softwarevoraussetzungen auf den Client-PCs erfüllt sein:

Betriebssystem:	Windows 10 (64-Bit), Windows 11
Software:	.Net Framework 4.0 oder höher Wird für die Produkte **forpeople** und **forprocess** bei Nutzung folgender Funktionen benötigt: • Drag-and-Drop von E-Mails aus Outlook in den Postkorb von forpeople • Kopieren von Dokumenten aus einer forprocess-Anwendung in die Windows-Zwischenablage • Drag-and-Drop von Dokumenten bzw. E-Mails in eine forprocess-Anwendung
Rechte:	Administratorrechte auf Client-PCs (nur bei Installation)
HTTPS-Unterstützung:	Zertifikate interner CAs („Zertifizierungsstellen“) müssen auf Client-PCs verteilt werden*

** Standardmäßig werden vom fdc nur Zertifikate akzeptiert, die durch offizielle Zertifizierungsstellen (Root-CAs) ausgestellt wurden. Selbstsignierte Zertifikate werden nicht akzeptiert.*
Werden in ihrer Organisation HTTPS-Zertifikate verwendet, die von einer firmeneigenen Zertifizierungsstelle ausgestellt wurden, müssen das zugehörige CA Root-Zertifikat und evtl. existierende Intermediate-Zertifikate auf den Client-PCs bekannt sein. Der fdc wertet Zertifikate in den folgenden Windows Certificate Stores aus:

- *Zertifikate – Aktueller Benutzer | Vertrauenswürdige Stammzertifizierungsstellen*
- *Zertifikate – Aktueller Benutzer | Zwischenzertifizierungsstellen*

2.2 forcont Zusatzkomponenten (32-Bit-Office-Version)

Zur Installation und Anwendung der Zusatzkomponenten mit MS Office-Anwendungen (32-Bit) müssen folgende Softwarevoraussetzungen auf den Client-PCs erfüllt sein:

Betriebssystem	Windows 10, Windows 11
Software	» Microsoft Office 2013, 2016 (jeweils 32-Bit) » Microsoft 365 Version 16 (Outlook 16.0, Word 16.0, Excel 16.0, PowerPoint 16.0) » Adobe Acrobat DC bis Version 2020
Rechte	Administratorrechte auf Client-PCs (nur bei Installation)

2.3 forcont Zusatzkomponenten (64-Bit-Office-Version)

Zur Installation und Anwendung der Zusatzkomponenten mit MS Office-Anwendungen (64-Bit) müssen folgende Softwarevoraussetzungen auf den Client-PCs erfüllt sein:

Betriebssystem	Windows 10, Windows 11
Software	» Microsoft Office 2016, 2019 (jeweils 64-Bit) » Microsoft 365 Version 16 (Outlook 16.0, Word 16.0, Excel 16.0, PowerPoint 16.0) » Adobe Acrobat DC bis Version 2020
Rechte	Administratorrechte auf Client-PCs (nur bei Installation)

2.4 factory-Server

Voraussetzung für die Unterstützung und Aktivierung des fdc auf den factory-Servern ist die Installation aller verfügbaren Hotfixes für die factory-Versionen 7.4 und 7.5. Ab factory-Version 7.6 enthält der factory-Server bereits alle Schnittstellen zur Kommunikation mit dem fdc. Um die Hotfixes zu erhalten, kontaktieren Sie bitte unseren Support per Telefon (+49 341 48503-75) oder E-Mail (factory-support@forcont.de).

3 Vorbereitung und Installation

3.1 Umstieg auf forcont Desktop Connector

Wenn Sie von der forcont Desktop Integration 7 auf den forcont Desktop Connector umsteigen wollen, beachten Sie, dass die bisherige Installation vollständig entfernt werden muss. Führen Sie dazu über die Systemsteuerung die Deinstallation durch (**Systemsteuerung > Programme > Programme und Features > forcont desktop integration 7 <Version>**) oder verwenden Sie die *`Uninstall forcont Desktop Integration 7.exe`* aus Ihrem Installationsverzeichnis.

3.2 Funktionsweise und Konfiguration der Server-Whitelist

Funktionsweise des fdc über eine Server-Whitelist

Um die Kommunikation des client-seitig installierten fdc mit den factory-Anwendungsservern abzusichern, wird ein Whitelist-Verfahren verwendet. Zunächst kontaktiert der Client einen der in seiner Konfiguration festgelegten Whitelist Head Server und lädt von diesem eine Liste der factory-Server herunter, mit welchen er Kontakt aufnehmen darf. Wurde der Zielserver über die Server-Whitelist validiert, nimmt der fdc Kontakt zu diesem auf und führt die gewünschte Funktion auf dem Client-PC aus.

Im Hinblick auf die Konfiguration und Ablage der Server-Whitelist sind zwei Fälle zu unterscheiden:

1. Es existiert nur ein factory-Anwendungsserver.
2. Es werden mehrere factory-Anwendungsserver betrieben.

Im ersten Fall übernimmt der einzelne factory-Server zugleich die Rolle des Whitelist Head Servers. Im zweiten Fall müssen aus den vorhandenen factory-Servern ein oder mehrere Server ausgewählt werden, die die Rolle des Whitelist Head Servers übernehmen.

Um den eventuellen Ausfall eines Whitelist Head Servers kompensieren zu können, gibt es die Möglichkeit, mehrere Whitelist Head Server in die Konfiguration aufzunehmen. Fällt der erste in der Liste aufgeführte Whitelist Head Server aus, versucht der Client die weiteren in der Konfiguration festgelegten Whitelist Head Server zu kontaktieren, um die Server-Whitelist von diesen zu beziehen.

Konfiguration der Server-Whitelist

Zunächst wird auf einem der ausgewählten factory-Server die Whitelist abgelegt und gepflegt. Nachfolgend kann sie dann auf andere, als Head Server definierte factory-Server kopiert werden.

Achtung – Auswahl der Whitelist Head Server

Wählen Sie für die Bereitstellung der Server-Whitelist möglichst factory-Server aus, die eine hohe Verfügbarkeit garantieren. Dies ist insbesondere in den Fällen essenziell, in denen nur ein einzelner Whitelist Head Server konfiguriert ist.

Die Funktionalität des fdc kann nur gewährleistet werden, wenn mind. einer der Whitelist Head Server permanent erreichbar ist.

» Navigieren Sie in das folgende Windows-Verzeichnis des factory-Servers, welchen Sie als Whitelist Head Server definiert haben:
<FACTORY_HOME>\ff\WEB-INF
» Öffnen Sie die Datei *di.json* (Server-Whitelist) mit einem beliebigen Editor.
» Tragen Sie in die Liste die **URLs** aller **factory Server** ein, welche den fdc benötigen (siehe Beispiel unten).

Die bereits vorhandenen Einträge sind die URLs der factory-Server der forcont Cloud (Voreinstellungen für Cloud-Kunden).

» Speichern und schließen Sie die Datei.

Beispiel:

Wenn Sie Ihre factory-Anwendung über **https://factoryapp.mydomain.de/...** aufrufen, muss folgende URL ergänzt werden: **https://factoryapp.mydomain.de/**.

Wenn Sie Ihre factory-Anwendung zusätzlich, im internen Netz, über **http://factoryapp/...** aufrufen, muss außerdem folgende URL hinzugefügt werden: **http://factoryapp/**.

```
{
    "whitelistserver":

          [
                "https://factoryapp.mydomain.de/",
                "http://factoryapp/",
                "https://cloud.forcont-services.de/",
                "https://demo.forcont-services.de/"
          ]
 }
```

Hinweis – Fully Qualified Domain Name (FQDN) und Server-Kurzname

Sprechen Sie die factory-Server nicht nur über den FQDN, sondern auch über ihren Kurznamen (ohne Domain) an, tragen sie bitte sowohl den FQDN als auch den Kurznamen in die Server-Whitelist ein.

Beispiel:

```
"http://anwendungsserver1.beispieldomain.com/",
"http://anwendungsserver1/"
```

Achtung – Formatierungsregeln einhalten

Stellen Sie sicher, dass die Datei ***di.json*** (Server-Whitelist) auf den Whitelist Head Servern frei von Formatierungsfehlern ist.

Formatierungsregeln: URLs enden mit Schrägstrich (/), stehen in Anführungszeichen ("") und sind durch Kommata getrennt (,) (siehe Beispiel oben).

Achtung – Verwendung mehrerer Whitelist Head Server

Verwenden Sie mehrere Whitelist Head Server, kopieren Sie die o. g. Datei ***di.json*** in die entsprechenden Verzeichnisse aller factory-Server, die Sie als weitere Whitelist Head Server definiert haben.

Pflege der Server-Whitelist

Kommen zu einem späteren Zeitpunkt neue factory-Server hinzu, welche über den fdc angesprochen werden, muss die **Server-Whitelist** um die URLs dieser factory-Server ergänzt werden. Bitte denken sie in diesem Fall daran, die erweiterte Server-Whitelist auch auf den eventuell anderen vorhandenen Whitelist Head Servern zu aktualisieren.

3.3 Herunterladen und Prüfen des Installationspakets

forcont stellt Ihnen alle Dateien zur Installation des fdc als **ZIP-Archiv** zur Verfügung.

» Laden Sie das Installationspaket unter dem folgenden Link herunter:

https://forcont.de/forcont-desktop-connector/fdc-zusatzkomponenten

Hash-Wert prüfen

Neben dem Installationspaket wird auf der obigen Website, zusätzlich zum Downloadlink, eine Prüfsumme (SHA256 Hash) angezeigt, die es Ihnen ermöglicht, das heruntergeladene Installationspaket auf seine Integrität zu prüfen. Bei Nutzung des Betriebssystems *Windows 10* bzw. Windows 11 bietet sich dafür die Kommandozeilenanwendung **CertUtil** an.

» Wechseln Sie in das Verzeichnis, in welches Sie das Installationspaket heruntergeladen haben.

» Öffnen Sie das Kommandozeilenfenster (Shift + Rechtsklick > PowerShell-Fenster hier öffnen) und geben Sie den folgenden Befehl ein:

```
Certutil -hashfile FDC32_Install_package.zip SHA256
```

bzw.

```
Certutil -hashfile FDC64_Install_package.zip SHA256
```

» Vergleichen Sie den ausgegebenen Hash-Wert mit dem am Downloadlink hinterlegten Wert.

Wenn beide Werte übereinstimmen, ist das Installationspaket unverändert.

Hinweis – Virenprüfung

Das Installationspaket wurde von forcont auf Viren geprüft. Trotzdem bitten wir Sie, dieses mit Ihrer eigenen Antivirenlösung noch einmal zu prüfen.

3.3.1 Konfiguration des Installationspakets

Alle Einstellungsparameter des **forcont Desktop Connector** befinden sich in der *default.json* im Installationsverzeichnis. Die *default.json* liegt bei der Installation neben der *forcont desktop connector.exe*. Bei der Installation wird durch die *forcont desktop connector.exe* die *default.json* ins Programmverzeichnis geschrieben und gegebenenfalls angepasst.

Folgende Konfigurationsparameter sind verfügbar:

Name Parameter	Beschreibung
server	URL zum Head Server der factory
proxy	URL zum verwendeten Proxy oder "" (default)
proxyUser	Benutzer zum verwendeten Proxy oder "" (default)
proxyPassword	Proxypasswort zum verwendeten Proxy oder "" (default)
secureProxyPassword	verschlüsseltes Proxypasswort zum verwendeten Proxy oder "" (default)
noproxy	Array von Hostnamen für die bei der Verbindung zur factory kein Proxy verwendet werden soll.

Name Parameter	Beschreibung
useSystemTemp	temporäre Anwendungsdaten werden im System Temp abgelegt true: (default) %USERPROFILE%\AppData\Local\Temp\forcont desktop connector\"Funktion" false: %USERPROFILE%\AppData\Roaming\forcont desktop connector\.temp\"Funktion"
debug (v1.6.0)	true: Stellt Loglevel auf debug. Kann auch als Kommandozeilenparameter mitgegeben werden. "c:\Program Files\forcont desktop connector\forcont desktop connector.exe" debug false: (default)

Beispiel:

```
{
    "server" : "http://localhost/ff/appcfg",
    "proxy" : "",
    "proxyUser" : "",
    "proxyPassword" : "",
    "secureProxyPassword" : "",
    "noproxy" : [
        "localhost"
    ]
}
```

Verwendung Proxy

Eine typische Proxy-URL mit Authentifizierung lautet
https://TestUser:Password@proxy.test.com/

Bei der Verwendung eines Proxys mit Authentifizierung muss vor der Installation der Benutzer unter `proxyUser` und das Passwort unter `proxyPassword` eingetragen werden. Während der Installation wird das `proxyPassword` verschlüsselt und unter `secureProxyPassword` abgelegt. Das `proxyPassword` wird gelöscht. Die *default.json* kann für den Ausrollprozess vorbereitet werden, indem ein Administrator eine lokale Referenzinstallation vornimmt und so ein `secureProxyPassword` erzeugt. Diese *default.json* mit `secureProxyPassword` kann dann zum Ausrollen benutzt werden, d.h. beim eigentlichen Ausrollen auf die Clientrechner wird kein `proxyPassword` im Klartext benötigt.

Beispiel:

```
{
    "server" : "http://localhost/ff/appcfg",
    "proxy" : "https://proxy.test.com",
    "proxyUser" : "TestUser",
    "proxyPassword" : "",
    "secureProxyPassword" : " 20b87f9d8ecdb365e39c17b9",
    "noproxy" : [
        "localhost"
    ]
}
```

3.3.2 Konfigurationsdatei setup.ini

Die Datei ***setup.ini*** dient der Konfiguration der Zusatzkomponenten **Office Integration**, **COM-Schnittstelle (Droplet)** und optional **Adobe Integration**. In der Konfigurationsdatei werden die möglichen Ziele der Dokumentablage über den Parameter `Params` definiert.

Zur Konfiguration gehen Sie abhängig davon, ob Sie Cloud- oder On-Premises-Anwendungen (ggf. in Kombination mit Cloud-Anwendungen) einsetzen, wie folgt vor.

3.3.2.1 Cloud-Anwendungen

Setzen Sie ausschließlich Cloud-Anwendungen wie forpeople und/oder forcontract ein, enthält das Installationspaket bereits angepasste Konfigurationsvorlagen. Für die Verwendung einer dieser Konfigurationsvorlagen (z. B. *forpeople_setup.ini*) erstellen Sie im selben Verzeichnis eine Kopie der Vorlagendatei mit dem Dateinamen ***setup.ini***.

Zur Konfiguration gehen Sie abhängig davon, ob Sie ausschließlich forpeople oder **forcontract**, oder beide Cloud-Anwendungen parallel einsetzen, wie folgt vor.

Konfiguration für forpeople

» Bei Installation der Zusatzkomponenten für eine **32-Bit-Office-Version** kopieren Sie in Ihrem Konfigurationsverzeichnis die Datei
.*Office_Integration\forpeople_setup.ini* nach
.*Office_Integration\setup.ini*.

» Bei Installation der Zusatzkomponenten für eine **64-Bit-Office-Version** kopieren Sie in Ihrem Konfigurationsverzeichnis die Dateien
.*Office_Integration\32Bit\forpeople_setup.ini* nach
.*Office_Integration\32Bit\setup.ini* sowie
.*Office_Integration\64Bit\forpeople_setup.ini* nach
.*Office_Integration\64Bit\setup.ini*.

Konfiguration für forcontract

» Bei Installation der Zusatzkomponenten für eine **32-Bit-Office-Version** kopieren Sie in Ihrem Konfigurationsverzeichnis die Datei
.*Office_Integration\forcontract_setup.ini* nach
.*Office_Integration\setup.ini*.

» Bei Installation der Zusatzkomponenten für eine **64-Bit-Office-Version** kopieren Sie in Ihrem Konfigurationsverzeichnis die Dateien
.*Office_Integration\32Bit\forcontract_setup.ini* nach
.*Office_Integration\32Bit\setup.ini* sowie
.*Office_Integration\64Bit\forcontract_setup.ini* nach
.*Office_Integration\64Bit\setup.ini*.

Konfiguration für forpeople **und** forcontract

» Bei Installation der Zusatzkomponenten für eine **32-Bit-Office-Version** kopieren Sie in Ihrem Konfigurationsverzeichnis die Datei
.*Office_Integration\forpeople_forcontract_setup.ini* nach
.*Office_Integration\setup.ini*.

» Bei Installation der Zusatzkomponenten für eine **64-Bit-Office-Version** kopieren Sie in Ihrem Konfigurationsverzeichnis die Dateien
.*Office_Integration\32Bit\forpeople_forcontract_setup.ini* nach
.*Office_Integration\32Bit\setup.ini* sowie
.*Office_Integration\64Bit\forpeople_forcontract _setup.ini* nach
.*Office_Integration\64Bit\setup.ini*.

3.3.2.2 On-Premises-Anwendungen (ggf. in Kombination mit Cloud-Anwendungen)

Setzen Sie einzelne oder mehrere On-Premises-Anwendungen wie forpeople, forcontract, oder forprocess, oder eine Kombination aus On-Premises- und Cloud-Anwendungen ein, enthält das Installationspaket bereits angepasste Konfigurationsvorlagen. Für die Verwendung dieser Konfigurationsvorlagen (*on-premises_setup.ini*) erstellen Sie im selben Verzeichnis eine Kopie der Vorlagendatei mit dem Dateinamen ***setup.ini*** und folgen den weiteren Anweisungen.

Wenden Sie sich zur Unterstützung der Konfiguration bitte an forcont. forcont stellt Ihnen die für die Konfiguration benötigten Dokumentablageszenarien der Zusatzkomponenten Ihrer Anwendung(en) bereit, die Sie im Folgenden in die Datei ***setup.ini*** übernehmen müssen.

Konfiguration

» Bei Installation der Zusatzkomponenten für eine **32-Bit-Office-Version** kopieren Sie in Ihrem Konfigurationsverzeichnis die Datei *.\Office_Integration\on-premises_setup.ini* nach *.\Office_Integration\setup.ini*.
» Öffnen Sie die Konfigurationsdatei *setup.ini* in Ihrem Konfigurationsverzeichnis mit einem beliebigen Editor.
» Ersetzen Sie die Konfigurationsparameter `Params` in **Zeile 1** (siehe unten) durch die von forcont bereitgestellten Dokumentablageszenarien der Zusatzkomponenten Ihrer Anwendung(en).

» Bei Installation der Zusatzkomponenten für eine **64-Bit-Office-Version** kopieren Sie in Ihrem Konfigurationsverzeichnis die Dateien *.\Office_Integration\32Bit\on-premises_setup.ini* nach *.\Office_Integration\32Bit\setup.ini* sowie *.\Office_Integration\64Bit\on-premises_setup.ini* nach *.\Office_Integration\64Bit\setup.ini*.
» Öffnen Sie die Konfigurationsdateien *.\32Bit\setup.ini* sowie *.\64Bit\setup.ini* in Ihrem Konfigurationsverzeichnis mit einem beliebigen Editor.
» Ersetzen Sie in beiden Konfigurationsdateien die Konfigurationsparameter `Params` in **Zeile 1** (siehe unten) durch die von forcont bereitgestellten Dokumentablage-szenarien der Zusatzkomponenten Ihrer Anwendung(en).

Zeile 1: `Params=label="DOCU" appid=1 configid=1234`

3.4 Deinstallation des forcont Desktop Connector

Vor der Installation der Softwarekomponente fdc ist es zwingend notwendig, dass alle bereits vorhandenen fdc-Komponenten deinstalliert werden. Das kann – analog zur Installation – manuell oder automatisiert (skript-basiert) geschehen.

Hinweis – Sichern der Konfigurationsdateien

Die **setup.ini**-Datei(en) aus den Verzeichnissen .\Office_Integration (im Falle einer 32Bit-Installation) oder .\Office_Integration\32Bit und .\Office_Integration\64Bit (im Falle einer 64Bit-Installation) können grundsätzlich wiederverwendet werden. Bei einem Upgrade einer alten Zusatzkomponenten muss man aber aufpassen, dass die oben erwähnte Zeile 1 mit dem Inhalt *Loader=c:\Program Files (x86)\forcont\Start Center\Start Center.exe* aus der/den setup.ini-Datei(en) entfernt werden muss.

Für eine manuelle Deinstallation führen Sie die folgenden Schritte durch:

» Schließen Sie alle MS Office-Anwendungen.
» Führen Sie die Batch-Datei ***uninstall.cmd*** im aktuellen Installationsverzeichnis des fdc als **Administrator** aus.

3.5 Installation des forcont Desktop Connector

Die Installation des fdc kann über eine manuelle Installation auf den Client-PCs oder über eine Softwareverteilung erfolgen.

Hinweis – Digitale Signaturen

Die Installationssoftware sowie alle ausführbaren Dateien des fdc sind mit einem **Code Signing-Zertifikat** versehen. Diese digitale Signatur garantiert, dass die Software von forcont stammt und nach der Veröffentlichung nicht verändert wurde.

Nach Ablauf von zwei Jahren verliert die verwendete digitale Signatur ihre Gültigkeit. Bitte laden Sie aus diesem Grund stets das aktuelle Installationspaket herunter (siehe Kapitel 3.1).

Manuelle Installation

» Starten Sie die Installation mit Doppelklick auf die Datei „forcontDesktopConnector_Setup.exe“.

Da die Installation in das Windows-Verzeichnis „C:\Program Files“ bzw. „C:\Programme“ erfolgt, werden Sie aufgefordert, die Installation über einen Windows-Account mit administrativen Rechten auszuführen.

» Melden Sie sich an Ihrem Benutzerkonto entsprechend an.

Wenn Ihnen Benutzername und Kennwort nicht bekannt sind, wenden Sie sich bitte an Ihren Systemadministrator.

» Klicken Sie auf **Ja**.

Die Installation startet und zeigt den Installationsfortschritt an. Wenn die Installation abgeschlossen ist, öffnet sich ein Fenster zur Bestätigung.

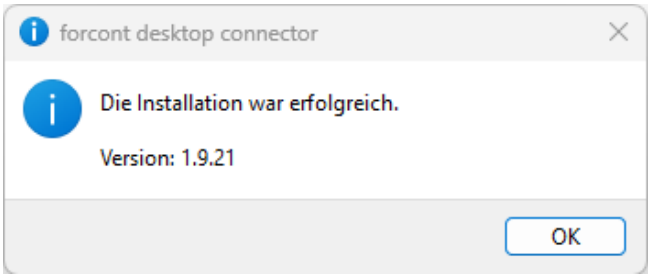

Abbildung 2: Bestätigungsabfrage nach Abschluss der Installation

» Klicken Sie auf **OK**.

Die Installation ist abgeschlossen und Sie finden die installierte Software nun in einem der folgenden Verzeichnisse:

C:\Program Files\forcont desktop connector bzw.

C:\Programme\forcont desktop connector

Hinweis – Deinstallation

Bei Bedarf können Sie die Anwendung über **Systemsteuerung** > **Programme > Programme und Features** > **forcont desktop connector <Version>** deinstallieren.

Softwareverteilung

Das oben erwähnte Installationspaket kann auch im Rahmen einer Softwareverteilung genutzt werden, um den fdc im Sinne einer unbeaufsichtigten Installation auf die Client-PCs zu verteilen.

Hinweis – Anpassen der Konfigurationsdateien vor Installation

Bitte beachten Sie, dass die dem Installationspaket beiliegenden ***setup.ini***-Dateien vor der Installation bzw. Softwareverteilung angepasst werden müssen. Die Anpassungen sind entsprechend der in Kapitel 3.2 beschriebenen Konfigurationsschritte vorzunehmen.

Das gemäß der Beschreibung in Kapitel 3.2 vorkonfigurierte Installationspaket kann sowohl für eine manuelle Installation als auch als Vorlage für eine automatisierte (skriptbasierte) Softwareverteilung verwendet werden. Für eine manuelle Installation führen Sie die folgenden Schritte durch:

» Kopieren Sie das vorkonfigurierte Installationspaket aus dem Konfigurationsverzeichnis (siehe Kapitel 3.2) in das gewünschte Installationsverzeichnis des Client-PCs (z. B. *C:\Programme\forcont desktop connector*)
» Schließen Sie alle MS Office-Anwendungen.
» Installation fdc ohne Zusatzkomponenten:
Führen Sie die Batch-Datei ***installfdc_only.cmd*** im heruntergeladenen Installationspaket als **Administrator** aus.
oder
» Installation fdc mit Zusatzkomponenten:
Führen Sie die Batch-Datei ***installfdc_full.cmd*** im heruntergeladenen Installationspaket als **Administrator** aus.

3.6 Angabe der Whitelist Head Server

» Entpacken Sie das heruntergeladene ZIP-Archiv „forcont_Desktop_Connector.zip“ in einen temporären Ordner.

Das Archiv enthält die beiden Dateien „default.json“ und „forcontDesktopConnector_Setup.exe“.

» Öffnen Sie die Datei **default.json** mit einem beliebigen Editor.
» Ersetzen Sie die Inhalte des Attributs `server` **https://cloud.forcont-services.de/ff/appcfg** (Voreinstellung für Cloud-Kunden) durch die URLs Ihrer gewählten Whitelist Head Server **http://<servername>/ff/appcfg** bzw. **https://<servername>/ff/appcfg** (siehe folgendes Beispiel).

» Speichern und schließen Sie die Datei.

Beispiel:

Für den Fall zweier Whitelist Head Server, die über das HTTPS-Protokoll angesprochen werden, würde die Konfiguration wie folgt aussehen:

```
{
        "server": [
             "https://myheadserver1.mydomain.de/ff/appcfg",
             "https://myheadserver2.mydomain.de/ff/appcfg"
        ],

        "proxy": "",
        "noproxy":
               [
                     "localhost"
               ]
}
```

Hinweis – Verwendung eines Whitelist Head Servers

Im Falle eines einzelnen Whitelist Head Servers entfällt der zweite, durch Komma abgetrennte Eintrag des Attributes `server` (einschließlich des Kommata).

3.7 Konfiguration eines Proxy Servers und von Proxy-Ausnahmen

Hinweis – Proxy-Konfigurationen überspringen

Die Konfiguration eines Proxy Servers und der Proxy-Ausnahmen ist nur erforderlich, wenn Sie beim Zugriff auf Ihren factory-Server bzw. die forcont Cloud einen Proxy Server verwenden. Ist dies nicht der Fall, fahren Sie bitte direkt mit Kapitel 3.8 fort.

Proxy Server

» Entpacken Sie das heruntergeladene ZIP-Archiv „forcont_Desktop_Connector.zip“ in einen temporären Ordner.

Das Archiv enthält die beiden Dateien „default.json“ und „forcontDesktopConnector_Setup“.

» Öffnen Sie die Datei **default.json** mit einem beliebigen Editor.

» Tragen Sie als Wert des Attributs `proxy` die URL Ihres Proxy Servers ein **http://IP-Adresse:Port** bzw. **https://IP-Adresse:Port** (siehe folgendes Beispiel).

Beispiel:

```
{
        "server": [
             "https://myheadserver1.mydomain.de/ff/appcfg",
             "https://myheadserver2.mydomain.de/ff/appcfg"
        ],

        "proxy": "https://192.168.1.1:3128",
        "noproxy":
               [
                     "localhost"
               ]
  }
```

Proxy-Ausnahmen

» Tragen Sie als Wert des Attributs `noproxy` in der **default.json** die Namen aller Hosts ein, welche als **Ausnahme** gelten und nicht über den angegebenen Proxy Server angesprochen werden sollen (siehe folgendes Beispiel).
» Speichern und schließen Sie die Datei.

Beispiel:

```
        …
        "proxy": "https://192.168.1.1:3128",
        "noproxy":
               [
                     "localhost",
                     "myhost.mydomain.com"
               ]
        …
```

Proxy mit Benutzer-Authentifizierung

» Tragen Sie in der **default.json** als Wert des Attributs `proxyUser` den Benutzernamen und als Wert des Attributs `proxyPassword` das Passwort im Klartext ein.
» Während der Installation wird das Passwort verschlüsselt und im Attribut `secureProxyPassword` abgelegt.

Hinweis – Softwareverteilung

Die **default.json** kann für die Softwareverteilung vorbereitet werden, indem ein Administrator eine lokale Referenzinstallation vornimmt und so den Wert für `secureProxyPassword` erzeugt. Die **default.json** mit `secureProxyPassword` kann zur Verteilung benutzt werden, um zu vermeiden, dass bei der Installation auf den Client-PCs ein Passwort im Klartext benötigt wird.

Beispiel nach der Installation:

```
…
"proxy": "https://192.168.1.1:3128",
"proxyUser": "Benutzername",
"proxyPassword": "",
"secureProxyPassword": "Passwort als verschlüsselter String",
"noproxy":
        [
                "localhost",
                "myhost.mydomain.com"
        ]
…
```

Hinweis – Änderung der Benutzerattribute

Bei Änderung des Benutzernamens und/oder Passworts der Proxy-Benutzer-Authentifizierung muss die **default.json** angepasst und erneut verteilt werden.

3.8 Nachträgliche Änderung der Konfiguration

3.8.1 Änderung an der Konfiguration eines Whitelist Head Servers

Die nachträgliche Änderung eines Whitelist Head Servers kann notwendig sein, wenn der bisher verwendete factory-Server nicht mehr den Anforderungen eines Whitelist Head Servers (Aktualität, permanente Aktivität etc.) genügt oder abgeschaltet werden soll oder muss.

Hinweis – Nachträgliche Änderungen nur mit vorheriger Deinstallation und anschließender Neuinstallation

Die in der *setup.ini* vorgenommenen Einstellungen sind für den bereits installierten Client nicht mehr möglich. Sie müssen stattdessen mit *uninstall.cmd* den fdc sowie die Zusatzkomponenten deinstallieren, die gewünschten Anpassungen in der/n *setup.ini* Datei(en) vornehmen und das Installationspaket mit *installfdc_full.cmd* neu installieren.

Um die Whitelist Head Server zu einem späteren Zeitpunkt zu ändern, gibt es zwei Möglichkeiten:

1. **Erneute**, vollständige **Konfiguration und Installation** des fdc (siehe ab Kapitel 3.3).
2. **Ändern** der URL **des Whitelist Head Servers** in der Datei ***default.json*** im untenstehenden Installationsverzeichnis des fdc **und Verteilen** der geänderten ***default.json*** **auf** die **Client-PCs**.

   C:\Program Files\forcont desktop connector bzw.

   C:\Programme\forcont desktop connector

3.8.2 Änderung an der Konfiguration der Zusatzkomponenten

Die Änderung an der Konfiguration der Dokumentablage über Zusatzkomponenten erfolgt über Anpassungen in der *setup.ini*-Datei. Um die Änderungen vollständig ausführen zu können, gehen Sie wie folgt vor:

1. **Deinstallation** des forcont Desktop Connector (siehe Kapitel 3.3).
2. **Anpassen** der ***setup.ini***-Datei(en) (siehe Kapitel 3.2).
3. **Erneute Installation** des forcont Desktop Connector (siehe Kapitel 3.4).

3.9 Verwendung eines Citrix-Clients

Damit der fdc bei Verwendung eines Citrix-Clients lauffähig bleibt, müssen an dem Client die Citrix-API-Hooks für die fdc-Anwendung abgeschaltet werden. Wir empfehlen die Konfiguration über folgende Registrierungsschlüssel (Windows 64-Bit):

- **Registry Keys**:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxHook
  - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook
- **Value Name**: ExcludedImageNames
- **Type**: REG_SZ
- **Value**: forcont desktop connector.exe

Diese Registry-Einstellungen können ebenso in einem Installationsskript mit folgenden Befehlen geschrieben werden:

```
reg add "HKLM\SOFTWARE\Citrix\CtxHook" /v ExcludedImageNames /t REG_SZ /d
"forcont desktop connector.exe"
```

```
reg add "HKLM\SOFTWARE\Wow6432Node\Citrix\CtxHook" /v ExcludedImageNames
/t REG_SZ /d "forcont desktop connector.exe"
```

Weiterführende Hinweise finden Sie unter: https://support.citrix.com/article/CTX107825

Die Anpassungen an der Konfiguration des Citrix-Clients sind notwendig, damit die fdc-Funktionen, die eine Visualisierung auf dem Client-PC erfordern, in der Citrix-Umgebung ausgeführt werden können.

4 Funktionsprüfung

4.1 Funktionsprüfung der Grundkomponente des fdc

Im Folgenden wird beschrieben, wie Sie die Funktionsfähigkeit des fdc nach erfolgreicher Installation überprüfen können. Auf gleichem Weg erhalten Sie Informationen über die fdc-Version, sowie die hinterlegte Server-Whitelist.

Hinweis – Konfiguration des factory Servers für den fdc

Bitte beachten Sie, dass die nachfolgende Prüfung nur erfolgreich verläuft, wenn der factory-Server, der als Whitelist Head Server verwendet wird, bereits für die Unterstützung des fdc konfiguriert wurde.

» Öffnen Sie das Installationsverzeichnis des fdc unter:

C:\Program Files\forcont desktop connector bzw.
C:\Programme\forcont desktop connector

» Führen Sie die Datei **forcont desktop connector.exe** per Doppelklick aus.

Es öffnet sich das Informationsfenster des fdc.

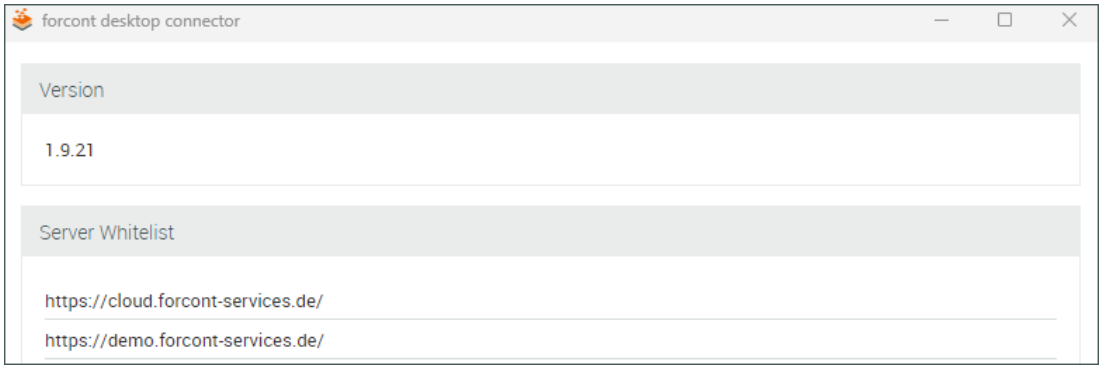

Abbildung 3: Informationsfenster „forcont desktop connector“ mit Versionsangabe und Server-Whitelist

Das Informationsfenster des fdc zeigt Ihnen die Version des installierten fdc sowie den Inhalt der vom ersten erreichbaren Whitelist Head Server gelesenen Server-Whitelist an.

Nach erfolgreicher Konfiguration und Installation des fdc muss die Server-Whitelist die URLs aller factory Server beinhalten, auf denen factory-Anwendungen laufen, welche den fdc benötigen.

4.2 Funktionsprüfung der Grundkomponente des fdc und der Zusatzkomponenten

Im Folgenden wird beschrieben, wie Sie die Funktionsfähigkeit des fdc und der Zusatzkomponenten nach erfolgreicher Installation überprüfen können. Auf gleichem Weg erhalten Sie Informationen über die fdc-Version, sowie die hinterlegte Server-Whitelist.

Hinweis – Konfiguration des factory-Servers für den fdc

Bitte beachten Sie, dass die nachfolgende Prüfung nur erfolgreich verläuft, wenn der factory-Server, der als Whitelist Head Server verwendet wird, bereits für die Unterstützung des fdc konfiguriert wurde.

Die Funktionsfähigkeit des fdc erfolgt wie unter Kapitel 4.1 aufgeführt.

Die Funktionsfähigkeit der Zusatzkomponenten kann nach erfolgreicher Installation überprüft werden.

Führen Sie für die Office-Integration die folgenden Schritte durch:

» Öffnen Sie eine von den Zusatzkomponenten unterstützte MS Office-Anwendung und prüfen Sie, ob die Registerkarte **factory** im oberen Menüband vorhanden ist.

Führen Sie für die Adobe Integration folgende Schritte durch:

» Öffnen Sie eine von den Zusatzkomponenten unterstützte Adobe-Anwendung und prüfen Sie, ob die Registerkarte **factory** im oberen Menüband vorhanden ist.

Führen Sie für das Droplet die folgenden Schritte durch:

» Starten Sie aus dem Installationsverzeichnis des Installationspakets das Programm *..\Office_Integration\DesktopWin\FFDroplet.exe* und kontrollieren Sie, dass anschließend das Icon für das Droplet erscheint.

Wenn Sie über einen Zugang zur factory-Anwendung verfügen, können Sie die Funktionsfähigkeit außerdem wie folgt überprüfen (Anmeldung notwendig):

» Öffnen Sie eine von den Zusatzkomponenten unterstützte MS Office-Anwendung und legen Sie über ein Office-, Acrobat-Plug-In bzw. Droplet ein Dokument in der Registerkarte **factory** im oberen Menüband in eine factory-Anwendung ab.

» Prüfen Sie, ob das abgelegte Dokument nach dem Attribuieren und Abschicken der Maskeneingaben in der factory-Anwendung recherchierbar ist.

5 Update

Bevor ein Update des fdc durchgeführt werden kann, muss die bisherige Version samt Zusatzkomponenten (falls vorhanden) deinstalliert werden. Das kann – analog zur Installation – manuell oder skript-basiert geschehen (siehe Kapitel 3.5).

Hinweis – Kopieren der Datei *default.json*

Kopieren und Sichern Sie die Konfigurationsdatei ***default.json*** und ggf. die ***setup.ini*** im aktuellen Installationsverzeichnis des fdc, bevor Sie die Deinstallation durchführen. Das erleichtert die Übertragung der kundenspezifischen Konfigurationsdaten nach der notwendigen Neuinstallation (Update).

Wurde der fdc vollständig deinstalliert, folgen Sie den Anweisungen ab Kapitel 3.2, um die aktuelle Version des fdc und ggf. der Zusatzkomponenten zu installieren und das Update abzuschließen.

Ist ein Update der Zusatzkomponenten erforderlich, führen Sie dazu die folgenden Schritte durch:

- Deinstallieren Sie die bisherige Version der Zusatzkomponenten (siehe Kapitel 3.3).
- Konfigurieren Sie das heruntergeladene Installationspaket (siehe Kapitel 3.2), oder verwenden Sie die alten Konfigurationsdateien wieder.
- Installieren Sie die aktuelle Version der Zusatzkomponenten (siehe Kapitel 3.4).

Das Update des alten Clients (also die alten Zusatzkomponenten) kann auf die gleiche Weise (zuerst *uninstall.cmd* und dann *install.cmd* ausführen, siehe 3.3 und 3.4) vorgenommen werden. Grund für die Vorgehensweise ist, dass die *uninstall.cmd* alle vorhandenen Client-Komponenten (alt oder neu) deinstalliert.

Die vorhandenen Konfigurationen *default.json* für den fdc und ggf. *setup.ini* mit 32- und 64-Bit für die Zusatzkomponenten sollten vorher gesichert und in das neue Installationspaket übernommen werden.

6 Erneuerung des Code Signing-Zertifikats

Aus Sicherheitsgründen ist die Softwarekomponente fdc und die Zusatzkomponenten mit einem Code Signing-Zertifikat signiert, dessen Gültigkeit zeitlich befristet ist. Nach dem Ablauf des Zertifikats erscheint bei der Installation des fdc und bei den Zusatzkomponenten eine Fehlermeldung bzw. Sicherheitswarnung. Für künftige Installationen ist die aktualisierte fdc-Version mit neuem Code Signing-Zertifikat zu verwenden.

Hinweis – Neusignierung wichtig bei fdc-Neuinstallation

Die Erneuerung des Code Sigining-Zertifikats ist **nur wichtig für die Neuinstallation des fdc**. Die Signatur des Office-Add-Ins der Zusatzkomponenten wird dagegen bei jedem Start der Office-Anwendung geprüft. Aus dem Grund muss im Falle einer Installation des fdc mit Zusatzkomponenten diese nach jeder Neusignierung **aktualisiert** werden.

» Laden Sie dazu die aktuelle fdc-Version unter folgendem Link herunter: https://forcont.de/forcont-desktop-connector/fdc

Das Code Signing-Zertifikat der Softwarekomponente fdc wird ausschließlich während der Installation geprüft. Somit muss lediglich bei allen künftigen Installationen die aktualisierte Version des Installationspakets verwendet werden.

» Verwenden Sie bei allen künftigen Installationen auf den Client-PCs die aktuelle Version des Installationspakets und führen Sie bei Bedarf ein Update durch (siehe Kapitel 5 „Update“).

Office Integration

Das Code Signing-Zertifikat der Zusatzkomponente **Office Integration** wird während der Installation sowie während des Betriebs geprüft. Um die Zusatzkomponente auch nach Ablauf des Zertifikats verwenden zu können, ist ein Update auf die aktuelle Version erforderlich.

» Führen Sie (vor Ablauf des Zertifikats) ein Update der Zusatzkomponente auf den Client-PCs durch (siehe Kapitel 5 „Update“).

7 Hilfe bei Problemen

Bei der Verwendung des fdc sowie bei der Konfiguration, Installation und Ausführung der Zusatzkomponenten kann es, beispielsweise durch eine falsche Konfiguration der Server-Whitelist, eine temporäre Inaktivität aller konfigurierten Whitelist Head Server oder andere äußere Umstände, zu verschiedenen Fehlern kommen.

In der folgenden Tabelle finden Sie sowohl mögliche Fehlermeldungen als auch Lösungen zur Behebung der Fehlerursachen, die in der Konfiguration, Installation oder dem Betrieb Ihrer factory-Server sowie des fdc liegen können.

Bei Fehlermeldungen, die hier nicht aufgeführt sind, kontaktieren Sie bitte unseren Support per Telefon (+49 341 48503-75) oder E-Mail (factory-support@forcont.de).

Fehlermeldungen

Nr.	Fehlermeldung	Mögliche Lösung
1	Die Konfiguration der default.json ist fehlerhaft.	• Prüfen Sie, ob die Datei *default.json* im Installationsverzeichnis des fdc (Client-PC) abgelegt wurde. • Prüfen Sie, ob die Datei *default.json* frei von Tipp- und Formatierungsfehlern ist. **Formatierungsregeln**: URLs enden mit Schrägstrich (/), stehen in Anführungs-zeichen („“) und sind durch Kommata getrennt (,) (siehe Beispiel Kapitel 3.3).
2	Die Verbindung zum Server konnte nicht hergestellt werden.	• Prüfen Sie, ob der angegebene Server aktiv ist und über das Netzwerk vom Client-PC aus erreicht werden kann. • Falls Sie einen Proxy Server verwenden, prüfen Sie, ob dieser sowie etwaige Proxy-Ausnahmen korrekt konfiguriert wurden (siehe Kapitel 3.4)
3	Die Server-Whitelist konnte nicht gelesen werden. Prüfen Sie die Konfiguration.	• Prüfen Sie, ob der notwendige Server-Hotfix installiert wurde (siehe Kapitel 2.2) • Prüfen Sie, ob die Datei *di.json* (Server-Whitelist) auf allen Whitelist Head Servern abgelegt wurde (siehe Kapitel 3.1).

Nr.	Fehlermeldung	Mögliche Lösung
4	Die Server-Whitelist konnte nicht gelesen werden. Prüfen Sie die Konfiguration. Formatierungsfehler!	• Prüfen Sie, ob die URLs der Whitelist Head Server in der Datei *default.json* im Installationsverzeichnis des fdc (Client-PC) korrekt sind (siehe Kapitel 3.3). • Prüfen Sie, ob die Datei *di.json* (Server-Whitelist) auf den Whitelist Head Servern frei von Tipp- und Formatierungsfehlern ist. **Formatierungsregeln**: URLs enden mit Schrägstrich (/), stehen in Anführungszeichen („“) und sind durch Kommata getrennt (,) (siehe Beispiel Kapitel 3.1).
5	Die Antwort des factory-Servers konnte nicht gelesen werden. Formatierungsfehler!	• Die Client-Server-Verschlüsselung ist fehlerhaft, es wird ein falscher Wert gesendet. • Prüfen Sie, ob die Datei *di.keystore* im factory-Verzeichnis der Whitelist Head Server existiert. Ist das nicht der Fall, wenden Sie sich bitte an unseren Support.
6	Es sind nur Verbindungen zu einem Server der Server-Whitelist zulässig.	• Prüfen Sie, ob Ihr aktueller factory-Server in der Server-Whitelist gepflegt wurde. • Prüfen Sie, ob die Datei *di.json* (Server-Whitelist) auf den Whitelist Head Servern frei von Tipp- und Formatierungsfehlern ist. **Formatierungsregeln**: URLs enden mit Schrägstrich (/), stehen in Anführungszeichen („“) und sind durch Kommata getrennt (,) (siehe Beispiel Kapitel 3.1).
7	Die Server-Whitelist ist leer. Prüfen Sie die Konfiguration.	• Prüfen Sie, ob in der Datei *di.json* (Server-Whitelist) auf den Whitelist Head Servern Einträge vorhanden sind (siehe Kapitel 3.1). • Prüfen Sie, ob die Datei *di.json* (Server-Whitelist) auf den Whitelist Head Servern frei von Tipp- und Formatierungsfehlern ist. **Formatierungsregeln**: URLs enden mit Schrägstrich (/), stehen in Anführungszeichen („“) und sind durch Kommata getrennt (,) (siehe Beispiel Kapitel 3.1).

Nr.	Fehlermeldung	Mögliche Lösung
8	Die Installation der Zusatzkomponenten schlägt aufgrund eines Schreibfehlers in der Windows-Registrierungs-datenbank (Registry) fehl.	• Die Installation der Zusatzkomponenten wurde möglicherweise ohne Administratorrechte ausgeführt. • Führen Sie die Installation der Zusatzkomponenten mit Administrator-rechten erneut aus (siehe Kapitel 3.4).

Tabelle 1: fdc-Fehlermeldungen

Protokolldaten (.log)

Detaillierte technische Informationen zu den aufgetretenen Fehlern werden im Hintergrund protokolliert und im folgenden Verzeichnis gespeichert:

C:\Users\<Username>\AppData\Local\Temp