HiCrypt™ 2.0

Configuration with floating license (with a hardware USB dongle)

digitronic
computersysteme gmbh

Oberfrohnaer Straße 62
D-09117 Chemnitz
Phone: +49 371 81539-0
Fax: +49 371 81539-900
Internet: www.digitronic.net
Mail: info@digitronic.net

Author: digitronic
Revision: 1.1
Release: August 27th 2021

TABLE OF CONTENTS

Table of contents

CHAPTER 1

1 Introduction

This document describes how to proceed when setting up HiCrypt™ 2.0 using floating licenses with a WIBU CodeMeter USB dongle.

In order to make the licenses available in the network, a license server must first be installed to which the USB dongle can then be plugged. After that you can HiCrypt™ 2.0 can be installed on any system in the network.

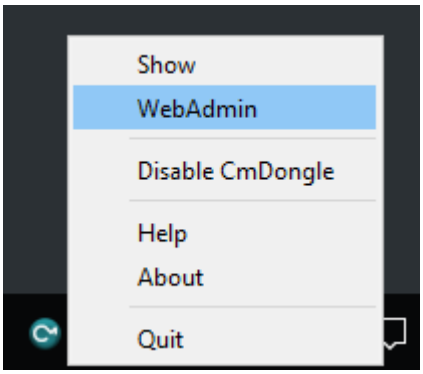
CHAPTER 2

2 Configuration of license server

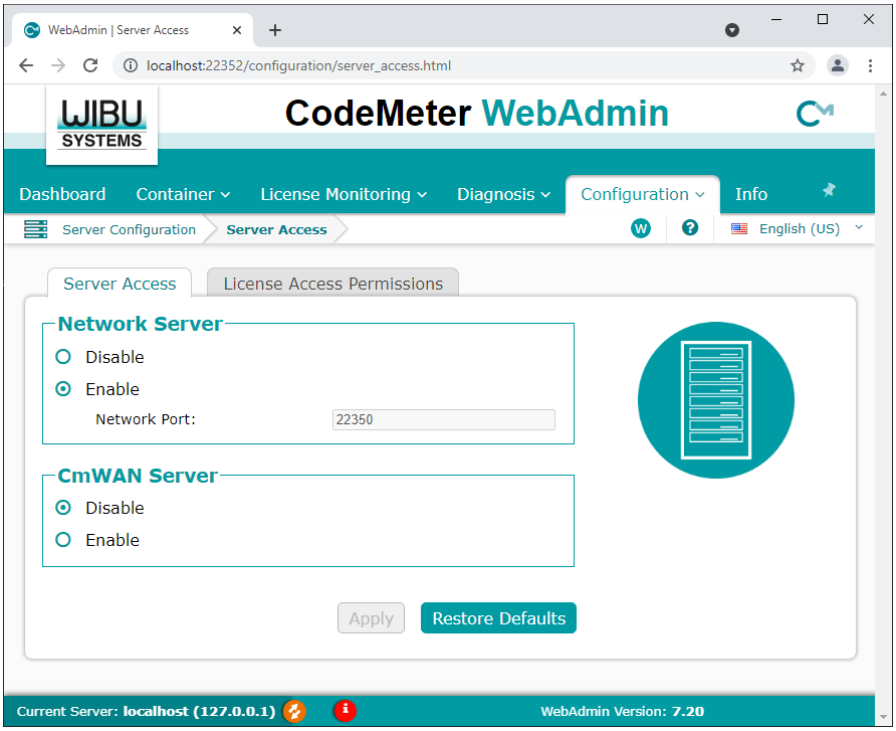
The CodeMeter Runtime environment must be on the system that is to serve as the license server to be installed. Any server or client PC can be used for this, as long as it is always accessible in the network and has a USB port.

The latest version can be found in the ***Software for Users*** section at https://www.wibu.com/.

After installing the CodeMeter Runtime, the CodeMeter Control Center icon is in the Find Systray. The WebAdmin must now be started by right-clicking on the icon, as seen in the following figure.



Enable the ***Network Server*** in ***WebAdmin*** under ***Settings*** -> ***Server Configuration*** -> ***Server Access*** and confirm with ***Apply***.



The licenses for all CodeMeter dongles connected to this system are then made available in the network, which are released for use in the network.

Now you can connect the supplied USB dongle to the license server.

CHAPTER 3

3 Configuration of HiCrypt™ 2.0

3.1 Installation

3.1.1 CodeMeter Runtime

HiCrypt requires the ***CodeMeter User Runtime for Windows*** in the 32-bit version. This must be installed before the installation of HiCrypt. The current version can be downloaded from the ***Software for Users*** section at https://www.wibu.com/. The installation does not have to be adjusted.

3.1.2 HiCrypt™ 2.0

The HiCrypt.msi setup is carried out for the installation of HiCrypt. A restart is then required.

As of version 2.4.4, the license server can no longer be specified during setup. The specification of the MSI parameter ***HICRYPT_LICENSE_SERVER*** is also no longer supported. According to this, the license server is determined by default by means of broadcast.

If it is necessary to explicitly specify the license server to be used, this is configured with the ***CodeMeter Control Center***, which is installed with the CodeMeter Runtime. Further information can be found in the CodeMeter documentation.

3.2 Terminalserver

In order not to exceed the number of licenses, two parameters should be configured in the registry on a terminal server. These are described in the Frequently Asked Questions (FAQs for short) at https://hicrypt.com/en/faq/.

3.2.1 How can I define the users being allowed to use HiCrypt™ 2.0?

By default HiCrypt™ 2.0 starts automatically for all users after logging on to the system. This applies to all users of a workstation.

If more users use the same computer or if you even use a terminal server than you can limit the user group who is allowed to use HiCrypt™ 2.0. For that a value in the Windows Registry is used which defines the user group who is allowed to use HiCrypt™ 2.0.

Please follow the instructions below to give the two example groups "HiCrypt-User" and "HiCrypt-Manager" access to HiCrypt™ 2.0 (you need to have administrative privileges on this computer to proceed).

- Start the Windows Registry.
- Open the key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HiCryptSvc\Parameters and create a "Multi-String-Value" with the name AllowedUserGroups.
- Enter the two groups "HiCrypt-User" and "HiCrypt-Manager" – each in a separate line. For that use the format for Down Level-Logon-Names (DOMAIN\GroupName) or the UPN format (GroupName@DNSDomainName.com).
- Reboot the computer for the changes to take effect.

3.2.2 How to prevent HiCrypt™ 2.0 to be started by users not being allowed to use the software?

After you have limited the group of users who are allowed to use HiCrypt™ 2.0 as described above you can use another value in the Windows Registry to avoid that HiCrypt™ 2.0 is started for all non-authorized users.

Please follow the instructions below (you need to have administrative privileges on this computer to proceed).

- Start the Windows Registry.
- Open the key HKEY_LOCAL_MACHINE\Software\digitronic\HiCrypt (32bit) or the key
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\digitronic\HiCrypt (64bit) and create a "DWORD-Value (32-Bit)" with the name SilentQuitIfUserIsNotInAllowedGroups.
- Set its value to 1 to prevent the start of HiCrypt™ 2.0 for users who are not authorized to use HiCrypt™ 2.0.
- Reboot the computer for the changes to take effect.

Please note: this configuration is available since HiCrypt™ 2.0 version 1.0.7.