INSTALLATIONSANLEITUNG

forcont Desktop Integration 7 (Version 1.7.0)

Stand: 12.02.2024

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 ... 4
2 Softwarevoraussetzungen ... 5
2.1 Client-PCs ... 5
2.2 factory Server ... 5
3 Vorbereitung und Installation ... 6
3.1 Funktionsweise und Konfiguration der Server Whitelist ... 6
3.2 Herunterladen und Prüfen des Installationspakets ... 8
3.3 Angabe der Whitelist Head Server ... 9
3.4 Konfiguration eines Proxy Servers und von Proxy-Ausnahmen ... 10
3.5 Installation der Desktop Integration 7 ... 12
3.6 Änderung eines Whitelist Head Servers ... 14
3.7 Verwendung eines Citrix-Clients ... 14
4 Funktionsprüfung ... 15
5 Update ... 16
6 Erneuerung des Code Signing-Zertifikats ... 16
7 Hilfe bei Problemen ... 17
A Versionshistorie ... 20

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 Integration 7** auf dem PC des Benutzers (Client-PC) installiert sein.

Bei der forcont Desktop Integration 7 – im Weiteren **DI7** 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 der DI7 notwendig sind.

2 Softwarevoraussetzungen

2.1 Client-PCs

Zur Installation und Anwendung der DI7 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 von der DI7 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. Die DI7 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 der DI7 auf den factory Servern ist die Installation des aktuellen Hotfixes für die factory-Versionen 7.0b bis einschließlich 7.1b. Ab factory-Version 7.1c ist der factory Server für die Verwendung der DI7 vorbereitet.

» Installieren Sie den aktuellen Hotfix für den factory Server.

Den aktuellen Hotfix für Ihren factory Server sowie die Installationsanleitung können Sie unter folgender URL herunterladen:

https://www.forcont.de/desktop-integration7-hotfix/

3 Vorbereitung und Installation

3.1 Funktionsweise und Konfiguration der Server Whitelist

Funktionsweise der DI7 über eine Server Whitelist

Um die Kommunikation der client-seitig installierten DI7 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 die DI7 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, zum Head Server bestimmte 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 der DI7 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 bestimmt 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 die DI7 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 Kommas 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 bestimmt haben.

Pflege der Server Whitelist

Kommen zu einem späteren Zeitpunkt neue factory Server hinzu, welche über die DI7 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, evtl. vorhandenen Whitelist Head Servern zu aktualisieren.

3.2 Herunterladen und Prüfen des Installationspakets

forcont stellt Ihnen alle Dateien zur Installation der DI7 als **ZIP-Archiv** zur Verfügung.

» Laden Sie das Installationspaket unter dem folgenden Link herunter:

https://www.forcont.de/desktop-integration7-client/

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* 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 forcont_Desktop_Integration_7.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 Angabe der Whitelist Head Server

» Entpacken Sie das heruntergeladene ZIP-Archiv „forcont_Desktop_Integration_7.zip“ in einen temporären Ordner.

Das Archiv enthält die beiden Dateien „default.json“ und „forcont_Desktop_Integration_7.exe“.

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

» Ersetzen Sie die Inhalte des Attributs `server` **https://cloud.forcont-services.de/appcfg** und **https://demo.forcont-services.de/appcfg** (Voreinstellung für Cloud-Kunden) durch die URLs Ihrer gewählten Whitelist Head Server **http://<servername>/ff/fxsc** bzw. **https://<servername>/ff/fxsc** (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/fxsc",
             "https://myheadserver2.mydomain.de/ff/fxsc"
        ],

        "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 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 3.5 fort.

Proxy Server

» Entpacken Sie das heruntergeladene ZIP-Archiv „forcont_Desktop_ Integration_7.zip“ in einen temporären Ordner.

Das Archiv enthält die beiden Dateien „default.json“ und „forcont_Desktop_ Integration_7.exe“.

» 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/fxsc",
             "https://myheadserver2.mydomain.de/ff/fxsc"
        ],

        "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.

3.5 Installation der Desktop Integration 7

Die Installation der DI7 kann über eine manuelle Installation auf den Client-PCs oder über eine Softwareverteilung erfolgen.

Hinweis – Digitale Signaturen

Die Installationssoftware sowie alle ausführbaren Dateien der DI7 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

» Starten Sie die Installation mit Doppelklick auf die Datei „forcont_Desktop_Integration_7.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.

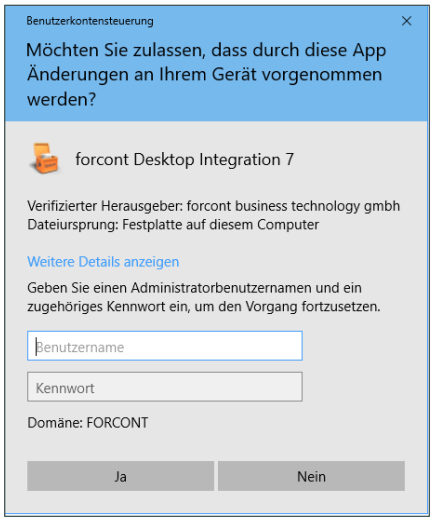

Abbildung 1: Benutzerkontensteuerung für die Eingabe des Administratoren-Benutzerkontos

» Geben Sie folgende Angaben ein:

Benutzername: Eingabe des Windows-Accounts mit Administratorrechten

Kennwort: Passwort für den Windows-Account

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.

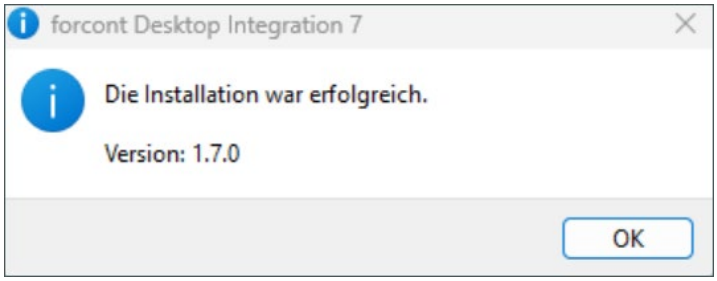

Abbildung 2: Bestätigungsabfrage nach Abschluss der Installation

» 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 Integration 7

C:\Programme\forcont Desktop Integration 7

Hinweis – Deinstallation

Bei Bedarf können Sie die Anwendung über **Systemsteuerung** > **Programme und Funktionen** > **forcont Desktop Integration 7** deinstallieren.

Softwareverteilung

Das oben erwähnte Installationspaket kann auch im Rahmen einer Softwareverteilung genutzt werden, um die DI7 im Sinne einer unbeaufsichtigten Installation auf die Client-PCs zu verteilen.

Da es für die Installation von Softwarepaketen mittels Softwareverteilung eine Vielzahl von Möglichkeiten und Anwendungen gibt, soll an dieser Stelle nur **beispielhaft** auf eine Verteilung mittels Windows-Bordmitteln (Group Policies + Windows Batch-Skript) hingewiesen werden. Die folgenden Batch-Kommandos können dabei als Vorlage dienen:

Installation:

```
<DRIVE>:\PATH_TO_EXE\forcont_Desktop_Integration_7.exe /S
```

Alternative:

```
start /wait <DRIVE>:\PATH_TO_EXE\forcont_Desktop_Integration_7.exe /S
```

Deinstallation:

Die Deinstallation kann im Silent-Modus, mithilfe des „Uninstallers“ der DI7 erfolgen.

```
"C:\Program Files\forcont Desktop Integration 7\Uninstall forcont Desktop Integration 7.exe" /S
```

Hinweis – Anpassung der *default.json*

Bitte beachten Sie, dass, vor Beginn der Verteilung der Software, die dem Installationspaket beiliegende Datei ***default.json*** angepasst werden muss. Die Anpassungen sind entsprechend der in Kapitel 3.3 beschriebenen Vorgaben für **Whitelist Head Server** sowie der in Kapitel 3.4 beschriebenen Vorgaben für **Proxy-Server** vorzunehmen.

Bei der Installation der DI7 wird die Datei ***default.json*** in das Installationsverzeichnis der DI7 auf den Client-PCs geschrieben. Spätere Änderungen der Whitelist Head Server oder des Proxy Servers in der Datei ***default.json*** erfordern eine Neuinstallation der DI7 oder das Verteilen der geänderten Datei ***default.json*** auf die Client-PCs.

3.6 Änderung eines Whitelist Head Servers

Die 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/muss.

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

1. **Erneute**, vollständige **Konfiguration und Installation** der DI7 (siehe ab Kapitel 3.3).
2. **Ändern** der URL **des Whitelist Head Servers** in der Datei ***default.json*** im untenstehenden Installationsverzeichnis der DI7 **und Verteilen** der geänderten ***default.json*** **auf** die **Client-PCs**.

   C:\Program Files\forcont Desktop Integration 7 bzw.

   C:\Programme\forcont Desktop Integration 7

3.7 Verwendung eines Citrix-Clients

Damit die DI7 bei Verwendung eines Citrix-Clients lauffähig bleibt, müssen an dem Client die Citrix-API-Hooks für die DI7-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 Integration 7.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 Integration 7.exe"
```

```
reg add "HKLM\SOFTWARE\Wow6432Node\Citrix\CtxHook" /v ExcludedImageNames /t REG_SZ /d "forcont Desktop Integration 7.exe"
```

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

Die Anpassungen an der Konfiguration des Citrix-Clients sind notwendig, damit die DI7-Funktionen, die eine Visualisierung auf dem Client-PC erfordern, in der Citrix-Umgebung ausgeführt werden können.

4 Funktionsprüfung

Im Folgenden wird beschrieben, wie Sie die Funktionsfähigkeit der DI7 nach erfolgreicher Installation überprüfen können. Auf gleichem Weg erhalten Sie Informationen über die DI7-Version, sowie die hinterlegte Server Whitelist.

Hinweis – Konfiguration des factory Servers für die DI7

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 der **DI7** konfiguriert wurde.

» Öffnen Sie das Installationsverzeichnis der DI7 unter:

C:\Program Files\forcont Desktop Integration 7 bzw.

C:\Programme\forcont Desktop Integration 7

» Führen Sie die Datei **forcont Desktop Integration 7.exe** per Doppelklick aus.

Es öffnet sich das Informationsfenster der DI7.

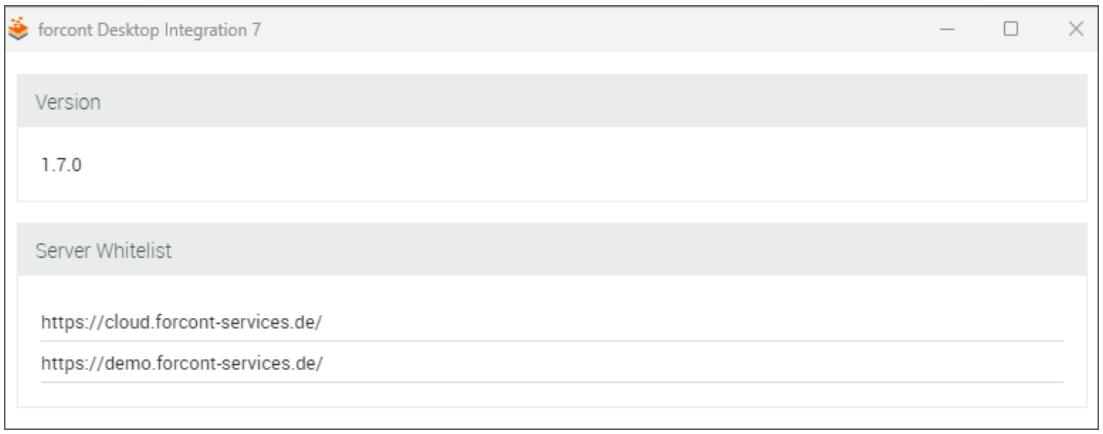

Abbildung 3: Informationsfenster „forcont Desktop Integration 7“ mit Versionsangabe und Server Whitelist

Das Informationsfenster der DI7 zeigt Ihnen die Version der installierten DI7 sowie den Inhalt der vom ersten erreichbaren Whitelist Head Server gelesenen Server Whitelist an.

Nach erfolgreicher Konfiguration und Installation der DI7 muss die Server Whitelist die URLs aller factory Server beinhalten, auf denen factory-Anwendungen laufen, welche die DI7 benötigen.

5 Update

Bevor ein Update der DI7 durchgeführt werden kann, muss die bisherige Version 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*** im aktuellen Installationsverzeichnis der DI7, bevor Sie die Deinstallation durchführen. Das erleichtert die Übertragung der kundenspezifischen Konfigurationsdaten nach der notwendigen Neuinstallation (Update).

Wurde die DI7 vollständig deinstalliert, folgen Sie den Anweisungen ab Kapitel 3.2, um die aktuelle Version der DI7 zu installieren und das Update abzuschließen.

6 Erneuerung des Code Signing-Zertifikats

Aus Sicherheitsgründen ist die Softwarekomponente DI7 mit einem Code Signing-Zertifikat signiert, dessen Gültigkeit zeitlich befristet ist. Nach dem Ablauf des Zertifikats erscheint bei der Installation der DI7 eine Fehlermeldung bzw. Sicherheitswarnung. Für künftige Installationen ist die aktualisierte DI7-Version mit neuem Code Signing-Zertifikat zu verwenden.

» Laden Sie dazu die aktuelle DI7-Version 1.7.0 unter folgendem Link herunter: http://www.forcont.de/desktop-integration7-client/

Das Code Signing-Zertifikat der Softwarekomponente DI7 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“).

Hinweis – Bestehende DI7-Installationen nicht betroffen

Das Code Signing-Zertifikat der DI7 wird ausschließlich bei der Installation der Softwarekomponente geprüft. Bestehende DI7-Installationen auf den Client-PCs sind nicht betroffen und müssen nicht aktualisiert werden.

7 Hilfe bei Problemen

Bei der Verwendung der DI7 kann es, beispielsweise durch eine falsche Konfiguration der Server Whitelist, eine temporäre Inaktivität aller konfigurierten Whitelist Head Server oder andere äußere Umstände, zu 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 der DI7 liegen können.

Bei Fehlermeldungen, die hier nicht aufgeführt sind, kontaktieren Sie bitte unseren Support per Telefon (+49 341 48503-75) oder http (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 der DI7 (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 Kommas 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 der DI7 (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 Kommas 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 Kommas 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 Kommas getrennt (,) (siehe Beispiel Kapitel 3.1).

Tabelle 1: DI7-Fehlermeldungen

Protokolldaten (.log)

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

C:\Users\<Username>\AppData\Roaming\forcont Desktop Integration 7\logs

A Versionshistorie

DI7-Version	Änderungen
1.0.5	» Aktualisierung der Electron-Version » Aktualisierung und Ergänzung der Liste der SSL Root-Zertifikate » Angabe mehrerer Whitelist Head Server möglich (Fallback) » Korrekte Auswertung des Proxy Reply „http 503“ (Nichterreichbarkeit des Whitelist Head Servers) » Einträge in der Server Whitelist sind „case-insensitive“ (Groß- und Kleinschreibung wird nicht berücksichtigt)
1.1.0	» Verbesserte Prüfung von SSL-Zertifikaten und Einträgen der Server Whitelist » Optimierungen beim Hoch- und Herunterladen von Dateien per Drag-and-Drop » Fehlerbehebungen beim Versenden von E-Mail-Benachrichtigungen » Überarbeitete Lokalisierung
1.2.0	» Erneuerung des Code Signing-Zertifikats im Installationspaket
1.3.0	» Aktualisierung der Electron-Version » Aktualisierung der verwendeten Bibliotheken » MS Office-Funktionalität vollständig über native Erweiterung „OutlookUtil“ bereitgestellt » Proxy mit Benutzer-Authentifizierung möglich » Änderung des temporären DI7-Verzeichnisses mittels Parameter *useSystemTemp* möglich (nicht im Standard vorhanden) » Überarbeitete Lokalisierung » Code-Optimierungen und Fehlerbehebungen
1.4.0	» Erneuerung des Code Signing-Zertifikats im Installationspaket
1.5.0	» Optimierungen im Build-Prozess
1.6.0	» Problem mit zahlreichen Zertifikaten gelöst » Installation der neuen DI7 bei manuell umbenannter alter Installation nun möglich
1.7.0	» Erneuerung des Code Signing-Zertifikats im Installationspaket