

Installation Guide

# **daccord User Frontend**

Version 1.6

## Ihr Kontakt

**G+H Netzwerk-Design**  
**Gesellschaft für IT Consulting mbH**

Ludwigstraße 8  
63067 Offenbach am Main  
Deutschland

Telefon: +49 (0) 69 85 00 02 -0

Fax: +49 (0) 69 85 00 02 -51

Email: [info@netzwerk-design.de](mailto:info@netzwerk-design.de)

Web: [www.netzwerk-design.de](http://www.netzwerk-design.de)

## Versionsnachweis

Dieses Dokument wird von der G+H Netzwerk-Design gepflegt und fortlaufend aktualisiert. Größere Änderungen an Inhalt und Umfang führen zu einer neuen Versionsnummer. Die folgende Liste gibt die Historie dieses Dokumentes wieder.

Version	Datum	Author	Änderungsgrund
0.5	08.07.2013	Sebastian Kornblueh	Initial Version
1.0	12.09.2013	Sebastian Kornblueh	Finale Version
1.5	30.04.2014	Kevin Bauer und Thomas Gertler	Kompatibilität zu daccord Version 1.5
1.6	18.12.2015	Rene Leitz und Thomas Gertler	Kompatibilität zu daccord Version 1.6

Tabelle 1: Versionsübersicht

## Rechtliche Hinweise

Die G+H Netzwerk-Design leistet keinerlei Gewähr bezüglich des Inhaltes oder Gebrauchs dieser Dokumentation. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Die G+H Netzwerk-Design behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt die G+H Netzwerk-Design für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich die G+H Netzwerk-Design das Recht vor, G+H Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für die G+H Netzwerk-Design die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Copyright © MySQL ist ein Produkt der Oracle Corporation, 500 Oracle Parkway, Redwood Shores, CA 94065, USA

Copyright © Java ist ein Produkt der Oracle Corporation, 500 Oracle Parkway, Redwood Shores, CA 94065, USA

Copyright © SUSE Linux Enterprise Server ist ein Produkt der SUSE Linux GmbH, Maxfeldstr. 5 D-90409 Nürnberg

Copyright © Red Hat ist ein Produkt der Red Hat, Inc., 100 East Davie St, Raleigh, NC 27601, USA

Copyright © daccord ist ein Produkt der G+H Netzwerk-Design Gesellschaft für IT Consulting mbH.

Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>6</b>
<b>2</b>	<b>Vorraussetzungen</b>	<b>7</b>
<b>3</b>	<b>Installations- und Konfigurationsprozess</b>	<b>8</b>
3.1	Ausführen des Installationsscripts . . . . .	8
3.2	Konfiguration . . . . .	9
3.2.1	Basiskonfiguration . . . . .	10
3.2.2	Frontendkonfiguration . . . . .	11
3.2.3	Autorisierungskonfiguration . . . . .	12
3.2.4	Konfiguration der Zusatzmodule . . . . .	13
3.2.5	Abschluss der Konfiguration . . . . .	13
<b>4</b>	<b>Betrieb</b>	<b>14</b>
4.1	Starten . . . . .	14
4.2	Stoppen . . . . .	14
4.3	Deinstallieren . . . . .	14
4.4	Log-Datei . . . . .	14
4.4.1	Installation Log-Datei . . . . .	14
4.4.2	daccord User Frontend Log-Datei . . . . .	14
4.4.3	daccord User Frontend Engine Log-Datei . . . . .	15
<b>5</b>	<b>Appendix</b>	<b>16</b>
5.1	Manuelle Zuweisung einer JVM (Java Virtual Machine) . . . . .	16
5.2	Erweiterung des Java-Speichers . . . . .	16
5.3	Aktivieren von HTTPS . . . . .	17
5.4	Einbinden von Zertifikaten . . . . .	17
5.4.1	Einrichten von Tomcat zur Nutzung eines neuen öffentlichen Zertifikates . . . . .	17
5.5	Automatische Weiterleitung von HTTP zu HTTPS . . . . .	19
5.6	Anzeige von jexec is broken . . . . .	19
<b>6</b>	<b>FAQ</b>	<b>21</b>
6.1	daccord User Frontend startet nicht . . . . .	21

# 1 Einleitung

Das webbasierte daccord User Frontend dient dem Endanwender zum Zugriff auf die Informationen zu Benutzern und Berechtigungen aus den angeschlossenen Systemen. Je nach Konfiguration des daccord User Frontends, individueller Berechtigung sowie Zuordnung innerhalb des daccord Systems werden ihm die Informationen in folgenden Kategorien dargestellt:

1. Meine Benutzerkonten - Der Anwender erhält eine Darstellung seiner Benutzerkonten und deren Berechtigungen in den verschiedenen Systemen.
2. Meine Rollen - Der Anwender erhält eine Übersicht der Rollen, denen er zugeordnet ist, die Berechtigungen die er aufgrund der Zuordnung haben sollte, sowie eine Darstellung der Abweichungen von seinen realen Berechtigungen.
3. Meine Historie - Der Anwender erhält die Möglichkeit sich die Veränderung in den Systemen anzeigen zu lassen. In verschiedenen Übersichten werden dem Anwender die Vorgänge die seine eigene Person, die eigenen Benutzerkonten und Berechtigungen betreffen, sowie die Vorgänge die er initiiert oder in die er involviert war, dargestellt.
4. Personen - Der Anwender erhält eine Darsteller aller Personen, die ihm zugeordnet sind, sowie deren Benutzerkonten und Berechtigungen.
5. Systeme - Der Anwender erhält eine Darstellung aller Benutzerkonten und Berechtigungen für die Systeme, für die er als Verantwortlicher definiert wurde.
6. Berechtigungen - Der Anwender erhält eine Darstellung der Berechtigungen, für die er als Verantwortlicher definiert wurde. Er kann die Inhaber der Berechtigung einsehen und die Korrektheit der Zuordnung bestätigen.

Dieser Guide soll Sie dabei unterstützen das daccord User Frontend 1.6 zu installieren und zu konfigurieren.

**Hinweis:** Bitte beachten Sie, dass diese Dokumentation sich auf die Installation des daccord User Frontends auf einem manuell vorbereiteten Server bezieht. Für die Installation des daccord User Frontends auf Basis der daccord Appliance ist eine separate Dokumentation verfügbar.

Mehr zum daccord System erfahren Sie hier:

<http://www.daccord.de>

## 2 Voraussetzungen

**Hinweis:** Damit die Installation des daccord User Frontends erfolgreich sein kann, stellen Sie sicher, dass zuvor das daccord Admin Frontend installiert wurde und somit bereits eine daccord Umgebung vorhanden ist. Halten Sie den Decryption Hash, welchen Sie bei der Installation des daccord Admin Frontends vergeben haben bereit, da dieser bei der Konfiguration des daccord User Frontends erneut benötigt wird.

Bevor Sie mit der Installation beginnen können, stellen Sie sicher, dass Sie die folgenden Schritte ausgeführt haben:

1. Laden Sie die ZIP-Datei aus dem Kundencenter der daccord Website > Kundencenter > Downloads herunter. Die notwendigen Zugangsdaten erhalten Sie von Ihrem Vertriebskontakt.
2. Übertragen Sie die Datei auf den vorgesehenen Server in ein dediziertes Verzeichnis (z.B. /software)
3. Entpacken Sie nun die ZIP-Datei mit dem folgenden Befehl:

```
unzip dateiname.zip -d /Zielverzeichnis
```

Zur Installation des daccord User Frontends wird entweder ein dedizierter Server oder eine virtuelle Instanz eines Servers benötigt. Folgende Systemvoraussetzung sind zur Installation des daccord User Frontends zu erfüllen:

Hardware	Speichermenge in MB
Hauptspeicher (RAM)	min. 512
freier Festplattenplatz	min. 3 - 4

Tabelle 2: Hardwarevoraussetzungen

Betriebssystem	Version
SUSE Linux Enterprise Server (SLES)	11
OpenSUSE	13
Red Hat (64Bit)	Kernel min. v2.6.27

Tabelle 3: Betriebssystemvoraussetzungen

Software	Version
Java	min. v1.5
Bash	min. v3.2.39
RPM	min. v4.4.2.3

Tabelle 4: Softwarevoraussetzungen

Sie können nun mit der Installation des daccord User Frontends, wie im nächsten Kapitel beschrieben, beginnen.

**Hinweis:** Das Paket enthält neben dem daccord User Frontend weitere Komponenten, die mit dem Installationsscript installiert werden können.

### 3 Installations- und Konfigurationsprozess

In diesem Kapitel erhalten Sie einen Überblick über den daccord User Frontend Installations- und Konfigurationsprozess.

In ihrem Zielverzeichnis finden Sie neben dem Installationskript (install.sh), RPM Pakete, die über das Installationsscript installiert werden.

#### 3.1 Ausführen des Installationsscripts

Um das Installationsskript auszuführen, stellen Sie sicher, dass Sie sich im Installationspfad befinden, in dem das Installationsskript abgelegt ist. Geben Sie `./install.sh` ein um das Installationsskript zu starten.

**Hinweis:** Innerhalb der eckigen Klammern finden Sie stets die default Einstellungen für den jeweiligen Parameter, welchen Sie über die Enter-Taste übernehmen können.

Nachdem Sie Ihre Eingabe mit der Enter-Taste bestätigt haben, werden Sie dazu aufgefordert die Lizenzbestimmungen zu akzeptieren. Geben Sie „y“ ein um diese zu akzeptieren und bestätigen Sie die Eingabe mit der Enter-Taste um mit der Installation fortzufahren.

Geben Sie die „3“ zur Auswahl des daccord User Frontends ein, um die weiteren Installationsschritte auszuführen.

```
[1] Admin Frontend (installed and running)
[2] Collector Engine (not installed)
[3] User Frontend (not installed)
[4] Notification Engine (not installed)
[v] View the logfile!
[q] Quit

Please select the component by entering the corresponding number/letter! [1/2/3/4/v/q]
```

Das System weist Sie nun darauf hin, dass es mit der Installation des daccord User Frontends beginnen möchte. Geben Sie „yes“ ein um die Installation zu beginnen oder geben Sie „quit“ ein um die Installation abzubrechen.

```
daccord User Frontend will be installed on this system!
Type [yes] to continue, or [quit] to go back! [yes/quit]
```

Geben Sie „yes“ ein um fortzufahren.

Im nächsten Schritt werden Sie durch das Skript dazu aufgefordert den DNS-Namen oder die IP-Adresse des daccord Servers anzugeben.

```
Please enter the DNS name or IP address of the daccord server:
```

Dabei muss es sich um die IP Adresse oder die DNS Bezeichnung handeln, über die der Server innerhalb Ihrer IT-Infrastruktur erreichbar ist.

**Hinweis:** Für diesen Parameter ist „localhost“ kein gültiger Wert.

Sie werden nun aufgefordert den Port zu bestimmen, über den das Frontend erreichbar sein soll.

```
Please enter the port for the http connection: [80]
```

Anschließend fordert Sie das Installationskript auf einen Verification-Code einzugeben.

```
Please enter the verification code to restrict the access to the configuration page:
```

Der „Verification Code“ dient der Sicherheit Ihrer daccord Installation und verhindert, dass Unberechtigte auf das webasierte Konfigurationsfrontend zugreifen können. Der Code kann aus Ziffern und Zeichen bestehen. Ausgenommen sind jedoch Sonderzeichen.

**Hinweis:** Der Standart Verification Code ist „1234567890“

Das daccord User Frontend wird nun auf Ihrem System installiert.

```
daccord User Frontend has been installed successfully!
```

```
To finalize your installation please configure the component with the corresponding web-based wizard!
```

```
User Frontend configuration wizard:
```

```
http://servername:port/user/admin.html?command=getConfig  
&verificationCode=1234567890&style=admin
```

Die Installation auf dem Server wurde nun erfolgreich abgeschlossen. Um die abschließenden Konfigurationseinstellungen vorzunehmen, starten Sie einen Webbrowser und geben Sie die generierte URL ein.

**Hinweis:** Sollten bei der Installation Probleme auftreten, finden Sie einige Hinweise zu möglichen Problemlösungen im Kapitel Troubleshooting.

## 3.2 Konfiguration

Sie haben daccord erfolgreich installiert. Nun müssen Konfigurationseinstellungen vorgenommen werden, damit Sie das daccord User Frontend nutzen können. Ein Konfigurationswizard wird Sie durch die einzelnen Konfigurationsschritte leiten. Dieses Kapitel soll Ihnen einen Überblick über die einzelnen Konfigurationsoptionen geben.

**Hinweis:** Die Konfiguration des daccord User Frontends können sie jederzeit unter folgender URL vornehmen:

```
HTTP(S)://SERVERIP:PORT/user/admin.html?command=getConfig  
&verificationCode=[VERIFICATIONCODE]&style=admin
```

### 3.2.1 Basiskonfiguration

Während der Installation haben Sie bereits einige der Einstellungsparameter eingegeben, welche automatisch übernommen wurden. Bei Bedarf haben Sie die Möglichkeit diese Einstellungen zu überarbeiten.

Parameter	Beschreibung
Engine Protokoll	Netzwerkprotokoll des daccord User Frontends. <i>Hinweis: http oder https</i>
Engine Host	Hostname oder IP des daccord User Frontends. <i>Hinweis: „localhost“ ist kein gültiger Wert.</i>
Engine Port	Port des daccord User Frontends.
Decryption Hash	Der Decryption Hash dient zur Verschlüsselung von Passwörtern innerhalb des daccord Systems. <i>Hinweis: Erfragen Sie den Decryption Hash bitte bei Ihrem daccord Administrator.</i>
Verification Code	Der Verification Code dient der Sicherheit Ihrer daccord Installation und verhindert, dass Unberechtigte auf das webasierte Konfigurationsfrontend zugreifen können. <i>Hinweis: Der Code kann aus Ziffern und Zeichen bestehen. Ausgenommen sind jedoch Sonderzeichen.</i>
daccord Datenbank Host	Geben Sie den Hostnamen oder IP des daccord Datenbank Servers ein. <i>Hinweis: Es wird nur eine gültige und in der Version kompatible daccord System Datenbank akzeptiert.</i>
daccord Datenbank Port	Tragen sie den Port des daccord Datenbank Servers ein.
daccord Datenbank Benutzer	Tragen sie den Benutzernamen für den Zugriff auf die daccord Datenbank ein.
daccord Datenbank Passwort	Tragen sie das Passwort für den Zugriff auf die daccord Datenbank ein.

Tabelle 5: Basiskonfiguration

Bestätigen Sie mit „Weiter“ und der Wizard prüft nun, ob mit den eingetragenen Parametern eine Datenbankverbindung aufgebaut werden kann. Sollte keine Verbindung zur System Datenbank aufgebaut werden können, wird ein entsprechender Hinweis links vom „Weiter“-Button eingeblendet.

Konnte der Wizard eine Verbindung zur Systemdatenbank aufbauen, leitet Sie der Wizard zum nächsten Konfigurationspunkt weiter.

### 3.2.2 Frontendkonfiguration

In diesem Schritt haben Sie die Möglichkeit die notwendigen Parameter zur Konfiguration des daccord User Frontend einzutragen.

Parameter	Beschreibung
Verfügbare Frontends	<p>Wählen Sie hier aus, ob Sie eine bereits existierende Frontendkonfiguration verwenden möchten, oder definieren Sie eine neue.</p> <p><i>Hinweis: Wenn sie ein vorhandenes Frontend aktualisiert haben oder durch eine Neuinstallation ersetzen wollen, dann wählen Sie hier ein vorhandenes Frontend aus, um die Konfiguration zu übernehmen. Alternativ können Sie ein neues Frontend konfigurieren.</i></p>
Name	Geben Sie an dieser Stelle den Namen des daccord User Frontends an.
Beschreibung	Geben Sie eine detaillierte Beschreibung des daccord User Frontends ein.
Datenbank ID	<p>Auswahl der Datenbank des daccord User Frontends.</p> <p><i>Hinweis: Die Datenbank muss vorher über das daccord Admin Frontend angelegt worden sein. Es wird nur eine gültige und in der Version Kompatible daccord Daten Datenbank akzeptiert.</i></p>
Log Level	<p>Auswahl des Log Levels des daccord User Frontends.</p> <p><i>Hinweis: Wählen Sie „Debugging“ zum Aufspüren von Fehlern, „Info“ für allgemeine Informationen wie Programmstart und Verbindungsaufbau und „Error“ um Fehler wie das Abfangen von Ausnahmen anzuzeigen.</i></p>
Datenbank Debugging	Der Parameter Datenbank Debugging wird zum Analysieren der Datenbankperformance verwendet und sollte im Normalfall deaktiviert sein.
Session Timeout	Der Session Timeout legt fest nach wie vielen Minuten eine Session ausläuft. Der Standardwert beträgt 30 Minuten.
Hierarchy Depth	<p>Über diese Einstellung legen Sie fest über wie viele Hierarchieebenen in der Ansicht „Personen“ die Informationen maximal kaskadiert werden sollen.</p> <p>Beispiel: Bei dem Hierarchiewert „2“ bekommt die angemeldete Person sowohl die ihm zugewiesenen Personen, als auch deren Personenzuweisungen angezeigt.</p>

Tabelle 6: Frontendkonfiguration

Bestätigen Sie mit „Weiter“ und der Wizard prüft nun, ob mit den eingetragenen Parametern eine Datenbankverbindung aufgebaut werden kann. Sollte keine Verbindung zur daccord Datenbank aufgebaut werden können, wird ein entsprechender Hinweis links vom „Weiter“-Button eingeblendet.

Konnte der Wizard eine Verbindung zur daccord Datenbank aufbauen, werden die übrigen Parameter gespeichert und der Wizard leitet Sie zum nächsten Konfigurationspunkt weiter.

### 3.2.3 Autorisierungskonfiguration

Für die Autorisierungskonfiguration sind folgende Einstellungen vorzunehmen:

Parameter	Beschreibung
Autorisierungssystem	Geben Sie das zur Benutzer-Autorisierung genutzte System an.  <i>Hinweis: Bevor Sie ein Autorisierungssystem auswählen können, muss zunächst ein System über das Admin Frontend angelegt werden, welches die Daten für die zu autorisierenden User enthält. Über dieses System wird dann die Zuordnung zur „Person“ (natürliche Person) abgeleitet.</i>
Erforderliche Berechtigung	Auswahl einer Berechtigung zum Zugriff auf das daccord User Frontend.  <i>Hinweis: Dieser Parameter bestimmt, welche daccord Rolle eine Benutzer haben muss, um sich am UserFrontend anzumelden. Im Normalfall wählen Sie „Zugang zum User Frontend“.</i>
JDBC Autorisierung Stores	Auswahl einer oder mehrerer Datenbanken gegen die eine Autorisierung vorgenommen werden soll.  <i>Hinweis: Dieser Parameter bestimmt, in welchen Datenbanken daccord interne Benutzer gesucht werden. Im Normalfall wählen Sie die Ihnen angezeigte Datenbank.</i>
LDAP Autorisierung Stores	Auswahl einer oder mehrerer Verzeichnisdienste gegen die eine Autorisierung vorgenommen werden soll.  <i>Hinweis: Dieser Parameter bestimmt, in welchen LDAP Verzeichnissen daccord interne Benutzer gesucht werden. Dieser Schritt ist optional.</i>

Tabelle 7: Autorisierungskonfiguration

Bestätigen Sie mit weiter um zum nächsten Konfigurationsschritt zu gelangen.

*Hinweis: Mit Abschluss des Schrittes 4.2.3 ist die grundlegende Konfiguration des daccord User Frontends/ abgeschlossen. Sie haben die Möglichkeit das daccord User Frontend jetzt direkt neu zu starten um es produktiv nutzen zu können. Alternativ können Sie vor der Produktivnahme die optionalen Module konfigurieren.*

### 3.2.4 Konfiguration der Zusatzmodule

Sie haben die Möglichkeit innerhalb von daccord unterschiedliche Module zu benutzen. Über die Zusatzmodule können zusätzliche Funktionalitäten in den Frontends aktiviert oder deaktiviert werden.

Parameter	Beschreibung
„Meine Benutzerkonten“ aktiv.	Aktivieren/Deaktivieren des Moduls „Meine Benutzerkonten“  <i>Hinweis: Mit dieser Einstellung können sie festlegen, ob die Sichtweise „Meine Benutzerkonten“ im daccord User Frontend angezeigt werden soll.</i>
Rollenmodul aktivieren	Aktivieren / Deaktivieren des Rollenmoduls  <i>Hinweis: Mit dem Rollenmodul erhält der Anwender eine Übersicht der Rollen, denen er zugeordnet ist, die Berechtigungen die er aufgrund der Zuordnung haben sollte, sowie eine Darstellung der Abweichungen von seinen realen Berechtigungen.</i>
Antragssmodul aktivieren	Aktivieren / Deaktivieren des Antragssmoduls  <i>Hinweis: Mit diesem Modul erhält der Anwender die Möglichkeit Aktivitäten aus den Frontends zu initiieren.</i>
Re-/Zertifizierungsmodul aktivieren	Aktivieren / Deaktivieren des Re-/Zertifizierungsmoduls  <i>Hinweis: Mit diesem Modul erhält der Anwender in der Berechtigungsansicht die Möglichkeit die Korrektheit der Zuordnung zu bestätigen.</i>
Historienmodul aktivieren	Aktivieren / Deaktivieren des Historienmoduls  <i>Hinweis: Mit diesem Modul erhält der Anwender die Möglichkeit sich die Veränderung in den Systemen anzeigen zu lassen.</i>
Mitteilungsmodul aktivieren	Aktivieren / Deaktivieren des Mitteilungsmoduls  <i>Hinweis: Mit diesem Modul erhält der Anwender den Zugang zu seiner persönlichen Mitteilungsbox, welche ihn über daccord interne Informationen benachrichtigt.</i>

Tabelle 8: Konfiguration des Zusatzmoduls

Bestätigen Sie mit „Weiter“ um zum abschließenden Konfigurationsschritt zu gelangen.

### 3.2.5 Abschluss der Konfiguration

Sobald die nötigen Konfigurationen abgeschlossen sind, wird das daccord User Frontend neu gestartet.

Nach dem erfolgreichen Neustart, werden Sie zum daccord User Frontend weiter geleitet. Über das daccord Admin Frontend können Sie jederzeit Konfigurationen an den installierten daccord User Frontends vornehmen.

## 4 Betrieb

Sobald das daccord User Frontend installiert ist, können Sie über das Installationsscript das User Frontend starten, stoppen, deinstallieren sowie dessen Log-Dateien einsehen.

```
User Frontend installed and running
```

```
[u] Uninstall the User Frontend
[s] Start/Stop the User Frontend
[v] View User Frontend logfile
[q] Quit
```

### 4.1 Starten

Sie können das daccord User Frontend über das install Script manuell starten. Geben Sie dafür im Menü des daccord User Frontends den Buchstaben „s“ ein.

```
Please select the component by entering the corresponding letter! [u/s/v/q]
```

### 4.2 Stoppen

Sie können das daccord User Frontend über das install Script manuell stoppen. Geben Sie dafür im Menü des daccord User Frontends den Buchstaben „s“ ein.

```
Please select the component by entering the corresponding letter! [u/s/v/q]
```

### 4.3 Deinstallieren

Um das daccord User Frontend zu deinstallieren, geben sie in der Kommandzeile den Buchstaben „u“ ein und drücken sie „Enter“.

```
Please select the component by entering the corresponding letter! [u/s/v/q]
```

*Hinweis: Sobald das daccord User Frontend deinstalliert ist, steht es ihnen nicht mehr zur Verfügung!*

### 4.4 Log-Datei

Um das Verhalten von daccord und des daccord User Frontends analysieren zu können stehen Ihnen drei Log-Dateien zur Verfügung.

#### 4.4.1 Installation Log-Datei

Während der Installation wird eine Log-Datei namens install-daccord.log angelegt, die jeden einzelnen Installationsschritt inklusive der vergebenen Werte aufzeichnet. Sollten bei der Installation des daccord User Frontends Fehler auftreten können Sie diese jederzeit hier nachlesen und ggf. analysieren.

Um die Log-Datei zu öffnen stellen Sie sicher, dass Sie sich im Verzeichnis befinden in welchem auch das install.sh Skript liegt und geben Sie den folgenden Befehl ein:

```
less install-daccord.log
```

Drücken Sie die q-Taste um zur Konsole zurückzukehren.

#### 4.4.2 daccord User Frontend Log-Datei

Beim ersten Start des daccord User Frontend wird eine UserFrontend.log angelegt. Diese protokolliert alle im User Frontend ausgelösten Ereignisse.

```
less /opt/GuH/daccord-UserFrontend/Frontend-SL/logs/UserFrontend.log
```

Alternativ können Sie mit dem Installationsscript direkt auf das Log-File zugreifen. Geben Sie hierzu in der Konsole den entsprechenden Buchstaben „v“ ein und drücken Sie „Enter“.

```
Please select the component by entering the corresponding letter! [u/s/v/q]
```

Drücken Sie die q-Taste um zur Konsole, bzw. dem Installationsscript zurück zu kehren.

#### 4.4.3 daccord User Frontend Engine Log-Datei

Bei der catalina.out handelt es sich um eine Tomcat Log-Datei der daccord User Frontend Engine. Sollten Engine bezogene Fehler auftreten, so kann diese Log-Datei sehr hilfreich bei der Fehleranalyse sein.

Über den folgenden Befehl können Sie die catalina.out aufrufen:

```
less /opt/GuH/daccord-UserFrontend/Engine/logs/catalina.out
```

Drücken Sie die q-Taste um zur Konsole zurückzukehren.

## 5 Appendix

In diesem Abschnitt finden Sie Informationen zu erweiterten Konfigurationsmöglichkeiten des daccord User Frontends.

### 5.1 Manuelle Zuweisung einer JVM (Java Virtual Machine)

Bei Bedarf können Sie das daccord User Frontend auf einer von Ihnen festgelegten JVM betreiben. Hierfür navigieren Sie zum Pfad: „opt/GuH/daccord-UserFrontend/Engine/bin/ext“ und öffnen dort die Datei „engine.env“

**Hinweis:** Denken Sie daran, dass die Änderungen an der engine.env erst nach einem Neustart des daccord User Frontend aktiv sind.

Suchen Sie die folgende Zeile:

```
#JAVA_HOME= ""
```

Entfernen Sie das #-Zeichen um die Zeile zu aktivieren und geben Sie den Pfad zur gewünschten JVM an.

Beispiel:

```
JAVA_HOME= '/usr/java/default/jre'
```

### 5.2 Erweiterung des Java-Speichers

Bei Bedarf können Sie den verfügbaren Speicher für das daccord User Frontenderhöhen. Navigieren Sie zum Pfad: „opt/GuH/daccord-UserFrontend/Engine/bin/ext“ und öffnen Sie dort die Datei „engine.env“.

**Hinweis:** Denken Sie daran, dass die Änderungen an der engine.env erst nach einem Neustart des daccord User Frontend aktiv sind.

Passen Sie in der engine.env die Parameter in der Umgebungsvariable JAVA\_OPTS an.

Parameter	Beschreibung
-Xms	Der Parameter legt die minimale Größe des benutzbaren Heap-Speichers nach Start der Anwendung fest. Standardmäßig liegt der Wert bei 512 MB.
-Xmx	Legt die maximale Größe des Heap-Speichers fest  <b>Hinweis:</b> Dieser Wert sollte identisch zum Parameter -Xms gewählt werden um die nachträgliche Zuweisung von zusätzlichem Speicher zu verhindern.  Standardmäßig liegt der Wert bei 512 MB.

Tabelle 9: Parameter zur Erweiterung des Java-Speichers

Beispiel:

```
JAVA_OPTS="-Xmx512m -Xms512m"
```

In dem genannten Beispiel wird die maximale Größe des Heap-Speichers beim Start der Anwendung auf eine Größe von 512 MB festgelegt.

## 5.3 Aktivieren von HTTPS

Bei Bedarf haben Sie die Möglichkeit durch die Aktivierung von SSL, die Serverkommunikation auf das sicherere HTTPS umzustellen.

Um HTTPS zu aktivieren öffnen Sie die „Server.xml“, welche Sie unter „opt/GuH/daccord-User-Frontend/Engine/conf/“ finden. Suchen Sie in der Server.xml den folgenden Abschnitt, welcher mit dem Kommentarzusatz „SSL“ gekennzeichnet ist.

```
<!--SSL
  <Connector port="443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    keystoreFile="/opt/GuH/daccord-UserFrontend/Engine/conf/.keystore"
    keystorePass="changeit"
    clientAuth="false" sslProtocol="TLS"/>
SSL-->
```

In dem Sie den Abschnitt auskommentieren, aktivieren Sie die SSL Verschlüsselung.

**Hinweis:** Wird HTTPS bzw. SSL aktiviert, arbeitet dieses zunächst mit einem Standard-Zertifikat. Das Standard-Zertifikat liegt in dem Schlüsselspeicher, welchen Sie unter „./opt/GuH/daccord-UserFrontend/Engine/conf/.keystore“ finden können.

**Hinweis:** Beachten Sie, dass die Änderung erst nach einem Neustart des daccord User Frontends aktiv ist.

## 5.4 Einbinden von Zertifikaten

Dieses Kapitel beschreibt, wie ein öffentliches Zertifikat für das daccord User Frontend eingerichtet wird. Dabei werden zwei Einrichtungsfälle beschrieben. Der erste Fall beschreibt wie Sie ein neues öffentliches Zertifikat einrichten. Der zweite Fall erläutert wie Sie ein bestehendes Zertifikat für Ihr daccord User Frontend zur Verfügung stellen können.

### 5.4.1 Einrichten von Tomcat zur Nutzung eines neuen öffentlichen Zertifikates

**Hinweis:** Wenn ein Zertifikat beim Aufruf des daccord User Frontend geladen werden soll, muss https aktiviert sein (siehe Abschnitt 5.3).

Um ein öffentliches Zertifikat für Ihr daccord-System zu erstellen und einzurichten, gehen Sie wie folgt vor. Melden Sie sich am Server an, im Zweifelsfall als Benutzer „root“.

Navigieren Sie zum Pfad in dem der Schlüsselspeicher liegt:

```
cd /opt/GuH/daccord-UserFrontend/Engine/conf
```

Damit Sie bei Bedarf zum Standardzertifikat zurückkehren können, sichern Sie den bestehenden Schlüsselspeicher mit dem folgenden Befehl:

```
cd mv .keystore .keystore.back
```

**Hinweis:** Für den nächsten Schritt benötigen Sie das von Java mitgelieferte keytool Werkzeug. Um den Pfad zum keytool zu ermitteln geben Sie den folgenden Befehl ein:

```
find / -name keytool
```

Geben Sie den folgenden Befehl ein, um einen neuen Schlüsselspeicher zu generieren:

```
Pfad zum keytool/ keytool -keystore .keystore -genkeypair -alias Tomcat -keyalg RSA
```

Geben Sie die entsprechenden Informationen ein, wenn Sie dazu aufgefordert werden.

Der Administrator der Zertifikats-Autorität (certificate authority, CA) kann Sie mit den gewünschten Informationen für diese Felder versorgen.

**Hinweis:** Es muss das standardmäßige Tomcat Schlüsselspeicher-Kennwort „changeit“ benutzt werden, da sonst das Frontend den Schlüsselspeicher nicht lesen kann. Ein anderes Schlüsselspeicher-Kennwort führt dazu, dass das Frontend nicht ordnungsgemäß funktioniert.

Tippen Sie zweimal das neue Kennwort „changeit“ für den Schlüsselspeicher ein.

Wenn Sie aufgefordert werden, Ihren Vor- und Nachnamen einzugeben, muss der vollqualifizierte Domänenname (Fully Qualified Domain Name) für den daccord Server eingegeben werden, auf welchem das Frontend ausgeführt wird.

Bestätigen Sie die folgende Anweisung mit der Enter-Taste, um das gleiche Kennwort wie das Schlüsselspeicher-Kennwort zu benutzen.

```
Enter key password for <Tomcat> (RETURN if same as keystore password)
```

**Hinweis:** Es ist nicht möglich ein anderes Kennwort als das standardmäßige Tomcat-Kennwort „changeit“ zu benutzen, wenn Sie dazu aufgefordert werden, das Schlüsselspeicher-Kennwort einzugeben. Dies trifft selbst dann zu, wenn Sie am Ende zur Eingabe eines alternativen <Tomcat>-Kennwortes aufgefordert werden. Die zwei abgefragten Kennwörter (Schlüsselspeicher- und <Tomcat>-Kennwort) müssen beide den Wert „changeit“ haben.

**Hinweis:** Die oben eingegebenen Werte werden auch benutzt, um ein selbstsigniertes Zertifikat im neuen Schlüsselspeicher zu generieren. Die Benutzung eines selbstsignierten Zertifikates resultiert in der Anzeige von „Die Identität der Website Ihrer Frontend.url kann nicht verifiziert werden“, solange die PCs der Benutzer nicht darauf eingestellt wurden, dem selbstsignierten Zertifikat zu vertrauen.

Erstellen Sie eine Zertifikatssignierungsanforderung (certificate signing request) durch die Eingabe des folgenden Befehls:

```
Pfad zum Keytool/ keytool -keystore .keystore -certreq -alias Tomcat -file TomcatCert.req
```

Senden Sie die „TomcatCert.req“-Datei an Ihre Zertifikats-Autorität (öffentlich oder intern). Anschließend fordern Sie eine Base64-codierte, binäre (x.509) Datei an. Als Antwort werden Sie entweder eine „.crt“ oder „.cer“ zurück erhalten.

Importieren Sie das Rootzertifikat der Zertifikats-Autorität (CA) (angenommen, Ihr Rootzertifikat befindet sich in der Datei „./tmp/TomcatCert.cer“) auf folgende Weise:

```
Pfad zum keytool/ keytool -keystore .keystore -importcert -trustcacerts -alias rootCA  
-file ./tmp/RootCA.cer
```

Importieren Sie das durch die Zertifikats-Autorität (CA) signierte Zertifikat (angenommen, Ihr signiertes Zertifikat befindet sich in der Datei „./tmp/Tomcat.cer“) auf folgende Weise:

```
Pfad zum keytool/ keytool -keystore .keystore -importcert -trustcacerts -alias Tomcat  
-file ./tmp/TomcatCert.cer
```

**Hinweis:** Starten Sie das daccord User Frontend neu, damit die Änderungen geladen werden.

## 5.5 Automatische Weiterleitung von HTTP zu HTTPS

Vorausgesetzt, dass Sie HTTPS aktiviert haben, können Sie bei Bedarf die automatische Weiterleitung von HTTP zu HTTPS aktivieren. Hierdurch kann sichergestellt werden, dass alle Seitenaufrufe über das sicherere HTTPS Protokoll erfolgen.

Um die automatische Weiterleitung (redirect) von http zu https zu aktivieren, öffnen Sie die „web.xml“, welche Sie unter dem Pfad „opt/GuH/daccord-UserFrontend/Engine/conf/“ finden können. Am Ende der web.xml finden Sie den folgenden auskommentierten Abschnitt:

```
<!--REDIRECT
  <security-constraint>
    <display-name>A Configuration Security Constraint</display-name>
    <web-resource-collection>
      <web-resource-name>Protected Area</web-resource-name>
      <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
  </security-constraint>
REDIRECT-->
```

Entfernen Sie die mit „REDIRECT“ gekennzeichneten Kommentare, um die Weiterleitung von http zu https zu aktivieren.

```
<security-constraint>
  <display-name>A Configuration Security Constraint</display-name>
  <web-resource-collection>
    <web-resource-name>Protected Area</web-resource-name>
    <url-pattern>/*</url-pattern>
  </web-resource-collection>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>
```

**Hinweis:** Starten Sie das daccord User Frontend neu, damit die Änderungen geladen werden.

## 5.6 Anzeige von jexec is broken

Bei installieren des RPM Paketes kann es vorkommen, dass Sie auf die folgende Fehlermeldung stoßen:

```
insserv: Script jexec is broken: incomplete LSB comment. insserv: missing 'Required:'
entry: please add even if empty.
```

**Hinweis:** Es handelt sich bei dieser Meldung um einen rein kosmetischen Fehler, dieser hat keinerlei Auswirkung auf das System.

Bei dieser Fehlermeldung handelt es sich um einen fehlenden Eintrag in der jexec die mit Java ausgeliefert wird.

Um die Fehlermeldung zu beseitigen öffnen Sie die jexec Datei, welche Sie unter /etc/init.d finden können. Innerhalb der jexec ergänzen Sie den folgenden Block um die fett gedruckte Zeile:

```
### BEGIN INIT INFO
# Provides: binfmt_misc
# Required-Start: $local_fs
# Required-Stop:
# Default-Start: 1 2 3 4 5
# Default-Start: 0 6
# chkconfig: 12345 95 05
# Description: Supports the direct execution of binary formats.
### END INIT INFO
```

## 6 FAQ

### 6.1 daccord User Frontend startet nicht

Mögliche Ursache	Fehleranalyse	Hinweis zur Fehlerbeseitigung
Der bei der Konfiguration des daccord User Frontends angegebene Port wird bereits von einer anderen Anwendung belegt.	Zur Fehleranalyse sehen Sie, den Abschnitt 4.4.3 daccord User Frontend Engine Log-Datei, ein. Sollte es sich um eine doppelte Port Belegung handeln, so ist folgende Fehlermeldung zu finden:  Caused by: java.net.BindException: Address already in use	In einem solchen Fall bieten sich zwei Möglichkeiten zur Fehlerbehebung an.  <ol style="list-style-type: none"><li>1. Führen Sie die Installation des daccord User Frontends erneut aus und wählen Sie einen freien Port.</li><li>2. Sie beenden die Anwendung die den Port Blockiert und ändern deren Port.</li></ol>

Tabelle 10: FAQ

## Tabellenverzeichnis

1	Versionsübersicht . . . . .	3
2	Hardwarevoraussetzungen . . . . .	7
3	Betriebssystemvoraussetzungen . . . . .	7
4	Softwarevoraussetzungen . . . . .	8
5	Basiskonfiguration . . . . .	10
6	Frontendkonfiguration . . . . .	11
7	Autorisierungskonfiguration . . . . .	12
8	Konfiguration des Zusatzmoduls . . . . .	13
9	Parameter zur Erweiterung des Java-Speichers . . . . .	16
10	FAQ . . . . .	21

**G+H Netzwerk-Design  
Gesellschaft für IT Consulting mbH**

Ludwigstraße 8  
63067 Offenbach am Main

Tel.: +49 (0) 69 85 00 02-0  
Fax: +49 (0) 69 85 00 02-51

Email: [info@netzwerk-design.de](mailto:info@netzwerk-design.de)  
Web: [www.netzwerk-design.de](http://www.netzwerk-design.de)

