# ATOSS Time Control 11.5

# Installation

## Systemhandbuch

ATC_Installationshandbuch
Letzte Aktualisierung: 29.05.2024



ATOSS CSD Software GmbH
Rodinger Straße 19
93413 Cham, Deutschland

https://www.atoss.com/de/atoss-time-control

# Inhaltsverzeichnis

# 1 Allgemeines

### Zielsetzung und Zielgruppe

Diese Dokumentation beinhaltet Informationen für die erfolgreiche Installation und Konfiguration der ATOSS Time Control. Basierend auf häufig wiederkehrenden Anwendungsszenarien finden Sie zudem Leitlinien, die Sie bei der Abschätzung von Anforderungen an Server-Hardware und -Software unterstützen.

Die vorliegende Dokumentation richtet sich an ATOSS Time Control-Administratoren, die die Software verwalten und konfigurieren

### Geschlechtsneutralität der Dokumentation

Im Interesse einer besseren Lesbarkeit wird davon abgesehen, bei Fehlen einer geschlechtsneutralen Formulierung sowohl die männliche als auch weitere Formen aufzuführen. Die gewählten Formulierungen gelten deshalb uneingeschränkt für die weiteren Geschlechter.

### Verfügbare Dokumentation

ATOSS Time Control wird gemeinsam mit einer Online-Hilfe und folgender Dokumentation ausgeliefert:

- ATOSS Time Control Installationshandbuch: zur Unterstützung bei der Hardware- und Softwareinstallation
- ATOSS Time Control Referenzhandbuch: ein detailliertes Nachschlagewerk mit Informationen zur Funktionalität aller Dialoge

Zusätzlich dazu stehen Ihnen folgende Dokumentationen zur Verfügung:

- ATOSS Time Control Anwenderhandbuch
- ATOSS Time Control Systemfreigaben und Voraussetzungen (für On Premises-Installationen)
- ATOSS Time Control Systemfreigaben und Voraussetzungen für ATOSS CLOUD24/7 und ATOSS Cloud Solution
- ATOSS Time Control (Mobile)
- ATOSS Time Control (Mobile) Datensicherheit und Datenschutz

## 1.1 Typografische Gestaltungsmittel

In der vorliegenden Dokumentation sind Bedienelemente der ATOSS Time Control oder des Betriebssystems typografisch hervorgehoben. Folgende Gestaltungsmittel werden verwendet:

### Perspektiven, Ansichten und Registerkarten

Der Name von Perspektiven, Ansichten und Registerkarten ist in 'Hochkommas' eingeschlossen.

Beispiel: Dieser Abschnitt beschreibt die Ansichten in der Perspektive 'Wartung'.

Beispiel: Das Layout ist über die Registerkarte 'Geeignete Mitarbeiter' der Ansicht 'PEP-Szenarien' konfigurierbar.

### Bedienelemente

Wenn die Beschreibung auf Elemente der grafischen Bedienoberfläche Bezug nimmt, also z. B. auf Namen und Einträge von Menüs, Schaltflächen und Feldnamen sowie Werte, so sind diese folgendermaßen dargestellt:

Beispiel: Menü **Datei**

Beispiel: Menüeintrag **Speichern**

Beispiel: Wählen Sie **Datei** > **Speichern unter**.

Beispiel: Feld **Dateiname**

Beispiel: Schaltfläche **Schließen**

### Variablen

Variable Texte und Zeichenfolgen werden durch Platzhalter dargestellt. Sie sind in Kleinbuchstaben und *kursiv* angegeben. Ersetzen Sie diese durch den im jeweiligen Kontext zutreffenden konkreten Wert.

Beispiel: Nach dem ersten Start der ATOSS Time Control wird die Datei `atc.properties` in das über die Variable *CONF_DIRECTORY* definierte Konfigurationsverzeichnis geschrieben.

Um den Inhalt einer Umgebungsvariable zu referenzieren, wird der Variablenname abhängig vom Betriebssystem mit Sonderzeichen erweitert: Unter Windows wird der Variablenname in %-Zeichen eingeschlossen, unter Unix wird ein $-Zeichen vorangestellt.

Beispiel: HTTPS aktivieren Sie, indem Sie nun den Keystore in das Konfigurationsverzeichnis kopieren und ihn unter `${CONF_DIRECTORY}/atc.properties` auf `ssl.keystore=../config/keystore` setzen.

### Pfadnamen und Dateinamen

Namen von Dateiverzeichnissen und Dateien sind in `dicktengleicher Schrift` dargestellt.

Beispiel: Datei `atc.properties`

In Pfadangaben wird generell der Gegenschrägstrich ('\') verwendet. Ersetzen Sie diesen unter Unix durch einen Schrägstrich ('/').

Beispiel: `C:\Programme\PCS-Systemtechnik\INTUSCOM`

### Programmcode

Programmcode, Java-Code, Ausdrücke und Datei-Inhalte sind im Fließtext ebenfalls hervorgehoben.

Beispiel: Wenn dieses Attribut den Wert `externalimport.record.datasetdelete` hat und der Wert des Felds ungleich 0 ist , wird der Datensatz inaktiv.

### Hinweise

Spezielle Hinweise für den Benutzer sind durch ein Piktogramm gekennzeichnet:

**Achtung:** Bei Nichtbeachtung oder Nichteinhaltung der hier beschriebenen Maßnahmen können Daten verloren gehen.

**Hinweis:** Dieser Punkt weist Sie auf eine Besonderheit hin, die Sie beachten sollten.

**Tipp:** Hier finden Sie zusätzliche Informationen, die den vorhergehend erklärten Sachverhalt ergänzen.

**Einschränkung:** Hier finden Sie Hinweise auf Einschränkungen, die beispielsweise durch das Fehlen benötigter Lizenzen begründet sind.

# 2 Neuerungen in ATOSS Time Control 11.0

Dieses Kapitel beschreibt die wichtigsten Änderungen bei der Installation der ATOSS Time Control 11.0.

- Migration der H2-Datenbank:
  Aufgrund von Sicherheitslücken in Komponenten der H2-Datenbank empfiehlt ATOSS, mindestens die Version 2.1 für die H2-Datenbank zu verwenden. Um auf die aktuelle Version zu wechseln, führen Sie eine manuelle Migration durch. Weitere Informationen dazu finden Sie unter *H2-Datenbank manuell migrieren* auf Seite 15.
- TLS-Einstellungen für gRPC-Backend in Registry:
  TLS-Einstellungen für das gRPC-Backend werden nun in der Registry gespeichert. Auf diese Weise sind sie nun über die Umgebungsvariable verfügbar und müssen nicht länger über die Systemeigenschaften gesetzt werden.

# 3 Überblick

ATOSS Time Control ist ein Client/Server-basiertes Programmpaket mit folgenden Komponenten:

- Serverkomponenten
- Clientkomponenten
- Softwarekomponenten
- Online-Hilfe

Die Serverkomponenten auf der einen Seite liefern Daten an die angeschlossenen Clients auf der anderen Seite. Server und Clients kommunizieren über das TCP/IP-Protokoll. Dieses Konzept bietet folgende Vorteile:

- geringe Netzlast
- hohe Ausfallsicherheit
- Skalierbarkeit des Gesamtsystems

Die Lizenzierung der ATOSS Time Control ist unabhängig von der Anzahl der möglichen Clients: die mögliche Anzahl an verwendbaren Clients bestimmt allein die Anzahl möglicher Verbindungen des von Ihnen verwendeten Betriebssystems.

## 3.1 Serverkomponenten

ATOSS Time Control verwendet mehrere Serverkomponenten, die jeweils für spezielle Client-Anwendungen bestimmte Aufgaben erledigen:

| Komponente | Zugang | Aufgabe |
|---|---|---|
| Server | `server/atcs.exe`<br>(im Dienst- oder Konsolenmodus) | • Direkte Kommunikation mit der Datenbank: Behandelt Anfragen von Clients, die Stammdaten oder Bewegungsdaten lesen und schreiben.<br>• Bereitstellung der Weboberfläche<br>• Kommunikation mit den einzelnen Geräteklassen, z. B. Terminals und Zutrittsleser |
| Wartungsmodus | `http://localhost:8080/atc/console` | Wartungsmodus zur Durchführung von datenbankspezifischen Aufgaben |
| Konsole | über Browser:<br>`http://localhost:8080/atc/client` | Konfiguration der ATOSS Time Control-Server-Komponenten:<br>Einstellung u. a. von<br>• Datenbanktyp/-pfad<br>• Lizenzangaben<br>• Protokollierungsstufen<br>• Server-Konstanten<br>• Geräteprozessen<br>Installation von:<br>• Systemskripten<br>• Workflows<br>• Vorgabedaten |

**Hinweis:** Um die erforderlichen Geschwindigkeiten auch bei großen Installationen mit vielen angeschlossenen Clients sowie eine höchstmögliche Skalierbarkeit Ihres Systems zu gewährleisten,

führen Sie unter aktuellen Windows-Systemen mit aktivierter Benutzerkontensteuerung (UAC) die Serveranwendungen explizit als Administrator aus. Die Serverkomponenten können dabei auf unterschiedlichen Computern installiert sein. Ein solches Vorgehen ermöglicht Ihnen ein Anpassen Ihres Zeiterfassungssystems an wachsende Anforderungen.

## 3.2 Softwarekomponenten

ATOSS Time Control beinhaltet verschiedene Softwarekomponenten für unterschiedliche Einsatz- und Aufgabengebiete. Unterschieden wird dabei Software für Server- sowie für Geräteprozesskomponenten.

Welche der Softwarekomponenten Ihnen zur Verfügung stehen, hängt von drei Faktoren ab:

- Installierte Komponenten
- Lizenzierung der Komponenten
  Viele Komponenten sind nach der Installation nur mit gültiger Lizenz aufrufbar. Weitere Informationen finden Sie im Dokument 'ATOSS Time Control Freigaben und Voraussetzungen'.
- Berechtigungsverwaltung innerhalb von ATOSS Time Control
  Mit Hilfe von Berechtigungsgruppen ist eine Einschränkung der Aufrufmöglichkeit installierter und lizenzierter Komponenten möglich.

  Weitere Informationen dazu finden Sie in der Online-Hilfe.

## 3.3 Verfügbare Lizenzen

Für ATC Time Control sind folgende Lizenzen verfügbar:

| Lizenz | Erläuterung |
|---|---|
| Zeiterfassung (Grundmodul) | Erfassung von Personalarbeitszeiten<br>Immer erforderlich für eine Standardinstallation der ATOSS Time Control |
| Zutrittskontrolle | Erfassung von Zutrittsberechtigungen |
| Projektverfolgung | Erfassung von Projektarbeitszeiten |
| Personaleinsatzplanung | Erfassung von Personalressourcen |
| Workflow-ESS | Erfassung von Arbeitsabläufen über den Webbrowser |
| Arbeitsplatz-Zeiterfassung | Zeiterfassung im ATOSS Time Control-Client |
| ATOSS Mobile Workforce Management | Mobile Anwendung (App) |
| Interaktion PEP <-> PZE | |
| Lohn & Gehalt: Gruppe I | |
| Lohn & Gehalt: Gruppe II | |
| Lohn & Gehalt: Individuell | |
| ATOSS-Endgerätelizenz PZE | |
| Softwareterminal | |
| ATOSS-Endgerätelizenz ZK | |

| Lizenz | Erläuterung |
|---|---|
| PCS-Endgerätelizenz PZE | |
| PCS-Endgerätelizenz ZK | |
| KABA-Endgerätelizenz PZE | |
| KABA-Endgerätelizenz ZK | |
| SONSTIGE Endgerätelizenz PZE | |
| SONSTIGE Endgerätelizenz ZK | |
| Dokumentenablage | |
| Umsatz- und tageseigenschaftsbezogenes Laden von Planungsmustern | Erweiterung der Planungsoberfläche in der Personaleinsatzplanung (PEP) |

# 4 Neuinstallation der Serversoftware

**Hinweis:** Informieren Sie sich in jedem Fall über gültige Systemfreigaben und nötige Voraussetzungen, bevor Sie mit der Installation beginnen. Detaillierte Informationen dazu finden Sie im Dokument 'ATOSS Time Control Freigaben und Voraussetzungen'.

Dieser Abschnitt führt Sie Schritt für Schritt durch eine typische Neuinstallation von ATOSS Time Control auf einen Server-Computer.

**Hinweis:**

- Beim Einsatz von SQL-Datenbanken wird im Folgenden ein installierter und betriebsbereiter Datenbankserver mit leerer Datenbank vorausgesetzt, die von einem Benutzer mit Schreibberechtigungen über ein Kennwort zugänglich ist.
- Für Informationen zu Release-Wechsel und Updates siehe *Updates und Release-Wechsel* auf Seite 43.
- Beim Einsatz von MySQL/MariaDB setzen Sie auf Datenbankseite folgende Konfigurationsparameter in der angegebenen Reihenfolge:

| Schritt | Einstellung | Wert | Erläuterung |
|---|---|---|---|
| 1 | lower_case_table_names | 1 | Informationen dazu finden Sie in der *MySQL Referenzdokumentation*. |
| 2 | innodb_file_format | Barracuda | Mindestanforderung an das Dateiformat ist Barracuda.<br>Weiterführende Informationen finden Sie in der *MySQL Referenzdokumentation*. |
| 3 | innodb_large_prefix | 1 | Informationen dazu finden Sie in der *MySQL Referenzdokumentation*. |

Eine Neuinstallation der Serversoftware umfasst folgende Schritte:

1. *Systemanforderungen prüfen*
2. *Vollständigkeit der Lizenzen prüfen*
3. *Jetty-Webserver und Startseite Webclient konfigurieren*
4. *Server über die Konsole konfigurieren*
5. *Startvariante konfigurieren*

Anschließend haben Sie die Möglichkeit, die *Sprache der Serverdienste zu ändern*.

Um zusätzlich die mobile Anwendung ATOSS Mobile Workforce Management für ATOSS Time Control einsetzen zu können, sind Einstellungen am ATOSS Mobile Information Server (AMIS) erforderlich. Informationen dazu finden Sie unter

## 4.1 Systemanforderungen prüfen

Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Weitere Informationen finden Sie im Handbuch 'ATOSS Time Control Freigaben Voraussetzungen'.

Um sicherzugehen, dass das System alle Anforderungen für eine Installation erfüllt, führen Sie folgende Schritte aus:

1. Prüfen Sie unter **Systemsteuerung** > **Regions- und Sprachoptionen** > **Regionale Einstellungen**, ob die Servereinstellungen für Datum und Uhrzeit das Format 'TT.MM.JJJJ' verwenden.

2. Weist das Datum ein längeres Format auf, ändern Sie das Format mit Hilfe der Schaltfläche **Anpassen**.

## 4.2 Vollständigkeit der Lizenzen prüfen

**Hinweis:**
- Für jeden Wechsel auf das nächsthöhere ATOSS Time Control Major Release ist eine neue Lizenz erforderlich.
- Bei Verwenden der Online-Lizenzierung stellt Ihnen der ATOSS-Lizenzserver nach Prüfung auf einen vorliegenden gültigen Lizenzvertrag automatisch eine neue Lizenz aus.

Um sicherzugehen, dass gültige Lizenzen für eine Installation vorliegen, führen Sie folgenden Schritt aus:

1. Prüfen Sie über die *Lizenzverwaltung*, ob Sie über eine gültige Lizenz für das von Ihnen verwendete Release der ATOSS Time Control verfügen.

   Ist keine aktuelle Lizenz vorhanden, wenden Sie sich dazu an Ihren ATOSS CSD-Berater oder den *Support*.

### 4.2.1 Neue Lizenz hinzufügen

Änderungen an Ihrer Lizenz (z. B. für einer Erhöhung der Anzahl lizenzierter Mitarbeiter) müssen Sie in ATOSS Time Control hinterlegen. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie einen Browser und geben Sie folgende Adresse ein: `http://SERVERNAME:8080/atc/console`.

   'SERVERNAME' ist dabei der Platzhalter für den Namen oder die IP-Adresse Ihres Time Control-Servers.

   Der Anmeldedialog der Serverkonsole öffnet sich.
2. Melden Sie sich mit Ihrem Benutzernamen und Ihrem Kennwort auf der Serverkonsole an.

   Nach der Anmeldung erfolgt eine Prüfung auf neue Versionen von ATOSS Time Control.
3. Lehnen Sie die Installation neuer Versionen ab.

1. Online-Aktivierung der Lizenz

   **Hinweis:** Wenn Sie die Online-Aktivierung der Lizenzen verwenden, erfolgt eine automatische Prüfung, ob eine neue Lizenz zur Verfügung steht. Eine Meldung informiert Sie über eine vorliegende neue Lizenz und fragt, ob Sie diese importieren möchten.

4. Bestätigen Sie diese Meldung mit **Ja**.
   Die Registerkarte 'Lizenzverwaltung' öffnet sich. Die neue Lizenz ist aktiviert und Sie sehen die Meldung 'Die Lizenz ist gültig (Online)'.
2. Offline-Aktivierung der Lizenz

   **Hinweis:** Ist der Server offline oder ohne Internetzugang, erscheint eine Fehlermeldung, dass keine Verbindung zum Time Control-Server hergestellt werden kann.

5. Öffnen Sie die Registerkarte 'Lizenzverwaltung'.
6. Wählen Sie die Schaltfläche **Importieren**.
7. Wählen Sie die zu importierende Lizenzdatei aus und bestätigen Sie mit **OK**.
   Die neue Lizenz ist aktiviert und Sie sehen die Meldung 'Die Lizenz ist gültig.'

**Tipp:** Prüfen Sie auf der Registerkarte 'Lizenzverwaltung', ob die entsprechende Lizenzanzahl der jeweiligen Module mit der von Ihnen bestellten Anzahl übereinstimmt.

## 4.3 Jetty-Webserver und Startseite Webclient konfigurieren

**Hinweis:**

- Vor der Neuinstallation von ATOSS Time Control ist es unbedingt erforderlich, ein bereits auf Ihrem System vorhandenes Release zu deinstallieren.
- Entfernen Sie vor der *Deinstallation* sämtliche Dienste manuell. Verwenden Sie dazu entweder die Konsole oder den Windows-SC-Befehl `SC delete DIENSTNAME`.

### 4.3.1 Informationen zum Jetty-Webserver

Jetty ist ein in Java geschriebener Servlet/JSP-Container und Webserver. Er dient als Basis für den ATOSS Time Control-Webserver.

#### 4.3.1.1 SSL-Zertifikat für Jetty-Webserver erstellen

Dieser Abschnitt beschreibt das Vorgehen, um eine verschlüsselte Kommunikation des Jetty-Webservers mit eigenem SSL-Zertifikat einzurichten.

**Hinweis:**

- Voraussetzung für den Einsatz des Jetty-Webservers mit eigenem SSL-Zertifikat ist neben dem installierten Java Runtime Environment (JRE) die Installation des Java Development Kits (JDK) 1.8.x. Es ist erhältlich unter *http://www.oracle.com/technetwork/java/javase/downloads/index.html*.
- Ein Einsatz des Jetty-Webservers mit eigenem SSL-Zertifikat erfordert immer auch eine manuelle Konfiguration der Clients, damit automatische Updates auch weiterhin möglich sind.

##### Keystore erstellen

**Tipp:** Teil aller JRE-Installationen ist die Datei `keytool.exe` von Java, mit der Sie einen Keystore erstellen können. Dieser Keystore enthält ein öffentliches und ein privates Schlüsselpaar, mit dem Sie die in Identity Audit enthaltenen Standardzertifikate ersetzen können.

Gehen Sie zum Erstellen eines Keystores wie folgt vor:

1. Stellen Sie sicher, dass JRE sowie JDK 1.8.x installiert sind.
2. Öffnen Sie eine Windows Eingabeaufforderung und navigieren Sie im Installationsverzeichnis des JDKs in das `/bin`-Verzeichnis.
3. Führen Sie folgenden Befehl aus:
   ```
   keytool -keystore keystore -alias atc -genkey -keyalg RSA -ext san=IP:SERVERIP
   ```
   'SERVERIP' ist dabei der Platzhalter für die IP-Adresse des Time Control-Servers.

   **Hinweis:** Bei aktivierter Windows-Benutzerkontensteuerung ist es möglich, dass Sie im Verzeichnis 'Programme' keine Schreibberechtigungen besitzen. Erstellen Sie in diesem Fall die Datei `keystore` in einem anderen Pfad, indem Sie anstatt `-keystore keystore` z. B. folgendes angeben:
   ```
   -keystore c:\temp\keystore
   ```
4. Geben Sie ein Kennwort für den Keystore ein.
   Dieses Kennwort wird beim Import des Truststores verwendet.

   **Hinweis:** Um Truststore und Keystore gleich zu setzen, ergänzen Sie folgende Parameter in der Datei `%programmdata%/server/wrapper.conf`:
   ```
   javax.net.ssl.trustStore=%PFAD_ZUM_KEYSTORE%
                javax.net.ssl.trustStorePassword=%KEYSTORE_PASSWORT%
   ```
5. Geben Sie die folgenden Informationen ein:

- Vor- und Nachname
- Organisatorische Einheit
- Organisation
- Stadt oder Gemeinde
- Bundesland/-staat
- Zweistelliger Ländercode

6. Überprüfen Sie die Informationen.
7. **Tipp:** Geben Sie hier zusätzlich den Parameter **-validity** (Anzahl Tage) an. Bei Nichtangabe des Parameters ist das Zertifikat lediglich 90 Tage gültig.

   Drücken Sie die Eingabetaste, um dasselbe Kennwort wie das Keystore-Kennwort zu verwenden.

   Die Datei `keystore` wird mit einem privaten Schlüssel und dem entsprechenden öffentlichen Schlüssel (Zertifikat) erstellt.

Führen Sie nun folgende Konfigurationen durch:

- *Jetty-Webserver für SSL konfigurieren*

#### 4.3.1.1.1 Jetty-Webserver für eigenes SSL-Zertifikat konfigurieren

Wenn Sie keine Java Keystore-Datei haben, sondern das Zertifikat im PKCS12-Format (Datei mit der Endung `.p12` oder `.pfx`) vorliegt, ist es erforderlich, zunächst mit dem Keytool von Java eine Java Keystore-Datei im korrekten Format zu erzeugen.

**Konvertierung von PKCS12-Zertifikaten**

Eine geeignete keystore-Datei erzeugen Sie mit der Datei `keytool.exe` von Java:

```
keytool -importkeystore -deststorepass geheimespasswort -destkeypass geheimespasswort -destkeystore
${KEYSTORE}
        -srckeystore ${TEMP_PKCS12} -srcstoretype PKCS12
```

Dabei ist `${KEYSTORE}` die zu erzeugende Keystore-Datei und `${TEMP_PKCS12}`: die `*.p12`-Zertifikatsdatei.

In diesem Beispiel liegen die beiden Dateien in dem Unterordner, aus dem `keytool.exe` aufgerufen wird. Die Passwörter sind hier jeweils mit 'masterkey' angegeben:

```
keytool -importkeystore -deststorepass masterkey -destkeypass masterkey -destkeystore keystoretest
        -srckeystore zertifikattest.p12 -srcstoretype PKCS12
```

Liegt nun die JAVA Keystore-Datei vor, führen Sie folgende Schritte aus:

**Jetty-Webserver konfigurieren**

**Hinweis:** Achten Sie bei Pfadangaben unbedingt darauf, den Schrägstrich (/) zu verwenden. Bei Verwenden eines Backslashes (\) wird die angegebene Keystore-Datei nicht gefunden.

**Hinweis:** In diesem Beispiel hat die Keystore-Datei den Namen `keystore`. Zusätzlich wird hier die Buchstabenfolge 'masterkey' sowohl für das Passwort als auch für das Key-Passwort der Datei verwendet.

1. Stellen Sie sicher, dass Ihr vorliegendes SSL-Zertifikat in einem Java-Keystore-Format vorliegt und konvertieren Sie ggf. Ihre Zertifikatdatei.

   Für weitere Informationen dazu wenden Sie sich an Ihren Zertifikatanbieter.
2. Kopieren Sie Ihre Keystore-Datei in den Workspace des Servers (z. B. `C:\ProgramData\atc\server`).
3. Öffnen Sie die Datei `\config\atc.properties` mit einem Editor.

   Diese Datei finden Sie üblicherweise unter `C:\Program Files\ATOSS\timecontrol\config\atc.properties`.
4. Passen Sie die Parameter im folgenden Bereich an:

| Zeilennummer | Eintrag |
|---|---|
| 1 | ssl.keystore=C:/ProgramData/atc/server/keystore |
| 2 | ssl.password=masterkey |
| 3 | ssl.keypassword=masterkey |
| 4 | #ssl.needclientauth=false |
| 5 | #ssl.wantclientauth=false |
| 6 | #ssl.protocol= |
| 7 | #ssl.algorithm= |
| 8 | #ssl.keystoretype= |

5. Speichern Sie die Änderungen.
6. Starten Sie den Jetty-Webserver.
7. Um eine SSL-Verbindung mit dem Jetty-Webserver herzustellen, öffnen Sie auf dem Servercomputer einen Browser und geben Sie die folgende Adresse ein: `https://127.0.0.1:8443`.
   Die SSL-Verbindung zwischen Server und Jetty-Webserver wird hergestellt.

#### 4.3.1.1.2 Jetty-Webserver SSL-Port ändern

Der Standard-SSL-Port des Jetty Webservers ist '8443'. Um diesen Port zu ändern, führen Sie folgenden Schritt aus:

1. Geben Sie in der Datei `%instdir%/config/atc.properties` bei `webserverport.https=%port%` anstatt `'%port%'` die neue Portnummer an.

#### 4.3.1.2 HTTPS aktivieren

Nach dem ersten Start der ATOSS Time Control wird die Datei `atc.properties` in das über die Variable *CONF_DIRECTORY* definierte Konfigurationsverzeichnis geschrieben. HTTPS aktivieren Sie, in dem Sie nun den Keystore in das Konfigurationsverzeichnis kopieren und ihn unter `${CONF_DIRECTORY}/atc.properties` auf `ssl.keystore=../config/keystore` setzen.

### 4.3.2 Umleitung der Startseite des Webclients

Bei Aufruf der Adresse `http://`*`SERVERNAME`*`:8080` werden Sie nun nicht mehr auf eine Startseite geführt, sondern standardmäßig direkt auf den Webclient mit der Adresse `http://SERVERNAME:8080/atc/client` weitergeleitet.

Sie können die Startseite des Webclients aber auch auf ein selbst konfiguriertes Ziel umleiten. Dies konfigurieren Sie in der Datei `atc.properties`.

Um z. B. eine Umleitung zu `atc/terminal` einzurichten, fügen Sie Folgendes in die Datei `atc.properties` ein:

```
redirection=atc/terminal
```

### 4.3.3 ATOSS Time Control-Dienste

Der ATOSS Time Control-Windows-Dienst bezieht seine Parameter aus folgenden Dateien:

- `%INSTDIR%\config\atc.properties`
- `%INSTDIR%\wrapper\wrapper_%product%.conf`
- `%WORKSPACE%\%PRODUCT%\wrapper.conf (customer parameters. override the default)`

### Installation eines Dienstes

Die Installation eines Windows-Dienstes führen Sie mit folgendem Batch-Aufruf durch:

```
%INSTDIR%\wrapper\service_installer.bat
```

Dabei greift auch dieser Aufruf auf Parameter aus den oben genannten Dateien zurück.

### Deinstallation eines Dienstes

Änderungen an den Serverdiensten sind nur über Windows-Bordmittel möglich. Verwenden Sie dazu das im Resource Kit enthaltene SC-Tool (Sc.exe).

Folgender Aufruf deinstalliert den Datenserverdienst von ATOSS Time Control:

```
sc delete atcs1
```

## 4.4 ATOSS Time Control-Vollversion installieren (Linux)

Sie installieren die ATOSS Time Control mit Hilfe von DEB-Paketen. Diese DEB-Pakete enthalten alles, was für die Installation erforderlich ist.

Die Pakete werden im Kundenbereich der Weblounge zur Verfügung gestellt:

*https://weblounge.atoss.com/de-de/kundenbereich-atc*.

**Hinweis:** Für den Zugriff auf die Weblounge ist eine Anmeldung erforderlich.

Um ATOSS Time Control unter Linux zu installieren, gehen Sie wie folgt vor:

1. Installieren Sie 'ttf-mscorefonts'.
2. Laden Sie das DEB-Paket herunter.
3. Um das Paket zu installieren, führen Sie den folgenden Befehl in der Kommandozeile aus:
   ```
   sudo apt install ./timecontrol-server_1x.x.x.qualifier.deb
   ```
   Ersetzen Sie dabei *1x.x.x* durch Ihr aktuelles Release und *qualifier* durch den aktuellen Wert.

   Beispiel für den Befehl für ATOSS Time Control 10.4:
   ```
   sudo apt install ./timecontrol-server_10.4.0.v20211020-1037_amd64.deb
   ```
4. Geben Sie die Berechtigungen zum Ausführen der Java-Komponente an:
   ```
   sudo chmod +x /opt/timecontrol/install/server/plugins/jre.linux_x86_64_21.0.0/jre/lib/jspawnhelper
   ```
5. Starten Sie den Time Control-Server:
   ```
   sudo systemctl start timecontrol-server
   ```

## 4.5 Server über die Konsole konfigurieren

Den Server konfigurieren Sie über die Konsole. Diese steht Ihnen über Ihren Browser zur Verfügung.

### Konsole über den Browser starten

Beim ersten Start öffnet sich Ihr Browser mit der Adresse `http://localhost:8080/atc/console` und stellt Ihnen zur Konfiguration die Konsole zur Verfügung.

**Hinweis:** Bei einer Neuinstallation informiert Sie eine Meldung über eine ungültige Datenbank-Konfiguration. Bestätigen Sie die Meldung mit **OK**.

### Verfügbare Updates

Abhängig von den Einstellungen zur *automatischen Updateprüfung* werden Sie beim Start der Konsole über zur Verfügung stehende Updates für das verwendete Major Release informiert. Bei einer installierten ATOSS Time Control 7.2 können z. B. 7.2.x-Updates vorliegen.

Bei einem vorliegenden Update haben Sie die Möglichkeit, dessen Installation zu bestätigen oder abzulehnen.

**Tipp:** ATOSS CSD empfiehlt, bei einer Erstinstallation alle verfügbaren Aktualisierungen zu installieren.

Nach der Installation der Updates erfolgt ein Neustart der Serverdienste.

**Hinweis:** Führen Sie im Anschluss an eine Updateinstallation und vor dem Neustart des Datenservers unbedingt eine Tabellenaktualisierung durch! Weitere Informationen zum Installieren von Updates finden Sie unter *Updates und Release-Wechsel* auf Seite 43.

### Serverkonfiguration ausführen

Den Server konfigurieren Sie mithilfe der in der Konsole verfügbaren Registerkarten. Folgende Schritte sind für eine vollständige Serverkonfiguration erforderlich:

1. *H2-Datenbank manuell migrieren*
2. *Verbindung zur Datenbank herstellen*
3. *Tabellenstruktur aktualisieren*
4. *Lizenzen aktivieren*
5. *Anwendungen konfigurieren*
6. ggf. *SSL-Zertifikat erstellen*
7. *Einstellungen des Applikationsservers festlegen*
8. *Grundlegende Installationseinstellungen des Servers festlegen*
9. *Grundlegende Geräteprozesseinstellungen des Servers festlegen*
10. *Serverkonfigurationen übernehmen*

**Hinweis:** Vermeiden Sie Änderungen auf der Registerkarte 'Ereignisse'. Änderungen an Einstellungen zu Server-Ereignissen können dazu führen, dass Clients keine aktuellen Daten anzeigen.

## 4.5.1 H2-Datenbank manuell migrieren

Um von der H2-Datenbank Version 1.4 auf die aktuelle Version 2.1 zu wechseln, führen Sie die Migration der Datenbank manuell durch. Dies ist erforderlich, da die H2-Datenbank Version 2.1 nicht mit älteren Versionen kompatibel ist. Um die Datenbank manuell zu migrieren, gehen Sie wie folgt vor:

1. Laden Sie folgende ZIP-Dateien unter *http://www.h2database.com/html/download-archive.html* herunter:
   - 2.1.212: 'Platform-Independent Zip'
   - 1.4.197: 'Platform-Independent Zip'
2. Entpacken Sie die ZIP-Dateien in separate Verzeichnisse, z. B. `h2-2.1.212/` und `h2-1.4.197/`.
3. Fahren Sie den ATOSS Time Control-Serverdienst bzw. die Serveranwendung vollständig herunter.
4. Suchen Sie die verwendeten Datenbankdateien mit den Endungen '*.h2.db' oder '*.mv.db'.
5. Sichern Sie die Datenbankdateien in einem separaten Verzeichnis.
6. Öffnen Sie die Kommandozeile und wechseln Sie in das Verzeichnis `h2-1.4.197/bin/`.
7. Passen Sie den Pfad des Verzeichnisses an Ihre Datenbankdatei an, wie am Beispiel für `C:\database\atc_105_H2-14.mv.db` erläutert:
   a) Ersetzen Sie den Datenbankbenutzer und das zugehörige Passwort.

b) Führen Sie anschließend einen Datenbankexport mit folgendem Befehl aus, z. B. für `atc_export.sql`:

```
java -cp h2-1.4.197.jar org.h2.tools.Script -url "jdbc:h2:C:\database\atc_105_H2-14" -user
"timecontrol" -password "masterkey" -script "C:\database\atc_export.sql"
```

**Hinweis:** Geben Sie beim Verzeichnispfad keine Dateinamenerweiterung an. Abhängig von der ATOSS Time Control-Version können die ausgelieferte Version des Java Runtime Environments (JRE) und dementsprechend das Verzeichnis abweichen. Wenn Java auf Ihrem System nicht installiert ist, verwenden Sie das in der ATOSS Time Controlmitgelieferte JRE.

c) Ergänzen Sie den Aufruf mit `%INSTALLATIONSVERZEICHNIS-ATC%\server\plugins\jre.win_x86_64_11.0.15\jre\bin\`.

8. Wechseln Sie in das Verzeichnis `h2-2.1.212/bin/`.
9. Passen Sie den Pfad an Ihre Datenbankexportdatei an, wie am Beispiel für `C:\database\atc_export.sql` erläutert:
   a) Importieren Sie mit folgendem Befehl die exportierte Datenbank in eine neue Datenbankdatei, z. B. für `atc_105_H2-21`: `java -cp h2-2.0.202.jar org.h2.tools.RunScript -url "jdbc:h2:C:\database\atc_105_H2-21" -user "timecontrol" -password "masterkey" -script "C:\database\atc_export.sql" -options FROM_1X`.

   **Hinweis:** Geben Sie beim Verzeichnispfad keine Dateinamenerweiterung an.

   b) Geben Sie den Benutzer und das Passwort für die neue Datenbank ein.
10. Starten Sie den ATOSS Time Control-Serverdienst bzw. die Serveranwendung.
11. Öffnen Sie die Serverkonsole und melden Sie sich mit dem Passwort für den Wartungsmodus an.
12. Wählen Sie in der Ansicht 'Datenbankeinstellungen' in der Auswahlliste **Datenbanktyp** 'H2 2.1' aus.
13. Geben Sie die verwendeten Zugangsdaten ein und wählen Sie im Feld **Name** die Datenbankdatei aus.
14. Bestätigen Sie Ihre Eingaben mit **Speichern**.
15. Aktualisieren Sie die Datenbanktabellen in der Ansicht 'Datenbankaktualisierung' mit **Aktualisieren**.

Die Migration ist nun abgeschlossen. Stellen Sie nach der Datenbankmigration ggf. Sicherungsmechanismen auf die neue Datenbankdatei um.

### 4.5.2 Verbindung zur Datenbank herstellen

Über die Registerkarte 'Datenbankeinstellungen' stellen Sie die Verbindung zur Datenbank her.

**Hinweis:** Open Database Connectivity (ODBC) ist für den Verbindungsaufbau zur Datenbank nicht erforderlich.

**Hinweis:** Wenn für eine MS SQL-Datenbank kein Port festgelegt ist, erfolgt nun eine dynamische Portzuweisung.

**Tipp:** Um zu große Protokolldateien zu vermeiden, verwenden Sie beim Betrieb einer Microsoft SQL Datenbank das Wiederherstellungsmodell 'einfach'. Die Einstellungsmöglichkeit dazu finden Sie im MS SQL Server unter **Datenbankeigenschaften der ATC-Datenbank** > **Optionen**. Details zu Protokolldateien und den Wiederherstellungsmodellen finden Sie in den Dokumentationen zum Microsoft SQL Server.

| **Verwendete Symbole:** | |
|---|---|
|  | **Die Datenbankeinstellungen sind gültig** |

1. Konfigurieren Sie die Datenbankverbindung mit den folgenden Bedienelementen:

| | |
|---|---|
| **Datenbank-Typ (MS SQL, H2, MariaDB/MySQL)**: | Wählen Sie das Datenbanksystem aus. |
| **Name**: | Name der Datenbank:<br>• MS SQL: Geben Sie den im SQL-Server verwendeten Namen der Datenbank an.<br>• H2 und MariaDB/MySQL: Geben Sie den Pfad und den Namen der jeweiligen Datenbank an. |
| **Host**: | Geben Sie die IP-Adresse oder den Hostnamen des MS SQL-Servers bzw. des Rechners der H2- oder MariaDB/MySQL-Datenbank an. |
| **Port**: | Diese Einstellung ist standardmäßig nicht relevant. |
| **Benutzername**: | Geben Sie den Namen des Benutzers an, der die Berechtigung für die ATOSS Time Control-Datenbank besitzt. |
| **Kennwort**: | Geben Sie das Kennwort des Datenbankbenutzers an. |

2. Bestätigen Sie die Einstellungen mit **Speichern**.
   Sind Ihre Eingaben korrekt, sehen Sie die Meldung 'Die Datenbankeinstellungen sind gültig'.

### 4.5.3 Tabellenstruktur aktualisieren

In diesem Schritt überprüfen Sie die Datenbanktabellen auf Vollständigkeit und Richtigkeit und haben bei Abweichungen die Möglichkeit, Fehler zu korrigieren. Die Tabellenstruktur aktualisieren Sie über die Registerkarte 'Aktualisierung'.

**Hinweis:** Aktualisieren Sie die Tabellenstruktur nach jeder Installation, um sicherzustellen, dass Sie keine veraltete Tabellenstruktur verwenden. Bei Verwenden einer veralteten Tabellenstruktur ist kein Arbeiten mit ATOSS Time Control möglich.

Nach dem Speichern der Datenbankeinstellungen im vorigen Schritt öffnet sich die Meldung zur Aktualisierung der Datenbanktabellen.

1. Bestätigen Sie die Meldung mit **OK**.
   Die Meldung, den Server für die Tabellenaktualisierung herunterzufahren, öffnet sich.
2. Um den Server herunterzufahren, bestätigen Sie die Meldung mit **OK**.
   Der die Daten bereitstellende Teil des Serverdienstes wird beendet und die Tabellenaktualisierung wird gestartet. Bei einer Neuinstallation werden die erforderlichen Tabellen vollständig angelegt.

   **Achtung:** Ein Abbrechen einer Neuinstallation während des Aktualisierungsvorgangs kann zu einer Beschädigung der Datenbank führen. Vermeiden Sie deshalb unbedingt ein Abbrechen der Neuinstallation!

   Nach erfolgreicher Tabellenaktualisierung sehen Sie die Meldung 'Die Tabellen sind auf dem neuesten Stand'. Danach startet der Server automatisch.

### 4.5.4 Lizenzen aktivieren

Ihre Lizenzen aktivieren und verwalten Sie über die Registerkarte 'Lizenzverwaltung'. Informationen zu erforderlichen und empfohlenen Lizenzen finden Sie im Dokument 'ATOSS Time Control Freigaben und Voraussetzungen'.

| Aktionen | |
|---|---|
|  | **Bearbeiten** |
|  | **Importieren** |
|  | **Aktivierungsschlüssel** |

**Tipp:**

- ATOSS CSD empfiehlt das Verwenden eines Schlüssels zur Online-Aktivierung der Lizenzen. Bei diesem Vorgehen ist ein aktives Anfordern von neuen Lizenzdateien für zusätzlich erworbene Module nicht notwendig. Nach Speichern der Lizenzinformationsänderung bei ATOSS CSD wird Ihre neue Lizenz automatisch freigeschaltet und ist online für Sie über die Aktion **Aktivierungsschlüssel** verfügbar.
- Der Aktivierungsschlüssel liegt standardmäßig dem gedruckten Installationshandbuch als separater Ausdruck bei.

Zur Aktivierung einer Lizenz führen Sie die folgenden Schritte aus:

1. Wählen Sie in der Spalte 'Lizenz' die zu aktivierende Lizenz aus.

   Ist der Server offline oder ohne Internetzugang, laden Sie die Lizenzdatei über die Schaltfläche **Importieren**.
2. Wählen Sie **Aktivierungsschlüssel**.
   Der modale Dialog 'Aktivierungsschlüssel' öffnet sich.
3. Geben Sie den Aktivierungsschlüssel für Ihre Lizenz in das Eingabefeld ein und bestätigen Sie mit **OK**.
   Die Gültigkeit der Lizenz wird online über unseren Lizenzierungsserver geprüft. Nach erfolgreicher Lizenzierung sehen Sie die Meldung 'Die Lizenz ist gültig (Online)'.

**Hinweis:** Der Zusatz '(Online)' erscheint nur bei Verwenden des Aktivierungsschlüssels.

### 4.5.5 Anwendungen konfigurieren

Anwendungen konfigurieren Sie über die Registerkarte 'Anwendungen':

| Aktionen | |
|---|---|
|  | **Anwendung aktivieren** |
|  | **Anwendung deaktivieren** |

1. Legen Sie für jede Anwendung über das Auswahlfeld den gewünschten Starttyp fest.

   Mögliche Starttypen sind:
   - Automatisch
   - Manuell
   - Deaktiviert
2. Verwenden Sie die Schaltflächen, um einzelne Anwendungen des Servers gezielt zu aktivieren oder zu deaktivieren.

### 4.5.6 SSL-Zertifikat erstellen

Dieser Abschnitt beschreibt das Vorgehen, um eine verschlüsselte Kommunikation des Applikationsservers mit eigenem SSL-Zertifikat einzurichten.

**Hinweis:**

- Voraussetzung für den Einsatz des Applikationsservers mit eigenem SSL-Zertifikat ist neben dem installierten Java Runtime Environment (JRE) die Installation des Java Development Kits (JDK) 1.8.x. Es ist erhältlich unter:
  *http://www.oracle.com/technetwork/java/javase/downloads/index.html*.
- Ein Einsatz des Applikationsservers mit eigenem SSL-Zertifikat erfordert immer auch eine manuelle Konfiguration der Clients, damit automatische Updates auch weiterhin möglich sind.

#### Keystore erstellen

**Tipp:** Teil aller JRE-Installationen ist die Datei `keytool.exe` von Java, mit der Sie einen Keystore erstellen können. Dieser Keystore enthält ein öffentliches und ein privates Schlüsselpaar, mit dem Sie die in Identity Audit enthaltenen Standardzertifikate ersetzen können.

Gehen Sie zum Erstellen eines Keystores wie folgt vor:

1. Stellen Sie sicher, dass JRE sowie JDK 1.8.x installiert sind.
2. Öffnen Sie eine Windows Eingabeaufforderung und navigieren Sie im Installationsverzeichnis des JDKs in das `/bin`-Verzeichnis.
3. Führen Sie folgenden Befehl aus:
   ```
   keytool -keystore keystore -alias atc -genkey -keyalg RSA -ext san=IP:SERVERIP
   ```
   'SERVERIP' ist dabei der Platzhalter für die IP-Adresse des Time Control-Servers.

   **Hinweis:** Bei aktivierter Windows-Benutzerkontensteuerung ist es möglich, dass Sie im Verzeichnis 'Programme' keine Schreibberechtigungen besitzen. Erstellen Sie in diesem Fall die Datei `keystore` in einem anderen Pfad, indem Sie anstatt `-keystore keystore` z. B. folgendes angeben:
   ```
   -keystore c:\temp\keystore
   ```
4. Geben Sie ein Kennwort für den Keystore ein.
   Dieses Kennwort wird beim Import des Truststores verwendet.

   **Hinweis:** Um Truststore und Keystore gleich zu setzen, ergänzen Sie folgende Parameter in der Datei `%programmdata%/server/wrapper.conf`:
   ```
   javax.net.ssl.trustStore=%PFAD_ZUM_KEYSTORE%
                javax.net.ssl.trustStorePassword=%KEYSTORE_PASSWORT%
   ```
5. Geben Sie die folgenden Informationen ein:
   - Vor- und Nachname
   - Organisatorische Einheit
   - Organisation
   - Stadt oder Gemeinde
   - Bundesland/-staat
   - Zweistelliger Ländercode
6. Überprüfen Sie die Informationen.
7. **Tipp:** Geben Sie hier zusätzlich den Parameter **-validity** (Anzahl Tage) an. Bei Nichtangabe des Parameters ist das Zertifikat lediglich 90 Tage gültig.

   Drücken Sie die Eingabetaste, um dasselbe Kennwort wie das Keystore-Kennwort zu verwenden.

Die Datei `keystore` wird mit einem privaten Schlüssel und dem entsprechenden öffentlichen Schlüssel (Zertifikat) erstellt.

#### .pfx-Datei erzeugen

Um eine verschlüsselte Kommunikation für die Client-Server-Verbindung nutzen zu können, ist für ein eigenes SSL-Zertifikat eine `*.pfx`-Datei erforderlich:

1. Führen Sie zusätzlich folgenden Befehl aus:
   ```
   keytool -importkeystore -srckeystore keystore -destkeystore keystore.pfx -deststoretype PKCS12
   ```
   Die Datei `keystore.pfx` wird erstellt.

   Geben Sie den Pfad zu dieser Datei in den Servereinstellungen der Konsole an.

### 4.5.7 Einstellungen des Applikationsservers

Die grundlegenden Einstellungen des Applikationsservers sind über die jeweiligen Registerkarten unter **Navigation** > **Einstellungen** der Konsole erreichbar.

Eine Konfiguration dieser Einstellungen kann folgende Schritte umfassen:

1. *Servereinstellungen konfigurieren*
2. *E-Mail-Versandoptionen konfigurieren*
3. *Kalenderintegration konfigurieren*
4. *Zutrittskontrolle konfigurieren*
5. *Speicher konfigurieren*
6. *Externe Datenquellen konfigurieren*
7. *Proxy-Server konfigurieren*
8. *Basisverzeichnisse anlegen*
9. *Mitarbeiterprüfungszeit konfigurieren*

#### 4.5.7.1 Servereinstellungen konfigurieren

Verwenden Sie dazu die Registerkarte 'Servereinstellungen'.

#### Gruppe 'Doppelte Stempelsatzprüfung'

**Doppelte Stempelsatzprüfung aktivieren**: Bei aktivierter Option wird global für jedes Zeiterfassungsgerät ermittelt, ob ein Mitarbeiter zweimal hintereinander auf dasselbe Zeitkonto gestempelt hat.

**Stunden nach der letzten Stempelung**: Geben Sie an, wie lange nach einer Stempelung auf dasselbe Zeitkonto geprüft wird.

**Kostenstelle berücksichtigen**: Aktivieren Sie diese Option, um zusätzlich die Kostenstelle als Unterscheidungsmerkmal bei der Prüfung zu berücksichtigen.

#### Gruppe 'Externer Import'

**Aufbewahrungsdauer alter Import-Logs (in Tagen)**: Geben Sie an, wie lange die Datenbank eine Protokollierung vor dem Überschreiben maximal speichert.

**Standard-Verzeichnis (für system.importfiles)**: Geben Sie ein Verzeichnis für zu speichernde Importdateien an, z. B. `C:\ProgramData\atc\server\importfiles`.

Über die Schaltfläche **…** öffnen Sie den modalen Dialog 'Erweiterte Eigenschaften' für weitere Angaben zum verwendeten Text-Datenbank-Treiber.

**Hinweis:** Bei Angabe eines Zeichensatzes müssen alle in das Standard-Verzeichnis importierten Dateien den angegebenen Zeichensatz verwenden.

### Gruppe 'Netzwerk'

**Schnittstellen**: Wählen Sie das Netzwerk aus, an das der Serverdienst angebunden wird. Diese Einstellung ist optional.

Bei Nichtauswahl werden alle Netzwerke verwendet. Bei Auswahl eines Netzwerks verarbeitet der Server nur Daten dieser ausgewählten Netzwerkschnittstellen.

**Port**: Port für die Kommunikation zwischen ATOSS Time Control-Clients und Server. Standardwert ist '2711'.

**Hinweis:**

- Ändern Sie diesen Port nur in Ausnahmesituationen (z. B. bei mehreren parallelen Installationen von ATOSS Time Control auf demselben Server).
- Für Testzwecke ist eine manuelle Angabe des ATOSS Time Control-Server-Ports über die Kommandozeile mit dem folgenden Aufruf möglich: `atcs.exe -port [Portnummer]`.

**SSL-Port**: Wert für den SSL-Port. Standardwert ist 0.

**Hinweis:** Für Testzwecke ist eine manuelle Angabe des ATOSS Time Control-SSL-Ports über die Kommandozeile mit dem folgenden Aufruf möglich: `atcs.exe -sslport [Portnummer]`.

**Zertifikatspeicher**: Für eine SSL-verschlüsselte Kommunikation zwischen Server und Clients geben Sie hier den Pfad zu der *Datei für das SSL-Zertifikat (*.pfx)* an.

**Passwort für Zertifikatspeicher**: Geben Sie hier das Kennwort für das Zertifikat an.

**Serverkommunikationsport**: Wert für die Serverkonsole. Standardwert ist 12711.

### Gruppe 'Optionen'

Diese Gruppe umfasst kundenspezifische Einstellungen, die von Ihrem ATOSS CSD-Berater bei der Installation vorgenommen werden.

Weitere Informationen zu dieser Gruppe finden Sie in der Online-Hilfe.

### Gruppe 'Sonstiges'

**Projektstatus bei Neuanlage** (frei, gesperrt, abgeschlossen): Definieren Sie einen Status für ein neu angelegtes Projekt. Diese Option ist nur bei installiertem Modul 'Projektverfolgung' verwendbar.

**Gerät für Arbeitsplatzzeiterfassung**: Definieren Sie das Gerät, das den zu verwendenden Belegungsplan für die Arbeitsplatz-Zeiterfassung enthält. Diese Option ist nur bei installiertem Modul 'Arbeitsplatz-Zeiterfassung' verwendbar.

### Gruppe 'Sicherheit'

**Authentifizierungsmodul** (Standard-Authentifizierung, Ausweis-Authentifizierung, Externe Authentifizierung, Kerberos-Authentifizierung, Systembenutzeranmeldung (ohne Passwort)): Bestimmen Sie die für die Clients zu verwendende Art der Anmeldung.

**Tipp:** Detaillierte Informationen zu den Time Control-Authentifizierungen finden Sie unter *Authentifizierungsmodule*.

**Server-Passwort**
Hier haben Sie die Möglichkeit, das Passwort für den Benutzer 'system' zu ändern.

**Hinweis:** Dokumentieren Sie das Passwort, um einen konstanten Zugriff auf ATOSS Time Control zu gewährleisten.

**Anmelde-Maske** und **Anmelderegeln**
Hier definieren Sie die Übergabe des Anmeldedialogs an ATOSS Time Control.

Weitere Informationen dazu finden Sie in der Online-Hilfe.

#### Gruppe 'Verarbeitung'

**Abgebrochene Berechnungen bei Serverstart neu einfügen** (ja, nein): Bei aktivierter Option werden beim Serverstart gefundene abgebrochene Berechnungen sofort nach Neustart neu berechnet. Bei deaktivierter Option werden alle nicht berechneten Daten erst bei der nächsten Neuberechnung berücksichtigt.

**Geplante Berechnungen bei Serverstart neu einfügen** (ja, nein): Bei aktivierter Option werden offene Neuberechnungsaufträge, die z. B. durch Beenden des Serverdienstes nicht abgeschlossen wurden, in die Neuberechnungswarteschlange eingereiht und abgearbeitet.

### 4.5.7.2 E-Mail-Versandoptionen konfigurieren

Für den E-Mail-Versand sind Optionen für den Workflow sowie für Spezialfälle konfigurierbar.

#### Versandoptionen für den Workflow

Konfigurieren Sie E-Mail-Versandoptionen für den Workflow über die Registerkarte 'E-Mail'.

**Host**: Geben Sie hier den Namen des Mailservers oder die IP-Adresse an.

**Port**: Geben Sie hier den Port an, über den der Mailserver für den Mailversand erreichbar ist. Standardwert ist '25'.

**Absender-Adresse**: Geben Sie hier eine Mail-Adresse an, die als Absender von Mails verwendet wird.

**Authentifizierung notwendig** (ja, nein): Eine aktivierte Option macht eine Authentifizierung für den Mailserver erforderlich.

#### Gruppe 'Zugangsdaten'

**Benutzer**: Geben Sie einen Benutzer an.

**Kennwort**: Geben Sie ein Kennwort an.

#### Gruppe 'Fehler per Mail versenden'

**Empfänger-Adresse (leer zum Deaktivieren)**: E-Mail-Adresse, an die Fehlermeldungen des Servers gesendet werden.

**Kundeninformation mitsenden** (ja, nein): Bei aktivierter Option sind die in der Lizenz hinterlegten Kontaktdaten des Kunden in der E-Mail enthalten.

**Tipp:** Die Schaltfläche **Testmail** ermöglicht Ihnen die Eingabe einer Mailadresse, an die zu Testzwecken eine Mail verschickt wird. Dies dient zur schnellen Prüfung der Mailversandfunktion.

#### Versandoptionen für Spezialfälle

Konfigurieren Sie E-Mail-Versandoptionen für Spezialfälle über die Registerkarte 'Kuriositäten'.

Weitere Informationen zu dieser Registerkarte finden Sie in der Online-Hilfe.

#### 4.5.7.3 Kalenderintegration konfigurieren

Konfigurieren Sie auf der Registerkarte 'Kalender-Integration', ob und wie in ATOSS Time Control eingetragene Fehlzeiten per E-Mail als Kalenderdaten nach dem iCalendar-Standard versandt werden.

Weitere Informationen zu dieser Registerkarte finden Sie in der Online-Hilfe.

#### 4.5.7.4 Zutrittskontrolle konfigurieren

Auf der Registerkarte 'Zutrittskontrolle' konfigurieren Sie, ob ein Zutrittsereignis eine automatische E-Mail-Benachrichtigung an einen definierten Empfänger auslöst. Bei aktivierter E-Mail-Benachrichtigung werden Alarmmeldungen bei folgenden Ereignissen versendet:

| Geräteklasse | Ereignis |
|---|---|
| PCS | PCS Sabotage Fehler |
| | Auswertung Türrahmenkontakt: Tür ist zu lange geöffnet |
| PWR | Auswertung Türrahmenkontakt: Tür ist zu lange geöffnet |
| | Auswertung Sabotage |
| Kaba | Stempelsätze mit der Satzart X aus der BCOMM |
| | Statussätze mit Fehlern |
| Allgemein | Ausweis ohne Mitarbeiterzuordnung |

Die E-Mail-Benachrichtigung aktivieren Sie wie folgt:

1. Aktivieren Sie in der Gruppe 'E-Mail-Einstellungen' das Kontrollkästchen **Per Mail versenden**.
   Das Feld **E-Mail-Adresse des Alarm-Mail-Empfängers:** wird aktiv.
2. Geben Sie die E-Mail-Adresse des Empfängers an.
3. Bestätigen Sie die Eingabe mit **Speichern**.

**Hinweis:** Angaben in der Gruppe 'Skript-Einstellungen' sind nur für kundenspezifische Installationen erforderlich.

#### 4.5.7.5 Speicher konfigurieren

Über die Registerkarte 'Speicher-Management' bearbeiten Sie die Speicherkonfiguration.

Unabhängig vom Lizenzumfang des Kunden beinhaltet die Registerkarte für die Gruppen 'Server-Dienst', 'Geräteprozess-Dienst' und 'Webserver-Dienst' eine Gegenüberstellung von aktuellen Werten und empfohlenen Werten, die sich an der Auswahl der Anzahl aktiver Mitarbeiter im Feld **Empfehlung** orientieren.

**Tipp:** In der Gruppe 'Server-Dienst' bestimmt das Feld **Verbindungen** die maximal mögliche Anzahl gleichzeitig aufbaubarer Verbindungen zum Datenserver. Damit ist es z. B. möglich, die Anzahl gleichzeitig angemeldeter Benutzer im Webclient zu begrenzen. Weitere Informationen zum Speicherbedarf in verschiedenen Anwendungsszenarien finden Sie im Dokument 'ATOSS Time Control Freigaben und Voraussetzungen'.

Unter dem Feld wird Ihnen die aktuelle Größe des Arbeitsspeichers sowie des Java-Heap-Speichers angezeigt.

Den Speicher konfigurieren Sie wie folgt:

1. Wählen Sie im Feld **Empfehlung** die Anzahl der aktiven Mitarbeiter.
   Die Felder der Gruppen passen die Inhalte der gewählten Anzahl Mitarbeiter an. Gültige Werte sind grün, ungültige Werte rot hinterlegt.
2. Konfigurieren Sie die Felder **Aktuell** entweder manuell oder mit der Schaltfläche **Vorgabewerte übernehmen**.

- Ein Anpassen der Werte in den Feldern **-Xms** und **-Xmx** ermöglicht eine verbesserte Anwendungsperformance. **-Xms** definiert die Anfangsgröße, **-Xmx** die maximale Größe des Java-Heap-Speichers. Bei ausreichend zur Verfügung stehendem Speicher tragen Sie für **-Xms** einen Wert ein, der mindestens einem Viertel des im jeweiligen Feld **-Xmx** eingetragenen Werts entspricht.
- Mit der Schaltfläche **Vorgabewerte übernehmen** werden die empfohlenen Werte in die Felder **Aktuell** übertragen.

3. Bestätigen Sie Ihre Konfiguration mit **Speichern**.
   Die Einstellungen werden für die einzelnen Dienste übernommen.

   **Hinweis:** Zusätzlich wird die aktuell ausgewählte Vorgabe gespeichert. Beim nächsten Aufruf der Registerkarte 'Speicher-Management' werden die ausgelesenen Speicherwerte gegen die Vorgabe geprüft.

   Die Dienste werden anschließend neu gestartet.

#### 4.5.7.6 Externe Datenquellen konfigurieren

Datenquellen für den externen Import über eine JDBC-Schnittstelle konfigurieren Sie auf der Registerkarte 'Externe Datenquellen'. Diese enthält eine Tabelle, die ggf. bereits definierte Datenquellen anzeigt.

**Tipp:** Normalerweise referenziert die Angabe des Data Source Name (DSN) in einer externen Importbeschreibung eine ODBC-Datenquelle. Findet der DSN eine hier konfigurierte Datenquelle, wird diese anstelle einer ODBC-Datenquelle für den externen Import verwendet.

Folgende Aktionen stehen Ihnen auf der Registerkarte zur Verfügung:

| Aktionen | |
|---|---|
|  | **Konfiguration einer neuen externen Datenquelle** |
|  | **Bearbeiten der ausgewählten Datenquelle** |
|  | **Löschen der selektierten Datenquelle** |

Eine neue externe Datenquelle legen Sie wie folgt an:

1. Wählen Sie die Aktion **Konfiguration einer neuen externen Datenquelle** aus.
   Der modale Dialog 'Datenquelle bearbeiten' öffnet sich.
2. Geben Sie einen Namen für die Datenquelle an, über den diese in der Beschreibung eines externen Imports referenziert wird.

   Der Name der Datenquelle darf in der Datenbank für externe Datenquellen nur einmal enthalten sein.
3. Geben Sie die Eigenschaften der Datenquelle an.

| Feld | Erläuterung |
|---|---|
| **Typ**: | Legen Sie den Typ (Treiber) der externen Datenquelle fest. Dieser Typ muss dem Datenbanksystem entsprechen, auf dem sich die externe Datenquelle befindet. Weitere Informationen dazu entnehmen Sie der Dokumentation des jeweiligen Datenbanksystems. |
| **Host**: | Geben Sie die IP-Adresse oder den DNS-Namen des Server an, auf dem sich die externe Datenquelle befindet.<br>Diese Angabe ist für verzeichnisbasierte Datenbanken (CSV, Apache Derby) nicht relevant. |

| Feld | Erläuterung |
|---|---|
| **Port**: | Geben Sie den TCP/IP-Port an, mit dem der Datenbankserver einer serverbasierten externen Datenquelle angesprochen wird.<br>Diese Angabe ist für verzeichnisbasierte Datenbanken (CSV, Apache Derby) nicht relevant. |
| **Benutzer**: | Geben Sie den Benutzernamen für die Verbindung mit dem Datenbanksystem der externen Datenquelle an. |
| **Passwort**: | Geben Sie das Passwort für den Datenbankbenutzer an. |
| **Datenbank**: | Wählen Sie die Datenbank auf dem externen Datenbanksystem aus. |

Mit der Schaltfläche **Erweitert** öffnen Sie den modalen Dialog 'Erweiterte Eigenschaften'. Hier haben Sie die Möglichkeit, zusätzliche Eigenschaften des Datenbanktreibers anzugeben.

4. Bestätigen Sie Ihre Angaben mit **OK**.
   Die Tabelle zeigt die erstellte externe Datenquelle an.

Angaben zu einer bereits in der Tabelle angezeigten externen Datenquelle bearbeiten Sie, indem Sie diese markieren und die Aktion **Bearbeiten der ausgewählten Datenquelle** ausführen. Der modale Dialog 'Datenquelle bearbeiten' öffnet sich dann mit den für diese Datenquelle definierten Angaben.

#### 4.5.7.7 Proxy-Server konfigurieren

Haben Sie ATOSS Time Control auf einem Computer ohne direkten Internetzugriff installiert, ist über die Registerkarte 'Proxy-Einstellungen' die Angabe eines Proxy-Servers möglich.

**Hinweis:** Diese Einstellungen sind nur für das Update der Online-Lizenzierung relevant. Eine Verbindung zum Lizenzserver ist nur mit gültigen Proxy-Einstellungen möglich.

Weitere Informationen zu dieser Registerkarte finden Sie in der Online-Hilfe.

#### 4.5.7.8 Basisverzeichnisse anlegen

Sie haben die Möglichkeit, jeweils ein Basisverzeichnis für Mitarbeiterdaten und eins für Dokumente anzulegen.

##### Basisverzeichnis für Mitarbeiterdaten

Ein Basisverzeichnis für Mitarbeiterdaten legen Sie über die Registerkarte 'Basisverzeichnis für Mitarbeiterdateien (Server)' an. Bei entsprechender Konfiguration des Clients werden automatisierte Auswertungen in ein angelegtes Basisverzeichnis geschrieben. Für jeden Benutzer wird bei Bedarf automatisch ein Unterverzeichnis angelegt. In ein konfiguriertes Basisverzeichnis ist z. B. mit Hilfe eines geplanten Tasks die Erstellung automatisierter Reports möglich.

##### Basisverzeichnis für Dokumente

Ein Basisverzeichnis für Dokumente legen Sie über die Registerkarte 'Basisverzeichnis für Dokumente (Server)' an. Ähnlich wie das Basisverzeichnis für Mitarbeiterdaten nutzt das 'Basisverzeichnis Dokumente' ebenfalls eine Ordnerstruktur. Im Client greifen Sie über **Mitarbeiterinformationen** > **Dokumentenablage** auf dieses Verzeichnis zu und können dort Dokumente ablegen.

Anwendungsbeispiele zu den Basisverzeichnissen finden Sie in der Online-Hilfe.

#### 4.5.7.9 Mitarbeiterprüfungszeit konfigurieren

Verwenden Sie die Mitarbeiterprüfungszeit, um auch für Tage mit Mitarbeiterfehlzeiten aktuelle Saldenwerte vorliegen zu haben. Zu diesem Zeitpunkt wird für alle Mitarbeiter für das aktuelle Intervall (i. d. R. der aktuelle Monat) eine Neuberechnung ausgelöst.

1. Aktivieren Sie die Mitarbeiterprüfung über das Kontrollkästchen **Aktivieren der Mitarbeiterprüfungszeit**.
2. Geben Sie eine Startzeit im Feld **Überprüfung der Mitarbeiter startet um** an.

   **Tipp:** Wählen Sie eine Zeit mit geringem Zugriff auf Serverressourcen.

3. Bestätigen Sie die Angaben mit **Speichern**.
   Sie sehen die Meldung 'Mitarbeiterprüfungszeit konfiguriert'. Zum angegebenen Zeitpunkt erfolgt für alle Mitarbeiter für das aktuellen Intervall, i. d. R. den aktuellen Monat, eine Neuberechnung.

### 4.5.8 Grundlegende Installationseinstellungen des Servers festlegen

Die grundlegenden Installationseinstellungen des Servers sind über die jeweiligen Registerkarten unter **Navigation** > **Installation** der Konsole erreichbar.

Eine Konfiguration der Installationseinstellungen kann folgende Schritte umfassen:

1. *Repositories für Updates und Client-Erweiterungen konfigurieren*
2. *ATOSS Time Control-Produkte installieren, deinstallieren oder updaten*

   **Hinweis:** Ein Installieren von Client-Erweiterungen ist bei Standard-Installationen nicht erforderlich.

   Weitere Informationen dazu finden Sie in der Online-Hilfe.

3. *Skripte installieren*
4. *Anträge installieren*

   **Hinweis:** Dieser Schritt ist nur relevant, wenn das Modul 'Workflow-ESS' lizenziert ist.

5. *Vorgabedaten installieren*

   **Hinweis:** Dieser Schritt ist nur für eine Neuinstallation relevant.

#### 4.5.8.1 Repositories für Updates und Client-Erweiterungen konfigurieren

In den auf der Registerkarte 'Repositories' aufgeführten Bereichen sucht ATOSS Time Control nach aktuelleren Software-Versionen.

Folgende Aktionen sind über Schaltflächen und/oder das Menü ausführbar:

| Aktionen | |
|---|---|
|  | **Repository hinzufügen** |
|  | **Repository bearbeiten** |
|  | **Speicher-Management** |
| | **Repository spiegeln** (nur über das Menü verfügbar) |

| Aktionen | |
|---|---|
| | **Repository bereinigen** (nur über das Menü verfügbar) |

### Neues Repository hinzufügen

Um eine neues Repository anzulegen, führen Sie folgende Schritte aus:

1. Wählen Sie **Neues Repository hinzufügen**
   Der modale Dialog 'Neues Repository hinzufügen' öffnet sich.
2. Geben Sie eine ID sowie eine URI für das neue Repository an.
3. Aktivieren Sie ggf. das Kontrollkästchen **Spiegeln**.
4. Bestätigen Sie die Angabe mit **OK**.
   Das neu angelegte Repository erscheint in der Liste.

### Vorhandenes Repository bearbeiten

Um eine bestehendes Repository zu bearbeiten, führen Sie folgende Schritte aus:

1. Markieren Sie das zu bearbeitende vorhandene Repository in der Liste.
2. Doppelklicken Sie das markierte Repository oder wählen Sie **Repository bearbeiten**.
   Der modale Dialog 'Repository bearbeiten' öffnet sich.
3. Übernehmen Sie anschließend geänderte Einstellungen mit **OK**.
   Die Änderungen werden übernommen.

**Hinweis:** Um geänderte Einstellungen an den Repositories auf die Standardeinstellungen zurückzusetzen, löschen Sie alle in der Liste vorhandenen Repositories. Schließen Sie die Registerkarte 'Repositories' und öffnen Sie diese erneut. Danach sind die Standard-Repositories für Ihre Version hinterlegt, z. B.:
`https://atoss-timecontrol.com/7.2/rap`

## 4.5.8.2 ATOSS Time Control-Produkte installieren, deinstallieren oder updaten

Die Registerkarte 'Updates' informiert Sie über derzeit installierten ATOSS Time Control-Produktversionen und die jeweils online verfügbare aktuelle Version.

| Verfügbare Aktionen | |
|---|---|
|  | **Nach Aktualisierungen suchen** |

Über die Aktion **Nach Aktualisierungen suchen** suchen Sie nach Aktualisierungen für die installierte ATOSS Time Control-Version.

### ATOSS Time Control-Produkt installieren

1. Zum Installieren eines neuen Produkts verwenden Sie die Schaltfläche **Installieren**
   Der modale Dialog 'Features installieren' öffnet sich.
2. Wählen Sie ein Repository.
3. Markieren Sie das zu installierende Produkt.
4. Starten Sie die Installation durch Bestätigen der Auswahl mit **Installieren**.

### ATOSS Time Control-Produkte deinstallieren

Deinstallieren Sie ein Produkt mit der Schaltfläche **Deinstallieren**. Nach Bestätigen der Meldung 'Wollen Sie das Feature wirklich deinstallieren?' wird das Produkt deinstalliert.

### ATOSS Time Control-Produkte aktualisieren

Eine installierte Version aktualisieren Sie über die Schaltfläche **Aktualisierungen installieren**.

#### 4.5.8.3 Skripte installieren

**Hinweis:** Führen Sie diesen Schritt bei einer Neuinstallation sowie nach jedem Update unbedingt aus, um sicherzustellen, dass die Datenbank aktuelle Skripte enthält.

Die Registerkarte 'Skript Installation' schlägt Ihnen eine Liste mit Skripten zur Installation vor.

| Verfügbare Aktionen | |
|---|---|
| | **Dokumentation anzeigen** |

Informationen zu einem Skript erhalten Sie über die Schaltfläche **Dokumentation anzeigen**.

**Tipp:**

- ATOSS Time Control erkennt automatisch die Aktualität der Skripte. Bereits installierte Skripte sind in der Liste nur enthalten, wenn Änderungen am Skript vorliegen, die eine Neuinstallation erfordern.
- ATOSS CSD empfiehlt für Neuinstallationen lediglich die Installation folgender Skripte:
  - Datenquelle Universal (für Auswertungen)
  - Verarbeitungsdaten exportieren (zur Fehlerbeseitigung)
  - Verarbeitungsdaten importieren (zur Fehlerbeseitigung)

Um ein Skript zu installieren, gehen Sie wie folgt vor:

1. Aktivieren Sie das Kontrollkästchen vor dem zu installierenden Skript.

   **Tipp:** Mit den Schaltflächen **Alle** und **Keine** aktivieren bzw. deaktivieren Sie sämtliche Kontrollkästchen auf einmal.

2. Starten Sie die Installation des gewählten Skripts durch Bestätigen der Auswahl mit **Jetzt installieren**.

#### 4.5.8.4 Anträge installieren

Anträge sind bei der Installation der ATOSS Time Control bereits enthalten. Sie werden bei jedem Update automatisch aktualisiert. Es ist jedoch möglich, zusätzliche Anträge anzulegen.

**Hinweis:** Dieser Schritt ist nur relevant, wenn das Modul 'Workflow-ESS' lizenziert ist.

| Verfügbare Aktionen | |
|---|---|
| | **Neu (Einfügen)** |

Um einen zusätzlichen Antrag anzulegen, gehen Sie wie folgt vor:

1. Öffnen Sie die Ansicht 'Arbeitsabläufe'.
2. Wählen Sie die Schaltfläche **Neu (Einfügen)**.

   Der Dialog 'Importiere Antragsdefinition' öffnet sich.

3. Wählen Sie eine der folgenden Optionen aus:
   - Importiere eine Standardantragsdefinition
   - Verwende eine Standardantragsdefinition als Vorlage
   - Erstelle eine leere Antragsdefinition
   - Aus Datei:
4. Bestätigen Sie Ihre Auswahl mit **OK**.
   Der Arbeitsablauf wird in der Tabelle der Ansicht hinzugefügt.

#### 4.5.8.5 Vorgabedaten installieren

Dieser Schritt ist nur für eine Neuinstallation relevant. Er dient dazu, nach der Installation bereits auf vordefinierte Datenbestände, z. B. Standardauswertungen, zurückgreifen zu können.

**Achtung:** Installieren Sie die Vorgabedaten nur bei einer Neuinstallation! Wenn Sie Vorgabedaten bei einem Update installieren, kann dies zur Zerstörung der zeitwirtschaftlichen Konfiguration führen.

**Hinweis:** Der einzige Datensatz, dessen Installation nach einem Update ohne negative Konsequenzen bleibt, ist 'Skriptgruppen für Standardauswertungen aller Module'.

Die Registerkarte 'Vorgabe-Daten' schlägt Ihnen eine Liste mit bereits vordefinierten Datenbeständen zur Installation vor.

| Verfügbare Aktionen | |
|---|---|
| | **Dokumentation anzeigen** |

Informationen zu ausgewählten Vorgabedaten erhalten Sie über die Schaltfläche **Dokumentation anzeigen**.

Um Vorgabedaten zu installieren, gehen Sie wie folgt vor:

1. Aktivieren Sie das Kontrollkästchen vor dem zu installierenden Datensatz.

   **Tipp:** Mit den Schaltflächen **Alle** und **Keine** aktivieren bzw. deaktivieren Sie sämtliche Kontrollkästchen auf einmal.

2. Starten Sie die Installation der gewählten Datensatzes durch Bestätigen der Auswahl mit **Jetzt installieren**.

### 4.5.9 Geräteprozesseinstellungen des Servers festlegen

Die Geräteprozesseinstellungen sind über die jeweiligen Registerkarten unter **Navigation** > **Geräteprozess** der Konsole erreichbar.

Die Konfiguration der Geräteprozesseinstellungen kann folgende Schritte umfassen:

1. *Log-Dateien einlesen*
2. *Grundlegende Geräteprozesseinstellungen konfigurieren*
3. *E-Mail-Versandoptionen konfigurieren*
4. *Treiber konfigurieren*

#### 4.5.9.1 Log-Dateien einlesen

**Achtung:** Unbedachtes Ausführen dieses Schritts kann zu Beschädigungen an korrekten Stempeldaten führen!

Die Registerkarte 'Log-Dateien einlesen' ermöglicht Ihnen, Stempelaktionen aus Log-Dateien von Gerätegruppen zu importieren, um so, z. B. bei einem Datenverlust, gezielt bestimmte Logdateien von

Zeiterfassungsgeräten nachzulesen. Folgende Log-Dateien können zum Einlesen von Stempeldaten geladen werden:

- intus.log, th_output.dat
- dtp.log
- tcbooking.log
- .booking

Um eine Log-Datei einzulesen, gehen Sie wie folgt vor:

1. Wählen Sie mit **Datei wählen** eine Log-Datei aus.
2. Schränken Sie ggf. den Zeitbereich der Log-Datei über die Felder **Von:** und **Bis:** ein.
3. Um Stempelaktionen für alle Geräte einzulesen, aktivieren Sie das Kontrollkästchen **Alle Geräte**.
4. Wählen Sie **Log-Datei einlesen**.
   Die Log-Dateien im angegebenen Zeitraum werden geladen und sind in der Tabelle sichtbar.
5. Starten Sie das Einlesen der Dateien mit **Import starten**.

#### 4.5.9.2 Grundlegende Geräteprozesseinstellungen festlegen

Nehmen Sie auf der Registerkarte 'Einstellungen' grundlegende Geräteprozesseinstellungen in den folgenden Gruppen vor:

##### Geräteprozess

**Port**: Port, über den der Geräteprozess mit dem Datenserver kommuniziert. Standardwert ist '2411'.

##### Server

**Host**: IP-Adresse oder Hostname des Datenservers. Verwenden Sie hier '127.0.0.1' oder die IP des ATOSS Time Control-Servers.

**Port**: Datenserverport. Standardwert ist '2711'.

**SSL**: Aktivieren Sie diese Option für einen über SSL verschlüsselten Datenserverdienst.

**Timeout**: Wird eine Anfrage nach der angegebenen Zeit vom Datenserver nicht beantwortet, wird ein Timeout protokolliert. Der Standardwert '10000' entspricht einer Zeit von 10 Sekunden.

**Kennwort**: Kennwort des Systembenutzers in ATOSS Time Control.

##### Zu verwaltende Geräte

**Hinweis:** Verwenden Sie diese Einstellungen für die Mehrfachinstallation eines Geräteprozesses. Für eine Standardumgebung ist keine Konfiguration erforderlich. Weitere Informationen zur Aufteilung des Geräteprozesses finden Sie im Anhang.

**Terminals**: Liste der in ATOSS Time Control zu überwachenden Geräte.

**Geräte-Busse**: Liste der in ATOSS Time Control zu überwachenden Geräte-Busse.

#### 4.5.9.3 E-Mail-Versandoptionen für den Geräteprozess konfigurieren

Legen Sie auf der Registerkarte 'E-Mail-Versand' die Versandoptionen für den Geräteprozess in den Gruppen 'Mailversand bei außerordentlichen Vorgängen' und 'SMTP-Einstellungen' vor.

#### 4.5.9.4 Treiber für den Geräteprozess konfigurieren

Treiber sind sowohl für Kaba-Geräte als auch PCS-Geräte konfigurierbar.

#### Kaba-Treibereinstellungen

**Applikationsschnittstelle: Port**: Port der B-COMM Java-Applikationsschnittstelle.

**RMI: Host**: IP oder Hostname des Servers, auf dem B-COMM Java läuft.

**RMI: Port**: RMI-Port, über den B-COMM Java erreichbar ist.

#### PCS-Treibereinstellungen

Für Informationen zum Einsatz von PCS-Fingerprint-Hardware wenden Sie sich an Ihren ATOSS CSD-Berater oder den *Support*.

### 4.5.10 Serverkonfiguration übernehmen

Ihre Änderungen an den Servereinstellungen übernehmen Sie mithilfe eines Neustarts des Datenservers:

1. Führen Sie die Aktion **Datei** > **Server neu starten** aus.
   Geöffnete Clients erhalten die Meldung, dass die Verbindung zum Datenserver getrennt wurde. Nach erfolgreichem Neustart ist eine manuelle erneute Anmeldung der Clients möglich.
2. Starten Sie anschließend ebenfalls den Webserverdienst sowie den Geräteprozessdienst neu.
   Über **Datei** > **Systemdienste** öffnen Sie einen modalen Dialog, der Ihnen das gezielte Starten, Stoppen oder Neustarten einzelner Dienste ermöglicht.
   Die Grundinstallation von ATOSS Time Control ist damit beendet.

## 4.6 Startvariante konfigurieren

Nach erfolgreicher Installation ist ATOSS Time Control für zwei Startvarianten konfigurierbar:

- *Windows-Dienst*
- *Konsolenanwendung*

Verwenden Sie für Produktivumgebungen generell den Windows-Dienst. Greifen Sie auf die Konsolenanwendung lediglich in Ausnahmefällen zu Testzwecken und zur Fehlersuche zurück.

### 4.6.1 ATOSS Time Control als Windows-Dienst starten

Nach der ATOSS Time Control-Installation startet der Windows-Dienst automatisch.

**Tipp:** Technisch nutzt jeder ATOSS Time Control-Dienst eine `service.exe`-Datei, die wiederum eine dazugehörige `java.exe`-Datei startet. Im Windows Task-Manager finden Sie unter 'Prozesse' daher mehrere `service.exe`- und `java.exe`-Dateien. Eine Zuordnung der Prozesse ist über den Task-Manager möglich, indem Sie sich zusätzlich die Befehlszeile anzeigen lassen: Dort finden Sie die Information zum Prozess, z. B.:

Server: `-Dosgi.instance.area=C:/ProgramData/atc/server`

Zum manuellen Starten des Windows-Dienstes gehen Sie wie folgt vor:

1. Wählen Sie in Ihrem Windows-Betriebssystem **Start** > **Systemsteuerung** > **System und Sicherheit** > **Verwaltung** > **Dienste**.
   Dort finden Sie die ATOSS Time Control-Dienste für den Server.
2. Markieren Sie einen Time Control-Dienst und führen Sie **Eigenschaften** aus.
3. Ändern Sie ggf. die Angabe im Feld **Starttyp** auf 'Automatisch' und bestätigen Sie mit **OK**.
   Mit dieser Einstellung startet bei einem Serverneustart dieser Dienst automatisch mit.
4. Führen Sie ggf. die Schritte 2 und 3 für weitere ATOSS Time Control-Dienste aus.
5. Markieren Sie den manuell zu startenden Serverdienst und führen Sie die Aktion **Starten** aus.

Der Serverdienst startet neu.

**Hinweis: Laden von kundenindividuellen Plugins verhindern**
Im Repository von ATOSS Time Control hinterlegte kundenindividuelle Plugins können, z. B. aufgrund von Inkompatibilitäten bei Updates, das Starten des Servers verhindern. Um diese Plugins beim Serverstart nicht zu laden, fügen Sie der Startparameterdatei (`atc.ini` für einen als Anwendung laufenden Server bzw. `wrapper.conf` im Verzeichnis `%programdata%/atc` für den Betrieb mit Windows-Diensten) den Parameter **-dignoreplugins** hinzu.

### 4.6.2 ATOSS Time Control als Konsolenanwendung starten

**Hinweis:**
- Greifen Sie auf die Konsolenanwendung lediglich in Ausnahmefällen zu Testzwecken und zur Fehlersuche zurück.
- Führen Sie bei aktivierter Benutzerkontensteuerung unter Windows den Start der Konsolenanwendung unbedingt als Administrator durch, da sonst der ATOSS Time Control-Server nicht startet.

Starten Sie die Konsolenanwendung über die Verknüpfung **Start** > **ATOSS Time Control** > **Server starten**.

Die verknüpfte Datei finden Sie unter `ATOSS Time Control/Server/atcs.exe`.

#### Log-Dateien in Workspaceverzeichnissen

Bei Fehlern werden von ATOSS Time Control (Server und Client) Logdateien in die Workspaceverzeichnisse geschrieben. Die Standard-Workspaces sind:

| | |
|---|---|
| Konsole: | `%programdata%/atc/.metadata/.log` |
| Client: | `%appdata%/atc/.metadata/.log` |

## 4.7 Sprache der Serverdienste ändern

Um die Sprache innerhalb der Serverdienste zu ändern, gehen Sie wie folgt vor:

1. Navigieren Sie zum ATC Server Workspace (`%WORKSPACE%\%PRODUCT%\wrapper.conf`),
   z. B. `C:\ProgramData\atc73\server\wrapper.conf` (für Server).
2. Bearbeiten Sie als Administrator die Datei `wrapper.conf`.
3. Um die Sprache auf 'Englisch' umzustellen, fügen Sie folgende Zeile nach der höchsten Nummer `%maxnummer%` ein: `wrapper.java.additional.%maxnummer+1%=-Dosgi.nl=en`
4. Speichern Sie die Datei.
5. Starten Sie die Serverdienste neu.

Möchten Sie mit mehreren Diensten arbeiten, z. B. einem Dienst für Deutsch und einem für Englisch, haben Sie die Möglichkeit, dem Dienst einen Parameter zu übergeben. Ersetzen Sie dazu den Aufruf

```
"C:\Program Files\ATOSS\timecontrol73\server\service.exe"
```

durch

```
"C:\Program Files\ATOSS\timecontrol73\server\service.exe atcconfig=c:\programdata\atc\server_english"
```

Durch einen direkten Aufruf der Datei `service.exe` ist es ebenfalls möglich, alle Einstellungen des Dienstes für den Aufruf in der Eingabeaufforderung zu verwenden. Dafür ist lediglich die Angabe des Parameters **-Wservice.mode=false** erforderlich:

```
"C:\Program Files\ATOSS\timecontrol73\server\service.exe atcconfig=c:\programdata\atc\server_english
-Wservice.mode=false"
```

Für weitere Informationen dazu wenden Sie sich an Ihren ATOSS CSD-Berater oder den *Support*.

### 4.7.1 Beispiel für Mehrsprachigkeit

Änderungen beim Verwenden von mehrsprachigen Datenbanken werden sprachabhängig gespeichert.

| | |
|---|---|
| **Hauptsprache der Datenbank**: | DE |
| **Mitarbeiter 'EN'**: | Einstellung der Sprache 'Englisch' |
| **Mitarbeiter 'DE'**: | Einstellung der Sprache 'Deutsch' |

Änderungen von Datensätzen funktionieren wie folgt:

1. Mitarbeiter 'DE' fügt der Datenbank einen neuen Datensatz hinzu: Arbeitsplatz 1 mit der Bezeichnung 'Kasse'.
2. Mitarbeiter 'EN' loggt sich ein: Arbeitsplatz 1 wird ihm als 'Kasse' angezeigt.
3. Mitarbeiter 'DE' loggt sich ein und ändert die Bezeichnung von Arbeitsplatz 1 von 'Kasse' zu 'Kasse neu'.
4. Mitarbeiter 'EN' loggt sich ein: Arbeitsplatz 1 heißt nun auch für ihn 'Kasse neu'.
5. Mitarbeiter 'EN' ändert Arbeitsplatz 1 zu 'Cash register'.
6. Mitarbeiter 'DE' loggt sich ein. Arbeitsplatz 1 heißt für ihn trotzdem weiter 'Kasse neu'.
7. Mitarbeiter 'DE' ändert den Namen von 'Kasse neu' zu 'Kasse neu zwei'.
8. Mitarbeiter 'EN' loggt sich ein. Arbeitsplatz 1 heißt für ihn noch immer 'Cash register'.

Ein Datensatz wird so lange in der eingestellten Hauptsprache der Datenbank angezeigt, bis er in einer anderen Sprache geändert wurde. Änderungen des Datensatzes in der Hauptsprache werden nach der Änderung des Datensatzes in der Fremdsprache in diese nicht automatisch übertragen.

## 4.8 AMIS für Mobile Workforce Management

**Einschränkung:** Diese Funktionalität können Sie nur nutzen, wenn Sie das Modul 'ATOSS Mobile Workforce Management' lizenziert haben.

**Hinweis:** Für den Betrieb von AMIS ist ein Applikationsserver (bevorzugt 'Apache Tomcat') mit JAVA 11 erforderlich. Dazu muss ein eigenes OpenJDK 11 eingesetzt werden.

Um über die Mobile Workforce Management Anwendung auf einem iPhone/iPad oder Android Smartphone/Tablet auf ATOSS Time Control zugreifen zu können, ist es erforderlich, den ATOSS Mobile Information Server (AMIS) im Applikationsserver zu aktivieren und das Mobilgerät mit AMIS zu verknüpfen.

Als Schnittstelle zur ATOSS Time Control ist AMIS die Zieladresse für mobile Anfragen. AMIS prüft und verarbeitet alle vom Benutzer im ATOSS Mobile WFM generierten Aktionen wie z. B. Anmeldung oder Antragsstellung und interpretiert alle ankommenden mobilen Anfragen.

#### Zugehörige Themen

*AMIS im Applikationsserver aktivieren* auf Seite 33

*AMIS.properties-Parameter konfigurieren* auf Seite 35

### 4.8.1 AMIS im Applikationsserver aktivieren

**Hinweis:** Das Modul AMIS ist nur einsetzbar, wenn Sie eine Lizenz für das Modul 'ATOSS Mobile Workforce Management' besitzen.

Ab ATOSS Time Control 8 ist es erforderlich, AMIS auf einem Applikationsserver (bevorzugt 'Apache Tomcat') zu installieren. Das AMIS Web Application Archive finden Sie im Server-Verzeichnis der Installation.

Die Beschreibung für das Installieren eines Web Application Archive finden Sie in den jeweiligen Dokumentationen zur Installation der Applikationsserver.

**Einschränkung:** Stellen Sie bei der Konfiguration des Moduls AMIS sicher, dass der Applikationsserver Apache Tomcat installiert ist. Für die Installation ist der Apache Tomcat 9-Applikationsserver notwendig.

**Hinweis:** Die ATOSS Time Control Mobile Workforce Management-Anwendung informiert Sie, z. B. bei Buchungen, mit einem Hinweis über ausgeschaltete Ortungsdienste. Detaillierte Informationen, wie Sie den Hinweis deaktivieren, finden Sie im 'ATOSS Time Control Referenzhandbuch' unter 'Hinweis bei ausgeschalteten Ortungsdiensten für Mobile Workforce Management-Anwendung deaktivieren'.

Wenn Sie Umlaute und andere Sonderzeichen für Passwörter verwenden, müssen Sie das Encoding bei der manuellen Installation des Apache Tomcat-Applikationsservers des 'Apache Tomcat' anpassen. Fügen Sie den neuen Eintrag zur Tomcat-Konfiguration wie folgt hinzu:

1. Führen Sie die Datei *tomcat path*`\bin\Tomcat9w.exe` aus.
2. Wechseln Sie zur Registerkarte 'Java'.
3. Unter 'Java Optionen' muss die folgenden Reihe enthalten sein:
   - `-Dfile.encoding=UTF-8`

### Weiterführende Links

Informationen zur Installation auf einem Apache Tomcat-Applikationsserver finden Sie unter folgenden Links:

- Tomcat Web Application Deployment:*https://tomcat.apache.org/tomcat-9.0-doc/deployer-howto.html*
- Tomcat Web Application Manager: *https://tomcat.apache.org/tomcat-9.0-doc/manager-howto.html*

**Hinweis:** Nach jedem Update ist es erforderlich, AMIS auch im Applikationsserver zu aktualisieren. Bei den meisten Applikationsservern reicht es aus, dazu das Web Application Archive zu überschreiben.

Bei Fragen dazu wenden Sie sich an Ihren ATOSS CSD-Berater oder den *Support*.

Für eine Funktionsprüfung führen Sie folgenden Schritt aus:

1. Öffnen Sie einen Browser und geben Sie folgende Adresse ein: `http://127.0.0.1:8080/AMIS`. Wenn der Text 'Welcome to AMIS!' erscheint, ist AMIS aktiviert.

## 4.8.2 Tomcat Log-Level konfigurieren

Sie können Tomcat so konfigurieren, dass nur eine bestimmte Art von Informationen protokolliert wird. Der Ordner für die Tomcat-Installation enthält die Datei *tomcat path*`\config\logging.properties`. Damit können das Protokoll für die Tomcat-Konsole und /oder das Protokoll, das in der Datei `catalina.log` gespeichert wird, konfiguriert werden. Folgende Log-Level können Sie in der angegebenen Sortierung (niedrigste zur höchsten konfigurierbaren Priorität) verwenden:

- OFF
- SEVERE
- WARNING
- INFO
- CONFIG
- FINE

- FINER
- FINEST

Wenn das Log-Level die Priorität 'INFO' oder höher besitzt, werden alle Informationen protokolliert, d. h. das Protokoll kann auch sensitive Informationen enthalten. Bei einem Log-Level 'WARNING' oder 'SEVERE' wird sensitive Information nicht mehr protokolliert.

Die Standard-Datei `logging.properties` enthält die Definitionen der Log-Level bereits.

**Einschränkung:** Stellen Sie bei der Konfiguration des Moduls AMIS sicher, dass der Applikationsserver Apache Tomcat installiert ist. Für die Installation ist der Apache Tomcat 9-Applikationsserver notwendig.

#### Sensitive Informationen für die Tomcat-Konsole ausblenden

Es ist möglich, sensitive Informationen für die Tomcat-Konsole auszublenden. Dazu haben Sie zwei Möglichkeiten:

1. Bei bereits existierender Datei `logging.properties`:
   Setzen Sie die Eigenschaften der bestehenden Datei wie folgt:
   a) Log-Level der Tomcat-Konsole einstellen:
   ```
   java.util.logging.ConsoleHandler.level = WARNING
   ```
   b) Log-Level der Log-Datei *tomcat path*`\logs\catalina.log`) einstellen:
   ```
   1catalina.org.apache.juli.AsyncFileHandler.level = WARNING
   ```

2. Bei noch nicht-existierender Datei `logging.properties`:
   a) Erstellen Sie diese Datei wie folgt neu:
   ```
   handlers=java.util.logging.FileHandler, java.util.logging.ConsoleHandler
   java.util.logging.ConsoleHandler.level=WARNING
   java.util.logging.ConsoleHandler.formatter=java.util.logging.SimpleFormatter
   java.util.logging.FileHandler.level=WARNING
   java.util.logging.FileHandler.formatter=java.util.logging.SimpleFormatter
   ```
   b) Fügen Sie die neue Datei wie folgt in die Tomcat-Konfiguration ein:
      a) Führen Sie die Datei *tomcat path*`\bin\Tomcat9w.exe` aus.
      b) Wechseln Sie zur Registerkarte 'Java'.
      c) Unter 'Java Optionen' müssen die folgenden beiden Reihen enthalten sein:
         - `Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager`
         - `Djava.util.logging.config.file=*tomcat path*\conf\logging.properties`

**Hinweis:** Bei Fragen dazu wenden Sie sich an Ihren ATOSS CSD-Berater oder den *Support*.

### 4.8.3 AMIS.properties-Parameter konfigurieren

Funktionen innerhalb der ATOSS Mobile Workforce Management Anwendung sind über AMIS.properties-Parameter anpassbar. Die folgende Tabelle enthält eine Übersicht über die möglichen Parameter, die in der Datei AMIS.properties verwendet werden.

| Parametername | Typ | Standardwert | Erläuterung |
|---|---|---|---|
| **amis.absencemodule.ignoredaytypes** | String | 1 | Aufgrund der Möglichkeit eigene Tagestypen zu definieren, können Arbeitstage eine eigene Tagesartennummer haben. Mit |

| Parametername | Typ | Standardwert | Erläuterung |
|---|---|---|---|
| | | | diesem Parameter kann der Fehltagekalender Arbeitstage ignorieren, deren Nummern in einer kommaseparierten Liste von Tagesartennummern enthalten sind. Diese Einstellung ist im Modul 'Fehltagekalender' nicht sichtbar. |
| **amis.timezone.usedevicetimezone** | Boolean | false | Um bei Buchungen die Zeitzone des Mobilgeräts zu verwenden, setzen Sie **usedevicetimezone** auf den Wert 'true'. Daraus ergeben sich folgende Buchungsdatensätze: `Zeitstempel des Buchungsdatensatzes = Zeitstempel des Servers - Differenz der Zeitzonen`, wobei `'Differenz der Zeitzonen' = Zeitzone des Servers - Zeitzone des Mobilgeräts` |
| **show.client.field** | Boolean | false | Um das Feld **Mandant** im Anmeldefenster auszublenden, setzen Sie **show.client.field** auf den Wert 'false'. Bei neuen Installationen ist 'false' der Standardwert für den Parameter. Bei Updates ist es erforderlich, den Parameter manuell anzupassen. |
| **accountfilter** | String | leer | Verwenden Sie diesen Filter, wenn der Aufruf des Parameters **getAccounts** für den Standardbenutzer der Anwendung alle möglichen Buchungsarten ausgibt. Durch Angabe einer kommaseparierten Nummernliste schließen Sie mit diesem Parameter Zeitkonten für eine Kontierung aus. Die angegebenen Zeitkonten stehen anschließend nicht für eine Kontierung zur Verfügung. Wenn Sie z. B. die Zeitkonten 1, 2, 5 und 6 für eine Kontierung ausschließen möchten, setzen Sie den Wert des Parameters auf '1,2,5,6'.<br>**Hinweis:** Zeitkonten, die durch den Parameter **accountfilter** ausgeschlossen werden, werden dem Benutzer beim Kontierungsvorgang nicht angezeigt. |

| Parametername | Typ | Standardwert | Erläuterung |
|---|---|---|---|
| **absence.accountfilter** | String | leer | Verwenden Sie diesen Filter, wenn Sie den Parameter **getAccounts** für Fehlzeitenkonten (Buchungen und Abwesenheitsanträge) aufrufen. Durch Angabe einer kommaseparierten Nummernliste schließen Sie mit diesem Parameter Zeitkonten aus, die für die Erstellung von Abwesenheiten verwendet werden können. Wenn Sie z. B. die Zeitkonten 1, 2, 5 und 6 von einer Kontierung ausschließen möchten, setzen Sie den Wert des Parameters auf '1,2,5,6'. **Hinweis:** Zeitkonten, die durch den Parameter **absence.accountfilter** ausgeschlossen werden, werden dem Benutzer beim Kontierungsvorgang nicht angezeigt. |
| **ases.services.deployment.location** | String | http://local-host:8080/atc/webser-vices | Gibt den Ort des ATC-Servers an, der die Webdienste für die mobile Verwendung veröffentlicht. Der Wert entspricht dem des Parameters **atc.services.deployment.location**, der zum Testen der Anbindung verwendet wird. |
| **ases.services.proxy.url.enabled** | Boolean | false | Aktiviert/deaktiviert eine bestimmte Ressourcenanforderung (WSDL) durch Übergabe eines Proxy-URL-Parameters. |
| **atc.services.deployment.location** | String | http://local-host:8080/atc/webser-vices | Gibt den Ort des ATC-Servers an, der die Webdienste für die mobile Verwendung veröffentlicht. |
| **presence.workflowType** | String | WT1 | Der bei der Erstellung eines neuen Antrags zu verwendende Anwesenheitsworkflowtyp. |
| **clockedTimeType.break.color** | String | \#C5B8B0 | Die Farben der statischen Stempelzeittypen für die Zeitbuchung des Anwesenheitsworkflows. |
| **clockedTimeType.presence.color** | String | \#008000 | Die Farben der statischen Stempelzeittypen für die Zeitbuchung des Anwesenheitsworkflows. |

| Parametername | Typ | Standardwert | Erläuterung |
|---|---|---|---|
| **geoType** | Integer | 1 | Mit diesem Parameter definieren Sie, ob die Standortkoordinaten beim Einstempeln verwendet werden:<br>geoType = 1: Standortkoordinaten deaktiviert, keine Meldung<br>geoType = 3: Standortkoordinaten aktiviert. Bei ausgeschalteter Standortübermittlung Meldung bei jedem Einstempeln mit Rückfrage, ob die Standortübermittlung eingeschaltet werden soll. |

## 4.9 Verbindungsmanagement des Jetty-Webservers anpassen

Der Jetty-Webserver erkennt standardmäßig Verbindungen, die, z. B. durch Abmelden oder durch Schließen des Browser-Fensters, getrennt werden. Er schließt diese Verbindungen dann automatisch. Unter bestimmten Umständen (z. B. besondere Netzwerkumgebungen, ungeplante Netzwerkabbrüche, Firewall-Einstellungen) kann es vorkommen, dass dieser Standardmechanismus nicht funktioniert.

Für diesen Fall ist es möglich, den mit ATOSS Time Control mitgelieferten Jetty-Webserver so zu konfigurieren, dass eine offene Verbindung nach einer festgelegten Zeit von Inaktivität automatisch geschlossen wird.

Um diese Funktion zu aktivieren, editieren Sie die Datei `%Installation%/config/atc.properties` mit einem Texteditor wie folgt:

1. Entfernen Sie die Raute vor der Zeile `#context.sessioninactiveinterval=`.
2. Tragen Sie den gewünschten Wert (in Sekunden) ein.

   Beispiel:

   ```
   context.sessioninactiveinterval=36000
   ```

   Mit diesem Wert wird eine inaktive Verbindung nach 36000 Sekunden, also 10 Stunden, beendet.

   Wenn die Zeile auskommentiert oder nicht vorhanden ist, wird der Standardwert '28800' verwendet. Dieser entspricht einer Dauer von acht Stunden.

   **Hinweis:** Benutzeranmeldungen in der Ansicht 'Angemeldete Benutzer' werden unter Umständen erst verspätet entfernt. Dies kann z. B. vorkommen, wenn eine Browser-Sitzung nicht regulär beendet wurde oder der Browser-Prozess zuvor unerwartet terminiert wurde.

   Wenn z. B. ein Sitzungs-Timeout von acht Stunden konfiguriert wurde, überprüft die integrierte Anmeldungsbereinigung (garbage collection) zyklisch alle acht Stunden, ob seit der letzten Sitzungsaktivität eine Zeitüberschreitung aufgetreten ist und entfernt ggf. die abgelaufene Anmeldung. In diesem Beispiel wird eine Anmeldung spätestens 16 Stunden nach Ablauf ungültig gesetzt.

   Beispiel:

   Ein Benutzer meldet sich um 02:00 Uhr an. Seine letzte Aktivität ist um 06:00 Uhr. Die erste Überprüfung der integrierten Anmeldungsbereinigung findet um 10:00 Uhr statt. Die Sitzung wurde bis dahin noch nicht beendet. Die zweite Überprüfung findet um 18:00 Uhr statt. Die Sitzung hat zwar ihre Zeit überschritten, wird aber nicht sofort nach acht Stunden, sondern erst 12 Stunden nach der letzten Aktivität entfernt.

**Hinweis:** Benutzeranmeldungen werden nun bei Inaktivität des Benutzers entfernt. Da zuvor ATOSS Time Control standardmäßig alle 25 Sekunden die letzte Aktivität einer Sitzung aktualisiert hat, so dass der konfigurierte Zeitüberschreitungswert für Sitzungen (Session-Timeout) nicht in allen Fällen wirksam war, kann bei Konfigurationen, in denen Verbindungen automatisch nach einer bestimmten Zeit geschlossen werden und bei denen die festgelegte Zeit kleiner ist als der Session-Timeout, daher eine Anpassung erforderlich sein.

Z. B. können beim Einsatz von 'Reverse-Proxys' Verbindungen standardmäßig bereits nach 60 Sekunden geschlossen werden, auch wenn der ATOSS Time Control-Sitzungstimeout wesentlich höher ist. Passen Sie in diesem Fall ggf. die Timeout-Werte entsprechend an.

3. Aktivieren Sie die Änderung, indem Sie den ATOSS Time Control-Serverdienst neu starten.

## 4.10 Erlaubte Verzeichnisse konfigurieren

Sie haben die Möglichkeit, die Anzeige der Server-Root-Verzeichnisse auf Verzeichnisse zu beschränken, die in einer xml-Konfigurationsdatei festgelegt werden. Dies wird über Änderungen in der Datei `allowedroots.xml` erreicht. Die Einstellungen aus dieser Datei werden von allen Datei- bzw. Verzeichnis-Auswahldialogen berücksichtigt.

Für Neuinstallationen wird die Datei `allowedroots.xml` mit folgenden Verzeichnissen generiert:

- Ordner 'Workspace'
- Benutzerverzeichnis des ATOSS Time Control-Benutzers

### Root-Element 'allowedRoots'

In diesem Element sind nur die folgenden Elemente des Typs 'allowedRoot' erlaubt:

| Element | Beschreibung |
|---|---|
| path | Pfad des erlaubten Root-Verzeichnisses. Umgebungsvariablen sind über das Makro `%env(...)%` verfügbar. |
| name | Beschreibender Name des erlaubten Root-Verzeichnisses |
| id | Eindeutige ID des erlaubten Root-Verzeichnisses |

## 4.11 gRPC-Service konfigurieren

Die gRPC-Einstellungen sind in der Registry gespeichert. Die folgende Tabelle gibt einen Überblick über die Einzelheiten:

| Einstellung | Typ | Registry: | Umgebung | Systemeigenschaft | Standardwert |
|---|---|---|---|---|---|
| Starttyp Backend-Service | Integer | - | ATC_BACKEND_ SERVICE_GRPC_ STARTTYPE | atc.backend. service.grpc. starttype | 2 (deaktiviert) |
| Port | Integer | Server/Daten-Server/gRPC/ Port | ATC_SERVER_ GRPC_PORT | atc.server.grpc. port | 3711 |
| Enabled | String | Server/Daten-Server/gRPC/ enabled | ATC_SERVER_ GRPC_ENABLED | atc.server. grpc.enabled | 1 |

| Einstellung | Typ | Registry: | Umgebung | Systemeigenschaft | Standardwert |
|---|---|---|---|---|---|
| Insecure | String | Server/Daten-Server/gRPC/insecure | ATC_SERVER_GRPC_INSECURE | atc.server.grpc.insecure | 0 |
| Server CN | String | Server/Daten-Server/gRPC/server.cn | ATC_SERVER_GRPC_SERVER_CN | atc.server.grpc.server.cn | localhost |
| Dateiname des Server-Zertifikats | String | Server/Daten-Server/gRPC/server.pem | ATC_SERVER_GRPC_SERVER_PEM | atc.server.grpc.server.pem | |
| Dateiname des Server-Zertifikatschlüssels | String | Server/Daten-Server/gRPC/server.key | ATC_SERVER_GRPC_SERVER_KEY | atc.server.grpc.server.key | |
| Dateiname des Client-Zertifikats | String | Server/Daten-Server/gRPC/client.pem | ATC_SERVER_GRPC_CLIENT_PEM | atc.server.grpc.client.pem | |
| Dateiname des Client-Zertifikatschlüssels | String | Server/Daten-Server/gRPC/client.key | ATC_SERVER_GRPC_CLIENT_KEY | atc.server.grpc.client.key | |

# 5 Client-Installation

**Hinweis:** Voraussetzungen für die Client-Installation sind eine abgeschlossene Installation der Serversoftware sowie ein Start beider ATOSS Time Control-Server-Komponenten, Server und Webserver. Nur wenn diese Voraussetzungen erfüllt sind, steht Ihnen die für die Client-Installation erforderliche Installationsdatei über den Webserver zur Verfügung.

### Webclient

Um mit ATOSS Time Control über einen Webbrowser zu arbeiten, installieren Sie den *Webclient*.

## 5.1 Systemanforderungen für Client-Installation prüfen

Stellen Sie sicher, dass die Systemanforderungen erfüllt sind. Weitere Informationen finden Sie im Dokument 'ATOSS Time Control Freigaben und Voraussetzungen'.

Um sicherzugehen, dass das System alle Anforderungen für eine Client-Installation erfüllt, führen Sie folgende Schritte aus:

1. Prüfen Sie, ob der ATOSS Time Control-Server vom Client aus erreichbar ist, indem Sie einen Ping auf die IP-Adresse des Servers durchführen oder ihn über die Netzwerkumgebung Ihres Betriebssystems suchen.
2. Prüfen Sie unter **Systemsteuerung** > **Regions- und Sprachoptionen** > **Regionale Einstellungen**, ob die Servereinstellungen für Datum und Uhrzeit das Format 'TT.MM.JJJJ' verwenden.
3. Weist das Datum ein längeres Format auf, ändern Sie das Format mit Hilfe der Schaltfläche **Anpassen**.

## 5.2 Webclient aufrufen

Mit der ATOSS Time Control können Sie ausschließlich über den Browser per Webclient arbeiten.

Rufen Sie den Webclient anhand folgender Schritte auf:

1. Öffnen Sie einen Browser und geben Sie folgende Adresse ein: `http://<SERVERNAME>:8080/atc/client`.
   'SERVERNAME' ist dabei der Platzhalter für den Namen oder die IP-Adresse Ihres ATOSS Time Control-Servers.

   Der Webclient wird automatisch gestartet. Beim ersten Start öffnet sich der modale Dialog 'Server-Einstellungen'.

2. Konfigurieren Sie die Servereinstellungen mit Hilfe der im Dialog enthaltenen Felder:
   **Server**: Geben Sie den Namen bzw. die IP-Adresse an. Standardmäßig ist hier bereits der korrekte ATOSS Time Control-Server voreingestellt.

   **Port**: Geben Sie hier den Port an. Standardwert ist '2711'.

   **Benutzt SSL** (ja, nein): Aktivieren Sie das Kontrollkästchen nur, wenn Sie einen ausdrücklich für SSL eingerichteten Serverdienst verwenden. Standardwert ist 'nein'.

   **Timeout**: Geben Sie einen Timeout an. Der Client versucht während der angegebenen Zeit, die Verbindung zum Server aufzubauen. Bei Überschreitung der angegebenen Zeit geht der Geräteprozess davon aus, dass das Terminal nicht erreichbar ist. Der Standardwert '60000' entspricht einer Zeit von 60 Sekunden.

3. Bestätigen Sie die Einstellungen mit OK.

   **Hinweis:** Die Konfiguration wird direkt auf dem Server in der Datei `%programdata%\atc\webclient\atc.login.properties` gespeichert.

4. Melden Sie sich nun mit Benutzernamen und Kennwort am ATOSS Time Control-Webclient an.

## 5.3 Webclient in iFrames einbetten

Sie können die ATOSS Time Control in einen iFrame einbetten, um sie in ihrer eigenen internen Website anzuzeigen.

Dazu ist es erforderlich, in der Registry den Host des iFrames auf eine Art 'Whitelist' zu setzen. Die zulässigen Domänen, die die ATOSS Time Control aufrufen, müssen mit dem String-Registrierungsschlüssel `AllowedFrameAncestors` im globalen Abschnitt der ATC-Registrierung konfiguriert werden. Legen Sie mehrere Domänen in einer kommaseparierten Liste fest.

**Hinweis:** Wenn Sie den Registrierungsschlüssel `AllowedFrameAncestors` konfigurieren, ist es unbedingt erforderlich, den Eintrag `localhost` in der Registry anzugeben.

Prüfen Sie anschließend mit dem folgenden HTML-Code, ob es möglich ist, die ATOSS Time Control in einem Frame zu verwenden:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
       "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>Eingebettete Frames definieren</title>
</head>
<body>

<h1>Fenstergucker</h1>

<p>Gucken Sie mal SELFHTML im Fenster an:</p>

<iframe src="http://localhost:8080/atc/client"
width="95%" height="1200" name="Atoss_Test">

  <p>Ihr Browser kann leider keine eingebetteten Frames anzeigen:
  Sie können die eingebettete Seite über den folgenden
  Verweis aufrufen:
  https://customer-url/atc/client
  </p>
</iframe>

</body>
</html>
```

# 6 Updates und Release-Wechsel

In diesem Abschnitt finden Sie Informationen zu Updates und Release-Wechsel.

### Updates

Updates beziehen sich auf Aktualisierungen innerhalb eines Major Releases zur Fehlerbehebungen Ihrer ATOSS Time Control-Software. Für einen einfachen und schnellen Aktualisierungsprozess verfügt ATOSS Time Control über einen automatischen Updatemechanismus, der Ihnen innerhalb eines Major Releases (z. B. von 7.3.x auf 7.3.y) die jeweils aktuelle Version zur Verfügung stellt. Die automatische Aktualisierung umfasst Server und Clients.

**Hinweis:** Um manuelle Anpassungen an Ihrer Standardinstallation (z. B. Webserveranpassungen, eigene SSL-Zertifikate, angepasste HTML-Seiten) nach einem Update wieder an den dafür vorgesehenen Platz manuell zurückkopieren zu können, sichern Sie diese unbedingt, bevor Sie mit dem Update beginnen. Informationen zu Abweichungen von der Standardinstallation finden Sie im Installationsprotokoll.

### Release-Wechsel

Release-Wechsel umfassen regelmäßigen Softwareaktualisierungen, die mit einem Wechsel auf das nächste Major-Releases einhergehen.

## 6.1 Automatische Prüfung auf Updates einstellen

Sie haben die Möglichkeit einzustellen, ob und zu welcher Gelegenheit eine automatische Prüfung auf vorliegende Updates für das verwendete Major Release stattfindet:

1. Öffnen Sie die Registerkarte 'Updates' über **Navigation** > **Installation** > **Updates**.
2. Wählen Sie im Feld **Automatische Updateprüfung** eine der folgenden Optionen:
   - 'Beim Starten der Serverkonsole': Eine Prüfung auf Updates findet nur beim Starten der Serverkonsole statt.
   - 'Täglich': Eine Prüfung auf Updates findet täglich um Mitternacht statt.
   - 'Deaktiviert': Es findet keine Prüfung auf Updates statt.

   Informationen über vorhandene neue Versionen von ATOSS Time Control werden an die Clients weitergegeben.

## 6.2 Gruppierte Indizes mit eingeschlossenen Spalten für MS SQL-Server verwenden

SQL Server-Indizes mit sogenannten eingeschlossenen Spalten (Include Columns) werden verwendet, um die Performance beim Zugriff auf Datenbanktabellen zu erhöhen. Ein Index enthält Schlüssel, die aus einer oder mehreren Spalten in der Tabelle erstellt werden. Wenn Indizes neu erzeugt werden, verwendet der eindeutige Index jeder Tabelle sogenannte 'Gruppierte Indizes' (Clustered Indices). Gruppierte Indizes sortieren und speichern die Datenzeilen in der Tabelle basierend auf ihren Schlüsselwerten. Dies sind die Spalten, die in der Indexdefinition enthalten sind.

Aktuell ist die Neuerstellung der Indizes für bereits existierende Datenbanken nur über einen besonderen jvm-Parameter möglich.

**Hinweis:** Die Neuerstellung der Indizes ist bei großen Datenbanken extrem zeitaufwändig. Führen Sie die optimierte Indexerstellung mit den Feldern **clustered** und **include** nicht während der regulären Arbeitszeit aus, da das System durch die Neuerstellung voll ausgelastet ist und für andere Aufgaben

dann nicht mehr zur Verfügung steht. Bei Fragen oder Problemen wenden Sie sich an Ihren ATOSS CSD-Berater oder den Support.

### Indizes für ATOSS Time Control als Serviceinstallation neu erstellen

Wenn ATOSS Time Control als Service installiert ist, gehen Sie dazu wie folgt vor:

1. Aktualisieren Sie alle Datenbanktabellen auf die neueste Tabellenstruktur des Datenmodells.
2. Gehen Sie zum Ordner des Arbeitsbereichs der ATC-Installation.
3. Öffnen Sie im Ordner `server` die Datei `wrapper.conf`.
4. Fügen Sie hier eine neue Zeile mit dem neuen jvm-Parameter hinzu. Beachten Sie dabei die Anzahl der bereits vorhandenen Einträge.

   **Beispiel**:

   ```
   wrapper.java.additional.2=-DrebuildIndices=true
   ```

   '2 ' ist dabei die Folgenummer der bereits vorhandenen Parameter.
5. Speichern Sie Ihre Änderungen.
6. Führen Sie einen Neustart des Servers durch.

   **Achtung:** Bei einem Neustart des Servers mit diesem Parameter umfasst die Tabellenaktualisierung lediglich die Neustrukturierung des Index. Indizes bestehender Tabellen werden nicht automatisch in das neue Format konvertiert, sondern werden gelöscht und alle Indizes werden gemäß des Datenmodells neu erstellt. Daher ist der folgende Schritt unbedingt erforderlich.
7. Entfernen Sie den hinzugefügten Parameter wieder.
8. Führen Sie einen erneuten Neustart des Servers durch.

### Indizes für ATOSS Time Control als Anwendungsinstallation neu erstellen

Wenn ATOSS Time Control als Anwendung installiert ist, gehen Sie wie folgt vor:

1. Aktualisieren Sie alle Datenbanktabellen auf die neueste Tabellenstruktur des Datenmodells.
2. Gehen Sie zum Ordner 'Installation'.
3. Öffnen Sie im Ordner `server` die Datei `atcs.ini`.
4. Fügen Sie hier in den Abschnitt 'vmargs' folgende neue Zeile hinzu:

   ```
   -DrebuildIndices=true
   ```
5. Speichern Sie Ihre Änderungen.
6. Führen Sie einen Neustart der Anwendung durch.

   **Achtung:** Bei einem Neustart der Anwendung mit diesem Parameter umfasst die Tabellenaktualisierung lediglich die Neustrukturierung des Index. Indizes bestehender Tabellen werden nicht automatisch in das neue Format konvertiert, sondern werden gelöscht und alle Indizes werden gemäß des Datenmodells neu erstellt. Daher ist der folgende Schritt unbedingt erforderlich.
7. Entfernen Sie den hinzugefügten Parameter wieder.
8. Führen Sie einen erneuten Neustart der Anwendung durch.

## 6.3 Server aktualisieren

Nach der Erstinstallation der Software auf Server und Client-Computern ist es jederzeit möglich festzustellen, ob eine aktuellere Version der installierten Software vorliegt:

1. Öffnen Sie einen Browser und geben Sie folgende Adresse ein: `http://SERVERNAME:8080/atc/console`

'SERVERNAME' ist dabei der Platzhalter für den Namen oder die IP-Adresse Ihres Time Control-Servers; befinden Sie sich direkt am Server, verwenden Sie stattdessen 'localhost'.

Abhängig von den Einstellungen zur *Automatischen Updateprüfung* werden Sie beim Start der Konsole über zur Verfügung stehende Updates für das verwendete Major Release informiert. Bei verfügbaren Updates öffnet sich eine Meldung mit der Frage, ob Sie diese Updates installieren möchten.

2. Um Updates zu installieren, bestätigen Sie die Meldung.
   Die aktuelle Version wird geladen und installiert. Die Teile des Serverdienstes werden im Anschluss automatisch neu gestartet: Die Benutzer werden automatisch abgemeldet.

   **Hinweis:** Eine erneute Anmeldung ist erst nach Abschluss des Updatevorgangs möglich.

3. Melden Sie sich nach Abschluss des Updatevorgangs, wie in Schritt 1 beschrieben, erneut an der Konsole an.
4. *Aktualisieren Sie die Tabellenstruktur.*

   **Hinweis:** Nur mit einer Aktualisierung der Tabellenstruktur stellen Sie sicher, dass Sie keine veraltete Tabellenstruktur verwenden. Bei Verwenden einer veralteten Tabellenstruktur ist kein Arbeiten mit ATOSS Time Control möglich.

   **Achtung:** Ein Abbruch bei der Aktualisierung der Tabellenstruktur kann zu einer Beschädigung der Datenbank führen. Vermeiden Sie deshalb unbedingt ein Abbrechen des Aktualisierungsvorgangs! Erst wenn diese Tabellenprüfung fertiggestellt wurde, startet der Datenserver wieder!

   Nach erfolgreicher Tabellenaktualisierung sehen Sie die Meldung 'Die Tabellen sind auf dem neuesten Stand'. Danach startet der Server automatisch und die Aktualisierung des Servers ist abgeschlossen.

Zur Sicherheit können Sie bei den Windows-Diensten prüfen, ob alle ATOSS Time Control-Dienste wieder gestartet wurden.

**Hinweis:** Beachten Sie bei einem erforderlichen Neustart der Dienste die Reihenfolge:

1. Server
2. Webserver
3. Geräteprozess

**Hinweis:** Führen Sie ein Online-Update bei als Anwendung gestarteten Time Control-Servern durch, ist es erforderlich, diese Anwendungen nach erfolgreichem Update zu beenden und neu zu starten.

## 6.4 Clients aktualisieren

**Hinweis:** Eine Aktualisierung der Clients ist nur bei laufendem Webserver möglich.

Beim Start eines Clients führt dieser auf dem Server eine Prüfung auf verfügbare neue Versionen durch. Vorliegende neue Versionen werden Ihnen über eine Meldung mitgeteilt. Bestätigen Sie die Meldung mit **Ja**, aktualisiert sich im Anschluss der Client automatisch. Damit ist innerhalb der installierten ATOSS Time Control-Version ein einheitlicher Softwarestand gewährleistet.

**Hinweis:** Wurde der ATOSS Time Control-Client in das Verzeichnis `Programme` installiert und ist die Windows-Benutzerkontensteuerung aktiv, ist ein einmaliger Start der Client-Aktualisierung als Administrator erforderlich, damit das Update in dasselbe Verzeichnis installiert wird.

**Tipp:**

- Servername, -port und weitere Einstellungen des Clients sind in der Datei `%appdata%/atc/atc.login.properties` abgelegt. Bei Problemen, z. B. bei Angabe eines falschen Servernamens, finden Sie die notwendigen Einstellungen zur Korrektur in dieser Datei.
- Eine weitere Möglichkeit zur Lösung von Problemsituationen besteht darin, diese Datei an anderer Stelle zu sichern und anschließend zu löschen: Beim nächsten Start des Clients wird diese Datei nach Angabe der Verbindungseinstellungen neu erzeugt.

## 6.5 Releasewechsel durchführen

**Achtung:** Lassen Sie einen Releasewechsel (z. B. von 7.2.x auf 7.3.x) nur von Ihrem ATOSS CSD-Berater durchführen, da neben Neuerungen möglicherweise auch bestehende Datenstrukturen anzupassen sind!

1. Starten Sie die Konsole, indem Sie folgende Adresse im Browser eingeben:
   `http://SERVERNAME:27112/atc/console`

   'SERVERNAME' ist dabei der Platzhalter für den Namen oder die IP-Adresse Ihres Time Control-Servers.
2. Wählen Sie die Ansicht 'Servereinstellungen'.
3. In der Gruppe 'ATOSS Time Control Online-Update' geben Sie im Feld **Repository** den Pfad zu dem zu aktualisierenden Repository ein.
4. Wählen Sie **Nach Updates suchen**.

   ATOSS Time Control sucht nach nach Windows-Softwareupdates und Webclient-Updates. Wenn ein Update verfügbar ist, wird Ihnen dies unter dem Feld angezeigt.

   **Hinweis:** Ohne gültige Lizenz ist kein Betrieb von ATOSS Time Control möglich.
5. Prüfen Sie, ob Sie eine aktuelle Lizenz für ATOSS Time Control besitzen bzw. ob Ihre Lizenz online über den Lizenzserver aktiviert wurde.
6. Wenn eine gültige Lizenz für ATOSS Time Control vorliegt, wählen Sie **Jetzt aktualisieren**.
   Der Releasewechsel wird durchgeführt.
7. Wenn Sie in Ihrer Datenbank mindestens eine Tabelle mit fehlenden Indizes haben und Daten bereits in diesen Tabellen erstellt wurden, bereinigen Sie diese Tabellen. Eine Tabelle mit fehlenden Indizes und erstellten Daten bereinigen Sie folgendermaßen:
   - Löschen Sie die Daten der Tabellen, die fehlende Indizes enthalten und in denen der Primärschlüssel in der Tabelle verletzt wird.
   - Löschen Sie den Schlüssel 'databaseTableHash' aus der Registry oder starten Sie den Server mit dem Parameter **DforceTableUpdate=true**.
   - Die Indizes werden nach einem Update der Tabellen wieder korrekt erstellt.

Nach dem automatischen Neustart der Dienste ist der Wechsel zum nächsten Release abgeschlossen.

Nehmen Sie ggf. weitere *Konfigurationen des Servers über die Konsole* vor.

## 6.6 Prüfung für Updates von älteren Releases

Bei Updates von älteren Releases, z. B. von 6.5 LTS oder 7.3 LTS auf ATOSS Time Control 8.3, stellt sich die Herausforderung, alle in der Zeit zwischen den Releases zu der Software hinzugekommenen Änderungen und Neuerungen in dem Update abzudecken und die daraus potentiell auftretenden Probleme zu lösen. Als Hilfestellung dazu stellt Ihnen ATOSS Time Control einen Assistenten zur Analyse und Prüfung von möglichen Problemen beim Update zur Verfügung, der Sie durch den Prüfungsprozess führt.

Um die Prüfung für ein Update durchzuführen, gehen Sie wie folgt vor:

1. Wählen Sie **Hilfe** > **Updateprüfung für 8.3 LTS**.
   Der Startdialog des Assistenten öffnet sich und informiert Sie über die Inhalte der Prüfung.
2. Wählen Sie **Weiter**.
   Ein Modaldialog mit Einträgen zu relevanten Protokolltabellen, die während des Updates bereinigt werden müssen, öffnet sich.
3. Aktivieren Sie die Kontrollkästchen für die Tabellen, die beim Update bereinigt werden sollen und geben Sie jeweils das Datum an, bis zu dem die Daten anschließend gelöscht werden.

   Rechts finden Sie Informationen über die Anzahl an Datensätzen, die bei einem Update für die gewählte Tabelle gelöscht werden.
4. Wählen Sie **Weiter**.
   Ein Modaldialog mit Informationen zu den in Ihrem System vorhandenen Individualisierungen öffnet sich. Diese müssen vor dem Update gesondert geprüft und ggf. angepasst oder umgestellt werden.
5. Um sich diese Information zusammengefasst als E-Mail schicken zu lassen, wählen Sie den E-Mail-Client aus.
6. Starten Sie das Mailprogramm mit **Senden**.
   Die Ergebnisse der Prüfung sind automatisch Inhalt der Mail.
7. Beenden Sie den Assistenten mit **Schließen**.

# 7 Authentifizierungsmodule

**Tipp:** Dieser Abschnitt enthält weiterführende Informationen zu den in der Referenzdokumentation beschriebenen Servereinstellungen.

**Einschränkung:** Die Funktionalität der Serverkonsole ist ausschließlich über den Webclient verfügbar.

Für die Anmeldung eines Clients am Server gibt es folgende Authentifizierungsmodule:

- *Standard-Authentifizierung*
- *Ausweis-Authentifizierung*
- *Externe Authentifizierung*
- *Kerberos-Authentifizierung*

Die gewünschte Authentifizierungsvariante ist in der Serverkonsole unter **Einstellungen** > **Server** auf der Registerkarte 'Servereinstellungen' in der Gruppe 'Sicherheit' auswählbar.

## 7.1 Standard-Authentifizierung

Bei der Standard-Authentifizierung meldet sich der Benutzer mit seinen ATOSS Time Control-Benutzerdaten (Mitarbeiternummer und dem in den Mitarbeiterstammdaten hinterlegten Kennwort) an.

**Tipp:** Eine Alternative zur Authentifizierung durch die Mitarbeiternummer ist die Verwendung eines Alias. Diesen hinterlegen Sie für einen Mitarbeiter in den Stammdaten.

## 7.2 Ausweis-Authentifizierung

Die Ausweis-Identifizierung verwendet eine Ausweisnummer zur Identifikation des zugehörigen Mitarbeiters. Die Eingabe eines Kennworts ist dabei nicht erforderlich.

**Hinweis:** Für diese Art der Anmeldung gelten folgende Voraussetzungen:

- Es ist ein One-Touch-Ausweislesegerät erforderlich. Um ein One-Touch-Ausweislesegerät über ATOSS CSD zu beziehen, wenden Sie sich an Ihren ATOSS CSD-Berater oder den Support.
- Um den Ausweisleser verwenden zu können, ist auf dem Client, auf dem der Ausweisleser verwendet wird, die Installation von mindestens Java 11 erforderlich.
- Für den Mitarbeiter ist ein hinterlegter One-Touch-Ausweis erforderlich.

## 7.3 Externe Authentifizierung

Dieses Authentifizierungsmodul ermöglicht die Anbindung einer externen Authentifizierung an ATOSS Time Control. Die Schnittstelle erfordert eine zur Verfügung gestellte *Java-Klasse* in einem *Java-Archiv*, die zum Austausch von Benutzerinformationen aufgerufen wird.

### 7.3.1 Java-Schnittstellenklasse

Die Klasse stellt eine öffentliche Methode mit folgender Signatur bereit:

```
public void authenticate( Map<String, Object> parameters )
```

Sämtliche Daten werden über die Java Map-Parameter ausgetauscht (**input** und **output**). Die folgende Tabelle gibt einen Überblick über die von der Schnittstelle unterstützten Parameter:

| Parameter | Datentyp | Richtung | Erläuterung |
|---|---|---|---|
| atc.user.name | String | In | Benutzername aus dem Anmeldedialog des ATOSS Time Control Client (Desktop und Web) |
| atc.user.password | String | In | Passwort aus dem Anmeldedialog (Klartext). Für mehr Sicherheit verwenden Sie das SSL-Protokoll. |
| auth.accessGranted | Boolean | Out | Angabe, ob das externe System den Zugriff auf ATOSS Time Control gewährt. Bei Verweigerung des Zugriffs liefert der Parameter **auth.message** die entsprechende Fehlermeldung. |
| auth.message | String | Out | Fehlermeldung beim Scheitern der Authentifizierung |
| auth.atc.employee | String | Out | ATOSS Time Control Mitarbeiternummer (wenn abweichend von `atc.user.name`) |

### 7.3.2 Java-Archivstruktur

Das Java-Archiv erfordert ein Manifest (`/META-INF/MANIFEST.MF`) mit einem ATC-Authentifizierungsattribut. Dieses Attribut gibt den Namen der Schnittstellenklasse an.

#### Beispiel für ein Manifest

Manifest-Version: 1.0

ATC-Authentication: `com.atoss.atc.external.auth.demo.DemoAuthentication`

#### Implementierungsbeispiel

```
package com.atoss.atc.external.auth.demo;

import java.util.HashMap;
import java.util.Map;

public class DemoAuthentication
{
private static final String AUTH_ATC_EMPLOYEE = "auth.atc.employee"; //$NON-NLS-1$
private static final String AUTH_MESSAGE = "auth.message"; //$NON-NLS-1$
private static final String AUTH_ACCESS_GRANTED = "auth.accessGranted"; //$NON-NLS-1$
private static final String ATC_USER_PASSWORD = "atc.user.password"; //$NON-NLS-1$
private static final String ATC_USER_NAME = "atc.user.name"; //$NON-NLS-1$
private static Map<String, String> users = new HashMap<String, String>()
{
private static final long serialVersionUID = 1L;
{
put( "x1", "y1" ); //$NON-NLS-1$//$NON-NLS-2$
put( "x2", "y2" ); //$NON-NLS-1$//$NON-NLS-2$
put( "x3", "y3" ); //$NON-NLS-1$//$NON-NLS-2$
put( "x4", "y4" ); //$NON-NLS-1$//$NON-NLS-2$
}
};

public void authenticate( Map<String, Object> parameters )
{
String userName = (String)parameters.get( ATC_USER_NAME );
String password = (String)parameters.get( ATC_USER_PASSWORD );

if( userName == null || password == null )
```

```
return;

// do some checks
System.out.println( String.format(
"User %s logging in with password %s", userName, password ) ); //$NON-NLS-1$

// map userName to ATC employee id
String atcEmployeeId = getATCEmployeeId( userName );
if( atcEmployeeId == null )
{
fail( parameters, String.format( "User %s is unknown", userName ) ); //$NON-NLS-1$
return;
}

if( !password.equals( "secret" ) ) //$NON-NLS-1$ )
{
fail( parameters, "Wrong password provided" ); //$NON-NLS-1$
return;
}

parameters.put( AUTH_ACCESS_GRANTED, true );
parameters.put( AUTH_ATC_EMPLOYEE, atcEmployeeId );
}

private void fail( Map<String, Object> parameters, String errorMessage )
{
parameters.put( AUTH_ACCESS_GRANTED, false );
parameters.put( AUTH_MESSAGE, errorMessage );
}

private String getATCEmployeeId( String userName )
{
return users.get( userName );
}
}
```

## 7.4 Kerberos-Authentifizierung

Die Kerberos-Authentifizierung erfolgt über einen zentralen Authentifizierungsdienst (z. B. Microsoft Active Directory Domain Services oder Apache Directory Service).

Im Folgenden finden Sie weitere Hilfestellung zu den Einstellungen:

- *Dialog 'Kerberos-Authentifizierungsmodul'* auf Seite 52
- *Dialog 'Konfiguration der Benutzererkennung'* auf Seite 53
- Dokument 'ATOSS Time Control Installation' unter:
  - Ablauf der Authentifizierung
  - Systemkonfiguration für Windows und Active Directory
  - Hilfe bei Konfigurationsproblemen

**Hinweis: Passwortänderung in ATOSS Time Control bei aktiver Kerberos-Authentifizierung:**

Bei aktiver Kerberos-Authentifizierung ist es einem angemeldeten ATOSS Time Control-Benutzer möglich, sein eigenes Passwort zu ändern. Durch Anwendung der Passwortrichtlinien kann es vorkommen, dass ein neues Passwort, z. B. aufgrund mangelnder Komplexität, abgelehnt wird. Eine solche Ablehnung teilt Ihnen ATOSS Time Control ohne Angabe von Gründen lediglich mit der Meldung mit, dass eine Passwortänderung nicht möglich ist. Details zu der abgelehnten Änderung finden Sie in den Logdateien.

Wenden Sie sich bei Fragen dazu an den Support.

### 7.4.1 Ablauf der Authentifizierung

**Hinweis:** Eine in der Serverkonsole aktivierte Kerberos-Authentifizierung kann von allen anderen Benutzer- und Passwortanmeldevorgängen, z. B. solche, die über den Webclient mit AMIS erfolgen, verwendet werden.

Eine Kerberos-Authentifizierung läuft nach den folgenden Schritten ab:

1. Sie melden sich mit dem ATOSS Time Control-Client am Key Distribution Center (KDC) an:
   - mit Ihrem Benutzernamen und Kennwort oder
   - bei Verwenden des Kerberos-Prinzipals 'benutzer@REALM' mit 'benutzer'
2. Nach erfolgreicher Authentifizierung fordert der ATOSS Time Control-Client ein Ticket vom KDC an.
3. Nach Erhalt des Tickets sendet der ATOSS Time Control-Client dieses Ticket an den ATOSS Time Control-Server.
4. Der ATOSS Time Control-Server meldet sich mit dem Dienstnamen aus der Konfiguration beim KDC an und verifiziert die Gültigkeit des erhaltenen Tickets.
5. Der ATOSS Time Control-Server extrahiert den Kerberos-Prinzipal aus dem Ticket.
6. Der ATOSS Time Control-Server ermittelt über den Kerberos-Prinzipal mit Hilfe der eingestellten Benutzererkennung den ATOSS Time Control-Mitarbeiter.

   **Hinweis:** Nach einer fehlerhaften SSO-Authentifizierung wird der Standard-Anmeldedialog angezeigt.

### 7.4.2 Dialog 'Kerberos-Authentifizierungsmodul'

In diesem modalen Dialog konfigurieren Sie das Kerberos-Authentifizierungsmodul.

**Typ**, Auswahlliste (Microsoft Active Directory, Apache Directory Service): Wählen Sie den Typ des Authentifizierungsdienstes aus.

**Key Distribution Service**, Textfeld: Geben Sie die Adresse des Key Distribution Service (Kerberos-Server) an. Ist der Dienst auf Ihrem Computer nicht über den Kerberos-Standardport '88' verfügbar, ist bei der Angabe des Ports eine durch Doppelpunkt getrennte Schreibweise möglich.

**Beispiel:**

```
kdchost:60088
192.168.1.1
```

**Realm**, Textfeld: Geben Sie den Bereich der Kerberos-Servers in Großbuchstaben an.

**Beispiel:**

```
ATOSS-CSD.DE
```

**Dienstname**, Textfeld: Geben Sie den beim Active Directory angelegten Dienstprinzipalnamen ('servicePrincipalName') an. Über den hier angegebenen Dienst auf dem Active Directory findet anschließend die Kommunikation mit Time Control statt.

**Hinweis:** Der Dienstprinzipalname ist nicht der im Kontext der Time Control-Dienste verwendete Benutzername.

**Beispiel:**

```
sptimecontrol
```

**Tipp:** Verwenden Sie zum Anlegen des Dienstprinzipalnamens den Windows-Befehl `setspn`.

**Dienstpasswort**, Textfeld: Passwort für den angelegten Dienstprinzipalnamen (servicePrincipalName) beim Kerberos-Server.

**LDAP-Protokoll**: Geben Sie den Namen des LDAP-Protokolls an. Möglich ist die Auswahl der Werte 'LDAP' oder 'LDAPS'.

**LDAP Host**, Textfeld: Geben Sie die Adresse des LDAP-Servers an.

**LDAP-Port**: Geben Sie den LDAP-Port an. Standard-LDAP-Port ist '389', Standard-LDAPS-Port ist '636'.

**LDAP Base DN**, Textfeld: Geben Sie einen 'Basis Distinguished Name' für die Suche nach Benutzern im LDAP-Verzeichnis an.

**Beispiel:**

```
ou=Users,dc=atoss-csd,dc=de
```

**Benutzererkennung konfigurieren**, Schaltfläche: Öffnet den modalen Dialog *Konfiguration der Benutzererkennung*. Hier bestimmen Sie, wie dem Verzeichnisdienst die jeweilige Mitarbeiternummer zugeordnet wird. Diese Konfiguration ermöglicht dem Active Directory, dem Windows-Benutzer eine Time Control-Mitarbeiternummer zuzuordnen.

### 7.4.3 Dialog 'Konfiguration der Benutzererkennung'

In diesem Dialog konfigurieren Sie die Benutzererkennung. Die Benutzererkennung erfolgt in der hier angegebenen Reihenfolge.

Folgende Methoden der Benutzererkennung sind auswählbar:

- **Im Verzeichnisdienst suchen (Attribut/Mitarbeiternummer)**, Kontrollkästchen
- **In der Tabelle EmployeePrincipal suchen**, Kontrollkästchen
- **Vollständige Benutzererkennung als Mitarbeiternummer**, Kontrollkästchen
- **Vollständige Benutzererkennung als Mitarbeiteralias**, Kontrollkästchen
- **Benutzererkennung als Mitarbeiternummer**, Kontrollkästchen
- **Benutzererkennung als Mitarbeiteralias**, Kontrollkästchen

Folgende Aktionen sind verfügbar:

| Aktion | Schaltfläche | Erläuterung |
|---|---|---|
| **Erkennungsmethode nach oben verschieben** |  | Um die gewünschte Reihenfolge der Suche zu definieren, ändern Sie die Reihenfolge bei mehreren aktivierten Erkennungsmethoden über die Pfeil-Schaltflächen. |
| **Erkennungsmethode nach unten verschieben** |  | |
| **Erkennungsmethode konfigurieren** |  | Nur für die Methode 'Im Verzeichnisdienst suchen (Attribut/Mitarbeiternummer)' verfügbar. Öffnet den modalen Dialog 'Einstellungen für die Verzeichnisdienst-Benutzererkennung': Geben Sie hier ein Attribut an, das als Mitarbeiternummer verwendet wird. |

### 7.4.4 Systemkonfiguration für Windows und Active Directory

Single-Sign-on (SSO) bietet dem Benutzer die Möglichkeit, sich nach einmaliger Authentifizierung an einem Arbeitsplatz auf alle Computer und Dienste, für die er lokal berechtigt (autorisiert) ist, zuzugreifen, ohne dass jedes Mal eine erneute Anmeldung erforderlich ist.

Damit es Windows-Benutzern möglich ist, Single-Sign-On mit einem Active Directory-Server zu verwenden, sind bestimmte Einstellungen auf dem Client und dem Active Directory-Server erforderlich. Informationen dazu finden Sie unter:

- *Browser-Client einrichten* auf Seite 54
- *Einstellungen am Active Directory-Server* auf Seite 56

#### 7.4.4.1 Browser-Client einrichten

**Hinweis:** Um Einstellungen für den Browser-Client vornehmen zu können, werden Erfahrungen im Umgang mit Kerberos, Principals und der Funktionsweise der Authentifizierung vorausgesetzt.

**Hinweis:** Um Single-Sign-on (SSO) verwenden zu können, ist es für Browser erforderlich, auf dem Active Directory einen speziellen Prinzipal anzulegen. Um Single-Sign-On im Browser verwenden zu können, muss der **servicePrincipalName** `HTTP/%SERVERNAME%` eindeutig sein. Daher darf er nur bei einem Active Directory-Account hinterlegt sein.

Sie können SSO mit einem Browser nur bei solchen Websites verwenden, die Kerberos-Tickets akzeptieren. Websites können einen Browser um eine grundlegende Authentifizierung mit den Benutzer-/Passwort-Einstellungen (Standard für alle Websites) bzw. eine 'ausgehandelte Authentifizierung' bitten.

Wenn ein nicht ausgehandelter HTTP-Client Informationen von der Website anfordert, liefert der Webserver eine Challenge-Response zurück und bittet den Browser um eine Authentifizierung. Diese kann grundlegend oder, für ein Kerberos-Ticket, ausgehandelt sein.

Bei einer ausgehandelten Authentifizierung verwendet der Browser ein lokales Kerberos-Ticket, um ein gültiges 'Simple and Protected GSSAPI Negotiation Mechanism-Ticket' (SPNEGO-Ticket) für die Website zu erhalten, auf die er zugreifen möchte. Dieses Ticket gilt für genau diesen Webserver-Namen und funktioniert auch nur für diesen Server. Der Browser meldet sich weder beim Kerberos-Server an, noch verwendet er Passwörter. Das SPNEGO-Ticket enthält den Namen des Prinzipals aus dem Browsercomputer. Es ist kein gültiges Ticket, mit dem Zugriff auf Ressourcen erworben werden kann, sondern funktioniert nur, wenn es mit einem für den Webserver-Prozess bereitgestellten echten Kerberos-Ticket abgeglichen wird. Wenn der Computer, auf dem der Browser läuft, nicht authentifiziert werden kann, wird kein SPNEGO-Ticket bereitgestellt. Wenn der Browser ein SPNEGO-Ticket liefert, wird dieses mit der Base64-Codierung an den Webserver gesendet.

Anschließend aktiviert der Webserver das SPNEGO-Ticket und versucht, es mit seinem eigenen Ticket von Kerberos abzugleichen. Nach Abschluss des Java-Anmeldemechanismus kann der Prinzipal aus dem SPNEGO-Ticket gelesen werden und es erfolgt ein Abgleich mit einem echten Mitarbeiter aus dem ATOSS Time Control-Server.

### Kerberos-Server einrichten

Um einen Kerberos-Server in einem Netzwerk einzurichten, ist es erforderlich, dass dieser Zugriff auf einen DNS-Server( Domain Name System-Server) hat, der die Computernamen in IP-Adressen auflösen kann. Außerdem muss die umgekehrte Namensauflösung (IP zu Computername) mindestens für den Webserver funktionieren.

`AES256(aes256-cts-hmac-sha1-96)` ist die Standardverschlüsselung für die Browser-SPNEGO-Tickets für nicht konfigurierte Kerberos-5-Server der Versionen 1.3 und höher. Die aktuelle Kerberos-Version ist 1.13, die meisten Serversysteme verwenden allerdings die Versionen 1.11 oder 1.12.

### Webserver-Principal

Für die Authentifizierung fordert der Browser ein SPNEGO-Ticket für den Website-Namen mit folgendem Format an: `HTTP/[Webservername]`.

Der Kerberos-Server muss entweder einen Prinzipal `HTTP/atcweb` oder `HTTP/atcweb@`*`SPEZIFISCHEDOMÄNE`* mit einem dazugehörigen Passwort enthalten. Die Anmeldung erfolgt für genau diesen Prinzipal. Der authentifizierte Kontext wird zur Validierung des für `HTTP/atcweb` generierten SPNEGO-Tickets verwendet.

Mit dem folgenden Aufruf erhalten Sie eine Liste aller registrierten **ServicePrincipalNames** für den Benutzer 'atc':

```
setspn atc
HTTP/atcweb.atc.local atc <- sso
```

```
atc/atcweb.atc.local atc
atc/atcweb atc <- rcp client
```

Mit dem weiteren Aufruf erhalten Sie Optionen zum Hinzufügen bzw. Löschen eines **ServicePrincipalName**:

```
setspn
```

Normalerweise kann der Prinzipal für den ATOSS Time Control-Server auch als Prinzipal für HTTP verwendet werden. Sie können daher auch einen Service-Prinzipal zum Benutzer des ATOSS Time Control-Servers hinzufügen. Der Name des Prinzipals muss dann für jeden Computer, auf dem der Webclient läuft, wie oben beschrieben lauten.

### Browser einrichten

**Hinweis:** Es wird angenommen, dass auf dem Computer, auf dem der Browser läuft, bereits ein gültiges Kerberos-Ticket vorhanden ist und die Anmeldung über das Betriebssystem möglich ist.

**Firefox**

Fügen Sie auf der Website `about:config` dem Wert `network.negotiate-auth.trusted-uris` den Webserver-Namen hinzu. Authentifizierungsanfragen von diesem Server werden mit einem SPNEGO-Ticket bereitgestellt.

Wenn Ihr SPN `HTTP/atcweb` lautet, müssen Sie den Wert 'atcweb' zu `network.negotiate-auth.trusted-uris` hinzufügen.

**Chrome**

Starten Sie den Browser mit dem folgenden zusätzlichen Kommandozeilenparameter: `--auth-server-whitelist="webserver_name"`. Wie bei Firefox werden Authentifizierungsanfragen von diesem Server mit einem SPNEGO-Ticket bereitgestellt.

Wenn Ihr SPN `HTTP/atcweb` lautet, müssen Sie den Wert 'atcweb' zu `--auth-server-whitelist` hinzufügen.

### Single-Sign-On beim ATC-Webclient

Beim ATOSS Time Control-Webclient unterscheidet sich SSO leicht von normalen Websites. Die Authentifizierung erfolgt für die gesamte HTTP-Sitzung , RAP kann jedoch in einer Sitzung über mehrere Registerkarten mit eigenen, separaten Umgebungen und separaten ATOSS Time Control-Verbindungen verfügen.

Daher verwendet lediglich die erste Registerkarte der Sitzung die SSO-Authentifizierung. Dies ist insofern nützlich, da sich ein Benutzer auf diese Weise mit anderen Mitarbeitern anstatt nur mit sich selbst verbinden kann.

Die Validierung des Tickets (`HTTP/[`*`Webservername`*`]`) und des SPNEGO-Tickets erfolgt durch den ATOSS Time Control-Server bei der Anmeldung der ATOSS Time Control-Verbindung. Auf Websites ohne ATOSS Time Control-Server o. Ä. kann diese Ticketvalidierung auf der Webserver-Java-VM stattfinden. In dem vorliegenden Fall ist die Validierung jedoch nicht zweimal erforderlich. Daher wird das SPNEGO-Ticket an den ATOSS Time Control-Server weitergeleitet.

### SSO-Authentifizierung für Computer außerhalb der Domäne

Wenn die SSO-Challenge-Response einmal an den Browser gesendet wird, wird die IP-Adresse für die nächste Anfrage gespeichert. Wenn der Browser kein SPNEGO-Ticket bereitstellen kann, wird über einen Zeitraum von zehn Sekunden die Authentifizierungsanfrage nicht erneut an dieselbe IP-Adresse gesendet. Der Benutzer kann somit einen erneuten Anmeldeversuch starten.

Wenn die Kerberos-Authentifizierung obligatorisch ist und der Browser für die Website kein Ticket bereitstellen kann, ist ein Zugriff auf die Website nicht möglich.

### Bekannte Probleme

Pro Sitzung kann ein Browser lediglich ein Kerberos-SPNEGO-Ticket anfordern. Das bedeutet, dass mit der SSO-Anmeldung keine zweite Registerkarte geöffnet werden kann. Wenn die erste Registerkarte geschlossen wird, ist es mit der SSO-Anmeldung nicht möglich, eine neue Registerkarte zu öffnen, da der Browser das Kerberos-Ticket bereits verwendet hat. Dieses Verhalten ist eine Sicherheitsmaßnahme, die verhindert, dass Tickets wiederholt verwendet werden, um Zugriff auf Ressourcen zu gewinnen. In einem solchen Fall müssen alle Fenster des Browsers geschlossen und erneut geöffnet werden. Erst dann wird ein neues SPNEGO-Ticket für SSO angefordert.

#### 7.4.4.2 Einstellungen am Active Directory-Server

Für eine erfolgreiche Konfiguration sind folgende Punkte unbedingt erforderlich:

- Dienstprinzipal und Dienstprinzipalname (Service Principal Name (SPN)) müssen denselben Namen haben:
  - Der ATC-Server benötigt einen Prinzipal im Kerberos-Realm. Dieser Benutzer muss den in der Konfiguration vorgegebenen Namen haben (z. B.: <dienstname>@<active-directory-domäne>).
  - Der Kerberos-Prinzipal muss einen SPN mit dem konfigurierten Namen und dem Host haben, auf dem der ATC-Server läuft (z. B.: <dienstname>/<atc-server-host>)
- Der LDAP Base DN muss eine Organisationseinheit enthalten (z. B.: OU=Users,DC=<kundenname>,DC=<land>).

### Weitere Informationen

- *Beispiel zum Anlegen eines Dienstprinzipalnamens (SPN)* auf Seite 56
- *Verschlüsselung* auf Seite 56

##### 7.4.4.2.1 Verschlüsselung

Beim Active Directory-Account darf folgende Option nicht aktiviert sein: 'Use Kerberos DES encryption types for this account.'

Konfigurieren Sie das Active Directory so, dass es die AES-128- und AES-256-Verschlüsselung unterstützt.

Mit Java 11 wurden die schwachen Verschlüsselungen DES3 und RC4 deaktiviert. Weitere Informationen dazu finden Sie unter:
*https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/unsupported-etype-error-accessing-trusted-domain*

##### 7.4.4.2.2 Beispiel zum Anlegen eines Dienstprinzipalnamens (SPN)

Den Dienstprinzipalnamen (servicePrincipalName) legen Sie mithilfe des Befehls `setspn` fest. 'ATCSERVER' ist dabei der Name des verwendeten Time Control-Servers:

```
setspn -A sptimecontrol/ATCSERVER sptimecontrol
```

Mögliche Ausgabemeldung:

```
Registering ServicePrincipalNames for CN=sptimecontrol
sptimecontrol,CN=Users,DC=atoss-csd
,DC=de
        sptimecontrol/ATCSERVER
Updated object
```

**Hinweis:** Für eine funktionierende DNS-Auflösung bei dieser Konfiguration ist die Angabe der IP-Adresse des Active Directory-Servers als DNS-Server bei den Netzwerkeinstellungen unbedingt erforderlich.

### 7.4.5 Hilfe bei Konfigurationsproblemen

Verwenden Sie bei Problemen, deren Ursache Ihnen nicht sofort ersichtlich ist, die Systemeigenschaft 'kerberos.debug': Fügen Sie dazu in der Datei `<installationsverzeichnis>/client/atcc.ini` die folgende Zeile hinzu:

```
-Dkerberos.debug=true
```

Auf der Konsole werden daraufhin Informationen zu möglichen Fehlern ausgegeben.

Fügen Sie diese Informationen in Form einer Textdatei Ihrer Supportanfrage für den Second Level Support hinzu.

#### Weitere Themen

*Fehlermeldungen beim Active Directory Service* auf Seite 57

#### 7.4.5.1 Fehlermeldungen beim Active Directory Service

Hier finden Sie eine Auflistung möglicher Fehlermeldungen beim Active Directory Service.

**Tipp:** Eine vollständige Liste mit Fehlermeldungen finden Sie unter folgendem Link: *http://www.adiscon.com/common/en/securityreference/kerberos-failures.php*

| Fehlermeldung | Erläuterung |
|---|---|
| `KrbException: Message stream modified (41)` | Die Meldung wird durch einen falsch geschriebenen Realm-Namen erzeugt. |
| `KrbException: Server not found in Kerberos database (7)` | Die Meldung wird durch einen fehlenden oder falsch geschriebenen Service Principal Name erzeugt. Korrigieren Sie den Fehler entweder mit `setspn -A atc/<host> <ad-user>` oder verwenden Sie dazu den ADSI-Editor (adsiedit.msc). |
| `ErrorCode: 4 com.atoss.atc.dscomm.LoginException: Service principal <name> could not be authenticated with the KDC` | Die Meldung wird durch Eingabe eines falschen Kennworts für den `service principal name` erzeugt. |
| | Die Meldung wird durch einen nicht auf das Microsoft Active Directory gesetzten Typ erzeugt. |
| `ErrorCode: 2 com.atoss.atc.dscomm.LoginException: Login Versuch des unbekannten Benutzers` | Die Meldung wird durch eine fehlende Zuordnung des Benutzers zum atcNumber-Attribut erzeugt. Korrigieren Sie den Fehler mit Hilfe des ADSI-Editors (adsiedit.msc). |

| Fehlermeldung | Erläuterung |
|---|---|
| | Die Meldung wird durch eine falsche LDAP Base DN erzeugt. |
| `javax.security.auth.login.LoginException: Unable to obtain Princpal Name for authentication` | Die Meldung wird durch ein fehlendes Kerberos-Ticket für SSO erzeugt. |
| `javax.security.auth.login.LoginException: Client not found in Kerberos database` | Die Meldung wird durch eine Anmeldung mit einem ungültigen Benutzernamen erzeugt. |
| `javax.security.auth.login.LoginException: Pre-authentication information was invalid` | Die Meldung wird durch die Eingabe eines falschen Passworts bei der Anmeldung erzeugt. |
| `Clock skew too great` | Die Meldung wird erzeugt, wenn sich die Zeiten auf dem Client und auf dem KDC (Active Directory-Server) zu sehr unterschieden. Synchronisieren Sie die Zeiten mithilfe von NTP. |
| `Exception: Message stream modified (41)` | Die Meldung wird erzeugt, wenn der Realm- Name nicht komplett in Großbuchstaben geschrieben ist. |

# 8 Performance-Optimierungen

Hier finden Sie einen Leitfaden, mit dem Sie Einstellungen zur Performance-Optimierung vornehmen können. Befolgen Sie die Hinweise und Empfehlungen, wenn Sie den Eindruck haben, dass die Gesamt-Performance der ATOSS Time Control nicht optimal ist. Prüfen Sie jeden Hinweis ggf. in der individuellen Kunden-Installation.

Die Optimierungsmöglichkeiten sind in folgende Kategorien unterteilt:



## 8.1 Allgemeine Hinweise

Folgende allgemeine Hinweise können Ausgangspunkte für eine Performance-Optimierung sein:

- Prüfen Sie die aktuellen Systemvoraussetzungen und Empfehlungen für die verwendete Version. Weitere Informationen finden Sie der Dokumentation ATOSS Time Control Systemfreigaben und Voraussetzungen bzw. ATOSS Time Control Systemfreigaben und Voraussetzungen für ATOSS CLOUD24/7 und ATOSS Cloud Solution.
- ATOSS empfiehlt die Verwendung eines dedizierten Hochleistungsservers für den alleinigen Betrieb des ATOSS Time Control-Servers.
- Prüfen Sie, ob sich die von Drittanbieter-Komponenten und Drittanbieter-Software verursachte Systemlast auf die Performance der ATOSS Time Control auswirkt. Drittanbieter-Software beinhaltet u. a.:
  - Antiviren-Software: Um den Dateizugriff zu beschleunigen, empfiehlt ATOSS, die ATOSS Time Control-Installationsverzeichnisse auf die Whitelist zu setzen.
  - Proxy: Stellen Sie den Proxy so ein, dass er einen lokal zugänglichen Client umgeht.
- Halten Sie Drittanbieter-Software aktuell und genehmigen Sie die Drittanbieter-Software. Zu Drittanbieter-Software zählen z. B. Windows, Browser, Antiviren-Software usw.

Im Folgenden finden Sie Hinweise zu möglichen Performance-Optimierungen, die sich speziell auf die ATOSS Time Control beziehen.

### Drosselung der Verarbeitung

Für eine optimale Serverauslastung können Sie CPU-Kerne, die für die Verarbeitungsmechanismen verfügbar sind, beschränken.

Verwenden Sie dazu die Einstellung 'Prozentualer Anteil verwendeter Prozessorkerne' in der Ansicht 'Servereinstellungen' in der Serverkonsole.

Geben Sie einen Prozentwert im Bereich von 0 bis 100 an. Wenn Sie den Prozentwert 0 angeben, verwendet der Server die maximale Anzahl von Prozessoren. Die Berechnung der Anzahl von Prozessoren berücksichtigt den Prozentwert 0 nicht.

### Ereignisse

Rufen Sie nur von Ihnen initiierte Ereignisse (sendOnlySelfInitiatedEvents) ab.

Verwenden Sie dazu folgenden Pfad und Registry-Schlüssel:

```
Pfad: Server/Daten-Server/Global
Schlüssel: sendOnlySelfInitiatedEvents
```

**Hinweis:** Beachten Sie, dass von anderen Benutzern durchgeführte Änderungen unter Umständen erst nach manueller Aktualisierung berücksichtigt werden.

### API-Hooks

Prüfen Sie, ob API-Hooks vorhanden sind. Weitere Informationen zu API-Hooks finden Sie im ATOSS Time Control Referenzhandbuch.

### Verarbeitungsregeln

Prüfen Sie die Verwendung von Verarbeitungsregeln. Nicht benötigte Verarbeitungsregeln verlangsamen die Verarbeitung. Weitere Informationen zu Verarbeitungsregeln finden Sie finden Sie im ATOSS Time Control Referenzhandbuch.

### Berechtigungsgruppen

Prüfen Sie die Berechtigungsgruppen. In der Regel reicht eine Berechtigungsgruppe pro Mitarbeiter aus. Weitere Informationen zu Berechtigungsgruppen finden Sie im ATOSS Time Control Referenzhandbuch.

### Geplante Reports

Während der Arbeitszeit generierte Reports können die ATOSS Time Control verlangsamen. ATOSS empfiehlt, die Reporterstellung über Nacht in einem geplanten Task.

### Kundenindividuelle Skripte

Prüfen Sie, ob Kundenskripte verwendet werden. Weitere Informationen zu Skripten finden Sie im ATOSS Time Control Referenzhandbuch.

### Session-Handling

ATOSS empfiehlt, dass Sie ein Sitzungs-Timeout anwenden. Weitere Informationen finden Sie unter *Verbindungsmanagement des Jetty-Webservers anpassen* auf Seite 38.

### Personaleinsatzplanung

In diesem Abschnitt finden Sie allgemeine Tipps für die Arbeit mit dem Mitarbeiterplan und der Personaleinsatzplanung.

**PEP-Szenarien**

- Bleiben Sie bei den Spalten, die Sie für die aktuelle Aufgabe benötigen.
- Erstellen Sie abhängig von der Aufgabe unterschiedliche PEP-Szenarien und beschränken Sie die Spaltenanzahl in einem allgemeinen Szenario. Szenarien mit einer hohen Spaltenanzahl haben eine lange Ladezeit.
- Deaktivieren Sie die Option **Mehrere Zeilen für Planungen und Fehlzeiten anzeigen**, wenn Sie die Option nicht benötigen. Sie deaktivieren die Option unter **PEP-Szenarien** > **Allgemein** > **Mehrere Zeilen für Planungen und Fehlzeiten anzeigen**.
- Deaktivieren Sie die Option **Einträge zur Berechnung des Urlaubs**, wenn Sie die Option nicht benötigen. Sie deaktivieren die Option unter **PEP-Szenarien** > **Spaltenzuordnung** > **Einträge zur Berechnung des Urlaubs**.
- Deaktivieren Sie die Option **Anzeigen von Salden**, wenn Sie die Option nicht benötigen. Sie deaktivieren die Option unter **PEP-Szenarien** > **Spalten** > **Spaltentyp**. Deaktivieren Sie alle Einträge, die Sie nicht benötigen, in der Auswahlliste.
- Schließen Sie nicht benötigte Ansichten in der verwendeten Perspektive. Nicht benötigte Ansichten mit langen Ladezeiten, wie z. B. die Ansicht 'Personalbedarf', beeinträchtigen die Performance erheblich.

**Arbeitsplätze**

Reduzieren Sie die Anzahl der Mitarbeiter pro Arbeitsplatz. Jeder zusätzliche Mitarbeiter erfordert zusätzliche Ladezeit für das gesamte PEP-Szenario.

Wechseln Sie von monatsweiser Zeitplanung zu kürzeren Zeitintervallen, z. B. zu Zeitintervallen von einer bis zwei Wochen.

### Protokollierung

Ein niedriger Protokollierungslevel produziert weniger Einträge in der Protokolldatei. Eine hohe Anzahl an Einträgen in der Protokolldatei kann das System verlangsamen.

### Komprimierung

Aktivieren Sie Komprimierung, um die Größe der übertragenen Daten zwischen dem Webclient und der ATOSS Time Control zu reduzieren. In Umgebungen mit geringer Bandbreite verbessert das Aktivieren der Komprimierung die Performance der ATOSS Time Control.

### TextSize-Cache

Prüfen Sie bei sehr großen Mengen an Datensätzen (z. B. viele Arbeitsplätze, Mitarbeiter, Projekte), ob der Cache-Parameter **TextSize** korrekt gesetzt ist. Die maximale Anzahl der Einträge in diesem Cache ist standardmäßig auf 10000 festgelegt. Diese Anzahl wird bei großen Datenbanken schnell überschritten. Das führt dazu, dass der verwendete Cache gelöscht und neu befüllt wird. Dabei gehen alle bereits ermittelten Textgrößen verloren, was zu Performance-Verlust führt. Die optimale Anzahl von Einträgen hängt von der Anzahl der Datensätze ab, die gleichzeitig in einer Liste angezeigt werden. Wenn sich die Anzahl von Projekten, Kostenstellen, Arbeitsplätzen, Mitarbeitern im Bereich mehrerer tausend Datensätze bewegt, wird der Cache bei der Anzahl 10000 schnell überlaufen und immer wieder neu aufgebaut. Um den Cache-Parameter **TextSize** anzupassen, gehen Sie wie folgt vor:

1. Prüfen Sie die Größe des konfigurierten Speichers.
2. Erhöhen Sie die Anzahl der Einträge im Cache moderat, z. B. in Schritten 50000, 100000, 150000 unter Berücksichtigung des konfigurierten Speichers.
3. Führen Sie nach jeder Änderung einen Server-Neustart durch.

**Hinweis:** Eine Verbesserung erkennen Sie daran, dass z. B. nach dem Öffnen der Mitarbeiter-/Arbeitsplatz-Administration und anschließendem mehrfachen Aktualisieren die Fortschritts-Sanduhr nicht mehr erscheint.

Weitere Informationen und ein Beispiel zur Konfigurierung von VM-Parametern finden Sie unter 'Indizes für ATOSS Time Control als Serviceinstallation neu erstellen' im ATOSS Time Control Installationshandbuch. Konfigurieren Sie den VM-Parameter neu, indem Sie sich an diesem Beispiel orientieren.

### Server-Cache

Ein Server-Cache wird verwendet, um Daten auf effiziente Weise zu speichern. Mit dem Server-Cache können Anfragen nach bereits abgerufenen Daten schneller aus dem Speicher geladen werden, anstatt diese bei jeder Anfrage aus der Datenbank anzufordern und erneut zu verarbeiten.

Die Gesamtleistung des Systems kann beeinträchtigt werden, wenn benutzerdefinierte Skripte, API-Hooks oder Erweiterungen aktiviert sind, die den Cache durch den Aufruf der API-Funktion `GetServerInformation` mit dem Parameter **resetcache** zurücksetzen. Einige API-Funktionen, z. B. `DataSetCopy`, können auch einen Cache-Reset auslösen. Um einen Neuaufbau des Server-Cache zu vermeiden, der die Gesamtleistung der ATOSS Time Control beeinträchtigt, überprüfen Sie, ob benutzerdefinierte Skripte, API-Hooks oder Erweiterungen aktiviert sind, und deaktivieren Sie diese ggf.

### HTTP-Threads

Über die Datei `atc.properties` können Sie die Anzahl an Threads steuern.

Beispiel:

```
http.minThreads, default = 8
http.maxThreads, default = 200
```

Über die Begrenzung von Threads wird die maximale Anzahl der angemeldeten Benutzer implizit begrenzt. Wenn gleichzeitig viele Benutzer angemeldet sind, können Sie den Wert für `http.maxThreads` auf einen höheren Wert als '200' setzen.

## 8.2 Hardware

In diesem Abschnitt finden Sie Informationen zu Hardware-Einstellungen, die zur Performance-Optimierung der ATOSS Time Control beitragen.

### Speichermanagement

Zur Verbesserung der allgemeinen Performance speichert der Stammdaten-Cache alle Stammdaten des Systems und vermeidet dadurch unnötige Datenbankzugriffe. Diese Funktionalität erfordert ausreichend Speicher- und Rechenleistung.

**Server**

- Prüfen Sie die Speichereinstellungen in **Server-Konsole** > **Speichereinstellungen**.
- Stellen Sie sicher, dass die Anzahl der Mitarbeiter für die aktuelle Installation korrekt ist.
- Stellen Sie sicher, dass die Einstellungen für den initialen und den maximalen Java Heap grün dargestellt werden.
- Tragen Sie bei ausreichend freiem Speicherplatz in das Ganzzahlfeld **-Xms** einen Wert ein, der mindestens einem Viertel des im Feld **-Xmx** eingetragenen Werts entspricht.

### CPU-Kerne

Die umfangreichen Berechnungen zur Zeitdatenverarbeitung erfordern eine performante Prozessorausstattung des Applikationsservers:

- Verwenden Sie für Installationen mit höheren administrativen Benutzerzahlen oder ESS-Benutzerzahlen Prozessoren mit 8, 16 oder mehr Kernen.
- ATOSS empfiehlt die Verwendung eines CPU-Kerns pro fünf aktiver Benutzer für den Webserver.
- ATOSS empfiehlt die Verwendung eines CPU-Kerns pro zehn gleichzeitig aktive ESS-Benutzer.
- Um zu vermeiden, dass alle verfügbaren CPU-Kerne verwendet werden und so zu wenig Leistung für ein flüssiges Arbeiten mit der Benutzeroberfläche zur Verfügung steht, begrenzen Sie die Hintergrund-Berechnungen. Detaillierte Informationen zum Vorgehen finden Sie unter 'Drosselung der Verarbeitung' unter *Allgemeine Hinweise* auf Seite 59.

## 8.3 Netzwerk

In diesem Abschnitt finden Sie Informationen zu hilfreichen Netzwerk-Einstellungen zur Performance-Optimierung der ATOSS Time Control.

### Latenz

- Prüfen Sie die Latenz zwischen dem Server und der Datenbank.
- Prüfen Sie die Latenz von einem Client (z. B. Webclient, Mobile) zum Server. Gehen Sie dazu wie folgt vor:

1. Rufen Sie die Entwicklertools des Browsers mit Strg + Umschalt + I auf.
2. Wählen Sie die Registerkarte 'Netzwerk' aus.
3. Wählen Sie auf der Registerkarte 'Netzwerk' die Aktion **Cache deaktivieren** aus.
4. Laden Sie die ATOSS Time Control-Webserver-Startseite unter `http://<serverip>:8080` neu.

   Im Prüf-Fenster sehen Sie die Ladezeit **tosscsd_logo_de.jpg**. Auf `localhost` beträgt die Ladezeit 3-10 ms. In der ATOSS Time Control-Umgebung beträgt die Ladezeit ca. 200 ms (Standort Berlin zum ATC-Server).

### VPN

Prüfen Sie Ihr Netzwerk auf vorhandene VPN-Verbindungen. VPN-Verbindungen können die Gesamt-Performance der ATOSS Time Control beeinflussen.

### Bandbreite

Wenn Sie einen Webclient verwenden, benötigen Sie eine Internetanbindung mit mindestens 6 Mbit/s.

## 8.4 Datenbank

In diesem Abschnitt finden Sie Informationen zu Datenbank-Einstellungen, die zur Performance-Optimierung der ATOSS Time Control beitragen.

### Allgemein

Analysieren Sie die SQL-Statements wie folgt:

- Suchen Sie mit dem SQL-Profiler kostenaufwändige SQL-Statements (z. B. SQL-Statements, die länger als 100 ms dauern).
- Suchen Sie nach duplizierten SQL-Statements und wenden Sie sich an Ihren ATOSS-Berater oder zertifizierten ATOSS-Partner.
- Analysieren Sie die SQL-Ausführungspläne und fügen Sie nach Möglichkeit Indizes, Einschränkungen usw. hinzu.

  **Hinweis:** Selbst hinzugefügte Indizes werden bei der Aktualisierung der Datenbankstruktur nur beibehalten, wenn der Name der Indizes mit dem Präfix 'udi' beginnt.

- Melden Sie Ihre individuellen Optimierungen an Ihren ATOSS-Berater oder zertifizierten ATOSS-Partner.

### Microsoft SQL-Datenbank

Optimierte Einstellungen innerhalb der Datenbank-Engine können sich auf die Performance auswirken.

**Kompatibilitätslevel**

Um alle Performance-Gewinne und Optimierungen zu nutzen, die für die aktuell verwendete Datenbankversion verfügbar sind, geben Sie die aktuelle Version des SQL-Servers an, den die Datenbank unterstützt. Beim Upgrade einer SQL-Server-Datenbank wird der Kompatibilitätslevel für diese Datenbank beibehalten oder auf den Mindestlevel geändert, der für die neue SQL-Server Version unterstützt wird. Bei einer Kompatibilität auf Mindestlevel sind die neuesten Verbesserungen nicht nutzbar.

**Wiederherstellungsmodell**

Die Sicherungs- und Wiederherstellungsoperationen des SQL-Servers finden im Kontext des Wiederherstellungsmodells der Datenbank statt. Mit Wiederherstellungsmodellen wird die Wartung von Transaktionsprotokollen gesteuert. Sie umfassen:

- die Art der Protokollierung der Transaktionen
- Aspekte zur Sicherung des Transaktionsprotokolls

- Arten der verfügbaren Wiederherstellungsoperationen

Folgende Wiederherstellungsmodelle sind verfügbar:

- einfach
- vollständig
- massenprotokolliert

Eine Datenbank verwendet üblicherweise das vollständige oder das einfache Wiederherstellungsmodell. Sie können die Datenbank jederzeit auf ein anderes Wiederherstellungsmodell umstellen. Die Performance kann unabhängig vom Typ des Wiederherstellungsmodells beeinträchtigt werden. Prüfen Sie das Wiederherstellungsmodell mit der verwendeten Sicherungsstrategie sorgfältig.

**Änderungsnachverfolgung**

Die Änderungsnachverfolgung kann sich ebenfalls deutlich auf die Performance auswirken. ATOSS empfiehlt, die Funktion 'Änderungsnachverfolgung' zu deaktivieren, da die ATOSS Time Control bereits eine Nachverfolgung für wichtige Daten enthält.

**Wachstumsfaktoren**

Niedrige Werte in MB werden als schlecht angesehen. ATOSS empfiehlt, einen Prozentwert von z. B. 10% einzugeben.

**Partition mit empfohlener Sektor-Größe**

ATOSS empfiehlt, die Installation der SQL-Server-Datenbankdateien auf einer eigenen NTFS-formatierten Partition mit einer Sektor-Größe von 4096 KB zu installieren.

**Index-Fragmentierung prüfen**

Mit folgender Abfrage erhalten Sie die Statistik über den Index:

```
SELECT OBJECT_NAME(ind.OBJECT_ID) AS TableName,
ind.name AS IndexName, indexstats.index_type_desc AS IndexType,
indexstats.avg_fragmentation_in_percent
FROM sys.dm_db_index_physical_stats(DB_ID(), NULL, NULL, NULL, NULL) indexstats
INNER JOIN sys.indexes ind
ON ind.object_id = indexstats.object_id
AND ind.index_id = indexstats.index_id
WHERE indexstats.avg_fragmentation_in_percent > 30
ORDER BY indexstats.avg_fragmentation_in_percent DESC
```

Das Programm Management Studio bietet ihnen die Möglichkeit, einen Index über die Kontextmenüeinträge **Neu erstellen** oder **Neu organisieren** neu aufzubauen bzw. zu reorganisieren. Oder Sie reorganisieren alle Indizes wie folgt:

```
declare @tableName nvarchar(500)
declare @indexName nvarchar(500)
declare @indexType nvarchar(55)
declare @percentFragment decimal(11,2)

declare FragmentedTableList cursor for
 SELECT OBJECT_NAME(ind.OBJECT_ID) AS TableName,
   ind.name AS IndexName, indexstats.index_type_desc AS IndexType,
   indexstats.avg_fragmentation_in_percent
 FROM sys.dm_db_index_physical_stats(DB_ID(), NULL, NULL, NULL, NULL) indexstats
   INNER JOIN sys.indexes ind ON ind.object_id = indexstats.object_id
        AND ind.index_id = indexstats.index_id
  WHERE
-- indexstats.avg_fragmentation_in_percent , e.g. >30, you can specify any number in percent
   indexstats.avg_fragmentation_in_percent > 5
  AND ind.Name is not null
  ORDER BY indexstats.avg_fragmentation_in_percent DESC

    OPEN FragmentedTableList
    FETCH NEXT FROM FragmentedTableList
    INTO @tableName, @indexName, @indexType, @percentFragment
```

```
   WHILE @@FETCH_STATUS = 0
   BEGIN
     print 'Processing ' + @indexName + 'on table ' + @tableName + ' which is ' + cast(@percentFragment
as nvarchar(50))
     + ' fragmented'

     if(@percentFragment<= 30)
     BEGIN
           EXEC( 'ALTER INDEX ' +  @indexName + ' ON ' + @tableName + ' REBUILD; ')
      print 'Finished reorganizing ' + @indexName + 'on table ' + @tableName
     END
     ELSE
     BEGIN
        EXEC( 'ALTER INDEX ' +  @indexName + ' ON ' + @tableName + ' REORGANIZE;')
       print 'Finished rebuilding ' + @indexName + 'on table ' + @tableName
     END
     FETCH NEXT FROM FragmentedTableList
       INTO @tableName, @indexName, @indexType, @percentFragment
   END
   CLOSE FragmentedTableList
   DEALLOCATE FragmentedTableList
```

**Statistiken aktualisieren**

Statistiken aktualisieren Sie mit:

```
EXEC sp_updatestats;
```

### H2-Datenbank

ATOSS empfiehlt, die H2-Datenbank nicht für den produktiven Einsatz zu verwenden. H2 ist aufgrund seiner Eigenschaften für kleine Test- und Demosysteme mit häufigem Datenbankwechsel geeignet und ersetzt nicht einen eigenständigen Datenbankserver.

Auch mit URL-Optionen kann die Performance verbessert werden, z. B.:

- `CACHE_SIZE`
- `QUERY_CACHE_SIZE`
- `EARLY_FILTER`

Weitere Informationen zu URL-Optionen finden Sie unter: *http:///www.h2database.com/html/features.html*

Ab der ATOSS Time Control 10 können Sie mit der Eigenschaft `database.url` der Datei `com.atoss.database.dbi.prefs` zusätzliche Optionen setzen.

Beispiel:

```
database.url=jdbc:h2:C:/data/database/h2/10.0/database14;
          LOCK_TIMEOUT=10000;
          ARLY_FILTER=true;
          EQUERY_CACHE_SIZE=32;CACHE_SIZE=32768
```

# 9 Anhang

## 9.1 Liste der verwendeten Netzwerkports

Hier finden Sie eine Übersicht über die von Time Control und der eingesetzten Hardware verwendeten Standardports.

| ATOSS Time Control und Hardware | Port |
|---|---|
| ATOSS Time Control-Webserver | 443 |
| | 8080 |
| ATOSS Time Control-Server | 2711 |
| | 12711 |
| ATOSS Time Control-Geräteprozess | 2411 |
| PCS-Hardware | 3001 |
| | 3040 |
| | 3041 |
| | 3020 |
| | 3021 |
| PCS-Hardware: Wartung Terminal | 57005 |
| | 3121 |
| DHCM I/II Hardware | 21 |
| | 1010 |
| Kaba-Hardware | 3005 |
| | 1099 |
| Datafox-Geräte | 8000 |
| | 9090 |
| Online-Lizenzierung (IP 5.45.96.70) | 8443 |

# Index

## L



## M



## N



## P



## R



## S



## T



## U



## V