

# Signavio Process Manager Administratorenhandbuch

12.3.3





# Inhalt

1	Erfahrungsprofil der Administratoren	4
2	Systemlandschaft und Komponenten	5
2.1	Systemlandschaft	5
2.2	Softwarekomponenten	6
3	Installation	9
3.1	Systemvoraussetzungen	9
3.2	Das Betriebssystem konfigurieren (Webserver und Datenbankserver)	11
3.3	Das Netzwerk konfigurieren	11
3.4	Java installieren (Webserver)	12
3.5	Den Webserver konfigurieren	12
3.6	Den Datenbankserver konfigurieren	15
3.7	JDBC-Treiber installieren	18
3.8	Den Signavio Process Manager installieren	19
3.9	Den Signavio Process Manager konfigurieren	20
3.10	Konfigurationsfehler mithilfe des Diagnostics-Tools beheben	22
3.11	Nutzer registrieren	22
3.12	HTTP Basic Authentifizierung konfigurieren	23
3.13	Konfiguration des SAP Solution Manager Konnektors (optional)	24
3.14	Die GitHub-Integration für RedHat JBoss BRMS-Projekte konfigurieren (optional)	28
3.15	Den Collaboration Hub mit Active Directory-Anbindung konfigurieren (optional)	29
3.16	Die Signavio Collaboration Hub SharePoint-Komponente konfigurieren (optional)	33
3.17	Freigabe-Workflow mit Signavio Workflow Accelerator konfigurieren (optional)	35
3.18	Den Signavio Simulationsserver konfigurieren (optional)	35
3.19	Apache Solr Server konfigurieren (optional)	36
3.20	Imageserver konfigurieren (optional)	37
3.21	Den Mailing-Server konfigurieren (optional)	37
3.22	HTTPS verwenden (optional)	38
3.23	Installation in einem Tomcat Cluster (optional)	41
3.24	Manuelle Funktionstests durchführen	42
4	Betriebsanleitung	44
4.1	Als Nutzer auf den Signavio Process Manager zugreifen	44
4.2	Datenbackups durchführen	44
4.3	Typische Störfälle	45
4.4	Den Server warten	46
4.5	Monitoring	46
4.6	Das Datenbank- oder Betriebssystem aktualisieren	47
4.7	Den Server auf neue Hardware umziehen	47
5	Updateanleitung für den Signavio Process Manager	48
6	Die Lizenzdatei austauschen	50
7	Den Signavio Process Manager als Nutzer konfigurieren	51



## 8 Support

52

Dieses Dokument erläutert die Installation und den Betrieb des Signavio Process Managers in der On-Premise-Version.



## Kapitel 1

# Erfahrungsprofil der Administratoren

Wie jede Software ist auch der Signavio Process Manager von externen Softwarekomponenten abhängig. Die Installationsanleitung setzt Vorkenntnisse in den abhängigen Technologien voraus. Die Administratoren, die mit der Installation und dem Betrieb des Signavio Process Managers beauftragt werden, müssen Erfahrung mit den folgenden Technologien haben:

- Dem verwendeten Betriebssystem
- Dem verwendeten Datenbanksystem
- Oracle Java
- Apache Tomcat
- Der Anbindung eines Emailservers
- Wenn HTTPS verwendet wird, SSL/HTTPS
- Wenn verwendet, der Anbindung eines Microsoft Active Directory
- Wenn verwendet, der Installation und Konfiguration eines Microsoft SharePoint Webparts

---

### **Wichtig: Hinweis für Kunden der Signavio Small Business Edition**

Die Signavio Small Business Edition (verfügbar bis Frühjahr 2013) wurde zur Vereinfachung der Installation mit einem vorkonfigurierten VMware Image ausgeliefert. Der Betrieb und die Wartung der virtuellen Maschine obliegt allerdings in der Verantwortung des Kunden. Durch die Weiterentwicklung des Signavio Process Managers sind auch die Hardwareanforderungen gestiegen. Aus diesem Grund erfüllt das vorkonfigurierte VMware Image nicht mehr die Mindestanforderungen für den Betrieb des Signavio Process Managers ab der Version 8.3.0. Wenn Sie das vorkonfigurierte VMware Image im Einsatz haben und auf die Version 8.3.0 oder höher aktualisieren möchten, dann migrieren Sie bitte zuvor den Signavio Process Manager auf eine wie in diesem Handbuch beschriebene Systemlandschaft.

---



## Kapitel 2

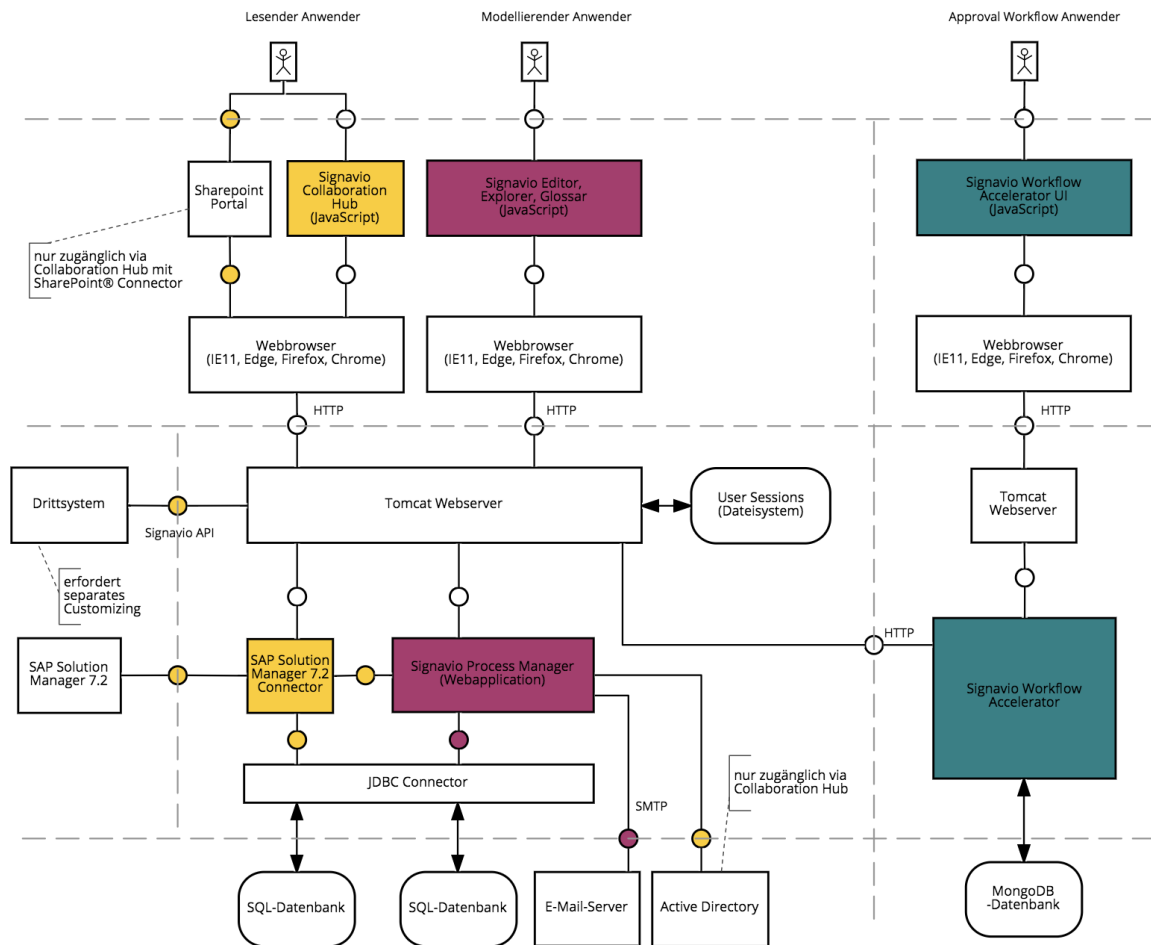
# Systemlandschaft und Komponenten

Dieses Kapitel erklärt die typische Systemlandschaft für den Process Manager und beschreibt kurz die Software-Komponenten.

### 2.1 Systemlandschaft

Das folgende Diagramm zeigt die typische Systemlandschaft für den Signavio Process Manager und enthält eine Übersicht über alle Softwarekomponenten.

Sämtliche rot dargestellten Systemkomponenten sind im Standardlieferumfang der Software enthalten. Die gelb eingefärbten Komponenten oder Schnittstellen sind aufpreispflichtig und durch Signavio separat zu beziehen. Die grün eingefärbten Komponenten sind für Kunden der Enterprise Edition erforderlich, wenn die **Freigabeworkflow-Funktion** verwendet werden soll.



Übersicht über die Systemlandschaft

## 2.2 Softwarekomponenten

### 2.2.1 Signavio Collaboration Hub (JavaScript)

Das Frontend läuft per JavaScript vollständig im Browser. Die Komponente erlaubt Lesezugriff auf freigegebene Prozesse. Der Collaboration Hub kann an ein Active Directory gekoppelt werden, gegen das sämtliche Lesezugriffe auf die Prozesse geprüft werden (mittels Single-Sign-On). Damit ist es möglich, feingranular die Rollen/Rechte für den Lesezugriff zu konfigurieren.

Der Signavio Collaboration Hub unterstützt alle gängigen Browser (siehe: <https://www.signavio.com/browser-compatibility/>).

### 2.2.2 Signavio Process Manager (Webanwendung)

Das Frontend wird als JavaScript ausgeführt und kann komplett über einen Browser aufgerufen werden.

Die Anmeldung eines Nutzers erfolgt über die Eingabe einer E-Mailadresse und einem selbstgewählten Passwort.



### 2.2.3 Signavio Process Manager (Webanwendung)

Die Backend-Logik läuft als Java-Applikation in der Tomcat-Umgebung.

### 2.2.4 JDBC-Schnittstelle

Der Zugriff auf das Datenbanksystem geschieht mittels JDBC. Passende Adapter für die unterstützten Datenbanken müssen von den entsprechenden Herstellerseiten heruntergeladen werden (siehe Kapitel 3.7 JDBC Treiber installieren).

### 2.2.5 Browser

Nutzer rufen die Applikation über Ihren Browser auf. Die unterstützten Browser entnehmen Sie bitte den Systemvoraussetzungen.

Das Signavio-Frontend setzt eine performante JavaScript-Engine voraus und läuft daher nicht im Microsoft Internet Explorer 11 oder älteren Versionen.

### 2.2.6 Apache Tomcat

Der Applikationsserver stellt die Laufzeitumgebung für das Java-Backend dar. Unterstützte Tomcat-Versionen entnehmen Sie bitte den Systemvoraussetzungen. Für die Nutzer-Sessions verwendet der Signavio Process Manager den Session-Mechanismus des Tomcat. Diese Sessions werden im Dateisystem des Servers gehalten. Selbst wenn der Tomcat heruntergefahren wird, sind die Nutzer-Sessions nach dem erneuten Hochfahren noch vorhanden und für den Nutzer ist nicht ersichtlich, dass der Server zwischenzeitlich nicht verfügbar war.

Weiterhin wird für eine Modellierung im Frontend keine ständige Verbindung zum Backend benötigt (außer beispielsweise für Lade- und Speichervorgänge sowie Glossar-Lookups). Das Backend kann also prinzipiell heruntergefahren werden während Anwender modellieren. Diese verbringen die meiste Zeit in der Modellierungsoberfläche. Wird für die Phase des heruntergefahrenen Tomcat Servers nicht versucht, das Diagramm abzuspeichern und ist der Tomcat zeitnah wieder erreichbar, merkt der modellierende Endanwender nichts. Der Collaboration Hub ist während des heruntergefahrenen Tomcat Servers nicht erreichbar.

Für die Verbindung zwischen Browser und Tomcat kommt wahlweise HTTP oder HTTPS (SSL) zum Einsatz.

### 2.2.7 Mailserver (SMTP)

Als Mailserver können Sie einen beliebigen SMTP-fähigen E-Mailserver verwenden.

### 2.2.8 Datenbanksystem

Die Datenbank enthält sämtliche Nutzerdaten des Signavio Process Managers. Sämtliche Daten werden im UTF-8 Zeichensatz abgelegt. Unterstützte Datenbanken entnehmen Sie bitte den Systemvoraussetzungen.



### 2.2.9 Active Directory

Für die Verwendung des Collaboration Hub wird ein Active Directory (AD) angekoppelt. Die im AD hinterlegten Nutzer/Nutzergruppen sind ausschließlich für die Steuerung des lesenden Zugriffs im Collaboration Hub verwendbar. Die Modellierungsnutzer sind nach wie vor vom AD entkoppelt und werden innerhalb des Signavio Process Managers verwaltet.

---

**Wichtig:** Falls Sie **Kerberos** als Authentifizierungsprotokoll verwenden, muss der Server des Signavio Process Managers zur Kopplung an das AD unter Microsoft Windows 64Bit installiert werden und zu der Domäne gehören, auf dessen Active Directory zugegriffen werden soll.

---

### 2.2.10 SharePoint Portal

Signavio bietet optional ein SharePoint-Webpart in Form eines WSP-Packages an. Dieses bietet eine nahtlose Frontend-Integration für den Lesezugriff in das SharePoint-Portal. Das Look-and-Feel des Signavio Collaboration Hubs lässt sich direkt im Webpart komfortabel anpassen.

### 2.2.11 Drittsystem

Beliebige Drittsysteme (wie zum Beispiel ein Ticket-Tracking System) können über eine REST-API eingebunden werden. API-Lizenzen müssen zusätzlich bezogen werden.

### 2.2.12 Signavio Workflow Accelerator

Signavio Workflow Accelerator ist ein Workflow-Automatisierungssystem, das für die Verwendung der Funktion „Freigabe-Workflow“ vorausgesetzt wird. Signavio Workflow Accelerator wird für Kunden mit einer zusätzlich kostenpflichtigen Lizenz zur Verfügung gestellt. Das Backend ist eine Java-Webanwendung, die auf einem separaten Server installiert werden muss. Signavio Workflow Accelerator verwendet Oracle Java 8, Apache Tomcat 7 oder 8 und als Datenbank MongoDB 3.4 oder 3.6. Näheres zu den Systemvoraussetzungen entnehmen Sie bitte dem separaten Administratorenhandbuch für Signavio Workflow Accelerator unter <https://docs.signavio.com/adminguide/workflow/de/>.

### 2.2.13 Signavio Workflow Accelerator UI

Mit einem Browser wird auf die Benutzerschnittstelle von Signavio Workflow Accelerator zugegriffen.





## Kapitel 3

# Installation

Dieses Kapitel beschreibt die Installation des Signavio Process Managers. Voraussetzung für die Installation ist, dass Sie über die Installationsdateien des Signavio Process Managers als ZIP-Archiv sowie Ihre Lizenzdatei verfügen.

---

**Bemerkung:** In den Installationsanweisungen wird der Begriff `$ TOMCAT_DIR` in Kommandozeilenanweisungen verwendet, um den Pfad zur Apache Tomcat-Instanz anzugeben. Diese Instanz sollte auf das Verzeichnis über den Verzeichnissen `bin` und `webapps` verweisen, auf dem die Signavio Process Manager-Webanwendung läuft. Setzen Sie eine entsprechende Umgebungsvariable, um die Befehle nach dem Kopieren und Einfügen sofort ausführen zu können.

---

### 3.1 Systemvoraussetzungen

Der Signavio Process Manager ist eine Client-Server-Anwendung, die aus mindestens zwei Servern besteht: Einem **Datenbankserver** und einem **Webserver**. Beide Server können auf derselben Maschine ausgeführt werden.

#### 3.1.1 Hardware-Mindestvoraussetzung für den Webserver

Sie benötigen die folgende Hardware, um den Webserver des Signavio Process Manager auszuführen:

- Mindestens 2 CPU-Kerne (Virtualisierung ist möglich)
- 64Bit Unterstützung
- 4 GB RAM (dediziert für den Applikationsserver verfügbar)
- 20 GB Festplattenspeicher

#### 3.1.2 Hardware-Mindestvoraussetzung für den Datenbankserver

Sie benötigen die folgende Hardware, um den Datenbankserver von Signavio Process Manager auszuführen:

- Mindestens 2 CPU-Kerne (Virtualisierung ist möglich)
- 64Bit Unterstützung
- 4 GB RAM (dediziert für die Datenbank verfügbar)



- 30 GB Festplattenspeicher (ausreichend für ca. 20000 Diagramm-Revisionen bei der Verwendung einer MySQL-Datenbank)

Sie können den Webserver und den Datenbankserver auf einem logischen Server zusammen betreiben. In diesem Fall akkumulieren sich die Hardware-Mindestvoraussetzungen entsprechend.

Rechnen Sie bei der Nutzung einer Oracle Datenbank bezüglich des Festplattenspeicherverbrauchs mit einem zusätzlichen Faktor 1,5 pro Diagramm. Für 20000 Diagrammrevisionen müssen Sie also 45GB einplanen.

### 3.1.3 Software-Voraussetzungen für den Webserver

Sie benötigen die folgende Software, um den Webserver des Signavio Process Manager auszuführen:

- Betriebssystem:
  - Debian Stable Release 64Bit
  - Microsoft Windows 64-Bit
- Oracle Java8 (64Bit)
- Apache Tomcat 8.5.x

64Bit ist Voraussetzung, um der Java VM mehr als 1,5 GB Heap Space zuweisen zu können.

Zudem ist es notwendig, dass Sie den Signavio Process Manager mit einen E-Mail-Server verbinden. Stellen Sie hierfür sicher, dass der E-Mail-Server für den Signavio Process Manager erreichbar ist und richten Sie ein E-Mail-Konto für den Process Manager ein.

---

**Bemerkung:** Wenn Sie den Collaboration Hub erworben haben und Kerberos-Authentifizierung für Single-Sign-On verwenden möchten, müssen Sie den Webserver zur Anbindung an Ihr Active Directory auf einem Microsoft Windows 64Bit Server installieren.

---

### 3.1.4 Software-Voraussetzungen für den Datenbankserver

Sie benötigen die folgende Software, um den Datenbankserver des Signavio Process Manager auszuführen:

- Betriebssystem:
  - Debian Stable Release 64Bit
  - Microsoft Windows 64Bit
- Database:
  - Empfohlen: MySQL Standard Edition 5.x (InnoDB Storage Engine):  
oder  
MySQL Enterprise Edition 5.x (InnoDB Storage Engine)
  - Oracle 11g
  - Oracle 12
  - MS SQL Server 2008
  - MS SQL Server 2012
  - MS SQL Server 2014
  - MS SQL Server 2016



### 3.1.5 Mindestanforderungen an den Client (Hardware)

- Processor: 2,00 GHz oder mehr
- 4 GB RAM
- 1 GB freier Festplattenspeicher

### 3.1.6 Software-Voraussetzungen für den Client

- Betriebssystem:
  - Microsoft Windows
  - Mac OS X
  - Linux
- Browser
  - Microsoft Edge
  - Microsoft Internet Explorer 11
  - Mozilla Firefox ab Version 52
  - Apple Safari ab Version 10
  - Google Chrome ab Version 50

### 3.1.7 Systemvoraussetzungen für Signavio Workflow Accelerator (optional)

Sie müssen einen Signavio Workflow Accelerator-Server einrichten, um die **Freigabe-Workflow**-Funktion der Enterprise Edition nutzen zu können. Signavio Workflow Accelerator muss auf einem separaten Server installiert werden. Weitere Informationen zu Anforderungen und Installationsprozess finden Sie im [Workflow Accelerator Administratorenhandbuch](#)<sup>1</sup>.

## 3.2 Das Betriebssystem konfigurieren (Webserver und Datenbankserver)

Wenn Sie eine Linux-Distribution verwenden, stellen Sie sicher, dass Ihr Betriebssystem die Kodierung UTF-8 als Standardkodierung benutzt. Bitte schlagen Sie im Benutzerhandbuch Ihres Betriebssystems nach, wie Sie die Kodierung einstellen müssen.

## 3.3 Das Netzwerk konfigurieren

Sie können für Ihr Signavio System in Ihrem Netzwerk einen DNS-Eintrag anlegen. Stellen Sie sicher, dass die IP-Adresse oder der DNS-Eintrag in der Konfiguration des Signavio Process Managers eingestellt ist.

<sup>1</sup> <https://docs.signavio.com/adminguide/workflow/en/>



## 3.4 Java installieren (Webserver)

Installieren Sie eine Java JRE in der 64 Bit-Variante.

Laden Sie das Installationspaket über den folgenden Link herunter:

<https://www.java.com/de/download/>

---

**Wichtig:** Beachten Sie die Versionsnummer. Signavio Process Manager unterstützt momentan noch kein Java 9.

---

## 3.5 Den Webserver konfigurieren

### 3.5.1 Apache Tomcat installieren

Sie können die Installationsdateien für den Apache Tomcat unter der folgenden URL herunterladen:

<https://tomcat.apache.org/download-80.cgi>

---

**Bemerkung:**

**Das Apache Tomcat Team gab bekannt, dass die Unterstützung für Apache Tomcat 8.0.x am 30. Juni 2018 beendet**

Daher unterstützt Signavio ausschließlich die Tomcat-Version 8.5.x.

---

Außerdem bieten einige Paketverwaltungen von Linux-Distributionen die einfache Installation vom Apache Tomcat an. Wenn Sie ein Debian Betriebssystem ab der Version 6.0 nutzen, können Sie das Advanced Packaging Tool (APT) für die Installation verwenden. Nutzen Sie den folgenden Befehl:

```
apt-get install tomcat8
```

Für Windows bietet Ihnen Apache den Windows Service Installer an (Downloadpaket 32-bit/64-bit Windows Service Installer).

Dieser ermöglicht es Ihnen, den Apache Tomcat über einen Installations-Assistenten zu installieren und direkt als Dienst auf Ihrem Windows-Server einzurichten.

---

**Bemerkung:** Nach der Installation von Tomcat, wird dieser bei jedem Serverstart automatisch gestartet.

---

Achten Sie bei der Installation darauf, dass Sie das Installationsprogramm mit Administratorrechten ausführen.

---

**Wichtig:** Bitte stellen Sie sicher, dass der Systemnutzer, welcher den Apache Tomcat ausführt, über Lese-/Schreibrechte auf den Ordner `$TOMCAT_DIR/webapps` und deren Unterordner verfügt.

---

Für Windows empfehlen wir, den Apache Tomcat direkt unter `C:\` zu installieren. Das stellt sicher, dass der ausführende Nutzer später Lese-/Schreibzugriff auf die entsprechenden Ordner hat.

### 3.5.2 Apache Tomcat konfigurieren

Weisen Sie dem Apache Tomcat so viel Arbeitsspeicher wie möglich zu. Wir empfehlen, mindestens 4096 MB RAM zuzuweisen.



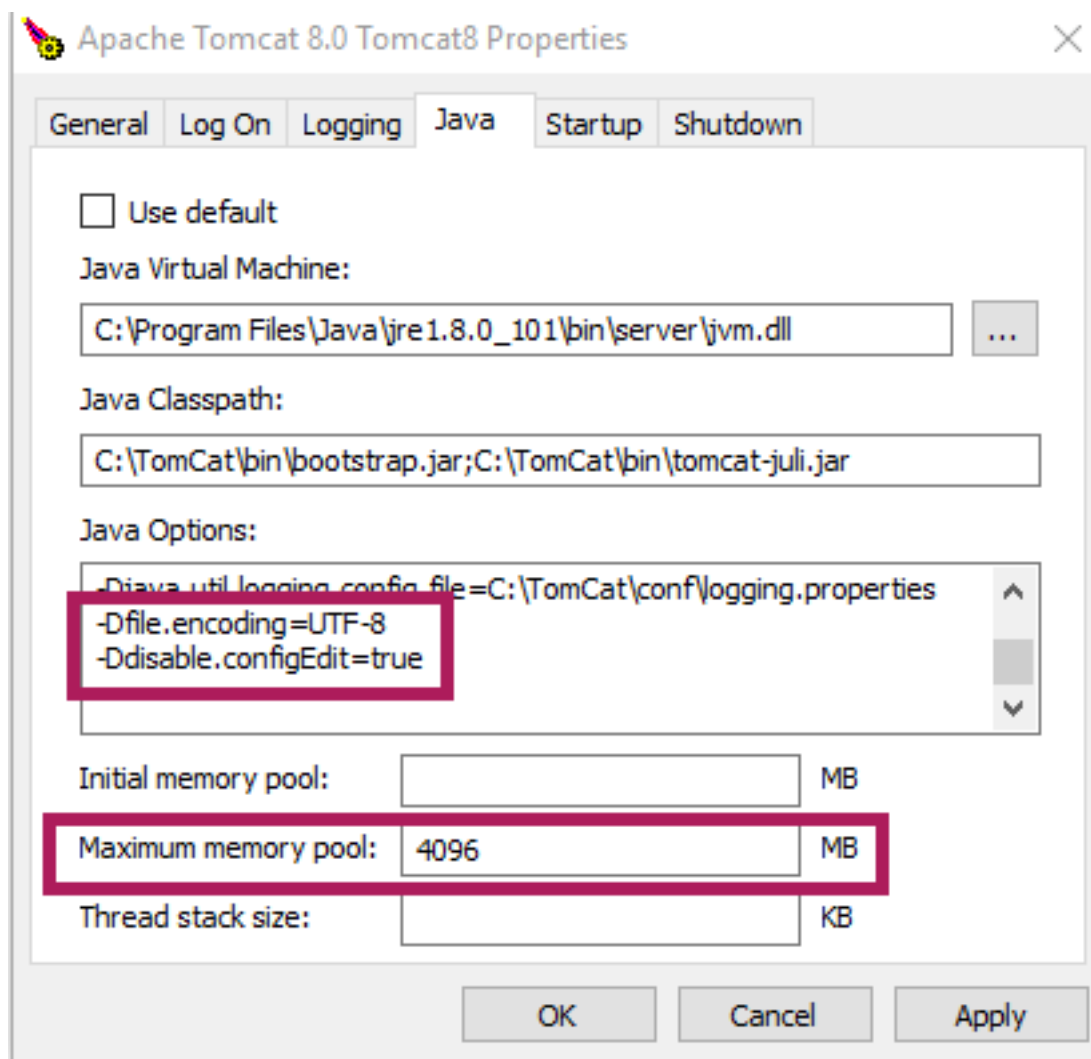
Konfigurieren Sie hierzu die JVM Variable `Xmx` (zum Beispiel `-Xmx4096m`). Wenn Sie auf einem Windows System den Installer von Apache Tomcat verwenden, dann können Sie JVM-Variablen im Konfigurationsdialog von Apache Tomcat angeben.

Stellen Sie sicher, dass Apache Tomcat UTF-8 als default encoding verwendet und *configuration editing* deaktiviert hat. Setzen Sie die JVM-Variable `Dfile.encoding` auf UTF-8 und `-Ddisable.configEdit` auf true:

```
-Dfile.encoding=UTF-8  
-Ddisable.configEdit=true
```

Falls Sie **Windows** verwenden, öffnen Sie hierzu im Windows-Startmenü **Programme - Apache Tomcat X - Configure Tomcat**.

Wechseln Sie in das **Java**-Tab und geben Sie die folgenden Werte an:



#### Apache Tomcat konfigurieren

**Unter Linux** erstellen Sie die Umgebungsvariable `JAVA_OPTS` mit dem folgenden Wert, indem Sie den folgenden Befehl ausführen:

```
export JAVA_OPTS="$JAVA_OPTS -Xmx4096m -Dfile.encoding=UTF-8 -Ddisable.configEdit=true"
```

Für alle Betriebssysteme: Stellen Sie sicher, dass die XML-Datei `$TOMCAT_DIR/conf/web.xml` UTF-8-codiert ist oder ändern Sie die Einstellungen gegebenenfalls.



Die erste Zeile der XML-Datei muss wie folgt aussehen:

```
<?xml version="1.0" encoding="UTF-8"?>
```

Fügen Sie außerdem in der Datei \$TOMCAT\_DIR/conf/server.xml dem HTTP/1.1-Konnektor das Attribut `URIEncoding=ÜTF-8` hinzu.

Für eine Verringerung der zu übertragenden Daten sollten Sie außerdem die automatische Komprimierung von Daten aktivieren.

Fügen Sie die folgenden Attribute zum Connector-Element hinzu:

```
compressableMimeType="
    text/css,text/plain,
    image/svg+xml,
    application/xhtml+xml,
    text/html,
    text/xml,
    text/javascript,
    application/xml,
    application/x-javascript,
    application/javascript"

compression="on"

compressionMinSize="2048"
```

Im HTTP/1.1-Konnektor geben Sie außerdem den Port an, den der Apache Tomcat nutzen soll (Attribut `port`). Der voreingestellte Standardport ist 8080. Wenn Sie verhindern möchten, dass die Nutzer des Signavio Process Managers den Port in die Adresszeile des Browsers eingeben müssen (zum Beispiel `http://signavio.ihrUnternehmen.com:8080`), dann ändern Sie den Port auf 80.

Um Diagramme zu unterstützen, die eine Größe von 2 MB (reines text-basiertes Datenformat) überschreiten, fügen Sie die folgende Zeile zur Konnektoren-Definition hinzu:

```
maxPostSize="33554432"
```

**Beispiel** eines vollständig konfigurierten Konnektors:

```
<Connector port="80" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443"
    URIEncoding="UTF-8"
    compressableMimeType="
        text/css,text/plain,
        image/svg+xml,
        application/xhtml+xml,
        text/html,
        text/xml,
        text/javascript,
        application/xml,
        application/x-javascript,
        application/javascript"
    compression="on"
    compressionMinSize="2048"
maxPostSize="33554432"
/>
```

---

#### Bemerkung:

- Der Signavio Process Manager benutzt das spezielle webapps Verzeichnis ROOT. Dies kann zu Problemen führen, wenn Sie weitere Anwendungen auf demselben Tomcat-Server betreiben. Daher raten wir davon ab, den Tomcat-Server für weitere Anwendungen zu benutzen.



- Wenn Sie HTTPS verwenden wollen, stellen Sie sicher, dass das Zertifikat von einer vertrauenswürdigen Certificate Authority (CA) ausgestellt wurde und, dass die JVM, mit dem der Apache Tomcat ausgeführt wird, dem Zertifikat vertraut. Weitere Informationen zur Verwendung von HTTPS entnehmen Sie dem Abschnitt *HTTPS verwenden (optional)* (Seite 38).
- Wenn Sie mehrere Konnektoren verwenden, wenden Sie die korrekten Einstellungen auf alle Anschlüsse an.
- Wenn Sie den Tomcat-Server mittels des AJP-Konnektors in ein System integrieren möchten, stellen Sie sicher, dass die Codierung des AJP-Konnektors auf UTF-8 eingestellt ist.

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" URIEncoding="UTF-8" />
```

## 3.6 Den Datenbankserver konfigurieren

**Wichtig:** Die Installation eines Datenbanksystems sollte von einem Datenbank-Administrator durchgeführt werden, da hierfür in der Regel Expertenwissen erforderlich ist. Die Installation und Konfiguration der verschiedenen Datenbanksysteme unterscheidet sich sehr stark und wird hier nicht näher erläutert.

Im folgenden Abschnitt wird beschrieben, wie Sie den Datenbankserver konfigurieren.

**Hinweis:** Falls Sie keine spezifischen Anforderungen bezüglich des Datenbanksystems haben, empfehlen wir Ihnen die Verwendung von MySQL Standard Edition 5.x (InnoDB Storage Engine) oder MySQL Enterprise Edition 5.x (InnoDB Storage Engine).

Wichtig ist, dass das Datenbanksystem **Transaktionen** unterstützt.

Wenn Sie in Ihrem Unternehmen ein Datenbank-Cluster betreiben, können Sie auch in dem Cluster eine Datenbank für den Signavio Process Manager anlegen.

Sie müssen für den Signavio Process Manager in Ihrer Datenbank einen Nutzer anlegen.

Der Datenbanknutzer muss innerhalb der Signavio Datenbank neben den Standard-SQL-Befehlen SELECT, UPDATE, INSERT und DELETE auch die Befehle `edit` und `delete tables` und `views` sowie `indexes` ausführen sowie, `locks` setzen können.

Routines (gespeicherte Prozeduren) werden nicht vom Signavio Process Manager-Konto erstellt. Darüber hinaus ändert das System keine Kontoeinstellungen von Datenbanknutzern.

Um das *Diagnostics-Tool für Systemadministratoren* (Seite 22) verwenden zu können, muss Ihr Datenbanknutzer zudem Sichten erstellen können. Dies können Sie mit dem folgenden Befehl sicherstellen (alle unterstützen Datenbanksysteme):

```
GRANT CREATE VIEW ON <db_schema> TO <dbuser>
```

, wobei <dbuser> für Ihren Datenbanknutzer und <db\_schema> für den Namen des Datenbankschemas steht.

Zudem ist es für die Verwendung des Diagnostic-Tools notwendig, die folgenden Berechtigungen auf Metadatentabellen zu erteilen:

### Oracle

```
GRANT SELECT ON user_tab_columns TO <dbuser>
GRANT SELECT ON user_tables TO <dbuser>
GRANT SELECT ON user_ind_columns TO <dbuser>
```



```
GRANT SELECT ON user_constraints TO <dbuser>
GRANT SELECT ON user_cons_columns TO <dbuser>
```

## MySQL

```
GRANT SELECT ON information_schema.columns TO <dbuser>
GRANT SELECT ON information_schema.tables TO <dbuser>
GRANT SELECT ON information_schema.statistics TO <dbuser>
GRANT SELECT ON information_schema.table_constraints TO <dbuser>
GRANT SELECT ON information_schema.key_column_usage TO <dbuser>
```

## SQL-Server

```
GRANT SELECT ON information_schema.columns TO <dbuser>
GRANT SELECT ON sys.dm_db_partition_stats TO <dbuser>
GRANT SELECT ON sys.objects TO <dbuser>
GRANT SELECT ON sys.indexes TO <dbuser>
GRANT SELECT ON sys.index_columns TO <dbuser>
GRANT SELECT ON sys.foreign_keys TO <dbuser>
GRANT SELECT ON sys.foreign_key_columns TO <dbuser>
```

, wobei <dbuser> für Ihren Datenbanknutzer steht.

Die Kommunikation zwischen dem Signavio Process Manager und dem Datenbankserver erfolgt über einen JDBC-Treiber. Stellen Sie sicher, dass die Datenbank über das Netzwerk vom Server des Signavio Process Managers aus erreichbar ist.

**Hinweis:** Für die Konfiguration der Datenbankanbindung benötigen Sie eine JDBC-URL für Ihre Datenbank. Bitte erfragen Sie die JDBC-URL bei dem zuständigen Datenbankadministrator.

### 3.6.1 MySQL konfigurieren

**Wichtig:** Nur beim Einsatz einer MySQL Datenbank erforderlich

Stellen Sie sicher, dass die MySQL Datenbank standardmäßig die InnoDB Storage Engine und UTF-8 als Kodierung nutzt. Die InnoDB Storage Engine ist die einzige Storage Engine im Lieferumfang von MySQL, die Transaktionen unterstützt. Setzen Sie außerdem die maximale Paketgröße auf 16 MB.

**Hinweis:** Wir empfehlen Ihnen, die MySQL Workbench zu installieren. Die Administration des MySQL-Servers ist damit viel einfacher.

Konfigurieren Sie bitte die folgenden Variablen in der MySQL-Konfigurationsdatei (`my.ini` bzw. `my.cnf`). Die Datei sollte sich in dem entsprechenden Programmverzeichnis befinden (zum Beispiel `C:\ProgramData\MySQL\MySQL Server 5.5` unter Windows und `/etc/mysql` unter Debian-basierten Linux-Distributionen).

Wenn Sie **MySQL bis einschließlich Version 5.5.2** einsetzen, verwenden Sie die folgende Konfiguration:

```
[mysqld]

max_allowed_packet=16M

default-character-set=utf8

default-collation=utf8_general_ci
```





```
default-storage-engine=innodb  
  
max_connections=160
```

Wenn Sie **MySQL ab der Version 5.5.3** einsetzen, verwenden Sie die folgende Konfiguration:

```
[mysql]  
  
default-character-set=utf8  
  
[mysqld]  
  
max_allowed_packet=16M  
  
character-set-server=utf8  
  
collation-server=utf8_general_ci  
  
default-storage-engine=INNODB  
  
max_connections=160  
  
query_cache_limit = 32M  
  
query_cache_size = 128M  
  
query_cache_type = 1
```

Erstellen Sie ein leeres Datenbankschema für den Signavio Process Manager.

**Hinweis:** Bitte achten Sie darauf dass bei der manuellen Anpassung der Konfigurationsdatei die einzutragenden Variablen bereits vorhanden sein können. Stellen Sie in diesem Fall sicher dass unterhalb der manuell hinzugefügten Variablen keine Duplikate mit anderen Werten vorhanden sind. Kommentieren Sie diese gegebenenfalls mit dem Zeichen # am Zeilenbeginn aus.

**Hinweis:** Sollten Sie die entsprechenden Konfigurationsdateien nicht finden, können diese Attribute auch komplett innerhalb der MySQL Workbench angepasst werden.

### 3.6.2 Microsoft SQL-Server konfigurieren

**Wichtig:** Nur bei Einsatz einer Microsoft SQL-Server-Datenbank erforderlich

Wenn Sie den MSSQL-Server nicht über ein Microsoft Windows-Betriebssystem bereitstellen, stellen Sie sicher, dass das Hostsystem UTF-8-Codierung unterstützt.

Aktivieren Sie außerdem das Protokoll TCP/IP für Ihre Datenbankinstanz. Starten Sie hierzu das Programm **SQL Server Configuration Manager** und wählen Sie in der Liste **SQL Server-Netzwerkkonfiguration - Protokolle für 'INSTANZNAME'** aus. Aktivieren Sie das TCP/IP-Protokoll. Starten Sie den SQL-Server nach der Aktivierung neu.

Legen Sie einen Datenbanknutzer an, der die SQL-Server-Authentifizierung nutzt. Den hier eingestellten Nutzernamen und das Passwort müssen Sie später in der Konfiguration des Signavio Process Managers hinterlegen. Stellen Sie sicher, dass in den Sicherheitseinstellungen des Microsoft SQL-Servers die Option **SQL Server- und Windows Authentifizierungsmodus** aktiviert ist.



Erstellen Sie eine leere Datenbank für den Signavio Process Manager und weisen Sie dem Datenbanknutzer für die Datenbank die **Mitgliedschaft** db\_owner zu. Stellen Sie für den Datenbanknutzer als **Standardschema** dbo ein. Konfigurieren Sie als *Collation* der Datenbank Latin1\_General\_CI\_AS.

### 3.6.3 Oracle Datenbanksystem konfigurieren

---

**Wichtig:** Nur bei Einsatz einer Oracle Datenbank erforderlich

---

Stellen Sie sicher, dass die Datenbank UTF-8 als Codierung nutzt und legen Sie eine leere Datenbank für den Signavio Process Manager an.

Unter Linux finden Sie die Konfigurationsdatei standardmäßig in der Datei `oracle/network/admin/sqlnet.ora`.

## 3.7 JDBC-Treiber installieren

Damit der Signavio Process Manager Ihre Datenbank verwenden kann, ist der für Ihr Datenbanksystem kompatible JDBC-Treiber im Apache Tomcat zu hinterlegen. Hierfür müssen Sie den JDBC-Treiber von der Herstellerseite Ihres Datenbanksystems herunterladen. Bitte beachten Sie die Lizenzbestimmungen des Herstellers zur Verwendung des JDBC-Treibers.

---

**Hinweis:** Achten Sie darauf, genau die in den folgenden Abschnitten beschriebene Version des JDBC-Treibers zu installieren. Die Verwendung einer anderen als der hier beschriebenen Version kann zu unerwartetem Verhalten der Anwendung führen.

Nachdem Sie den JDBC-Treiber erfolgreich heruntergeladen haben, kopieren Sie die Jar-Bibliothek des JDBC-Treibers in den im Tomcat-Installationsverzeichnis (im Weiteren mit `$TOMCAT_DIR` bezeichnet) befindlichen Ordner **`$TOMCAT_DIR/lib`**.

---

### 3.7.1 Den JDBC-Treiber für MySQL herunterladen

Laden Sie den MySQL-Connector/JDBC-Treiber in der **Version 5.1.45** über einen der folgenden Links herunter:

**Linux:**

<http://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-java-5.1.45.tar.gz>

**Windows:**

<http://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-java-5.1.45.zip>

Alternativ, navigieren Sie in Ihrem Browser zur Downloadseite des MySQL-Connectors/JDBC-Treibers:

<http://dev.mysql.com/downloads/connector/j/>

Bitte achten Sie hier auf die Auswahl der Version 5.1.45 und wählen Sie als Plattform **Platform Independent** aus.

Entpacken Sie das Archiv in ein Verzeichnis Ihrer Wahl. Der JDBC-Treiber ist die im Archiv enthaltene Datei `mysql-connector-java-5.1.45-bin.jar`.



### 3.7.2 Den JDBC-Treiber für Microsoft-SQL-Server-Datenbanken herunterladen

Laden Sie den Microsoft JDBC-Driver in der **Version 6.0** von der Downloadseite von Microsoft herunter:

<https://www.microsoft.com/download/details.aspx?id=11774>

Klicken Sie auf **Herunterladen** und wählen Sie die entsprechende Datei aus (Windows: sqljdbc\_6.0.8112.100\_enu.exe, Linux: sqljdbc\_6.0.8112.100\_enu.tar.gz). Klicken Sie auf **Next**. Entpacken Sie den Treiber unter einem Pfad Ihrer Wahl. Der richtige JDBC-Treiber ist die Datei `enu\jre8\sqljdbc42.jar` im `$TOMCAT_DIR/libs`-Ordner.

### 3.7.3 Den JDBC-Treiber für Oracle Datenbanken herunterladen

Für den Download des JDBC-Treibers ist ein Account für `oracle.com` notwendig. Dieser Account steht Ihnen als Kunde von Oracle zur Verfügung. Unabhängig von der von Ihnen eingesetzten Oracle-Datenbankversion, laden Sie bitte den Oracle-Database-JDBC-Driver in der Version 12.1.0.1 von der Oracle-Downloadseite herunter:

<http://www.oracle.com/technetwork/database/features/jdbc/jdbc-drivers-12c-download-1958347.html>

Lesen und akzeptieren Sie zunächst die Lizenzbedingungen von Oracle (OTN Development and Distribution License Agreement). Laden Sie bitte die Dateien `ojdbc7.jar` und `orai18n.jar` herunter. Falls Sie sich noch nicht auf `oracle.com` angemeldet sind, werden Sie vor dem Download gebeten, sich anzumelden. Der JDBC-Treiber besteht aus den beiden Dateien `ojdbc7.jar` und `orai18n.jar`.

Der JDBC-Treiber besteht aus den beiden Dateien `ojdbc7.jar` und `orai18n.jar`.

**Bemerkung:** In neueren Tomcat-Versionen ist der JAR-Scan standardmäßig aktiviert. Er scannt Manifeste von Bibliotheken und protokolliert fehlende Abhängigkeiten zu `stdout` \*. *Fehlende Abhängigkeiten des Oracle-Treibers können ignoriert werden, um die Protokolldatei sauber zu halten. Schließen Sie "orai18n" und gdk\_custom.jar aus dem JAR-Scan aus, indem Sie `$TOMCAT_DIR/conf/catalina.properties` modifizieren.*

```
tomcat.util.scan.StandardJarScanFilter.jarsToSkip=\
orai18n-*,\
gdk_custom.jar,\
```

## 3.8 Den Signavio Process Manager installieren

Die Installation der Programmdateien des Signavio Process Managers erfolgt in wenigen Schritten.

1. Im Installationsverzeichnis des Tomcats (im Weiteren mit `$TOMCAT_DIR` bezeichnet) finden Sie das Verzeichnis `webapps`. In diesem Verzeichnis müssen die Programmdateien der Webanwendungen liegen, die von dem Apache Tomcat-Server ausgeführt werden sollen. Es wird davon ausgegangen, dass Sie eine Erstinstallation des Signavio Process Managers auf einem neu installierten Apache Tomcat durchführen, der keine weiteren Webanwendungen ausführt.
2. Stoppen Sie den Apache Tomcat (falls dieser ausgeführt wird).
3. Löschen Sie alle Dateien im Verzeichnis `$TOMCAT_DIR/webapps`.
4. Löschen Sie das Verzeichnis `$TOMCAT_DIR/conf/Catalina` (falls vorhanden).
5. Löschen Sie das Verzeichnis `$TOMCAT_DIR/work/Catalina` (falls vorhanden).
6. Entpacken Sie das ZIP-Archiv mit den Installationsdateien.



7. Kopieren Sie den gesamten Inhalt des in den Installationsdateien enthaltenen Verzeichnisses `files` in das Verzeichnis `$TOMCAT_DIR/webapps`. Beachten Sie, **nur den Inhalt des Verzeichnisses** zu kopieren, nicht das Verzeichnis selbst.

## 3.9 Den Signavio Process Manager konfigurieren

Bevor Sie die Anwendung starten, ist es notwendig, den Signavio Anwendungsserver zu konfigurieren. Die ZIP-Datei enthält die Konfigurationsvorlage `configuration.xml`. Legen Sie diese Datei zusammen mit der Lizenzdatei des Signavio Process Manager `configuration_signed.xml` und der Datei `simulation.xml` im Verzeichnis ```$TOMCAT_DIR/conf` ab. `$TOMCAT_DIR` steht hierbei für das Root-Verzeichnis der Tomcat-Instanz.

Passen Sie nun die folgenden Konfigurationsoptionen in der Datei `configuration.xml` an:

- **Server**

Die URL unter dem der Ziel-Server erreichbar ist. Es darf nicht mit / (Slash) enden.

Format: `http(s)://<DNS-Eintrag oder IP-Adresse>(<port>)`

Beispiele: `http://signavio.mycompany.com`, `http://159.234.37.47:8080`

- **defaultLanguageCode**

Die Standardsprache des Systems. Diese Einstellung ist nur für Systeme wichtig, die den Collaboration Hub (Gastnutzerzugang) nutzen. Mögliche Werte sind:

- `de` (Deutsch)
- `en` (Englisch)
- `es` (Spanisch)
- `fr` (Französisch)
- `ja` (Japanisch)
- `ko` (Koreanisch)
- `nl` (Niederländisch)
- `ru` (Russisch)
- `zh` (Chinesisch)

- **externalconfigurationpath**

Absoluter Pfad zu einem existierenden Ordner auf dem Ziel-Server, auf den der Systemnutzer Schreibrechte besitzt, der den Tomcat-Server ausführt. Der Pfad sollte außerhalb des `webapps`-Ordners liegen, da der Inhalt des `webapps`-Ordners bei einem Update des Signavio Process Managers gelöscht wird. Dieser Ordner enthält gegebenenfalls zur Laufzeit Dateien, die zwischengespeichert werden. Der Inhalt dieses Ordners muss nicht gesichert werden.

- **Datenbankkonfiguration:**

In der Vorlage der Konfigurationsdatei finden Sie bereits Vorgaben für die Anbindung einer MySQL, Oracle und MS SQL Server Datenbank. Nutzen Sie bitte diese Vorgaben und passen Sie sie entsprechend an.

- `driverClass`: Java-Klassenname des JDBC-Treibers.

Mögliche Werte sind:

- **MySQL**: `com.mysql.jdbc.Driver`
- **Oracle 11, 12**: `oracle.jdbc.driver.OracleDriver`
- **MS SQL Server**: `com.microsoft.sqlserver.jdbc.SQLServerDriver`



- url: Die URL des Datenbanksystems

Beispiele:

- \* **MySQL:** jdbc:mysql://localhost/platform
- \* **MS SQL Server:** jdbc:sqlserver://localhost;databaseName=signavio;

- username: Benutzername des Datenbanknutzers.
- password: Passwort des Datenbanknutzers.
- dialect: Hibernate-spezifischer SQL-Dialekt.

Mögliche Werte sind:

- \* **MySQL:** org.hibernate.dialect.MySQL5InnoDBDialect
- \* **Oracle:** org.hibernate.dialect.Oracle10gDialect
- \* **MS SQL Server:**  
com.signavio.hibernate.dialect.CustomSQLServerDialect

#### • E-Mail-Server Konfiguration:

Konfigurieren Sie den E-Mail-Server, der Systemmails wie Benachrichtigungen und Registrierungs-E-Mails verschickt.

- SMTP\_HOST\_NAME: Hostname des E-Mail-Servers
- SMTP\_EMAIL: Absender-E-Mail-Adresse für ausgehende E-Mails
- SMTP\_AUTH\_USER: Benutzername des zu benutzenden E-Mail-Kontos
- SMTP\_AUTH\_PWD: Passwort des zu benutzenden E-Mail-Kontos
- SMTP\_PORT: Port des E-Mail-Servers
- SMTP\_SECURE: Nutzung von TLS/SSL. Mögliche Werte: true oder false

#### • Support E-Mail-Adresse (optional):

An diese Adresse werden die aus dem Signavio Process Manager gesendeten Supportanfragen geschickt. Bitte tragen Sie die entsprechende E-Mail-Adresse Ihres Ansprechpartners ein. z. B.: `<supportMailAddress>support@signavio.com</supportMailAddress>`.

#### • Maximale Diagrammanzahl für Reports einstellen (optional):

Fügen Sie die folgende Zeile hinzu:

```
<maxDiagramCount>500</maxDiagramCount>
```

In diesem Beispiel wird der Wert auf maximal 500 Diagramme angehoben. Der Standardwert ist 250.

Fügen Sie zudem im selben Verzeichnis in der Datei `context.xml` innerhalb des `<Context>`-Tags die folgenden Zeilen ein:

```
<Parameter name="configfile" value="${catalina.base}/conf/configuration.xml" />
<Parameter name="licensefile" value="${catalina.base}/conf/configuration_signed.xml"
/>
<Parameter name="configfile.simulation" value="${catalina.base}/conf/simulation.xml"
/>
```

**Bemerkung:** Der Pfad, unter dem die Konfigurationsdateien abgelegt werden, hat sich mit Version 9.7.0 geändert. Folgen Sie den Anweisungen unter *Schritt 6 im Update-Kapitel* (Seite 48), um die Dateien entsprechend zu verschieben.



Überprüfen Sie, ob der Systemnutzer, der den Tomcat ausführt, Zugriff auf die soeben kopierten Dateien hat. Falls dies nicht der Fall ist, passen Sie die entsprechenden Berechtigungen an.

### Starten Sie nun den Tomcat-Server.

Sie können den Signavio Process Manager nun unter dem hinterlegten DNS-Eintrag oder der IP-Adresse über einen Browser erreichen (z. B. <http://signavio.ihrunternehmen.de>).

Falls Sie zu einem späteren Zeitpunkt Änderungen an der Konfiguration vornehmen, müssen Sie den Tomcat-Server neu starten, um die Änderungen anzuwenden.

**Hinweis:** Kunden der On-Premise-Edition erhalten vor Ablauf der aktuellen Lizenz automatisch eine neue Lizenzdatei welche rechtzeitig ausgetauscht werden muss.

## 3.10 Konfigurationsfehler mithilfe des Diagnostics-Tools beheben

Rufen Sie die URL `<baseURL>/diagnostics` auf (z. B.: <https://mycompanysignavio.de:8080/diagnostics>), um zu überprüfen, ob der Tomcat ohne Fehler gestartet werden konnte.

Es öffnet sich das folgende Fenster:

Test Status	Test Name	Details	Advice
✓	Read Configuration File		
✗	Software installation size	The folder S:\tomcat8-second\webapps\images does not exist.	Please copy all files from SignavioEnterprise\files into your empty <tomcat>\webapps\ folder. ⓘ
✓	Java Version		

### Das Diagnostics-Tool nutzen

Klicken Sie auf **Run Diagnostics Test**. Das Tool überprüft nun automatisch die Logeinträge. Falls Fehler auftreten, werden Ihnen Problembeschreibungen und detaillierte Lösungsansätze angezeigt.

Falls Sie verhindern wollen, dass beliebige Nutzer die Diagnostics-Ergebnisse einsehen können, folgen Sie den Anweisungen im Kapitel *HTTP Basic Authentifizierung konfigurieren*.

Ersetzen Sie in den Code-Snippets `diagnostics` mit `register`, beziehungsweise fügen Sie anstelle von `<url-pattern>/p/register/*</url-pattern>` `<url-pattern>/diagnostics/*</url-pattern>` ein.

## 3.11 Nutzer registrieren

Um einen Nutzer zu registrieren, öffnen Sie bitte die folgende URL in Ihrem Browser:

<http://<IP-Adresse oder DNS des Systems>/p/register>

Füllen Sie das Formular aus und klicken Sie auf **Registrieren**. Wiederholen Sie den Vorgang für jeden weiteren zu registrierenden Nutzer. Nutzer loggen sich ein, indem sie ihre E-Mail-Adresse und ein persönlich gewähltes Passwort eingeben.



**Hinweis:** Die E-Mail-Adresse eines Nutzers ist der eindeutige Bezeichner für einen Nutzer. Ein nachträgliches Ändern der E-Mail-Adresse ist nicht möglich.

Der erste Nutzer, der sich auf dem System registriert, wird automatisch der speziellen Nutzergruppe **Administratoren** hinzugefügt. Alle weiteren Nutzer werden nicht automatisch dieser Nutzergruppe hinzugefügt. Nutzer, die der Gruppe **Administratoren** angehören, haben erweiterte Rechte, wie das Verwalten von Nutzergruppen oder das Anlegen von Modellierungsrichtlinien. Dadurch kann der erste Nutzer weitere Nutzer zur der Nutzergruppe **Administratoren** hinzufügen.

## 3.12 HTTP Basic Authentifizierung konfigurieren

Um zu verhindern, dass unautorisierte Personen über den Link `http://<IP-Adresse oder DNS des Systems>/p/register` einen Nutzer registrieren, können Sie das Aufrufen dieser URL durch eine **HTTP Basic Authentifizierung** schützen.

Öffnen Sie hierzu die Datei `$TOMCAT_DIR/conf/web.xml` in einem Texteditor und fügen Sie die folgenden Zeilen am Ende der Datei, aber vor dem schließenden XML-Tag `</web-app>` ein:

```
<security-role>

    <role-name>register</role-name>

</security-role>

<security-constraint>

    <display-name>
        Security constraint for the user registration page
    </display-name>

    <web-resource-collection>

        <web-resource-name>
            Protected Area
        </web-resource-name>

        <url-pattern>
            /p/register/*
        </url-pattern>

    </web-resource-collection>

    <auth-constraint>

        <role-name>
            register
        </role-name>

    </auth-constraint>

</security-constraint>

<login-config>

    <auth-method>
        BASIC
    </auth-method>

    <realm-name>
```



```

        Register
      </realm-name>
</login-config>

```

Sie haben nun konfiguriert, dass nur Tomcat-Nutzer mit der Rolle `register` Zugriff auf die Ressource `/p/register` bekommen.

Sie müssen jedoch noch die Rolle `register` definieren sowie einen Nutzer anlegen und dem Nutzer diese Rolle zuweisen.

Öffnen Sie hierzu die Datei `$TOMCAT_DIR/conf/tomcat-users.xml` in einem Texteditor und ersetzen Sie den Inhalt der Datei mit den folgenden Zeilen:

```

<?xml version="1.0" encoding="UTF-8"?>

<tomcat-users>

    <role rolename="register"/>

    <user username="signavio" password="signavio" roles="register"/>

</tomcat-users>

```

Diese Zeilen definieren die Rolle `register` und erstellen einen Nutzer mit dem Nutzernamen `signavio` und dem Passwort `signavio`, dem die Rolle `register` zugeordnet wurde.

Ändern Sie bitte die Attribute `username` und `password` und geben Sie diese Informationen nur an autorisierte Personen weiter, die neue Nutzer in Ihrem System anlegen dürfen.

### 3.13 Konfiguration des SAP Solution Manager Konnektors (optional)

Um den SAP Solution Manager 7.2 (SolMan) Konnektor zu verwenden, müssen Sie zuerst Apache Tomcat und Signavio Process Manager installieren. Anweisungen dazu finden Sie im Kapitel *Installation* (Seite 9).

**Bemerkung:** Sie müssen den Konnektor auf einem anderen Datenbankschema ausführen, als dem Datenbankschema, welches Sie für Signavio Process Manager verwenden.

#### 3.13.1 Installieren des Konnektors

Um den SAP Solution Manager Konnektor zu installieren, benötigen Sie zwei Dateien: `solman72.yml` und `configuration.xml`. Die Datei `solman72.yml` wird verwendet, um den SAP Solution Manager Konnektor zu konfigurieren, während `configuration.xml` die Datei ist, die zum Konfigurieren von Signavio Process Manager verwendet wird. Beide sind in der .zip-Datei enthalten, die mit der On-Premise-Edition von Signavio Process Manager geliefert wird.

Kopieren Sie zuerst die `solman72.yml`-Datei in den Tomcat `conf`-Ordner. Öffnen Sie die Datei `solman72.yml` und suchen Sie folgenden Abschnitt:

```

signavio:
  client:
    # the shared secret for communication between Signavio Process Manager and solman72-service
    # must be the same as the <sharedJwtSecret> in configuration.xml
    sharedJwtSecret: SHARED_SECRET_CHANGE_ME
  platform:
    # the URL of the Signavio Process Manager
    # must be the same as the <server> in configuration.xml without a slash at the end

```





```
url: http://localhost:8080
resource:
  userInfoUri: ${signavio.platform.url}/p/solman72ConnectorUserinfo
  # maximum level of nested directories to read on an export
  maxRecursionLevel: 20
```

So konfigurieren Sie die einzelnen Parameter:

- **sharedJwtSecret:** Hier müssen Sie den Schlüssel (geteilter Schlüssel) festlegen. Dieser muss in den Dateien `solman72.yml` und `configuration.xml` identisch sein.
- **platform:** Die URL des Servers, auf dem Sie Signavio Process Manager ausführen. Sie können diese URL benennen, wie Sie möchten, aber sie muss dem Parameter `<server>` in der Datei `configuration.xml` entsprechen.
- **userInfoUri:** Verwendet die gleiche Definition wie der Plattformparameter. Diese Definition müssen Sie nicht ändern.
- **username:** Benutzername für das Datenbankbenutzerkonto.
- **password:** Passwort für das Datenbankbenutzerkonto.
- **URL:** Die URL der Datenbank, die Sie für den Solution Manager Konnektor verwenden. Stellen Sie sicher, dass es sich von `configuration.xml` unterscheidet.
- **driverClassName:** Der Name des Treibers, der für Ihre Datenbank verwendet wird. Dies ist derselbe wie der `driverClass`-Parameter, der beim Einrichten des Signavio Process Managers verwendet wird.
- **database encryption secret:** Setzen Sie diesen Parameter auf einen geheimen und komplexen Wert. Dieser Wert wird verwendet, um das gespeicherte Passwort des Solution Manager Nutzers zu verschlüsseln, welches anschließend in der Anwendung konfiguriert wird. Ändern Sie das Passwort nicht, nachdem Sie es festgelegt haben. Andernfalls können Sie das gespeicherte Kennwort nicht entschlüsseln und Sie können den Solution Manager Konnektor nicht mehr ohne manuelle (nicht unterstützte) Änderungen an der Datenbank verwenden.
- **Nur für MS SQL erforderlich:** Entfernen Sie das `#` aus der Zeile `#spring.jpa.properties.hibernate.dialect: com.signavio.hibernate.dialect.CustomSQLServerDialect`. Dies aktiviert die korrekte Zuordnung von Datenbanktypen in der Anwendung.

### 3.13.2 Konfiguration des Konnektors

Die Konfiguration des Konnektors ähnelt der für Signavio Process Manager verwendeten Konfiguration. Verwenden Sie im Code Environment anstelle von Parameter.

Öffnen Sie `context.xml` im Tomcat conf-Ordner und fügen Sie folgendes Code-Snippet innerhalb des Context-Tags unter anderen Parametern hinzu:

```
<Environment name="spring.config.location" value="${catalina.base}/conf/solman72.yml" type=
↪ "java.lang.String"/>
```

Als nächstes öffnen Sie `configuration.xml` und fügen Sie folgendes hinzu:

```
<sharedJwtSecret>SHARED_SECRET_CHANGE_ME</sharedJwtSecret>

<gatewaymappings>solman72=http://localhost:8080/solman72</gatewaymappings>
```

Folgende Parameter müssen konfiguriert werden:

- **sharedJwtSecret:** Genau wie bei der Vorlagendatei, legen Sie hier den Schlüssel fest. Er muss in den Dateien `solman72.yml` und `configuration.xml` identisch sein.



- gatewaymappings: Das sind Ihr Host und Ihr Port. `http://localhost:8080` ist der Standardwert. `-solman72` ist der Name des Verzeichnisses im Tomcat *webapps*-Ordner und sollte nicht verändert werden.

**Hinweis:** Stellen Sie sicher, dass die Parameter in der Vorlage und in den Konfigurationsdateien konsistent sind.

### 3.13.3 Verwendung der Solution-Administration

Informationen zur Verwendung des Konnektors finden Sie im [Signavio Nutzerhandbuch](#)<sup>2</sup>.

### 3.13.4 Generieren des SSL-Zertifikats (optional)

Dieser Abschnitt ist nur relevant, wenn Sie HTTPS mit Signavio Process Manager verwenden. Weitere Informationen finden Sie im Kapitel *HTTPS verwenden (optional)* (Seite 38).

Wenn Sie HTTPS verwenden, benötigt Apache Tomcat ein SSL-Zertifikat mit mehreren DNS-Namen, um den Konnektor auszuführen.

Erstellen Sie zuerst eine Konfigurationsdatei namens `selfsigned.conf` und verwenden Sie diese, um das SSL-Zertifikat zu generieren. Im Folgenden finden Sie eine Beispiel-Konfigurationsdatei, welche Sie als Vorlage verwenden können.

```
[ req ]
default_bits = 2048
default_keyfile = localhost.pem
distinguished_name = subject
req_extensions = req_ext
x509_extensions = x509_ext
string_mask = utf8only

[ subject ]
countryName = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = NY

localityName = Locality Name (eg, city)
localityName_default = New York

organizationName = Organization Name (eg, company)
organizationName_default = Example, LLC

commonName = Common Name (e.g. server FQDN or YOUR name)
commonName_default = Example Company

emailAddress = Email Address
emailAddress_default = test@example.com

[ x509_ext ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer

basicConstraints = CA:FALSE
```

<sup>2</sup> [https://docs.signavio.com/userguide/editor/de/workspace\\_admin/sap\\_solman/solman72/index.html](https://docs.signavio.com/userguide/editor/de/workspace_admin/sap_solman/solman72/index.html)



```
keyUsage = digitalSignature, keyEncipherment
subjectAltName = @alternate_names
nsComment = "OpenSSL Generated Certificate"

[ req_ext ]
subjectKeyIdentifier = hash

basicConstraints = CA:FALSE
keyUsage = digitalSignature, keyEncipherment
subjectAltName = @alternate_names
nsComment = "OpenSSL Generated Certificate"

[ alternate_names ]
DNS.1 = localhost
DNS.2 = 127.0.0.1
DNS.3 = mycompany.com
DNS.4 = signavio.mycompany.com

# Add these if you need them
# DNS.5 = mycompany.de
# DNS.6 = mycompany.co.uk
# DNS.7 = 127.0.0.1

# IPv6 localhost
# DNS.8 = ::1
# DNS.9 = fe80::1]
```

Als Nächstes ändern Sie die DNS-Parameter so, dass sie mit den Adressen übereinstimmen, die Sie für den Zugriff auf die Plattform verwenden. Verwenden Sie in der Kommandozeile `openssl req -config selfsigned.conf -new -x509 -sha256 -newkey rsa:2048 -nodes -keyout localhost.key.pem -days 365 -out localhost.cert.pem`, um das Zertifikat zu generieren. Verwenden Sie anschließend den Befehl `openssl pkcs12 -export -out localhost.pfx -inkey localhost.key.pem -in localhost.cert.pem`, um eine PFX-Datei zu erzeugen.

### 3.13.5 SSL-Zertifikaten in Tomcat vertrauen (optional)

Als letzten Schritt weisen Sie Ihren Tomcat an, Ihrem selbstsignierten Zertifikat zu vertrauen.

Erstellen Sie einen vertrauenswürdigen Java Keystore. Fügen Sie in der Befehlszeile das selbstsignierte Zertifikat hinzu, indem Sie den Befehl `keytool -importcert -file localhost.cert.pem -keystore keystore.jks -alias „localhost“` verwenden. Wählen Sie ein neues Passwort, wenn Sie dazu aufgefordert werden.

Konfigurieren Sie Ihren Tomcat so, dass er dem gerade erstellten Keystore vertraut, indem Sie Tomcat mit den Java-Parametern `-Djavax.net.ssl.keyStore`, `-Djavax.net.ssl.keyStorePassword`, `-Djavax.net.ssl.trustStore` und `-Djavax.net.ssl.trustStorePassword`. Eine Möglichkeit dazu ist durch die Umgebungsvariable `CATALINA_OPTS`, z. B.: .. code

```
bash_profile
export CLIENT_CERT=/path/to/keystore.jks
export CATALINA_OPTS="$CATALINA_OPTS -Djavax.net.ssl.keyStore=$CLIENT_CERT -Djavax.net.ssl.
↪keyStorePassword=mypassword -Djavax.net.ssl.trustStore=$CLIENT_CERT -Djavax.net.ssl.
↪trustStorePassword=mypassword"
```

Schließlich müssen Sie Ihren Tomcat so konfigurieren, dass er Ihre neu erstellte PFX-Datei verwendet. Folgen Sie den Anweisungen im Kapitel [HTTPS verwenden](#) (Seite 38).



### 3.13.6 System diagnostics

On-premise-Kunden können auf der Seite **System diagnostics** überprüfen, ob ihre Konnektor-Installation erfolgreich war. Weitere Informationen finden Sie im Kapitel *Konfigurationsfehler mithilfe des Diagnostics-Tools beheben* (Seite 22).

## 3.14 Die GitHub-Integration für RedHat JBoss BRMS-Projekte konfigurieren (optional)

**Bemerkung:** Konfigurieren Sie die Integration nur, wenn Sie wirklich planen, mit dem Signavio Process Manager Diagramme in Ihre RedHat JBoss BRMS-Projekte auf GitHub zu überführen.

Die *Integration des Signavio Process Editors mit GitHub*<sup>3</sup> ermöglicht es Ihnen, Diagramme nahtlos vom Signavio Process Manager in RedHat JBoss BRMS-Projekte auf GitHub zu überführen.

Gehen Sie wie folgt vor, um die GitHub-Integration mit Ihrem System zu konfigurieren:

1. Erstellen Sie eine GitHub OAuth-Anwendung.

Loggen Sie sich in Ihren GitHub-Account ein und öffnen Sie <https://github.com/settings/applications/new>. Fügen Sie nun einen Anwendungsnamen, eine Homepage und eine Beschreibung Ihrer Wahl hinzu. Tragen Sie zudem als **Authorization callback URL** die Basis-URL Ihres On-Premise-Systems ein, zum Beispiel `https://mysignavio.acme.com:8080`.

### Register a new OAuth application

#### Application name

Something users will recognize and trust

#### Homepage URL

The full URL to your application homepage

#### Application description

This is displayed to all users of your application

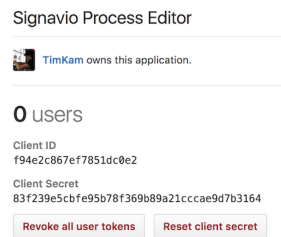
#### Authorization callback URL

Your application's callback URL. Read our [OAuth documentation](#) for more information.

2. Klicken Sie auf **Register application**.

Lassen Sie die Website offen, um die Token Client ID und Client Secret später zu kopieren.

<sup>3</sup> [https://editor.signavio.com/userguide/de/explorer/export/redhat\\_to\\_github.html](https://editor.signavio.com/userguide/de/explorer/export/redhat_to_github.html)



3. Hinterlegen Sie die Authentifizierungsdaten der GitHub-Anwendung in der Konfigurationsdatei des Signavio Process Managers.

Öffnen Sie die Datei `configuration.xml` in dem Verzeichnis `$TOMCAT_DIR/conf/`. `$TOMCAT_DIR` bezeichnet hierbei das Root-Verzeichnis Ihres Tomcats.

Fügen Sie die folgenden Zeilen über dem abschließenden `</configuration>`-Tag hinzu.

```
<githubClientId><myClientId></githubClientId>
<githubClientSecret><myClientSecret></githubClientSecret>
```

Ersetzen Sie `<myClientId>` mit Ihrer *Client ID* und `<myClientSecret>` mit Ihrem *Client Secret*.

### 3.15 Den Collaboration Hub mit Active Directory-Anbindung konfigurieren (optional)

Wenn Sie den Collaboration Hub mit Single-Sign-On verwenden möchten, müssen Sie die Konfiguration zur Anbindung des Signavio Process Managers an Ihr Active-Directory-System angeben.

**Hinweis:** Für eine Verwendung von Kerberos-SSO muss der Signavio-Server unter Microsoft Windows 64 Bit installiert werden und zu der Domäne gehören, auf dessen Active Directory zugegriffen werden soll.

**Hinweis:** Um die Verbindung an das Active Directory zu testen, können Sie den kostenlosen **LDAP Browser** der Firma Softterra verwenden. Sie können überprüfen, ob der Nutzernamen und das Passwort korrekt sind und der Nutzer Zugriff auf die relevanten Bereiche des Active Directory hat. Den Softterra LDAP-Browser können Sie über den folgenden Link herunterladen:

<http://www.ldapbrowser.com/download.htm>

**Hinweis:** Vor der Aktivierung bzw. Deaktivierung der SSO-Funktionalität empfiehlt es sich, alle bisherigen Freigaben zu entfernen, da sonst möglicherweise Diagramme nicht für den korrekten Personenkreis freigegeben sind.

In der `configuration.xml`-Vorlage finden Sie eine Beispielkonfiguration für eine Active-Directory-Anbindung:

```
<ldap>

  <ldapHost>ldap://192.168.0.100/</ldapHost>

  <ldapSearchRoots>

    <ldapSearchRoot>CN=Users,DC=company,DC=com</ldapSearchRoot>
```



```

<ldapSearchRoot>CN=Groups,DC=company,DC=com</ldapSearchRoot>

</ldapSearchRoots>

<ldapUser>CN=LdapUser,CN=Users,DC=company,DC=com</ldapUser>

<ldapPw>password</ldapPw>

<ldapSsoMode>KERBEROS</ldapSsoMode>

<ldapModelerSsoSupported>true</ldapModelerSsoSupported>

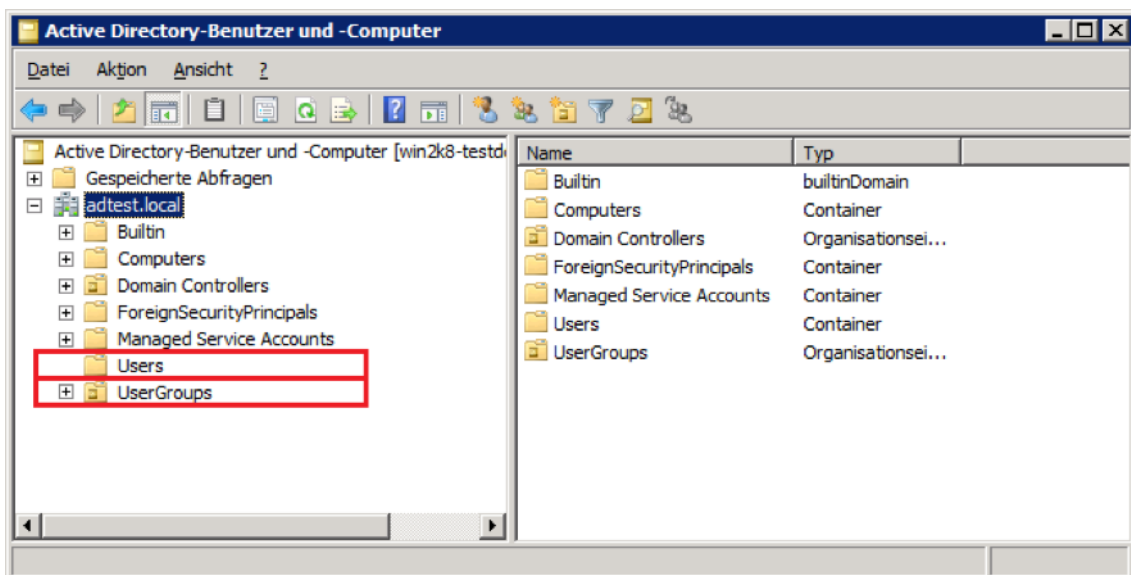
<ldapAdminMail>admin@company.com</ldapAdminMail>

</ldap>

```

Für die Anfragen an das Active-Directory werden LDAP-Schnittstellen verwendet. Passen Sie hierfür die Datei `configuration.xml` wie folgt an:

- **IdapHost:** URL für den Zugriff auf das Active Directory mittels LDAP.
- **IdapSearchRoots:** Mehrere Ordnerobjekte, die als Wurzelverzeichnis für die Suche verwendet werden. Die Objekte müssen als Distinguished Names angegeben werden. Als Wurzelknoten können *Organisationseinheiten* und *Container* eingetragen werden. Beachten Sie zudem, dass Nutzergruppen **nicht** als Container von Nutzern fungieren, sondern diese nur referenzieren. Die folgenden zwei Beispiele zeigen Möglichkeiten, wie ein Active Directory in der Beispieldomäne `adtest.local` strukturiert sein kann und welche Ordnerobjekte in diesen Fällen gesetzt werden müssen:
  - Falls die Container *Users* und *UserGroups* in Ordnern unterhalb des Domain-Wurzelknoten liegen, müssen die rot markierten Ordner als `searchRoots` gesetzt werden:



*Beispiel: Nutzergruppen auf Root-Ebene im Active Directory*

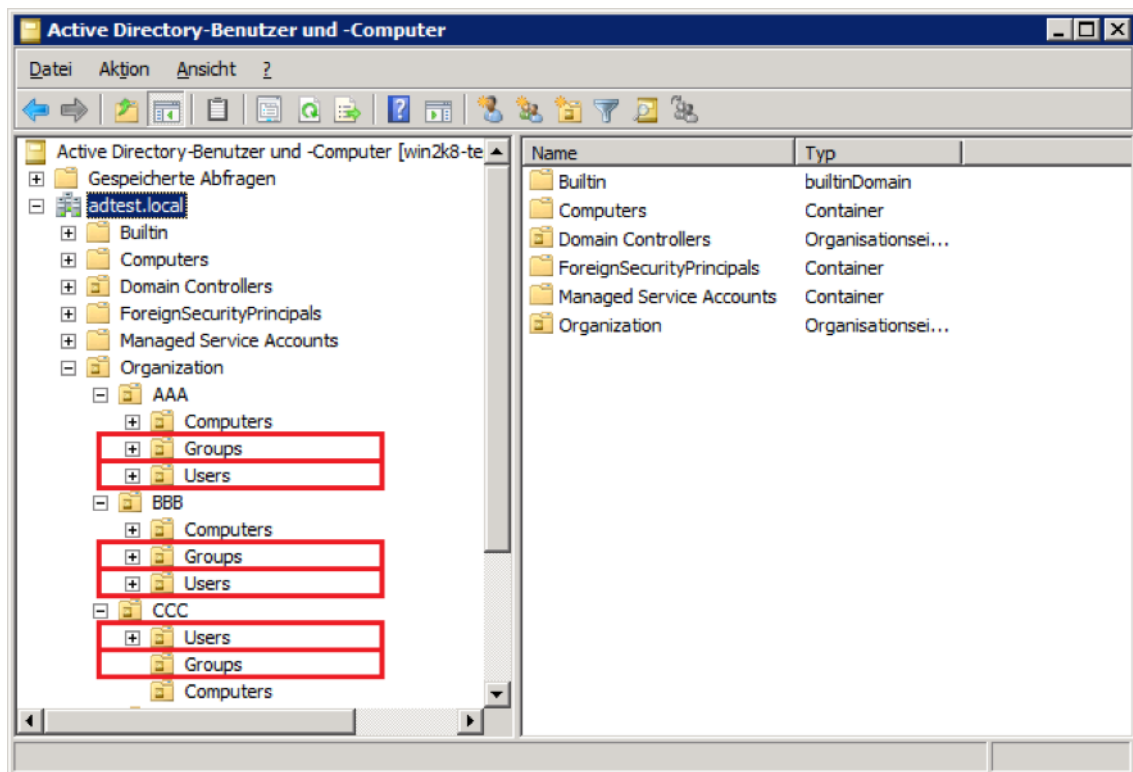
Die *Distinguished Names* sind in diesem Beispiel:

```

CN=Users,DC=adtest,DC=local
OU=UserGroups,DC=adtest,DC=local

```

Falls das Active Directory zunächst nach Standorten oder Organisationseinheiten unterteilt ist, sollten die jeweiligen Unterordner, die Gruppen und Nutzer enthalten, als `searchRoots` gesetzt werden:



*Beispiel: Nutzergruppen auf Organisationsebene im Active Directory*

Die *Distinguished Names* sind in diesem Beispiel:

```
OU=Groups,OU=AAA,OU=Organization,DC=adtest,DC=local
OU=Users,OU=AAA,OU=Organization,DC=adtest,DC=local
OU=Groups,OU=BBB,OU=Organization,DC=adtest,DC=local
OU=Users,OU=BBB,OU=Organization,DC=adtest,DC=local
OU=Groups,OU=CCC,OU=Organization,DC=adtest,DC=local
OU=Users,OU=CCC,OU=Organization,DC=adtest,DC=local
```

- **IdapUser:**

Nutzerobjekt für den Zugriff auf das Active Directory. Je nach Version und Konfiguration des Active Directory gibt es bis zu drei verschiedene Schreibweisen für den Nutzernamen:

Bitte probieren Sie die Schreibweisen in dieser Reihenfolge aus. Falls der Zugriff nicht funktioniert, probieren Sie bitte die nächste Schreibweise:

1. Distinguished Name (z. B.: CN=LdapUser,CN=Users,DC=company,DC=com)
2. Nutzer-UPN-Anmeldungsname (z. B.: LdapUser@company.com)
3. SamAccountName (z. B.: company\LdapUser)

- **IdapPw:**

Passwort des Nutzerobjekts.

- **IdapSsoMode:**

Zu verwendender SSO-Mechanismus. Mögliche Werte sind KERBEROS oder LDAPQUERY (Authentifizierung per LDAP-Nutzer und -Passwort). Sollten Sie Kerberos verwenden, muss



der Signavio Process Manager unter Microsoft Windows 64 Bit installiert werden. Sollten Sie LDAP-Anfragen verwenden, können Sie zusätzlich ein `ldapQueryLoginPattern` spezifizieren (siehe unten).

- **IdapQueryLoginPattern** (optional): Ermöglicht eine Vervollständigung eines eingegebenen Nutzernamens bei der LDAP- Anfragen-basierten Authentifizierung.

Beispiel: Über das Pattern `$login$@company.com` kann eingerichtet werden, dass anstatt der Nutzereingabe `m.mustermann` der folgende Nutzername zur Authentifizierung verwendet wird: `m.mustermann@company.com`.

- **IdapModelerSsoSupported**

Steuert, ob sich Nutzer aus dem Active-Directory als Modellierer am Signavio Process Manager anmelden können ohne ein eigenes Signavio-Passwort eingeben zu müssen. Mögliche Werte sind `true` und `false` (Standardwert).

Voraussetzung für die Verwendung ist, dass ein Modellierungsnutzer im Signavio Process Manager mit der im Active-Directory hinterlegten E-Mail-Adresse registriert ist.

- **IdapAdminMail**

E-Mail-Adresse des für die LDAP-Konfiguration verantwortlichen Administrators. Diese wird für wichtige Systemmeldungen verwendet und muss daher gesetzt sein.

Kopieren Sie anschließend Ihre angepasste `configuration.xml` und die Ihnen bereitgestellte Lizenzdatei `configuration_signed.xml` in das Verzeichnis `$TOMCAT_DIR/conf/` und starten den Tomcat-Server neu.

Vergeben Sie anschließend gemäß dem Kapitel [Zugriffsverwaltung auf das BPM Collaboration Hub in der On-Premise Edition](#)<sup>4</sup> des Signavio Nutzerhandbuchs Leseberechtigungen für das BPM Collaboration Hub an Nutzer und/oder Nutzergruppen.

Mit dem Collaboration Hub erwerben Sie ein Kontingent für eine bestimmte Anzahl von Active-Directory Nutzern, die Leseberechtigungen auf Modelle im Signavio Collaboration Hub besitzen dürfen. Es werden hierfür sämtliche Nutzer für alle freigegebenen Diagramme zusammengerechnet.

Falls die Anzahl 80% des Nutzer-Kontingentes überschreitet, wird automatisch eine Benachrichtigungs-E-Mail an den Administrator des Arbeitsbereiches gesendet.

Bei einer etwaigen Überschreitung des Kontingentes wird der Lesezugriff auf den Signavio Collaboration Hub vorübergehend deaktiviert. Es wird kein Lesezugriff auf die Prozesslandschaft möglich sein. Ein Login der lizenzierten Modellierungsnutzer bleibt jedoch zu jedem Zeitpunkt möglich.

---

**Hinweis:** Um die automatische Authentifizierung über den Kerberos Nutzer im Internet Explorer zu aktivieren, fügen Sie den Hostnamen des Signavio Servers zur Sicherheitszone **Lokales Intranet** hinzu und stellen Sie sicher, dass für die Option **Benutzerauthentifizierung - Anmeldung** dieser Sicherheitszone der Wert **Automatisches Anmelden nur in der Intranetzone** ausgewählt ist.

---

Zur Aktivierung einer Kerberos-Authentifizierung im Mozilla Firefox müssen Sie **about:config** im Adressfeld des Browsers eingeben und aufrufen. In der so geöffneten Ansicht müssen Sie den Wert für `network.negotiate-auth.trusted-uris` auf den in der `configuration.xml` gesetzten Server des Signavio-Systems setzen. Sollten hier bereits ein oder mehrere Hosts gesetzt sein, erweitern Sie die Komma-separierte Liste um die Server-URL.

---

<sup>4</sup> [https://docs.signavio.com/userguide/editor/de/workspace\\_admin/manage\\_users\\_access/portal\\_managing\\_user\\_access.html?highlight=access](https://docs.signavio.com/userguide/editor/de/workspace_admin/manage_users_access/portal_managing_user_access.html?highlight=access)





### 3.16 Die Signavio Collaboration Hub SharePoint-Komponente konfigurieren (optional)

Dieser Abschnitt beschreibt die Installation der optionalen Komponente **Signavio Collaboration Hub Webpart** für die Integration des Collaboration Hubs in ein Microsoft SharePoint System.

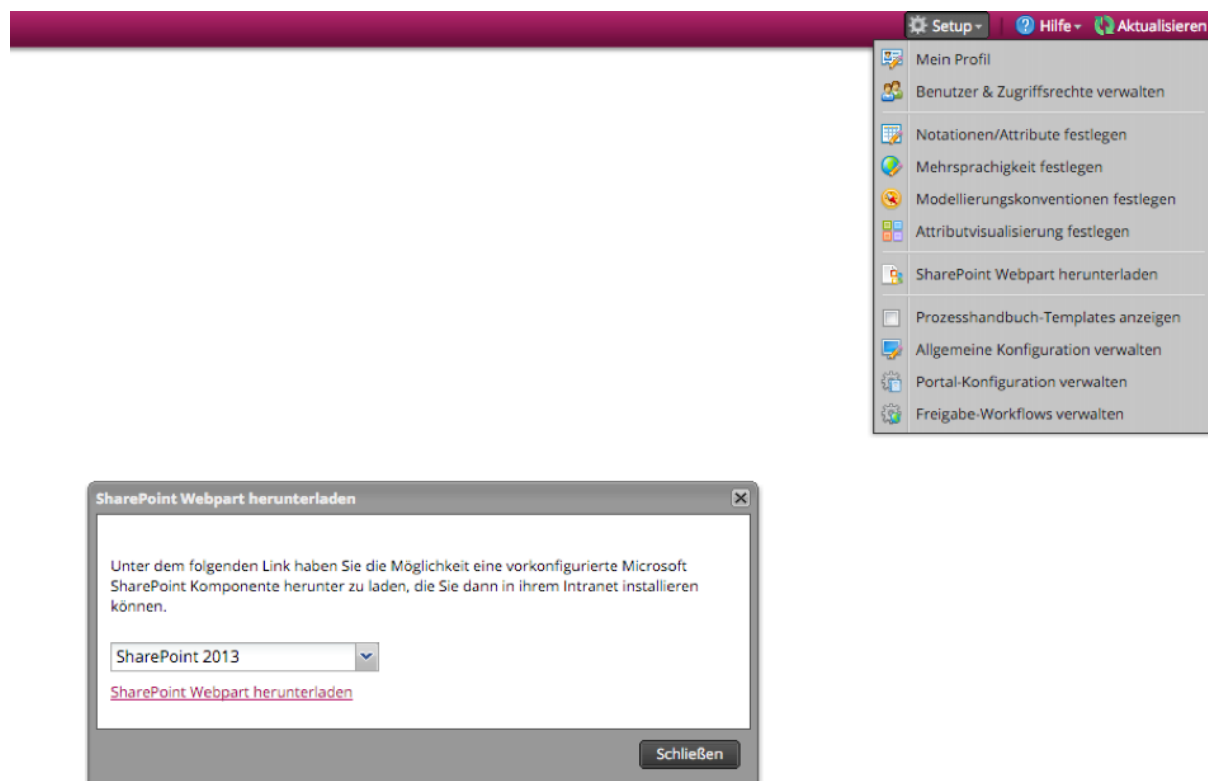
Für die Installation benötigen Sie einen Microsoft Office SharePoint Server (<http://sharepoint.microsoft.com>)

**Bemerkung:** Eine Integration von **SharePoint for Office 365** (SharePoint Online) ist lediglich mit dem Software-as-a-Service Angebot von Signavio möglich.

**Wichtig:** Nachdem Microsoft® den Mainstream-Support für Microsoft® SharePoint® 2007 und 2010 am **09.10.2012**<sup>5</sup>, beziehungsweise am **13.10.2015**<sup>6</sup> hat auslaufen lassen, ist es zunehmend schwierig, zeitgemäße Funktionen des Collaboration Hubs in den genannten Versionen von SharePoint® zur Verfügung zu stellen. Den Collaboration Hub möchten wir auch weiterhin aktuell halten und Ihnen dafür den bestmöglichen Support bieten. Daher haben wir die Unterstützung für Microsoft® SharePoint® 2007 und 2010 zum **1. April 2017** eingestellt.

Diese Komponente ist ein Webpart, welches eine vorkonfigurierte Sicht auf den Collaboration Hub ermöglicht. Diese Zusatzkomponente muss kostenpflichtig separat erworben werden.

Laden Sie die Webpart-Datei aus dem Signavio Explorer unter **Setup - SharePoint Webpart herunterladen** herunter:



Laden Sie den Signavio Web Part herunter

<sup>5</sup> <https://support.microsoft.com/de-de/lifecycle?p1=11373>

<sup>6</sup> <https://support.microsoft.com/de-de/lifecycle?p1=14944>



Kopieren Sie die SignavioViewer2013\_2016.wsp-Datei in ein Verzeichnis Ihrer Wahl auf dem SharePoint-Server. Installieren Sie die SharePoint Solution nach der Anleitung ihrer Microsoft SharePoint-Version.

### 3.16.1 Installation des Webparts

Dieser Abschnitt beschreibt die Installation mit den verschiedenen SharePoint Server-Versionen. Die Variable <SharePointServerURL> steht für die URL der Webanwendung des SharePoint Servers.

Das Signavio Collaboration Hub-Webpart verwendet eine SSL-Verbindung für die Kommunikation mit dem Signavio Service. Falls Sie sehr strikte Sicherheitseinstellungen für Ihren SharePoint-Server vorgenommen haben, muss die von Signavio verwendete Zertifizierungsstelle unter Umständen in den Microsoft SharePoint 2010 **Trusted Root Certificate Store** importiert werden. Das Zertifikat geotrust.cer können Sie unter

- <https://editor.signavio.com/sharepoint/geotrust.zip> (Europa), beziehungsweise
- <https://app-us.signavio.com/sharepoint/geotrust.zip> (USA) oder
- <https://app-au.signavio.com/sharepoint/geotrust.zip> (Australien) herunterladen.

Um das geotrust-Zertifikat zu installieren, führen Sie bitte die folgenden Schritte durch:

- Stellen Sie sicher, dass der Windows Dienst **SharePoint Administraton** ausgeführt wird.
- Öffnen Sie die **Microsoft SharePoint 2013/2016 Zentraladministration**.
- Navigieren Sie zu **Sicherheit > Vertrauensstellung verwalten** und klicken Sie auf **Neu**.
- Geben Sie einen beliebigen Namen an und navigieren Sie zur geotrust.cer-Datei.

Um den Webpart zu installieren, öffnen Sie die SharePoint Verwaltungs-Shell und führen Sie die folgenden Befehle aus:

```
Add-SPSolution -LiteralPath <Path>\SignavioViewer2013_2016.wsp  
  
Install-SPSolution -Identity SignavioViewer2013_2016.wsp -WebApplication  
<SharePointServerURL> -GACDeployment
```

Sie können den Installationsstatus in der SharePoint Zentraladministration über die folgende URL überprüfen: [http://<SharePointServerURL>:<ADMIN\\_PORT>/\\_admin/SolutionStatus.aspx?ItemName=signavioviewer2013\\_2016.wsp&Lcid=0](http://<SharePointServerURL>:<ADMIN_PORT>/_admin/SolutionStatus.aspx?ItemName=signavioviewer2013_2016.wsp&Lcid=0).

Weitere Information über die Installation einer .wsp-Datei auf einem Microsoft SharePoint Server finden Sie unter <http://technet.microsoft.com/de-de/library/cc262995.aspx>

### 3.16.2 Den Webpart konfigurieren

Nachdem Sie die SharePoint Solution auf Ihrem SharePoint Server installiert haben, können Sie auf der gewünschten Seite die Signavio Komponente einbinden.

1. Navigieren Sie zu **Seite** und klicken Sie auf **Neu**.
2. Binden Sie anschließend über **Webpart hinzufügen** die installierte Komponente ein.
3. Wählen Sie **Signavio Collaboration Hub Webpart** und fügen Sie es hinzu.
4. Klicken Sie auf **Bearbeiten** und tragen Sie auf der rechten Seite im Konfigurationsabschnitt **Signavio** die **Signavio URL** ein, die entweder zum Signavio Server zeigt oder die URL zu einem beliebigen Einstiegsdiagramm definiert (URL aus der Collaboration Hub-Vorschau). Außerdem haben Sie in den anderen Konfigurationsabschnitten die Möglichkeit, detailliert auf die Erscheinung der Komponente Einfluss zu nehmen. Dazu können Sie z. B. den Titel oder die Ausmaße konfigurieren.



Weitere Information zum Einbinden eines Webparts auf eine SharePoint-Seite finden Sie unter <http://office.microsoft.com/de/HA010097463.aspx>.

### 3.17 Freigabe-Workflow mit Signavio Workflow Accelerator konfigurieren (optional)

Für Kunden, die eine Signavio Workflow Accelerator-Lizenz haben, ist das **Freigabe-Workflow**-Feature verfügbar. Die Verwendung der Funktion erfordert eine Integration mit dem Signavio Workflow Accelerator-System.

Näheres zu der Installation und der Konfiguration von Signavio Workflow Accelerator entnehmen Sie bitte dem Signavio Workflow Accelerator Administratorenhandbuch unter <https://docs.signavio.com/adminguide/workflow/de/>.

---

**Hinweis:** Bitte stellen Sie bei der Installation sicher, dass Ihre Process Manager-Version mit der Signavio Workflow Accelerator-Version, die Sie installieren, kompatibel ist. Eine Kompatibilitätsliste finden Sie unter <https://docs.signavio.com/adminguide/workflow/de/signavio.html#compatibility-list>.

---

### 3.18 Den Signavio Simulationsserver konfigurieren (optional)

Die Ausführung der Simulation von Prozessen erfolgt in einer eigenständigen Webapplikation, die standardmäßig auf demselben Tomcat-Server installiert wird, wie auch der Rest der Anwendung. Um eine Überlastung des Webserver durch ein komplexes Simulationsszenario zu verhindern, werden Simulationsinstanzen bei Erreichen bestimmter vorkonfigurierter Grenzen abgebrochen. Sie können diese Grenzen auf eigene Gefahr erhöhen. Um eine Überlastung des Webserver zu verhindern, kann die Simulationskomponente außerdem auf einen eigenen Tomcat-Server ausgelagert werden.

#### 3.18.1 Die Eigenschaften des Signavio Simulationsservers konfigurieren

Zur Konfiguration des Simulationsservers muss die Datei `simulation.xml` angepasst werden, die unter `$TOMCAT_DIR/conf/` zu finden ist.

Entfernen Sie die Kommentierungszeichen der entsprechenden XML-Tags und passen die Tags wie folgt an:

- **maxResults:** Definiert das Maximum der Simulationsergebnisse, die vom Simulationsserver zu einem Zeitpunkt zwischengespeichert werden können. Der Standardwert ist 100.
- **maxCachedInstances:** Definiert das Maximum der laufenden Simulationsinstanzen, die vom Simulationsserver zu einem Zeitpunkt zwischengespeichert werden können. Der Standardwert ist 100.

$$\text{NrOfParallelNCasesRuns} \times \frac{\text{maxLogEntries} \times 15}{100.000} \text{MB}$$

- **resultTimeout:**  
Definiert den Zeitraum (in Sekunden) nach dem ein Simulationsergebnis als 'alt' angesehen wird und gelöscht werden kann. Der Standardwert ist 600.
- **instanceTimeout:** Definiert den Zeitraum (in Sekunden) nach dem eine Simulationsinstanz als 'alt' angesehen wird und gelöscht werden kann. Der Standardwert ist 600.



---

**Hinweis:** Wenn Sie den Simulationsserver mit den Standardeinstellungen betreiben möchten, brauchen Sie nach der Entfernung der Kommentierungszeichen die Einstellungen nicht anzupassen.

---

### 3.18.2 Signavio Simulationsserver in einem separaten Tomcat installieren (optional)

---

**Wichtig:** In den meisten Fällen ist es nicht notwendig den Signavio Simulationsserver in einem separaten Tomcat zu installieren. Valide Gründe hierfür gibt es nur, wenn die folgenden Bedingungen beide zutreffen:

- Sie verwenden die Enterprise Edition von Signavio.
  - Viele Ihrer Geschäftsprozessmodellierer verwenden regelmäßig das n-case Simulationsfeature.
- 

Um den Simulationsserver in einem separaten Tomcat zu betreiben, stellen Sie einen weiteren Server bereit und installieren und konfigurieren Sie einen Apache Tomcat-Server analog zum Process Manager-Server (siehe: *Den Webserver konfigurieren* (Seite 12)).

---

**Hinweis:** Sollte der zweite Tomcat auf demselben Server / in derselben VM laufen, stellen Sie bitte sicher, dass die Ports der beiden Tomcat Server **nicht** identisch sind.

---

---

**Hinweis:** Stellen Sie bitte sicher, dass bei einem Update des Signavio Process Managers auch der Simulationsserver aktualisiert wird. Unterschiedliche Versionen sind zueinander inkompatibel.

---

Gehen Sie abschließend wie folgt vor:

1. Stoppen Sie die Tomcat-Server, falls diese zur Zeit laufen.
2. **Verschieben** (nicht kopieren) Sie den Ordner `simulationsservice` aus dem `webapps`-Verzeichnis des Signavio-Tomcats in das `webapps`-Verzeichnis des Simulations-Tomcats.
3. Passen Sie die Datei `simulation.xml`, die unter `<haupt-tomcat>\conf` zu finden ist, wie folgt an (auch hier müssen die Auskommentierungszeichen der entsprechenden XML-Tags entfernt werden):
  - `host`: Definiert den Hostnamen des Servers über dem der Simulationsserver erreichbar ist, z.B. `http://mysignaviosimulationsservice:8180`.
  - `path`: Definiert den URL-Pfad unter dem der Simulationsserver abgelegt ist, normalerweise `/simulationsservice/`.
4. Starten Sie die beiden Tomcat Server (die Reihenfolge spielt keine Rolle).

## 3.19 Apache Solr Server konfigurieren (optional)

Für die Suche nach Diagrammen, Ordnern, hochgeladenen Dokumenten sowie Glossareinträgen wird ein Apache Solr Server eingesetzt, der standardmäßig in demselben Tomcat Server installiert wird, wie der Rest der Anwendung.

Der Apache Solr Server kann alternativ auf einem separaten Webserver installiert werden, in der Regel ist dies jedoch nicht erforderlich. Wenn Sie ein Signavio System mit einen der folgenden Parameter betreiben, dann kann es zur besseren Lastverteilung sinnvoll sein, einen separaten Webserver zu verwenden:

- Sie verwenden das System mit mehr als 1000 Modellierern.



- Sie verwenden das System mit mehr als 50000 Collaboration Hub Nutzern.
- Ihre Prozesslandschaft besteht aus über 5000 Diagrammen.
- Sie betreiben Signavio in einem Webserver-Cluster.

Um den Solr Server in einem separaten Apache Tomcat zu betreiben, stellen Sie einen weiteren Server bereit und installieren und konfigurieren Sie einen Apache Tomcat Server analog zum Signavio Server (siehe: *Den Webserver konfigurieren* (Seite 12)).

**Hinweis:** Sollte der zweite Tomcat auf demselben Server / in derselben VM laufen, stellen Sie bitte sicher, dass die Ports der beiden Tomcat Server **nicht** identisch sind.

Gehen Sie abschließend wie folgt vor:

1. Stoppen Sie die beiden Tomcat Server, falls diese zur Zeit laufen.
2. **Verschieben** (nicht kopieren!) Sie den Ordner solr aus dem webapps-Verzeichnis des Signavio-Tomcats in das webapps-Verzeichnis des Solr-Tomcats.
3. Passen Sie die Datei configuration.xml, die unter <signavio-tomcat>\conf zu finden ist, an. Fügen Sie am Ende der Datei, aber vor der Zeile </configuration> die folgende Zeilen hinzu:  

```
<solrUrl>http://localhost:8080/solr</solrUrl>
```

Tauschen Sie die URL `http://localhost:8080/solr` mit der URL aus, unter der der Solr Server zu erreichen ist. Achten Sie darauf, auch den Kontextpfad der Webanwendung anzugeben (standardmäßig solr).
4. Starten Sie den Solr-Tomcat.
5. Starten Sie den Signavio-Tomcat.

**Hinweis:** Achten Sie immer darauf, dass der Solr Server bereits läuft, wenn Sie den Signavio Server starten. Anderenfalls schlägt die Erstellung des Suchindexes fehl.

## 3.20 Imageserver konfigurieren (optional)

Analog zur Konfiguration des Apache Solr Server lässt sich der Imageserver konfigurieren.

Folgenden Sie hierfür den Anweisungen unter *Apache Solr Server konfigurieren (optional)* (Seite 36).

Verschieben Sie diesmal allerdings den Ordner imageservice aus dem webapps-Verzeichnis des Signavio-Tomcats in das webapps-Verzeichnis des Imageserver-Tomcats und fügen Sie die folgende Zeile zur configuration.xml hinzu:

```
<imageServiceHost>http://localhost:8080</imageServiceHost>
```

Ersetzen Sie die URL `http://localhost:8080` mit der URL Ihres Imageservers.

## 3.21 Den Mailing-Server konfigurieren (optional)

Für das Versenden von E-Mails wird ein Mailing Server verwendet, der standardmäßig in demselben Tomcat-Server installiert wird, wie der Rest der Anwendung. Der Mailing-Server kann alternativ auf einem separaten Webserver installiert werden. In der Regel ist dies jedoch nicht erforderlich. Falls einer der folgenden Punkte auf Ihr Anwendungsszenario zutrifft, kann es zur besseren Lastverteilung sinnvoll sein, einen separaten Webserver zu verwenden:



- Sie verwenden das System mit mehr als 1000 Modellierern.
- Sie verwenden das System mit mehr als 50000 Portalnutzern.
- Sie betreiben Signavio in einem Webserver-Cluster.

Um den Mailing Server in einem separaten Apache Tomcat zu betreiben, stellen Sie einen weiteren Server bereit und installieren und konfigurieren Sie einen Apache Tomcat Server analog zum Signavio Server (siehe: *Den Webserver konfigurieren* (Seite 12)). Stellen Sie außerdem sicher, dass der Mailing Server Zugriff auf die Signavio Datenbank erhält. Wir empfehlen denselben Datenbanknutzer zu verwenden, wie für den Signavio Server, da dies das Setup vereinfacht.

---

**Hinweis:** Sollte der zweite Tomcat auf demselben Server/in derselben VM laufen, stellen Sie bitte sicher, dass die Ports der beiden Tomcat Server **nicht** identisch sind.

---

Gehen Sie anschließend wie folgt vor:

1. Stoppen Sie die Tomcat-Server, falls diese zur Zeit laufen.
2. **Verschieben** (nicht kopieren) Sie den Ordner `mailingservice` aus dem `webapps`-Verzeichnis des Signavio-Tomcats in das `webapps`-Verzeichnis des Mailing-Tomcats.
3. Passen Sie die Datei `configuration.xml` im Verzeichnis `<signavio-tomcat>/conf` entsprechend an.
4. Starten Sie den Signavio-Tomcat.
5. Starten Sie den Mailing-Tomcat.

---

**Hinweis:** Achten Sie immer darauf, dass der Signavio-Server bereits läuft, wenn Sie den Mailing-Server starten. Anderenfalls schlägt die Initialisierung des Mailingservices fehl.

---

## 3.22 HTTPS verwenden (optional)

Der Signavio Process Manager unterstützt verschlüsselte Kommunikation mittels HTTPS. Die Verwendung von HTTPS ist beispielsweise sinnvoll, wenn Nutzer über unsichere Netzwerkverbindungen auf den Signavio Server zugreifen.

Wenn Sie HTTPS verwenden möchten, ist eine zusätzliche Konfigurationen in der Anwendung nötig. Es wird vorausgesetzt, dass der zuständige Administrator Erfahrung in der Benutzung von HTTPS mit dem Apache Tomcat hat. Für weitere Hilfen zur Einrichtung von HTTPS im Apache Tomcat lesen Sie bitte die Dokumentation des Apache Tomcat.

---

**Hinweis:** Stellen Sie bitte sicher, dass das Zertifikat von einer vertrauenswürdigen Certificate Authority (CA) ausgestellt wurde und stellen Sie sicher, dass die JVM, mit dem der Apache Tomcat ausgeführt wird, dem Zertifikat sowie der CA vertraut. Hierzu müssen beide Zertifikate dem Java Truststore hinzugefügt werden.

---

Eine fehlerhafte HTTPS Konfiguration führt in der Regel zu einem oder mehreren der folgenden Effekte:

- Die Suche nach Diagrammen und Glossareinträgen gibt keine Ergebnisse zurück.
- Im Glossar werden keine Einträge angezeigt.
- Abgespeicherte Diagramme können nicht als PNG exportiert werden und die Diagrammvorschau im Explorer zeigt kein Diagramm an, das Collaboration Hub zeigt keine grafische Darstellung an und in der Simulation und dem Diagrammvergleich wird keine grafische Darstellung angezeigt.
- Die Simulation kann nicht ausgeführt werden.



- Es werden keine E-Mail-Benachrichtigungen verschickt.

Der Grund für diesen Effekt ist, dass die unterschiedlichen Funktionen von einzelnen Webanwendungen bereitgestellt werden, die per HTTP(S) kommunizieren.

Bei der Verwendung von HTTPS ist es für eine reibungslose Kommunikation daher erforderlich, dass die JVM Instanz das verwendete Zertifikat akzeptiert. Wenn Sie einen oder mehrere dieser Effekte beobachten, kontrollieren Sie die Logdateien vom Tomcat Server. Die Fehlermeldungen enthalten häufig konkrete Hinweise, welche Ursache das Problem hat.

### 3.22.1 Tomcat SSL-Zertifizierung

**Bemerkung:** Das Apache Tomcat Team gab bekannt, dass der Support für Apache Tomcat 8.0.x am 30. Juni 2018 beendet wurde. Daher unterstützt Signavio ausschließlich die Tomcat Version 8.5.x.

Eine detaillierte englischsprachige Anleitung zur SSL-Zertifizierung finden Sie in der offiziellen **Tomcat 8.5-Dokumentation** unter:

<https://tomcat.apache.org/tomcat-8.5-doc/ssl-howto.html>

Bitte stellen Sie sicher, dass UTF-8 als URLEncoder des HTTPS-Connectors gesetzt ist.

Eine korrekte Konfiguration kann zum Beispiel wie folgt aussehen:

```
<Connector port="443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
  maxThreads="150"
  SSLEnabled="true" scheme="https" secure="true"
  keystoreFile="Path/to/.keystore"
  keystorePass="mypassword"
  clientAuth="false" sslProtocol="TLS"
URIEncoding="UTF-8" />
```

**Bemerkung:** Das SSL-Protokoll für Tomcat 8.5 hat sich geändert. Das vorherige TLS-Protokoll wird nicht mehr von allen Browsern unterstützt. Daher können Sie Ihre Anwendung nicht erreichen, wenn Sie versuchen, das Standard-TLS-Protokoll zu verwenden. Um dies zu beheben, müssen Sie eine zusätzliche TLS-Version definieren.

Ihr Konnektor könnte zum Beispiel wie folgt aussehen:

```
<Connector
  port="443"
  protocol="org.apache.coyote.http11.Http11NioProtocol"
  maxThreads="200"
  SSLEnabled="true"
  scheme="https"
  secure="true"
  keystoreFile="D:/cert/localhost.pfx"
  keystorePass="123456"
  clientAuth="false"
  sslProtocol="TLSv1+TLSv1.1+TLSv1.2"
  keystoreType="PKCS12"
  URIEncoding="UTF-8"
  compressableMimeType="text/css,text/plain,image/svg+xml,application/xhtml+xml,text/html,text/
  ↪xml,text/javascript,application/xml,application/javascript"
  compression="on"
  compressionMinSize="2048"
  maxHttpHeaderSize="16384"/>
```



Für sehr große Active Directories müssen Sie den Parameter `maxHttpHeadersize` verdoppeln oder vervierfachen. Andernfalls wird Tomcat 8.5 den Vorgang abbrechen.

**Hinweis:** Die `keystore`-Zeilen sind optional und können abhängig von der Art des Zertifikats, welches Sie verwenden möchten, geändert werden (unser Beispiel ist für PFX). Bearbeiten Sie Ihren Code dementsprechend.

### 3.22.2 Einen Apache Webserver vor den Tomcat schalten, um SSL zu ermöglichen (Alternative zu 3.20.1)

Anstatt einen Tomcat HTTPS Connector zu konfigurieren, können Sie einen Apache Webserver (der HTTPS verwendet) vor den Tomcat schalten.

Um die Konfiguration durchzuführen, folgen Sie den Anweisungen in der offiziellen Tomcat Dokumentation unter [https://tomcat.apache.org/connectors-doc/webserver\\_howto/apache.html](https://tomcat.apache.org/connectors-doc/webserver_howto/apache.html).

### 3.22.3 Das Signavio-System konfigurieren

Führen Sie zusätzlich zu den Standardinstallationsschritten die folgenden Schritte aus.

Stoppen Sie hierzu den Tomcat-Server.

**Wichtig:** In diesen Anweisungen gehen wir davon aus, dass der Signavio Applikationsserver, der Mailingserver, der Imageserver, der Simulationsserver und der Apache Solr auf der selben Maschine laufen. Falls dies nicht der Fall ist, passen Sie bitte die entsprechenden URLs Ihrem Systemsetup entsprechend an und limitieren Sie eingehende Requests an den Tomcat in Schritt 1) **nicht** auf localhost (kein `address="127.0.0.1"`). Stattdessen können Sie Zugriffsbeschränkung zum Beispiel über **Remote Address Filter**<sup>7</sup> vornehmen.

Um das Signavio System für die Verwendung von HTTPS zu konfigurieren, gehen Sie wie folgt vor:

1. Aktivieren Sie einen **HTTP Connector** in der Datei `server.xml` (im Tomcat-Verzeichnis `conf`) wie unter **Apache Tomcat konfigurieren** beschrieben. Stellen Sie sicher, dass der Connector ausschließlich auf lokale Anfragen reagiert (`address="127.0.0.1"`). Eine korrekte Konfiguration sieht typischerweise wie folgt aus:

```
<Connector
  address="127.0.0.1"
  port="80" protocol="HTTP/1.1"
  connectionTimeout="20000"
  redirectPort="8443"
  URLEncoding="UTF-8"
  compression="on"
  compressionMinSize="2048"
/>
```

**Wichtig:** Es ist notwendig, dass alle anderen Services der Anwendung Requests an diesen Connector senden (siehe unten). Falls stattdessen der HTTPS Connector verwendet wird, kann es vorkommen, dass einige Anwendungsfunktionen nicht verlässlich verfügbar sind.

2. Passen Sie die Signavio Konfigurationsdatei `configuration.xml` (im Tomcat-Verzeichnis `conf`) an:
  - (a) Fügen Sie folgen Zeilen vor dem Schluss-Tag (`</configuration>`) ein:

<sup>7</sup> [http://tomcat.apache.org/tomcat-8.0-doc/config/valve.html#Remote\\_Address\\_Filter](http://tomcat.apache.org/tomcat-8.0-doc/config/valve.html#Remote_Address_Filter)





```
<solrUrl>
  http://localhost/solr
</solrUrl>
<imageServiceHost>
  http://localhost
</imageServiceHost>
<platformHostForMailingService>
  http://localhost
</platformHostForMailingService>

<decisionTableVerificationHost>
  http://localhost
</decisionTableVerificationHost>

<bdmSimulationServiceHost>
  http://localhost
</bdmSimulationServiceHost>

<droolsExportServiceHost>
  http://localhost
</droolsExportServiceHost>
```

- (a) Stellen Sie sicher, dass der Eintrag host in der Datei `simulation.xml` im selben Verzeichnis wie folgt aussieht:

```
<entry key="host">http://localhost</entry>
```

2. Passen Sie die Konfiguration des Apache Solr Servers an:

- (a) Öffnen Sie die Datei `$TOMCAT_DIR/webapps/solr/META-INF/context.xml`.

- (b) Fügen Sie dem XML-Element `Valve` im Attribut `allow` den Wert `YOUR_IP` hinzu.

`YOUR_IP` ist die IP-Adresse des Signavio Servers. Wenn Ihre IP-Adresse zum Beispiel `192.168.90.152` lautet, dann sieht die Zeile wie folgt aus:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
  allow="localhost|127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:1|
  192.168.90.152"
/>
```

3. Überprüfen Sie die Einstellungen wie unter *Konfigurationsfehler mithilfe des Diagnostics-Tools beheben* (Seite 22) beschrieben.

### 3.23 Installation in einem Tomcat Cluster (optional)

Der Signavio Process Manager kann in einem Apache Tomcat Cluster betrieben werden, wobei alle Knoten des Clusters dieselbe Datenbank verwenden.

Der Betrieb im Cluster kann die **Performanz** (Skalierbarkeit bei hoher Last) und **Verfügbarkeit** des Systems erhöhen.

Auf Grund des höheren administrativen Mehraufwands empfehlen wir jedoch, den Signavio Process Manager **nicht** in einem Cluster zu betreiben.

Die Software skaliert auch bei über 1000 Modellieren sehr gut, so dass keine spürbaren Performanceverbesserungen durch einen zweiten Tomcat Server zu erwarten sind. Lediglich der dem Tomcat zugewiesene Arbeitsspeicher sollte bei einer hohen Anzahl von Nutzern erhöht werden (zum Beispiel auf 16GB).

Um die Ausfallsicherheit zu erhöhen, empfehlen wir, einen passiven Webserver bereitzuhalten oder den Webserver als virtuelle Maschine in einer ausfallsicheren Infrastruktur zu betreiben. Dadurch wird die



Ausfallsicherheit auf Serverebene und nicht auf Anwendungsebene erhöht. Außerdem empfehlen wir ein Monitoring für den Tomcat Server einzurichten, sodass der Tomcat Server im Falle eines Ausfalls entweder automatisch oder zeitnah manuell neugestartet wird.

Wenn Sie den Signavio Process Manager in einem Tomcat Cluster betreiben möchten, beachten Sie bitte die folgenden Punkte:

- Für jeden Signavio Server wird eine separate Signavio Lizenz benötigt.
- Stellen Sie sicher, dass in jeder Tomcat-Instanz eine eindeutige JVM-Route gesetzt ist. Editieren Sie hierzu die Tomcat-Konfigurationsdatei `$TOMCAT_DIR/conf/server.xml` und fügen im XML-Element Engine das Attribut `jvmRoute` hinzu, z.B.:

```
<Engine name="Catalina" defaultHost="localhost" jvmRoute=ÜNIQUE_ID">
```

- Verwenden Sie einen Tomcat-Session-Cluster.
- Konfigurieren Sie den vorgeschalteten Loadbalancer so, dass alle Anfragen einer Session an denselben Applikationsserver weitergeleitet werden (*sticky sessions*).
- Stellen Sie sicher, dass der Mailing-Server auf nur einer Instanz betrieben wird (siehe: 3.19 Mailing Server konfigurieren (optional)). Anderenfalls wird jede laufende Instanz des Mailing-Servers Emails versenden.
- Stellen Sie sicher, dass der Solr Server nur auf einer Instanz betrieben wird (siehe: 3.17 Apache Solr Server konfigurieren (optional)).
- Ändern Sie für jede Tomcat-Instanz die Datei `configuration.xml` unter `<signavio-tomcat>/conf/` wie folgt:

- Fügen Sie die folgende Zeile hinzu:

```
<enableMultiplePlatformInstances>true</enableMultiplePlatformInstances>
```

- Setzen Sie den Eintrag `enableInternalKeyValueCache` auf `false`. Falls der Eintrag nicht vorhanden ist, fügen Sie die folgende Zeile vor dem schließenden `</configuration>`-Tag ein:

```
<enableInternalKeyValueCache>false</enableInternalKeyValueCache>
```

## 3.24 Manuelle Funktionstests durchführen

Um sicherzustellen, dass Ihr System nach einer Installation/einem Update ordnungsgemäß funktioniert, testen Sie bitte die folgenden Abläufe:

- (Nur bei Neu-Installation): Registrieren Sie mindestens zwei Signavio Nutzer.
- Loggen Sie sich als Modellierungsnutzer ein.
- Erstellen Sie einen Ordner und ein Diagramm (inkl. Glossarbegriffe).
- Veröffentlichen Sie das Diagramm im Collaboration Hub.
- Versenden Sie eine Einladung zum Kommentieren für das Diagramm.
- Erstellen Sie ein Prozesshandbuch.
- Erstellen Sie einen Excel-Report.
- Verwenden Sie die BPMN Simulation.
- Verwenden Sie das Glossar (editieren Sie zum Beispiel einen existierenden Eintrag).
- Loggen Sie sich als Modellierungsnutzer aus.
- Öffnen Sie den Collaboration Hub als Portalnutzer:
  - (Nur falls konfiguriert): Wird der Nutzer korrekt im Single-Sign-On erkannt?



- Ist das Diagramm dort freigegeben?
- Überprüfen Sie, ob E-Mail-Benachrichtigungen mit der eingestellten Häufigkeit verschickt werden.



## Kapitel 4

# Betriebsanleitung

Dieses Kapitel erläutert, wie Sie den Signavio Process Manager betreiben können.

### 4.1 Als Nutzer auf den Signavio Process Manager zugreifen

Sie können mit jedem Browser auf den Signavio Process Manager zugreifen. Unter <http://www.signavio.com/de/browser-compatibility/> finden Sie eine Liste aller unterstützten Browser.

Falls Sie beim Zugriff auf den Signavio Process Managers auf Probleme stoßen, überprüfen Sie die Netzwerk- und Proxy-Einstellungen Ihres Browsers.

Für den Zugriff auf Inhalte ist die Eingabe der E-Mail-Adresse und des Passworts eines zuvor registrierten Nutzers notwendig.

Bei der Verwendung des Collaboration Hub ohne die Single-Sign-On Funktion können in jedem Browser die zuvor veröffentlichten Diagramme betrachtet werden, von dem aus der Signavio Server erreichbar ist. Wenn Personen, Gruppen oder ganze Unternehmensbereiche die veröffentlichten Diagramme im Collaboration Hub nicht sehen sollen, muss der Zugriff auf Netzwerkebene verhindert werden.

Bei der Nutzung der Single-Sign-On-Funktion des Collaboration Hubs haben hingegen die Nutzer des Signavio Process Managers die Möglichkeit, auf Basis eines Active Directorys detailliert einzustellen, für welche Personen bzw. Gruppen ein Diagramm veröffentlicht wird.

### 4.2 Datenbackups durchführen

Um eine sichere Wiederherstellung sämtlicher Repository-Daten zu gewährleisten, genügt ein Backup sämtlicher in der Datenbank befindlicher Daten aus.

Die folgenden Objekte werden nicht in der Datenbank gespeichert:

- der Suchindex (der automatisch generiert wird, sobald der Tomcat neu gestartet wird),
- Nutzer-Sessions (dies bedeutet, dass sich Nutzer nach einem Re-Deployment des Tomcats neu einloggen müssen).

Je nach Datenbanksystem und bereits vorhandener Infrastruktur kann für das Datenbank-Backup auf bestehende Backup-Strategien zurückgegriffen werden. Wir empfehlen mindestens ein tägliches Backup sowie eine rotierende Backup-Strategie, die auch Monats-Backups vorhält.

Die Backups sollten auf separater Hardware an einem separaten Ort oder auf externen Medien möglichst feuerschutzgehalten werden.



## 4.3 Typische Störfälle

Dieser Abschnitt zeigt die häufigsten Ursachen für eine Beeinträchtigung des täglichen Betriebs und mögliche Lösungsansätze:

**Der Tomcat-Server oder das Datenbanksystem werden nach Wartungsarbeiten nicht wieder hochgefahren.**

Versuchen Sie, sich jedes Mal nach den Wartungsaktivitäten anzumelden, um zu überprüfen, ob das System ordnungsgemäß gestartet wurde.

**Der Datenbank steht nicht genügend Festplattenspeicherkapazität zur Verfügung.** Sie können mit ca. 1 MB Brutto-Platzbedarf pro Diagrammrevision rechnen. Wird ein Diagramm also 10-mal abgespeichert, werden 10 MB Festplattenplatz verbraucht. Wir empfehlen, den Festplattenplatz großzügig zu kalkulieren sowie auf Betriebssystem-Ebene eine Monitoring-Funktion einzurichten, der bei knappem Festplattenplatz eine Benachrichtigung an den Administrator ausgibt.

**Der Tomcat-Server hat nicht genügend Arbeitsspeicher zugewiesen bekommen.** Dies zeigt sich durch Verzögerungen und lange Ladezeiten - es können sogar `OutOfMemoryExceptions` auftreten und der Tomcat kann abstürzen. Weisen Sie dem Tomcat mehr Arbeitsspeicher zu. Lesen Sie hierzu das Kapitel *Den Webserver konfigurieren* (Seite 12).

**Wenn man die URL des Signavio Servers in einem Browser öffnet, wird man auf localhost weitergeleitet.**

Die Konfiguration wurde nicht übernommen. Stellen Sie sicher, dass Sie die Installationsanweisungen korrekt befolgt haben und starten Sie den Apache Tomcat-Server neu.

**In der Benutzeroberfläche des Signavio Process Managers oder in den verschiedenen Diagrammexportformaten**

Der Apache Tomcat benutzt nicht UTF-8 als Kodierung. Bitte überprüfen Sie die Konfiguration des Betriebssystems, der Datenbank und des Webservers (siehe Installationsanweisungen).

**Es werden keine Benachrichtigungs-E-Mails versendet.** Überprüfen Sie die SMTP-Konfiguration des Servers (siehe Installationsanweisungen).

**Benachrichtigungs-E-Mails aus dem Signavio System kommen bei Empfängern innerhalb Ihres Netzwerks/Unternehmens**

Eine Einstellung am E-Mail-Server verhindert das Versenden von E-Mails an externe Empfänger (Relay Einstellungen). Dies ist bei vielen E-Mail-Servern für anonyme Zugriffe (bei einer Konfiguration ohne Benutzernamen und Passwort) als Standardeinstellung konfiguriert. Bitte wenden Sie sich an den für den E-Mail-Server zuständigen Administrator.

**Tomcat Server startet nicht korrekt und gibt im Log 'Waiting for changelog lock...' aus.** Wenn zuvor der Tomcat Server auf Grund eines Fehlers während der Initialisierung abgebrochen wurde (weil beispielsweise dem Tomcat-Server zu wenig Arbeitsspeicher zugewiesen wurde), dann kann es passieren, dass dieser Fehler auftritt. Um den Fehler zu beheben, stoppen Sie zuerst den Tomcat-Server. Melden Sie sich anschließend an der Datenbank an und öffnen Sie die Tabelle `DatabaseChangelogLock`. Die Tabelle enthält in der Regel eine Zeile. Setzen Sie in dieser Zeile den Wert der Spalte `LOCKED` von 1 auf 0. Starten Sie anschließend den Tomcat-Server.

**Sehr große Diagramme können nicht abgespeichert werden** Standardmäßig unterstützt der Tomcat das Abspeichern von sehr großen Diagrammen (> 2 MB text-basiertes Datenformat) nicht. Sie können diese Begrenzung erhöhen, indem Sie die `maxPostSize`-Eigenschaft des Konnektors in der `server.xml`-Datei des Tomcats setzen. Lesen Sie mehr unter *Den Webserver konfigurieren* (Seite 12).

**Einige Features funktionieren nicht wie erwartet.**

- Die Suche nach Diagrammen und Glossareinträgen gibt keine Ergebnisse zurück.
- Im Glossar werden keine Einträge angezeigt.
- Diagramme können nicht als PNG exportiert werden und die Diagrammvorschau im Explorer zeigt kein Diagramm an, der Collaboration Hub zeigt keine grafische Darstellung an und auch in der Simulation und dem Diagrammvergleich wird keine grafische Darstellung angezeigt.
- Die BPMN-Simulation kann nicht ausgeführt werden.
- Es werden keine täglichen E-Mail-Benachrichtigungen verschickt.



Die verschiedenen Funktionen werden von verschiedenen Web Services bereitgestellt, die über HTTP(S) kommunizieren. Für eine reibungslose Kommunikation ist es erforderlich, dass die JVM-Instanz das verwendete Zertifikat akzeptiert. Wenn Sie einen oder mehrere dieser Effekte beobachten, überprüfen Sie bitte die Tomcat-Protokolldateien. Die Fehlermeldungen enthalten Hinweise auf das Problem.

## 4.4 Den Server warten

Wenn Wartungsarbeiten am Server durchgeführt werden müssen und diese ein Herunterfahren des Systems erfordern, berücksichtigen Sie bitte die folgenden Punkte:

### 4.4.1 Informieren Sie Ihre Nutzer

Wenn Wartungsarbeiten am Server durchgeführt werden müssen und diese ein Herunterfahren des Systems erfordern, weisen Sie alle Nutzer rechtzeitig darauf hin, dass der Signavio Process Manager für eine bestimmte Zeit nicht erreichbar ist.

Arbeitsbereichsadministratoren des Signavio Process Managers können in der Nutzerverwaltung eine Liste der Emailadressen aller auf dem System registrierten Nutzer abrufen. Mit Hilfe dieser Liste können Sie eine E-Mail an alle Nutzer des Systems senden.

### 4.4.2 Die Datenbank im Falle eines Neustarts richtig verwalten

Der Signavio Process Manager arbeitet nur auf Datenbanksystemen, die Transaktionen unterstützen.

Grundsätzlich kann daher das Signavio System zu jeder Zeit heruntergefahren werden, ohne in Gefahr zu laufen, einen inkonsistenten Zustand in der Datenbank zu erzeugen. Ausgenommen ist jedoch die Initialisierungsphase beim Starten des Tomcats, da hier Operationen auf der Datenbank ausgeführt werden, die nicht auf allen Datenbanksystemen innerhalb einer Transaktion ablaufen. Sie sollten daher unbedingt vermeiden, während der Startphase des Tomcat Servers den Tomcat Prozess zu stoppen. Wenn Wartungsarbeiten am Datenbankserver erfordern, dass das Datenbanksystem heruntergefahren werden muss, dann muss **zuvor** der **Tomcat Server heruntergefahren** werden.

### 4.4.3 Nutzer-Sessions während eines Restart verwalten

Bei einem Neustart des Tomcat Servers bleiben die User Sessions erhalten, so dass die aktuell angemeldeten Nutzer angemeldet bleiben. Beim Herunterfahren des Tomcat Servers werden die Sessions in eine Datei innerhalb des Tomcat Servers gespeichert (bei Standardkonfiguration finden Sie die Datei unter `$TOMCAT_DIR/work/Catalina/localhost/_/SESSIONS.ser`). Diese Datei wird beim Hochfahren wieder ausgelesen. Ist die Unterbrechung nur sehr kurz, bekommen die zurzeit angemeldeten Nutzer unter Umständen gar nicht mit, dass der Server kurzzeitig nicht erreichbar war. Hat ein Nutzer aber beispielsweise genau in dieser Zeit versucht, ein Diagramm abzuspeichern, so wird dem Nutzer ein Fehler angezeigt. Sobald der Tomcat Server wieder hochgefahren ist, kann der Nutzer allerdings den Speichervorgang wiederholen und das Diagramm abspeichern.

## 4.5 Monitoring

Um eine hohe Verfügbarkeit zu gewährleisten, sollten Sie sowohl den Datenbankserver als auch den Apache Tomcat Server überwachen. Beim Datenbankserver ist vor allem darauf zu achten, dass genügend freier Festplattenspeicher zur Verfügung steht. Richten Sie am Besten auf dem Datenbankserver eine Benachrichtigung an den zuständigen Administrator ein, wenn der freie Speicher zur Neige geht oder ein Problem beim Erstellen der Datenbank-Backups auftritt. Falls Anfragen an



den Signavio Process Manager nur mit einer hohen Latenz beantwortet werden, lassen Sie bitte von einem Datenbank-Administrator die Konfiguration der Datenbank überprüfen (beispielsweise, ob die Datenbank-Caches korrekt konfiguriert sind oder ob bei jeder Anfrage die Daten von der Festplatte gelesen werden müssen).

Die grundsätzliche Erreichbarkeit des Apache Tomcat-Servers kann einfach dadurch überprüft werden, dass Sie eine HTTP-Anfrage an den Server senden und sich im Signavio System anmelden. Zusätzlich sollte der Tomcat-Prozess selbst sowie der Arbeitsspeicherverbrauch des Tomcat-Prozesses überwacht werden. Wenn der Tomcat-Prozess auf den Swap-Bereich zugreifen und Teile des Arbeitsspeichers auf die Festplatte auslagern muss, wird das System sehr träge und antwortet sehr langsam. Daher sollte dies auf jeden Fall vermieden werden.

## 4.6 Das Datenbank- oder Betriebssystem aktualisieren

Der Signavio-Server verwendet JDBC und Apache Tomcat, um vom Datenbank- und Betriebssystem zu abstrahieren.

Daher sollte das Einspielen von Patches im Regelfall zu keiner Beeinträchtigung im Betrieb des Signavio-Systems führen und keine Hilfe vom Signavio Support-Team benötigen.

Stellen Sie vor einem Update jedoch sicher, dass das gewünschte Datenbank- oder Betriebssystem unterstützt wird.

---

**Wichtig:** Sichern Sie vor dem Update Ihre Daten. Beachten Sie, dass vor dem Herunterfahren des Datenbanksystems der Tomcat-Server heruntergefahren werden muss.

---

## 4.7 Den Server auf neue Hardware umziehen

Der Umzug auf andere Hardware ist grundsätzlich unproblematisch. Um den Signavio Process Manager auf andere Webserver-Hardware umzuziehen, ist es lediglich nötig, die Konfiguration auf das neue System zu übertragen. Stellen Sie außerdem sicher, dass sämtliche Fremdsysteme (Mailserver, Datenbank, Active Directory, SharePoint, etc.) vom neuen Server aus erreichbar sind.

---

**Wichtig:** Sichern Sie vor einem Umzug Ihre Daten und stoppen Sie den Tomcat-Server, bevor Sie den Datenbank-Server herunterfahren.

---



## Kapitel 5

# Updateanleitung für den Signavio Process Manager

---

### Wichtig:

- Falls Sie eine MS SQL-Datenbank verwenden und vom Signavio Process Manager Version 10.x oder niedriger zu Version 11.x oder höher updaten, folgen Sie den Anweisungen unter *Den JDBC-Treiber für Microsoft-SQL-Server-Datenbanken herunterladen* (Seite 19), um den neuen JDBC-Treiber herunterzuladen und zu installieren. **Löschen Sie die alte Treiberdatei** `sqljdbc4.jar`, welche Sie im `lib`-Verzeichnis des Tomcats finden.
- Falls Sie eine Oracle-Datenbank verwenden und von einer 9.x-Version auf eine 10.x-Version oder neuer updaten, laden Sie bitte den neuen Oracle JDBC-Treiber wie unter *Den JDBC-Treiber für Oracle Datenbanken herunterladen* (Seite 19) beschrieben, herunter und ersetzen Sie den alten Treiber mit den heruntergeladenen Dateien.
- Falls Sie Signavio Process Manager mit Freigabe-Workflows verwenden, stellen Sie bei der Installation sicher, dass die zu installierende Version von Signavio Process Manager mit der Signavio Workflow Accelerator-Version, die Sie verwenden, kompatibel ist. Eine Kompatibilitätsliste finden Sie im 'Workflow Accelerator-Administratorenhandbuch' <<https://docs.signavio.com/adminguide/workflow/en/signavio.html#compatibility-list>>'. Um Probleme mit bestimmten Funktionen zu vermeiden, stellen Sie sicher, dass Signavio Workflow Accelerator während des Updates von Signavio Process Manager nicht verwendet wird (und vice versa).

---

Dieses Kapitel beschreibt das Einspielen eines Updates für Signavio Process Manager. Voraussetzung ist, dass Ihnen das Update als ZIP-Archiv zur Verfügung gestellt wurde.

**Stellen Sie bitte sicher, dass während des Einspielens des Updates das Signavio System nicht in Benutzung ist.**

1. Stoppen Sie den Apache Tomcat-Server.
2. Erstellen Sie eine Sicherung der Datenbank und der aktuellen Programmdateien. Sie finden die Programmdateien im Deployment-Ordner (`webapps`) des Apache Tomcat-Verzeichnisses. Sie könnten ebenso die Ordner `work` und `conf/Catalina` des Tomcat säubern.
3. **Falls Sie ein Update von Version 8.6.0 oder älter vornehmen**, folgen Sie zusätzlich den Anweisungen im Kapitel *JDBC-Treiber installieren*.
4. Kopieren Sie das Update-Archiv `SignavioEnterpriseX.X.X.zip` auf den Server.
5. Entpacken Sie das ZIP-Archiv. Das Archiv enthält das Verzeichnis `files`, in dem die neuen Programmdateien liegen.
6. **Falls Sie ein Update von einer Version, die älter ist als 9.7.0 vornehmen**, kopieren Sie die Konfigurationsdateien sowie die Lizenzdatei zu den neuen Installationsdateien. Die





Dateien müssen aus verschiedenen Verzeichnissen des Tomcats in den Ordner `conf` des Root-Verzeichnisses des Tomcats kopiert werden. In den folgenden Anweisungen wird das Root-Verzeichnis des Tomcats mit der Variablen `$TOMCAT_DIR` dargestellt. Der Zielordner ist entsprechend `$TOMCAT_DIR/conf`.

**Kopieren Sie die folgenden Dateien nach `$TOMCAT_DIR/conf`:**

- `$TOMCAT_DIR/webapps/ROOT/WEB-INF/classes/configuration.xml`
- `$TOMCAT_DIR/webapps/ROOT/WEB-INF/classes/configuration_signed.xml`

Falls vorhanden:

- `$TOMCAT_DIR/webapps/ROOT/WEB-INF/classes/simulation.xml`

Falls vorhanden und falls Sie HTTPS verwenden, kopieren Sie die folgende Datei, die Sie **nach dem Einspielen der neuen Dateien** wieder einfügen:

- `$TOMCAT_DIR/webapps/solr/META-INF/context.xml`

Zudem ist es notwendig, die entsprechenden Dateipfade unter `$TOMCAT_DIR/conf` in der Datei `context.xml` innerhalb des `<Context>`-Tags wie folgt zu definieren:

```
<Parameter name="configfile" value="{catalina.base}/conf/configuration.xml" />
<Parameter name="licensefile" value="{catalina.base}/conf/configuration_signed.xml" />
<Parameter name="configfile.simulation" value="{catalina.base}/conf/simulation.xml" />
```

7. Löschen Sie die alten Programmdateien aus `$TOMCAT_DIR/webapps`.
8. Verschieben Sie die neuen Programmdateien aus dem Verzeichnis `files` nach `$TOMCAT_DIR/webapps`. Überprüfen Sie, ob der Systemnutzer, der den Tomcat ausführt, Zugriff auf die soeben kopierten Dateien hat. Falls dies nicht der Fall ist, passen Sie die entsprechenden Berechtigungen an.
9. Starten Sie den Apache Tomcat-Server.

**Wichtig:** Stoppen Sie den Tomcat-Server niemals, solange Datenmigrationen im Zuge eines Versionsupdates laufen, selbst wenn Konfigurationsfehler vorliegen, die das Verwenden von Teilen der Anwendung verhindern. Ob eine Datenmigration läuft, können Sie in den Logs des Tomcats überprüfen. Wenn Sie einen Tomcat-Cluster verwenden, starten Sie nur einen der Tomcat-Server und warten Sie, bis alle Migrationen abgeschlossen sind.

10. Verwenden Sie das *Diagnostics-Tool* (Seite 22), um sicherzustellen, dass das System korrekt konfiguriert ist.
11. Löschen Sie das Archiv `SignavioEnterpriseX.X.X.zip` sowie den Ordner `SignavioEnterpriseX.X.X`.

Falls das Update nicht eingespielt werden kann, ersetzen Sie die Datenbank durch die Sicherung sowie die Programmdateien und Suchindexdateien, um mit dem alten System weiterarbeiten zu können.

**Hinweis:** Ab der Version 8.3.0 wird nach jedem Update (nicht nach jedem Neustart, nur nach einem Versionsupdate) der Suchindex neu generiert. Dies kann je nach Datenmenge einige Minuten dauern. Beachten Sie insbesondere, dass im Glossar kein Inhalt angezeigt wird, bis der Suchindex neu erstellt wurde.



## Kapitel 6

# Die Lizenzdatei austauschen

Sollte es erforderlich werden die Lizenzdatei auszutauschen (z. B. nach Buchung weiterer Nutzer, oder nach Zustellung einer neuen Lizenz bei einer On-Premise Edition), folgen Sie den Anweisungen in diesem Artikel.

---

**Wichtig:** Erstellen Sie vor dem Austausch ein **Backup der Datenbank**, da es zu irreversiblen Anpassungen in der Datenbank kommen kann.

---

1. Stoppen Sie den Apache Tomcat-Server.
2. Navigieren Sie in das Verzeichnis `$TOMCAT_DIR/conf/`.
3. Sichern Sie die alte Lizenzdatei `configuration_signed.xml`.
4. Kopieren Sie die neue Lizenzdatei in das Verzeichnis.
5. Starten Sie den Tomcat-Server neu.



## Kapitel 7

# Den Signavio Process Manager als Nutzer konfigurieren

Der Signavio Process Manager bietet Ihnen umfangreiche Konfigurationsmöglichkeiten, um das System an die individuellen Anforderungen Ihrer Organisation anzupassen.

Detaillierte Anweisungen bezüglich der Konfiguration des Systems über das User Interface durch einen *Arbeitsbereichsadministrator* finden Sie unter [https://editor.signavio.com/userguide/de/workspace\\_admin/index.html](https://editor.signavio.com/userguide/de/workspace_admin/index.html).



## Kapitel 8

# Support

Falls Sie Probleme bei der Installation des Signavio Process Managers bzw. beim Einspielen des Updates haben oder im laufenden Betrieb Probleme auftreten, sichern Sie bitte die Logdatei des Tomcat-Servers und senden Sie die Logdatei, zusammen mit anderen Probleminformationen, an den Signavio Support.

**Kundenportal** unter: <http://support.signavio.com/>

Sie erreichen den Support per **E-Mail** unter: [support@signavio.com](mailto:support@signavio.com)

oder **telefonisch** unter: 030 / 856 21 54 – 21 (Mo - Fr, 9 - 17Uhr)