cockpit
IT Service Manager

Cockpit ITSM installation - Windows

Technical specification

Table of contents

Introduction

I. Object

This document describes the stages to be followed in order to install a Cockpit IT Service Manager instance on a host running the Windows operating system.
A Cockpit IT Service Manager instance is composed of several elements.

- One database
- One or several portals
- Eventually one or several monitoring engines

II. Assumptions

This installation guide has been written under certain assumptions.

- Database engine will be MariaDB, it will be listening to the default port (3306)
- Search engine will be Solr, it will be listening to the default port (8983)
- Cockpit ITSM - Portal will be listening to the port 80 or 443 (SSL)
- Cockpit ITSM - Manager will be listening to the port 8081

III. Installation order

The Cockpit IT Service Manager components must be installed in a certain order.

1. Database (only one)
2. Manager (one on each server running Portal)
3. Portal (one or several)
4. Search engine (only one)

Prerequisites

I. Software to download

Usage	Software and version	Download
Database server	MariaDB Server 10.3 (64 bits)	https://downloads.mariadb.org/
Search engine	Apache Solr	https://archive.apache.org/dist/lucene/solr
Cockpit ITSM - Database	SQL file	https://download.cockpit-itsm.-com/exp/stable/
Cockpit ITSM - Portal	koaly-exp-portal-service-XXX-setup.exe	
Cockpit ITSM - Manager	koaly-management-interface-XXX-setup.exe	

II. Configuration

A. Operating system

The supported operating systems are:

- **Windows Server 2019 (64 bits)**
- **Windows Server 2016 (64 bits)**

The system must be installed in **english (US)**.

The **database** and the **portals** need to be installed on machines configured in the same time zone and with system clocks differing less than one minute.

B. Server specifications

Volume	Element	Specifications
Up to 10 operators Up to 200 monitored equipments Up to 3 monitoring engines	Architecture	Single virtual server (Portal + Database)
	Processor	2 cores - 64 bits
	Memory	6 Gb
	Storage	120 Gb
Up to 30 operators Up to 1000 monitored equipments Up to 20 monitoring engines	Architecture	Single virtual server (Portal + Database)
	Processor	4 cores - 64 bits
	Memory	8 Gb
	Storage	160 Gb
Up to 100 operators Up to 5000 monitored equipments	Architecture	Single virtual server (Portal + Database)
	Processor	6 cores - 64 bits

Up to 100 monitoring engines	Memory	16 Gb
	Storage	320 Gb

C. Memory allocation

This installation manual is based on a default deployment: All necessary components are installed on a single machine with 4Gb of physical RAM.

For larger deployments, you will need to adapt the memory allocation for each component according to the total physical RAM of the machine.

To customize memory allocation, you will need to update the configuration of each component individually as described in the following table.

Component	File	Parameter	Default value
Database	C:\Program Files\MariaDB 10.X\data\my.ini	innodb_buffer_pool_size	512M
Portal	C:\koaly\exp\portal\conf\koaly-exp-portal-service.config	maxHeap	2048m

The following table contains recommended memory allocation for a standard deployment of all components on a single machine.

Physical RAM	Database	Portal
4 Gb	512M	2048m
6 Gb	1024M	3072m
8 Gb	2048M	6144m
16 Gb	4096M	10240m

> Note: For larger deployments, it is recommended to install each component on a separate machine. In this case, the memory allocation should be adapted according to the specific workload of each component.

If your deployment differs from the default setup on a single machine, please contact the support team for sizing recommendations adapted to your specific workload and architecture.

Directories

I. Documents

Create the following directories.

- C:\koaly\exp\documents\alert\mib
- C:\koaly\exp\documents\doc\online
- C:\koaly\exp\documents\doc\archive
- C:\koaly\exp\documents\report\attachment
- C:\koaly\exp\documents\report\specific
- C:\koaly\exp\documents\ticket\attachment
- C:\koaly\exp\documents\ticket\msg_attachment

> Note: This directory will store documents, reports, ticket attachments and SNMP MIB files.

II. Update source

If you use a single server for Cockpit IT Service Manager, create the following directories.

- C:\koaly\update\koaly-exp-db
- C:\koaly\update\koaly-exp-engine\ext\lib
- C:\koaly\update\koaly-exp-portal\lib

> Important: This directory will contain new versions of Cockpit IT Service Manager and external libraries. Cockpit Manager will use the files in this directory to update Cockpit IT Service Manager Portals and Engines installed on this server. If you use several servers for Cockpit IT Service Manager, you can set up a single shared directory (e.g. using NFS) or website to store new versions of Cockpit IT Service Manager and external libraries. Cockpit Manager will connect to this shared directory or website to update current Cockpit IT Service Manager Portals and Engines. Note that the update files can be uploaded through Koaly Manager as well.

Database

> Note: MariaDB is a binary-compatible replacement for MySQL. The use of MySQL instead of MariaDB is supported.

I. File preparation

Create the following directory.

- C:\koaly\exp\database

Extract the SQL dump file (koalyexp.sql) from koaly-exp-database.zip to the directory C:\koaly\exp\.

II. MariaDB

A. Installation

Launch the MariaDB installation executable.

Accept the license agreement.

Hit "Next"

Select all components in the group "MariaDB Server".

All other components are not need (choose "Entire feature will be unavailable").

Hit "Next"

Check the option "Modify password for user 'root'" and choose your root password.

Leave the option "Enable access from remote machines for 'root' user" unchecked.

Leave the option "Create An Anonymous Account" unchecked.

Check the option "Use UTF-8 as default server's character set".

Hit "Next"

Check the option "Install as service".

Check the option "Enable networking".

Choose TCP port 3306 (default).

Check the option "Optimize for transactions" and set the buffer pool size to 1024 Mb.

Hit "Next"

Uncheck the feedback option.

Hit "Next"
Hit "Install"
Hit "Finish"

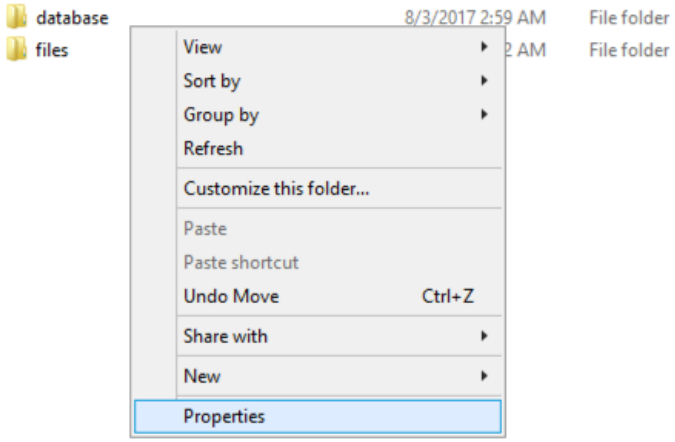
III. Configuration

Stop MariaDB server using Windows Management Console (command: services.msc).

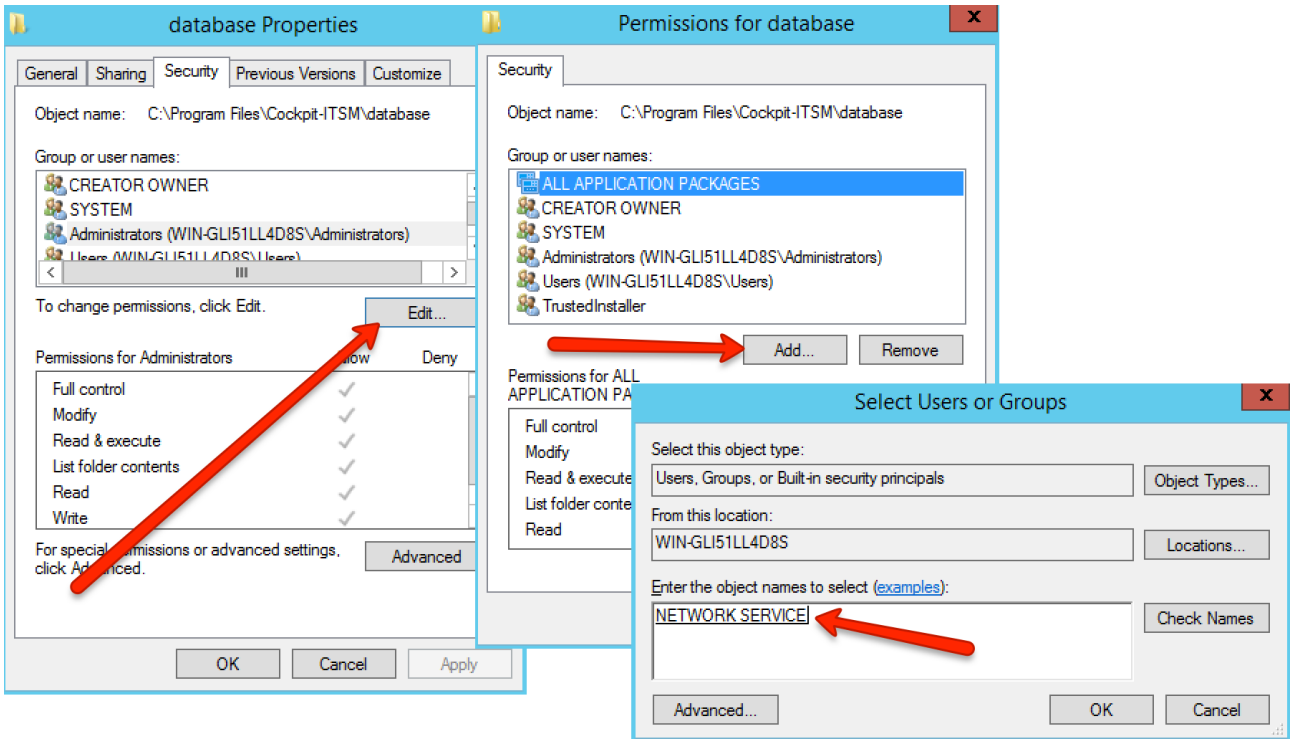
Move "C:\Program Files\MariaDB 10.X\data\mysql" to "C:\koaly\exp\database\mysql".

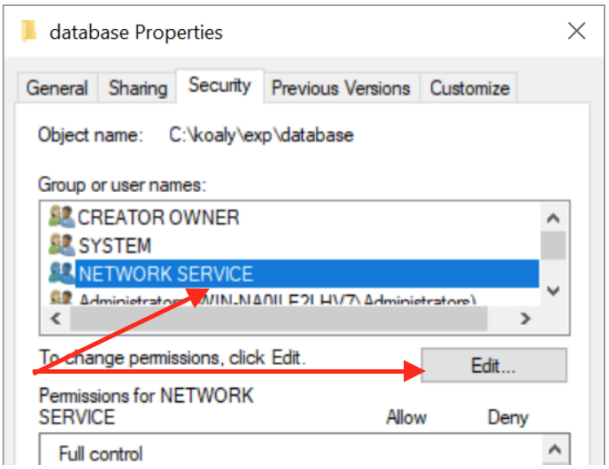
Move "C:\Program Files\MariaDB 10.X\data\performance_schema" to "C:\koaly\exp\database\performance_schema".

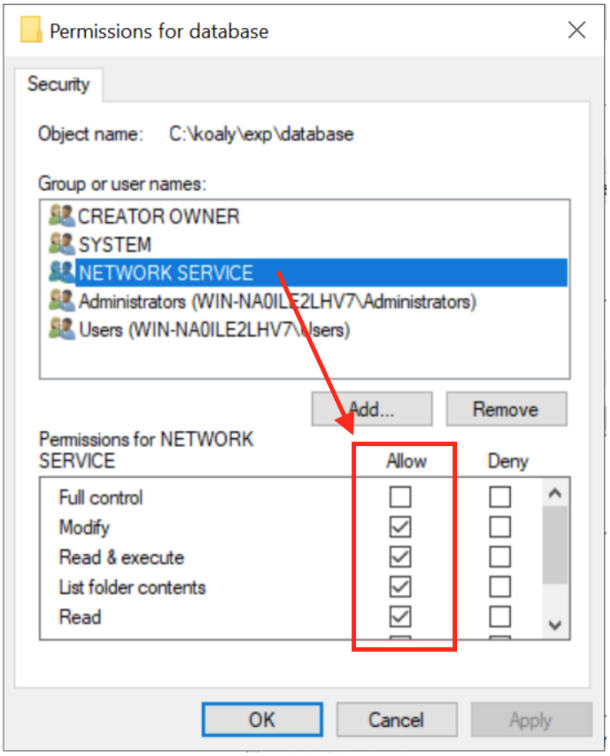
Open "C:\koaly\exp\database" folder properties.



Add "NETWORK SERVICE" user write access.







Open the file "C:\Program Files\MariaDB 10.X\data\my.ini" and add replace its content with the following text.

```
[client]
default-character-set = utf8

[mysqld]
# Set default character set
character-set-server = utf8mb4
character_set_server = utf8mb4
collation_server = utf8mb4_unicode_ci
collation-server = utf8mb4_unicode_ci

datadir = C:/koaly/exp/database/
log-error = C:/koaly/exp/database/error.log

# Try number of CPU's*2 for thread_concurrency
thread_concurrency = 4

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address = 127.0.0.1

# Fine Tuning
max_connections = 800
optimizer_search_depth = 5

# InnoDB

# InnoDB is enabled by default with a 10MB datafile in /var/lib/mysql/.
# Read the manual for more InnoDB related options. There are many!
default_storage_engine = InnoDB
```

```
# you can't just change log file size, requires special procedure
innodb_log_file_size = 256M
innodb_buffer_pool_size = 512M
innodb_log_buffer_size = 32M
innodb_file_per_table = 1

# Binary logs
log-bin = mysql-bin
expire_logs_days = 10
log_bin_trust_function_creators = 1

# Replication

# For the master server
# server-id = 1

# For the slave server
# log-bin
# server-id = 2
# master-host =
# master-port = 3306
# master-user = replication
# master-password =
```

Test start and stop MariaDB server using Windows Management Console.

Check MariaDB log file: "C:\koaly\exp\database\error.log".

Check if there some errors.

Check XtraDB status, it must be started:

```
InnoDB: 10.X.X started; log sequence number XXXXXXXX; transaction id XXX
```

IV. Cockpit IT Service Manager installation

Copy SQL dump (koalyexp.sql) to "C:\koaly\exp\".

Connect MariaDB server.

C:\Program Files\MariaDB 10.X\bin\mysql -u root -p

Create "koalyexp" database.

CREATE DATABASE koalyexp CHARSET utf8 COLLATE utf8_unicode_ci;

Create the MariaDB user "koalymgr" for Cockpit Manager.

CREATE USER 'koalymgr'@'localhost' IDENTIFIED BY 'my_password';
*GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER, CREATE TEMPORARY TABLES, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, EXECUTE ON `koalyexp`. * TO 'koalymgr'@'localhost';*

Create the MariaDB user "koalyprt" for Cockpit ITSM - Portal.

CREATE USER 'koalyprt'@'localhost' IDENTIFIED BY 'my_password';
*GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, EXECUTE, CREATE TEMPORARY TABLES ON `koalyexp`. * TO 'koalyprt'@'localhost';*

Import the SQL dump file.

```
use koalyexp;
source c:/koaly/exp/koalyexp.sql;
```

Quit the SQL client.

```
exit
```

Restart MariaDB.

Check the log file: "C:\koaly\exp\database\error.log".

Delete the file "C:\koaly\exp\koalyexp.sql".

Cockpit ITSM - Manager

I. Prerequisites

The database must be installed and configured before Cockpit Manager.

II. Service installation

Execute the setup program (administration rights necessary): koaly-management-interface-vXX-setup.exe

Hit "Next".

Select "All users".

Modify the default installation directory (C:\koaly\management-interface) if necessary.

Modify the default shortcut directory (Koaly\Koaly Management Interface) if necessary.

Hit "Next".
Hit "End".

Open the installation directory.

> **Option for very high level security system:**
> If you want to use a system-specific encryption key, use "Cockpit Portal installation - System-specific encryption key" documentation.
> 1/ Generate the koaly.key file
> 2/ Copy the koaly.key file to "C:\koaly\management-interface\conf"

Open the service list in the Windows Management Console.

Start the service "Koaly Management Interface".

The service should now be in the state "Started".

III. Firewall

To allow the HTTP traffic through the Windows firewall, you need to create a new rule. Open a command prompt **as administrator** and execute the following command.

netsh advfirewall firewall add rule name="Allow Cockpit ITSM - Manager" dir=in action=allow protocol=TCP localport=8081

> Important: If UAC is active on your machine, just being logged on as administrator does not provide you the necessary rights. You need to right-click the Command Prompt item in the start menu and choose "Run as administrator".

IV. Service configuration

Open a web browser.
Navigate to the following address: https://localhost:8081/ or https://your_server:8081.
Accept the security exception.
Use the default password (admin123) to connect.
Enter the database connection parameters (use "koalymgr" SQL user).
Hit "Next".

Specify the directory or URL that will contain future updates of the Cockpit IT Service Manager components (default is C:\koaly\update).
Specify the client library directory (default: C:\koaly\update; see the chapter "External libraries" for details).

> Note: The update files for each service need to be provided in specific sub-directories. These are displayed on this screen for your information.

Specify the HTTP port the management server shall listen on (default: 8081).
Hit "Next".

Modify the current password.
Save.

The configuration is now saved but not active yet.
Hit "Restart".

Wait until the page is refreshed.

> Note: Do not reload the page at this stage.

Once the page is refreshed, the management service is fully operational. You can review its configuration in the "Parameters" section.

V. Change password of user koalyadm

In the main menu, choose "Tools" and set a password for the user "koalyadm".

Cockpit ITSM - Portal

I. Prerequisites

Cockpit Manager must be installed on the server before Cockpit ITSM - Portal.

II. Service installation

Execute the setup program (administration rights necessary): koaly-exp-portal-vXXX-setup.exe.

Hit "Next".

Select "All users".

Modify the default installation directory (C:\koaly\exp\portal) if necessary.

Hit "Install".
Hit "Next".
Hit "Finish".

> Option for very high level security system:
> If you want to use a system-specific encryption key, use "Cockpit ITSM - Portal installation - System-specific encryption key" documentation.
> 1/ Generate the koaly.key file
> 2/ Copy the koaly.key file to "C:\koaly\exp\portal\conf"

III. Setup without SSL

By default, the portal listens for (unencrypted) HTTP connections on port 80.

To allow the HTTP traffic through the Windows firewall, you need to create a new rule. Open a command prompt as administrator and execute the following command.

netsh advfirewall firewall add rule name="Allow HTTP" dir=in action=allow protocol=TCP localport=80

> Important: If UAC is active on your machine, just being logged on as administrator does not provide you the necessary rights. You need to right-click the Command Prompt item in the start menu and choose "Run as administrator".

IV. Setup with SSL

A. Keystore file generation

In the next step, we need to create a PKCS12 keystore for use by the portal. If your SSL certificate authority does not provide PKCS12 keystore files, you can generate it with the following procedure.

You will need access to an installation of OpenSSL. If you do not want to install OpenSSL on the server, you can install it on any other machine and copy the generated file to the target directory. If you have access to a Linux machine, you can use this as well. Openssl is pre-installed on all major Linux distributions.

We assume the following files are present in the current working directory.
server.crt - PEM format file of CA
server.key - private key
server.ca-bundle - CA bundle file

Concatenate the files to provide a full certification path.
copy server.key+server.crt+server.ca-bundle target.key

The following command will ask you for a keystore password. Please use the same password each time you are asked for it. Don't forget to update the file server.xml with this password if you have not done so already.

Open a command prompt and execute the following command (openssl.exe must be on your PATH).
openssl pkcs12 -export -in target.key -nodes -name tomcat -out tomcat.p12

To finish, move the file tomcat.p12 to the directory C:\koaly\exp\portal\conf\ on your server.

B. Portal configuration

Open the file "C:\koaly\exp\portal\conf\server.xml" in a text editor.

Replace the following lines.

```
            <!-- HTTP (No SSL): Uncomment the following 4 lines -->
        <Connector executor="tomcatThreadPool" URIEncoding="UTF-8" server="Koaly EXP Portal"
                   port="80" protocol="HTTP/1.1"
                   compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript,application/
json,application/xml"
                   compression="on"
                   connectionTimeout="20000"/>

        <!-- HTTP (SSL): Uncomment the following 10 lines -->
        <!--
        <Connector executor="tomcatThreadPool" URIEncoding="UTF-8" server="Koaly EXP Portal"
                   port="8443" protocol="HTTP/1.1" SSLEnabled="true"
                   scheme="https" secure="true"
                   compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript,application/
json,application/xml"
                   compression="on"
                   clientAuth="false" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"

ciphers="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_S
```

```
HA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,T
LS_ECDHE_RSA_WITH_RC4_128_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WI
TH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SH
A256,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA"
                keystoreType="PKCS12"
                keystoreFile="${catalina.base}/conf/tomcat.p12"
                keystorePass="koaly2009"/>
        -->
```

With.

```
        <!-- HTTP (No SSL): Uncomment the following 4 lines -->
        <Connector executor="tomcatThreadPool" URIEncoding="UTF-8" server="Koaly EXP Portal"
                port="80" protocol="HTTP/1.1"
                compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript,application/
json,application/xml"
                compression="on"
                connectionTimeout="20000"
                redirectPort="443"/>

        <!-- HTTP (SSL): Uncomment the following 10 lines -->
        <Connector executor="tomcatThreadPool" URIEncoding="UTF-8" server="Koaly EXP Portal"
                port="8443" protocol="HTTP/1.1" SSLEnabled="true"
                scheme="https" secure="true"
                compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript,application/
json,application/xml"
                compression="on"
                clientAuth="false" sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"

ciphers="TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_S
HA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,T
LS_ECDHE_RSA_WITH_RC4_128_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WI
TH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SH
A256,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA"
                keystoreType="PKCS12"
                keystoreFile="${catalina.base}/conf/tomcat.p12"
                keystorePass="{password}"/>
```

> Note: The {password} is the password of your PKCS12 keystore

> Note: The port 80 (HTTP) is configured to proved automatic redirection to port 443 (HTTPS)

Open the file "C:\koaly\exp\portal\conf\web.xml" in a text editor.

Replace the following lines.

```
<!-- ================== Built In Filter Definitions ===================== -->
<!-- NOTE: An SSI Servlet is also available as an alternative SSI         -->
```

With.

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Protected Context</web-resource-name>
      <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <!-- auth-constraint goes here if you requre authentication -->
    <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
<!-- ================== Built In Filter Definitions ===================== -->
<!-- NOTE: An SSI Servlet is also available as an alternative SSI         -->
```

> Note: This insures HTTP requests are redirected to the HTTPS port.

C. Firewall

To allow HTTP and HTTPS traffic through the Windows firewall, you need to create a new rule. Open a command prompt as administrator and execute the following commands.

netsh advfirewall firewall add rule name="Allow HTTP" dir=in action=allow protocol=TCP localport=80
netsh advfirewall firewall add rule name="Allow HTTPS" dir=in action=allow protocol=TCP localport=443

> Note: The port 80 (HTTP) is opened to allow automatic redirection to port 443 (HTTPS).

> Important: If UAC is active on your machine, just being logged on as administrator does not provide you the necessary rights. You need to right-click the Command Prompt item in the start menu and choose "Run as administrator".

V. Database configuration

Connect to Cockpit Manager in a web browser (default address: https://localhost:8081/).
In the main menu, choose "Portals".
Hit "Add".

Enter the required information.

> Notes:
> The portal ID is a unique identifier (0-N) for each portal in a Cockpit IT Service Manager instance.
> The description is a unique name for each portal in a Cockpit IT Service Manager instance (easier to remember than an ID).

If it's the first portal of a new installation, set:

- Portal ID: 0
- Copy: 0 - To be configured

Hit "Save".

VI. Technical settings

Select the tab "Technical settings".

Enter the required information.

> Notes:
> Use "koalyprt" SQL user for database connection parameters
> Storage: Please enter the document directory you created earlier
> The default directory is C:\koaly\exp\documents
> JMS parameters: If this portal is the main portal:
> Check the option "Main portal"
> Specify a listen address:
> if you use a single server for your Cockpit IT Service Manager instance you can use local address (127.0.0.1)
> if you use several servers for your Cockpit IT Service Manager instance you must use a public address
> if you want to listen on all interfaces, use the address 0.0.0.0
> Specify a listen port (default: 61616)
> JMS parameters: If this portal is not the main portal:
> Uncheck the option "Main portal"
> Specify the main portal's listen address
> Specify the main portal's listen port

VII. Functional settings

Select the tab "Functional settings".

Activate the desired modules and options.

Hit "Save".

You be redirected to the list of portals installed on this machine. Note that portals installed on other machines will be displayed but can only be modified by their respective Manager.

VIII. Start the service

In the portal list, click on the "Control" action for the newly installed portal.

Select the tab "Control".

The status should be "STOPPED".

Hit "Start".

Select the tab "Logs".

Select the file "koaly_exp_error.log".

There should not be any errors at this point.

IX. License

A license file is needed for each Cockpit IT Service Manager instance. This license contains a list of physical addresses of servers authorized to run the portal.

For each portal, get the network physical address.

C:\>ipconfig /all

Send the list of physical addresses to license@cockpit-itsm.com. Cockpit IT Service Manager support will send you a system-specific license file.

X. Test

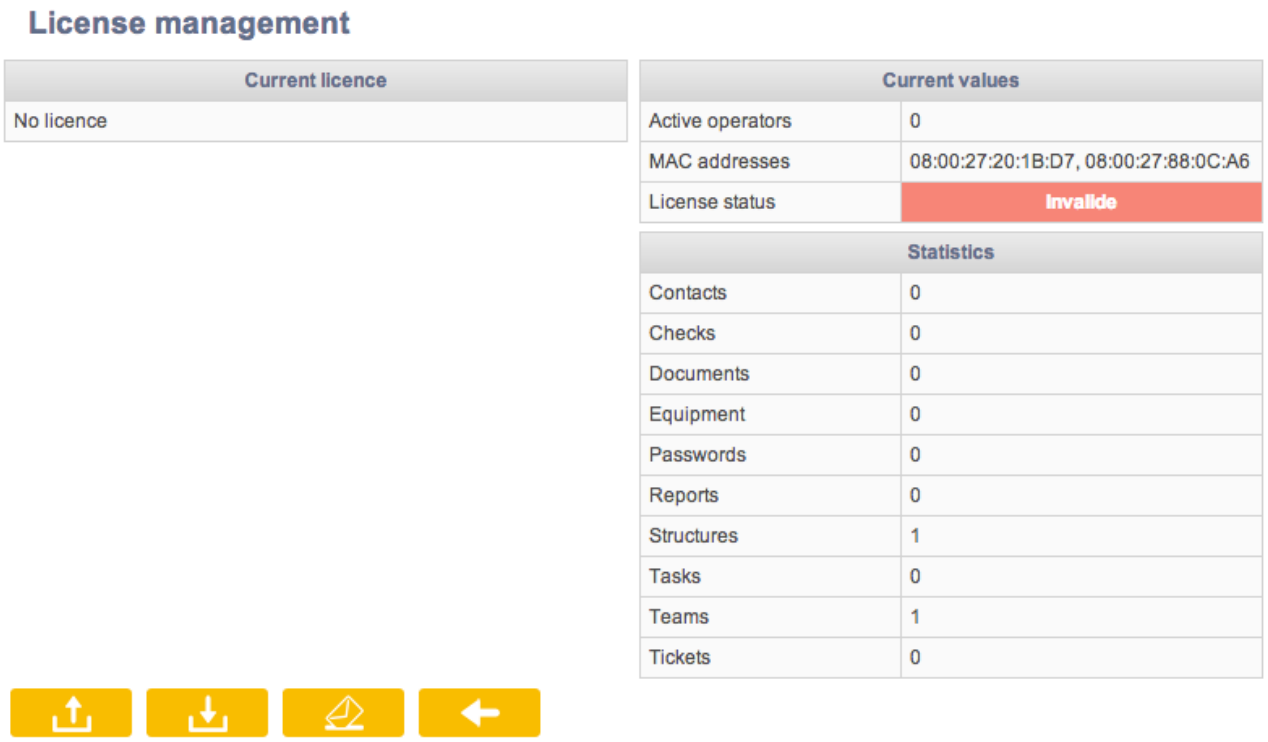
Connect to the Cockpit ITSM - Portal.

http://yourserver

User: koalyadm

Password: *******

Once connected, you will be redirected to the license management panel.



Upload the license file.

Search engine - Solr

I. Prerequisites

Cockpit ITSM - Portal must be installed on the server before the search engine.

II. Service installation

If the server does not access the internet, download Solr:

1. Check the Solr version to install in the file "c:\koaly\exp\portal\solr\solr_version.txt".
2. Download the version on "https://archive.apache.org/dist/lucene/solr/X.X.X/solr-X.X.X.tgz".
3. Copy the "solr-X.X.X.tgz" file on the directory "c:\koaly\exp\portal\solr\".

Open a PowerShell windows as administrator and execute the following commands.

```
Get-ExecutionPolicy
Set-ExecutionPolicy -ExecutionPolicy AllSigned -Scope Process
```

If confirmation is requested, please confirm the operation by replying "Yes". This will allow the execution of signed PowerShell scripts for the remainder of this PowerShell session.

Change the directory to the portal installation directory.

```
cd c:\koaly\exp\portal\solr
```

Set the JAVA

```
$Env:JAVA_HOME = "c:\koaly\exp\portal\rt"
```

Execute the installation script.

```
.\install.ps1
```

If confirmation is requested, please confirm the operation by replying Run once.

The script downloads, installs and starts Solr.
You should see the following message once the installation is complete.

```
Installation succeeded, Solr is ready for use.
```

Solr is installed into %PROGRAMFILE%.
You can now close the PowerShell session:

```
exit
```

III. Service status

Connect the portal.

Go to "Administration > Indexing".

Check the status, it must be "Online".

Document end