| Dokumentnamn / Document name | | Sida / Page |
|---|---|---|
| RI0107_CleanCashServerManual | | 1 (15) |
| | Datum / Date<br>2010-10-29 | Reg. nr. / Doc. no. |
| | | |
| | | Utgåva / Revision<br>B4 |

# Installation and operation

# of

# CleanCash® Server

## Table of contents

1. Revision history ... 3

2. Overview ... 3
   2.1. Purpose ... 3
   2.2. Scope and limitations ... 3

3. Installation and configuration ... 4
   3.1. System overview ... 4
   3.2. System requirements ... 4
   3.3. Operation under Linux ... 4
   3.4. Installation ... 5
   3.5. Configuration options ... 5
   3.6. Initial configuration ... 5

4. CleanCash Server Console ... 6
   4.1. Dashboard ... 6
   4.2. Server Settings ... 7
   4.3. Ports ... 8
   4.4. Routes ... 9
   4.5. Users ... 10
   4.6. Log settings ... 11
   4.7. Security ... 12

5. Configuration files ... 12
   5.1. Windows ... 12
   5.2. Linux ... 12
   5.3. CleanCash.*.exe.config ... 12
   5.4. Router.config ... 13

6. SSL Certificate Information ... 14
   6.1. Create self signed certificate using OpenSSL or Microsoft MakeCert ... 14
   6.2. Create self signed certificate using Pluralsight Self-Cert ... 14

7. Transaction Logs ... 14

# 1. Revision history

| Rev | Sign | Date | Changes since last revision |
|---|---|---|---|
| B4 | KR | 2010-10-29 | Added instructions for initial configuration and extra information about SSL certificates. |
| B3 | KR | 2010-09-09 | Updated for CleanCash Server 2.2 |
| B2 | KR | 2010-07-30 | Updated for CleanCash Server 2.1 |
| B1 | KR | 2010-06-07 | Minor updates about routing. |
| B0 | KR | 2010-05-26 | Updated to CleanCash Server 2.0 |
| A4 | KR | 2010-02-01 | - Corrected routing information |
| A3 | KR | 2010-02-01 | - Added authentication information<br>- Added new routing information |
| A2 | KR | 2009-12-17 | Updated with platform information |

# 2. Overview

## 2.1. Purpose

This document contains information on installations and operations of CleanCash® Server.

This document may only be used with permission from Retail Innovation.

## 2.2. Scope and limitations

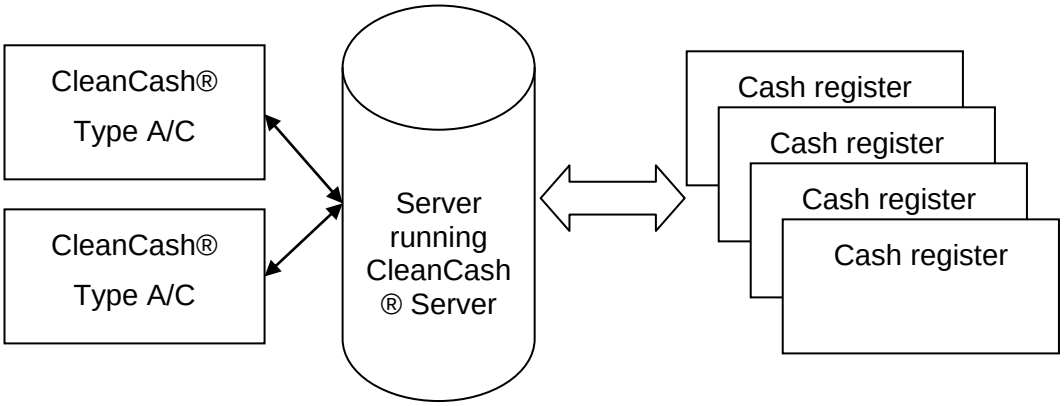
CleanCash® Server is a software provided by Retail Innovation for sole use by software providers to communicate with control units of the following types:

- Retail Innovation CleanCash® Type A
- Retail Innovation CleanCash® MultiUser Type $C_1$
- Retail Innovation CleanCash® MultiUser Type $C_5$
- Retail Innovation CleanCash® MultiUser Type $C_{10}$
- Retail Innovation CleanCash® MultiUser Type $C_{20}$
- Retail Innovation CleanCash® MultiUser Type $C_{20+}$
- Retail Innovation CleanCash® MultiUser Type $C_F$

The software developer will use CleanCash® Server as a part of their software solution and is registered to Skatteverket through the Manufacturers Declaration of the software provider. Retail Innovation will not make any Manufacturers Declaration to Skatteverket on CleanCash® Server but will provide supporting documents to facilitate a smooth inclusion in the software provider's Manufacturers Declaration.

# 3. Installation and configuration

## 3.1. System overview




CleanCash® Server is installed on a server connected to a network possible to access from the individual Point-of-Sales workstations to be serviced. The CleanCash® control units are connected to the actual server running CleanCash® Server.

## 3.2. System requirements

### 3.2.1. Microsoft Windows

The following versions of Microsoft Windows are recommended for CleanCash® Server:

- Windows XP Professional SP 2 or later
- Windows Server 2003
- Windows Server 2008, 2008R2
- Windows Vista Business, Ultimate and Enterprise
- Windows 7 Professional, Ultimate and Enterprise

Other versions such as Windows XP Home, Vista Home etc have TCP/IP connection limitations which may affect the performance of CleanCash® Server.

### 3.2.2. Linux

A linux platform with Novell Mono v2.4 or later is required for running CleanCash® Server. Initialization scripts are provided for Ubuntu and most other debian based distributions.

### 3.2.3. OS X

OS X is currently not supported due to bugs in the OS X port of Mono. Retail Innovation AB are working on a solution.

## 3.3. Operation under Linux

### 3.3.4. Directory layout

/etc/ccserver.d – Location for configuration files

/etc/ccserver.d/default – Location for default configuration files

/opt/ccserver – Root for server installation

/opt/ccserver/bin – Linux executeable(s)

/opt/ccserver/lib - .Net Exe-file(s) and dynamic link libraries.

/var/log/ccserver – Default location for log files.

#### 3.3.5. Executeable files

/etc/init.d/ccserverd – Debian / Ubuntu init-script for CleanCash Server.

/opt/ccserver/bin/ccserver – CleanCash Server start script.

#### 3.3.6. Limitations

In version 2.1 of CleanCash Server the admin console is disabled due to bugs in Mono. Retail Innovation are looking at workarounds.

Auto detection of USB-connected devices is only available if run under a Linux system with udev support.

## 3.4. Installation

#### 3.4.7. Microsoft Windows

Install CleanCash® Server by running CleanCashServer_x_z_z.msi. This will generate a self-installed Service located in the following location:

%ProgramFiles%\Retail Innovation HTT AB\CleanCash Server (For 32-bit systems)

%ProgramFiles(x86)%\Retail Innovation HTT AB\CleanCash Server (For 64-bit systems)

**Note:**
CleanCash Server Setup Guide is no longer recommended for use with CleanCash Server.

#### 3.4.8. Linux

1. Unpack the tarball in a temporary directory.
2. Run install_ccserver.sh as root.
3. Create a link to */etc/init.d/ccserverd* from the appropriate run level directory. If running under a non-debian based distribution then the ccserverd script may have to be replaced with an appropriate script for your distribution.
4. */opt/ccserver/bin/ccserver* may need to be edited to point to the correct location for Novell Mono.

## 3.5. Configuration options

#### 3.5.9. Microsoft Windows

CleanCash Server can be configured by two different methods.

1. Using a web based administration interface. (CleanCash Server Console)
2. By editing CleanCash Server configuration files manually.

**Note:**
CleanCash Server Setup Guide is no longer recommended for use with CleanCash Server.

## 3.6. Initial configuration

This section describes the initial steps that should be taken when configuring CleanCash Server for the first time. This example shows how to do this using CleanCash Server Console.

#### 3.6.10. Step 1, Access CleanCash Server Console

Open a web browser and connect to http://127.0.0.1:8081/admin.

Login with user “admin” and password “admin”.

#### 3.6.11. Step 2, Configure port options [CleanCash Type A only]

If CleanCash Type A units are used then add the port(s) that they are connected to. (*See section 4.3 Ports*)

#### 3.6.12. Step 3, Add default route

If all cash registers shall be routed to the same CleanCash unit then add a route with “*” as PosId and the CleanCash unit’s serial number. (*See section 4.4 Routes*)

#### 3.6.13. Step 4, Add username/password for cash registers

Add a username / password for all cash registers or separate usernames for all cash registers. (*See section 4.5 Users*)

#### 3.6.14. Step 5, Change admin password [optional]

Change the admin user’s password. (*See section 4.5 Users*)

#### 3.6.15. Step 6, Setup encrypted SSL communication [optional]

Select SSL certificate and enable HTTPS communication. (*See section 4.2 Server Settings*)

#### 3.6.16. Step 7, Change logging settings [optional]

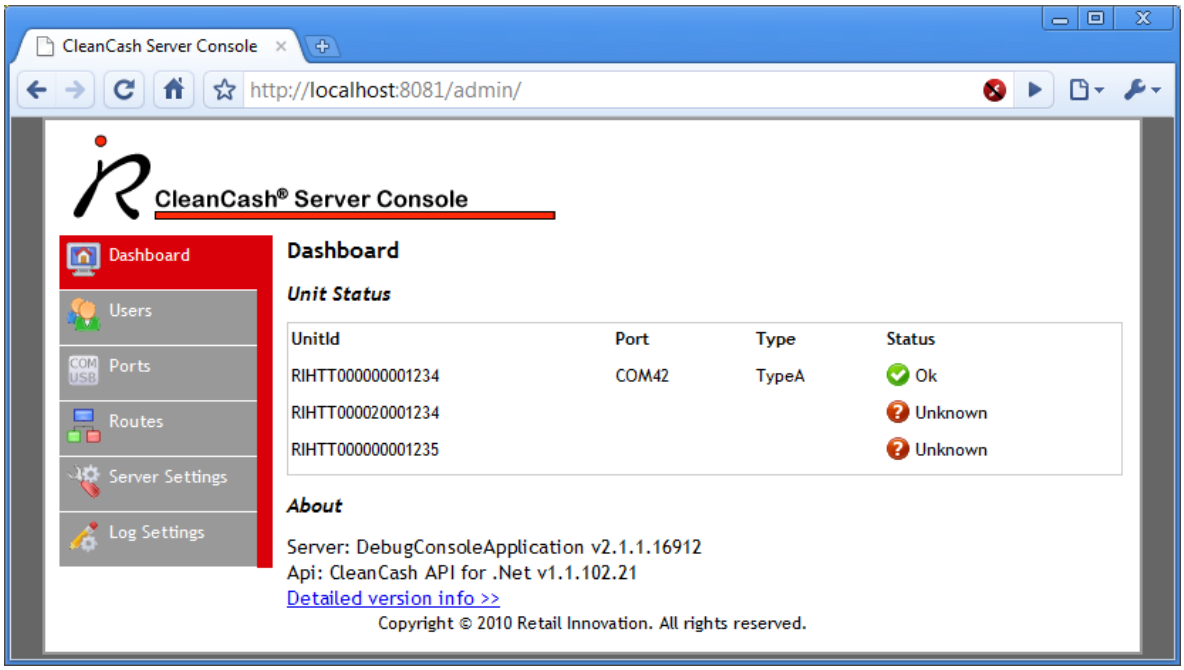
At least select the location for log files. (*See section 4.6 Log settings*)

# 4. CleanCash Server Console

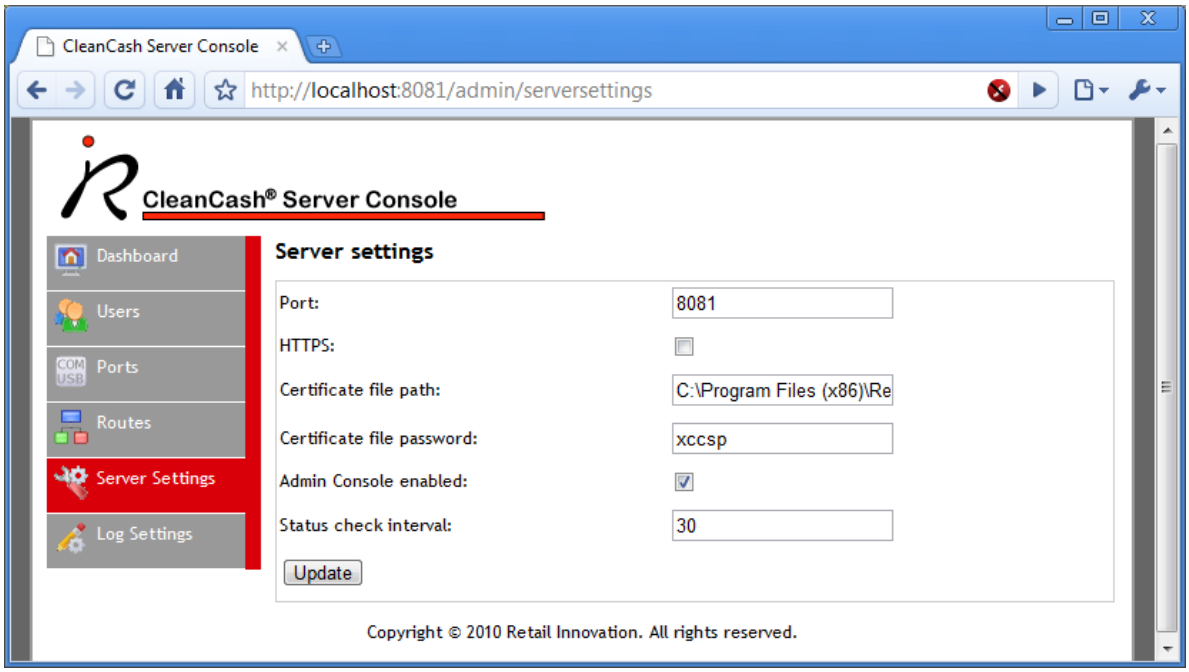
CleanCash Server Console can be accessed by connecting to http://127.0.0.1:8081/admin (default configuration) and user “admin” with password “admin”.

## 4.1. Dashboard

The Dashboard shows a summary of the system status. Detailed version information can also be obtained.




## 4.2. Server Settings




The Server settings page contains settings for configuring the protocol and port for CleanCash Server. This page configures the XML-setting <HttpListener>.

### 4.2.17. Port

The port number which CleanCash Server should listen on. (Default 8081 for http)

### 4.2.18. HTTPS

Check this box if CleanCash Server should use HTTPS (encryption) for communication. If HTTPS is checked, then a certificate file and password must be specified.

#### 4.2.19. Certificate file path

The certificate file which should be used for HTTPS communication. CCServer ships with a test certificate *CleanCashServerCert.p12*.

***Important:*** See section 6 SSL Certificate Information before configuring HTTPS.

#### 4.2.20. Certificate file password

This is the certificate's password. (*CleanCashServerCert.p12* has password "xccsp")

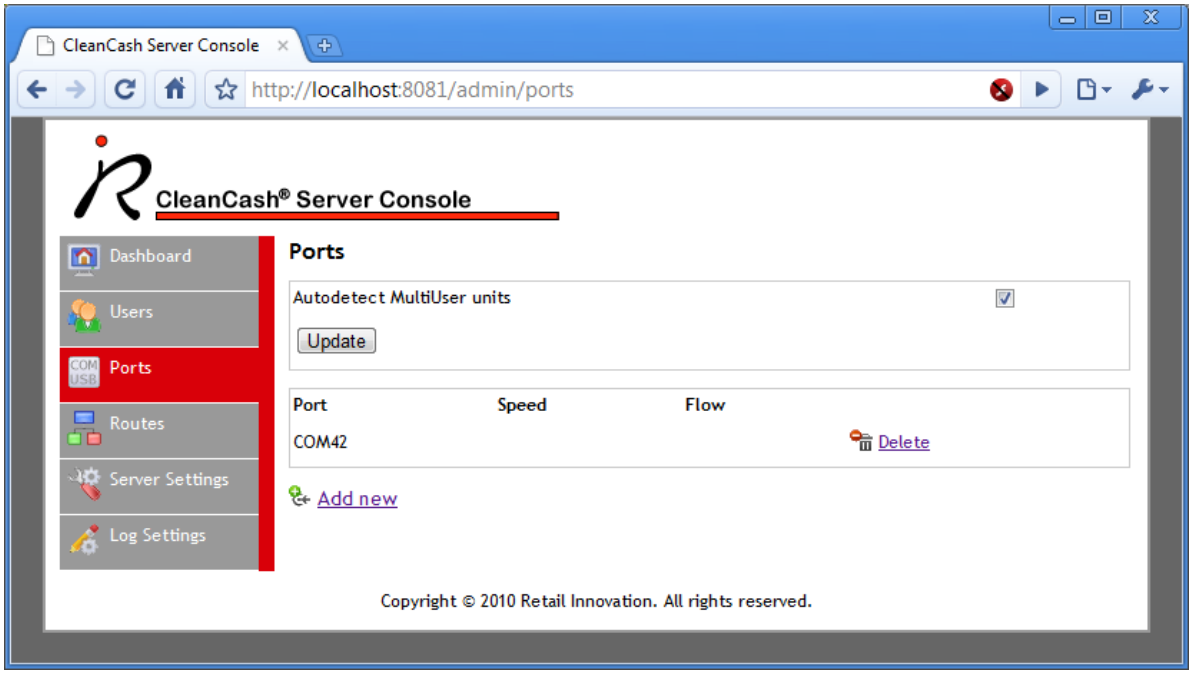
#### 4.2.21. Admin console enabled

Uncheck this box if the Admin console should be disabled.

#### 4.2.22. Status check interval

The interval in seconds between each unit status check. The system will check all units periodically and report any errors.

### 4.3. Ports




The Ports page defines which ports that CleanCash Server should probe for attached CleanCash units.

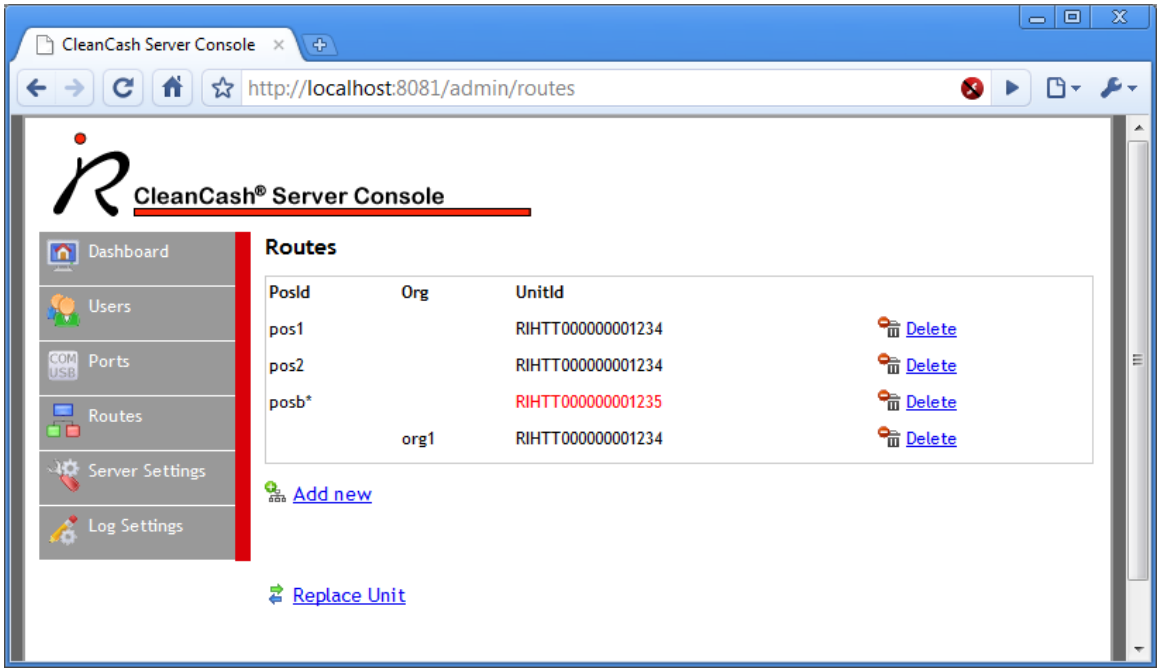
#### 4.3.23. Autodetect MultiUser units

Check this unit if CleanCash Server should detect CleanCash MultiUser units automatically. (Strongly recommended as USB units receive different port names depending on which USB port they are inserted into)

#### 4.3.24. Port

Ports that CleanCash Type A units are connected to. (or MultiUser units if autodetect is off)

## 4.4. Routes




The Routes page allows the administrator to define routing information.

A route is a rule defining which messages a unit should receive. A route contains two parameters; a source (PosId or Organization number) and a destination (UnitId).

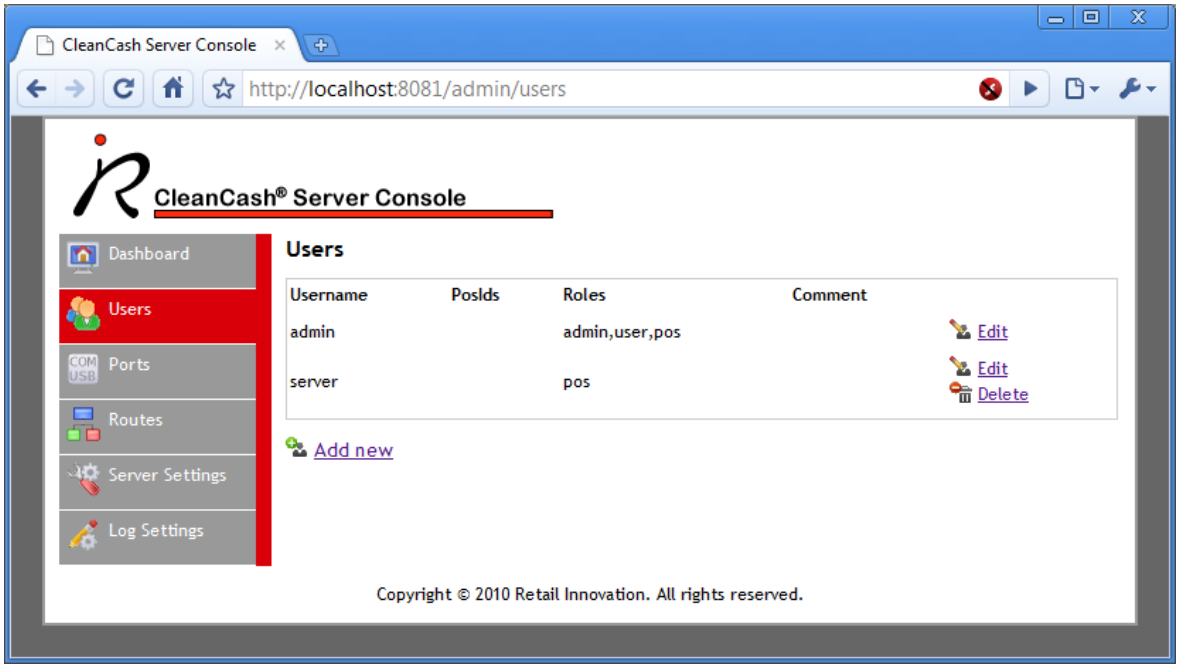
Routes are matched in the following order:

1. Specific pos routes. (E.g PosId="Pos1")
2. Specific organization number routes. (E.g Org="5566778899")
3. Wildcard routes. (E.g PosId="Pos*")

Examples:

- PosId: "pos1", UnitId "RIHTT00000001234" – Routes all messages from pos1 to RIHTT00000001234
- PosId: "posb*", UnitId "RIHTT00000001234" – Routes all messages with a pos id starting with "posb" to RIHTT00000001234.
- PosId "*", UnitId "RIHTT00000001234" – Routes all messages to RIHTT00000001234.
- Org "5566778899", UnitId "RIHTT00000001234" – Routes all messages with organisation number 556677-8899 to RIHTT00000001234.

## 4.5. Users




This page configures authentication information.

### 4.5.25. Username

The username of the user.

### 4.5.26. PosIds

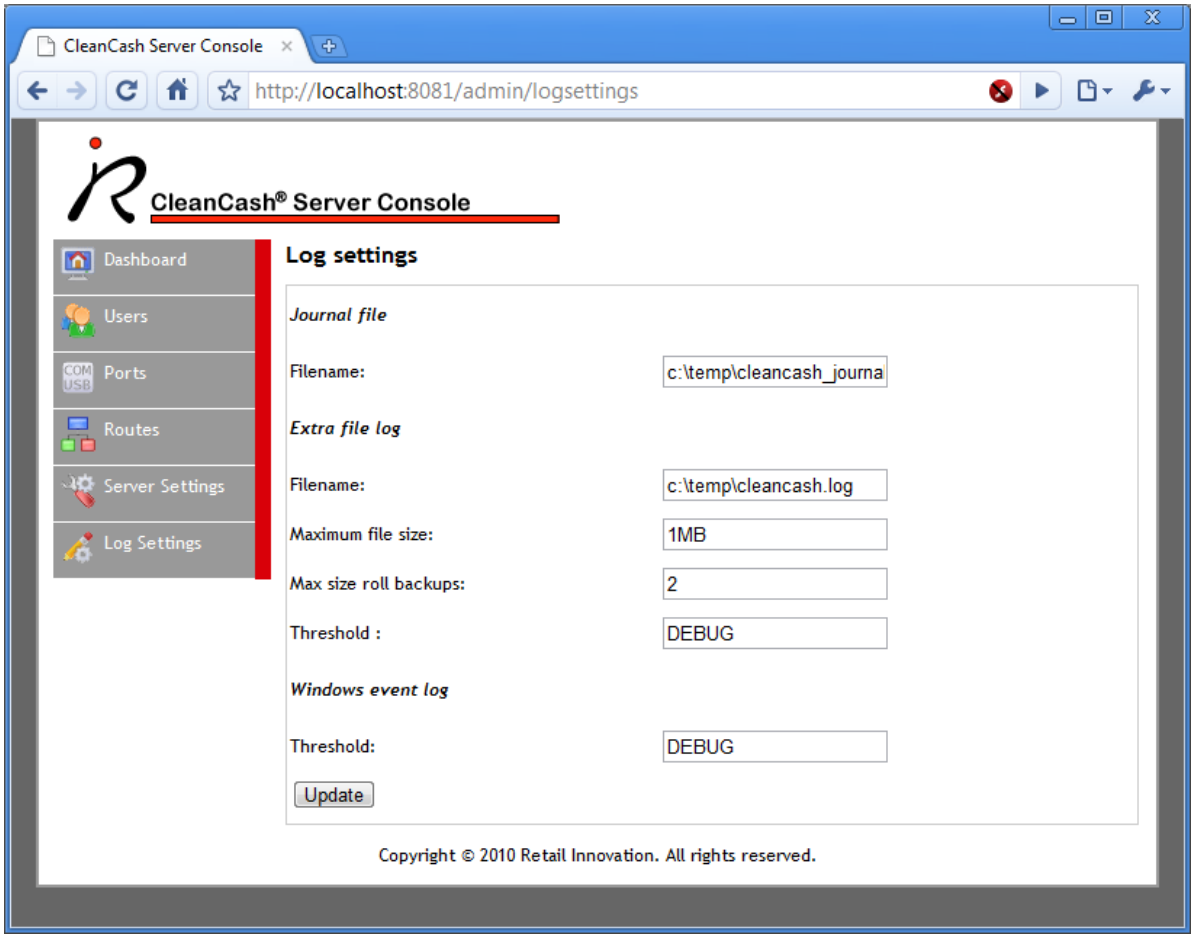
Which pos id:s can authenticate using this user. (Wildcard * = all pos id:s)

### 4.5.27. Roles

One of the following roles (access levels):

- Admin – is allowed to use the admin console and edit settings. (No pos id should be defined for this role)
- User – is allowed to see status in the admin console.
- Pos (default) – A user used for pos identification.

## 4.6. Log settings




The log settings page is for configuring logging.

Logging can be set using several levels:

- Fatal – Only log fatal errors
- Error – Log all errors
- Warn – Log warnings and errors
- Info – Log informational messages, warnings and errors
- Debug – Log all messages.

### 4.6.28. Journal file

This is a mandatory logging file which always logs using level Info.

### 4.6.29. Extra log file

This is a log file which can be used for logging with other settings than the journal file.

### 4.6.30. Windows event log

Logging to Windows event log.

## 4.7. Security

CleanCash® Server supports communication over https with user authentication with user/password pair.

# 5. Configuration files

## 5.1. Windows

CleanCash® Server uses two XML files located in the same location as CleanCash Server. The files are designated with the following file names:

CleanCash.Service.exe.config

Router.config

If the configuration files are changed, the CleanCash® Server Service will automatically restart to load the new configuration parameters.

## 5.2. Linux

CleanCash® Server uses two XML files located in */etc/ccserver.d*. The files are designated with the following file names:

CleanCash.LinuxServer.exe.config

Router.config

If the configuration files are changed, the CleanCash® Server Service will automatically restart to load the new configuration parameters.

## 5.3. CleanCash.*.exe.config

This is the main configuration file used by CleanCash® Server.

### 5.3.31. Port and HTTPS certificate

The following line designates what port the Service is to monitor.

```
<HttpListener Port="88" X509Certificate="C:\myserver.cer"
X509Password="myPassword" HTTPS="true" AdminConsole="false"/>
```

Port designates the http/https port that the CleanCash® Server Service is to monitor
`X509Certificate` designates the https secure communication certificate
`X509Password` designates the password protecting the certificate
`HTTPS` controls if https or http should be used (default true)
`AdminConsole` controls if administration console should be enabled or not (default true)

If the attribute X509Certificate points to a valid certificate CleanCash® Server and HTTPS=true then CleanCash® Server will use https encrypted communication mode. If a valid certificate is not present or activated CleanCash® Server will use native http communication.

***Important:*** *See section 6 SSL Certificate Information* before configuring HTTPS communications.

### 5.3.32. Authentication

Authentication can be set for all POSs or separately for each POS.

```
<Authentication>
    <add Username="test1" Password="test1" PosId="*" Roles="admin"/>
    <add Username="test2" Password="test2" PosId="pos1,pos2" Roles="pos"/>
</Authentication>
```

### 5.3.33. Physical Control Units

The following lines designate to which ports physical CleanCash® control units are connected to the server.

```
<Units AutoDetect="true">

  <add Port="COM42" Speed="9600" FlowControl="RtsCts" />
  <add Port="USB1" />

</Units>
```

If AutoDetect is set to true, then all USB-connected devices will be detected automatically.

Port designates the virtual or physical port name provided by the operating system
Speed is the communication speed of the port set in the operating system
FlowControl is the communication handshake selected for the port set in the operating system

### 5.3.34. Router configuration

The following line designates a secondary file containing the routing information used by CleanCash® Server.

```
<Router configSource="router.config"/>
```

## 5.4. Router.config

```
<Router>
  <Routes>
    <add PosId="pos1" UnitId="RIHTT000000001234"/>
    <add PosId="pos2" UnitId="RIHTT000000001234"/>
    <add OrganizationId="5566771234" UnitId=" RIHTT000000001234"/>
  </Routes>
</Router>
```

PosId designates the Point-of-Sales application license running on a workstation
UnitID designates the name of each control unit
OrganizationId designates the actual organization number of the company runing the Point-of-Sales application license

This file contains routing information on what broadcast messages received by CleanCash® Server should be sent to each physical unit connected to the server.

A route is a rule defining which messages a unit should receive. A route contains two parameters; a source (PosId or Organization number) and a destination (UnitId).

Examples:

- PosId: "pos1", UnitId "RIHTT00000001234" – Routes all messages from pos1 to RIHTT00000001234

- PosId: “posb*”, UnitId “RIHTT00000001234” – Routes all messages with a pos id starting with “posb” to RIHTT00000001234.
- PosId “*”, UnitId “RIHTT00000001234” – Routes all messages to RIHTT00000001234.
- Org “5566778899”, UnitId “RIHTT00000001234” – Routes all messages with organisation number 556677-8899 to RIHTT00000001234.

In the structure above Router.config effectively ties the ”pos1” Point-of-Sales application license to the ”RIHTT000000001234” CleanCash® control unit – and hence all messages coming from ”pos1” is thereafter routed to the ”RIHTT000000001234” CleanCash® control unit.

Finally a line is included to connect all messages from a given organization number to a designated CleanCash® control unit. In the example "5566771234" is connected to the “RIHTT000000001234” CleanCash® control unit.

# 6. SSL Certificate Information

For development purposes the supplied test certificates *localhost.cer* (no password) and *CleanCashServerCert.p12* (password “xccsp”) can be used for securing communication

For production systems **DO NOT USE** the supplied certificates since they are available to anyone thus removing most of the advantage of using SSL encryption.

For production environments there exists two options:

1. Purchase a commercial certificate from VeriSign, Thawte, GoDaddy or other SSL certificate providers. This provides the highest security, but increases complexity and should only be used by people familiar with SSL security.
2. Create your own self signed certificate file.

## 6.1. Create self signed certificate using OpenSSL or Microsoft MakeCert

The most flexible solution for creating a self signed certificate is using the software OpenSSL or Microsoft MakeCert. Instructions for using them can be found at http://webserver.codeplex.com/wikipage?title=HTTPS

## 6.2. Create self signed certificate using Pluralsight Self-Cert

A simpler alternative which does not let the user specify as much information in the certificate is to use Pluralsight’s Self-Cert application. Read more at http://www.pluralsight-training.net/community/blogs/keith/archive/2009/01/22/create-self-signed-x-509-certificates-in-a-flash-with-self-cert.aspx.

# 7. Transaction Logs

CleanCash® Server uses log4net to log the transactions performed.

Log4net is a general framework used for logging data transactions to multiple destinations.

The supplied sample configuration of log4net generates the log output to the following target file: c:\cleancashserver.log

It also creates a Windows debug output. Please use a tool like DebugView to check log output sent to Windows debug output. You can find DebugView on this link: http://technet.microsoft.com/en-us/sysinternals/bb896647.aspx

For further reference on log4net, please check the following web site:
http://logging.apache.org/log4net/index.html