INSTALLATIONSANLEITUNG

forcont Desktop Connector

Stand: 02.03.2026

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
- Ggfs. 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.

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.*

Werden in ihrer Organisation HTTPS-Zertifikate verwendet, die von einer firmeneigenen Zertifizierungsstelle ausgestellt wurden (selbstsigniert), 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 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 Genereller Ablauf der Installation

Der generelle Ablauf der fdc-Installation beinhaltet die folgenden Schritte:

- Herunterladen des Installationspakets (ZIP-Archiv) von der forcont-Website und Prüfung der Integrität
- Entpacken des ZIP-Archivs auf einem beliebigen PC und Durchführung von Anpassungen an den enthaltenen Konfigurationsdateien
- Kopieren des angepassten Installationspakets auf die Client-PCs
- Deinstallation ggf. bereits vorhandener, älterer fdc-Komponenten bzw. von Komponenten der forcont Desktop Integration 7, welche den Vorgänger des fdc darstellt
- Neuinstallation des fdc

3.2 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

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 FDC_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.

» Entpacken Sie das heruntergeladene ZIP-Archiv in einen temporären Ordner ihrer Wahl. Es entsteht das Verzeichnis **FDC_Install_package**.
» Nehmen Sie die unter Kapitel 3.4 beschriebenen Anpassungen an den im Installationspaket enthaltenen Konfigurationsdateien vor. Beachten Sie dabei bitte auch die im folgenden Kapitel enthaltenen Informationen zur (server-seitigen) Konfiguration der Server-Whitelist.

3.3 Funktionsweise und server-seitige 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.

Die Verwendung mehrerer Whitelist Head Server ermöglicht es, den Ausfall eines der Head Server kompensieren zu können. Daher 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 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 Verzeichnis des factory-Servers, welchen Sie als Whitelist Head Server ausgewählt 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-Anwendungsserver** ein, mit welchen der fdc kommunizieren können soll/darf (siehe Beispiel unten).

Die beiden letzten der im untenstehenden Beispiel gezeigten Einträge entsprechen den URLs der factory-Server der forcont Cloud (Voreinstellungen für Cloud-Kunden).

» Speichern und schließen Sie die Datei.

Beispiel:

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

Wenn Sie Ihre factory-Anwendung zusätzlich im internen Netz über den Kurznamen **http://factoryapp/...** aufrufen möchten, muss ergänzend die 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-Anwendungsserver 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 anderen, eventuell vorhandenen Whitelist Head Servern zu aktualisieren.

3.4 Konfiguration des Installationspakets

3.4.1 Konfigurationsdatei default.json

Alle Einstellungsparameter des **forcont Desktop Connector** befinden sich in der Datei ***default.json*** im Unterverzeichnis **fdc** des von ihnen vorab entpackten Installationspakets. Diese Datei wird später im Zuge der Installation des fdc auf den Client-PCs mit ins Programmverzeichnis des fdc geschrieben. Das heißt, alle Anpassungen an der ***default.json***, die Sie hier bei der Vorbereitung des Installationspakets vornehmen, werden in die fdc-Konfiguration der Client-PCs übernommen.

Folgende Konfigurationsparameter sind verfügbar:

Name Parameter	Beschreibung
server	URL zum Head Server der factory (siehe Kapitel 3.4.1.1)
proxy	URL zum verwendeten Proxy (siehe Kapitel 3.4.1.2) oder "" (default)
proxyUser	Benutzer zum verwendeten Proxy (siehe Kapitel 3.4.1.2) oder "" (default)
proxyPassword	Proxypasswort zum verwendeten Proxy (siehe Kapitel 3.4.1.2) oder "" (default)

Name Parameter	Beschreibung
secureProxyPassword	verschlüsseltes Proxypasswort zum verwendeten Proxy (siehe Kapitel 3.4.1.2) oder "" (default)
noproxy	Array von Hostnamen für die bei der Verbindung zur factory kein Proxy verwendet werden soll. (siehe Kapitel 3.4.1.2)
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)

Tabelle 1: Konfigurationsparameter in default.json für den forcont Desktop Connector

3.4.1.1 Angabe der Whitelist Head Server

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**.

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 Kommas).

3.4.1.2 Konfiguration eines Proxy Servers und von Proxy-Ausnahmen

Hinweis – Proxy-Konfiguration 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, können Sie dieses Kapitel überspringen.

Proxy Server

» 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).
» Speichern und schließen Sie die Datei.

Beispiel:

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

        "proxy": "http://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": "http://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 des fdc wird das Passwort automatisch verschlüsselt, im Attribut `secureProxyPassword` abgelegt und das Klartextpasswort wird aus dem Attribut `proxyPassword` entfernt.

Hinweis – Softwareverteilung

Die ***default.json*** kann für die Softwareverteilung dahingehend vorbereitet werden, dass ein Administrator eine lokale Referenzinstallation vornimmt und auf diesem Wege eine ***default.json*** erzeugt, die den Wert für `secureProxyPassword` bereits enthält. Diese ***default.json*** mit `secureProxyPassword` kann dann nachfolgend zur Verteilung benutzt werden. Damit wird vermieden, dass bei der Installation auf den Client-PCs das Proxy-Passwort im Klartext ersichtlich ist.

Beispiel nach der Installation:

```
…
"proxy": "http://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.

3.5 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 3.2).

Manuelle Installation

Das gemäß der Beschreibung in Kapitel 3.4 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 bitte die untenstehenden Schritte aus. Bitte **beachten** Sie, dass Sie für die Aktionen, die Sie auf den **Client-PCs** ausführen, **administrative Berechtigungen** benötigen.

- Kopieren Sie das vorab vorbereitete Verzeichnis **FDC_Install_package** in das Verzeichnis **C:\Programme** der Client-PCs.
- Führen Sie im Verzeichnis **C:\Programme\FDC_Install_package** der Client-PCs zunächst die Batch-Datei ***uninstall.cmd*** aus, um sicherzustellen, dass alle Komponenten einer älteren fdc- oder auch DI7-Version ordnungsgemäß deinstalliert werden.
- Führen Sie nachfolgend die Batch-Datei ***install.cmd*** im Verzeichnis **C:\Programme\FDC_Install_package** aus, um den fdc neu zu installieren.
- **Bitte belassen** Sie das Installationspaket auch nach der Installation im Verzeichnis **C:\Programme\FDC_Install_package** der **Client-PCs**, da nur über die darin enthaltene Deinstallationsroutine eine spätere problemlose Deinstallation des fdc möglich ist.

3.6 Nachträgliche Änderung der Konfiguration

3.6.1 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.

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 3.4). oder
2. **Ändern** der URL **des Whitelist Head Servers** in der Datei ***default.json*** und erneute Verteilung dieser Datei auf die Client-PCs. Der Austausch der Datei muss dabei im untenstehenden Verzeichnis der Client-PCs erfolgen:

   C:\Programme\forcont desktop connector

Im Hinblick auf den Arbeitsaufwand ist die zweite Variante sicherlich in den meisten Fällen die zu bevorzugende.

3.7 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 dem gleichen 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:\Programme\forcont desktop connector

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

Es öffnet sich das Informationsfenster des fdc.

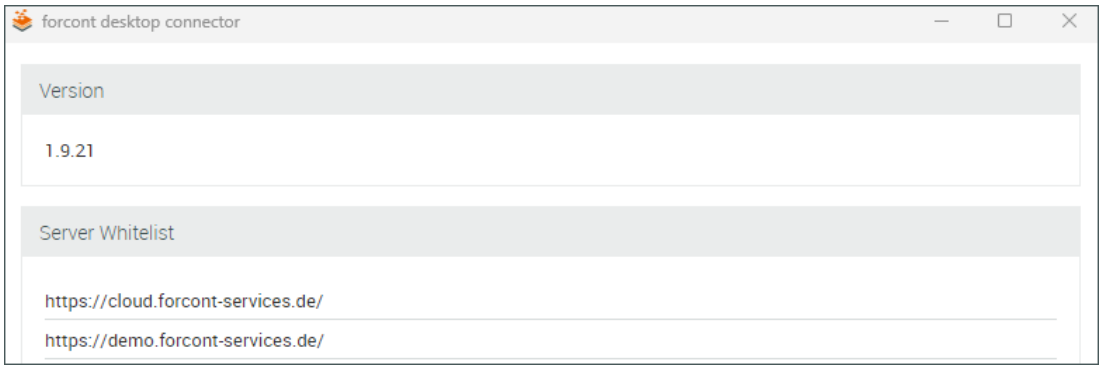

Abbildung 1: Informationsfenster „forcont desktop connector“ mit Versionsangabe und Server-Whitelist

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.

5 Update

Bevor ein Update des fdc durchgeführt werden kann, muss die bisherige Version deinstalliert werden.

Hinweis – Sichern der Datei *default.json*

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

- Bereiten Sie zunächst das Installationspaket der neuen fdc-Version entsprechend Kapitel 3.4 vor.
  Sollte sich in der fdc-Konfiguration gegenüber der bisherigen Version nichts geändert haben, können Sie die vorab gesicherte ***default.json*** für das neue Installationspaket **wiederverwenden**.
- Führen Sie nachfolgend auf den Client-PCs im Verzeichnis **C:\Programme\FDC_Install_package** die Batch-Datei ***uninstall.cmd*** aus, um alle Komponenten der bisherigen fdc-Version zu deinstallieren. **Bitte beachten** Sie dabei, dass Sie für diese und die nachfolgenden Aktionen **administrative Rechte** benötigen.
- **Ersetzen** Sie bitte nach erfolgter Deinstallation das Verzeichnis **C:\Programme\FDC_Install_package** durch das gleichnamige Verzeichnis des vorab vorbereiteten Installationspakets der neuen fdc-Version.
- Führen Sie nun die Batch-Datei ***install.cmd*** im Verzeichnis **C:\Programme\FDC_Install_package** des jeweiligen Client-PCs aus.
- Prüfen Sie bitte nach abgeschlossener Installation die Funktionstüchtigkeit des fdc nach der Anleitung in Kapitel 4.

Hinweis – Deinstallation der alten Version

Sollte das Verzeichnis **C:\Programme\FDC_Install_package** auf den Client-PCs nicht zur Verfügung stehen, um die bisherige Version des fdc deinstallieren zu können, kopieren Sie bitte das gleichnamige Verzeichnis der neuen fdc-Version nach **C:\Programme** und führen Sie nachfolgend die Batch-Datei ***uninstall.cmd*** im Verzeichnis **C:\Programme\FDC_Install_package** aus.
Danach kann dann durch Ausführung der Batch-Datei ***install.cmd*** im gleichen Verzeichnis die neue fdc-Version installiert werden.

6 Erneuerung des Code Signing-Zertifikats

Aus Sicherheitsgründen ist die Softwarekomponente fdc mit einem Code Signing-Zertifikat signiert, dessen Gültigkeit zeitlich befristet ist. Nach dem Ablauf des Zertifikats erscheint bei der Installation des fdc 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**.

» 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).

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 Anführungszeichen ("") und sind durch Kommata getrennt (,) (siehe Beispiel Kapitel 3.4).

Nr.	Fehlermeldung	Mögliche Lösung
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 3.4.1.2)
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 3.3).
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 3.4). • 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 Anführungs-zeichen ("") und sind durch Kommata getrennt (,) (siehe Beispiel Kapitel 3.3).
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 Anführungs-zeichen ("") und sind durch Kommata getrennt (,) (siehe Beispiel Kapitel 3.3).

Nr.	Fehlermeldung	Mögliche Lösung
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 3.3). • 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 3.3).

Tabelle 2: fdc-Fehlermeldungen

Protokolldaten (.log)

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

C:\Benutzer\<Benutzername>\AppData\Roaming\forcont desktop connector\logs