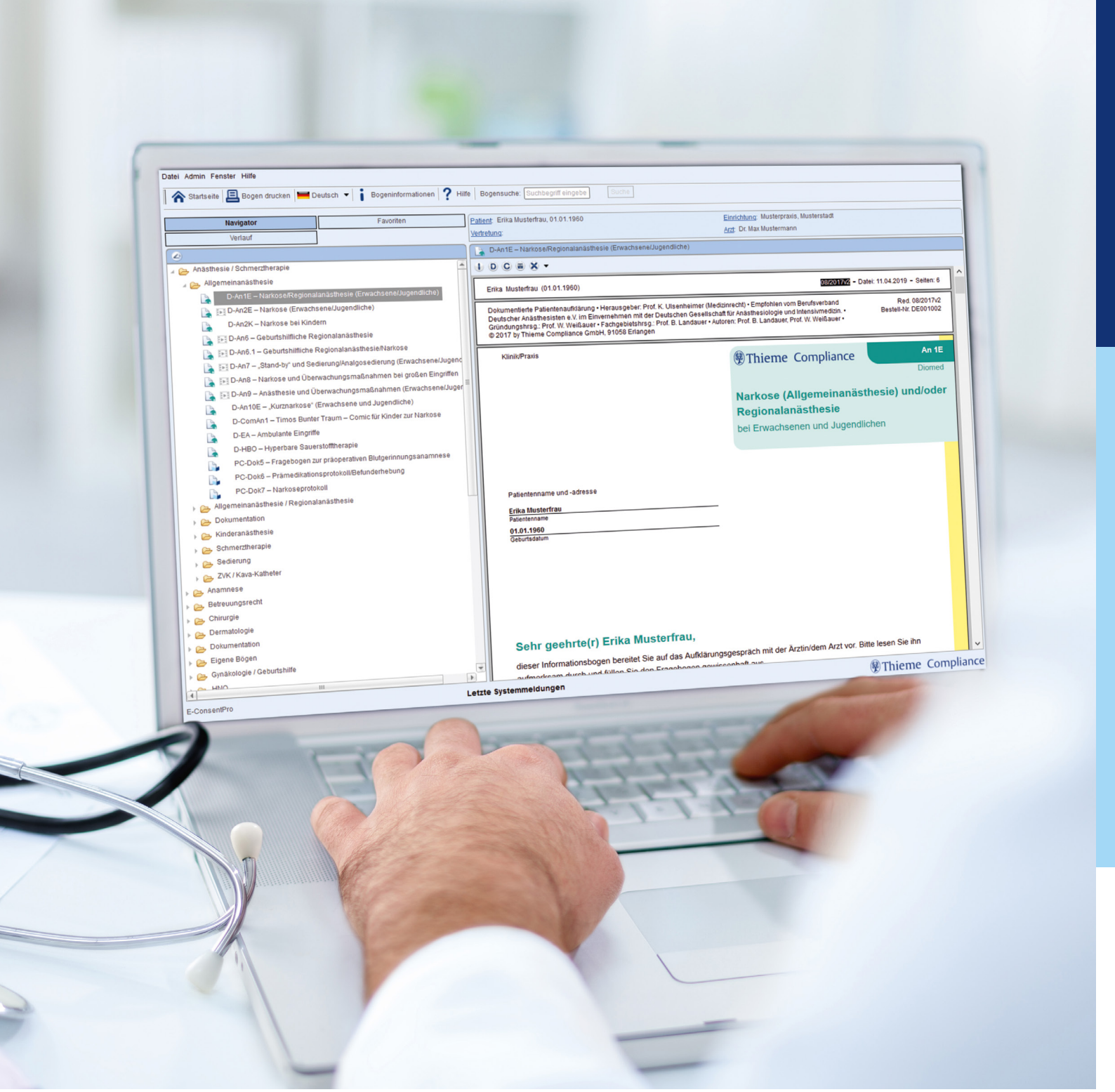

Umzugsanleitung 2.9

E-ConsentPro, E-ConsentPro mobile

Thieme Compliance

Inhalt

1 Über dieses Dokument

Diese Anleitung erklärt, wie Sie die Installation des E-ConsentPro-Grundmoduls ab Version 2.6 auf einen neuen Server umziehen oder eine Version 2.4 oder 2.5 beim Serverwechsel auf die neueste Version aktualisieren.

Darstellungsmittel

In diesem Dokument werden folgende Darstellungsmittel verwendet:

Darstellungsmittel	Bedeutung
Beispieltext	Hervorhebung von Elementen der Bedienoberfläche wie Schaltflächen, Fenster, Felder, o. ä.
`Beispieltext`	Namen von Dateien, Parametern, o. ä.
`Beispieltext`	Variable Nutzereingabe. Der Text ist durch konkrete Werte zu ersetzen.
1. Schritt	Handlungsanweisung mit mehreren Arbeitsschritten, in der angegebenen Reihenfolge auszuführen
‣ Schritt	Handlungsanweisung mit einem Arbeitsschritt
Resultat	Ergebnis einer Handlungsanweisung
Hinweis:	Tipps und zusätzliche Informationen
Achtung:	Warnungen vor Aktionen, die zu Datenverlust oder Fehlern führen können

Terminologie

In diesem Dokument werden folgende Begriffe verwendet:

Begriff	Bedeutung
Server	Rechner, auf dem E-ConsentPro installiert wird.
Client(s)	Alle Rechner (Arbeitsstationen), die lokal oder über das Netzwerk auf die E-ConsentPro-Installation zugreifen.
Hostname	Name eines Rechners im Netzwerk. Dies kann sowohl der Computername sein als auch ein Active Directory-Hostname (FQHN), z. B. server.mydomain.local.

2 Überblick über das Serverwechsel-Verfahren

Bei einem Serverwechsel ziehen Sie das E-ConsentPro-Grundmodul und alle Basiskomponenten (CouchDB-Datenbank, Apache Tomcat und Java) auf einen neuen Server um. Gegebenenfalls wird E-ConsentPro dabei auch auf die neue Version aktualisiert.

Ein Serverwechsel besteht aus folgenden Hauptschritten:

- Daten sichern
- E-ConsentPro auf dem neuen Server installieren mit Übernahme gewisser Sicherungsdaten
- Umgebung anpassen, z. B. Firewall, Schnittstellen
- Neues System testen

Hinweis:

Beachten Sie für die Wahl des neuen Servers folgende Hinweise:

- Falls Sie HTTPS verwenden wollen, klären Sie im Vorfeld, welches Zertifikat in Ihrem Netzwerk geeignet ist. Beachten Sie hierzu das Kapitel **Hinweise für die Verwendung von HTTPS** auf Seite 9.
- Stellen Sie sicher, dass dem Server eine feste IP-Adresse zugewiesen ist.
- Wir empfehlen, dass der Server für Bogenaktualisierung und Lizenzverlängerung Zugang zum Internet hat. Andernfalls müssen Sie diesen Vorgang regelmäßig manuell anstoßen.
- Passen Sie nach dem Serverwechsel den Aufruf von E-ConsentPro z. B. im Patientenverwaltungssystem entsprechend an.
- Bitte stellen Sie sicher, dass das von Ihnen verwendete Krankenhaus- oder Arztinformationssystem bei Nutzung des URL-Aufrufs UTF-8 encodierte URLs senden kann. Dies ist notwendig, da der verwendete Tomcat nur noch UTF-8 encodierte URLs verarbeitet. Sollte Ihr System keine UTF-8 encodierte URLs verarbeiten können, übernehmen wir keine Garantie für die volle Funktionalität und die korrekte Übernahme der Patientendaten.

3 Serverwechsel vorbereiten

Hinweis:
Zum Ausführen der nachfolgenden Schritte müssen Sie auf Betriebssystemebene des Servers als lokaler Administrator angemeldet sein.

Schritt 1 – Systemvoraussetzungen prüfen:

- Prüfen Sie die Systemvoraussetzungen.
  Die Systemvoraussetzungen sind in einem separaten Dokument zusammengestellt. Sie finden diese im Installationspaket und im Support-Bereich unserer Website:
  Downloadbereich E-ConsentPro
  - Prüfen Sie, ob auf dem neuen Server ausreichend Speicherplatz auf der Festplatte verfügbar ist und alle weiteren Systemvoraussetzungen erfüllt sind.
  - Prüfen Sie, ob die Clients (Arbeitsstationen), die auf den Server zugreifen, die Systemvoraussetzungen erfüllen.
  - E-ConsentPro mobile: Prüfen Sie, ob die Tablets weiterhin die Systemvoraussetzungen erfüllen.

Schritt 2 – Apps für die mobile Aufklärung aktualisieren:

- Wenn Sie E-ConsentPro mobile verwenden, prüfen Sie, ob eine aktuellere Version der Apps „Anamnese mobil“ und „Aufklärung mobil“ verfügbar ist, und installieren Sie diese.

Achtung:
Beim Update von Version 2.6.0 auf die Version 2.9.0 müssen Sie die Apps auf den Tablets erst deinstallieren und die neue Version aus dem App-Store herunterladen.
Beachten Sie, dass die Apps Version 2.9 nur mit der Software E-ConsentPro-Version 2.8.0 bzw. 2.9.0 kompatibel sind. Das Update Ihrer E-ConsentPro-Version muss zwingend parallel mit dem Austausch der Apps erfolgen.
Details zum Update von E-ConsentPro mobile finden Sie unter https://thieme-compliance.de/de/support/downloadbereich-econsentpro/information-e-consentpro-mobile/.

Schritt 3 – Installationsdateien bereitlegen:

1. Laden Sie die aktuellen Installationsdateien herunter. Diese finden Sie im Support-Bereich unserer Website:
   Downloadbereich E-ConsentPro
2. Legen Sie die Zip-Datei, die Sie heruntergeladen haben, auf dem Installationsserver ab. Extrahieren Sie die enthaltenen Dateien.

Schritt 4 – Wartungsfenster planen:

1. Planen Sie ein Wartungsfenster für den Serverwechsel ein.
2. Planen Sie ausreichend Zeit für die Übernahme individueller Einstellungen und für das Testen der Anwendung nach dem Update ein. Je nach Leistung Ihres Servers und Geschwindigkeit Ihrer Internetverbindung benötigen Sie zum Download des Softwareupdates und Durchführung der Bogenaktualisierung zwischen 20 Minuten und 2 Stunden, in Ausnahmefällen auch mehr.

4 Serverwechsel durchführen

Schritt 1 – Aufklärungsbögen online aktualisieren:

1. Öffnen Sie das aktuell installierte E-ConsentPro:
   `http://hostname_oder_ip:<HTTP Port>/ecp/ecp`
2. Melden Sie sich mit einem Administratorprofil an (Standard: `admin` ohne Kennwort).
3. Wählen Sie die Menüoption **Datei > Bogenaktualisierung**.
4. Lassen Sie die Option **Online (setzt Internetverbindung voraus)** aktiviert.

> **Hinweis:**
> Wenn die technischen Voraussetzungen für eine Online-Aktualisierung nicht gegeben sind: Brechen Sie die Bogenaktualisierung ab und fahren Sie mit **Schritt 2 – Anwendung für Nutzer sperren / Dienste stoppen** auf Seite 6 fort. Die technischen Voraussetzungen finden Sie in der E-ConsentPro-Online-Hilfe unter **Aktualisierung und Lizenz > Aufklärungsbögen aktualisieren**.

5. Klicken Sie auf **Weiter** und folgen Sie den Anweisungen des Assistenten.

   Ihre Lizenz wird geprüft und verlängert. Zudem werden Ihre Abrechnungsdaten übertragen sowie neue und geänderte Aufklärungsbögen heruntergeladen. Je nach Umfang kann dieser Vorgang längere Zeit in Anspruch nehmen.
6. Klicken Sie auf **Fertigstellen**.
7. Melden Sie sich mit der Menüoption **Datei > Abmelden** ab.

Schritt 2 – Anwendung für Nutzer sperren / Dienste stoppen:

1. Öffnen Sie die Windows Diensteverwaltung.
2. Stoppen Sie die Server-Dienste auf dem alten Server in folgender Reihenfolge:
   - **E-ConsentPro**
   - **E-ConsentPro Database**
3. Da das alte System nicht mehr verwendet wird, setzen Sie den Starttyp der Dienste auf **manuell**.

Schritt 3 – Datensicherung durchführen:

- Führen Sie die Datensicherung durch wie im Kapitel Datensicherung auf Seite 10 beschrieben.

Schritt 4 – Alte Installation entfernen:

- Entfernen Sie alte Installationen.

> **Achtung:**
> Erstellen Sie unbedingt eine Datensicherung gemäß Schritt 3, bevor Sie die alte Installation entfernen. Sonst sind Ihre bestehenden Daten und individuellen Einstellungen unwiederbringlich verloren.

Schritt 5 – Installation mit Datenübernahme vorbereiten:

1. Extrahieren Sie die Installationsdateien, falls noch nicht durchgeführt.
2. Legen Sie folgende Dateien aus Ihrer Sicherung (Schritt 3) neben die Setup-Datei:
   - `E-ConsentPro\ecp.config`
   - `E-ConsentPro\couchdb\var\lib\couchdb\accesscontrol.couch`
   - `E-ConsentPro\couchdb\var\lib\couchdb\ecp.couch`
   - `E-ConsentPro\couchdb\var\lib\couchdb\ecp_signature.couch`
   - `E-ConsentPro\couchdb\var\lib\couchdb\hl7_queue.couch`
   - `E-ConsentPro\couchdb\var\lib\couchdb\kis.couch`

Schritt 6 – E-ConsentPro auf dem neuen Server installieren:

1. Starten Sie die Installation mit Rechtsklick und **Als Administrator ausführen**.
2. Führen Sie die Installation aus.
3. Nur bei HTTPS: Prüfen Sie während der Installation im Fenster **E-ConsentPro Netzwerkkonfigurationen** die

Portnummern und passen Sie diese bei Bedarf an.

Beachten Sie außerdem das Kapitel **Hinweise für die Verwendung von HTTPS** auf Seite 9.

> **Achtung:**
> Vermeiden Sie Abweichungen bei Angaben im Installer zur bisherigen Installation (HTTP/HTTPS, verwendete Ports, usw.). Diese verursachen zusätzlichen Konfigurationsaufwand.
> Sollten Sie eine Patientenverwaltungssoftware mit Schnittstelle zu E-ConsentPro verwenden, kann dies zusätzliche (und mitunter kostenpflichtige) Anpassungen zur Folge haben.

4. Folgen Sie den Anweisungen des Installationsprogramms.

   Die Datenbanken des alten Systems sind damit im neu installierten System integriert. Alle Einstellungen, die Sie in E-ConsentPro vorgenommen haben, stehen Ihnen damit wieder zur Verfügung.

5. Stellen Sie vor weiteren Anpassungen sicher, dass die Migration der Datenbank abgeschlossen ist.

> **Hinweis:**
> Beim Start der neuen E-ConsentPro-Version wird geprüft, ob die Datenbank die nötigen Ergänzungen enthält. Fehlende Teile und Anpassungen werden mithilfe eines Migrationsjobs ergänzt.
> Die Dauer der Migration hängt davon ab, welche Version bisher verwendet wurde, wie groß die Datenbank ist und über welche Ressourcen Ihr Server verfügt.
> Während der Migration ist keine Anmeldung möglich. Es wird Ihnen auch kein Fortschrittsbalken angezeigt.
> Starten Sie E-ConsentPro nach 15 Minuten über den bekannten Link. Ist die Migration abgeschlossen, wird Ihnen das gewohnte Anmeldefenster angezeigt. Eventuell erscheint ein Hinweis, dass die Datenbank migriert wird. Wiederholen Sie in diesem Fall den Aufruf in regelmäßigen Abständen, bis das Anmeldefenster angezeigt wird.

> **Achtung:**
> Sollte auch nach zwei Stunden oder mehr keine Anmeldung möglich sein und wird dauerhaft die Meldung **Ihre Daten werden derzeit migriert** angezeigt, starten Sie den Dienst **E-ConsentPro Server** neu.

Schritt 7 – Weitere Anpassungen:

> **Achtung:**
> Im Folgenden sind Anpassungen erläutert, die zwingend nötig sind, sofern an der bisherigen Installation Änderungen durchgeführt wurden. Prüfen Sie diese Anpassung unbedingt, bevor Sie die Software den Anwendern zur Nutzung freigeben.

Falls Sie den Schnittstellenadapter nutzen:

1. Setzen Sie die Windows-Freigabe neu.
2. Konfigurieren Sie in den aufrufenden Systemen die neuen Einstiegspunkte.
3. Idealerweise haben Sie bisher auf einem Share gearbeitet und dieses auf den Anwender-PCs als Netzlaufwerk eingebunden. Dann empfehlen wir, den neuen Server und die Freigaben dort identisch anzulegen, da dies die Anpassung an jedem einzelnen Anwender-PC spart.

Falls Sie Skripte vom Hersteller Ihres Patientenverwaltungssystems verwenden:

- Passen Sie die Skripte an die neue Umgebung an.

Schritt 8 – Proxy-Einstellungen hinzufügen:

- Kontrollieren Sie, ob die Proxy-Einstellungen noch aktuell sind, falls Sie diese bisher verwendet haben.
  Die Vorgehensweise finden Sie im Kapitel **Proxy-Einstellungen ändern** auf Seite 12.

Schritt 9 – Aufklärungsbögen online aktualisieren:

1. Melden Sie sich in E-ConsentPro mit einem Administratorprofil an (Standard: `admin` ohne Kennwort).
2. Starten Sie die Bogenaktualisierung mit der Menüoption **Datei > Bogenaktualisierung** und der Option **Online (setzt Internetverbindung voraus)**.

Schritt 10 – Aufruf in der Patientenverwaltungssoftware prüfen:

1. Passen Sie gegebenenfalls den Aufruf von E-ConsentPro an, wenn Sie die Anwendung über Ihr KIS, PVS oder AIS

starten, (z. B. beim Wechsel auf einen anderen Port).

2. Teilen Sie den Nutzern gegebenenfalls die neue URL mit, wenn die Nutzer E-ConsentPro direkt im Web-Browser aufrufen.
3. Prüfen Sie, ob die Parameter zur URL in der Datei `adapter.ini` mit denen Ihres gewünschten Aufrufs übereinstimmen (HTTP oder HTTPS), wenn Sie den Aufruf über eine GDT- oder VDDS-Schnittstelle mit dem E-ConsentPro-Adapter auslösen. Wenn nicht, können Sie die alte funktionierende Konfiguration aus der gesicherten Datei `adapter_<timestamp>.ini` manuell übernehmen. Beide Dateien finden Sie im Installationsverzeichnis von E-ConsentPro `\E-ConsentPro\adapter`.
4. Passen Sie an jedem Client lokal die Datei `VDDS_MMI.ini` an, wenn Sie die VDDS-Schnittstelle verwenden.

> **Hinweis:**
> Details zur Schnittstellenkonfiguration finden Sie in der separaten Schnittstellenbeschreibung unter https://thieme-compliance.de/de/support/.

Schritt 11 – Anwendung testen:

- Prüfen Sie die häufig genutzten Funktionen der Anwendung wie Bogendruck und Bogenzuweisung. Prüfen Sie, ob alle Bogenindividualisierungen vorhanden sind. Prüfen Sie hierzu auch Ihre individuellen Einstellungen in der **Zugriffsverwaltung** und unter **Globale Einstellungen**.

5 Hinweise für die Verwendung von HTTPS

Mit einer HTTPS-Verbindung werden die übermittelten Daten verschlüsselt übertragen. Besonderes Augenmerk sollten Sie darauf richten, wenn Sie personenbezogene Daten wie Patientendaten in E-ConsentPro eingeben und standortübergreifend ohne ein VPN über das Internet versenden.

Dies setzt voraus, dass dem Client das benötigte Zertifikat bekannt ist und diesem vertraut wird. Ansonsten erhält der Nutzer zunächst eine Sicherheitsabfrage und müsste das Zertifikat selbst importieren. Standard-Nutzern fehlen hierzu oft die entsprechenden Rechte und Kenntnisse. Eine detaillierte Anleitung finden Sie im Support-Bereich unserer Website:

https://thieme-compliance.de/de/support/downloadbereich-econsentpro/

6 Datensicherung

Dieses Kapitel enthält eine Anleitung, welche Daten und Einstellungen Ihres bestehenden Systems gesichert werden müssen und wie Sie dabei vorgehen.

Vorbereitung

Bevor Sie Daten und Einstellungen sichern, stoppen Sie die Dienste des bestehenden Systems. So können die Dateien sicher kopiert werden und befinden sich nicht im Zugriff.

So stoppen Sie die Dienste:

1. Öffnen Sie die Windows Diensteverwaltung.
2. Stoppen Sie folgende Dienste:
   - zuerst den Dienst **E-ConsentPro**
   - anschließend den Datenbank-Dienst **E-ConsentPro Database**

Nun können Sie Sicherungskopien der unten aufgeführten Datenbank- und Konfigurationsdateien erstellen.

Installationsordner

Der Installationsordner liegt z. B. unter `C:\E-ConsentPro`. Er enthält alle Einstellungen und Daten wie Datenbank, Tomcat, Java, usw.

Diese Vorgehensweise stellt sicher, dass alle Daten von E-ConsentPro gesichert sind. Zur Wiederherstellung werden nur wenige spezielle Dateien benötigt.

So sichern Sie die Installationsdateien:

- Erstellen Sie regelmäßig Sicherungen mindestens folgender Dateien:
  - `E-ConsentPro\couchdb\var\lib\couchdb\accesscontrol.couch`
  - `E-ConsentPro\couchdb\var\lib\couchdb\ecp.couch`
  - `E-ConsentPro\couchdb\var\lib\couchdb\ecp_signature.couch`
  - `E-ConsentPro\couchdb\var\lib\couchdb\hl7_queue.couch`
  - `E-ConsentPro\couchdb\var\lib\couchdb\kis.couch`
  - `E-ConsentPro\ecp.config`
  - `E-ConsentPro\adapter\adapter.ini`
  - `E-ConsentPro\adapter\config.ini`
  - `E-ConsentPro\tomcat\conf\Ihre_Keystore_Datei.xml`
    Die Sicherung dieser Datei ist nur bei der Verwendung von HTTPS mit eigener `keystore`-Datei erforderlich. Ausführliche Informationen hierzu finden Sie in einer eigenen HTTPS-Anleitung (Zum Download im Support-Bereich von Thieme Compliance).

> **Hinweis:**
> Legen Sie die Sicherungskopie außerhalb des Installationsordners ab, im Idealfall auf einem speziellen Backup-Laufwerk

So sichern Sie die Dateien im PDF/A-Exportverzeichnis

- Sichern Sie zusätzlich für E-ConsentPro mobil das PDF/A-Exportverzeichnis, z. B. `\\SERVER\E-ConsentPro\PDFA`
  Das Exportverzeichnis enthält alle digital zu archivierenden Aufklärungsbögen und Protokolldateien.

> **Hinweis:**
> Das exakte Verzeichnis für Ihre Installation ermitteln Sie in E-ConsentPro unter **Admin > Zugriffsverwaltung >** Mandanten auswählen > Reiter **Digitaler Workflow**.
> Beachten Sie, dass Sie pro Mandant ein separates Verzeichnis angeben können und eventuell mehrere Verzeichnisse sichern müssen.

Netzwerkdrucker

Wenn Sie Netzwerkdrucker einsetzen, müssen diese auf dem neuen Server wieder eingerichtet werden. Eine Anleitung finden Sie in der Online-Hilfe zu E-ConsentPro.

So sichern Sie Ihre Proxy-Einstellungen:

1. Starten Sie das Programm **Monitor E-ConsentPro** auf dem Rechner, auf dem E-ConsentPro installiert ist, und öffnen dort den Reiter **Java**.
2. Kopieren Sie Ihre Proxy-Einstellungen aus dem Bereich **Java Options** und speichern Sie diese in einer Textdatei, z. B.

```
-Dhttps.proxyHost=Hostname_Ihres_Proxy-Servers
-Dhttps.proxyPort=Port_Ihres_Proxy-Servers
-Dhttps.nonProxyHosts=localhost|127.0.0.1|Weitere_Hosts
[-Dhttps.proxyUserName=[myDomain/]myProxyUsername]
[-Dhttps.proxyPassword=Kennwort]
```

7 Proxy-Einstellungen ändern

E-ConsentPro ermöglicht es Ihnen, die Aufklärungsbögen online – d. h. über das Internet – zu aktualisieren. Dazu verbindet sich E-ConsentPro mit folgender Adresse:

`https://ecp-update-prod.thieme.de:443`

Wenn Sie einen Proxy-Server verwenden, um diese Adresse zu erreichen, müssen Sie diesen in den Java-Einstellungen von E-ConsentPro Server angeben.

Hinweis:
Zum Ausführen der nachfolgenden Schritte müssen Sie auf Betriebssystemebene als lokaler Administrator angemeldet sein.

So ändern Sie die Proxy-Einstellungen:

1. Starten Sie das Programm **Monitor E-ConsentPro** auf dem Server, auf dem E-ConsentPro installiert ist und öffnen dort den Reiter **Java**.
2. Fügen Sie im Feld **Java Options** folgende Zeilen hinzu, ohne bestehende Einträge zu überschreiben. Angaben in eckigen Klammern [ ] sind optional.

```
-Dhttps.proxyHost=Hostname_Ihres_Proxy-Servers
-Dhttps.proxyPort=Port_Ihres_Proxy-Servers
-Dhttps.nonProxyHosts=localhost|127.0.0.1|Weitere_Hosts
[-Dhttps.proxyUserName=[myDomain/]myProxyUsername]
[-Dhttps.proxyPassword=Kennwort]
```

Achtung:
Übernehmen Sie die exakte Schreibweise der Angaben.

Weitere Informationen:

- `-Dhttps.nonProxyHosts`
  Liste der Rechner, die **nicht** über den Proxy-Server kontaktiert werden sollen. In der Regel sind dies die Rechner Ihres lokalen Netzwerks.

  Der Parameter muss mindestens die Angaben `localhost` und `127.0.0.1` enthalten. Sie können die IP-Adressen oder Hostnamen weiterer Rechner des lokalen Netzwerks angeben.

  Die einzelnen Angaben werden mit einem Verkettungszeichen | voneinander getrennt. Zwischen den Angaben dürfen keine Leerzeichen stehen.
- `-Dhttps.proxyUserName, -Dhttps.proxyPassword`
  Diese Parameter sind notwendig, wenn der Proxy-Server eine Authentifizierung erfordert.

  Wenn Sie eine NTLM2-Authentifizierung verwenden, geben Sie die Domäne vor dem Nutzernamen an: `Domäne/Proxy_Nutzername`. Ansonsten entfällt die Angabe der Domäne.

Achtung:
Einstellungen für **http** können zu Problemen führen. Tragen Sie deshalb ausschließlich die in Ihrer Netzwerkumgebung benötigten Einstellungen für **https** ein.

3. Klicken Sie auf **Übernehmen**.
4. Starten Sie in der Windows Diensteverwaltung den Dienst **E-ConsentPro Server** neu, damit die neuen Einstellungen übernommen werden.

Hinweis:
E-ConsentPro bezieht seine Aktualisierungsdaten von einem zertifikatsgesicherten Aktualisierungsserver. Das Zertifikat des Aktualisierungsservers wird beim Import der Lizenzdatei in E-ConsentPro importiert.

Die Adresse des Aktualisierungsservers lautet:

`https://ecp-update-prod.thieme.de`

Ein direkter Aufruf dieser URL ist wegen eines fehlenden Client-Zertifikats nicht möglich und ermöglicht somit keine Überprüfung, ob der Aktualisierungsserver erreichbar ist.

8 Verwendete Ports

Im Folgenden geben wir Ihnen einen Überblick, welche Ports E-ConsentPro standardmäßig verwendet.

Um den Zugriff auf die Anwendung über das Netzwerk zu erlauben, sind Ausnahmeregeln in der Firewall nötig. Es ist ausreichend, **eingehende Regeln** für die nötigen Ports zu definieren.

Protokoll	Port	Verwendung	Beschreibung
TCP	8082	HTTP Connector Port	HTTP-Kommunikation zwischen Clients und E-ConsentPro-Server
TCP	8445	HTTP Connector Port	HTTPS-Kommunikation zwischen Clients und E-ConsentPro-Server
TCP	5984	CouchDB	Kommunikation zwischen E-Consent-Pro-Server und Datenbank

Hinweis:

Es hat sich herausgestellt, dass der Standardport 8082 von Virenscannern der Hersteller Trend Micro oder Panda verwendet wird. Sollten Sie diese einsetzen, verwenden Sie einen anderen Port. Bewährt haben sich z. B. 8083 oder 8085.

Sie können auch die Standardports für HTTP (TCP 80) und HTTPS (TCP 443) konfigurieren, sofern diese von Ihrem Server nicht verwendet werden.

Online-Aktualisierung der Aufklärungsbögen

Bei der Online-Aktualisierung der Aufklärungsbögen kommuniziert Ihre E-ConsentPro-Installation über Port 443 mit unserem Aktualisierungsserver `ecp-update-prod.thieme.de`.

9 Kontakt

Unser technischer Support und Kundenservice sind gerne für Sie da:

Montag bis Donnerstag: 08:00 – 16:30 Uhr
Freitag: 08:00 – 15:00 Uhr

Technischer Support

Bei technischen Fragen steht Ihnen unser Support gerne zur Verfügung:
Tel.: +49 9131 93406-40
Fax: +49 9131 93406-74
E-Mail: support@thieme-compliance.de

Kundenservice

Bei Fragen zum Vertrag oder Ihrer Lizenz wenden Sie sich gerne an unseren Kundenservice:
Tel.: +49 9131 93406-40
Fax: +49 9131 93406-70
E-Mail: service@thieme-compliance.de

Stand: Februar 2020

Thieme Compliance GmbH
Am Weichselgarten 30a
91058 Erlangen

www.thieme-compliance.de

Thieme Compliance