cockpit
IT Service Manager

Cockpit ITSM - System-specific encryption key

Technical specification

Table of contents

Introduction

By default, all sensitive information in the Cockpit IT Service Manager database, such as passwords, are encrypted using a secret key contained in the application binaries. This means that an attacker with access to an EXP database and the application binaries will be able to gain full access to the sensitive information stored in this database. Hence, the protection level of the sensitive data depends on the protection level of the database.

If the protection of the database cannot be guaranteed or is not considered sufficient, it is possible to use a system-specific encryption key. Without this key, it is not possible to access any sensitive information stored in the Cockpit IT Service Manager database. To further strengthen security, this key can be bound to a fixed set of MAC addresses. The application will only accept such a key if one of the active MAC addresses of the machine running it matches one of the addresses specified in the key file.

If no MAC address is specified for a key, it will work on any machine. Note that it if you choose to do this, you need to make sure that the configuration directories containing the key file are protected accordingly.

> Warning:
> Using a system-specific key means that the protected data will be inaccessible without it. This means that the loss of the key file means the loss of all this data. It must be backed up accordingly.
> Another important impact to consider is that it is currently not possible to change the encryption key for an existing EXP database. This means you need to generate the key before a system is installed.

Key generation

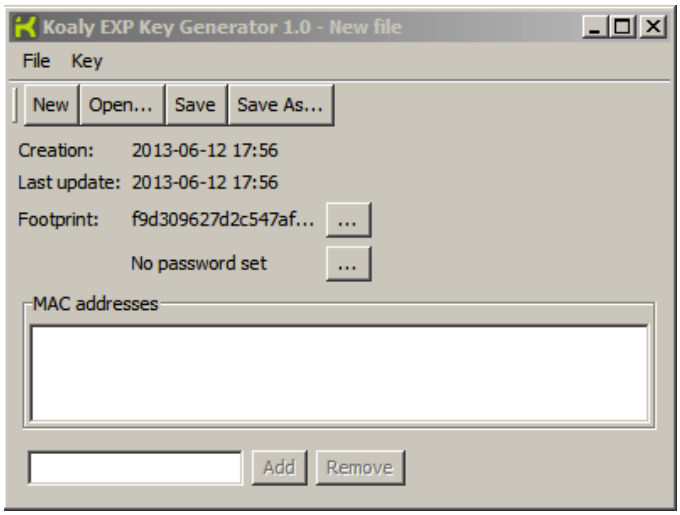
I. Key Generator installation

Download the “Cockpit IT Service Manager Key Generator”.
https://download.cockpit-itsm.com/tools/cockpit/itsm-cockpit-key-generator-V100-setup.exe

Execute the setup program (administration rights necessary): itsm-cockpit-key-generator-V100-setup.exe

Select “Next”.
Select “All users”.
Modify the default installation directory (C:\koaly\key-generator) if necessary.
Modify the default shortcut directory (Koaly\Koaly Key Generator) if necessary.
Select “Next”.
Select “Finish”.

Launch the Generator (Start\Koaly\Koaly Key Generator)
It can be used to create a key file as well as add or remove MAC addresses from an existing key file.



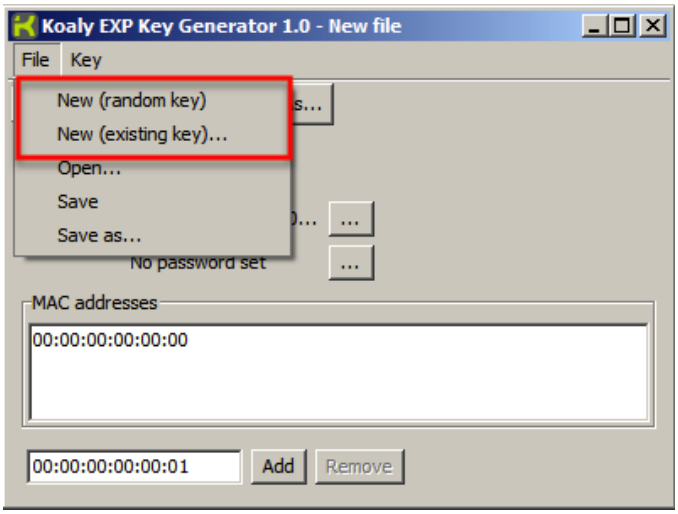
II. Create a new key file

Quick method:

To generate a new key file, simple start the Cockpit IT Service Manager Key Generator application, optionally add a set of MAC addresses, define a password and then save the file (file name: koaly.key)
This default method will generate a random key.

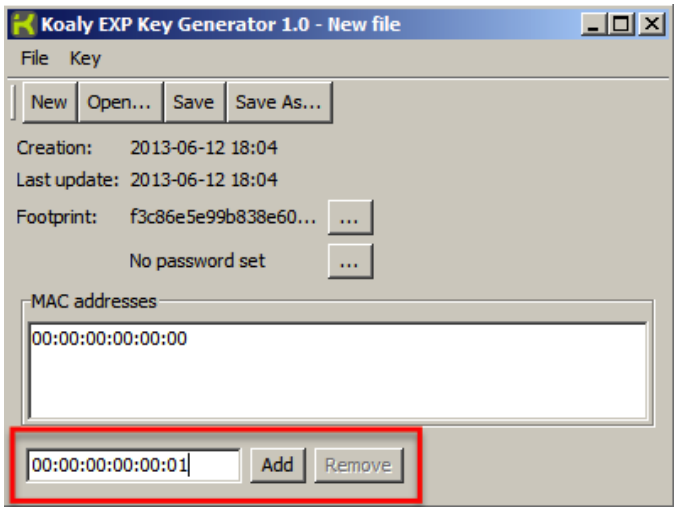
The key:

- If you want to create a file with a random key, use File / New (random key)
- If you want to specify a key explicitly, use File / New (existing key). You will be asked to enter a key in the form of a string of 32 ASCII characters.



MAC addresses:

- If you want to add a set of authorized MAC addresses, use the MAC addresses management menu.



Password:

To protect a key file from modification, a password may be assigned. Modifying a password-protected key file is only possible after typing the correct password.

III. Add a new machine to an existing key file

To add a new machine to an existing system, its MAC address needs to be added to the koaly.key file. This can be done by loading the file in the Cockpit IT Service Manager Key Generator application. After typing the key password, the new MAC address can be added. After saving the new key file, it needs to be deployed to all services on this machine as described above.

Note that is recommended, albeit not necessary, to distribute the modified key to all services in the systems (managers, portals and engines).

Key installation

I. Cockpit IT Service Manager - Manager

To install a key for a new system, you may use the following procedure:

- After installing the binaries for the Cockpit IT Service Manager - Manager
- Generate the koaly.key file
- Copy the koaly.key file to the configuration directory (default: c:\koaly\management-interface\conf)
- Continue the normal installation procedure for the Manager

Once the Cockpit IT Service Manager - Manager is configured, change the password of the user koalyadm through the “Tools” menu in Cockpit IT Service Manager - Manager.

II. Cockpit IT Service Manager - Portal

For each portal added to the system, you need to copy the key file to the corresponding configuration directory as follows:

- After installing the Cockpit IT Service Manager - Portal binaries
- Generate the koaly.key file
- Copy the koaly.key file to the configuration directory (default: c:\koaly\exp\portal\conf)
- Continue the installation procedure for the Portal

III. Cockpit IT Service Manager - Engine

For each engine added to the system, you need to copy the key file to the corresponding configuration directory as follows:

- After installing the Cockpit IT Service Manager - Engine binaries
- Generate the koaly.key file
- Copy the koaly.key file to the configuration directory (default: c:\koaly\exp\engine\conf)
- Continue the installation procedure for the Engine

Document end